भारतीय मानक

Indian Standard

IS/ISO/IEC 27402 : 2023

साइबर सुरक्षा — आईओटी सुरक्षा और गोपनीयता — डिवाइस आधारभूत अपेक्षाएँ

Cybersecurity — IoT Security and Privacy — Device Baseline Requirements

ICS 35.030

© BIS 2024
© ISO/IEC 2023

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुर शाह ज़फर मार्ग, नई दिल्ली - 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110002
www.bis.gov.in www.standardsbis.in

September 2024 **Price Group 9**

Information Systems Security and Privacy Sectional Committee, LITD17

NATIONAL FOREWORD

This Indian Standard which is identical to ISO/IEC 27402 : 2023 'Cybersecurity — IoT security and privacy — Device baseline requirements' issued by the International Organization Standardization (ISO) and International Electrotechnical Commission (IEC) was adopted by the Bureau of Indian Standards on the recommendations of the Information Systems Security and Privacy Sectional Committee and approval of the Electronics and Information Technology Division Council.

The text of ISO/IEC standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions and terminologies are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'; and

b) Comma (,) has been used as a decimal marker while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards, which are to be substituted in their respective places, are listed below along with their degree of equivalence for the editions indicated. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary	IS/ISO/IEC 27000 : 2018 Information technology — Security techniques — Information Security management systems — Overview and vocabulary (*first revision*)	Identical
ISO/IEC 27400 : 2022 Cybersecurity — IoT security and privacy — Guidelines	IS/ISO/IEC 27400 : 2022 Cybersecurity — IoT security and privacy — Guidelines	Identical
ISO 31000 : 2018 Risk management — Guidelines	IS/ISO 31000 : 2018 Risk management — Guidelines (*first revision*)	Identical

Contents

Page

Introduction ..... **iv**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 3

4 Overview **3**

5 Requirements **4**
5.1 Requirements for IoT device policies and documentation 4
5.1.1 Risk management 4
5.1.2 Information disclosure 5
5.1.3 Vulnerability disclosure and handling processes 6
5.2 Requirements for IoT device capabilities and operations 6
5.2.1 General 6
5.2.2 Configuration 7
5.2.3 Software reset 7
5.2.4 User data removal 8
5.2.5 Protection of data 8
5.2.6 Interface access 10
5.2.7 Software and firmware updates 11
5.2.8 User notifications 12

Annex A (informative) **Risk management guidance** **13**

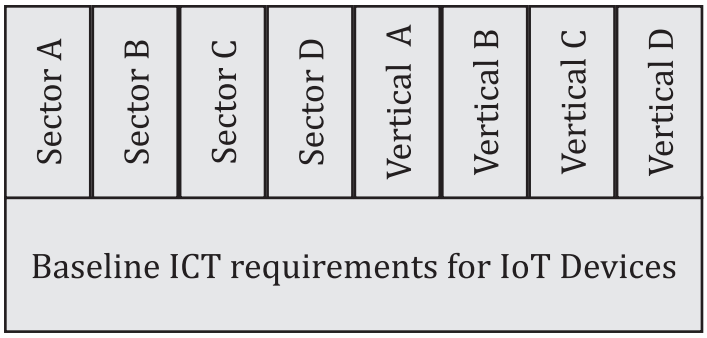
Bibliography **15**

Introduction

With the increasing number of Internet of Things (IoT) devices and increasing reliance on such devices, the security and privacy risks relating to those "things" are expected to grow. Their widespread deployment in networks and systems make them easy and prime targets for cyber attacks.

This document provides a baseline set of information and communication technologies (ICT) requirements so that IoT devices are able to support security and privacy controls. A risk assessment is critical to develop a risk treatment plan that identifies the necessary IoT device features and countermeasures. The management of systems which use IoT devices depends upon the capabilities of those devices (among other factors).

Broadly speaking, this document addresses ICT requirements for IoT devices that are made available to the market. The requirements in this document are intended as a baseline, upon which vertical markets (such as health, financial services, industrial, consumer electronics and transportation) can build additional requirements for the expected use and risks of IoT devices in their applications, as depicted in Figure 1. In addition to this document, various sectors (e.g. private/industrial, public, defence, national security) and vertical markets have sector- or vertical-specific requirements, for example those found in ETSI EN 303 645[11] for consumer devices and the IEC 62443 series for industrial devices and systems. While this document can provide requirements for a conformity assessment scheme, it is expected that stakeholders for specific sectors and vertical markets will develop consensus around requirements specific to their contexts, building "on top" of this document. Subsequently, conformity assessment programmes can be developed around those specific sectors and vertical markets. This document would be effectively integrated into such programmes while providing a common set of baseline requirements.



