सत्यमेव जयते
Department of Telecommunications
Ministry of Communications
Government of India

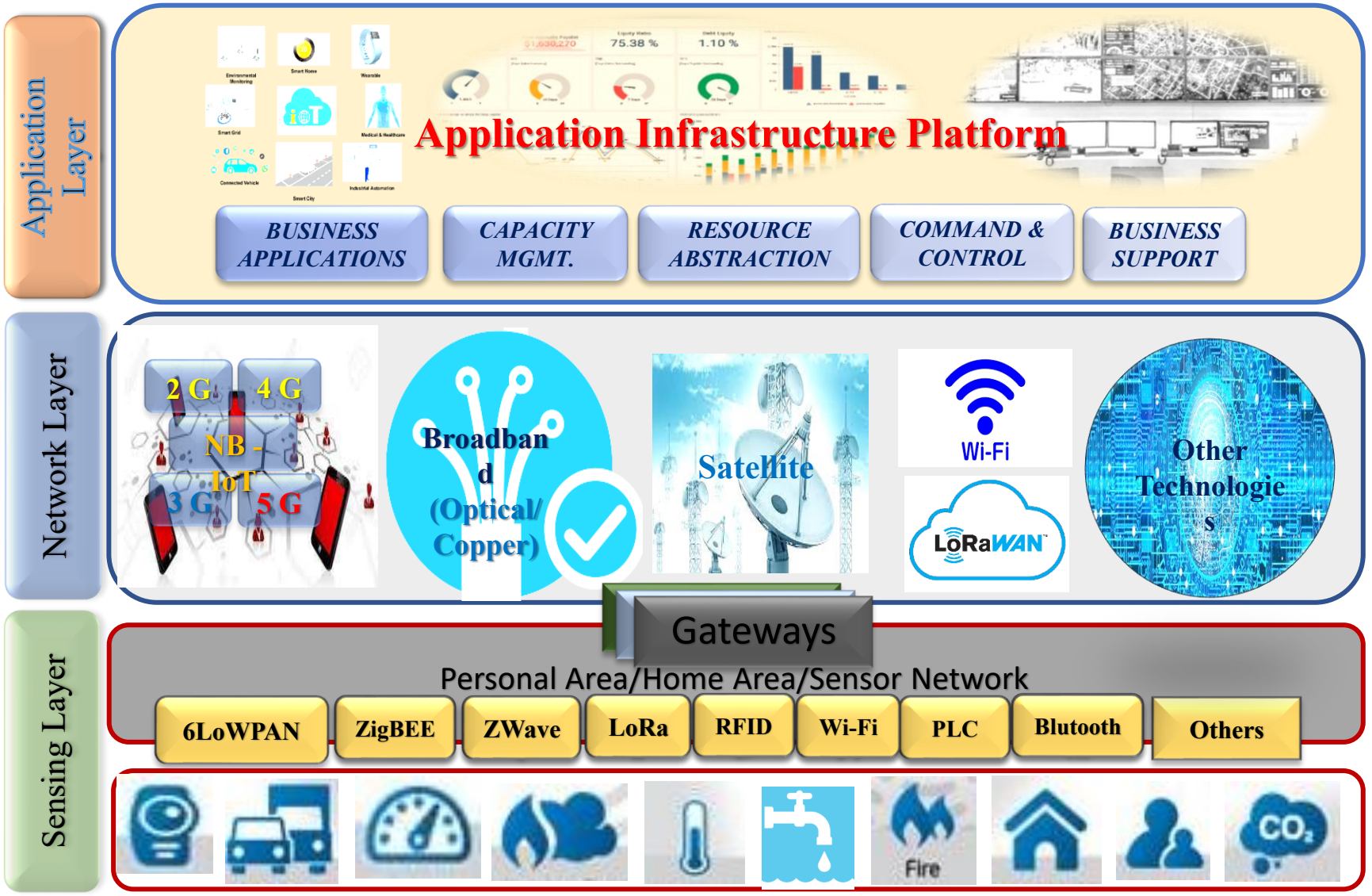
ISO 9001:2015

Enablers of Satellite based IoT ecosystem

R. S. Singh, ITS
Deputy Director General (IoT)
Telecommunication Engineering Centre,
Department of Telecommunications
Government of India

Typical IoT/M2M Architecture

- The sensing layer contains the sensors and actuators which connect to the gateways using any of the PAN/LAN technologies.
- The gateway devices typically connect using any network technologies shown in the Network Layer to the Application Infrastructure Platform shown in the Application Layer.
- The information pertaining to the sensors, actuators, gateways etc. are tightly coupled with the Application Layer entities.



