Preface

In the era of rapid technological advancement, the Internet of Things (IoT) has emerged as a pivotal force transforming industries, economies, and daily life. The interconnectedness of devices, systems, and people is redefining the way we interact with our environment, offering unprecedented opportunities for efficiency, innovation, and sustainability. The draft handbook you are about to explore is a comprehensive guide to understanding the intricate landscape of IoT, emphasizing its relevance, applications, and the critical role of standardization and conformity assessment.

IoT's journey from a conceptual framework to a tangible, everyday reality is marked by significant milestones driven by technological advancements and the growing demand for connectivity. From its early roots in the 1980s with basic networked devices to the sophisticated, sensor-rich environments of today, IoT's evolution underscores its transformative potential. This handbook delves into the multifaceted applications of IoT across various sectors-smart homes, industrial automation, healthcare, agriculture, and smart cities-highlighting how IoT solutions enhance efficiency, safety, and decision-making.

The cornerstone of IoT's success lies in the standardization and conformity assessment processes. These frameworks ensure interoperability, security, reliability, and quality across diverse IoT devices and systems. The sections on standardization provide a detailed look at the international and national bodies that develop and enforce these standards, ensuring that IoT technologies meet specific quality and performance criteria. Organizations like BIS, ISO, IEC, ITU and various national entities are pivotal in shaping a cohesive and secure IoT ecosystem.

Conformity assessment bodies play an equally crucial role by validating that IoT products comply with established standards. This ensures that devices not only perform reliably but also adhere to safety and security protocols, fostering consumer trust and facilitating market access. The handbook outlines the significance of these assessments and the organizations involved in maintaining the integrity of IoT implementations.

Moreover, the regulatory landscape for IoT is complex and evolving, with various international and national regulations addressing issues of data privacy, security, and interoperability. Understanding these regulatory frameworks is essential for stakeholders to navigate the challenges and opportunities presented by IoT technologies.

Premier institutions like the Indian Institutes of Technology (IITs) and Indian Institutes of Information Technology (IIITs) are at the forefront of IoT research and innovation in India. Their collaborative projects, industry partnerships, and academic initiatives are pivotal in driving technological advancements and addressing real-world challenges through IoT solutions.

This handbook has been prepared primarily for the students of IoT to apprise them primarily about the role played by Standardization and Conformity assessment in the operations of IoT. This handbook is also useful tool for policy makers and professionals as in addition to Standardization and Conformity Assessment it attempts to address aspects related to regulatory requirements/framework applicable to the area of IoTequipping readers with the knowledge to harness IoT's potential responsibly and effectively.

As we step into a future increasingly shaped by IoT, this handbook will be an indispensable guide, illuminating the path toward a more connected, intelligent, and sustainable world.

Acknowledgement

The author extends heartfelt gratitude to all individuals who have contributed to the preparation of this reference handbook.

Shri Pramod Kumar Tiwari, IAS, Director General of the Bureau of Indian Standards, has been the driving force for the development of this reference handbook. His unstinted support and encouragement have made this work possible. The Author expresses his gratitude and thanks to him for successfully completing this endeavour.

The author expresses deep appreciation to the standardization fraternity both at National and International Level, who over the years have work laboriously for developing standards in the field of Internet of Things (IoT). The work done by the standardizers has made this reference handbook possible as it is based on the standards primary made by the Technical Committees LITD 27-Internet of Things and & Digital Twin, LITD 28-Smart Infrastructure Sectional Committeeof BIS at National Level and ISO/IEC/JTC 1/SC 41 - Internet of things and digital twin at the international level.

The author also acknowledges the contributions of Shri Vikas Meena, Deputy Director &Scientist C, WRO, and Shri Shivang Bhardwaj, PA to DDGW, without whose help, it would not have possible to complete this piece of work.

The author expresses gratitude to the publishers for their meticulous and professional preparation of this reference book

CONTENTS

CHAPTER I
INTRODUCTION

CHAPTER I

INTRODUCTION

HISTORY

The concept of the Internet of Things (IoT) has evolved significantly since its inception, reflecting the dynamic interplay of technology and innovation over the past several decades. The roots of IoT can be traced back to the early 1980s when the idea of adding sensors and intelligence to basic objects was first explored. The term "Internet of Things" itself was coined by Kevin Ashton in 1999 during his work at Procter & Gamble, where he envisioned a system where the internet would be connected to the physical world via ubiquitous sensors.

The 1990s saw the advent of RFID (Radio Frequency Identification) technology, which played a pivotal role in the development of IoT. RFID allowed objects to be identified and tracked automatically, laying the groundwork for a more interconnected world. During this period, advancements in networking technologies and the proliferation of the internet facilitated further exploration into connected devices.

The early 2000s marked a significant turning point with the rise of wireless technology, increased internet accessibility, and the miniaturization of sensors. The integration of these technologies enabled the practical implementation of IoT in various domains such as healthcare, manufacturing, and home automation. In 2008, the number of devices connected to the internet surpassed the global human population, signalling the dawn of a new era where the internet's primary function shifted from connecting people to connecting things.

In the following decade, IoT experienced exponential growth driven by the widespread adoption of smartphones, cloud computing, and advancements in artificial intelligence and machine learning. This period saw the emergence of smart homes, wearable technology, and industrial IoT applications, transforming everyday life and business operations. The introduction of IPv6 also addressed the challenge of accommodating the vast number of devices by providing an almost limitless IP address space.

Today, IoT continues to expand rapidly, integrating more sophisticated technologies like edge computing, blockchain, and 5G networks. These innovations are enhancing the capabilities of IoT systems, making them more efficient, secure, and scalable. The future of IoT promises even greater connectivity, automation, and intelligence, reshaping industries and revolutionizing the way we interact with the world.

In summary, the history of IoT is a testament to the relentless pursuit of connecting the physical and digital realms. From its early conceptual stages to its current state as a transformative force in technology, IoT exemplifies the profound impact of technological progress on society.

CHAPTER II

OVERVIEW OF INTERNET OF THINGS (IOT)

CHAPTER II

OVERVIEW OF INTERNET OF THINGS (IOT)

The concepts and definitions given in this handbook have majorly been taken from Indian and International Standards. For International Standards, the Terms and Definitions given in the Online Browsing Platform (OBP)- https://www.iso.org/obp , of International Organisation of Standards (ISO) has been used. This platform gives the Terms and Definitions given in different International Standards. The source from which the definition/concept has been taken is given in brackets at the end of the text.

DEFINITION

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**(ISO/IEC 20924:2024 Internet of Things (IoT) and digital twin - Vocabulary)**

IoT refers to a network of interconnected devices, sensors, actuators, and other physical objects that are embedded with software, electronics, and connectivity capabilities. These connected devices can communicate and exchange data with each other over the internet, enabling them to collect, transmit, and analyse information in real-time without human intervention.

The concept of IoT has evolved over the years, driven by advancements in technology and the increasing demand for connectivity and automation. The roots of IoT can be traced back to the early 1980s with the development of simple networked devices. However, it was the proliferation of internet connectivity and the miniaturization of sensors and processors in the 2000s that paved the way for the modern IoT era. Today, IoT has become a pervasive and transformative force across various industries, revolutionizing how we interact with the physical world.

Applications of IoT

IoT has a wide range of applications across industries and sectors, offering numerous benefits including increased efficiency, improved decision-making, enhanced safety, and better resource utilization. Some common applications of IoT include:

i) Smart Home Automation

Smart homes utilize IoT technology to enhance comfort, convenience, and energy efficiency within residential spaces. Devices such as smart thermostats, lighting systems, security cameras, and home assistants communicate with each other and can be controlled remotely via smartphones or voice commands. For instance, a smart thermostat can learn a user’s preferences and adjust the temperature accordingly, while smart lighting can be programmed to switch off when rooms are unoccupied, saving energy. Security systems can be monitored in real-time, offering peace of mind with alerts and remote access. This interconnected ecosystem creates a personalized and responsive living environment.

ii) INDUSTRIAL IOT (IIOT)

Industrial infrastructure of interconnected entities, people, systems and information resources, together with services which process and react to information from the physical world and the virtual world.IndustrialInternet of Things is used to identify the industrial specializations of IoT. **(ISO 24591-1:2024 – Smart water management – Part 1: General guidelines and governance, Cl. 3.1.7)**

In industrial settings, IoT facilitates the monitoring and optimization of manufacturing processes, equipment, and supply chains. IIoT applications include predictive maintenance, asset tracking, inventory management, and real-time production monitoring, leading to improved productivity and reduced downtime.Real-time monitoring and analytics optimize production processes, improving efficiency and product quality. Automated systems and robotics streamline complex tasks, reducing human error and increasing safety. Supply chain management benefits from IIoT through improved inventory tracking and logistics coordination. These advancements lead to cost savings, increased productivity, and more agile manufacturing operations.

iii) SMART CITIES

A smart city is one that increases the pace at which it provides social, economic, and environmental sustainability outcomes. Smart cities respond to challenges, such as climate change, rapid population growth, and political and economic instability by fundamentally improving how they engage society, apply collaborative leadership methods, work across disciplines and city systems, and use data information and modern technologies to deliver better services and quality of life to those in the city (residents, businesses, visitors), now and for the foreseeable future, without unfair disadvantage of others or degradation of the natural environment**. (IS 177378:2022 - Sustainable development of habitats — Indicators for smart cities)**

Smart cities leverage IoT technologies to improve urban living by enhancing infrastructure, public services, and environmental sustainability. Connected sensors and devices monitor and manage traffic flow, reducing congestion and improving transportation efficiency. Smart streetlights adjust brightness based on pedestrian and vehicle presence, conserving energy. Waste management systems use IoT to optimize garbage collection routes, reducing operational costs and environmental impact. Additionally, IoT-based environmental sensors track air quality and pollution levels, providing data to support public health initiatives and regulatory compliance. These integrations create more efficient, livable, and sustainable urban environments.

iv) HEALTHCARE

IoT in healthcare, often referred to as the Internet of Medical Things (IoMT), revolutionizes patient care through connected medical devices and health monitoring systems. Wearable devices like smartwatches and fitness trackers monitor vital signs such as heart rate, blood pressure, and glucose levels, sending data to healthcare providers for real-time analysis. This continuous monitoring enables early detection of potential health issues, timely interventions, and personalized treatment plans. Remote patient monitoring reduces hospital visits and improves patient outcomes, especially for chronic disease management, thereby enhancing the overall efficiency of healthcare systems.

v) AGRICULTURE (AGRITECH)

IoT applications in agriculture, known as smart farming, enhance productivity and sustainability through precise monitoring and management of agricultural activities. Sensors placed in fields measure soil moisture, nutrient levels, and weather conditions, providing data to optimize irrigation, fertilization, and pest control. Livestock monitoring systems track the health and activity of animals, ensuring timely interventions. Drones equipped with IoT devices survey large fields, offering insights into crop health and growth patterns. These technologies enable farmers to make data-driven decisions, improving yields, reducing resource consumption, and promoting sustainable farming practices.

vi) RETAIL AND LOGISTICS

IoT technologies are being used in retail and logistics to track inventory levels, monitor product shipments, optimize warehouse operations, and enhance the customer shopping experience. IoT-enabled solutions such as RFID tags, beacons, and smart shelves streamline supply chain management and improve inventory visibility.Fleet management systems use IoT to monitor vehicle conditions, driver behaviour, and fuel consumption, optimizing maintenance schedules and route planning. Connected vehicles communicate with each other and traffic infrastructure, reducing accidents and improving traffic flow

vii) ENERGY MANAGEMENT

IoT plays a crucial role in energy management by enabling smarter consumption and distribution of energy resources. Smart grids use IoT technology to monitor and manage the distribution of electricity, balancing supply and demand efficiently. Smart meters provide real-time data on energy usage, helping consumers and utilities to identify patterns and implement energy-saving measures. IoT devices in buildings control heating, ventilation, and air conditioning (HVAC) systems, lighting, and appliances to optimize energy use. Renewable energy sources like solar panels and wind turbines are integrated into the grid, enhancing sustainability and reducing carbon footprints.

viii) ENVIRONMENTAL MONITORING

IoT technology is pivotal in environmental monitoring, providing real-time data on various ecological parameters. Sensors deployed in natural habitats track air and water quality, temperature, humidity, and pollution levels. This data helps in detecting environmental changes and potential hazards early, facilitating timely interventions. IoT systems also monitor wildlife movements and behaviours, aiding in conservation efforts.

These are just a few examples of the diverse applications of IoT across various domains. As IoT continues to evolve and mature, it is expected to drive further innovation and transformation, reshaping industries, economies, and societies around the world.

This handbook attempts to gather the latest information with respect to national standardization, confromity assessment, applicable regulatory/legal aspects and an effort has been made to connect these aspects with the course curriculum of Internet of Things of various premier academic institutions.

CHAPTER III

RELEVANCE & IMPORTANCEOF STANDARDIZATION AND CONFORMITY ASSESSMENT

CHAPTER III
RELEVANCE & IMPORTANCEOF STANDARDIZATION AND CONFORMITY ASSESSMENT IN INTERNET OF THINGS (IoT)

Standardization and conformity assessment are critical components in the development and deployment of the Internet of Things (IoT) ecosystem. They ensure that devices and systems can interoperate, are secure, and perform reliably. Here's a detailed look at their relevance and importance:

1. *Interoperability*

Standardization ensures that devices from different manufacturers can communicate and work together seamlessly. It facilitates data exchange between devices, enabling more comprehensive and cohesive systems. This is essential in a heterogeneous IoT environment where devices, sensors, and systems need to share data and operate in unison.

Example: Protocols like MQTT, CoAP, and standards from organizations like IEEE and IETF allow diverse devices to interact regardless of their underlying technology.

2. *Security*

Standardization provides a framework for implementing security measures across IoT devices. Standards ensure that security protocols are robust and up to date, protecting against common vulnerabilities. They reduce vulnerabilities by implementing standardized encryption, authentication, and access control mechanisms.

Conformity Assessment validates that devices adhere to these security standards, ensuring they can resist attacks and protect user data.

Example: Standards like ISO/IEC 27001 for information security management systems help secure IoT deployments.

3. *Safety and Reliability*

Standardization establishes guidelines for the safe operation of IoT devices, reducing the risk of malfunctions that could lead to accidents or failures.

Conformity Assessment ensures that products meet these safety standards before they reach the market.

Example: IEC 61508 standard for functional safety of electrical/electronic systems ensures IoT devices operate safely and reliably.

4. *Quality Assurance*

Standardization defines quality benchmarks for IoT devices, ensuring consistency and reliability in their performance.

Conformity Assessment involves testing and certification processes that confirm devices meet these quality standards.

Example: ISO 9001 standards for quality management systems help maintain high-quality production processes in IoT manufacturing.

5. *Market Access and Consumer Confidence*

Standardization helps manufacturers comply with regulatory requirements, facilitating market access and consumer trust.

Certification marks (like CE marking in Europe) signal to consumers and regulators that a product meets all necessary standards.

Example: Products that pass conformity assessment processes are more likely to gain acceptance in global markets, enhancing consumer confidence.

6. *Innovation*

Standardization creates a foundation upon which new innovations can be built, ensuring new products and technologies are compatible with existing systems.

Conformity Assessment ensures that new and innovative products meet established standards, aiding their adoption and scalability.

Example: The adoption of 5G standards facilitates the development of new IoT applications by ensuring compatibility and performance.

7. *Cost Efficiency*

Standardization reduces costs by eliminating the need for proprietary solutions and enabling economies of scale.

Conformity Assessment prevents costly recalls and redesigns by ensuring products meet standards before they reach the market.

Example: Standardized protocols and interfaces reduce development costs and simplify integration processes.

8. *Scalability*

Standardization enables scalable IoT solutions that can expand without encountering compatibility issues. Scalability supports the growth of IoT networks by providing a stable foundation for adding new devices. Example: IPv6 addressing supports a vast number of devices compared to IPv4

Conformity Assessment is required for ensuring the performance, safety, security and interoperability of IoT products, thereby providing confidence to the users on these aspects. There are many organizations in different countries which work in the arena of IoT for Conformity Assessment. They provide Certification for the Products and Protocols used in IoT.

Standardization and conformity assessment are indispensable in the IoT landscape. They provide the necessary framework for interoperability, security, safety, quality, market access, innovation, and cost efficiency. By adhering to established standards and undergoing rigorous conformity assessment processes, IoT devices can achieve widespread adoption and deliver reliable, secure, and efficient performance.

CHAPTER IV

CONCEPTS IN INTERNET OF THINGS (IoT)

CHAPTER IV

CONCEPTS IN INTERNET OF THINGS (IoT)

The Internet of Things (IoT) is a broad and dynamic field involving a variety of concepts that collectively enable the integration and interaction of devices, systems, and services.

1. Architecture of IoT Systems

IoT systems comprise several interconnected components working together to collect, process, and analyse data from the physical world. Understanding the architecture of IoT systems is crucial for designing scalable, efficient, and secure deployments. The various components involved in IoT systems are:

a) Sensor Nodes:

Sensor nodes are sensor network elements that include at least one sensor and optionally actuators with communication capabilities and data processing capabilities. **[SOURCE: ISO/IEC 29182-2 - Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) - Part 2: Vocabulary and terminology, 2.1.8] (ISO/IEC 19762:2016(EN) – Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary, 09.01.25)**

Sensors: Devices that collect data from the physical environment, such as temperature, humidity, light, motion, and pressure.

Actuators: Devices that can perform actions based on commands from the IoT system, such as turning on a light, opening a valve, or adjusting a thermostat.

Sensor node is a node that enables the user to interact with the world in the scene graph hierarchy. Sensor nodes respond to user interaction with geometric objects in the world, the movement of the user through the world, or the passage of time **(ISO/IEC 14772-1:1997(en) - Information technology — Computer graphics and image processing — The Virtual Reality Modeling Language — Part 1: Functional specification and UTF-8 encoding, 3.91)**

Sensor nodes are responsible for capturing real-world data and converting it into digital signals. They play a crucial role in gathering environmental information and monitoring physical parameters in IoT applications. These small, embedded devices can measure various parameters such as temperature, humidity, pressure, light intensity, motion, and more. They collect raw data and transmit it to the network for further processing.

b) Connectivity:

It refers to the methods and technologies used to connect IoT devices to the internet and to each other. The connectivity of devices in IoT environment is maintained by various communication protocols like Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT, 5G, and Ethernet.Various Wireless Communication Technologies are explained below:

i) **Wi-Fi (IEEE 802.11):** Wi-Fi is a widely used wireless communication technology for IoT deployments, offering high-speed data transmission and a range of up to several hundred meters. It is suitable for indoor applications where power consumption is not a primary concern.

ii) **BLUETOOTH:** Bluetooth is a short-range wireless technology ideal for connecting IoT devices in close proximity, such as wearable devices, smart home appliances, and personal health monitors. Bluetooth Low Energy (BLE) variants offer low power consumption and support for intermittent data transmission.

Definition of Bluetooth as given in standard:

wireless technology standard for exchanging data over short distances.

Note 1 to entry: "Bluetooth" is a trademark owned by the Bluetooth SIG. **(IS/ISO/IEC 27033-6:2016(EN) – Information technology – Security techniques – Network security Part 6: Securing wireless IP network access, 3.3)**

iii) **ZIGBEE:** Zigbee is a low-power, low-data-rate wireless communication protocol commonly used in home automation, industrial control, and smart lighting applications. It operates on the 2.4 GHz frequency band and supports mesh networking, enabling devices to communicate with each other over extended distances.

iv) **Z-WAVE:** Z-Wave is a wireless communication protocol designed for low-power, low-latency IoT applications such as home automation, security systems, and smart energy management. It operates on sub-GHz frequencies, offering longer range and better penetration through walls and obstacles compared to Wi-Fi or Bluetooth.

v) **LORAWAN:** LoRaWAN (Long Range Wide Area Network) is a low-power, wide-area wireless communication protocol optimized for long-range communication and low data rates. It is suitable for IoT applications requiring connectivity over large geographical areas, such as smart agriculture, environmental monitoring, and asset tracking.

Network Topologies: Network topologies refer to the arrangement of different elements (links, nodes, etc.) in a computer network. They describe how different devices are interconnected and communicate with each other.

i) **Star Topology:** In a star topology, IoT devices communicate with a central hub or gateway, which then forwards data to the cloud or other network services. It offers centralized control, easy scalability, and simplified management but can be susceptible to single point of failure.

ii) **MESH TOPOLOGY:** Mesh topology allows IoT devices to communicate with each other directly, forming a self-healing network where data can be relayed through multiple paths. It offers redundancy, fault tolerance, and extended coverage but requires more complex routing algorithms and higher power consumption.

iii) **HYBRID TOPOLOGY:** Hybrid topologies combine elements of star and mesh topologies, allowing devices to communicate with both a central gateway and directly with each other. It provides flexibility, scalability, and resilience, suitable for large-scale IoT deployments with diverse connectivity requirements.

c) **Edge Computing:**

Adistributed type of computing in which processing and storage takes place at or near the edge, where the nearness is defined by the system's requirements. **(IS/ISO/IEC TR 23188:2020(EN) – Information technology – Cloud computing – Edge computing landscape, 3.1.3)**

- Distributed computing in which processing and storage takes place at or near the edge, where the nearness is defined by the system's requirements. **[SOURCE: IS/ISO/IEC TR 23188:2020– Information technology – Cloud computing – Edge computing landscape,3.1.3]**
- Note 1 to entry: The functions of the platform include resource collection, data aggregation, intelligent analysis, open sharing (e.g. of manuals, flyers), standards testing, technology verification, industrial data transfer, business resource management and industry monitoring.
- Note 2 to entry: A platform can be connected to a large number of heterogeneous industrial devices, including industrial internet of things, edge devices, and cyber-physical systems, some of which are not secure-by-design.**[SOURCE: IS/ISO/IEC TR 23188:2020 – Information technology – Cloud computing – Edge computing landscape, 3.1.3, modified]**

Edge computing brings computational capabilities closer to the data source, enabling real-time data processing, reduced latency, and bandwidth optimization. As IoT deployments continue to grow, edge computing becomes increasingly essential for handling data-intensive workloads, supporting low-latency applications, and ensuring privacy and security by processing sensitive data locally.

Edge computing complements cloud infrastructure by bringing computing resources closer to the data source, i.e., the edge of the network. Edge devices, such as gateways and edge servers, process and analyze IoT data locally before sending relevant information to the cloud. Edge computing reduces latency, bandwidth usage, and dependency on centralized cloud resources, making it ideal for applications requiring real-time processing, low latency, and offline operation. Edge devices often run lightweight operating systems and edge computing frameworks to execute edge analytics, machine learning algorithms, and automation logic.

Edge computing extends the capabilities of IoT systems by enabling local processing, analytics, and decision-making at the network edge. It reduces latency, conserves bandwidth, enhances privacy, and improves responsiveness by processing data closer to the data source. Edge devices preprocess data, filter noise, detect anomalies, and trigger actions in real-time, enabling timely responses and autonomous operations. Edge computing is instrumental in latency-sensitive applications, offline scenarios, and environments with limited connectivity to the cloud.

d) Cloud Computing

Cloud computing refers to the delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the internet ("the cloud"). It offers faster innovation, flexible resources, and economies of scale.

Cloud infrastructure provides a scalable and centralized platform for storing, processing, and analysing vast amounts of IoT data. It enables data aggregation, real-time analytics, historical analysis, and predictive insights, empowering organizations to derive actionable intelligence from IoT-generated data. Cloud platforms offer services for data storage, compute resources, machine learning, visualization, and integration, supporting various IoT use cases and applications.

e) Data Management:

This includes various techniques for collecting, storing, processing & managing the data generated by IoT devices. These techniques are explained as follows:

i) Data Collection:

Data Collection is the process for gathering information by different means (Note 1 to entry: This includes activities such as web monitoring.) **[IS/ISO 19731:2017(EN) – Digital analytics and web analyses for purposes of market, opinion and social search – Vocabulary and service requirements, 3.14]**

- Real-time Streaming: IoT devices often generate continuous streams of data. Techniques such as message queuing and stream processing platforms (e.g., Apache Kafka, MQTT) facilitate real-time ingestion and processing of streaming data.
- Batch Processing: For less time-sensitive data, batch processing techniques (e.g., Apache Spark, Hadoop) can be used to collect and process data in batches at regular intervals.

ii) Data Storage:

Data Storage is the persistent repository for digital data. A data store can be accessed by a single entity or shared by multiple entities via a network or other connection. **[SOURCE: ISO/IEC 20924:2021**

- Internet of Things (IoT) and digital twin - Vocabulary, 3.1.14] (ISO/IEC 5207:2024(EN - Information technology - IT Service Management - Overview and vocabulary, 3.58)

- Time-Series Databases: Time-series databases (e.g., InfluxDB, Prometheus) are optimized for storing and querying time-stamped data generated by IoT devices, making them ideal for storing sensor data.
- NoSQL Databases: NoSQL databases (e.g., MongoDB, Cassandra) offer scalability and flexibility for storing unstructured or semi-structured IoT data, such as device metadata and logs.
- Distributed File Systems: Distributed file systems (e.g., HDFS, Amazon S3) provide scalable storage for large volumes of IoT data, enabling fault-tolerant and distributed storage across multiple nodes.

iii) Data Processing:

Data Processing is the systematic performance of operations upon data. **[SOURCE: IS/ISO/IEC 2382:2015 –Information technology - Vocabulary]**

- Stream Processing: Stream processing frameworks (e.g., Apache Flink, Apache Storm) enable real-time analysis and processing of streaming data from IoT devices. They support operations such as filtering, aggregation, and enrichment in near real-time.
- Batch Processing: Batch processing frameworks (e.g., Apache Spark, Apache Beam) facilitate offline analysis and processing of historical IoT data. They support complex analytics, machine learning, and batch jobs on large datasets.

iv) Data Analysis

Data Analysis: systematic investigation of the data and their flow in a real or planned system. **[SOURCE: IS/ISO/IEC 2382:2015, 2122686 –Information technology - Vocabulary]**

Descriptive Analytics: Descriptive analytics techniques (e.g., statistical analysis, data visualization) provide insights into historical IoT data trends, patterns, and anomalies.

