



TABLE OF CONTENTS

Content Title	Page No.
IS 18004 (Part 1): 2021 “IoT System Part 1 Reference Architecture”	5
IS/ISO/IEC/TR 22417: 2017 “Information Technology-IoT Use Cases”	5
IS/ISO/IEC 21823-1: 2019 “Interoperability for IoT systems-Part 1: Framework”	5
IS/ISO/IEC 21823-2 : 2020 “Internet of Things IoT - Interoperability for IoT systems - Part 2: Transport interoperability”	5
IS/ISO/IEC 21823-3 : 2021 “Internet of Things IoT - Interoperability for IoT systems - Part5	5
IS/ISO/IEC 21823-4: 2022 “Internet of Things IoT - Interoperability for IoT systems - Part 4: Syntactic interoperability”	6
IS/ISO/IEC 27400: 2022 “Cyber security - IoT Security and Privacy - Guidelines”	6
IS/ISO/IEC 27402: 2023 “Cyber security - IoT Security and Privacy - Device Baseline Requirements”	6
IS/ISO/IEC 27033-6:2016 “Information Technology - Security Techniques - Network Security Part 6: Securing Wireless IP Network Access”	6
IS/ISO/IEC 30118 series “Open Connectivity Foundation (OCF)”	6-9




PREFACE

Bureau of Indian Standards (BIS) is the National Standards Body of India, responsible for establishing standards for products to ensure quality, safety, and efficiency.

This compendium aims at providing an overview of Indian Standards on safety of Internet of Things, offering insights into their interoperability requirements. It is intended for use by common consumers, manufacturers, construction professionals, engineers, quality control personnel, academic professionals, and regulatory authorities to enhance understanding and compliance with industry standards.

By compiling relevant standards for Internet of Things in a single document, this compendium serves as a ready reference for professionals involved in production of Internet of things, and safety assessment, contributing to improved construction safety.



Introduction

The Internet of Things (IoT) is a transformative technology that connects physical devices to the internet, enabling them to collect, share, and analyse data. These devices—ranging from everyday household items like smart thermostats and wearable fitness trackers to industrial machinery and autonomous vehicles—are embedded with sensors, software, and communication capabilities that allow them to interact with each other and with centralized systems.

IoT is the backbone behind creation of smarter environments through automation and data-driven decision-making in sectors such as healthcare, manufacturing, smart cities, energy, transportation, and agriculture.

IoT represents a revolutionary shift in the way devices, systems, and services interact through networked connectivity. This paradigm enables everyday objects—ranging from household appliances and industrial equipment to vehicles and wearable devices—to collect and exchange data seamlessly. Through the integration of sensors, actuators, embedded software, and connectivity solutions, IoT supports real-time monitoring, automation, and enhanced decision-making.

In essence, IoT represents a powerful shift toward a more connected and intelligent world, where devices not only respond to human input but also anticipate needs and act independently to improve quality of life and business outcomes.

As the IoT ecosystem expands, standardization becomes essential to ensure interoperability, security, reliability, and scalability of interconnected systems. Uniform standards enable diverse IoT components and platforms to work cohesively, regardless of manufacturer or region. They also help mitigate challenges such as data fragmentation, device heterogeneity, and cyber vulnerabilities.

This compendium provides a comprehensive overview of Indian initiatives on IoT standardization, with insights into ongoing work by the Bureau of Indian Standards (BIS).

The list of standards related to Internet of things, published by BIS under these Sectional Committees (LITD 27, LITD 17, LITD 28) & their short description is given as follows:

IS 18004 (Part 1): 2021 “IoT System Part 1 Reference Architecture”

This standard defines a common structure for designing IoT systems. It explains key components and how they interact, helping different devices and platforms work together smoothly and enabling secure, scalable, and interoperable IoT solutions.

IS/ISO/IEC/TR 22417: 2017 “Information Technology IoT Use Cases”

This standard presents real-life examples of how IoT is used across different sectors. It helps developers and planners understand practical applications, challenges, and requirements for building effective, interoperable, and scalable IoT systems.

IS/ISO/IEC 21823-1: 2019 “Interoperability Framework for IoT systems”

This standard provides a basic structure to ensure different IoT devices and systems can work together. It explains types of interoperability—network, syntactic, semantic, and others—to guide the design of seamless, connected, and collaborative IoT environments.