Challenges in IoT Domain

Connectivity

Latency, availability, coverage and cost are some of the factors deciding the appropriate communication technology.

Standardization

There is a need for standards for various elements of the IoT ecosystem to ensure long term sustainable solutions and to prevent vendor lock-in in case of proprietary solutions

Interoperability and open interfaces

Interoperability is required at the device, network and platform/ application levels.
Interoperability is important to achieve the economies of scale

High cost of satellite-based user terminals and IoT devices

Lack of indigenous manufacturing

Battery Technology

Technologies for sustainability/ long life batteries is required for sensors

Security of IoT devices/ eco system

required to build trust in the network and also to manage vulnerabilities. e.g. Privacy is very important especially in health-care

NTN Technology for Satellite IoT

- Emergence of Non-Terrestrial Networks (NTN), standardized under 3GPP Release 17.
- Integration of satellite communication systems—particularly LEO satellites—with terrestrial 5G core networks, allowing the use of technologies such as Narrowband-IoT (NB-IoT) and LTE-M over satellite links.
- IoT devices designed for terrestrial mobile networks can now connect to satellites using the same hardware and SIM cards.
- NB-IoT based NTN, have enabled 'Direct to Device' (D2D) satellite communication for IoT devices that have been traditionally used with cellular networks.
- Deployment of NB-IoT NTN offers Extended link budget (for very low data rate access).

NTN Technology for Satellite IoT ..contd.

- Extend connectivity in a scalable way, bridging the digital divide and enabling global access.
- Ensures reliable connectivity in underserved or unserved areas.
- Provides consistent connectivity even in harsh weather or geographically challenging locations, where traditional IoT networks may fail.
- Enhance operational efficiency, improve data accuracy and enable more resilient, wide-area networks for critical applications.

Direct-to-Satellite LoRa® Technology

Integrating LoRa® with satellite technology offers several advantages:

- **Extended Coverage**: direct communication of IoT devices with satellites, further expanding the reach of IoT networks.
- **Low Power Consumption**: ideal for IoT devices in remote locations with limited power sources.
- **Cost-Effectiveness**: provides an affordable solution for large-scale IoT deployments

Several industries have begun to leverage direct-to-satellite LoRa® technology, seeing significant improvements in operational efficiency and cost, data accuracy, sustainability and safety.

Regulatory & Policy Initiatives by Govt. in IoT/M2M domain

1. National Telecom M2M Roadmap – 2015
2. National Digital Communication Policy (NDCP)-2018
3. KYC Guidelines for M2M SIMs
4. Instructions for embedded-SIMs (e-SIMs)
5. 13-digit numbering scheme for M2M SIMs
6. Adoption of oneM2M Release 2 & 3 Standards as national standards for IoT/M2M.
7. Guidelines for registration of M2M service providers and WPAN/WLAN connectivity providers.
8. New license for UL(M2M) and UL-VNO(M2M) under UL and UL-VNO

SATCOM in India – An Overview

- SATCOM started in the country in 1982-83 with INSAT-1A & 1B Satellite.
- Presently, Department of Telecom (DoT) monitors 18 indigenous satellites and 19 foreign satellites providing Satellite-based communication services.
- DoT issues Licenses/ Authorizations/ permissions for providing Satellite-based communication services.

Satellite Services: Regulatory framework

As on date, the following licenses are being issued for Satellite services :

- **Commercial VSAT CUG authorization under Unified License (UL)**
- **GMPCS authorization under UL**
- **Captive VSAT CUG license**
- **In flight and Maritime Connectivity (IFMC)**

NLD authorization holder under UL is also permitted to provide services through Satellite after certain clearances.