NOTE Additional requirements can be developed or required by specific sectors and vertical markets.

Figure 1 — Relationship between baseline requirements in this document and potential additional requirements

As the complex technical landscape of IoT devices evolves, this document can support a scalable globally harmonized approach to the baseline security and privacy requirements and inform technical policy and regulatory initiatives.

Indian Standard

CYBERSECURITY — IOT SECURITY AND PRIVACY — DEVICE BASELINE REQUIREMENTS

1 Scope

This document provides baseline ICT requirements for IoT devices to support security and privacy controls.

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

ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*

ISO 31000:2018, *Risk management — Guidelines*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27400, ISO 31000, 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/

3.1.1
identifier
information that unambiguously distinguishes one entity from another one in a given identity context

[SOURCE: ISO/IEC 23093-1:2022, 3.2.7]

3.1.2
user interface
set of all components of an interactive system that provide information and controls for the user to accomplish specific tasks with the interactive system

[SOURCE: ISO 9241-110:2020, 3.10]

3.1.3
internet of things
IoT
infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2021, 3.2.4]

3.1.4
IoT system
system providing functionalities of *internet of things (IoT)* (3.1.3)

Note 1 to entry: An IoT system can include, but is not limited to, *IoT devices* (3.1.5), *IoT gateways* (3.1.7), sensors, and actuators.

Note 2 to entry: Conventional IT devices such as smartphones and laptops can form part of an IoT system.

Note 3 to entry: IoT systems also include cloud and network connectivity.

[SOURCE: ISO/IEC 20924:2021, 3.2.9, modified — notes 2 and 3 to entry have been added.]

3.1.5
IoT device
entity of an *internet of things (IoT) system* (3.1.4) that interacts and communicates with the physical world through sensing or actuating

Note 1 to entry: An IoT device can be a sensor or an actuator.

Note 2 to entry: An IoT device, in this context, is an assembled device usable for its intended IoT functions without relying on being embedded or integrated into any other product.

Note 3 to entry: IoT devices generally interact via communication interfaces.

[SOURCE: ISO/IEC 20924:2021, 3.2.6, modified — notes 1, 2 and 3 to entry have been added.]

3.1.6
IoT device developer
entity that creates an assembled final *internet of things (IoT) device* (3.1.5)

Note 1 to entry: "Final" in this definition means the stage of delivery to the IoT service developer in the assemble process.

[SOURCE: ISO/IEC 27400:2022, 3.4]

3.1.7
IoT gateway
entity of an IoT system that connects one or more proximity networks and the IoT devices on those networks to each other and to one or more access networks

[SOURCE: ISO/IEC 20924:2021, 3.2.8]

3.1.8
trusted computing base
TCB
totality of protection mechanisms within a computer system, including hardware, firmware and software, the combination of which is responsible for enforcing a security policy

3.1.9
cryptographic module
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

3.1.10
critical security parameter
CSP
security-related information whose disclosure or modification can compromise the security of a *cryptographic module* (3.1.9)

Note 1 to entry: A CSP can be plaintext or encrypted.

Note 2 to entry: In the example, "certificates" refers to private keys matching public keys inside certificates.

EXAMPLE 1 Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

EXAMPLE 2 Configuration settings required for initialization.

[SOURCE: ISO/IEC 19790:2012, 3.18, modified — note 2 to entry and example 2 have been added.]

3.1.11
sensitive security parameter
SSP
critical security parameters (3.1.10) and public security parameters

[SOURCE: ISO/IEC 19790:2012, 3.110]

3.1.12
factory default
state of the device after factory reset or after final production/assembly

Note 1 to entry: This includes the physical device and software (including firmware) that is present on it after assembly.