IS/ISO/IEC 21823-2: 2020 “Internet of Things IoT - Interoperability for IoT systems- Part 2: Transport interoperability”

This standard focuses on how data is transmitted between IoT devices. It defines methods to ensure smooth, reliable, and secure communication across different networks, enabling various IoT systems to exchange information effectively.

IS/ISO/IEC 21823-3: 2021 “Internet of Things IoT - Interoperability for IoT systems - Part 3: Semantic interoperability”

This standard ensures that IoT devices understand the meaning of shared data. It defines how to use common vocabularies and data models so that different systems can interpret and use information correctly and meaningfully.

IS/ISO/IEC 21823-4: 2022 “Internet of Things IoT - Interoperability for IoT systems - Part 4: Syntactic interoperability”

This standard defines how data should be formatted and structured so that different IoT devices can read and process it correctly. It ensures smooth data exchange by using common data formats across various systems.

IS/ISO/IEC 27400: 2022 “Cyber security - IoT Security and Privacy - Guidelines”

This standard provides guidance on identifying and managing security and privacy risks in IoT systems. It outlines principles and controls to protect data, devices, and networks, ensuring safe and reliable IoT deployments across various sectors.

IS/ISO/IEC 27402: 2023 “Cyber security - IoT Security and Privacy - Device Baseline Requirements”

This standard specifies essential security and privacy requirements for Internet of Things (IoT) devices. It ensures that devices support necessary controls to protect data and user privacy, fostering safer and more reliable IoT deployments.

IS/ISO/IEC 27033-6:2016 “Information Technology - Security Techniques - Network Security Part 6: Securing Wireless IP Network Access”

This standard offers guidelines to protect wireless IP networks, such as Wi-Fi and Bluetooth. It identifies security threats, outlines protective measures, and provides design techniques to ensure secure wireless communications in various environments.

IS/ISO/IEC 30118 series “Open Connectivity Foundation (OCF)”
IS/ISO/IEC 30118-1: 2021 “Part 1: Core specification”

This standard defines the foundational framework for IoT device interoperability. It specifies the core architecture, interfaces, protocols, and services that enable seamless communication and integration across diverse IoT devices and platforms. By standardizing these elements, it ensures consistent and secure interactions in IoT ecosystems.

IS/ISO/IEC 30118-2: 2021 “Part 2: Security specification”

This standard outlines security objectives and mechanisms for OCF-based IoT systems. It specifies protocols for secure device on boarding, data encryption, and access Control, ensuring trusted communication and privacy across diverse IoT devices and platforms.

IS/ISO/IEC 30118-3: 2021 “Part 3: Bridging specification”

This standard defines how IoT devices from different ecosystems can communicate through bridging platforms. It specifies requirements for bridging devices and virtual object device (VODs), enabling seamless interoperability between diverse IoT networks.

IS/ISO/IEC 30118-4: 2021 “Part 4: Resource type specification”

This standard defines standardized resource types that IoT devices can expose, Such as temperature sensors or locks. It ensures consistent communication and Interoperability across diverse devices and applications within the OCF ecosystem. Built on the OCF Core Specification, it supports scalable device implementations.

IS/ISO/IEC 30118-5: 2021 “Part 5: Resource to AllJoyn interface mapping specification”

This standard provides detailed definitions for IoT devices based on the Open Connectivity Foundation (OCF) framework. It builds upon the OCF Core Specification and Resource Type Specification to define device models, ensuring interoperability and scalability Across diverse IoT ecosystems.

IS/ISO/IEC 30118-6: 2021 “Part 6: Resource to AllJoyn interface mapping specification”

This standard provides a structured mapping between Open Connectivity Foundation (OCF) Resources and All Joyn interfaces. It defines how All Joyn device types correspond to OCF device types and specifies the property-by-property equivalence using JSON Schema extensions, Facilitating seamless interoperability between All Joyn and OCF Ecosystems.

IS/ISO/IEC 30118-6: 2021 “Part 6: Resource to AllJoyn interface mapping specification”

This standard provides a structured mapping between Open Connectivity Foundation (OCF) resources and AllJoyn interfaces. It defines how AllJoyn device types correspond to OCF device types and Specifies the property-by-property equivalence using JSON schema extensions, facilitating seamless interoperability between AllJoyn and OCF ecosystems.