Commercial VSAT CUG Service License

- The scope of this service is to provide, inter-alia, data connectivity between various sites scattered within territorial boundary of India using VSATs in a Closed User Group (CUG).
- Commercial VSAT CUG license can be used to provide backhaul connectivity to the Access Service providers for cellular mobile services and for establishing WiFi hotspots. However, PSTN/PLMN connectivity is not permitted.
- The licensee may also use the VSAT terminal to aggregate the traffic from M2M/loT devices/aggregator devices of the CUG and also to provide backhaul connectivity to service providers having license/ Authorization/ Registration for M2M services.
- User terminal stations on moving platform(s) are also permitted for provisioning of connectivity subject to compliance to relevant TEC standard(s) and conditions mentioned therein.

Captive VSAT Services Authorization

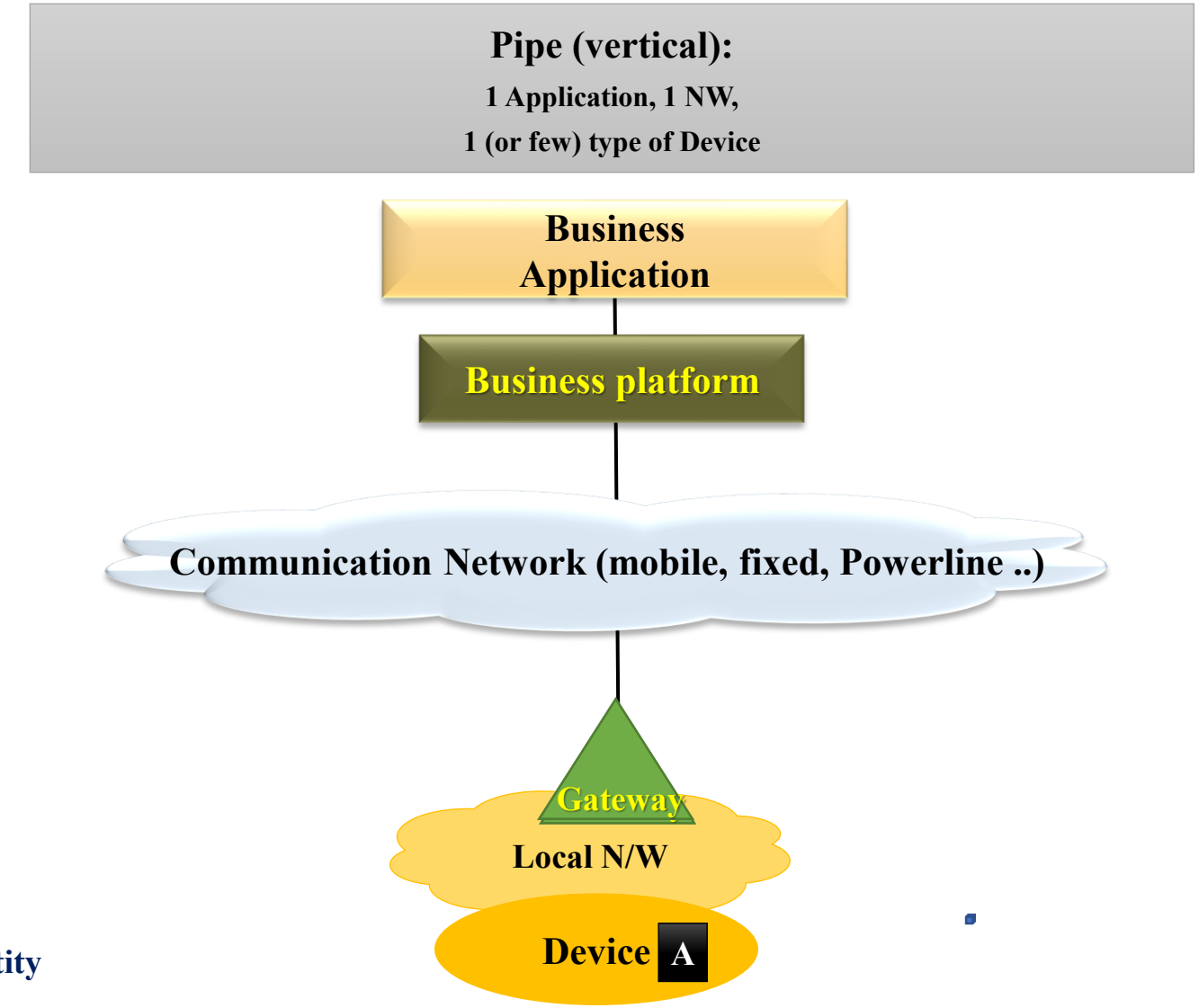
- License conditions are almost same as on Commercial VSAT Scope of Service, except the following:
- Network will be used only for internal communication & non-commercial purposes of Licensee.
- No long distance carrier rights.
- Licensees can set up any number of CUG for their own use.
- No Roll Out Obligations
- Mainly used for the Government Departments and organizations