3.1.13
fail-safe mode
device or feature which, in the event of failure, responds in a way that causes no harm, or minimizes the harm, to other devices, and causes no danger, or minimizes the danger, to personnel

[SOURCE: ISO 25197:2020, 3.32]

3.2 Abbreviated terms

API application programming interface

ASLR address space layout randomization

CPU central processing unit

CSP critical security parameter

ICT information and communication technologies

IoT internet of things

PIN personal identification number

PSP public security parameter

RoT root of trust

TCB trusted computing base

SWID software identification

XML extensible markup language

4 Overview

IoT systems bring security and privacy risks, and ISO/IEC 27400 provides general information and guidance about these risks and threats to security and privacy. To address these risks, users (organizations and consumers) should implement appropriate controls, which are also detailed in

ISO/IEC 27400. These controls cannot be implemented if the IoT devices do not have the supporting functionality (process policies, capabilities etc.)

The IoT system developers are expected to develop their own requirements and seek IoT devices that support them. This document provides baseline ICT requirements for IoT devices. In many cases, additional requirements will be imposed or are expected to address the security and privacy risks of specific vertical markets or higher risk environments.

5 Requirements

5.1 Requirements for IoT device policies and documentation

5.1.1 Risk management

5.1.1.1 Requirements

5.1.1.1.1 IoT devices shall have documentation recording the results of a risk assessment process performed at the IoT device level in the context of a risk assessment at the system level.

5.1.1.1.2 The risk assessment process shall take into account intended outcomes for the intended use case.

5.1.1.1.3 The risk assessment process shall also take into account the needs and expectations of interested parties (e.g. those parties on networks to which the IoT device is connected), including physical and logical undesired effects.

NOTE 1 Risk assessment techniques can be found in IEC 31010 and ISO/IEC 27005.

NOTE 2 IoT device developers usually perform the risk assessments and produce the risk treatment plans.

5.1.1.1.4 The risk assessment shall take into account that IoT devices can be constrained (e.g. limited battery, little memory, "weak" CPU), which informs the risk treatment process.

5.1.1.1.5 Risk assessment and treatment processes shall be defined and applied as follows:

a) determine if separate risk assessment and treatment processes are necessary for different products;

b) select appropriate risk treatment options, taking account of the risk assessment results;

NOTE 1 Sector- or vertical market-specific standards can be used in addition to this document. Such a standard can provide a risk assessment and/or risk treatment plan specific to the sector or vertical market. Complying with such standards can be used to satisfy requirements in this document.

c) determine all controls that are necessary to implement the risk treatment option(s) chosen;

d) identify all security and privacy features of the IoT device from the controls identified in c) above;

NOTE 2 IoT device developers can design features as required or identify them from any appropriate source, such as an industry standard or sector guidance.

e) compare the features identified in d) above with those in 5.2, and verify that no necessary features have been omitted;

NOTE 3 5.2 contains a list of baseline features. Users of this document are directed to 5.2 to ensure that no requirements are overlooked.

NOTE 4 The features listed in 5.2 are not exhaustive. Additional features and controls can be necessary based on specific vertical market segments or to address higher-risk use cases.

f) produce a statement of applicability that contains the necessary features [see steps d) and e)] and justification for inclusions and the justification for exclusions of features from 5.2;

g) if other standards related to device requirements are used, implement the requirements of those standards after steps a) through to f);

h) formulate a risk treatment plan;

i) inform the risk owner of the risk treatment plan and any residual risks, or where applicable, obtain their approval of the plan and acceptance of the residual risks.

5.1.1.1.6 IoT devices shall implement the features and controls identified as necessary in its statement of applicability, as well as features and controls identified in 5.1.1.1.5**,** step g).

5.1.1.1.7 The documentation shall be available for the supported lifetime of the product.

5.1.1.2 Additional recommendation(s)

The risk assessment and treatment processes should follow a widely-accepted method such as the one given in ISO 31000. For additional guidance on using ISO 31000, see Annex A.

5.1.1.3 Additional information

Interested parties, such as IoT device developers, system integrators, importers, retailers or regulatory bodies can perform such risk assessments.

IoT devices can contain security and privacy features and controls identified from any source such as sector- or vertical market-specific standards as well those defined in this document. IoT devices may contain additional controls other than those identified as necessary by the risk assessment.

5.1.2 Information disclosure

5.1.2.1 Requirements

5.1.2.1.1 IoT devices shall have user documentation that lists the features that the IoT device provides to support controls for security and privacy, making it clear if any of the IoT device requirements in 5.2 are not included.