IS/ISO/IEC 30118-7: 2021 “Part 7: Wi-Fi easy setup specification”

This standard defines extensions to the OCF Core Specification to facilitate the easy setup of IoT devices over Wi-Fi networks. It introduces new resource types and functionalities, enabling devices to securely and seamlessly connect to Wi-Fi networks with minimal user intervention.

IS/ISO/IEC 30118-8: 2021 “Part 8: OCF resource to oneM2M resource mapping specification”

This standard provides detailed mappings between Open Connectivity Foundation (OCF) resources and oneM2M module classes, facilitating interoperability between these two IoT ecosystems. It defines unidirectional mappings for device types and property-level equivalencies using JSON schema extensions, enabling seamless integration between OCF and oneM2M devices.

IS/ISO/IEC 30118-9: 2021 “Part 9: Core optional specification”

This standard defines optional features and extensions to the OCF Core Specification, enabling enhanced functionalities for IoT devices. It provides guidelines for implementing advanced capabilities, ensuring scalability and adaptability in diverse IoT ecosystems. By specifying optional components, it allows manufacturers to tailor devices to specific use cases while maintaining interoperability.

IS/ISO/IEC 30118-10: 2021 “Part 10: Cloud API for cloud services specification”

This standard defines functional requirements for the Open Connectivity Foundation (OCF) Cloud-to-Cloud Application Programming Interface (API). It facilitates secure and standardized communication between cloud services, enabling seamless device management, event handling, and synchronization across different cloud platforms. The specification includes Oath 2.0-Based authentication, device and resource management APIs, and event subscription mechanisms to ensure interoperability and scalability in IoT ecosystems.

IS/ISO/IEC 30118-11: 2021 “Part 11: Device to cloud services specification”

This standard defines functional extensions to the capabilities defined in ISO/IEC 30118-1 to meet the requirements of the OCF Cloud.

IS/ISO/IEC 30118-12: 2021 “Part 12: Cloud security specification”

This standard defines security requirements for Open Connectivity Foundation (OCF) devices interacting with cloud services. It specifies authentication, authorization, data protection, and secure communication protocols to ensure trusted and safe interactions between IoT devices and cloud platforms.

IS/ISO/IEC 30118-13: 2021 “Part 13: Onboarding tool specification”

This standard defines the mechanisms supported by an Open Connectivity Foundation (OCF) Onboarding Tool (OBT). It includes security requirements for the OBT and may reference other OCF documents related to the base or security specifications.

IS/ISO/IEC 30118-14: 2021 “Part 14: OCF resource to BLE mapping specification”

This standard provides detailed mappings between Bluetooth Low Energy (BLE) services and Open Connectivity Foundation (OCF) resources. It defines how BLE characteristics correspond to OCF resource properties, facilitating seamless interoperability between BLE devices and OCF-compliant systems. The specification uses Python-like syntax to describe these mappings, ensuring clarity and precision in device communication.

IS/ISO/IEC 30118-15: 2021 “Part 15: OCF resource to EnOcean mapping specification”

This standard provides detailed mapping information between EnOcean-defined EnOcean Equipment Profiles (EEPs) and Open Connectivity Foundation (OCF)-defined devices and resources. It enables seamless interoperability between EnOcean-based devices and OCF-compliant systems, facilitating integration in IoT ecosystems.

IS/ISO/IEC 30118-16: 2021 “Part 16: OCF resource to UPlus mapping specification”

This standard provides detailed mapping information between UPlus (U+) and Open Connectivity Foundation (OCF) defined Resources. It facilitates interoperability between UPlus devices and OCF-compliant systems by defining how UPlus device functionalities correspond to OCF resource types.

IS/ISO/IEC 30118-17: 2021 “Part 17: OCF resource to Zigbee cluster mapping specification”

This standard provides detailed mappings between Zigbee-defined clusters and Open Connectivity Foundation (OCF)-defined resources. It facilitates interoperability by aligning Zigbee device functionalities with OCF resource types, enabling seamless communication across diverse IoT ecosystems.

IS/ISO/IEC 30118-18: 2021 “Part 18: OCF resource to Z-wave mapping specification”

This standard provides detailed mapping information between Z-Wave and Open Connectivity Foundation (OCF) defined Resources. It facilitates interoperability between Z-Wave devices and OCF-compliant systems by defining how Z-Wave device functionalities correspond to OCF Resource types.