- Predictive Analytics: Predictive analytics techniques (e.g., machine learning, time-series forecasting) leverage historical IoT data to make predictions about future trends, events, or outcomes.
- Prescriptive Analytics: Prescriptive analytics techniques (e.g., optimization, simulation) recommend actions or decisions based on IoT data analysis to optimize processes or achieve desired outcomes.

v) Data Visualization:

Dashboards: Interactive dashboards (e.g., Grafana, Kibana) provide visual representations of IoT data in real-time, enabling users to monitor and analyze key metrics and KPIs.

- Charts and Graphs: Charts, graphs, and heatmaps visually represent IoT data trends, patterns, and correlations, facilitating data exploration and decision-making.
- Geospatial Visualization: Geospatial visualization techniques (e.g., maps, GIS) display IoT data on geographic maps, enabling spatial analysis and visualization of sensor data.

f) Machine Learning and Artificial Intelligence (ML &AI)

Artificial Intelligence

branch of computer science devoted to developing data (3.1) processing systems that perform functions normally associated with human intelligence, such as reasoning, learning and self-improvement. **[SOURCE: ISO/IEC/IEEE 24765:2017 – Systems and software engineering – Vocabulary, 3.234] (ISO 24591-2:2024(en) – Smart water management Part 2: Data management guidelines, 3.2)**

<discipline>research and development of mechanisms and applications of AI systems.

Note 1 to entry: Research and development can take place across any number of fields such as computer science, data science, natural sciences, humanities, mathematics and natural sciences.**[SOURCE: IS/ISO/IEC 22989:2022 – Information technology – Artificial intelligence – Artificial intelligence concepts and terminology, 3.1.3]**

<engineered system> set of methods or automated entities that together build, optimize and apply a model so that the system can, for a given set of predefined tasks, compute predictions, recommendations, or decisions.

Note 1 to entry: AI systems are designed to operate with varying levels of automation.

Note 2 to entry: "Predictions" can refer to various kinds of data analysis or production (including translating text, creating synthetic images, or diagnosing a previous power failure). The term does not imply anteriority.**(ISO/TR 6026:2022(en) – Electronic fee collection- Pre-study on the use of vehicle licence plate information and automatic number plate recognition (ANPR) technologies, 3.3)**

Machine Learning

The process of optimizing model parameters through computational techniques, such that the model's behaviour reflects the data or experience. **[SOURCE: IS/ISO/IEC 22989:2022 – Information technology – Artificial intelligence – Artificial intelligence concepts and terminology, 3.3.5]**

The technology of getting computers to act without being explicitly programmed. Example:Speech recognition, effective web search.**(IS/ISO 19731:2017(en) – Digital analytics and web analyses for purposes of market, opinion and social search – Vocabulary and service requirements)**

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing IoT by enabling intelligent decision-making, predictive analytics, and automation. Integrating AI and ML algorithms into IoT systems allows for more efficient data analysis, anomaly detection, and pattern recognition, unlocking valuable insights and improving operational efficiency across various domains such as predictive maintenance, healthcare monitoring, and smart manufacturing.

Some Applications: Predictive maintenance, anomaly detection, automated control, and personalization.

g) IoT Platforms

The infrastructure that enables the deployment, management and operation of IoT devices. **(IS/ISO/IEC 27400:2022(EN) – Cybersecurity – IoT security and privacy - Guidelines, 3.5)**

IoT data collected from sensor nodes is transmitted to cloud platforms for storage, analysis, and visualization. Cloud-based IoT platforms offer features such as data ingestion, real-time processing, device management, security, and integration with other enterprise systems. Examples of cloud providers offering IoT services include Amazon Web Services (AWS), Microsoft Azure IoT, Google Cloud IoT, and IBM Watson IoT. Various Cloud Platforms used in the IoT infrastructure and computing are:

AWS IOT: Amazon Web Services (AWS) IoT is a cloud-based platform for developing, managing, and deploying IoT applications at scale. It offers services for device management, data ingestion, analytics, and integration with other AWS services, enabling end-to-end IoT solutions.

- **MICROSOFT AZURE IOT:** Microsoft Azure IoT is a comprehensive IoT platform offering device management, data processing, analytics, and machine learning capabilities. It provides tools and services for developing, deploying, and managing IoT applications across diverse industries.
- **GOOGLE CLOUD IOT:** Google Cloud IoT is a fully managed platform for building and deploying IoT solutions on Google Cloud Platform (GCP). It offers services for device registry, telemetry ingestion, data processing, and integration with GCP's data analytics and machine learning tools.
- **PARTICLE.IO:** Particle.io is an IoT platform that provides hardware, software, and cloud services for building connected devices and applications. It offers development kits, cloud-based device management, and integration with popular IoT protocols and services.

2. Device Integration

a) Interoperability:

Achieving interoperability and compatibility among diverse IoT systems requires adherence to standard communication protocols, data formats, and interoperability frameworks. Some key considerations for achieving interoperability include:

i) **Standardized Protocols:** Using standardized communication protocols such as MQTT, CoAP, HTTP, and OPC UA ensures interoperability between IoT devices, gateways, and cloud platforms.

ii) **OPEN APIS AND MIDDLEWARE:** Open APIs and middleware platforms provide standardized interfaces for integrating IoT devices and services, enabling seamless interoperability and data exchange.

- API: Standard interface and set of function calls between application software and data access libraries of vehicle navigation systems, in accordance with this International Standard.**(ISO 17267:2009(en) –Health informatics - Requirements for an electronic health record architecture, 2.4).**
- Boundary across which a software application uses facilities of programming languages to invoke software services. (**ISO/IEC 13522-6:1998(en) –Information technology - Coding of multimedia and hypermedia information - Part 6: Support for script interpretation, 3.3)**
- Application Programming Interface: set of functions that may be triggered by a program.**[SOURCE: ISO 13584-101:2003(en) – Industrial automation systems and integration Parts Library – Part 101: Geometrical view exchange protocol y parametric program, 3.1]**

b) IoT Hardware Platforms

i) **Arduino:** Arduino is a popular open-source hardware platform that provides a range of microcontroller-based development boards suitable for prototyping and building IoT applications. Arduino boards are user-friendly, versatile, and supported by a vast community and ecosystem of libraries and shields for sensor and actuator interfacing.

ii) **RASPBERRY PI:** Raspberry Pi is a low-cost, credit card-sized computer that runs Linux-based operating systems. It offers GPIO pins for interfacing with sensors and actuators, making it suitable for IoT projects requiring more computing power and connectivity options.

iii) **ESP8266/ESP32:** These are low-cost, low-power Wi-Fi and Bluetooth-enabled microcontroller platforms commonly used for IoT applications. They offer built-in Wi-Fi connectivity and support for various sensors and actuators, making them ideal for projects requiring wireless communication and internet connectivity.

iv) **PARTICLE PHOTON/ELECTRON:** Particle offers a range of IoT development boards equipped with Wi-Fi and cellular connectivity options. These boards are designed for cloud-connected IoT applications and offer a robust development environment and cloud platform for building and managing IoT devices.

v) **BEAGLE BONE:**Beagle Bone is another single-board computer platform that offers more processing power and connectivity options compared to Arduino and Raspberry Pi. It features built-in Ethernet, USB, and HDMI ports, making it suitable for IoT projects requiring multimedia capabilities.

c) Development Boards:

Development boards provide a platform for prototyping and developing IoT applications. They typically include integrated components such as microcontrollers, connectivity modules, and GPIO pins for interfacing with sensors and actuators. Some popular development boards for IoT include Arduino Uno, Raspberry Pi 4, ESP32 Development Board, Particle Photon, and BeagleBone Black.

d) Operating Systems:

IoT devices often run lightweight operating systems optimized for resource-constrained environments. Some commonly used operating systems for IoT include:

i) **Raspberry Pi OS (formerly Raspbian):** A Debian-based Linux distribution optimized for Raspberry Pi boards, offering a familiar environment for developers and support for a wide range of software packages and libraries.

ii) **ARDUINO IDE (INTEGRATED DEVELOPMENT ENVIRONMENT):** Arduino IDE is a cross-platform software tool used for programming Arduino boards. It provides a simple and intuitive interface for writing, compiling, and uploading code to Arduino-based devices.

iii) **FREERTOS:**FreeRTOS is a popular open-source real-time operating system (RTOS) designed for embedded systems, including IoT devices. It offers a small footprint, pre-emptive multitasking, and support for various microcontroller architectures.

iv) **CONTIKI OS:** Contiki OS is an open-source operating system specifically designed for IoT devices and wireless sensor networks. It provides built-in support for low-power communication protocols such as 6LoWPAN and RPL, making it suitable for battery-operated IoT applications.

3. Challenges and Strategies for Managing IoT Data Effectively:

a) **Volume:** IoT devices generate massive volumes of data, posing challenges for storage, processing, and analysis. Strategies include data compression, aggregation, and tiered storage to manage storage costs and scalability.

Data Volume: Extent of the amount of data (3.1.5) relevant to impacting computation and storage resources and their management during data processing

Note 1 to entry: Data volume becomes important in dealing with large datasets (3.1.11), **[IS/ISO/IEC 20546:2019(en) – Information Technology - Big Data - Overview and Vocabulary]**

VELOCITY: Real-time data streams from IoT devices require fast and efficient processing to extract insights in near real-time. Stream processing platforms and edge computing help handle high data velocity by processing data closer to the source.

Data Velocity: Rate of flow at which data (3.1.5) is created, transmitted, stored, analysed or visualised**[IS/ISO/IEC 20546:2019(en) – Information Technology - Big Data - Overview and Vocabulary]**

b) **VARIETY:** IoT data comes in diverse formats and structures, including time-series data, sensor readings, images, and text. Techniques such as data normalization, schema evolution, and flexible data models address the variety of IoT data sources.

Data Variety: Range of formats, logical models, timescales, and semantics of a dataset (3.1.11)

Note 1 to entry: Data variety refers to irregular or heterogeneous data structures, their navigation, query, and data typing.**[IS/ISO/IEC 20546:2019(en) – Information Technology - Big Data - Overview and Vocabulary]**

c) **VERACITY:** IoT data may be noisy, incomplete, or inaccurate, leading to unreliable insights. Quality assurance techniques, data cleansing, and anomaly detection help ensure data accuracy and reliability.

Data Veracity: Completeness and/or accuracy of data (3.1.5)

Note 1 to entry: Data veracity refers to descriptive data and self-inquiry about objects to support real-time decision-making.**[IS/ISO/IEC 20546:2019(en) – Information Technology - Big Data - Overview and Vocabulary]**

d) **SECURITY AND PRIVACY:** IoT data often contains sensitive information that must be protected from unauthorized access, tampering, and breaches. Strategies include encryption, access control, and data anonymization to safeguard IoT data privacy and security.

e) **SCALABILITY:** IoT deployments must scale to accommodate growing data volumes and device counts. Scalable storage and processing architectures, along with cloud-based solutions, support the scalability requirements of IoT deployments.

f) **INTEROPERABILITY:** IoT systems may consist of heterogeneous devices and platforms, posing challenges for data integration and interoperability. Standardized protocols, APIs, and data formats promote interoperability and compatibility among diverse IoT systems.

Data Interoperability: interoperability concerning the creation, meaning, computation, use, transfer, and exchange of data. **[SOURCE: ISO/IEC 20944-1:2013 – Information technology — Metadata Registries Interoperability and Bindings (MDR-IB) — Part 1: Framework, common vocabulary, and common provisions for conformance, 3.21.12.4](ISO/IEC 30182:2017(EN) – Smart city concept model - Guidance for establishing a model for data interoperability, 2.5)**

g) **REGULATORY COMPLIANCE:** IoT data handling must comply with data protection regulations (e.g., GDPR, CCPA) and industry standards to ensure legal and ethical data practices. Compliance frameworks, data governance, and privacy-by-design principles address regulatory requirements and mitigate risks.

By employing these techniques and strategies, organizations can effectively collect, store, process, analyze, and visualize IoT data, deriving actionable insights and driving value from their IoT deployments while addressing the challenges inherent in managing large volumes of IoT data

4. IoT Gateways:

IoT gateways serve as intermediaries between IoT devices and the cloud, facilitating communication, data aggregation, and protocol translation. They perform various functions such as:

- **PROTOCOL CONVERSION**: IoT gateways support multiple communication protocols and standards, allowing them to bridge the gap between heterogeneous IoT devices and cloud services.

- **DATA AGGREGATION**: IoT gateways collect data from multiple devices and sensors, aggregate it, and transmit it to the cloud in a unified format, reducing bandwidth usage and latency.

  Data Aggregation: process by which information is collected, manipulated, and expressed in summary form.

  Note 1 to entry: Data aggregation is primarily performed for reporting purposes, policy development, health service management, research, statistical analysis, and population health studies.**[SOURCE: ISO/TS 18308:2004 – Health informatics — Requirements for an electronic health record architecture] (ISO/TR 12300:2014(EN) – Health informatics — Principles of mapping between terminological systems, 2.1.4)**

- **EDGE PROCESSING**: Some IoT gateways support edge computing capabilities, enabling local data processing, analytics, and decision-making to reduce dependency on cloud resources and enhance real-time responsiveness.

- **SECURITY:** IoT gateways implement security measures such as encryption, authentication, and access control to protect IoT data and devices from unauthorized access, tampering, and breaches.
- **CONNECTIVITY MANAGEMENT**: IoT gateways manage network connectivity, handle network protocols, and ensure reliable communication between IoT devices and cloud services, even in challenging environments with limited connectivity.

Overall, wireless communication technologies, network topologies, middleware solutions, and IoT gateways play crucial roles in enabling reliable, scalable, and secure IoT deployments, facilitating seamless communication, data exchange, and integration between IoT devices, edge devices, and cloud platforms.

5. IoT Security and Privacy:

a) Security Threats in IoT Deployments:

i) **Unauthorized Access:** Hackers may attempt to gain unauthorized access to IoT devices, networks, or data, compromising the confidentiality and integrity of IoT systems.

ii) **DATA BREACHES:** Data breaches occur when sensitive information stored or transmitted by IoT devices is accessed or stolen by unauthorized parties, leading to privacy violations and financial losses.

Data Breach: compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed.**[SOURCE: IS/ISO/IEC 27040:2015 – Information technology — Security techniques — Storage security, 3.7] (IS/ISO/IEC 27018:2019(EN) – Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, 3.1)**

iii) **DENIAL OF SERVICE (DOS) ATTACKS:** DoS attacks aim to disrupt IoT services by overwhelming devices or networks with excessive traffic, rendering them inaccessible to legitimate users.

DoS: prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users. **(IS/ISO/IEC 27033-1:2015(EN) – Information technology — Security techniques — Network security — Part 1: Overview and concepts, 3.9)**

iv) **MAN-IN-THE-MIDDLE (MITM) ATTACKS:** MitM attacks intercept and modify data exchanged between IoT devices and servers, enabling attackers to eavesdrop, tamper with, or steal sensitive information.

Man-in-the-middle attack: attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge. **(ISO/IEC 29115:2013(EN) – Information technology — Security techniques — Entity authentication assurance framework, 3.16)**

v) **DEVICE COMPROMISE:** Vulnerable IoT devices may be compromised and repurposed as bots in botnets, enabling attackers to launch large-scale attacks or execute malicious activities.

Device Compromise: successful defeat of the physical or logical protections provided by the SCD (3.28), resulting in the potential disclosure of sensitive information (3.30) or unauthorized use of the SCD. **(ISO 13491-1:2016(EN) - Financial services - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods, 3.13)**

b) **Encryption Techniques:**

i) **Transport Layer Security (TLS):** TLS encrypts data transmitted between IoT devices and servers, ensuring confidentiality and integrity during communication. It protects against eavesdropping, tampering, and data interception.

transport layer security: protocol for secure communication over the internet**(ISO 5231:2022(en) – Extended farm management information systems data interface (EFDI) — Concept and guidelines, 3.21)**

ii) **END-TO-END ENCRYPTION:** End-to-end encryption ensures that data is encrypted at the source device and decrypted only by the intended recipient, preventing unauthorized access or tampering throughout the communication path.

iii) **DATA ENCRYPTION:** Data encryption techniques such as AES (Advanced Encryption Standard) encrypt sensitive data stored on IoT devices or transmitted over networks, safeguarding it from unauthorized access or theft.

iv) **PUBLIC KEY INFRASTRUCTURE (PKI):** PKI establishes trust and enables secure communication between IoT devices and servers through digital certificates, key management, and cryptographic protocols.

PKI: A framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies. **(ISO/IEC 24775-2:2021(EN) – Information technology — Storage management — Part 2: Common Architecture, 3.1.50)**

c) **Authentication Mechanisms:**

i) **Device Authentication:** Device authentication verifies the identity of IoT devices before granting access to network resources or sensitive data. Techniques include pre-shared keys, digital certificates, and mutual authentication protocols.

ii) **USER AUTHENTICATION:** User authentication ensures that only authorized users can access IoT devices or platforms, typically through passwords, biometrics, two-factor authentication (2FA), or multi-factor authentication (MFA).

d) **Best Practices for Ensuring IoT Security and Privacy:**

i) **Patch Management:** Regularly update and patch IoT devices, firmware, and software to address known vulnerabilities and security flaws.

Processes applied during patch development and patch release. **(ISO/IEC TS 9569:2023(en) – Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045, 3.12)**

ii) **SECURE CONFIGURATIONS:** Configure IoT devices and networks with secure settings, disable unnecessary services, change default passwords, and implement access controls to minimize attack surfaces.

iii) **NETWORK SEGMENTATION:** Segment IoT devices into separate networks or VLANs (Virtual Local Area Networks) to isolate them from critical infrastructure and limit the impact of potential breaches.

iv) **SECURITY MONITORING:** Implement intrusion detection systems (IDS), intrusion prevention systems (IPS), and security analytics to monitor IoT networks for suspicious activities, anomalies, and breaches.

v) **DATA MINIMIZATION:** Collect and store only the minimum amount of data necessary for IoT operations, adhere to data retention policies, and anonymize or pseudonymize sensitive information to protect privacy.

vi) **SECURE COMMUNICATION:** Encrypt data in transit and at rest using strong encryption algorithms and protocols, enforce secure communication standards, and validate the integrity of transmitted data.

CHAPTER V

STANDARDIZATION – INDIAN STANDARDS ON INTERNET OF THINGS (IoT)

CHAPTER V

STANDARDIZATION – INDIAN STANDARDS ON INTERNET OF THINGS (IoT)

This Section focuses on the standardization work being done by Bureau of Indian Standards (BIS) in the major areas/fields of Internet of Things (IoT).

BIS is a founder member of International Organization of Standards (ISO) and works closely with International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in the standardization work in many technological areas including the Internet of Things (IoT). BIS actively participates in the standardization work being undertaken at the International level through the various technically committees set up and holds leadership position in some of the International technical committees.

This section contains information on various Indian standards applicable in the major areas of Internet of Things (IoT). As the work is being done in coordination with the International Standards bodies, references appear to the applicable international committees along with the national technical committees of BIS. The details of abbreviations used for various BIS technical committees and the International technical committees of ISO and IEC which the user encounters in the information given in this section is given below along with a brief description of the work of the committee:

Technical committees of BIS

LITD 27-Internet of Things and & Digital Twin Sectional Committee

Scope: To develop standards in the field of Internet of Things and related technologies including sensor networks.

Liaison Details:

ISO/IEC/JTC1 TC- SC-41 (O)
ISO/IEC JTC 1/SC 41
ISO/IEC/JTC1 TC- SC-41 (P): Internet of Things and Digital Twin

LITD 28 – Smart Infrastructure Sectional Committee

Scope: Standardization in the field of Smart Cities (Electro-technical and ICT aspects) and related domains including Smart Home/Building and Active assisted living.

Liaison Details:

IEC TC- (P): SyC Smart Cities; ISO/IEC TC- (P): Smart Cities.
LITD 30 - Artificial Intelligence Sectional Committee

Scope: Standardization in the area of Artificial Intelligence and Big Data

Liaison Details:

ISO/IEC/JTC1 TC- SC-42 (P): Artificial intelligence;

LITD 31 - Cloud Computing, IT & Data Centres Sectional Committee

Scope: To establish Indian standards in the field of a) Cloud Computing and Distributed Platforms including Foundational concepts and technologies, Operational issues, and Interactions among Cloud Computing systems and with other distributed systems b) Assessment methods, design practices, operation and management aspects to support resource efficiency, resilience and environmental sustainability for and by information, data centres and other facilities and infrastructure necessary for service provisioning

Liaison Details:

ISO/IEC/JTC1 TC- SC-38 (P): Cloud Computing Fundamentals (CCF)
ISO/IEC/JTC1 TC- SC-38 (P): Data in cloud computing and related technologies
ISO/IEC/JTC1 TC- SC-39 (P): Sustainability, IT and data centres
ISO/IEC/JTC1 TC- SC-39 (P): Resource Efficient Data Centres
ISO/IEC/JTC1 TC- SC-39 (P): Sustainable facilities and infrastructures
ISO/IEC/JTC1 TC- SC-39 (P): Eco-design of digital services;

LITD 32 - Biometrics Sectional Committee

Scope: Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems.

Liaison Details:

ISO/IEC/JTC1 TC- SC-37 (P): Biometrics;

Technical committees of ISO

ISO/IEC JTC 1

ISO-IEC Joint Technical Committee (JTC 1) is a consensus based, voluntary international standards group focussing on information technology (IT).

Scope: Standardization in the field of information technology

ISO/IEC JTC 1/SC 27 Technical Committee on Information security, cybersecurity and privacy protection

Scope: The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;

- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

ISO/IEC/ JTC 1/SC 29 Technical committee on coding of audio, picture, multimedia and hypermedia information

Scope: Standardization in the field of

- Efficient coding of digital representations of images, audio and moving pictures, including
- Conventional (natural, computer-generated and immersive) images, moving pictures and audio
- Invisible light and other sensory (such as medical and satellite) images
- Static and dynamic graphic objects
- Efficient coding of other digital information, including
- Multimedia, environment and user related metadata
- Sensor and actuator information related to audiovisual information
- Other digital data in agreement with the relevant committee, such as genomics
- Digital information support, including
- Synchronization, presentation, storage and transport of single or combinations of media
- Media security and privacy management
- Quality of Experience evaluation and system performance metrics

ISO/IEC JTC 1/SC 41: Technical committee on Internet of things and digital twin

ISO/IEC JTC 1/SC 41 is being supported administratively by IEC (International Electrotechnical Commission). All information related to ISO/IEC JTC 1/SC 41 is available on the IEC web site also.

Scope: Standardization in the area of Internet of Things and related technologies.

- Serve as the focus and proponent for JTC 1's standardization programme on the Internet of Things and Digital Twin, including their related technologies.
- Provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things and Digital Twin related applications.

Working Groups under ISO/IEC JTC 1/SC 41

a) ISO/IEC JTC 1/SC 41/WG 3: IoT Architecture

b) ISO/IEC JTC 1/SC 41/WG 4: IoT Interoperability

c) ISO/IEC JTC 1/SC 41/WG 5: IoT Applications

d) ISO/IEC JTC 1/SC 41/WG 6: Digital Twin

e) ISO/IEC JTC 1/SC 41/WG 7: Maritime, Underwater IoT and Digital Twin Applications

(https://www.iso.org/committee/6483279.html)

ISO/TC 184 Technical committee on Automation systems and integration

Scope: Standardization in the field of automation systems and their integration for design, sourcing, manufacturing, production and delivery, support, maintenance and disposal of products and their associated services. Areas of standardization include information systems, automation and control systems and integration technologies.

Note: There will be active collaboration with the relevant technical committees responsible for areas such as machines, manufacturing resources and facilities, robotics, electrical and electronic equipment, PLC for general application, quality management, industrial safety, information technologies, multi-media capabilities, and multi-modal communication

To give an actual glimpse of the coverage of a standard, the abstract/introduction/ scope of the standard has been included in this section.

Indigenous standards formulated by Bureau of Indian Standards can be freely downloaded (see https://www.bis.gov.in for details). However, the Indian Standards formulated by adopting International Standards are not included as part of free downloads.

A. BASIC/GENERAL STANDARDS ADDRESSING (IoT)

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

This standard has been prepared by the Smart Infrastructure Sectional Committee, LITD 28 of the Electronics and Information Technology Division Council.

This standard defines the reference architecture for IoT systems, providing a structured framework for designing and implementing IoT solutions. This standard outlines the key components and interactions required for a successful IoT deployment, ensuring that all elements work together effectively.

The standard is essential for guiding the development of IoT systems, as it establishes a common architecture that supports scalability, interoperability, and integration. It helps organizations design IoT solutions that meet their specific needs while aligning with industry best practices and ensuring scalability, security and interoperability.

The IoT Reference Architecture given in the standards includes a concept model, reference models, architectures and deployment views.

The clauses on Introduction and Scope of this standard are reproduced below:

INTRODUCTION

0.1 Background

The Internet of Things (IoT) or Machine to Machine (M2M) ecosystem generally comprises of devices and/or sensors which generate information in the form of data which flows through various electronic communication means to a set of Digital Infrastructure for storing, forwarding, analysis, and subsequent actions by humans or machines including actuators.