5.1.2.1.2 Such information shall be publicly available for the period of time the IoT device is supported.

5.1.2.1.3 IoT devices shall be covered by a security support policy and other supporting documentation wherein users are made aware in advance of when security updates will be discontinued.

5.1.2.2 Additional recommendation(s)

The requirements 5.1.2.1.1 to 5.1.2.1.3 should first be provided at the time of sale.

Guidance should be made available to the user post-purchase, possibly as part of the installation process, highlighting future IoT device events (such as updating software) and offering a means for the user to receive future communications.

The period of time when support is provided, as defined in the IoT device documentation, should be appropriate relative to the risks and to the expected lifetime of the product. Changing announced support periods should be avoided as doing so can disrupt the planning and operational cycles of users.

Device documentation should include information on how users can discover if support periods have been subsequently changed.

Clear and understandable information about the user's responsibilities to set up and maintain security and privacy in using the device should be provided.

All licensing agreements with users should clearly define the scope of security and privacy controls and rights during the use of the product, including any data collected during this period. These agreements should be provided in clear and easy to understand language.

Dependency information about third-party software components relevant for IoT device security should be provided. This information can be provided in a machine-readable format. Software identification (SWID) tags (see ISO/IEC 19770-2) can be used to identify software components.[16]

5.1.2.3 Additional information

Communication to the user can be done via an online reference, in a mobile application, in printed documentation for the IoT device and/or given on a label on the packaging. More than one method can be used.

Many different people can interact with, or be sensed by, any specific IoT device. The same person can interact with the IoT device in several different roles, e.g. as purchaser, installer, active user of functionality and passive target of sensing. When planning and executing communications with users, it is essential to be clear and accurate about the target of each communication and make it easy for users to access those communications both in role-specific and all-roles-for-one-person perspectives.

Communication can include a minimum period of support (in addition to the required communication on discontinuing updates).

5.1.3 Vulnerability disclosure and handling processes

5.1.3.1 Requirements

5.1.3.1.1 IoT devices shall have documentation that defines the vulnerability disclosure and handling processes that will apply for the supported lifetime of the device.

5.1.3.1.2 Vulnerability disclosure and handling processes shall include, at a minimum, a capability to receive reports of potential vulnerabilities from the public.

5.1.3.2 Additional recommendation(s)

Requirements 5.1.3.1.1 and 5.1.3.1.2 should be implemented in accordance with ISO/IEC 29147 (vulnerability disclosure) and ISO/IEC 30111 (vulnerability handling processes).

5.2 Requirements for IoT device capabilities and operations

5.2.1 General

This clause includes IoT device features to be used with a risk assessment and treatment process in accordance with 5.1.1.

The required IoT device features in this document are included because they are suitable for a baseline standard. Each of the requirements in 5.2 are broadly applicable, technically feasible, impactful and can be assessed.

5.2.2 Configuration

5.2.2.1 Requirements

5.2.2.1.1 If the configuration settings of the IoT device can be modified, only authorized entities shall be able to modify the configuration settings of the IoT device.

NOTE Authorized entities can be a person or another device.

5.2.2.1.2 If IoT devices are capable of changing the configuration of IoT and other devices, they shall only be capable of making such changes when authorized.

5.2.2.2 Additional recommendation(s)

A procedure to update or change configuration settings should also include:

a) a way for authorized entities to transfer configuration data to the IoT device and store it on the device in validated data structure and/or data format;

b) a way to validate the integrity of the transmitted configuration settings before use;

c) a means for secure transmission of the settings including validation of the source of the update;

d) a way to confirm the settings have been successfully updated.

5.2.2.3 Additional information

Depending on device constraints, authorization for modifying configuration settings may be granted in different ways. Some examples include: having separate user roles as in modern operating systems, having physical access to the device (e.g. being able to press the “reset” button), being able to perform certain action(s) in a particular way (e.g. irradiate devices with a specially modulated signal on a specific frequency). The examples given here are for illustration purposes and are not exhaustive.

5.2.3 Software reset

5.2.3.1 Requirements

5.2.3.1.1 If IoT devices have the capability to be reset, that process shall be secure.

5.2.3.1.2 This capability shall only be executable by an authorized entity.

5.2.3.2 Additional information

Sometimes a vulnerability is remedied by changing the configuration, and by reverting to the factory defaults after such a remedy, the vulnerability can become exploitable again. An example of such a scenario is changing the current configuration to prevent the device from using cypher suites that are deemed insecure. The factory default can allow all cypher suites, so restoring to factory default in this scenario would expose vulnerabilities again.