Space Based Applications

Satellite IoT is increasingly becoming a vital solution across various sectors, offering enhanced connectivity and real-time data management. Key use cases include:

- **Logistics and Supply Chain:** Global asset tracking and monitoring in remote locations. Provides real-time tracking of containers and shipments in remote areas, improving operational efficiency.
- **Remote Infrastructure Monitoring**: Continuous monitoring of infrastructure in hard-to-reach areas, improving reliability and reducing downtime.
- **Remote Healthcare**: Transmission of real-time data from rural or isolated regions.
- **Transportation and Fleet Management**: Satellite connectivity ensures uninterrupted communication for transportation systems, optimizing routes and enhancing safety. GNSS-enabled tolling systems, which use satellite signals for accurate vehicle tracking and location-based fee collection, have been a significant innovation in improving traffic management and reducing congestion on highways.
- **Energy:** Enables remote monitoring of critical infrastructure, such as oil rigs and renewable energy installations.
- **Disaster Management:** Assists in emergency response efforts by offering reliable communication and data services in disaster-affected areas.
- **Military and Defence:** Facilitates secure communications, surveillance, and reconnaissance for armed forces.
- **Wildlife:** Satellite IoT helps in monitoring and protecting wildlife by enabling real-time tracking of animals and detecting illegal poaching activities, supporting conservation efforts.

Present IoT/M2M Deployment Architecture



Issues with this proprietary siloed deployment

- Interoperability: Due to non-standardised proprietary implementations the devices and applications do not interoperate; giving rise to higher TCO
- Data Sharing: Siloed Nature of the Applications make sharing of data amongst divergent applications very difficult and controlled by the Application Provider(s)
- Vendor Lock-In: All the applications are deployed and controlled by a single vendor. New Application onboarding difficult
- Security- Device Security, Authentication, Communication Security, Data Integrity, Data Privacy, Lawful Interception