0.2 Motivation & Objectives

IoT is considered to be a significant element of the digital infrastructure and is an integral part of the 'Unified digital infrastructure ICT Reference Architecture (ICTRA) defined in IS 18000. Therefore, it is necessary to provide a special focus on the standardization of the IoT Ecosystem.

This Standard recommends a blueprint for realizing the digital infrastructure required for scalable, secure and globally interoperable IoT solutions. The IoT Reference Architecture described in this Standard includes a concept model, reference models, architectures and deployment views, along with references to global standards and specifications, such as to facilitate an orderly proliferation of the IoT Ecosystem.

A significant other motivation is to ensure that the IoT sub-systems seamless integrate with the sub- systems involved with performing towards the ICT RA specifications. The IoT RA focuses on the three key principles enshrined in the ICT RA, namely:

a) Interoperability — Refers to the ability of diverse systems and components to work together, even as parts from diverse set of suppliers are substituted and integrated;

b) Composability — Refers to the ability to combine discrete components into a complete system to achieve a set of goals and objectives; and

c) Harmonization — Refers to achieving compatibility between technologies and systems, even when they at first appear incompatible.

The Standard is useful for anyone involved in the design, development, deployment, and implementation or certification of an IoT device, network or application ecosystem. Further, the IoT Reference Architecture assists in obtaining the objectives of IS 18000, which are to provide a unified digital infrastructure architecture that can serve as a template for both the city administrators and those who are the consumers of such IoT and ICT based solutions, as well as the IoT and ICT solution providers who develop and deploy such solutions.

SCOPE

This Indian Standard describes the Internet of Things (IoT) Reference Architecture, that comprises IoT Concept Model, IoT Reference Models (Domain based IoT reference model, Entity based IoT reference model) and IoT Deployment Views.

IoT Concept Model and Reference models elaborate the interactions between various entities, both digital and non-digital.

2) IS/ISO/IEC/TR 22417: 2017 - Information Technology – Internet of Things (IoT) – IoT Use Cases

This standard has been brought out by Internet of Things and Related Technologies Sectional Committee, LITD 27 of **the Electronics and Information Technology Division Council and is i**dentical with IS/ISO/IEC TR 22417 : 2017 'Information technology — Internet of things (IOT) — IOT use cases' issued by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) jointly**.**

This standard provides a comprehensive exploration of various IoT use cases across multiple domains. This standard is instrumental in illustrating how IoT technologies can be applied to address real-world challenges. It includes detailed examples from diverse sectors such as smart cities, healthcare, and industrial automation, demonstrating the practical benefits and applications of IoT solutions.

The standard aims to guide stakeholders in understanding the potential of IoT by showcasing practical implementations. It serves as a reference for deploying IoT technologies in a way that enhances operational efficiency and effectiveness. Through case studies and illustrative scenarios, the document highlights how IoT can solve specific industry problems and improve service delivery.

The scope of the standard covers the identification and detailed description of various IoT use cases. It provides an overview of how IoT can be effectively implemented in different domains to address particular challenges. By examining specific scenarios, the standard offers valuable insights into the practical deployment of IoT technologies and their impact on various sectors.

This standard serves as a guide for organizations looking to understand and adopt IoT solutions, offering a framework for assessing the benefits and applications of IoT in real-world settings. It outlines the integration of IoT technologies into existing systems and processes, facilitating informed decision-making and strategic planning.

The clauses on Introduction and Scope of this standard are reproduced below:

INTRODUCTION

This document captures the results of a use case input process that began with the call for contributions of IoT (Internet of Things) use cases in 2015-05. The current document reflects contributions and discussions by ISO/IEC JTC 1 experts and liaison members, JTC 1 national mirror committees, and user organizations. This document also contains material gathered from reports, IoT research projects and group output from the JTC 1 working group on the Internet of Things meetings in September 2015 (Ottawa), January 2016 (Shanghai) and May 2016 (Berlin). In total 25 IoT use cases were submitted by the end of July 2016. To start the project, the working group members were requested to submit use cases using the provided template.

The use case submissions consisted of the title of the use case, a description and the origin of the use case. Contributors did not always provide information for all the fields of the template and did not necessarily revise their input when a modified use case template was introduced. The use case template helped to group and categorizes the use cases according to the identified IoT requirements and experience of users. Understanding the application of IoT systems made it easier to identify categories and highlight use case commonalities. Where multiple use cases fall in the same category and had overlapping items, they were consolidated into one section or extended use case. All selected use cases have real-world validity. Gaps were filled by adding extra use cases and future developments were also considered. Functional requirements were extracted from the use cases and have assisted in the development of the IoT Reference Architecture. There is a natural mapping from the user experience-based use cases to the clustered technical use cases, where specific technical and functional requirements are expressed. Collecting the use cases allowed the working group to assess the general applicability of the IoT reference architecture in ISO/IEC 30141 to current IoT applications. Experts from the following national committees, liaison organizations and research projects contributed use cases on IoT: Canada, China, Japan, UK, JTC 1/SC 27, JTC 1/SC 29, ISO/TC 184, and the Vicinity Project. Technological advances have enormous potential to make the society more efficient and digitally inclusive and IoT implementations are demonstrating convergence of information and communications technology and their widespread application.

The target audience for this document includes:

- IoT service users who can understand how their IoT requirements are considered by anIoT service provider;
- IoT service providers who can learn about users IoT needs, and can also learn how tooperate active assisted living systems;
- IoT application developers who can develop IoT applications according to the needs of theIoT service users;
- controllable equipment and ICT device manufacturers who want to know what the IoTinterface requirements are;
- administrations and government authorities that have to act as IoT service users and IoTregulators.

SCOPE

This document identifies IoT scenarios and use cases based on real-world applications and requirements. This document comprises 25 use cases for Internet of Things submitted to the ISO/IEC JTC 1 working group on the Internet of Things between June 2015 and July 2016. Use cases are a well-known tool for expressing requirements at a high level and demonstrating their real-life relevance. The use cases provide a practical context for considerations on interoperability and standards based on user experience. Use cases clarify where existing standards can be applied and highlight where standardization work is needed. An objective of this document is to assist in the identification of potential areas for standardization in the IoT environment to ensure ease of operation and interoperability.

B) CONNECTIVITY AND INTEROPERABILITY STANDARDS FOR IoT

3) IS/ISO/IEC 21823-1: 2019 Internet of Things (IoT) — Interoperability for IoT systems Part 1 Framework *(Finalized Draft Standard under print at the time of preparation of this handbook)*

INTRODUCTION

Internet of Things (IoT) systems involves communications between different entities. This applies to connections between different IoT systems. It also applies to the many connections that exist within IoT systems. The various entities and their connections are described in ISO/IEC 30141.

The ISO/IEC 21823 series addresses issues that relate to interoperability of the communications between IoT systems entities. ISO/IEC 21823 1 describes a general framework for interoperability of IoT systems. This includes a facet model for interoperability which includes five facets of interoperability (i.e. transport, syntactic, semantic, behavioural and policy). This document addresses the framework to achieve interoperability for IoT; the specific facets are addressed in other parts of ISO/IEC 21823.

SCOPE

This document provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems.

This document ensures that all parties involved in building and using IoT systems have a common understanding of interoperability as it applies to IoT systems and the various entities within them.

4) IS/ISO/IEC 21823-2 : 2020 Internet of Things (IoT) — Interoperability for IoT systems Part 2 Transport interoperability

INTRODUCTION

Internet of Things (IoT) systems involve communications among different entities. This applies to connections between different IoT systems. It also applies to the many connections that exist within IoT systems. The various entities and their connections are described in ISO/IEC 30141.

The ISO/IEC 21823 series addresses issues that relate to interoperability of the communications between IoT systems entities, both between different IoT systems and within a single IoT system. ISO/IEC 21823-1 describes a general framework for interoperability for IoT systems. This includes a facet model for interoperability which includes five facets of interoperability: transport; syntactic; semantic; behavioural; policy. This document (ISO/IEC 21823-2) addresses the transport interoperability for IoT systems. The semantic facet of interoperability will be addressed in a future International Standard (ISO/IEC 21823-3). The potential other parts address the syntactic facet, the behavioural facet and the policy facet of interoperability.

As described in ISO/IEC 30141, IoT systems have multiple different types of networks connecting the various system entities – network connectivity, addressing the transport facet of the interoperability model, is thus of great importance in the description of interoperability for IoT systems. The different networks need to be combined to provide the necessary network connectivity between entities which are attached to each of the networks – in short, to enable those entities to be interoperable. An example are the centralized applications and services which need to receive data from remote sensors, or issue commands to remote actuators.

Network connectivity is the name given to the methods by which the various networks in an IoT system are connected to one another. This document specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system.

To provide seamless communication and interaction between and within networks, it is important to solve network level interoperability issues in

IoT systems. There are four types of networks in IoT systems, including user networks, service network, access network and proximity network, which are defined in ISO/IEC 30141 and used in ISO/IEC 21823-1. The relationship and interface among these networks for supporting networks interoperability need to be specified.

For this purpose, this document focuses on network connectivity, which is the precondition of interoperability in IoT systems.

SCOPE

This part of IEC 21823 specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies:

- transport interoperability interfaces and requirements between IoT systems;

- transport interoperability interfaces and requirements within an IoT system.

5) **IS/ISO/IEC 21823-3 : 2020 Internet of Things (IoT) — Interoperability for IoT systems Part 3 Semantic Interoperability** *(Finalized Draft Standard under print at the time of preparation of this handbook)*

The use of the Internet of Things (IoT) is increasing every year, in application areas such as manufacturing, healthcare, and new cross-domain applications related to smart cities (e.g. water, energy, transport, or health). Most IoT systems want to share information, which can be done by interoperability. Mechanisms are therefore needed on how to exchange information and use associated data and data description.

IoT interoperability is described as a successful interaction among entities specified in ISO/IEC 30141 (Internet of Things (IoT) – Reference Architecture), for instance between IoT services provided by different IoT service providers. It can be achieved using the interoperability facet model defined in ISO/IEC 21823 1, which defines five facets: transport, syntactic, semantic, and behavioural and policy interoperability.

IoT semantic interoperability is the facet which enables the exchange of data between IoT systems using understood data information models (or semantic meanings). Semantic interoperability means that information in different data information models can be translated into understandable meaning and exchanged between applications. Semantic interoperability provides the capability for applications to understand exchanged information. Semantic interoperability for IoT is achieved by invoking services, and by using specific knowledge and concepts of IoT

Semantic interoperability is achieved through the use of metadata, or descriptions of data. The approach of providing data and descriptions has been widely used in IT systems.

Two examples are:

a) conceptual schemas have been used to describe database content;

b) record layouts have been used to display the content of a database record.

Many services invoked by semantic interoperability involve metadata, thus enabling their discovery, understanding and (re)usability.

Metadata provides IoT systems with a common understanding of exchanged data.

Knowledge that metadata represents can be described using ontologies. In other words, semantic interoperability needs shared, unambiguous, machine-understandable metadata, to be able to perform exchange of information using metadata. The application of semantics in IoT has still been limited because most metadata are developed independently, making it difficult for IoT entities or applications to interoperate semantically. In this document, an ontology-driven approach for semantic interoperability is specified to design and specify metadata, so that the sensors, devices, systems and services can express metadata information and data by applying the ontologies to achieve semantic interoperability. Stakeholders targeted by this document include ontology engineers and IoT system engineers who are building semantic interoperability capabilities for IoT systems. This document also specifies methods and techniques to build semantic interoperability for IoT systems. Clause 5 focuses on the IoT semantic interoperability process. Clause 6 focuses on the IoT semantic interoperability life cycle management.

Informative annexes provide additional information and guidance. Annex A, Annex B and Annex C provide guidance on how to learn IoT semantic interoperability, develop IoT semantic interoperability, and manage IoT semantic interoperability life cycle, respectively. Annex D provides ontological specification of the IoT Reference Architecture specified in ISO/IEC 30141 (Internet of Things (IoT) – Reference Architecture). Annex E provides related existing ontologies that are applicable for IoT semantic interoperability.

(The above text has been taken from the INTRODUCTION given in the standard. However, the diagrams given in this clause in the document have not been reproduced here)

SCOPE

This document provides the basic concepts for IoT systems semantic interoperability, as described in the facet model of ISO/IEC 21823 -1, including:

– Requirements of the core ontologies for semantic interoperability;

– Best practices and guidance on how to use ontologies and to develop domain-specific applications, including the need to allow for extensibility and connection to external ontologies;

– Cross-domain specification and formalization of ontologies to provide harmonized utilization of existing ontologies;

– relevant IoT ontologies along with comparative study of the characteristics and approaches in terms of modularity, extensibility, reusability, scalability, interoperability with upper ontologies, and so on;

– use cases and service scenarios that exhibit necessities and requirements of semantic interoperability.

6) **IS/ISO/IEC 21823-4 : 2020 Internet of Things (IoT) — Interoperability for IoT systems Part 4 Syntactic Interoperability** *(Finalized Draft Standard under print at the time of preparation of this handbook)*

INTRODUCTION

In the world of the Internet of Things (IoT), heterogeneous systems and devices need to be connected and exchange data with others. How data exchange can be implemented becomes a key issue of interoperability among IoT industries. Information models (IMs), which can well represent specifications of data, are adopted and utilized to solve the interoperability problem. Meanwhile, as systems and devices in IoT can have different information models with different modelling methodologies and formats, interoperability based on different information models is recognized as an urgent problem. The IoT interoperability related systems and applications have an 11 trillion market potentially.

The ISO/IEC 21823 series standards address issues that relate to interoperability both between different IoT systems and within a single IoT system. ISO/IEC 21823-1 describes a general framework for interoperability for IoT systems. It includes a five facet model for interoperability that includes transport, syntactic, semantic, behavioural, and policy viewpoints.

Different parts of ISO/IEC 21823, based on one of the facets, provide specifications from their corresponding viewpoints. Each of the parts can refer to others but is independent. Currently, ISO/IEC 21823-2 defines specifications from the transport viewpoint, ISO/IEC 21823-3 defines requirements, provides guidance, etc. from the semantic viewpoint, and ISO/IEC 21823-4 specifies the syntactic interoperability.

Syntactic interoperability means that exchanged information can be understood by the participating IoT systems which contain IoT devices. In more detail, the syntactic interoperability is related to the information models' representing formats, structures, and grammar of their modelling languages such as a length of a data string, constraints on data types, and forbidden characters.

This document first provides the principle of how to achieve syntactic interoperability based on metamodel-driven approaches. In other words, the reason why the information exchange rules based on metamodels can support syntactic interoperability among different IoT systems will be elaborated. Secondly, requirements on information models such as metamodels and models of IoT systems including IoT devices are described. Features related to IoT devices such as the identifier, device type, setup environments, and functions need to be considered to accomplish syntactic interoperability among different information models utilized in IoT systems. Thirdly, a framework for processes on developing information exchange rules related to IoT devices from the syntactic viewpoint is provided. For example, the kinds of metamodels, and the types of entities and relationships that shall be selected are specified, and the procedure of how to build the information exchange rules from different information models is provided.

In Annex A, possible intrinsic and extrinsic properties of IoT devices are listed as additional information of Clause 6. In Annex B, a use case of how the syntactic interoperability in accordance with specifications in this document among industrial IoT systems and IoT devices is described.

With this document, system and device vendors, who need to improve and/or develop their products to comply with IoT requirements, can implement specifications of this document to their products for an automatic or semi-automatic realization of IoT syntactic interoperability.

SCOPE

This part of ISO/IEC 21823 specifies the IoT interoperability from a syntactic point of view. In this document, the following specifications for IoT interoperability from a syntactic viewpoint are included:

- a principle of how to achieve syntactic interoperability among IoT systems which include IoT devices;
- requirements on information related to IoT devices for syntactic interoperability;
- a framework for processes on developing information exchange rules related to IoT devices from the syntactic viewpoint.

7) **IS 18010 (Part 1): 2020 - Unified Digital Infrastructure - Unified Last Mile Communication Protocols Stack Part 1 Reference Architecture**

This standard has been prepared by the Smart Infrastructure Sectional Committee, LITD 28 of the Electronics and Information Technology Division Council. The standard provides reference architecture for unified last mile communication protocols within the digital infrastructure.

This standard outlines the protocols and technologies necessary for effective communication between IoT devices and the broader digital infrastructure, ensuring reliable and efficient data transmission.

The standard is important for ensuring that last mile communication in IoT systems is robust and interoperable. It defines the framework for integrating various communication protocols to support seamless data exchange and connectivity.

The standard includes the specification of the reference architecture for last mile communication protocols in unified digital infrastructure. It covers the protocols and technologies required for effective communication between IoT devices and the digital infrastructure.

This standard aims to support the development of reliable and interoperable communication solutions, facilitating seamless data transmission and connectivity within IoT systems.

The clauses on Introduction and Scope of this standard are reproduced below:

INTRODUCTION

Rapid urbanization over the past two decades has led to the mushrooming of megacities (accepted as those with a population in excess of ten million) around the world. The sheer size and scale of these cities place huge pressure on infrastructure development, public services provision, and environmental sustainability. Cities nationally and internationally are main drivers of economic activity, growth and in the current context, recovery, but this output depends on a comprehensive infrastructure to deliver physical and social resources the fuel of a city's 'economic engine'. The economic performance of a city is inextricably linked to its physical and communications infrastructures, and the delivery of resources through these infrastructures. The society, the business, the infrastructure, the services and all other aspects of the civilization on the planet Earth are going through a paradigm shift in the wake of technological advancements, especially in the field of ICT. All the ecosystems like smart cities, smart grid, smart buildings, smart factories etc. are in the process of making the following three classes of transformations:

a) Improvement of Infrastructure — To make it resilient and sustainable;

b) Addition of the Digital Layer — Which is the essence of the smart paradigm; and

c) Business Process Transformation — Necessary to capitalize on the investments in smart technologies.

Smart city technologies based on digital infrastructure and digital services offers a potential way of monitoring and managing physical and social resource in the city. Digital technologies can collect sufficiently large amounts of data to support very close matching of supply availability against demand requirements. The new communication potential from sensors on buildings, roads and other elements of the city and the sharing of data between service delivery channels, if integrated, will enable the city to improve services, monitor and control resource usage and react to real-time information. A defining feature of smart cities is the ability of the components and systems to function efficiently in an integrated manner as well as independently. The optimal use of resources across a complex urban environment depends on the interaction between different city services and systems. To identify the most effective use of resources, therefore, requires communication between the different component systems (for example, energy consumption monitored by smart metering combined with external temperature and sunlight monitoring on the building to reduce the energy consumption). Smart infrastructure is the result of combining physical infrastructure with digital infrastructure, providing improved information to enable better decision-making, faster and cheaper. However, the rapid growth in communication technologies for last more than four-five decades has provided the users with multiple choices with their respective diversities and USPs for different applications and use cases. As a result, stakeholders of different ecosystems have chosen different technologies and protocols to meet their respective applications needs. In some cases, even different segmented stakeholders of a common ecosystem have developed/adopted different, communication technologies, protocols, data semantics and standards. The soloed way of deploying the IoT/M2M infrastructure is not desirable and a need was felt to have a harmonized common last-mile communication architecture approach. In a smart city scenario, to enable interoperability between divergent devices as well as applications while maintaining identity and access control, it is desirable to have common last-mile communication architecture. This will also ensure feasibility in the sharing of data with ensured security and privacy. The IoT value chain is perhaps the most diverse and complicated value chain. Due to heterogeneity and lack of convergence the smart nodes of one network cannot talk to smart nodes of the other networks. The variety of solutions with limited interoperability exist for different areas like home automation, building automation, industrial automation etc. This limited interoperability is the major driving factor to consider developing Unified, resilient, secure and sustainable, ICT framework for smart infrastructure developments. The Standard IS 18000 'Unified digital infrastructure ICT reference architecture' (presently under development) defines a comprehensive ICT reference architecture for a resilient, secure and sustainable digital infrastructure for smart cities, districts, states or nations. The unified last mile communication protocols stack reference architecture is an integral part of the 'unified digital infrastructure ICT reference architecture' and it layouts the contours of unified communication for 'smart city' and 'smart infrastructure'.

SCOPE

1.1 This Indian Standard defines the Unified Last Miles Communication Protocol Stack – Reference Architecture (ULMCP-RA) for communication devices deployed in digital infrastructure.

1.2 The reference architecture described in this standard supports devices which operate using different communication technologies and deployed in any of the following topologies:

a) Personal Area Network (PAN);
b) Neighbour Area Network (NAN);
c) Field Area Network (FAN); and
d) Wide Area Network (WAN).

1.3 This standard also provides a brief description of other standards in the last mile communication protocol stack series.

NOTE — This standard covers only IPv6 based networks.

8) **IS/ISO/IEC 30118-1: 2021 - Information Technology – Open Connectivity Foundation (OCF) Specification Part 1: Core Specification**

This standard has been brought out by Internet of Things and Related Technologies Sectional Committee, LITD 27 of **the Electronics and Information Technology Division Council and is i**dentical with ISO/IEC 30118-1: 2021. It establishes the fundamental protocols and mechanisms required for effective communication and interoperability among IoT devices within the Open Connectivity Foundation (OCF) framework. This core specification defines the essential communication protocols that enable different IoT devices to interact seamlessly, ensuring that devices from various manufacturers can work together.

The standard is critical for developing a unified network where diverse IoT systems and devices can operate in concert. By standardizing communication protocols, IS/ISO/IEC 30118-1:2021 facilitates the integration of devices into a cohesive ecosystem, promoting interoperability and enhancing the overall functionality of IoT solutions.

The standard includes the specification of core communication protocols necessary for IoT device interaction within the OCF framework. It details the mechanisms for device discovery, communication, and data exchange, ensuring that devices from different manufacturers can operate together seamlessly.

This standard outlines the requirements for achieving interoperability and provides guidelines for implementing core communication functions. It aims to ensure that IoT devices can integrate effectively into a unified network, supporting consistent and reliable operations across diverse systems.

The clauses on Introduction and Scope of this standard are reproduced below:

INTRODUCTION

This document, and all the other parts associated with this document, were developed in response to worldwide demand for smart home focused Internet of Things (IoT) devices, such as appliances, door locks, security cameras, sensors, and actuators; these to be modelled and securely controlled, locally and remotely, over an IP network. While some inter-device communication existed, no universal language had been developed for the IoT. Device makers instead had to choose between disparate frameworks, limiting their market share, for developing across multiple ecosystems, increasing their costs. The burden then falls on end users to determine whether the products they want are compatible with the ecosystem they bought into, or find ways to integrate their devices into their network, and try to solve interoperability issues on their own. In addition to the smart home, IoT deployments in commercial environments are hampered by a lack of security. This issue can be avoided by having a secure IoT communication framework, which this standard solves. The goal of these documents is then to connect the next 25 billion devices for the IoT, providing secure and reliable device discovery and connectivity across multiple OSs and platforms. There are multiple proposals and forums driving different approaches, but no single solution addresses the majority of key requirements. This document and the associated parts enable industry consolidation around a common, secure, interoperable approach.

ISO/IEC 30118 consists of eighteen parts, under the general title Information technology – Open Connectivity Foundation (OCF) Specification. The parts fall into logical groupings as described herein:

- Core framework
  - Part 1: Core Specification
  - Part 2: Security Specification
  - Part 13: Onboarding Tool Specification
- Bridging framework and bridges
  - Part 3: Bridging Specification
  - Part 6: Resource to Alljoyn Interface Mapping Specification
  - Part 8: OCF Resource to oneM2M Resource Mapping Specification
  - Part 14: OCF Resource to BLE Mapping Specification
  - Part 15: OCF Resource to EnOcean Mapping Specification
  - Part 16: OCF Resource to UPlus Mapping Specification
  - Part 17: OCF Resource to Zigbee Cluster Mapping Specification
  - Part 18: OCF Resource to Z-Wave Mapping Specification
- Resource and Device models
  - Part 4: Resource Type Specification
  - Part 5: Device Specification
- Core framework extensions
  - Part 7: Wi-Fi Easy Setup Specification
  - Part 9: Core Optional Specification
- OCF Cloud
  - Part 10: Cloud API for Cloud Services Specification
  - Part 11: Device to Cloud Services Specification
  - Part 12: Cloud Security Specification

SCOPE

The OCF Core specifications are divided into a set of documents:

– Core specification (this document): The Core specification document specifies the Framework, i.e., the OCF core architecture, interfaces, protocols and services to enable OCF profiles implementation for Internet of Things (IoT) usages and ecosystems. This document is mandatory for all Devices to implement.

– Core optional specification: The Core optional specification document specifies the Framework, i.e., the OCF core architecture, interfaces, protocols and services to enable OCF profiles implementation for Internet of Things (IoT) usages and ecosystems that can optionally be implemented by any Device.

– Core extension specification(s): The Core extension specification(s) document(s) specifies optional OCF Core functionality that are significant in scope (e.g., Wi-Fi easy setup, Cloud).

9) IS/ISO/IEC 30118-2: 2021 Information technology Open Connectivity Foundation OCF Specification Part 2: Security specification

IS/ISO/IEC 30118-2:2021 addresses the security requirements essential for protecting IoT devices and communications within the OCF ecosystem. This specification provides detailed guidelines for implementing robust security measures, including authentication, encryption, and access control, to safeguard against unauthorized access and data breaches.

The standard is crucial for ensuring the security and privacy of IoT systems. By defining comprehensive security measures, IS/ISO/IEC 30118-2:2021 helps protect both device integrity and user data, fostering trust and reliability in IoT solutions.

The scope of IS/ISO/IEC 30118-2:2021 includes specifying security requirements for IoT devices and their communications within the OCF framework. It covers guidelines for implementing secure authentication, encryption, and access control mechanisms to protect against security threats.