This function can sometimes be combined with 5.2.4, so that configuration reset and user data removal can be performed in one action by an authorized entity. IoT device configuration and user data are sometimes combined or difficult to separate.

5.2.4 User data removal

5.2.4.1 Requirements

5.2.4.1.1 If the IoT device stores user data, it shall provide a function for deleting appropriate user data stored on the device in any type of memory.

5.2.4.1.2 The function shall be restricted to authorized entities only.

5.2.4.2 Additional recommendation(s)

The user should be provided with a notification that their data has been securely removed if the device is able to do so.

5.2.4.3 Additional information

User data may include personal data, user configuration data and cryptographic material such as keys.

Some IoT devices may implement this functionality by deleting all data for a group of users (perhaps even all data for all users). Deletion of more than the required data for a single user can be an acceptable means of complying with this requirement. However, this can result in user data being stored for longer than required to serve its purpose. This should therefore only be done with reasonable justification.

User data are often stored in other parts of the IoT system (e.g. in mobile applications and the cloud), and users expect that removal applies to all parts of the IoT system, not just the device itself.

5.2.5 Protection of data

5.2.5.1 Requirements

5.2.5.1.1 IoT devices shall be capable of protecting the data they store and transmit from unauthorized access, modification and disclosure.

5.2.5.1.2 This shall include configuration settings, identifying data, user data, event logs and sensitive security parameters.

5.2.5.1.3 IoT devices shall be capable of protecting their software (including firmware) from unauthorized access and modification.

5.2.5.1.4 IoT devices shall use cryptography (e.g. encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of data requiring protection from being compromised.

NOTE International and other globally recognized standards can be used for cryptography requirements.

5.2.5.2 Additional recommendation(s)

5.2.5.2.1 General

When IoT devices are started up, they should check the integrity and authenticity of the software and/or firmware and enforce security controls. If the IoT device fails these checks, it should:

— notify the user of any violation,

— render itself inoperable,

— operate in a fail-safe mode that provides security protection, or

— initiate device recovery if recovery actions can be performed with integrity.

Upon first installation or maintenance, IoT devices should set themselves to secure default configurations. User configuration options should prevent users from choosing insecure configurations or provide a warning.

If capable, IoT devices should have the ability to provide compartmentalization.

IoT devices should use function modules to restrict access to system resources, which should only be granted to authorized entities.

Trusted computing bases (TCB) should be kept as small as possible to minimize the surface that is exposed to attackers and to reduce the probability that a bug or feature can be used to circumvent security protections.

Memory protection mechanisms such as memory safe languages, stack canaries, address space layout randomization (ASLR) and limited or no execute permissions are recommended wherever applicable.

5.2.5.2.2 Event logging

If capable, IoT devices should record sufficient details for each event to facilitate an authorized entity's ability to identify anomalous events and meaningfully analyse the associated data.

IoT devices and event logs should be synced with an authoritative system or passed to centralized repositories if the data has been appropriately de-identified.

5.2.5.2.3 Sensitive security parameters

The outcome of the risk assessment in 5.1.1 should help determine whether an IoT device may include hard-coded or shared sensitive security parameters, if such parameters are unique per device and not universal.

5.2.5.3 Additional information

5.2.5.3.1 General

Hardware-based solutions such as built-in crypto accelerators and dedicated hardware can enhance the use of cryptographic modules and cryptographic key protection capabilities to protect the data in storage and transit to meet the performance requirements. Physical countermeasures can support resistance to side channel attacks. Such functions can include hardware-based root of trust (RoT). RoT is a foundational feature to provide platform integrity and ensure a foundation to develop and support the device's chain of trust. The root of trust is ideally based on a hardware-validated boot process to ensure the system can be started using code from an immutable source. As such, RoT is essential to enable platform attestation including for a verified boot process. When used to protect secrets and device correctness, hardware can support a foundational root of trust upon which rich software functionality can be implemented more securely and safely.

Compartments are protected by hardware-enforced boundaries to prevent a flaw or breach in one software compartment from propagating to other software compartments in the system. Compartmentalization introduces additional protection boundaries within the hardware and software stack to create additional layers of defence in depth. For example, a common technique is to use operating systems processes or independent virtual machines as compartments.