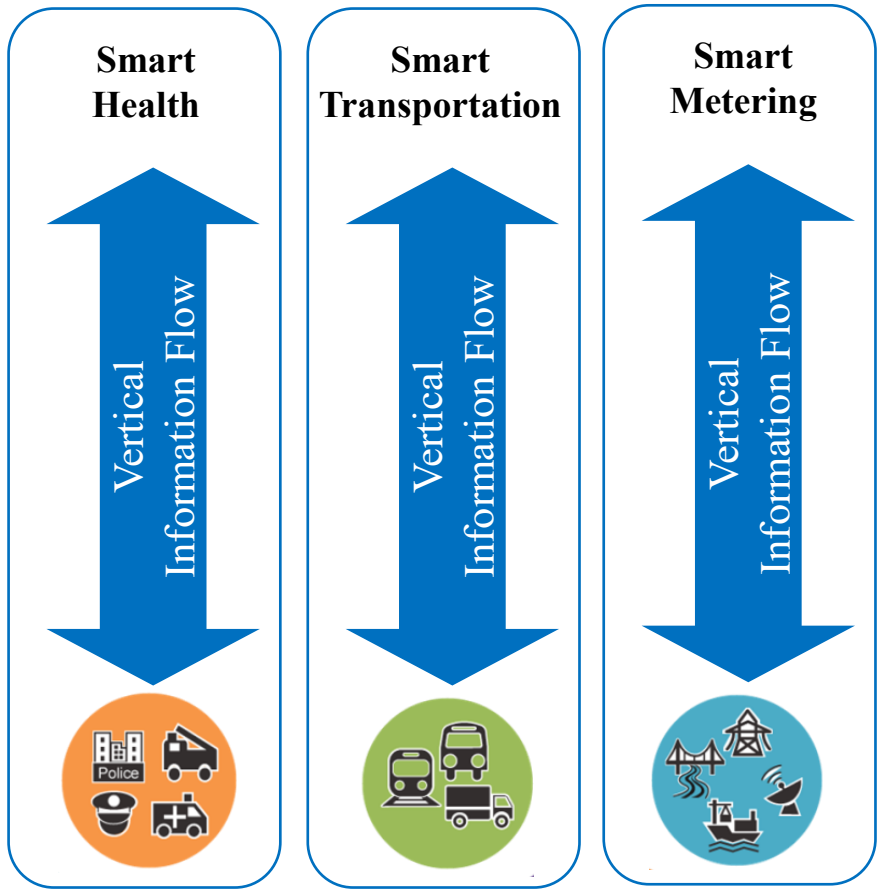
oneM2M Standards

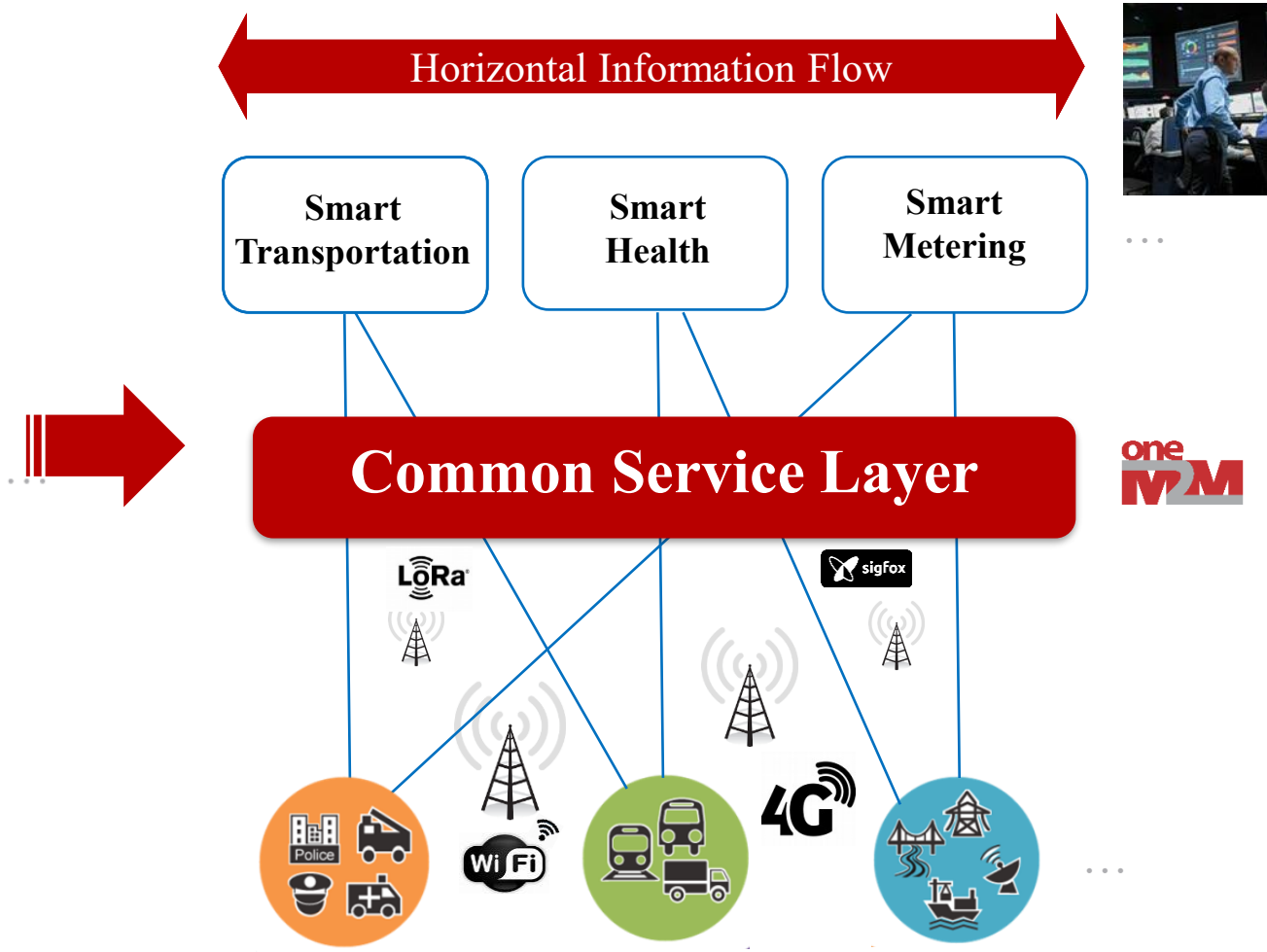
- TEC adopted TSDSI transposed **oneM2M Release 2 and Release 3** specifications as National Standards Standards in 2020 and 2022 respectively.