This standard aims to ensure that IoT devices operate securely within the OCF ecosystem, providing a framework for safeguarding against potential vulnerabilities and maintaining data privacy. It offers practical guidance for enhancing the security posture of IoT systems and protecting sensitive information.

SCOPE

This document defines security objectives, philosophy, Resources and mechanism that impacts OCF base layers of ISO/IEC 30118-1. ISO/IEC 30118-1 contains informative security content. The OCF Security Specification contains security normative content and may contain informative content related to the OCF base or other OCF documents.

10) **IS/ISO/IEC 30118-3: 2021 Information technology Open Connectivity**

IS/ISO/IEC 30118-3:2021 defines the protocols and mechanisms necessary for bridging different IoT systems, enabling interoperability across diverse technologies and standards. This specification is essential for integrating various IoT networks and ensuring effective communication between disparate systems.

The standard facilitates the connection of heterogeneous IoT networks, promoting broader connectivity and functionality. By outlining bridging protocols, IS/ISO/IEC 30118-3:2021 supports the integration of devices and systems, enhancing the overall interoperability of IoT solutions.

The scope of IS/ISO/IEC 30118-3:2021 includes specifying bridging protocols that connect different IoT systems. It provides guidelines for achieving interoperability between various networks and technologies, ensuring seamless communication across disparate IoT environments.

This standard aims to support the integration of diverse IoT systems, facilitating consistent and effective interaction between different technologies. It outlines the requirements for bridging protocols to enable connectivity and interoperability across various IoT networks.

SCOPE

This document specifies a framework for translation between OCF Devices and other ecosystems, and specifies the behaviour of a Bridging Function that exposes servers in non-OCF ecosystem to OCF Clients and/or exposes OCF Servers to clients in non-OCF ecosystem. Translation per specific Device is left to other documents (deep translation). This document provides generic requirements that apply unless overridden by a more specific document.

11) **IS/ISO/IEC 30118-4: 2021 Information technology Open Connectivity Foundation OCF Specification Part 4: Resource type specification**

IS/ISO/IEC 30118-4:2021 focuses on defining the types of resources managed and interacted with by IoT devices within the OCF framework. This specification provides a standardized approach to resource management, ensuring that resources are handled consistently across different devices and platforms.

The standard is important for effective resource allocation and operation, facilitating smooth interaction among IoT devices. By establishing a common framework for resource types, IS/ISO/IEC 30118-4:2021 supports uniform management of resources within the OCF ecosystem.

The scope of IS/ISO/IEC 30118-4:2021 includes specifying the types of resources that IoT devices manage and interact with. It defines the framework for resource management within the OCF ecosystem, ensuring consistency across devices.

This standard provides guidelines for efficient resource handling, supporting smooth operation and interaction among IoT devices. It aims to ensure that resource management practices are standardized, facilitating effective integration and functionality within the OCF framework.

SCOPE

This document specifies the Resources that have been defined by OCF that may be exposed by an OCF Device. Application profile device documents (for example those created for Smart Home or Healthcare) specify device types appropriate to the profile; such documents use Resource Type definitions from this document. This document is built on top of ISO/IEC 30118-1. ISO/IEC 30118-1 specifies the OCF Framework that enables the implementation of profiles for IoT usages and ecosystems. The OCF Core Framework is scalable to support simple devices (constrained device) and more capable devices (smart device).

12) IS/ISO/IEC 30118-5: 2021 Information technology Open Connectivity Foundation OCF Specification Part 5: OCF device specification

IS/ISO/IEC 30118-5:2021 outlines the requirements for devices that are compliant with the OCF framework. This specification details the capabilities, interfaces, and functionalities that devices must meet to ensure uniformity in features and interoperability within the OCF ecosystem.

The standard is crucial for ensuring that IoT devices adhere to consistent performance and compatibility criteria. By defining the necessary specifications, IS/ISO/IEC 30118-5:2021 supports the development of devices that can seamlessly integrate into the OCF network.

The scope of IS/ISO/IEC 30118-5:2021 includes specifying the requirements for OCF-compliant devices. It details the necessary capabilities, interfaces, and functionalities for devices to operate effectively within the OCF framework.

This standard provides guidelines for ensuring device interoperability and performance, supporting consistent operation across the OCF ecosystem. It aims to facilitate the development of devices that meet uniform criteria, enhancing integration and functionality within the network.

SCOPE

The Device definitions use Resource definitions from ISO/IEC 30118-4.

This document is built on top of ISO/IEC 30118-1. ISO/IEC 30118-1 specifies the core architecture, interfaces protocols and services to enable the implementation of profiles for IoT usages and ecosystems. ISO/IEC 30118-1 also defines the main architectural components of network connectivity, discovery, data transmission, device & service management and ID & security. The core architecture is scalable to support simple devices (constrained devices) and more capable devices (smart devices).

IS/ISO/IEC 30118-6:2021 to IS/ISO/IEC 30118-18: 2021

The specifications from IS/ISO/IEC 30118-6 to IS/ISO/IEC 30118-18:2021 address the integration and mapping of OCF resources to various communication protocols and technologies. These documents provide detailed guidelines for ensuring compatibility between OCF resources and standards such as AllJoyn, BLE, EnOcean, Zigbee, Z-Wave, and cloud services.

These standards are essential for facilitating seamless connectivity and interaction between diverse IoT systems. By defining how OCF resources interface with different technologies, they support the broader integration of IoT devices into varied ecosystems.

The scope of these specifications includes defining the mappings and integrations for OCF resources with multiple communication protocols and technologies. They provide guidelines for ensuring interoperability between OCF resources and other standards, facilitating smooth integration across different IoT environments.

These standards support the compatibility of IoT devices with various communication and networking technologies. They aim to ensure that OCF resources can effectively interact with a range of systems and technologies, promoting broader connectivity and functionality.

13) **IS/ISO/IEC 30118-6: 2021 Information technology Open Connectivity Foundation OCF Specification Part 6: Resource to All Joyn interface mapping specification**

SCOPE

This document provides detailed mapping information to provide equivalency between All Joyn defined Interfaces and OCF defined Resources.

This document provides mapping for Device Types (All Joyn to/from OCF), identifies equivalent OCF resources for both mandatory and optional All Joyn interfaces and for each interface defines the detailed Property by Property mapping using OCF defined extensions to JSON schema to programmatically define the mappings

14) **IS/ISO/IEC 30118-7: 2021 Information technology Open Connectivity Foundation OCF Specification Part 7: Wi-Fi easy setup specification**

SCOPE

This document defines functional extensions to the capabilities defined in ISO/IEC 30118-1 to meet the requirements of Wi-Fi Easy Setup. It specifies new Resource Types to enable the functionality and any extensions to the existing capabilities defined in ISO/IEC 30118-1

15) **IS/ISO/IEC 30118-8: 2021 Information technology Open Connectivity Foundation OCF Specification Part 8: OCF resource to oneM2M resource mapping specification**

SCOPE

This document provides detailed mapping information to provide equivalency between oneM2M defined Module Classes and OCF defined Resources.

A oneM2M Bridge is Asymmetric Client Bridge, therefore this document provides unidirectional mapping for Device Types (oneM2M Devices to OCF Devices), identifies equivalent OCF Resources for specific oneM2M Module Classes, and defines the detailed Property by Property mapping using OCF defined extensions to JSON schema to programmatically define the mappings.

16) **IS/ISO/IEC 30118-9: 2021 Information technology Open Connectivity Foundation OCF Specification Part 9: Core optional specification**

SCOPE

The OCF Core specifications are divided into a series of documents:

– Core specification: The Core specification document specifies the Framework, i.e., the OCF core architecture, interfaces, protocols and services to enable OCF profiles implementation for Internet of Things (IoT) usages and ecosystems. This document is mandatory for all Devices to implement.

– Core optional specification (this document): The Core optional specification document specifies the Framework, i.e., the OCF core architecture, interfaces, protocols and services to enable OCF profiles implementation for Internet of Things (IoT) usages and ecosystems that can optionally be implemented by any Device.

– Core extension specification(s): The Core extension specification(s) document(s) specifies optional OCF Core functionality that are significant in scope (e.g., Wi-Fi easy setup, Cloud).

17) **IS/ISO/IEC 30118-10: 2021 Information technology Open Connectivity Foundation OCF Specification Part 10: Cloud API for cloud services specification**

SCOPE

This document defines functional requirements for the OCF Cloud to Cloud Application Programming Interface (API).

18) **IS/ISO/IEC 30118-11: 2021 Information technology Open Connectivity Foundation OCF Specification Part 11: Device to cloud services specification**

SCOPE

This document defines functional extensions to the capabilities defined in ISO/IEC 30118-1 to meet the requirements of the OCF Cloud. This document specifies new Resource Types to enable the functionality and any extensions to the existing capabilities defined in ISO/IEC 30118-1.

19) IS/ISO/IEC 30118-12: 2021 Information technology Open Connectivity Foundation OCF Specification Part 12: Cloud security specification

SCOPE

The OCF Cloud specifications are divided into a series of documents:

– OCF Cloud security specification (this document): The cloud security specification document specifies the security requirements and definitions for OCF devices and OCF clouds implementations.

– OCF Device to Cloud Specification: The OCF Device to Cloud Specification document defines functional extensions and capabilities to meet the requirements of the OCF Cloud. This document specifies new Resource Types to enable the functionality and any extensions required to connect an OCF device to an OCF cloud.

– OCF Cloud API for cloud services specification: The Cloud API for cloud services specification defines the OCF cloud API.

20) IS/ISO/IEC 30118-13: 2021 Information technology Open Connectivity Foundation OCF Specification Part 13: Onboarding tool specification

SCOPE

This document defines mechanisms supported by an OCF Onboarding Tool (OBT). This document contains security normative content for the OBT and may contain informative content related to the OCF base or OCF Security Specification other OCF documents.

21) IS/ISO/IEC 30118-14: 2021 Information technology Open Connectivity Foundation OCF Specification Part 14: OCF resource to BLE mapping specification

SCOPE

This document provides detailed mapping information between BLE (Bluetooth Low Energy) and OCF defined Resources

22) IS/ISO/IEC 30118-15: 2021 Information technology Open Connectivity Foundation OCF Specification Part 15: OCF resource to EnOcean mapping specification

SCOPE

This document provides detailed mapping information between EnOcean defined EEPs and OCF defined Devices and Resources

23) IS/ISO/IEC 30118-16: 2021 Information technology Open Connectivity Foundation OCF Specification Part 16: OCF resource to UPlus mapping specification

SCOPE

This document provides detailed mapping information between UPlus (U+) and OCF defined Resource

24) **IS/ISO/IEC 30118-17: 2021 Information technology Open Connectivity Foundation OCF Specification Part 17: OCF resource to Zigbee cluster mapping specification**

SCOPE

This document provides detailed mapping information between Zigbee defined Clusters and OCF defined Resources.

25) IS/ISO/IEC 30118-18: 2021 Information technology Open Connectivity Foundation OCF Specification Part 18: OCF resource to Z-wave mapping specification

SCOPE

This document provides detailed mapping information between Z-Wave and OCF defined Resources

26) **IS 802.15.9: 2021 - Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams**

INTRODUCTION

IS 802.15.9:2021 provides recommendations for the transport of Key Management Protocol (KMP) datagrams within wireless networks. This standard is essential for securing communication in IoT systems by defining practices for the effective transport of cryptographic keys and security-related data.

The standard supports the implementation of secure communication protocols, ensuring that key management practices are robust and reliable. It helps organizations protect IoT systems from security threats by providing guidelines for secure key transport.

SCOPE

The scope of IS 802.15.9:2021 includes the specification of practices for transporting KMP datagrams within wireless networks. It provides guidelines for ensuring secure key management and communication in IoT systems.

This standard aims to support the implementation of secure communication protocols by defining practices for the effective transport of cryptographic keys, enhancing the overall security of IoT systems.

27) **IS/ISO/IEC/IEEE 8802-1X: 2013 - Port-based Network Access Control**

INTRODUCTION

IS/ISO/IEC/IEEE 8802-1X:2013 specifies port-based network access control mechanisms. This standard is crucial for securing network access in IoT environments by defining methods for authenticating and authorizing devices that connect to a network.

The standard supports the implementation of robust network security measures, ensuring that only authorized devices can access network resources. It helps organizations manage network access effectively and protect IoT systems from unauthorized access.

SCOPE

The scope of IS/ISO/IEC/IEEE 8802-1X:2013 includes the specification of port-based network access control mechanisms. It provides guidelines for authenticating and authorizing devices connecting to a network, ensuring secure access in IoT environments.

This standard aims to support the implementation of effective network security measures by defining methods for controlling access to network resources, enhancing the protection of IoT systems.

28) IS/ISO/IEC/IEEE 8802-11: 2018 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

INTRODUCTION

IS/ISO/IEC/IEEE 8802-11:2018 defines the Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Local Area Networks (WLANs). This standard is essential for enabling wireless communication in IoT systems, providing the technical requirements for MAC and PHY layers.

The standard supports the development of interoperable wireless networks, ensuring that IoT devices can communicate effectively over WLANs. It helps organizations implement reliable and efficient wireless communication solutions for IoT applications.

SCOPE

The scope of IS/ISO/IEC/IEEE 8802-11:2018 includes the specification of MAC and PHY layer requirements for WLANs. It provides guidelines for implementing wireless communication protocols, supporting interoperability and performance in IoT systems.

This standard aims to ensure effective wireless communication by defining technical requirements for MAC and PHY layers, facilitating reliable and efficient connectivity in IoT environments.

29) IS 802.15.4: 2021 - Low-Rate Wireless Networks

INTRODUCTION

IS 802.15.4:2021 provides specifications for low-rate wireless networks, which are fundamental for many IoT applications. This standard defines the physical and MAC layer requirements for low-power, low-data-rate communication in wireless networks.

The standard is crucial for supporting a wide range of IoT devices that require efficient and reliable communication over short distances. It helps ensure that low-rate wireless networks can operate effectively in various IoT scenarios, from smart home devices to industrial sensors.

SCOPE

The scope of IS 802.15.4:2021 includes the specification of physical and MAC layer requirements for low-rate wireless networks. It covers the technical standards for low-power, low-data-rate communication, supporting various IoT applications.

This standard aims to provide guidelines for implementing effective low-rate wireless networks, ensuring reliable communication and efficient operation for IoT devices and applications.

C) CLOUD COMPUTING AND ARTIFICIAL INTELLIGENCE

30) IS/ISO/IEC 17788: 2014Information technology Cloud computing Overview and vocabulary

SCOPE

This Standard provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards.

This Standard is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

31) IS/ISO/IEC 22123-1: 2021 Information technology Cloud computing Part 1: Vocabulary

SCOPE

This document provides terms and definitions for vocabulary used in the field of cloud computing.

32) IS/ISO/IEC 19944-1: 2020 Cloud computing and distributed platforms Data flow data categories and data use Part 1: Fundamentals

SCOPE

This document

— extends the existing cloud computing vocabulary and reference architecture in ISO/IEC 17788 and ISO/IEC 17789 to describe an ecosystem involving devices using cloud services,

— describes the various types of data flowing within the devices and cloud computing ecosystem,

— describes the impact of connected devices on the data that flow within the cloud computing ecosystem,

— describes flows of data between cloud services, cloud service customers and cloud service users,

— provides foundational concepts, including a data taxonomy, and

— identifies the categories of data that flow across the cloud service customer devices and cloud services.

This document is applicable primarily to cloud service providers, cloud service customers and cloud service users, but also to any person or organisation involved in legal, policy, technical or other implications of data flows between devices and cloud services.

33) IS/ISO/IEC TR 22678 : 2020 Information Technology — Cloud Computing — Guidance for Policy Development — Cloud Computing

SCOPE

This document provides guidance on the use of international standards as a tool in the development of those policies that govern or regulate cloud service providers (CSPs) and cloud services, and those policies and practices that govern the use of cloud services in organisations. This includes material that explains cloud computing concepts and the role of cloud computing international standards in formulating policies and practices. The document makes references to various international standards. Where possible, these standards are ISO/IEC standards. Where a suitable ISO/ IEC standard is not available, references are made to documents published by other WTO-registered standards bodies. As explained in the WTO Agreement on Technical Barriers to Trade (TBT), standards play a vital role in supporting technical regulations and conformity assessment; however this document does not cover matters of trade.

34) IS/ISO/IEC TR 22678 : 2020 Information Technology — Cloud Computing — Guidance for Policy Development — Cloud Computing

SCOPE

This document provides guidance on the use of international standards as a tool in the development of those policies that govern or regulate cloud service providers (CSPs) and cloud services, and those policies and practices that govern the use of cloud services in organisations. This includes material that explains cloud computing concepts and the role of cloud computing international standards in formulating policies and practices. The document makes references to various international standards. Where possible, these standards are ISO/IEC standards. Where a suitable ISO/ IEC standard is not available, references are made to documents published by other WTO-registered standards bodies. As explained in the WTO Agreement on Technical Barriers to Trade (TBT), standards play a vital role in supporting technical regulations and conformity assessment, however this document does not cover matters of trade.

35) IS/ISO/IEC 27018 : 2019 Information Technology — Security Techniques — Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors

INTRODUCTION

Cloud service providers who process Personally Identifiable Information (PII) under contract to their customers need to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of PII. The requirements and the way in which the requirements are divided between the cloud service provider and its customers vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer. Legislation which governs how PII is allowed to be processed (i.e. collected, used, transferred and disposed of) is sometimes referred to as data protection legislation; PII is sometimes referred to as personal data or personal information. The obligations falling on a PII processor vary from jurisdiction to jurisdiction, which makes it challenging for businesses providing cloud computing services to operate multinationally.

A public cloud service provider is a “PII processor” when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from a natural person, a “PII principal”, processing his or her own PII in the cloud, to an organization, a “PII controller”, processing PII relating to many PII principals. The cloud service customer can authorize one or more cloud service users associated with it to use the services made available to it under its contract with the public cloud PII processor. Note that the cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller can be subject to a wider set of obligations governing the protection of PII than the public cloud PII processor. Maintaining the distinction between PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer’s objectives.

NOTE Where the public cloud PII processor is processing cloud service customer account data, it can be acting as a PII controller for this purpose. This document does not cover such activity

The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. It has the following objectives:

— to help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract;

— to enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services;

— to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement;

— to provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place.

This document can assist by providing a common compliance framework for public cloud service providers, in particular those that operate in a multinational market.

SCOPE

This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services. This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations. The guidelines in this document can also be relevant to organizations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.

36) IS/ISO/IEC 27036-4 : 2016 Information Technology — Security Techniques — Information Security for Supplier Relationships

INTRODUCTION

This document provides guidance on information security to cloud service customers and cloud service providers. Its application should result in

— increased understanding and definition of information security in cloud services,

— increased understanding by the customers of the risks associated with cloud services to enhance the specification of information security requirements, and

— increased ability of cloud service providers to provide assurance to customers that they have identified risks in their service(s) and associated supply chains and have taken measures to manage those risks.

This document is intended to be used by all types of organizations that acquire or supply cloud services. The document is intended primarily for risk owners in cloud service customers, who finally accept the use of the cloud service, and the individual accountable for the cloud service provided by the cloud service provider. The guidance is primarily focused on the initial link of the first cloud service customer and cloud service provider, but the principal steps should be applied throughout the supply chain, starting when the first cloud service provider changes its role to being a cloud service customer and so on. The manner in which this change of roles is repeated and the manner in which the same steps are repeated for each new cloud service customer-cloud service provider link in the chain are central to this document. By following the guidance contained within this document, it should be possible to have a seamless linkage of information security priorities visible across the supply chain. Information security concerns related to supplier relationships cover a broad range of scenarios. Organizations that wish to improve trust within their cloud service provision should define their trust boundaries, evaluate the risk associated with their supply chain activities, and then define and implement appropriate risk identification and mitigation techniques to reduce the risk of vulnerabilities being introduced through their cloud service provision supply chain. ISO/IEC 27001 and ISO/IEC 27002 framework and controls provide a useful starting point for identifying appropriate requirements for customers and providers. ISO/IEC 27017 and ISO/IEC 27018 provide guidance on how a cloud service customer and cloud service provider can implement, manage and operate information security for a cloud service. ISO/IEC 27036 (all parts) provides further detail regarding specific requirements to be used in establishing and monitoring information security in supplier relationships. This document is based upon the premise that a cloud service customer has applied general information security according to an information security management system (ISMS) (ISO/IEC 27001). As a result, much of the content is focused on the cloud service provider and depends on the capabilities type, service category and deployment model of the actual cloud service. Typically, cloud services are purchased "as is"; a cloud service customer has no ability to specify or request changes to the cloud service being purchased. However, in certain cases, the customer has the ability to specify the service and the detail of that service, including the information security arrangements required of the supplier. ISO/IEC 27036 is written to cover both of these eventualities. This document is written to cover the first of these eventualities and refers to ISO/IEC 27036-1, ISO/IEC 27036-2 and ISO/IEC 27036-3 for the cases when security arrangements can be specified. For a cloud service customer, this means that when reading this document, it should be noted that it is only addressing what are cloud service-specific security processes and controls. It is assumed all other general information security processes and controls necessary for the cloud service customer organization are in place to handle information security in the cloud service to be or being used. The general information security processes and controls are found in other ISO/IEC standards and in particular ISO/IEC 27036-1, ISO/IEC 27036-2, ISO/IEC 27036-3, ISO/IEC 27017 and ISO/IEC 27018.

SCOPE

This document provides cloud service customers and cloud service providers with guidance on

a) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively, and

b) responding to risks specific to the acquisition or provision of cloud services that can have an information security impact on organizations using these services.

This document does not include business continuity management/ resiliency issues involved with the cloud service. ISO/IEC 27031 addresses business continuity. This document does not provide guidance on how a cloud service provider should implement, manage and operate information security. Guidance on those can be found in ISO/IEC 27002 and ISO/IEC 27017. The scope of this document is to define guidelines supporting the implementation of information security management for the use of cloud services.

37) IS/ISO/IEC/TR 24028: 2020 Information technology Artificial intelligence Overview of trustworthiness in artificial intelligence

INTRODUCTION

The goal of this document is to analyse the factors that can impact the trustworthiness of systems providing or using AI, called hereafter artificial intelligence (AI) systems. The document briefly surveys the existing approaches that can support or improve trustworthiness in technical systems and discusses their potential application to AI systems. The document discusses possible approaches to mitigating AI system vulnerabilities that relate to trustworthiness. The document also discusses approaches to improving the trustworthiness of AI systems.

SCOPE

This document surveys topics related to trustworthiness in AI systems, including the following: - approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; - engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and - approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems. The specification of levels of trustworthiness for AI systems is out of the scope of this document.

38) IS/ISO/IEC/TR 24030: 2021 Information technology Artificial intelligence AI Use cases

INTRODUCTION

This document provides a collection of use cases of artificial intelligence (AI) applications in a variety of domains. In total, 132 AI use cases were submitted by experts between July 2018 and the end of November 2019. In this document, the term "use cases" means "collection of submitted use cases". The rationale for this document is as follows: - illustrating the applicability of the AI standardization work across a variety of application domains; - input to and reference for AI standardization work; - sharing the collected use cases in support of AI standardization work with external organizations and internal entities to foster collaboration; - reach out to new stakeholders interested in AI applicability; - establishment of liaison organizations to collect requirements for AI via use cases; - by investigating use cases, it is possible to find the new technical requirements (standardized demand) from the market, accelerating the transformation of science and technology achievements. While a bottom-up approach was used to collect use cases, a top-down approach is used in this document to identify AI applications, and their deployment models, and their application domains, which is shown in Clause 5.

The first step taken to collect use cases was to identify application domains of AI systems (described in Clause 5) and to provide a use case template (described in 6.4 and Annex B). Contributors were requested to submit use cases using the provided template. For improving the quality of use cases, a guidance was provided for contributors. The guidance included identified acceptable sources (described in 6.3) and AI characteristics (described in 6.4) for preparing use cases. In this document, subclause 6.5 includes basic statistics of use cases. Subclause 6.6 and Annex C describe the findings from use case analysis. The use cases were grouped and categorized according to the identified application domains. In this document, use cases are summarized and grouped according to the application domains in Clause 7.

Readers of this document can find use cases of specific application domains and their original submissions at https://standards.iso.org/iso-iec/tr/24030/ed-1/en.

AI is an emerging field with use cases and solutions with a wide range of maturity and success. The descriptions are given for the convenience of users of this document and does not constitute an endorsement by ISO.

SCOPE

This document provides a collection of representative use cases of AI applications in a variety of domains.

39) IS/ISO/IEC/TR 24029-1: 2021 Artificial Intelligence AI Assessment of the robustness of neural networks Part 1: Overview

INTRODUCTION

When designing an AI system, several properties are often considered desirable, such as robustness, resiliency, reliability, accuracy, safety, security, privacy. A definition of robustness is provided in 3.6. Robustness is a crucial property that poses new challenges in the context of AI systems. For example, in AI systems there are some risks specifically tied to the robustness of AI systems. Understanding these risks is essential for the adoption of AI in many contexts. This document aims at providing an overview of the approaches available to assess these risks, with a particular focus on neural networks, which are heavily used in industry, government and academia. In many organizations, software validation is an essential part of putting software into production. The objective is to ensure various properties including safety and performance of the software used in all parts of the system. In some domains, the software validation and verification process is also an important part of system certification. For example, in the automotive or aeronautic fields, existing standards, such as ISO 26262 or Reference [2], require some specific actions to justify the design, the implementation and the testing of any piece of embedded software. The techniques used in AI systems are also subject to validation. However, common techniques used in AI systems pose new challenges that require specific approaches in order to ensure adequate testing and validation. AI technologies are designed to fulfil various tasks, including interpolation/regression, classification and other tasks. While many methods exist for validating non-AI systems, they are not always directly applicable to AI systems, and neural networks in particular. Neural network systems represent a specific challenge as they are both hard to explain and sometimes have unexpected behaviour due to their non-linear nature. As a result, alternative approaches are needed. Methods are categorized into three groups: statistical methods, formal methods and empirical methods. This document provides background on these methods to assess the robustness of neural networks. It is noted that characterizing the robustness of neural networks is an open area of research, and there are limitations to both testing and validation approaches.