Integrity checking and recovery modes may not be appropriate in safety critical applications where continuous operation is essential.

5.2.5.3.2 Event logging

Implementation of event logging, including editing of logs, depends on device storage capabilities. IoT devices can support remote logging.

Trusted Platform Modules (TPMs) are one example of hardware roots of trust. They can support cryptographically bound device identification and interface access to help prevent unauthorized access and use of data. More information about TPMs can be found in ISO/IEC 11889-1.

5.2.6 Interface access

5.2.6.1 Requirements

5.2.6.1.1 IoT devices shall have mechanisms to limit logical access to its interfaces to authorized entities only.

5.2.6.1.2 IoT devices shall employ appropriate authentication and access control mechanisms.

5.2.6.1.3 Security and privacy requirements shall be assessed when designing and implementing the functions of IoT devices regarding creation and use of identifiers.

5.2.6.1.4 IoT devices shall ensure that common values for critical security parameters, such as global private keys or standard passwords, are replaced by values that are unique per device or explicitly defined by an appropriate external entity before they are put into operation.

NOTE The risk assessment is the basis of what is “appropriate” in this context.

5.2.6.2 Additional recommendation(s)

The IoT device should be capable of being logically identified. While identifiers can enable a host of cybersecurity controls (such as asset management, automatic device discovery, and software updates), creating or using persistent identifiers should be avoided unless such use is unavoidable. Where such uses arise, the existence of such identifiers should be made clear to users.

Mechanisms to limit logical access (to authorized entities) should be applied to the following:

a) the ability to enable or disable, through software or hardware means, any interfaces (including local and network interfaces);

b) the ability to restrict access (e.g. through authentication) to all remote interfaces;

c) the ability to identify or block devices not supported by an IoT device when it is attempting to access interfaces.

All input and output data should be validated for all kinds of interfaces. Data should be validated for length, character type, acceptable values or ranges, and message format.

IoT devices with remote interfaces that can be used to make configuration changes or that support administrative functions should implement measures to prevent common attack types.

Secure coding practices should be followed including use of a type-safe language. If this is not possible, the IoT device should still implement bounds checking and use safe typing and safe string handling functions.

IoT devices should support one or more mechanisms to limit access to interfaces based on types or groups of users.

Allow-lists (of characters or other token types) should be used instead of deny-lists when filtering data.

5.2.6.3 Additional information

5.2.6.3.1 General

Examples of user interfaces include administrative consoles, web pages, APIs or other externally-exposed IoT device interfaces. Injection, XML external entities, cross site scripting and insecure deserialization are examples of common attacks to remote interfaces.

Hardware-based capabilities can harden interface access protection against privilege escalation and control-flow attacks.

5.2.6.3.2 Identifiers

IoT devices can use identifiers in order to operate within an IoT system. Examples of such identifiers include serial numbers, cryptographic keys, and certificates.

NOTE Physical and logical identifiers can represent the same value.

Hardware-based root of trust can protect identifiers from unauthorized modification and can be used to generate device specific identifiers. Hardware can include important properties that can be used to support device security such as a single purpose hardware supporting the prevention of unintended actions performed by unauthorized entities.

IoT device developers can augment a unique logical identifier by provisioning a strong cryptographic device identity during deployment (or manufacturing) or using other mechanisms to authenticate the physical device involved in specific network based inbound or outbound activity.

5.2.7 Software and firmware updates

5.2.7.1 Requirements

5.2.7.1.1 If the IoT device supports software updates, updates shall be performed using a secure procedure.

5.2.7.1.2 Updates shall only be initiated by authorized entities.

NOTE Firmware is a specific type of software.

5.2.7.1.3 Unexpected interruption of an update shall leave the IoT device in a state that minimizes potential for harm, taking into account the risks of the IoT device not functioning as expected.

5.2.7.2 Additional recommendation(s)

Each update procedure should include the following:

a) a way to confirm the validity, authenticity and integrity of any update before installing it;

b) configuration options that include:

   1) whether automatic updates are enabled or disabled;

   2) for remote update procedures, whether update downloads and installations are automatically or manually initiated;

   3) for remote update procedures, a way of scheduling automatic downloads and installations;

   4) whether notification occurs when an update is available (and who/what is notified).