SCOPE

This document provides background about existing methods to assess the robustness of neural networks.

40) IS/ISO/IEC 24668: 2022 Information technology Artificial intelligence Process management framework for big data analytics

INTRODUCTION

This document provides a process management framework for using big data analytics (BDA) across most functions of an organization. The quantum of data, the collection, storage, utilization, technology, the speed of data generation, structure and variety of data cannot be handled by the conventional data handling methods and frameworks.

This document provides a BDA process reference model (BDA PRM) and then provides process assessment model (BDA PAM). The BDA PAM are composed of two dimensions: process dimension that includes processes based on a set of PRMs including the BDA PRM and capability dimension based on process measurement framework (PMF).

This document defines a PRM and PAM as part of the framework for big data analytics, in accordance with the requirements of ISO/IEC 33004:2015 and ISO/IEC 33020:2019, for use in performing a conformity assessment in accordance with the requirements of ISO/IEC 33002:2015. Primary audiences of this document are implementers of BDA in organizations as well as BDA capability assessors. This document provides five process categories such as organization stakeholder, competency development, data management, analytics development, and technology integration. This framework can be used for: - managing the processes that are considered to be best practices; - enabling risk determination and process improvements of the incumbent organization. Value delivered through automation, either prediction, or decision-making support or both using BDA is valuable to organizations. Implementing, improving, and assessing BDA processes based on this document expect benefits such as: - competitive advantages; - better decision-making; - improve customer experiences; - sales improvement; - responsiveness to opportunities and threats; - mistakes and errors reduction; - cost reduction. Clause 5 provides an overview of PRM and Clause 6 details out the specific processes under each process categories for the PRM. Clause 7 provides an overview of the PAM and Clause 8 provides details of process attributes and process performance indicators and Clause 9 provides process capability indicators.

SCOPE

This document provides a framework for developing processes to effectively leverage big data analytics across the organization irrespective of the industries or sectors. This document specifies process management for big data analytics with its various process categories taken into account along with their interconnectivities. These process categories are organization stakeholder processes, competency development processes, data management processes, analytics development processes and technology integration processes. This document describes processes to acquire, describe, store and process data at an organization level which provides big data analytics services.

41) IS/ISO/IEC/TR 24372: 2021 Information technology Artificial intelligence AI Overview of computational approaches for AI systems

INTRODUCTION

Artificial intelligence (AI)-related products, systems and solutions have become more common in recent years thanks to rapid software and hardware improvements that boost computational performance, data storage capabilities and network bandwidth. The intent of this document is to look at computational methods and approaches within AI systems.

Based on ISO/IEC 229891), ISO/IEC 230532) and ISO/IEC TR 24030, this document provides a description of the characteristics of an AI system and its computational approaches. The illustration of computational approaches in AI systems includes both machine learning and non-machine learning methods. To reflect state-of-the-art methods used in AI, this document is structured as follows: - Clause 5 provides an overall description of computational approaches in AI systems; - Clause 6 discusses the main characteristics of AI systems; - Clause 7 provides a general taxonomy of computational approaches, including knowledge-driven and data-driven approaches; - Clause 8 discusses selected algorithms used in AI systems, including basic theories and techniques, main characteristics and typical applications. By giving an overview of different technologies used by AI systems, this document is intended to help users understand computational characteristics and approaches used in AI.

SCOPE

This document provides an overview of the state of the art of computational approaches for AI systems, by describing:

a) main computational characteristics of AI systems;

b) main algorithms and approaches used in AI systems, referencing use cases contained in ISO/IEC TR 24030.

42) IS/ISO/IEC 38507: 2022 Information technology Governance of IT Governance implications of the use of artificial intelligence by organizations

INTRODUCTION

The objective of this document is to provide guidance for the governing body of an organization that is using, or is considering the use of, artificial intelligence (AI). This document provides guidance on the role of a governing body with regard to the use of AI within their organization and encourages organizations to use appropriate standards to underpin their governance of the use of AI. This document addresses the nature and mechanisms of AI to the extent necessary to understand the governance implications of their use: what are the additional opportunities, risks and responsibilities that the use of AI brings? The emphasis is on governance (which is done by humans) of the organization's use of AI and not on the technologies making up any AI system. However, such governance requires an understanding of the implications of the technologies. Artificial intelligence (AI) AI embraces a family of technologies that bring together computing power, scalability, networking, connected devices and interfaces, together with vast amounts of data. Reference to 'AI' in this document is intended to be understood to refer to a whole family of technologies and methods, and not to any specific technology, method or application. Use of AI "Use of AI" is defined in this document in the broadest sense as developing or applying an AI system through any part of its life cycle to fulfil objectives and create value for the organization. This includes relationships with any party providing or using such systems.

Governance implications of the use of AI

The scope of this document is concerned with the implications for an organization of the use of AI. As with any powerful tool, the use of AI bringsnew risks and responsibilities that should be addressed by organizations that use it. AI is not inherently 'good' or 'evil', 'fair' or 'biased', 'ethical' or 'unethical' although its use can be or can seem to be so. The organization's purpose, ethics and other guidelines are reflected, either formally or informally, in its policies. This document examines both governance and organizational policies and their application and provides guidance to adapt these for the use of AI. The operational aspects of the policies are implemented through management. This document refers to other standards for details on related topics including social responsibility, trustworthiness (such as risk management, management of bias, and quality) and compliance management.

SCOPE

This document provides guidance for members of the governing body of an organization to enable and govern the use of Artificial Intelligence (AI), in order to ensure its effective, efficient and acceptable use within the organization. This document also provides guidance to a wider community, including: - executive managers; - external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies; - public authorities and policymakers; - internal and external service providers (including consultants); - assessors and auditors. This document is applicable to the governance of current and future uses of AI as well as the implications of such use for the organization itself. This document is applicable to any organization, including public and private companies, government entities and not-for-profit organizations. This document is applicable to an organization of any size irrespective of their dependence on data or information technologies.

43) IS/ISO/IEC/TR 24368: 2022Information Technology Artificial Intelligence Overview of Ethical and Societal Concerns

INTRODUCTION

Artificial intelligence (AI) has the potential to revolutionise the world and carry a plethora of benefits for societies, organizations and individuals. However, AI can introduce substantial risks and uncertainties. Professionals, researchers, regulators and individuals need to be aware of the ethical and societal concerns associated with AI systems and applications. Potential ethical concerns in AI are wide ranging. Examples of ethical and societal concerns in AI include privacy and security breaches to discriminatory outcomes and impact on human autonomy. Sources of ethical and societal concerns include but are not limited to: - unauthorized means or measures of collection, processing or disclosing personal data; - the procurement and use of biased, inaccurate or otherwise non-representative training data; - opaque machine learning (ML) decision-making or insufficient documentation, commonly and societal concerns has not kept pace with the rapid evolution of AI. Consequently, AI designers, developers, deployers and users can benefit from flexible input on ethical frameworks, AI principles, tools and methods for risk mitigation, evaluation of ethical factors, best practices for testing, impact assessment and ethics reviews. This can be addressed through an inclusive, interdisciplinary, diverse and cross-sectoral approach, including all AI stakeholders, aided by International Standards that address issues arising from AI ethical and societal concerns, including work by Joint Technical Committee ISO/ IEC JTC 1, SC 42.

SCOPE

This document provides a high-level overview of AI ethical and societal concerns. In addition, this document: - provides information in relation to principles, processes and methods in this area; - is intended for technologists, regulators, interest groups, and society at large; - is not intended to advocate for any specific set of values (value systems). This document includes an overview of International Standards that address issues arising from AI ethical and societal concerns. referred to as lack of explainability; - lack of traceability; - insufficient understanding of the social impacts of technology post-deployment. AI can operate unfairly particularly when trained on biased or inappropriate data or where the model or algorithm is not fit-for-purpose. The values embedded in algorithms, as well as the choice of problems AI systems and applications are used for to address, can be intentionally or inadvertently shaped by developers' and stakeholders' own worldviews and cognitive bias.

44) IS/ISO/IEC/TS 4213: 2022Information technology Artificial intelligence Assessment of machine learning classification performance

INTRODUCTION

As academic, commercial and governmental researchers continue to improve machine learning models, consistent approaches and methods should be applied to machine learning classification performance assessment. Advances in machine learning are often reported in terms of improved performance relative to the state of the art or a reasonable baseline. The choice of an appropriate metric to assess machine learning model classification performance depends on the use case and domain constraints. Further, the chosen metric can differ from the metric used during training. Machine learning model classification performance can be represented through the following examples: - A new model achieves 97,8 % classification accuracy on a dataset where the state-of-the-art model achieves just 96,2 % accuracy. - A new model achieves classification accuracy equivalent to the state of the art but requires much less training data than state-of-the-art approaches. - A new model generates inferences 100x faster than state-of-the-art models while maintaining equivalent accuracy. To determine whether these assertions are meaningful, aspects of machine learning classification performance assessment including model implementation, dataset composition and results calculation are taken into consideration. This document describes approaches and methods to ensure the relevance, legitimacy and extensibility of machine learning classification performance assertions. Various AI stakeholder roles as defined in ISO/IEC 22989:2022, 5.17 can take advantage of the approaches and methods described in this document. For example, AI developers can use the approaches and methods when evaluating ML models. Methodological controls are put in place when assessing machine learning performance to ensure that results are fair and representative. Examples of these controls include establishing computational environments, selecting and preparing datasets, and limiting leakage that potentially leads to misleading classification results. Clause 5 addresses this topic. Merely reporting performance in terms of accuracy can be inappropriate depending on the characteristics of training data and input data. If a classifier is susceptible to majority class classification, grossly unbalanced training data can overstate accuracy by representing the prior probabilities of the majority class. Additional measurements that reflect more subtle aspects of machine learning classification performance, such as macro-averaged metrics, are at times more appropriate. Further, different types of machine learning classification, such as binary, multi-class and multi-label, are associated with specific performance metrics. In addition to these metrics, aspects of classification performance such as computational complexity, latency, throughput and efficiency can be relevant. Clause 6 addresses these topics. Complications can arise as a result of the distribution of training data. Statistical tests of significance are undertaken to establish the conditions under which machine learning classification performance differs meaningfully. Specific training, validation and test methodologies are used in machine learning model development to address the range of potential scenarios. Clause 7 addresses these topics. Apart from these, this document does not address any issues related to benchmarking, applications or use cases.

SCOPE

This document specifies methodologies for measuring classification performance of machine learning models, systems and algorithms.

45) IS/ISO/IEC 22989: 2022 Information technology Artificial intelligence Artificial intelligence concepts and terminology

INTRODUCTION

Advancements in computing capacity, reduction of costs of computation, availability of large amounts of data from many sources, inexpensive online learning curricula and algorithms capable of meeting or exceeding human level performance in particular tasks for speed and accuracy have enabled practical applications of AI, making it an increasingly important branch of information technology. AI is a highly interdisciplinary field broadly based on computer science, data science, natural sciences, humanities, mathematics, social sciences and others. Terms such as “intelligent”, “intelligence”, “understanding”, “knowledge”, “learning”, “decisions”, “skills”, etc. are used throughout this document. However, it is not the intention to anthropomorphize AI systems, but to describe the fact that some AI systems can rudimentarily simulate such characteristics. There are many areas of AI technology. These areas are intricately linked and developing rapidly so it is difficult to fit the relevance of all technical fields into a single map. Research of AI includes aspects such as aspects including "learning, recognition and prediction", "inference, knowledge and language" and "discovery, search and creation". Research also addresses interdependencies among these aspects. The concept of AI as an input and output process flow is shared by many AI researchers, and research on each step of this process is ongoing. Standardized concepts and terminology are needed by stakeholders of the technology to be better understood and adopted by a broader audience. Furthermore, concepts and categories of AI allow for a comparison and classification of different solutions with respect to properties like trustworthiness, robustness, resilience, reliability, accuracy, safety, security and privacy. This enables stakeholders to select appropriate solutions for their applications and to compare the quality of available solutions on the market. As this document does provide a definition for the term AI in the sense of a discipline only, the context for its usage can be described as follows: AI is a technical and scientific field devoted to the engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives. This document provides standardized concepts and terminology to help AI technology to be better understood and used by a broader set of stakeholders. It is intended for a wide audience including experts and non-practitioners. The reading of some specific clauses can however be easier with a stronger background in computer science. These concerns are described primarily Clauses 5.10, 5.11 and 8, which are more technical than the rest of the document.

SCOPE

This document establishes terminology for AI and describes concepts in the field of AI. This document can be used in the development of other standards and in support of communications among diverse, interested parties or stakeholders. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, not-for-profit organizations).

46) IS/ISO/IEC 23053: 2022Framework for Artificial Intelligence AI Systems Using Machine Learning

INTRODUCTION

Artificial intelligence (AI) systems, in general, are engineered systems that generate outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives. AI covers a wide range of technologies that reflect different approaches to dealing with these complex problems. ML is a branch of AI that employs computational techniques to enable systems to learn from data or experiences. In other words, ML systems are developed through the optimisation of algorithms to fit to training data, or improve their performance based through maximizing a reward. ML methods include deep learning, which is also addressed in this document. Terms such as knowledge, learning and decisions are used throughout the document. However, it is not the intent to anthropomorphize machine learning (ML). This document aims to provide a framework for the description of AI systems that use ML. By establishing a common terminology and a common set of concepts for such systems, this document provides a basis for the clear explanation of the systems and various considerations that apply to their engineering and to their use. This document is intended for a wide audience including experts and non- practitioners. However, some of the clauses (identified in the overview in Clause 5), include more in- depth technical descriptions. This document also provides the basis for other standards directed at specific aspects of ML systems and their components.

SCOPE

This document establishes an Artificial Intelligence (AI) and Machine Learning (ML) framework for describing a generic AI system using ML technology. The framework describes the system components and their functions in the AI ecosystem. This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, that are implementing or using AI systems.

47) IS/ISO/IEC 8183: 2023 Information technology Artificial intelligence Data life cycle framework

INTRODUCTION

Artificial intelligence (AI) systems are being adopted by organizations of all types, sizes and purposes. Data are essential to the development and operation of AI systems. In the field of AI systems, there are many data life cycles in use and under consideration for different purposes (e.g. data quality, bias in data, data governance, development and use of AI systems). Without an overarching framework, these different data life cycles can be challenging to correctly interpret by those without previous knowledge, context and expertise. There is a risk that these multiple data life cycles will not be applied as intended. This document provides a data life cycle overview in Clause 5, describes a data life cycle framework in Clause 6 and provides more information on the stages or processes of the data life cycle in Clause 7.

SCOPE

This document defines the stages and identifies associated actions for data processing throughout the artificial intelligence (AI) system life cycle, including acquisition, creation, development, deployment, maintenance and decommissioning. This document does not define specific services, platforms or tools. This document is applicable to all organizations, regardless of type, size or nature, that use data in the development and use of AI systems.

48) IS/ISO/IEC 24029-2: 2023Artificial intelligence AI Assessment of the robustness of neural networks Part 2: Methodology for the use of formal methods

INTRODUCTION

Neural networks are widely used to perform complex tasks in various contexts, such as image or natural language processing and predictive maintenance. AI system quality models comprise certain characteristics, including robustness. For example, ISO/IEC 25059:2023,[1] which extends the SQuaRE International Standards to AI systems, considers in its quality model that robustness is a sub- characteristic of reliability.

Demonstrating the ability of a system to maintain its level of performance under varying conditions can be done using statistical analysis, but proving it requires some form of formal analysis. In that regard formal methods can be complementary to other methods in order to increase trust in the robustness of the neural network. Formal methods are mathematical techniques for rigorous specification and verification of software and hardware systems with the goal to prove their correctness. Formal methods can be used to formally reason about neural networks and prove whether they satisfy relevant robustness properties. For example, consider a neural network classifier that takes as input an image and outputs a label from a fixed set of classes (such as car or airplane). Such a classifier can be formalized as a mathematical function that takes the pixel intensities of an image as input, computes the probabilities for each possible class from the fixed set, and returns a label corresponding to the highest probability. This formal model can then be used to mathematically reason about the neural network when the input image is modified. For example, suppose when given a concrete image for which the neural network outputs the label “car” the following question can be asked: “does the network output a different label if the value of an arbitrary pixel in the image is modified?” This question can be formulated as a formal mathematical statement that is either true or false for a given neural network and image.

A classical approach to using formal methods consists of three main steps that are described in this document. First, the system to be analyzed is formally defined in a model that precisely captures all possible behaviours of the system. Then, a requirement is mathematically defined. Finally, a formal method, such as solver, abstract interpretation or model checking, is used to assess whether the system meets the given requirement, yielding a proof, a counterexample or an inconclusive result. This document covers several available formal method techniques. At each stage of the life cycle, the document presents criteria that are applicable to assess the robustness of neural networks and to establish how neural networks are verified by formal methods. Formal methods can have issues in terms of scalability; however, they are still applicable to all types of neural networks performing various tasks on several data types. While formal methods have long been used on traditional software systems, the use of formal methods on neural networks is fairly recent and is still an active field of investigation.

This document is aimed at helping AI developers who use neural networks and who are tasked with assessing their robustness throughout the appropriate stages of the AI life cycle. ISO/IEC TR 24029-1 provides a more detailed overview of the techniques available to assess the robustness of neural networks, beyond the formal methods described in this document.

SCOPE

This document provides methodology for the use of formal methods to assess robustness properties of neural networks. The document focuses on how to select, apply and manage formal methods to prove robustness properties.

D) SECURITY AND PRIVACY STANDARDS FOR IoT

49) IS/ISO/IEC 27400:2022 - Cybersecurity — IoT Security and Privacy — Guidelines

INTRODUCTION

Information security is a critical concern for any information and communication technology (ICT) system, and Internet of Things (IoT) systems are no exception. IoT systems face unique information security challenges due to their highly distributed nature and the large number of diverse entities involved. This leads to a very large attack surface and poses a significant challenge for the information security management system (ISMS) in applying and maintaining appropriate security controls across the entire system.

Privacy and the protection of personally identifiable information (PII) are major concerns for certain types of IoT systems. When an IoT system collects or uses PII, there are often laws and regulations governing the acquisition, storage, and processing of this information. Even in cases where regulations are not a primary concern, the handling of PII remains a matter of reputation and trust for the organizations involved. If PII is stolen or misused, it could potentially cause harm to the individuals identified by the information.

The security and privacy controls outlined in this document are designed for stakeholders in an IoT system environment. These controls are intended to be utilized by each IoT stakeholder throughout the system's life cycle.

SCOPE

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

50) IS 14990 (Part 1) : 2024 / ISO/IEC 15408-1:2022 - Information Security Cybersecurity and Privacy Protection Evaluation Criteria for IT Security Part 1: Introduction and General Model Third Revision

The IS/ISO/IEC 15408-1:2022, part of the Common Criteria series, provides a foundational framework for evaluating the security of IT products and systems. This standard outlines the general model and introductory principles for evaluating information security, focusing on the security attributes and assurance measures necessary for IT systems. It establishes the basic requirements for security evaluation and serves as the cornerstone for the entire ISO/IEC 15408 series.

The scope of this standard includes the introduction of evaluation criteria for IT security and a general model for security evaluation. It details the basic concepts of security evaluation, including the definition of security targets and the evaluation of security functionalities. This standard ensures that IoT devices and systems adhere to fundamental security principles and provides a structured approach for assessing their security properties.

INTRODUCTION

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

The ISO/IEC 15408 series is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

The ISO/IEC 15408 series is intentionally flexible, enabling a range of evaluation approaches to be applied to a range of security properties of a range of IT products. Therefore, users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the ISO/IEC 15408 series in conjunction with unsuitable evaluation methods/ activities, irrelevant security properties, or inappropriate IT products, can result in meaningless evaluation results. Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties, and methods to determine that an evaluation provides meaningful results.

Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs. The ISO/IEC 15408 series addresses the protection of assets from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The ISO/IEC 15408 series may also be applicable to aspects of IT security outside of these three categories. The ISO/IEC 15408 series is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. The ISO/IEC 15408 series may be applied in other areas of IT but makes no claim of applicability in these areas.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the ISO/IEC 15408 series. Some of these are identified below:

a) the ISO/IEC 15408 series does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls;

b) the ISO/IEC 15408 series does not address the evaluation methodology under which the criteria should be applied;

NOTE 1 The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

c) the ISO/IEC 15408 series does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series is intended to be used for evaluation purposes in the context of such a framework;

d) the procedures for use of evaluation results in accreditation are outside the scope of the ISO/IEC 15408 series. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors must make separate provisions for those aspects;

e) the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the ISO/IEC 15408 series. In the case that independent assessment of mathematical properties of cryptography is required, the evaluation scheme under which the ISO/IEC 15408 series is applied shall make provision for such assessments.

NOTE 2 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component.

In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type. The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

SCOPE

This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of the ISO/IEC 15408 series. It describes the various parts of the ISO/IEC 15408 series; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria is addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

This document introduces:

— the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;

— a description of the organization of security components throughout the model;

— the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;

— general information about the evaluation methods given in ISO/IEC 18045;

— guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;

— general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;

— information in regard to the scope of evaluation schemes.

51) IS 14990 (Part 2):2024/ISO/IEC 15408-2:2022 - Information security cybersecurity and privacy protection - Evaluation criteria for IT security Part 2: Security functional components Third Revision

This standard focuses on security functional components, specifying the security functions that IT systems should provide. It builds upon the general model established in Part 1 by detailing the specific security functionalities necessary to protect information and systems. This standard is critical for defining the security requirements that IoT devices must meet to ensure they can handle sensitive data and interactions securely.

This standard outlines the security functional components that must be evaluated in IT systems, including access control, cryptographic support, and audit logging. It provides detailed criteria for assessing whether IoT devices and systems implement the necessary security functions to protect data and maintain system integrity. By specifying these requirements, ISO/IEC 15408-2 helps ensure that IoT systems are equipped with the essential security capabilities.

INTRODUCTION

Security functional components, as defined in this document, are the basis for the security functional requirements (SFRs) or components expressed in a Protection Profile (PP), PP-Module, functional package or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP, PP-Module, functional package or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus. Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies. The audience for this document includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1:2022, 5.2, provides additional information on the target audience of the ISO/IEC 15408 series, and on the use of the ISO/IEC 15408 series by the groups that comprise the target audience. These groups use this document as follows:

a) consumers, who use this document when selecting components to express functional requirements which satisfy the security objectives expressed in a PP, PP-Module, functional package or ST. ISO/IEC 15408-1:20—, Clause 7, provides more detailed information on the relationship between security objectives and security requirements;

b) developers, who respond to actual or perceived consumer security requirements in constructing a TOE, will find a standardized method to understand those requirements in this document. They also use the contents of this document as a basis for further defining the TOE security functionality and mechanisms that conform with those requirements;

c) evaluators, who use the SFRs defined in this document in verifying that the TOE functional requirements expressed in the PP, PP-Module, functional package or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators use this document to assist in determining whether a given TOE satisfies stated requirements.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

SCOPE

This document defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that meets the common security functionality requirements of many IT products.

52) **IS 14990 (Part 3): 2024 / ISO/IEC 15408-3:2022 - Information Security Cybersecurity and Privacy Protection Evaluation Criteria for IT Security Part 3: Security Assurance Components Third Revision**

IS/ISO/IEC 15408-3:2022 addresses security assurance components, defining the measures and processes needed to evaluate the effectiveness of security functions. This standard complements the functional components outlined in Part 2 by focusing on the assurance that security measures are properly implemented and effective. It is essential for verifying that IoT systems not only have the required security functions but also that these functions perform as intended.

The scope of this standard includes the criteria for evaluating the assurance levels of security measures, such as development and testing processes, configuration management, and vulnerability assessment. It provides a framework for assessing whether the implemented security functions in IoT devices are reliable and resilient against threats. This standard is crucial for ensuring that IoT systems meet high assurance levels in their security implementations.

INTRODUCTION

Security assurance components, as defined in this document, are the basis for the security assurance requirements expressed in a Security Assurance Package, Protection Profile (PP), a PP-Module, a PPConfiguration, or a Security Target (ST). These requirements establish a standard way of expressing the assurance requirements for TOEs. This document catalogues the set of assurance components, families and classes. It also defines evaluation criteria for PPs, PP-Configurations, PP-Modules, and STs. The audience for this document includes consumers, developers, technical working groups, evaluators of secure IT products and others. ISO/IEC 15408-1:2022, Clause 5 provides additional information on the target audience of the ISO/IEC 15408 series, and on the use of the ISO/IEC 15408 series by the groups that comprise the target audience. These groups may use this document as follows:

a) Consumers, who use this document when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this document when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this document as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type. The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation

SCOPE

This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

53) IS 14990 (Part 4): 2024 / ISO/IEC 15408-4:2022 - Information Security Cybersecurity and Privacy Protection Evaluation Criteria for IT Security Part 4: Framework for the Specification of Evaluation Methods and Activities

IS/ISO/IEC 15408-4:2022 introduces a framework for specifying evaluation methods and activities. This part of the Common Criteria series provides guidance on how to conduct evaluations based on the criteria set forth in the previous parts. It ensures that evaluation methods are consistent, repeatable, and comprehensive.

The scope includes the development of evaluation methodologies, including the specification of activities and processes required to perform security evaluations. It covers the procedures for evaluating IoT devices and systems, ensuring that evaluations are conducted systematically and effectively. This standard helps in establishing a consistent approach to evaluating the security of IoT systems.

INTRODUCTION

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations, by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. ISO/

IEC 18045 provides a companion methodology for some of the assurance requirements specified in the ISO/IEC 15408 series.

The model of security evaluation in ISO/IEC 15408-1 identifies that high-level generic evaluation activities are defined in ISO/IEC 18045, but that more specific evaluation activities (EAs) can be defined as technology-specific adaptations of these generic activities for particular evaluation contexts, e.g. for security functional requirements (SFRs)or security assurance requirements (SARs) applied to specific technologies or target of evaluation (TOE) types. Specification of such evaluation activities is already occurring amongst practitioners and this creates a need for a specification for defining such evaluation activities.

This document describes a framework that can be used for deriving evaluation activities from work units of ISO/IEC 18045 and grouping them into evaluation methods (EMs). Evaluation activities or evaluation methods can be included in protection profiles (PPs) and any documents supporting them. Where a PP, PP-Configuration, PP-Module, package, or Security Target (ST) identifies that specific evaluation methods/evaluation activities are to be used, then the evaluators are required by ISO/IEC 18045 to follow and report the relevant evaluation methods/evaluation activities when assigning evaluator verdicts.

As noted in ISO/IEC 15408-1, in some cases an evaluation authority can decide not to approve the use of particular evaluation methods/evaluation activities: in such a case, the evaluation authority can decide not to carry out evaluations following an ST that requires those evaluation methods/ evaluation activities.

This document also allows for evaluation activities to be defined for extended SARs, in which case derivation of the evaluation activities relates to equivalent action elements and work units defined for that extended SAR. Where reference is made in this document to the use of ISO/IEC 18045 or ISO/IEC 15408-3 for SARs (such as when defining rationales for evaluation activities), then, in the case of an extended SAR, the reference applies instead to the equivalent action elements and work units defined for that extended SAR. For clarity, this document specifies how to define evaluation methods and evaluation activities but does not itself specify instances of evaluation methods or evaluation activities.

The following NOTE appears in other parts of the ISO/IEC 15408 series and in ISO/IEC 18045 to describe the use of bold and italic type in those documents. This document does not use those conventions, but the NOTE has been retained for alignment with the rest of the series.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type. The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

SCOPE

This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities. This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities. These aspects are a matter for those originating the evaluation methods and evaluation activities in their particular area of interest.

54) IS 14990 (Part 5): 2024 / ISO/IEC 15408-5:2022 - Information Security Cybersecurity and Privacy Protection Evaluation Criteria for IT Security Part 5: Pre-defined Packages of Security Requirements

IS/ISO/IEC 15408-5:2022 outlines pre-defined packages of security requirements, providing standardized sets of security requirements that can be applied to various IT systems. This part facilitates the application of security evaluations by providing predefined security requirements for different types of systems, including IoT devices.

The scope of this standard includes the specification of predefined security requirements packages that can be used to assess IoT devices and systems. It provides a set of security requirements that are applicable to various IT environments, helping organizations to streamline the security evaluation process for IoT systems.

INTRODUCTION

This document provides pre-defined packages of security requirements. Such security requirements can be useful for stakeholders as they strive for conformity between evaluations. Packages of security requirements can also help reduce the effort in developing Protection Profiles (PPs) and Security Targets (STs). ISO/IEC 15408-1 defines the term “package” and describes the fundamental concepts.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type. The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation

SCOPE

This document provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders.

Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs). This document presents:

— evaluation assurance level (EAL) family of packages that specify pre-defined sets of security assurance components that may be referenced in PPs and STs and which specify appropriate security assurances to be provided during an evaluation of a target of evaluation (TOE);

— composition assurance (CAP) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of composed TOEs;

— composite product (COMP) package that specifies a set of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of a composite product TOEs;

— protection profile assurance (PPA) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during a protection profile evaluation;

— security target assurance (STA) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during a security target evaluation.

The users of this document can include consumers, developers, and evaluators of secure IT products.

55) **IS 15671: 2024 / ISO/IEC 18045:2022 - Information Security Cybersecurity and Privacy Protection Evaluation Criteria for IT Security Methodology for IT Security Evaluation Second Revision**

IS/ISO/IEC 18045:2022 details the methodology for evaluating IT security, complementing the Common Criteria series by providing structured guidelines for conducting security evaluations. This standard focuses on the evaluation processes and procedures, ensuring that security assessments are thorough and reliable.

The scope includes the methodologies and procedures for evaluating the security of IT systems. It provides a structured approach to security evaluation, including test procedures and evaluation criteria. This standard is particularly relevant for IoT systems, where comprehensive evaluation methodologies are necessary to ensure that security measures are effective.

INTRODUCTION

The target audience for this document is primarily evaluators applying the ISO/IEC 15408 series and certifiers confirming evaluator actions. Evaluation sponsors, developers, protection profile (PP), PP-Module, PP-Configuration, and security target (ST) authors, and other parties interested in IT security, can be a secondary audience. This document cannot answer all questions concerning IT security evaluation and further interpretations may be needed. Individual schemes determine how to handle such interpretations, although these can be subject to mutual recognition agreements. A list of methodology-related activities that can be handled by individual schemes can be found in Annex A. This document is intended to be used in conjunction with the ISO/IEC 15408 series.

NOTE 1 Reference throughout the document to ISO/IEC 15408 implies the ISO/IEC 15408 series.

NOTE 2 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

SCOPE

This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.

56) IS/ISO/IEC 20547-4: 2020 - Information Technology Big Data Reference Architecture Part 4: Security and Privacy

IS/ISO/IEC 20547-4:2020 addresses security and privacy in Big Data environments, providing a framework for managing and protecting data in large-scale data processing systems. It focuses on the security and privacy challenges associated with Big Data technologies, which are increasingly relevant to IoT systems that generate and process large volumes of data.

The scope includes the guidelines for managing security and privacy in Big Data environments. It provides recommendations for protecting data and ensuring privacy in systems that handle vast amounts of data. This standard is relevant for IoT systems that integrate with Big Data technologies, ensuring that data privacy and security are maintained.

INTRODUCTION

Big data refers to the massive amount of digital information collected in various forms from different sources of digital and physical environments. This data is not only generated by traditional means of information exchange, but also from sensors embedded in physical environments, such as city surroundings, transportation vehicles, critical infrastructures, etc. The collection and processing of big data provides additional challenges not inherent in the traditional digital information exchange setting. This document was developed in response to the worldwide demand for a common baseline of security and privacy aspects for big data architectures to facilitate interoperability in big data systems without compromising privacy, confidentiality, or integrity. The big data paradigm blurs the security boundaries between data collection, storage and access — areas traditionally addressed independently — that now needs to be confronted holistically with a comprehensive security and privacy foundation, tightly coupled to all architecture components. Effective standardization of security and privacy is paramount to the development of mutual trust and cooperation amongst big data stakeholders.

SCOPE

This document specifies the security and privacy aspects applicable to the big data reference architecture (BDRA) including the big data roles, activities and functional components and also provides guidance on security and privacy operations for big data.

57) IS/ISO/IEC 24745: 2022 - Information security cybersecurity and privacy protection - Biometric information protection

IS/ISO/IEC 24745:2022 focuses on the protection of biometric information, specifying measures to secure biometric data such as fingerprints and facial recognition data. This standard is crucial for ensuring that biometric data is protected from unauthorized access and misuse.

The scope includes guidelines for securing biometric information, addressing the protection of data used for authentication and identification purposes. This standard is particularly relevant for IoT systems that utilize biometric data, ensuring that such data is safeguarded against potential threats.

INTRODUCTION

As the Internet becomes a more pervasive part of daily life, various services are being provided via the Internet, e.g. Internet banking, remote healthcare. In order to provide these services in a secure manner, the need for authentication mechanisms between subjects and the service being provided becomes even more critical. Some of the authentication mechanisms already developed include tokenbased schemes, personal identification and transaction numbers (PIN/TAN), digital signature schemes based on public key cryptosystems, and authentication schemes using biometric techniques.

Biometrics, the automated recognition of individuals based on their behavioural and physiological characteristics, includes recognition technologies based on, e.g. fingerprint image, voice patterns, iris image and facial image. The cost of biometric techniques has been decreasing while their reliability has been increasing, and both are now acceptable and viable for use as an authentication mechanism.

Biometric authentication introduces a potential discrepancy between privacy and authentication assurance. On the one hand, biometric characteristics are ideally an unchanging property associated with and distinct to an individual. This binding of the credential to the individual provides strong assurance of authentication. On the other hand, this strong binding also underlies the privacy concerns surrounding the use of biometrics, such as unlawful processing of biometric data, and poses challenges to the security of biometric systems to prevent or to be resilient to the compromise of biometric references (BRs). The usual solution to the compromise of an authentication credential (to change the password or issue a new token) is not generally available for biometric authentication because biometric characteristics, being either intrinsic physiological properties or behavioural traits of individuals, are difficult or impossible to change. At most, another finger or eye instance can be enrolled, but the choices are usually limited. Therefore, appropriate countermeasures to safeguard the security of a biometric system and the privacy of biometric data subjects are essential.

Biometric systems usually bind a BR with other personally identifiable information (PII) for authenticating individuals. In this case, the binding is needed to assure the security of the data record containing biometric information. The increasing linkage of BRs with other PII and the sharing of biometric information across legal jurisdictions make it extremely difficult for organizations to assure the protection of biometric information and to achieve compliance with various privacy regulations.

SCOPE

This document covers the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. It also provides requirements and recommendations for the secure and privacy-compliant management and processing of biometric information. This document specifies the following:

— analysis of the threats to and countermeasures inherent to biometrics and biometric system application models;

— security requirements for securely binding between a biometric reference (BR) and an identity reference (IR);

— biometric system application models with different scenarios for the storage and comparison of BRs;

— guidance on the protection of an individual's privacy during the processing of biometric information.

This document does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

58) IS/ISO/IEC 27001: 2022 - Information security cyber security and privacy protection - Information security management systems Requirements

IS/ISO/IEC 27001:2022 specifies the requirements for establishing, implementing, maintaining, and improving an information security management system (ISMS). It provides a comprehensive approach to managing information security risks and ensuring the confidentiality, integrity, and availability of information.

The scope includes the requirements for implementing an ISMS, covering aspects such as risk assessment, security controls, and management processes. This standard is essential for IoT systems, providing a structured framework for managing security risks and ensuring that IoT environments are protected from various threats.

INTRODUCTION

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

SCOPE

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

E) STANDARDS FOR APPLICATION OF IoT

a. General

The Standard **IS/ISO/IEC TR 22417: 2017 Information Technology – Internet of Things – IoT Use Cases** identifies IoT scenarios and Use cases based on real world applications and requirements. An IoT use case is description of a hypothetically possible situation where IoT concepts, products and services may be specified as a set of actions associated with actors in an IoT system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system. A total of 25 Use Cases are given in the Standard. These Use Cases provide a practical context for considerations on Interoperability and Standards on the basis of experience of users. The following use cases have been included in this Standard:

- IoT Network Security
- IoT Security threat detection and management
- Remote management of large equipment in a plant
- Automated ICC profile discovery
- Tracking of Farm products
- IoT application for warehouse goods monitoring
- Cooperation between Factories and Remote Applications
- Searching Systems for persons with cognitive impairment
- Sleep monitoring system
- Smart Glasses
- IoT endpoint (sensors and actuators) monitoring systems
- Intelligent assistive parking in urban areas
- Integrated Smart Pump System
- Remote Health monitoring
- Connected car analytics
- Real time motor monitor
- Smart Home Appliances

- Smart Home Insurance
- Machine Learning
- IoT based Energy Management System for Industrial Facilities
- Water Plant Management
- Smart Home Application
- Field Gateway Bridging IoT to Legacy Devices in Factories and Plants
- Production Monitoring of Textile Equipment
- Remote Management of Agricultural Greenhouses.

The Clause 7 of the Standard IS/ISO/IEC TR 22417:2017 describes the use case scenario which gives information on Scope and Objectives of Use Cases; Narrative of Use case; Actors; Issues: Legal Contracts, Legal Regulations, and Constraints; Refrenced Standards and/or Standardization Committees; Relation with Other known Use Cases; General Remarks (Domain, Role and Scenario); Security and Privacy; Conformity Aspects and Critical Requirements; Interaction between Actors and User Requirements; Diagram of Use Cases; and Data Flow Diagram of use cases.

Serial No. 2 of the section A) BASIC/GENERAL STANDARDS ADDRESSING (IoT) gives information about the Standard IS/ISO/IEC TR 22417: 2017 including its clauses on introduction and scope.

b. SMART CITIES

59) IS 18000: 2020 Unified Digital Infrastructure — ICT Reference Architecture (UDI-ICTRA)

INTRODUCTION

A smart city is one that can effectively leverage technology, infrastructure, public policy, government and citizen engagement to create an urban environment that fosters economic growth and productivity, innovation, social mobility, inclusiveness, and sustainability. Cities are complex entities having:

a) Diverse Stakeholders: Citizens, visitors, city administration, state government, central government, vendors, system integrators, business, academia, other organizations.

b) Diverse Geographical Entities: Parking lots, streets, buildings, electric stations, etc.

c) Diverse Services and Business Processes: With diverse functionality and consumers need to be developed.

d) Diverse ICT Technologies: Data systems, sensor technologies, software systems, networking systems etc.

While it is almost impossible to engineer a smart city from scratch, it will be possible to adopt the right architectural framework along with appropriate practices and policies to nudge the evolution towards smart cities. The three key principles for facilitating such an emergence/evolution towards a smart city ecosystem are:

1) Interoperability — Refers to the ability of diverse systems and components to work together, even as parts from diverse set of suppliers are substituted and integrated;

2) Composability — Refers to the ability to combine discrete components into a complete system to achieve a set of goals and objectives; and

3) Harmonization — Refers to achieving compatibility between technologies and systems, even when they at first appear incompatible.

This standard provides a reference architecture for achieving such a unified digital infrastructure and can serve as a template for both the City Administrators, who are the consumers of such ICT based solutions, as well as the ICT solution providers who develop and deploy such solutions.

SCOPE

1.1 This standard defines the reference architecture and models for information and communication technologies needed to realize a Unified Digital Infrastructure (UDI) in Smart Cities. The reference architecture includes functional reference models, technology reference models and information reference models. The standard offers a blueprint for realizing the unified digital infrastructure, but does not mandate any specific components. The reference architecture can be used to define various levels of architectural maturity, based on which components are included, from a basic level to an advanced level of the unified digital infrastructure. However, this categorization is not part of this standard.

1.2 The implementation details are also excluded from the scope of this standard

60) IS 18002 (Part 1) : 2021 Unified Digital Infrastructure - Data Layer Part 1 Reference Architecture

INTRODUCTION

Smart cities vision is to use digital technologies to provide integrated services to its citizens through free flow of information, to usher in an era of transparent governance. Designing smart cities ICT architecture is the essential first step in this direction. Cities are complex ecosystems, where government services pertaining to transportation, public safety, utilities, healthcare, education, social services, culture, economic development and more are provided by a multitude of government organizations.

Each Application/Component part of the Smarts Cities ICT Architecture deals with data and hence needs to align with principles defined in this document.

Data is generated by a variety of smart city applications, operated and managed by a host of departments and organizations, working towards a common goal of building and running city infrastructure to better serve the citizens. However, this multiplicity of data owners often causes problems related to accuracy, consistency and accessibility of right data at the right time.

There is a need to bring together a large amount of data available in cities, including energy, traffic and transport, parking, environment, ERP, water, solid waste, crowd sourced data, etc., curate data (by eliminating duplicate, invalid, outdated and wrong data) and provide a holistic view of the information with the aim of improvement and development of innovative smart city services. Integrated data plays a vital role in understanding the problem in the right context and providing a solution which is in the interest of administration as well as citizens. Trend analytics over weekly, monthly, and annual views of the data reveal insights and surprises that daily views cannot. In business terms, the key performance indicators of the city's health, progress, and objective results are found in the long-term analysis of data.

Smart City data management will thus enable and stimulate a proper understanding of how a city's infrastructure is utilized in different domains, what key performance parameters they indicate, the interdependencies between different elements of city infrastructure and the effects of external drivers like public policy, major events, exigencies, and weather.

Smart city data exhibits characteristics of 5 Vs namely Volume, Velocity, Variety, Veracity and Value which comes with their own individual challenges.

Volume: Data volume represents the extensive amount of data available for analysis to extract valuable information. An example of high volume of data, is the volume of data generated through surveillance cameras and sensors deployed across the city.

Velocity: Most of the real-world control applications need actionable insights in a real time basis. Streaming and Real time analytics utilize high velocity of data to generate real time operational alerts and insights. One example of such data is the real-time position of a utility vehicle plying in the city sending updates on its position every 5 seconds.

Variety: Variety in data arises due to the variety of sensors and systems deployed in the cities. Also, variety in data arises due to the same type of device or systems generating data in heterogeneous formats or recording data in different units of measurements.

Veracity: Veracity refers to the biases, noise and abnormality in data. Noise, abnormality in data is a major issue n smart city deployments. Many complex systems utilize AI models for pre-processing and filtering of data, and AI is prone to biases induced due to noise and abnormality in data. Additionally, measurements by sensors also suffer from drift due to various physical factors. Controlling veracity requires constant observations of the data, trends in time series data and taking timely remediations.

Value: Data is only as valuable as the business outcomes it makes possible. Smart cities are looking at data monetization and innovation on open data for future infrastructure development. For this, smart cities need to make choices on storage (long term vs. short term), types of data to be ingested, governance policies and security controls to be implemented on data to ensure that data is usable on a longer term.

The future of governance is data driven. Cities have begun to adapt to this change in their functioning. This data-driven change adapted by cities, apart from providing timely inputs on the impact of citizen services is also used to measure the impact of the investments made over a period.

This helps realistically assess the gaps between the outcomes and the desired goals. Data is an asset for cities, hence has a specific, measurable value for the Government and needs to be managed accordingly.

To overcome data integration issues, a city needs to have a robust Unified Data Architecture Framework that puts in place a mechanism to not only share the data amongst different departments but also a set of tools and technology to better use this data for decision making.

This standard defines the conceptual model (functional and technological), data principles and reference architecture for data in a smart city. A common data reference architecture spanning all the smart cities will help in bringing data in 'focus' to ensure a move towards outcome-based planning in governance.

The Data Layer Reference Architecture is intended to be used by stakeholders such as Smart city Data Officers, Smart City CEO's, Policy and Governance officers, Auditors and other stakeholders involved in smart city implementation to define the city's data architecture goals and to roll out solutions adhering to the defined goals.

SCOPE

This Standard describes the data layer reference architecture that comprises the key data principles that every smart city sub-system needs to adhere to, the core capabilities required to be implemented at the city level for realizing the data layer, the functional reference model and the technology reference model. This standard applies to data generated in smart cities across following streams:

a) Demand-side stream which can give better understanding of specific properties and characteristics of urban processes, e.g. buildings services, government-to-citizens services, andprovide solutions for improvement.

b) Supply-side stream to monitor incidents and crisis situations and the respective responses andsolutions with the aim of drawing conclusions and recommendations.

c) Analytical stream to identify data patterns and correlations in order to derive predictions forurban innovation, provide impact assessment, and demonstrate the challenges and opportunities inurban development.

d) Standardization stream to bring the city data in line with the international standards likeISO/TS 8000 Data Quality. While the technical reference architecture lists a set of technology components and provides an overview of each of them, individual choice of technologycomponents can vary from city to city while keeping the core data capabilities that should be fulfilled by the city

61) IS 18003 (Part 1): 2021 Unified Data Exchange Part 1 Architecture

INTRODUCTION

Data empowerment is a key aspect of any smart city implementation to harness maximum value from the enormous data cities generate. The current smart city implementations are unable to satisfy this need efficiently due to the proprietary and ad-hoc nature of the interfaces and their implementations. Hence, it is difficult to develop next generation AI/ML based applications for providing new solutions and services at scale, using the existing frameworks. The Data Exchange as discussed in this document aims to address this gap, by creating an architecture (Part 1) and interface specifications (Part 2) for interconnecting various IT systems of different government departments as well as external organizations.

The data exchange will provide three key services:

a) A catalogue service which will host a catalogue of meta-information about the various data sets, with information about the custodian of the data, data model for the data, the API endpoints, API methods etc.

b) One or more authorization services that will enable a data custodian (one who is responsible for the data) to regulate access to their data sets.

c) One or more resource access services which will allow a standardized way to access resources.

Security and privacy will be incorporated by design in this architecture. This architecture should simplify the life of the data custodian as well as the application developer.

The data exchange architecture will enable new applications to emerge that can take advantage of data from different IT Systems, to provide novel services. For example, a Women's safety index can calculate the live safety index of any street, combining data from smart streetlights, video analytics from traffic cameras, data from police databases along with analysis of land use. Such an index can be used by trip planning apps to allow for determining safe routes or used by the city or police to plan on patrolling.

By defining the architecture and specifying the interfaces and data models, the data exchange architecture standards will enable a whole new ecosystem of application developers to provide new, data driven, solutions and services. Additionally, adopting the data exchange architecture nationally, will enable economies of scale for the developers and will allow the same applications to run across the country. For data custodians – the data exchange architecture will allow a simple way to expose, provide consent, audit and track their data usage.

SCOPE

1.1 This Indian Standard (Part 1) describes the architecture for the data exchange, interfaces of data exchange components and the use cases that are enabled in this ecosystem. It also describes the responsibilities of various stakeholders, their interactions with other stakeholders in the system, and the respective consequences of those interactions.

1.2 This Standard (Part 1) also describes the high level architecture of the following three main components of the data exchange services:

a) Catalogue service that provides APIs to manage meta-information about resources;

b) Authorization service, that manages authorization to access the resources; and

c) Resource access service, that provides a standardized way to access resources. 1.3 A more detailed specification and the API definitions for the data exchange architecture is described in Part 2

62) IS 18003 (Part 2) : 2021 Unified Data Exchange Part 2 API specifications

INTRODUCTION

The next wave of smart cities intends to use data- driven innovative solutions to overcome the challenges of urbanization. Harnessing the value of enormous data generated by cities today can solve some of the key challenges faced by the cities. The current smart city implementations are unable to satisfy this need efficiently, due to the proprietary and ad-hoc nature of the interfaces and their implementations. This leads to data exchange bottlenecks thereby making it difficult to develop next generation data driven solutions, such as solutions based on the Artificial Intelligence/Machine learning (AI/ML) technologies, for providing new solutions and services at scale. The Data Exchange (DX) layer, which is an integral part of the Data Layer, as specified in IS 18002 : 2021 aims to address this gap by providing a standardized framework for accessing data in a unified format, allowing for authorized sharing of data between different entities, such as various departments in a city or between various public and private data providers and third party application developers etc. The seamless exchange of data is envisioned to lead to the development of innovative, data based solutions as well as provide an opportunity for data providers and application developers to participate in an urban data marketplace.

This Standard defines Unified Data Exchange interface specifications. It defines a set of APIs that enables controlled and secure any-to-any exchange of all forms of public and privately owned non-personal data between data providers and consumers.

Standardized APIs help build robust application ecosystems that not only improve development cycle times but also lead to improvement in reusability and extensibility of the developed applications. With this objective, this Standard defines APIs for interactions with the Data Exchange layer. The interfaces are described in terms of HTTP protocol bindings.

SCOPE

This Indian Standard (Part 2) defines the API specifications for the Data exchange interfaces identified in the Data exchange reference architecture described in Part 1 of this standard. The API specifications are defined for usage over HTTP protocol only.

The target audience for this standard (Part 2) is the community of software developers who may be the implementers of the Data exchange layer services or may be the users of the Data exchange layer, e.g., Data exchange data publishers or Data exchange data consumers wishing to write applications using data available with the Data exchange

63) IS 18003 (Part 3/Sec 1): 2021 Unified Data Exchange Part 2 API specifications

INTRODUCTION

The smart cities are generating an enormous amount of data. If harnessed in the right way, this data can empower the stakeholders namely, the providers, the consumers and the governing agencies in solving the key challenges faced by the cities and add value by building innovative applications. One issue faced by the current smart cities is the inability to exchange data efficiently due to the proprietary and ad-hoc nature of the interfaces and their implementations.

To address the data exchange bottlenecks, a unified data exchange (DX) layer, which provides a standardised framework for accessing data in a unified format and allowing authorized data sharing amongst different entities, was defined in the Indian Standard IS 18003 (Part 1) Unified data exchange: Part 1 Architecture and the Indian Standard IS 18003 (Part 2) Unified data exchange: Part 2 API specifications.

The data exchange (DX) layer specifies three sets of services, namely the catalogue service, the authorization service and the resource access service. The detailed application programming interface (API) specifications for each of these services are provided in — IS 18003 (Part 2): API specifications. In particular, the resource access service forms the data plane for the DX layer. It defines interfaces to allow data consumers to access data for a given resource as per the consent of the data provider. Further, it defines interfaces to allow data providers to publish data for a given resource.

This standard IS 18003 (Part 3) Compliance specifications: Part 1 (Resource access service) specifies the abstract test suite to define compliance to the resource access service as defined in IS 18003 (Part 2) API specifications. The test suite defines the minimum functionality required for a given functional profile for any compliant resource access service implementation.

The compliance specifications are divided into 5 clauses. Clause 1 gives the scope of this compliance specification document. Clause 2 lists the normative and informative references. Clause 3 gives the definitions on various terminologies and abbreviations used in this document. Clause 4 details the resource access service functional profiles and the details of the tests are presented in 5.