IoT devices should support automatic updates (in accordance with the requirements 5.2.7.1.1 to 5.2.7.1.3). IoT devices should have an update procedure that periodically checks whether a new security update is available, and if so, indicates this to the user.

IoT devices should ensure that the authenticity and integrity of software updates are verified prior to installing them. This can be performed using digital signatures and public key infrastructure. The update infrastructure, specifically the management of private keys, should be secure.

Leveraging the hardware root of trust-based capabilities to measure and verify the validity of the software and firmware updates should be considered.

Software updates should not impact the basic functioning of IoT devices, or where unavoidable, clear notification should be supplied to the user where an update will interrupt the functioning of an IoT device.

Software on IoT devices should be verified using secure boot mechanisms. If an unauthorized change is detected, the IoT device should alert the user or the local hub/IoT gateway to an issue. Further, the IoT device should terminate any network communication except to send the alert or initiate device recovery.

As part of secure development life cycle or similar, there should be a formal process for assessing either new, replaced, or modified components including firmware updates for material changes that can induce new risks or vulnerabilities.

5.2.7.3 Additional information

IoT devices can have safety relevant functions, and loss of those functions during an update can be an issue for some types of system if not considered and managed. Discarding an update or using a previous update can be used to recover from an interrupted update.

The software update procedure(s) can involve remote (e.g. network download) or local means (e.g. removable media or part replacement).

If the IoT device cannot directly communicate with the remote server, this functionality can be provided by a local hub/IoT gateway. The local hub can be configured to periodically check if new updates are available and, if they exist, download them.

Hardware replacement is a legitimate and acceptable way to perform an update.

5.2.8 User notifications

5.2.8.1 Information

It may be necessary or useful for IoT devices to notify users about to a variety of circumstances. There are several recommendations in this document that describe such circumstances. This clause is intended to provide information to support notifying IoT device users about a negative event or condition.

Some IoT devices do not have capabilities to actively inform the user (e.g. write a message on the screen, emit a sound or light), but they can respond with a message when queried or accessed remotely. IoT devices that do not have capabilities to directly inform users can send notifications and alerts via a local hub. A user query can be as simple as trying to access the device with a browser, mobile application, or something more complex. Alternatively, IoT devices can send a message to an alarm, monitoring, or logging device within the IoT system.

Annex A
(informative)

Risk management guidance

A.1 General

The guidance provided in ISO 31000:2018, 6.4.1 applies. IoT security and privacy risks should be identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization.

A.2 Risk identification

Risk assessment consists of risk identification, risk analysis and risk evaluation. The guidance provided in ISO 31000:2018, 6.4.2 applies. When identifying security and privacy risks of IoT devices, various risk sources should be considered. These risk sources depend on the nature of the IoT device and its applications.

A.3 Risk analysis

The guidance provided in ISO 31000:2018, 6.4.3 applies. Risk analysis may be undertaken in varying degrees of detail depending on the criticality of the values or previously identified assets of the organization, the extent of adverse and positive impacts that are already known, and any accrued knowledge, or experience including incidents (history) involving the organization.

A.4 Risk evaluation

The guidance provided in ISO 31000:2018, 6.4.4 applies. Once the risks have been identified and assigned likelihood and severity of consequence values, organizations should apply their risk acceptance criteria to determine whether or not the risks are acceptable. If they are not acceptable, then they should be prioritized for treatment.

A.5 Risk treatment

The guidance provided in ISO 31000:2018, 6.5.1 and 6.5.2 applies. Risk treatment options defined by the organization should consider the objectives of the organization, contractual, legal and regulatory requirements and the views of relevant interested parties. Risk treatment options may include:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— undertake further analysis to better understand the risk;

— reconsider objectives;

— removing the risk source;

— sharing the risk (e.g. through contracts, buying insurance);

— retaining the risk by informed decision.

A.6 Monitoring and review

The guidance provided in ISO 31000:2018, 6.6 applies. There should be coordinated activities to direct and control an organization with regard to risk.

A.7 Recording and reporting

The guidance provided in ISO 31000:2018, 6.7 applies. The organization should establish, record and maintain a system for the collection and verification of information on IoT devices and collect and review publicly available information on similar products on the market. This information should then be assessed for possible relevance on the trustworthiness of the IoT device.