SCOPE

This standard (Part 3/Sec 1) defines the compliance test suites for any implementation of the data exchange (DX) resource server data access service as specified in IS 18003 (Part 2) of the standards.

Compliance specifications for catalogue service and authorization service will be specified in the future versions of this standard.

The target audience for this standard are the developers of DX data access services and the developers of testing and compliance suites belonging to independent testing and certification agencies. This standard will also be helpful for DX consumers to understand the implementation details of the APIs and the functional profiles.

64) IS 18006 (Part 1): 2021 Municipal Governance Part 1 Reference Architecture

INTRODUCTION

A smart city is the one that can effectively leverage technology, infrastructure, public policy, government and citizen engagement to create an environment that fosters economic growth and productivity, innovation, social mobility, inclusiveness, and sustainability.

Cities are complex entities having:

a) Diverse Stakeholders: Citizens, visitors, city administration, state government, central government, vendors, system integrators, business, academia, other organizations.

b) Diverse Geographical Entities: Parking lots, streets, buildings, waste bins, etc.

c) Diverse Services and Business Processes: With diverse functionality and consumers need to be developed.

d) Diverse ICT Technologies: Data systems, sensor technologies, software systems, networking systems etc.

While it is almost impossible to engineer a smart city from scratch, it is possible to adopt the right architectural framework along with appropriate practices and policies to nudge the evolution towards smart city.

The three key principles for facilitating such an emergence or evolution towards a smart city ecosystem are:

a) Interoperability — Refers to the ability of diverse systems and components to work together, even as parts from diverse set of suppliers are substituted and integrated;

b) Composability — Refers to the ability to combine discrete components into a complete system to achieve a set of goals and objectives; and

c) Harmonization — Refers to achieving compatibility between technologies and systems, even when they at first appear incompatible.

This standard provides a reference architecture (RA) for achieving such a unified digital infrastructure for municipal governance and can serve as a template for both the City Administrators, who are the consumers of such ICT based solutions, as well as the ICT solution providers who develop and deploy such solutions.

The reference architecture heavily relies on some of the other standards developed as well as aligns itself to the parent standard, IS 18000 : 2020. The Municipal Governance RA is supported by IS 18004 (Part 1) and IS 18008 (Part 1) to achieve a lot of its functionality. For example, one of the core service infrastructure, “Location”, in the reference architecture is enabled by GIS reference architecture and this service supports functionalities such as GIS tracking of Project progress, GIS mapping of Asset and real estates and many others.

Further, this reference architecture also implements components from IS 18002 (Part 1) to ensure availability of quality data for effective decision making by city administrators.

This reference architecture described in these standard addresses stakeholders expectations for efficient municipal operations as well as to enable equitable service delivery to citizens. The cities or municipal corporations can also use this standard as a guide to compare their current initiatives and functionalities. Cities or Municipal corporation shall aim to, at the minimum, create a common Core Data Infrastructure and Core Service infrastructure layer. Cities can go with a phased approach to adopt the functionalities described in business layer , over a period of time.

(The above text has been taken from the INTRODUCTION given in the standard. However, the Figure 1 given in this clause in the document has not been reproduced here)

SCOPE

This Indian standard defines the reference architecture and models for Municipal Governance in Urban Local Bodies (ULBs). The reference architecture includes functional reference models, technology reference models and information reference models. The implementation details are excluded from the scope of this standard.

65) IS 18006 (Part 3/Sec 1): 2021 Municipal Governance - Part 3 Property Tax - Section 1 Taxonomy

INTRODUCTION

ULBs across India have different terminology and vocabulary for Municipal Governance. This is due to the federal structure of governance in India, state specific laws and different e-Governance system implementations. Non-standardized interfaces and storage also lead to data interpretation and interoperability issues. Hence, when municipal performance is measured, there are glaring inconsistencies, not merely city to city but also from state to state, with respect to what comprises it per se. Thus, without clear definitions, vocabulary, specifications and benchmarks for municipal governance, it is difficult to enable 'Data Driven Governance'.

The municipal governance standards are being designed to have minimum base elements common across ULBs to ensure interoperability, harmonization and data driven governance. These can then be adopted and built upon by ULBs with higher process complexities.

The Property tax taxonomy defined in this standard includes common property tax entities, processes, stakeholders and their definitions. All definitions in this standard are notional definitions for conceptual purposes. The actual definition of entities for tax purposes should be considered as per state and local legislations.

The taxonomy structure in this document is scalable both vertically and horizontally to accommodate ULB specific complexities as well as change in people, process and technology over time. Property Tax Taxonomy will be used in developing Property Tax Data Models and API Specifications as well as for creating metadata specifications. Few sample parameters and specification are also given in Annex 1 for understanding purpose.

Together these standards will ensure semantic and syntactic interoperability among all eGovernance systems in India.

The audience for this standard includes but is not limited to academics, architects, customers, users, tool developers, regulators, auditors and standards development organizations.

This document is also interrelated with other Indian standards such as IS 18000 and IS 18006 (Part 1).

SCOPE

This Indian standard provides a unified view of the Property Tax data and processes in a municipal corporation and introduces common and widely accepted terminologies and semantics that can be used across multiple systems.

66) IS 18008 (Part 1) : 2021 Smart Cities- GIS Reference Architecture

INTRODUCTION

0.1 Current Challenges of GIS in Smart Cities

At present, GIS is commonly used as a spatial information and visualisation tool in the existing Smart Cities. The utilisation of this powerful technology varies considerably across cities, often limited by non-availability of base maps and non-adaptability of Enteprise GIS Platforms. GIS will play a significant role in spatial decision making in Smart Cities when standards-based maps are developed and integrated into routine functioning of the Smart Cities.

Currently, cities are not completely aware about the overall functional requirements of the GIS and the technological architecture of the enterprise-wide GIS, which is important for collaborative decision making.

In absence of standards for the GIS layers that need to be adopted, the cities are not able to take the benefits of the Enterprise GIS for the decision making in the cities.

This standard has been developed with the objective of defining the GIS usability for the different stakeholders in smart cities. It provides a conceptual GIS architecture with functionalities to use as an enterprise system for spatial decision making.

To guide the cities in the usability of the GIS, the functional requirements are mentioned.

Lastly GIS application use cases are provided to guide the city in understanding the GIS applicability for the smart city in standardized ways.

This standard has to be read in conjunction with other standards on Smart Cities or Unified Digital Infrastructure such as IS 18000, IS 18002, IS 18004, IS 18006 etc.

Enterprise GIS is an architecture that integrates geospatial data and services and shares them across the organization. It can also be viewed as an infrastructure that extends and enables existing systems using geospatial data and services.

Core to enterprise GIS is the ability to meet organizational objectives through the delivery of geospatial capabilities that include the following:

a) Data management — data management is important in an enterprise setting. Enterprise GIS data management focuses on the efficient storage and retrieval of all of an organization's relevant geographic information. An enterprise GIS data may be decentralized, with appropriate data management standards and data governance processes defined, so as to ensure that the data integrity is maintained and also the data is available for usage by everyone in the organization.

b) Visualization — The visualization of information in a geographic context provides an intuitive means for accurate and rapid decision making. Visualization is the most obvious manifestation of enterprise GIS, however, enterprise GIS should fully exploit visualization capabilities by incorporating them into tasks and activities not traditionally associated with GIS like e-Governance applications or Business applications or ERP.

c) Spatial analysis — exploiting the wealth of geographic information in an organization is the goal of spatial analysis for the enterprise. Non-traditional users of GIS will benefit from this capability. A key objective of enterprise GIS architects and designers should be the geospatial enabling of other enterprise systems (e.g., IoT applications) with spatial analytical capabilities.

0.2 Key Stakeholder concern

The stakeholders in the current environment of the Smart City involves the Special purpose Vehicle (SPV), the Municipal Corporation, Citizens, Business, Researchers, Operation and Maintenance Team of cities, State Government and Central Government. Table 1 provides a summary of different stakeholders of smart city their business processes and their requirements from a GIS perspective.

Table 1 Stakeholders requirements from GIS perspective in Smart Cities

Stakeholder	**Business requirements**	**GIS Requirements**
Municipality	1. City Base Maps including different layers of information like Roads, sewerage network. public bins, street lights etc. 2. Tracking of different projects in the city for construction, maintenance and operations. 3. Strengthening the municipal finance through revenue enhancement and expenditure monitoring. 4. Tracking the performance of different city aspects like pollution, cleanliness, literacy, distribution of	1. City Geodata model with Defined layers, attributes, relationships and cartography. 2. Common Base maps for all Departments to collaborate on decision making. 3. Collect spatial information from various sources and utilize it across the enterprise. 4. Spatial tracking of municipal projects/activities. 5. Spatial tracking of municipal Income and expenditure. 6. Spatial tracking of performance of city as per different parameters.

	healthcare facilities in a ward/locality etc. 5. Covid- 19 related Contentment Zone, Vaccination Centre, Covid Center/Hospitals.	7. Spatial tracking of all city assets and resources. 8. GIS based mobile app with workflow for field operations in city level. 9. Survey apps to collect the pandemic related data and display as dashboards.
Smart City SPV	1. Planning the smart city in terms of planning, design, construction and operations. 2. Asset Inventory of the smart city and their coverage. 3. Real time tracking of the information flow and access to different spatial layers for a coordinated decision making.	1. Common Base Maps to understand the requirement of different stakeholders of smart city. 2. Municipal Assets inventory required for Smart City. 3. Spatial Area Based Development (ABD) planning. 4. Get the virtual view of the city and urban features and urban problems. 5. Spatial view of Smart City Components (Cameras, GPS enabled Devices, Sensors, IoT devices) with geo-spatial data for smooth operation and monitoring. 6. Real time vehicle tracking, citizen sentiment capture through social media integration. 7. Generation of hotspots and analytics of pollution, crime, incidents, events, grievances etc. 8. Geospatial dashboards for decision support system regarding the performance against the benchmarks or thresholds.
Citizens	1. Access to different locational information like, the amenities in the neighborhood.	1. Means to interact with city through GIS based Web Apps and Mobile Apps, like neighborhood services.

	2. Access to different spatial information like Road closure intimation, or traffic jam intimation. Participate in city governance. 3. Raise grievance through mobile Apps using location and geotagged images/ photos. 4. Locationinformation related to Pandemic/disease Spread.a Information related to hazards.	2. Participation in governance on Development Plans and Smart Developments and different urban issues. 3. Routing services for moving from one place to other Sharing location data and features with different people. 4. Mobile Apps for citizen's grievance management. 5. Apps to report incident or seek help in the event of Medical outbreak. 6. Integration with Sensors to cover the real time weather and Hard Information for public.
Utility Services	1. Maps for the existing location of the Assets. 2. The demand of services and supply of services. 3. Real time location of the problem areas and quick repair.	1. Common set of base maps for design and construction, operation and maintenance and decision making for utilities like electricity, water, sewerage, storm water drains, street light, piped gas, etc. 2. Utility asset GIS data model to generate inventories of all the assets of the utilities. 3. Spatial asset lifecycle management for under-standing age of the asset. 4. Spatial workflow based asset operation and maintenance for addressing the operational problems.
Business	1. Needs locational intelligence for setting up chains, service centers, new business, and branches.	1. Platform to integrate with open socio-economic data like, population density data, socio economic data, administrative boundaries, land use details.

Researchers	1. Needs access to spatial and non spatial data related to urban features/problems.	1. Platform to get open GIS data/ APIs for conducting spatial research on urban dynamics and issues.
Operation and Maintenance Term of City	1. Needs the details of the City properties and assets. 2. Need location of the problem areas for quick service delivery.	1. Location based workflows for reporting of urban issues and problems like water leakage or potholes on roads. 2. Location based alert generation as a part of spatial workflow. 3. City problem tracking and resolution status. 4. GIS based dashboard for tracking of O& M performance.
State Government	1. Needs to undertake monitoring of the projects progress under the mission cities in the state. 2. Needs to undertake the monitoring of funds utilization and requirement for mission objectives.	1. Monitoring of the Smart Cities projects in the state. 2. Smart City projects tracking Geographically with project management aspects. 3. Smart City fund tracking at state level.
Central Government	1. Needs to undertake monitoring of the projects progress under the mission cities in the country. 2. Needs to undertake the monitoring of funds utilization and requirement for mission objectives.	1. Monitoring of Smart City program progress. 2. Geographic Smart Cities project tracking. 3. Geographic Smart City fund tracking. 4. Smart city projects performance monitoring. 5. Enable gap based knowledge sharing between smart cities.

0.3 Role of GIS in Smart Cities

GIS plays an important role in the complete lifecycle of Smart City, from planning, designing, construction, operation and maintenance to management. Smart city GIS shall integrate with different survey tools, modelling software, different types of sensors and IoT devices, and other e-governance enterprise systems like land management applications, asset management systems etc. for spatial decision support.

a) **Planning and Design of Smart City:** GIS helps to analyse the location of the Assets and Properties in the city and the Gap in the provision as per population, area and distance norms. It helps to analyse the right sites for city development, view legal boundaries, and arrive at a right valuation of the existing or new sites. GIS integrates with different survey technologies like DRONE, Aerial Survey, LIDAR, GPR, etc and may be associated with design tools like Building information modelling (BIM), Computer Aided Design (CAD) for 3D analysis.

b) **Construct:** GIS should integrate with the project management and financial management systems and tools for construction monitoring of the different smart city projects.

c) **Operation and Maintenance:** GIS based asset Maintenance system create the models of all the assets and properties in the city for their maintenance, repair and refurbishment, real time update of functioning by integrating with SCADA, Smart Metering, Remote Transmission Unit (RTUs) etc and field operation management.

d) **City Expansion Plan:** This is important especially for the Green field Smart cities to create the land banks and inventory of infrastructure to attract buyers, tenants, business. Analyze demographics and market conditions to provide a more accurate picture of a property's suitability to needs.

e) **City Insights**: The GIS helps in the city management by creating intelligence of spatial distribution, collaborated operation and maintenance, dynamic real time dashboards about city functions, city economics (revenue and expenditure) and performances.

While defining the role of GIS in smart city, the following fundamental concepts should be taken care of:

a) Standardization: Standardization of urban processes, mobility and logistics, safety and security, information and communication, energy uses, and production etc.

b) Integration: integration of the different data system, processes, operational workflows, and real-time information.

c) Design thinking: Design thinking is an analytical and creative approach that focuses on the concerns, interests and values of the user. In the city's case, the user could be the citizen, the entrepreneurs, the academia and researchers, the builders and urban service providers.

d) Collaboration: collaboration should be across municipal departments, line departments, emergency services, businesses and NGOs, and most importantly, citizens. As an integral part of smart cities, citizens shall help public authorities to work more efficiently together by integrating citizen-sourced data from smart city apps, as well as individually reporting incidents or flagging concerns.

e) Innovation: City innovation in management, policy and technology. Since the unique context of each city shapes the technological, organizational and policy aspects of that city, a smart city can be considered a contextualized interplay among technological innovation, managerial and organizational innovation, and policy innovation.

(The above text has been taken from the INTRODUCTION given in the standard. However, the Figure 1 given in this clause in the document has not been reproduced here)

SCOPE

This Indian standard describes the Enterprise GIS reference architecture that comprises the functional architecture, technical reference model, and information reference model of the enterprise GIS. It also specifies the core capabilities and key design principles of the enterprise GIS. The implementation methodologies and deployment architecture of the GIS are excluded from the scope of this standard

67) IS 18010 (Part 1): 2020 Unified Digital Infrastructure - Unified Last Mile Communication Protocols Stack Part 1 Reference Architecture (UDI - ULMCPS - RA)

INTRODUCTION

Rapid urbanization over the past two decades has led to the mushrooming of megacities (accepted as those with a population in excess of ten million) around the world. The sheer size and scale of these cities place huge pressure on infrastructure development, public services provision, and environmental sustainability.

Cities nationally and internationally are main drivers of economic activity, growth and in the current context, recovery, but this output depends on a comprehensive infrastructure to deliver physical and social resources the fuel of a city's 'economic engine'. The economic performance of a city is inextricably linked to its physical and communications infrastructures, and the delivery of resources through these infrastructures.

The society, the business, the infrastructure, the services and all other aspects of the civilization on the planet Earth are going through a paradigm shift in the wake of technological advancements, especially in the field of ICT.

All the ecosystems like smart cities, smart grid, smart buildings, smart factories etc. are in the process of making the following three classes of transformations:

a) *Improvement of Infrastructure* — To make it resilient and sustainable;

b) *Addition of the Digital Layer* — Which is the essence of the smart paradigm; and

c) *Business Process Transformation* — Necessary to capitalize on the investments in smart technologies.

Smart city technologies based on digital infrastructure and digital services offers a potential way of monitoring and managing physical and social resource in the city. Digital technologies can collect sufficiently large amounts of data to support very close matching of supply availability against demand requirements. The new communication potential from sensors on buildings, roads and other elements of the city and the sharing of data between service delivery channels, if integrated, will enable the city to improve services, monitor and control resource usage and react to real-time information.

A defining feature of smart cities is the ability of the components and systems to function efficiently in an integrated manner as well as independently. The optimal use of resources across a complex urban environment depends on the interaction between different city services and systems. To identify the most effective use of resources, therefore, requires communication between the different component systems (for example, energy consumption monitored by smart metering combined with external temperature and sunlight monitoring on the building to reduce the energy consumption).

Smart infrastructure is the result of combining physical infrastructure with digital infrastructure, providing improved information to enable better decision-making, faster and cheaper.

However, the rapid growth in communication technologies for last more than four-five decades has provided the users with multiple choices with their respective diversities and USPs for different applications and use cases. As a result, stakeholders of different ecosystems have chosen different technologies and protocols to meet their respective applications needs. In some cases, even different segmented stakeholders of a common ecosystem have developed/adopted different, communication technologies, protocols, data semantics and standards.

The siloed way of deploying the IoT/M2M infrastructure is not desirable and a need was felt to have a harmonized common last-mile communication architecture approach. In a smart city scenario, to enable interoperability between divergent devices as well as applications while maintaining identity and access control, it is desirable to have common last-mile communication architecture. This will also ensure feasibility in the sharing of data with ensured security and privacy.

The IoT value chain is perhaps the most diverse and complicated value chain. Due to heterogeneity and lack of convergence the smart nodes of one network cannot talk to smart nodes of the other networks. The variety of solutions with limited interoperability exist for different areas like home automation, building automation, industrial automation etc. This limited interoperability is the major driving factor to consider developing Unified, resilient, secure and sustainable, ICT framework for smart infrastructure developments. The Standard IS 18000 'Unified digital infrastructure ICT reference architecture' (presently under development) defines a comprehensive ICT reference architecture for a resilient, secure and sustainable digital infrastructure for smart cities, districts, states or nations.

The unified last mile communication protocols stack reference architecture is an integral part of the 'unified digital infrastructure ICT reference architecture' and it layouts the contours of unified communication for 'smart city' and 'smart infrastructure'.

SCOPE

1.1 This Indian Standard defines the Unified Last Miles Communication Protocol Stack – Reference Architecture (ULMCP-RA) for communication devices deployed in digital infrastructure.

1.2 The reference architecture described in this standard supports devices which operate using different communication technologies and deployed in any of the following topologies:

a) Personal Area Network (PAN);
b) Neighbour Area Network (NAN);
c) Field Area Network (FAN); and
d) Wide Area Network (WAN).

1.3 This standard also provides a brief description of other standards in the last mile communication protocol stack series.

NOTE — This standard covers only IPv6 based networks.

68) **IS 18010 (Part 4/Sec 1): 2022 IEEE Std 2857 – 2021 Wireless Smart Utility Network Field Area Network (FAN) (Unified Digital Infrastructure Unified Last Mile Communication Protocols Stack Part 4 Network Access Interface Layer Section 1 Specification)**

SCOPE

This document defines the technical implementation and behavior of a Wi-SUN Field Area Network which fulfills the marketing requirements specified in [MRD]. With the details presented in this document, an implementer is enabled to construct an interoperable and certifiable implementation of the Wi-SUN FAN.

69) **IS 18010 (Part 5/Sec 1) : 2020 Unified Digital Infrastructure Unified Last Mile Communication Protocols Stack Part 5 Network Access Layer (IEEE 802.15.4) Section 1 Specification**

INTRODUCTION

The rapid growth in communication technologies for last more than four-five decades has provided the users with multiple choices with their respective diversities and USPs for different applications and use cases. As a result, stakeholders of different ecosystems have chosen different technologies and protocols to meet their respective applications needs. In some cases, even different segmented stakeholders of a common ecosystem have developed/adopted different, communication technologies, protocols, data semantics and standards.

The siloed way of deploying the IoT/M2M infrastructure is not desirable and need was felt to have a harmonized common last-mile communication architecture approach. In a smart city scenario, to enable interoperability between divergent devices as well as applications while maintaining identity and access control, it is desirable to have common last-mile communication architecture. This will also ensure feasibility in the sharing of data with ensured security and privacy.

The unified last mile communication protocols stack reference architecture is an integral part of the unified digital infrastructure ICT reference architecture and it layouts the contours of unified communication for 'Smart City' and 'Digital Infrastructure'.

The key characteristic of "Last-Mile" communication technologies and their respective communication protocols defined as one of the principal constituents of the unified digital infrastructure reference architecture is the need to connect heterogeneous devices with heterogeneous applications while maintaining the necessary interoperability across all such devices (irrespective of the diversity in the PHY and Link-Layer Technologies) and offer a seamless view to the Applications. They should also allow connectivity to existing infrastructures and to the internet.

The ULMCPS reference architecture is derived from the well-established and globally accepted standard – the OSI Model. The Standard OSI model has been improvised to ensure the multiple communication technologies can work in homogenous manner

This Standard establishes the network access layer of ULMCPS reference architecture and specifies the physical and medium access control layers based on IEEE 802.15.4 – 2020 specifications customized to comply with Indian spectrum regulatory notifications in the de-licensed Sub GHz 865 – 867 MHz band.

(The above text has been taken from the INTRODUCTION given in the standard. However, the Figure 1 and Figure 2given in this clause in the document have not been reproduced here)

SCOPE

1.1 This Standard (Part 5/Sec 1) establishes the network access layer of unified last mile communication protocol stack reference architecture (ULMCPS RA) and specifies requirements the physical layer and medium access control layer for the communication devices deployed in digital infrastructure.

1.2 This standard is based on IEEE 802.15.4 – 2020 and customized to comply with Indian spectrum regulatory notifications in the de-licensed Sub GHz 865 – 867 MHz band. The current specification adds the SUN-FSK modulation schemes only. Other modulation schemes defined in IEEE 802.15.4 - 2020 may be considered in the future revisions of this standard based on the requirements.

1.3 This standard is applicable for constrained application with for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements.

ANNEXURES

ANNEX I

CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies are organizations that conduct activities to determine whether products, services, systems, or processes comply with relevant standards and regulations. These bodies perform testing, certification, inspection, and accreditation to validate the performance, safety, and interoperability of IoT products. Here are some key conformity assessment bodies related to the Internet of Things**:**

1. Bureau of Indian Standards (BIS)

The Bureau of Indian Standards (BIS) is India's national standards body responsible for developing and implementing national standards, including those related to IoT. BIS provides certification and conformity assessment services to ensure that IoT products meet Indian standards for quality, safety, and interoperability.

Website: https://www.bis.gov.in/

2. Telecommunication Engineering Centre (TEC)

The Telecommunication Engineering Centre (TEC) is a technical arm of the Department of Telecommunications (DoT) in India. TEC is responsible for developing technical standards and specifications for telecom products, services, and networks, including IoT devices. TEC conducts testing and certification for ensuring compliance with these standards.

Website: https://www.tec.gov.in/

3. Standardisation Testing and Quality Certification (STQC) Directorate

The Standardisation Testing and Quality Certification (STQC) Directorate, an attached office of the Ministry of Electronics and Information Technology, Government of India, provides comprehensive quality assurance services in Electronics and IT through its network of accredited laboratories and centers. Offering services such as Testing, Calibration, IT & e-Governance, Training, and Certification, STQC supports both public and private organizations. The IoT System Certification Scheme (IoTSCS) operated by STQC aims to support IoT products and systems by evaluating all components, including sensors, actuators, communication protocols, IoT gateways, IoT cloud, end-user devices, and user interfaces, ensuring conformity and quality in IoT solutions.

Website: https://www.stqc.gov.in/node/614

4. International Electrotechnical Commission (IEC) System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

The IECEE operates worldwide conformity assessment schemes in the fields of electrical and electronic equipment. It provides certification for IoT products, ensuring they meet IEC standards for safety, performance, and interoperability.

Website: https://www.iecee.org/

5. Open Connectivity Foundation (OCF) Certification

OCF provides a certification program for IoT devices to ensure they comply with OCF standards for interoperability and security. OCF certification helps manufacturers demonstrate that their IoT products can seamlessly connect and interact with other OCF-certified devices.

Website: https://openconnectivity.org/

6. Connectivity Standards Alliance Certification (earlierZigbee Alliance)

The Connectivity Standards Alliance offers certification for IoT products that comply with Zigbee standards. This certification ensures interoperability and performance of Zigbee-enabled devices, facilitating their integration into IoT ecosystems.

Website: Connectivity Standards Alliance

ANNEX II

REGULATORY BODIES AND RELEVANT ACTS/ REGULATIONS/RULES

The rapid development of the Internet of Things (IoT) brings various regulatory challenges and considerations, such as security, privacy, data protection, and interoperability. Multiple regulatory bodies and relevant acts, regulations, and rules oversee these aspects to ensure the safe and effective deployment and operation of IoT systems. Here are some of the key regulatory bodies for IoT:

International Regulatory Bodies and Regulations

1. International Telecommunication Union (ITU)

ITU is a specialized agency of the United Nations responsible for issues related to information and communication technologies (ICTs) which are essential for ensuring the efficient use of radio frequencies for IoT communication.