Bibliography

[1] NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*

[2] NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*

[3] Broadband Internet Technical Advisory Group (BITAG). (2016) Internet of Things (IoT) Security and Privacy Recommendations. (Broadband Internet Technical Advisory Group (BITAG), Denver, CO). Available at: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[4] CTIA, 2018, CTIA Cybersecurity Certification Test Plan for IoT devices, Version1.0.1. CTIA, Washington, DC

[5] European Union Agency for Network and Information Security (ENISA). (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. (European Union Agency for Network and Information Security (ENISA), Athens, Greece). recommendations-for-iot

[6] Groupe Spéciale Mobile Association (GSMA). (2017) GSMA IoT Security Assessment. (Groupe Spéciale Mobile Association (GSMA), London, UK). Available at: https://www.gsma.com/iot/iot-security-assessment/

[7] Industrial Internet Consortium (IIC). (2016) Industrial Internet of Things Volume G4: Security Framework. (Industrial Internet Consortium (IIC), Needham, MA).

[8] IoT Security Foundation (IoTSF). (2017) IoT Security Compliance Framework, Release 1.1. (IoT Security Foundation (IoTSF), Livingston, Scotland). Available at: https://www.iotsecurityfoundation.org/best-practice-guidelines/

[9] Cloud Security Alliance (CSA) IoT Working Group. (2015) Identity and Access Management for the Internet of Things. (Cloud Security Alliance (CSA)).

[10] AgeLight Digital Trust Advisory Group. (2019) IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1. (AgeLight Advisory & Research Group, Bellevue, WA).

[11] European Telecommunications Standards Institute (ETSI) European Norm. (EN) (2020-06) Cyber; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI Technical Specification 303 645 V2.1.1. (European Telecommunications Standards Institute (ETSI), Sophia Antipolis Cedex, France). Available at: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[12] IEC 62443-4-1, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*

[13] IEC 62443-4-2, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*

[14] C2 Consensus on IoT Device Security Baseline Capabilities, Convene the Conveners Project, Available at: https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[15] ISO/IEC 19770-2, *Information technology — IT asset management — Part 2: Software identification tag*

[16] Security Specification Version O.C.F., 2.1.2, Available at: https://openconnectivity.org/specs/OCF_Security_Specification_v2.1.2.pdf

[17] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*

[18] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

[19] ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

[20] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[21] IEC 31010, *Risk management — Risk assessment techniques*

[22] ISO/IEC 23093-1, *Information technology — Internet of media things — Part 1: Architecture*

[23] ISO 25197, *Small craft — Electrical/electronic control systems for steering, shift and throttle*

[24] ISO/IEC 20924:2021, *Information technology — Internet of Things (IoT) — Vocabulary*

[25] ISO/IEC 11889-1, *Information technology — Trusted platform module library — Part 1: Architecture*

[26] ISO 9241-110:2020, *Ergonomics of human-system interaction — Part 110: Interaction principles*

This Page has been Intentionally left blank

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Head (Publication & Sales), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the website- www.bis.gov.in or www.standardsbis.in.

This Indian Standard has been developed from Doc No.: LITD 17 (25331).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: 601/A, Konnectus Tower -1, 6th Floor, DMRC Building, Bhavbhuti Marg, New Delhi 110002	2323 7617
Eastern	: 8th Floor, Plot No 7/7 & 7/8, CP Block, Sector V, Salt Lake, Kolkata, West Bengal 700091	2367 0012 2320 9474
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg, Chandigarh 160019	265 9930
Southern	: C.I.T. Campus, IV Cross Road, Taramani, Chennai 600113	2254 1442 2254 1216
Western	: 5th Floor/ MTNL CETTM Technology Street, Hiranandani Gardens, Powai, Mumbai 400076	2570 0030 2570 2715

Branches : AHMEDABAD, BENGALURU, BHOPAL, BHUBANESHWAR, CHANDIGARH, CHENNAI, COIMBATORE, DEHRADUN, DELHI, FARIDABAD, GHAZIABAD, GUWAHATI, HARYANA (CHANDIGARH), HUBLI, HYDERABAD, JAIPUR, JAMMU, JAMSHEDPUR, KOCHI, KOLKATA, LUCKNOW, MADURAI, MUMBAI, NAGPUR, NOIDA, PARWANOO, PATNA, PUNE, RAIPUR, RAJKOT, SURAT, VIJAYAWADA.

Published by BIS, New Delhi