Example: ITU-T Recommendations: Standards and protocols for IoT and smart cities, such as ITU-T Y.2060, which defines the IoT reference model.

2. European Union (EU)

The EU has established comprehensive regulations to address various aspects of IoT like:

- General Data Protection Regulation (GDPR):

  GDPR is an European Regulation that standardizes the rules for processing personal data by private businesses and government bodies in the whole European Union. **[SOURCE: NEN NPR 5326:2019, 3.3](ISO/IEC TR 7052:2023(en), 3.27)**

  GDPR mandates strict requirements for the collection, processing, and protection of personal data, including IoT data. Compliance involves obtaining user consent, ensuring data transparency, and implementing security measures to protect personal information.

- Radio Equipment Directive (RED): Sets essential requirements for safety, health, and efficient use of the radio spectrum.

- Cybersecurity Act: Establishes a framework for cybersecurity certification of ICT products, services, and processes.

3. National Institute of Standards and Technology (NIST)

NIST is a U.S. federal agency that develops standards and guidelines, including those for IoT like:

- NIST Special Publication 800-183: Networks of ‘Things’ offers guidelines for IoT architecture and security.

- NIST Cybersecurity Framework: Provides a policy framework for improving cybersecurity practices.

Indian Regulatory Bodies and Relevant Acts/Regulations/Rules

1. Department of Telecommunications (DoT)

The Department of Telecommunications (DoT) is responsible for the overall regulation of telecommunications in India, including IoT. The DoT issues guidelines and regulations to ensure the seamless integration and security of IoT networks.

Key Regulations:

National Digital Communications Policy 2018: It aims to enhance India's digital infrastructure and connectivity, emphasizing the development and integration of emerging technologies like the Internet of Things (IoT). The policy focuses on establishing a robust framework for IoT to support smart cities, agriculture, healthcare, and industrial automation. It advocates for secure, scalable, and interoperable IoT systems while promoting data protection and privacy. The policy also encourages innovation, investment, and capacity-building to position India as a global leader in IoT technology and services.

IoT Policy Documents: The DoT has released various policy documents and guidelines aimed at the proliferation of IoT technologies in India.

Website: DoT

2. Telecom Regulatory Authority of India (TRAI)

The Telecom Regulatory Authority of India (TRAI) regulates the telecommunications sector, including IoT services. TRAI focuses on ensuring fair competition, quality of service, and consumer protection in the telecom industry.

Key Regulations:

Recommendations on IoT: TRAI has issued recommendations on regulatory frameworks for IoT, addressing issues like data privacy, spectrum allocation, and network security.

Quality of Service Regulations: These regulations ensure that IoT services meet predefined quality standards.

Website: TRAI

3. Ministry of Electronics and Information Technology (MeitY)

The Ministry of Electronics and Information Technology (MeitY) is responsible for promoting digital technology and overseeing the implementation of policies related to IoT and other emerging technologies.

Key Regulations:

National IoT Policy (Under Development): This policy framework aims to create an IoT ecosystem in India, promoting research and development, standardization, and deployment of IoT technologies.

Digital Personal Data Protection Act, 2023: The act aims to safeguard personal data, emphasizing transparent, lawful processing, and explicit consent. It grants individuals rights to access, correct, and delete their data while mandating robust security and compliance measures for data fiduciaries. The bill significantly impacts the Internet of Things (IoT) by requiring stringent security protocols and clear data management practices to ensure privacy and regulatory adherence in a highly connected environment.

Website: MeitY

4. Reserve Bank of India (RBI)

The Reserve Bank of India (RBI) regulates IoT applications in the financial sector, particularly those related to digital payments and banking.

Key Regulations:

Guidelines on Payment Gateways and Payment Aggregators: These guidelines impact IoT-based payment solutions, ensuring secure and efficient transactions.

Regulations on Prepaid Payment Instruments (PPIs): These regulations govern IoT-enabled financial services and devices.

Website: RBI

5. National Critical Information Infrastructure Protection Centre (NCIIPC)

The NCIIPC is responsible for protecting India's critical information infrastructure, including IoT systems that are part of critical infrastructure sectors such as energy, banking, and transportation.

Key Regulations:

Guidelines for Protection of Critical Information Infrastructure: These guidelines include measures for securing IoT systems that are part of critical infrastructure.

Website: NCIIPC

6. Ministry of Home Affairs (MHA)

The Ministry of Home Affairs oversees internal security and has a role in regulating IoT applications that impact national security.

Key Regulations:

Cybersecurity Framework: The MHA issues guidelines and policies to ensure the cybersecurity of IoT devices and networks.

Website: MHA

7. Central Drugs Standard Control Organization (CDSCO)

For IoT applications in healthcare, the CDSCO regulates medical devices and ensures they meet safety and performance standards.

Key Regulations:

Medical Device Rules, 2017: These rules govern the approval and regulation of medical devices, including IoT-enabled devices used in healthcare.

Website: CDSCO

8. Telecommunication Engineering Centre (TEC)

TEC is a technical body under the DoT that develops standards for telecommunications equipment and networks.

- Technical Reports and Specifications: Guidelines for IoT and M2M communication, such as TEC TR on "IoT/M2M Ecosystem".

Website: TEC

ANNEX III
COURSE CURRICULUM

This section carries information on the course curriculums related to Internet of Things in some of the premier academic institutions in India

a. Introduction to internet of things, IIT Kharagpur

Internet of Things (IoT) is presently a hot technology worldwide. Government, academia, and industry are involved in different aspects of research, implementation, and business with IoT. IoT cuts across different application domain verticals ranging from civilian to defence sectors. These domains include agriculture, space, healthcare, manufacturing, construction, water, and mining, which are presently transitioning their legacy infrastructure to support IoT. Today it is possible to envision pervasive connectivity, storage, and computation, which, in turn, gives rise to building different IoT solutions. IoT-based applications such as innovative shopping system, infrastructure management in both urban and rural areas, remote health monitoring and emergency notification systems, and transportation systems, are gradually relying on IoT based systems. Therefore, it is very important to learn the fundamentals of this emerging technology.

Week 1: Introduction to IoT: Part I, Part II, Sensing, Actuation, Basics of Networking: Part-I

Week 2: Basics of Networking: Part-II, Part III, Part IV, Communication Protocols: Part I, Part II

Week 3: Communication Protocols: Part III, Part IV, Part V, Sensor Networks: Part I, Part II

Week 4: Sensor Networks: Part III, Part IV, Part V, Part VI, Machine-to-Machine Communications

Week 5: Interoperability in IoT, Introduction to Arduino Programming: Part I, Part II, Integration of Sensors and Actuators with Arduino: Part I, Part II

Week 6: Introduction to Python programming, Introduction to Raspberry Pi, Implementation of IoT with Raspberry Pi

Week 7: Implementation of IoT with Raspberry Pi (contd), Introduction to Software Defined Network (SDN) , SDN for IoT

Week 8: SDN for IoT (contd), Data Handling and Analytics, Cloud Computing

Week 9: Cloud Computing (contd), Sensor-Cloud

Week 10: Fog Computing, Smart Cities and Smart Homes

Week 11: Connected Vehicles, Smart Grid, Industrial IoT

Week 12: Industrial IoT (contd), Case Study: Agriculture, Healthcare, Activity Monitoring

Lecture Notes - https://archive.nptel.ac.in/content/storage2/courses/downloads_new/LectureNotes/106105166/106105166.zip

Book Link - https://drive.google.com/file/d/1ozJpedaHrcOCRZS1F2JOIWhsVL7S-r1w/view

Course Link - https://nptel.ac.in/courses/106105166

b. Introduction to Industry 4.0 and Industrial Internet of Things, IIT Kharagpur

Industry 4.0 concerns the transformation of industrial processes through the integration of modern technologies such as sensors, communication, and computational processing. Technologies such as Cyber Physical Systems (CPS), Internet of Things (IoT), Cloud Computing, Machine Learning, and Data Analytics are considered to be the different drivers necessary for the transformation. Industrial Internet of Things (IIoT) is an application of IoT in industries to modify the various existing industrial systems. IIoT links the automation system with enterprise, planning and product lifecycle.This course has been organized into the following modules:

Week 1 : Introduction: Sensing & actuation, Communication-Part I, Part II, Networking-Part I, Part II

Week 2 : Industry 4.0: Globalization and Emerging Issues, The Fourth Revolution, LEAN Production Systems, Smart and Connected Business Perspective, Smart Factories

Week 3 : Industry 4.0: Cyber Physical Systems and Next Generation Sensors, Collaborative Platform and Product Lifecycle Management, Augmented Reality and Virtual Reality, Artifical Intelligence, Big Data and Advanced Analysis

Week 4 : Cybersecurity in Industry 4.0, Basics of Industrial IoT: Industrial Processes-Part I, Part II, Industrial Sensing & Actuation, Industrial Internet Systems.

Week 5 : IIoT-Introduction, Industrial IoT: Business Model and RefereceArchiterture: IIoT-Business Models- Part I, Part II, IIoT Reference Architecture-Part I, Part II.

Week 6 : Industrial IoT- Layers: IIoT Sensing-Part I, Part II, IIoT Processing-Part I, Part II, IIoT Communication-Part I.

Week 7 : Industrial IoT- Layers: IIoT Communication-Part II, Part III, IIoT Networking-Part I, Part II, Part III.

Week 8 : Industrial IoT: Big Data Analytics and Software Defined Networks: IIoT Analytics - Introduction, Machine Learning and Data Science - Part I, Part II, R and Julia Programming, Data Management with Hadoop.

Week 9 : Industrial IoT: Big Data Analytics and Software Defined Networks: SDN in IIoT-Part I, Part II, Data Center Networks, Industrial IoT: Security and Fog Computing: Cloud Computing in IIoT-Part I, Part II.

Week 10 : Industrial IoT: Security and Fog Computing - Fog Computing in IIoT, Security in IIoT-Part I, Part II, Industrial IoT- Application Domains: Factories and Assembly Line, Food Industry.

Week 11 : Industrial IoT- Application Domains: Healthcare, Power Plants, Inventory Management & Quality Control, Plant Safety and Security (Including AR and VR safety applications), Facility Management.

Week 12 : Industrial IoT- Application Domains: Oil, chemical and pharmaceutical industry, Applications of UAVs in Industries, Real case studies :

c. Design for Internet of Things - IISc Banglore

Week 1 Introduction to IOTs - Improving Quality of Life

Week 2 Challenges to solve in IOTs - Energy I Power, Data Explosion, Security

Week 3 System design of an IOT System - Power supply, Processor, Memory Sensor Interface

Week 4 Wireless Interfaces - LAN - Bluetooth Low Enegy (BLE), Wi-Fi, Radio Frequency Identification (RFID), **low-power wide-area network** (**LPWAN**) ,**low-power wide-area** (**LPWA**), Long-Term Evolution Machine Type Communication LTE-M, NarrowBand-Internet of Things (*NB-IoT*)

Week 5 Power supply design - Low Dropouts (LDOs), Switching regulators - BuckBoostConverters,Energy Measurements

Week 6 Energy harvesting and battery life calculation - PV, RF , Kinetic Energy, TEGs, aeroelastic flutter, Harvesting ICs in silicon

Week 7 Protocols - loT MAC, REST based COAP, Publish subscribe- MQTI,AMQP, MONS

Week 8 Building an IOT System - Case Studies -Joule Jotter, Chhaya.

4. Vishwakarma Institute of Information Technology, Pune

1. **Introduction to IoT**:
   - Definitions, characteristics, history, and architectures of IoT.
   - Physical and logical design, enabling technologies, IoT frameworks, and IoT vs. M2M.
2. **Microprocessor & Microcontroller**:
   - Basics, types, evolution, and architecture of microcontrollers.
   - Pin configuration, port architecture, memory organization, and interfacing.
3. **IP-based Protocols for IoT**:
   - IPv6, 6LowPAN, RPL, REST, AMPQ, CoAP, MQTT.
   - Authorization and access control in IoT.
4. **IoT Security and Privacy**:
   - Challenges, threats, encryption, authentication techniques, privacy concerns, and best practices.
5. **Introduction to Sensors & Actuators**:
   - Definitions, working principles, sensor technology evolution, and characteristics.
6. **Types of IoT Sensors & Actuators**:
   - Temperature, humidity, motion, gas, smoke, pressure, image sensors, etc.
   - Basic actuators like servo motors, stepper motors, DC motors, relays, and solenoids.
7. **Applications**:
   - Use of smart sensors in IoT, Industry 4.0, robotics, and modern industrial applications.

8. **Interfacing**:

   o I/O interfaces for sensors, internet connectivity, memory/storage interfaces, signal conditioning, A/D conversion, noise reduction, and filtering.

- **IoT Concepts**:
  - o Understand fundamental concepts and architecture.
  - o Learn various IoT protocols.
  - o Gain knowledge on microcontrollers and their use in embedded systems.
- **Microcontrollers**:
  - o Basics, evolution, and architecture.
  - o Interfacing and memory organization.
- **IP-Based Protocols**:
  - o Learn protocols like IPv6, 6LowPAN, CoAP, MQTT.
  - o Understand access control and security challenges.
- **IoT Security**:
  - o Focus on encryption, authentication, and privacy.
  - o Best practices for securing IoT devices.
- **Smart Sensors**:
  - o Learn principles of smart sensors and actuators.
  - o Types include temperature, humidity, motion, gas, smoke sensors.
  - o Actuators like servo motors, stepper motors, relays.
- **Applications of Smart Sensors**:
  - o Use in Industry 4.0, robotics, modern industrial applications.
- **Interfacing and Signal Conditioning**:
  - o I/O interfaces, internet connectivity, A/D conversion, noise reduction.
- **Laboratory Work**:
  - o Hands-on projects with Arduino, Raspberry Pi, and other IoT platforms.
  - o Build IoT projects like temperature sensors, stepper motor control, home automation.

5. Indraprastha Institute of Information Technology, Delhi (IIIT, Delhi)

Course Name : Introduction to Internet of Things (IoT) –*Online Course*

(Same as IIT, Kharagpur)

Internet of Things (IoT) is presently a hot technology worldwide. Government, academia, and industry are involved in different aspects of research, implementation, and business with IoT. IoT cuts across different application domain verticals ranging from civilian to defence sectors. These domains include agriculture, space, healthcare, manufacturing, construction, water, and mining, which are presently transitioning their legacy infrastructure to support IoT. Today it is possible to envision pervasive connectivity, storage, and computation, which, in turn, gives rise to building different IoT solutions. IoT-based applications such as innovative shopping system, infrastructure management in both urban and rural areas, remote health monitoring and emergency notification systems, and transportation systems, are gradually relying on IoT based systems. Therefore, it is very important to learn the fundamentals of this emerging technology.

INTENDED AUDIENCE : CSE, IT, ECE, EE, Instrumentation Engg, Industrial Engineering

PREREQUISITES : Basic programming knowledge

Week 1: Introduction to IoT: Part I, Part II, Sensing, Actuation, Basics of Networking: Part-I

Week 2: Basics of Networking: Part-II, Part III, Part IV, Communication Protocols: Part I, Part II

Week 3: Communication Protocols: Part III, Part IV, Part V, Sensor Networks: Part I, Part II

Week 4: Sensor Networks: Part III, Part IV, Part V, Part VI, Machine-to-Machine Communications

Week 5: Interoperability in IoT, Introduction to Arduino Programming: Part I, Part II, Integration of Sensors and Actuators with Arduino: Part I, Part II

Week 6: Introduction to Python programming, Introduction to Raspberry Pi, Implementation of IoT with Raspberry Pi

Week 7: Implementation of IoT with Raspberry Pi (contd), Introduction to SDN, SDN for IoT

Week 8: SDN for IoT (contd), Data Handling and Analytics, Cloud Computing

Week 9: Cloud Computing (contd), Sensor-Cloud

Week 10: Fog Computing, Smart Cities and Smart Homes

Week 11: Connected Vehicles, Smart Grid, Industrial IoT

Week 12: Industrial IoT (contd), Case Study: Agriculture, Healthcare, Activity Monitoring

Course Name: **Smart Sensing for Internet of Things (IoT)**

This course will introduce students to sensors and sensing systems that are in the "real-world" and are increasingly connected to the internet and are accessible via web technologies. The objective of the course is to understand IoT sensing systems, protocols and technologies. An integral part of the course will be a IoT project that the students will have to design, build and demonstrate. The final project will span the full research cycle - from problem formulation to obtaining & analyzing results to paper writing. Specifically, the course aims to provide students with a comprehensive introduction to this area, a training in sensing mechanisms, protocols for such devices, as well as an in-depth understanding of networking mechanisms. The course will enable students to understand deployment and configuration of these sensors in the real world with a focus on energy efficiency, challenging deployment conditions, routing and data-gathering. A substantial emphasis will be placed on software implementation. All students are expected to learn (largely on their own) how to program (hardware) and run simulations.

Students are required to complete a group project as part of this course. This course also aims to train students in the craft of academic research. For this end the students will be asked to critique several papers on IoT. By the end of the course, students are expected to be able to read research papers in a critical and analytical manner.

Week 1 & 2 :	Introduction to IoT
	RF and Wireless Technology Overview
	Communication channels and techniques
	Wireless technology overview and standards
	WiFi and cellular: next generation and IoT
	Sensors and Sensing Systems
Week 3 & 4 :	Estimation Theory
	Low Power Sensors and Sensing
Week 5 & 6 :	Hardware Platforms & SW Architecture
	SW and HW: platforms and development
	Device architecture
	Embedded software development
Week 7 & 8 :	Introduction to Contiki OS
	Time Synchronization
	Localization and Mobility
Week 9 :	Low Power Networking Protocols
	6LowPAN
Week 10 & 11 :	Security and Privacy
	Cloud computing and data analytics
	Energy harvesting
Week 12 :	Recent research results in IoT
	Challenges: business models, monetization, hype
Week 13 :	Projects in Infrastructure, Homes, Healthcare
	Project presentations

Course Name: **Advanced Internet of Things**

This course will be dealing with advanced topics in Internet of Things. This course is a sequel of the Internet of Things course which introduced students to basics of foundational IoT technologies. This course delves deeper into some of the technologies pertinent to IoT. Students are expected to learn by implementing protocols etc. in their programmming assignments. They will be exposed to some of the latest research findings in IoT and expected to perform thought exercises by writing research project proposals extending the frontiers of current IoT research.

Finally, students will implement working prototypes of IoT systems inspired by algorithms proposed in research papers.

Week 1 & 2 :	IoT Basics: Concepts, Technologies, OS, Security, Machine Learning, Network
Week 3 & 4 :	IoT Device Architecture, IoT System Architecture; Cloud based Architecture; Analysis of system architecture and design in different IoT applications
Week 5 & 6 :	Sensing using Smartphones, Wearables, other body worn and body embedded systems; mHealth hardware design and debugging; Research frontiers in mobile based Sensing; Crowd sourcing
Week 7 :	Designing IoT User Interfaces
Week 8 & 9 :	IoT Protocols: Design and Implementation of network, management and other protocols in IoT applications
Week 10 & 11 :	Designing IoT Systems: Healthcare
Week 12 & 13 :	Designing IoT Systems: Smart Cities

6. BITS Pilani

Post Graduate Programme In Internet Of Things

IoT Technology and Applications (5 weeks)

Develop an understanding of IoT technology and Cyber-Physical Systems. Explore the vast spectrum of IoT applications and gain an appreciation of the building blocks of IoT.

Internet of Things is gaining widespread adoption across users and industries. With an estimated 43bn connected devices by 2023, hardware and software engineers will find it absolutely necessary to have at least an appreciation of the fundamentals behind this technology.

This five-week course provides an overview of IoT applications and their life cycles. Using case analysis and assignments, learners will acquire skills necessary to identify building blocks and design issues of each application.

The course also offers an introduction to IoT platforms, end devices, networks and cloud services.

Hardware Architectures for IoT (7 weeks)

Develop an understanding and use of typical processors & peripherals relevant to IoT, and design & build IoT hardware.

IoT systems are built on top of a network of components of varying complexity and computing capabilities, ranging from RFID tags, smart sensors and smartphones to multi-core embedded computers. It is important for hardware and software engineers to be able to architect custom hardware for IoT systems.

This seven-week course delves deep into the internal architecture of these individual components within the IoT system.

The learner will understand the characteristics and limitations of components such as processing units, memory, buses and associated peripherals in the context of IoT applications. This will enable the learner to analyses processing requirements of applications, design sub-modules to meet these requirements and architect the hardware using them. The analyses involved includes power consumption, timing and performance. Upon completion, the learner should be able to design these components

Communication and Networking Technologies in IoT (6 weeks)

Learn to assess, select and customize communication and networking technologies for IoT applications across a broad spectrum of domains.

IoT applications require data generated or acquired across geographically dispersed components to be processed collaboratively. This is achieved using appropriate communication systems and networks.

This six-week course provides an overview of various network models and technologies used in IoT systems. The learner gains insights into the characteristics of the complementary and competing technologies, analyses vulnerabilities and design network solutions.

Software and Programming in IoT (8 weeks)

Learn how to orchestrate the communication and collaboration between a large numbers of geographically distributed devices with diverse capabilities.

Software life-cycle of an IoT application differs significantly from that of conventional software. This eight-week course covers lifecycle of application software by focusing on IoT context at each stage:

1. Requirements (connectivity, constraint and scale of devices)
2. Architecture (hardware, software and communication)
3. Design (client-server software)
4. Deployment (distributed and constrained devices)

The learner will understand:

1. The impact of running an application on constrained devices
2. Design and implement a client software on smart devices
3. Design & implement RESTful services and deploy it on cloud

Sensors, Actuators and Signal Processing (6 weeks)

Learn how to connect the cyber world (computers and internet) with the physical world (e.g. human body, automobiles, factories).

IoT systems are made up of a large number of components that sense data or control events. Building IoT systems requires interfacing sensors and actuators with computing devices and networks. Often the raw sensor data has to be digitized and processed.

This six week course provides an understanding of technologies and interfacing requirements for sensors and actuators of varying complexity. The learner will obtain knowledge of signal processing techniques and interfacing techniques. Algorithms and techniques for fusing data from multiple sensors as well as for compressing data will also be covered.

Data Management in IoT (7 weeks)

Learn how to design and implement IoT applications that manage big data, streaming data, and/or distributed data.

The learner will be able to programme IoT applications to manage data where data volume and/or data rate is high or data is streamed. The course covers techniques to identify end-to-end data flow characteristics of an application and apply appropriate messaging models to build solutions. This seven-week course covers techniques for large scale processing of data on the server / cloud including analytics using tools. The course covers algorithms / techniques for specific patterns for distributed processing on the devices as well as techniques for fault-tolerant data processing.

Capstone Project

Demonstrate your knowledge and skills acquired in the Post Graduate Programme in Internet of Things by Designing and Implementing an end-to-end IoT system involving Hardware, Software and Networking elements

The Capstone project, by definition, involves identifying a problem in the real-world and developing a practical solution to the satisfaction of all users and stakeholders involved. Internet of Things (IoT) is a technology paradigm that has evolved with advancements in electronics, communication and information infrastructure to enable transformation of businesses, industries, governments and our own homes and living environments, etc.

The six-week Capstone is a culminating project which helps you leverage the knowledge and skills you have acquired during the study of various course modules of the PGP-IoT and design, develop and demonstrate an implementable solution to one such real-world problem. It is designed to encourage multidisciplinary skills in various technology and business domains, in addition to soft-skills such as teamwork, planning, communication and project management.

7. Vellore Institute of Technology

Certificate Program on "Internet of Things (IoT) using Sensors and Cloud computing

Microcontroller: (Hardware)

1. Programming in Embedded C
2. Digital and Analog interfacing
3. Serial port Programming
4. Interrupt Programming, ADC Programming
5. LCD interfacing , Relay interfacing
6. DC Motor control
7. PWM Programming

Sensors: (Hardware)

1. Temperature sensor, Hall Effect sensor
2. IR (InfraRed), LDR (Light Dependent Resistors) sensor

Java: (Software)

1. Basic Java programing, Eclipse IDE
2. Java Serial communication
3. Java Internet Protocols handling (HTTP)

Cloud Computing: (Software)

1. Introduction to cloud computing
2. Servlet for Java web server development
3. Introduction to Google App Engine (GAE))
4. Java Data Object (JDO) API for Data storage

8. SRM Institute of Science and Technology

B.Tech – Computer Science And Engineering with Specialization in Internet of Things

Programming for Problem Solving
Data Science
Computer Organization and Architecture
Data Structures and Algorithms
Object Oriented Design and Programming
Design and Analysis of Algorithms
Operating Systems
Software Engineering and Project Management
Advanced Programming Practice
Formal Language and Automata
Computer Networks
Database Management Systems
Artificial Intelligence
Fog Computing
Cloud Computing for loT
Introduction to loT: Sensors, Actuators and Microcontrollers
Introduction to Embedded Programming and Embedded OS
Internet of Things Architecture and Protocols
Machine Learning for loT
Introduction to Cloud Application Development for lo T
lo T Forensics
Network Programming for loT
Introduction to Security of Internet of Things and Cyber-Physical Systems
Data Visualization for loT
loT Techniques, Tools, and its application
Advanced Database Systems
Edge Computing
Energy Management for loT devices
Applied Software Techniques in loT Engineering
Fundamentals of Cybersecurity
Full Stack Development for loT
Deep Learning for loT
loT Privacy
Project
MOOC