- The important benefits of implementing oneM2M standards-based solution includes interoperability of device & application; authentication & authorization of devices; and Data security & Privacy. These specifications will enable the development of standardized IoT ecosystem in the country including smart cities.

- These TEC national standards have been referred by BIS in its standard on IoT Reference Architecture - IS 18004 (Part 1): 2021 and MoHUA in its Smart City RFP.

oneM2M Breaks Down the Silos





TEC Technical Reports on M2M/ IoT

- **Twenty-three Technical Reports** have been released by TEC covering various verticals such as Power, Automotive (Intelligent transport system), Remote Health Management, Safety & Surveillance, Smart homes, Smart cities, Smart Village & Agriculture, Smart manufacturing etc., and also in the horizontal layer (requirements common to all the verticals) such as M2M Gateway & Architecture, Communication Technologies, EMF Exposure from IoT devices and Security aspects in M2M/ IoT domain (https://tec.gov.in/M2M-IoT-technical-reports).

- **International recognition of TEC TR on M2M/ IoT**: International Telecommunication Union (ITU) has posted the following seven TEC Technical Reports on its Digital Transformation Resource Hub in IoT sections (2024, 2023, 2022 and 2021), recognizing as insightful technical resource for the benefit of global community (https://www.itu.int/cities/dt-resource-hub/iot/)-

    i. Revolutionizing Agriculture: The Digital Transformation of Farming
    ii. Security by Design for IoT Device Manufacturers
    iii. Framework of National Trust Centre for M2M/IoT Devices and Applications
    iv. IoT/ ICT Standards for Smart Cities
    v. Emerging Communication Technologies & Use Cases in IoT Domain
    vi. Code of Practice for Securing Consumer Internet of Things (IoT)
    vii. IoT/ ICT Enablement in Smart Village and Agriculture

Code of Practice for Securing Consumer IoT, released by TEC in Aug 2021

This document on Code of Practice for consumer IoT security provides 13 baseline requirement based on ETSI EN 303 645.

WEF Joint statement on consumer IoT Security released in Feb 2022

a. No universal default passwords
b. Implementing a vulnerabilities disclosure policy
c. Keeping software updated
d. Securely communicating
e. Ensure that personal data is secure

DoT has endorsed **Code of practice for securing consumer IoT** to all related stakeholders including M2M Service Providers (M2MSPs) to follow at least the first three guidelines.

The diagram represents the 5 levels of security as defined in the TEC Report on Security by Design for IoT Device Manufacturers. It proposed labeling each device with a level of security so that it becomes easy for the implementers to choose the right device for a specific use case category.

Proposal for Device Classification

Security Features	Security Requirements	Level-0	Level-1	Level-2	Level-3	Level-4
Confidentiality	Message Encryption	X	√	√	√	√
	Attack Protection	X	X	√	√	√
	Data Encryption	X	√	√	√	√
	Tamper Resistance	X	X	√	√	√
	Security Assessment Certificates	X	X	√	√	√
	Device ID Management (Physical/ Logical)	√	√	√	√	√
Integrity	Data Integrity	X	X	√	√	√
	Platform Integrity	X	X	√	√	√
	Secure Booting and Integrity Test / Self Test	X	X	X	√	√
Availability	Logging	√	√	√	√	√
	External Attack Prevention & Response	X	X	X	√	√
	Secure Monitoring	X	X	X	√	√
	Secure Firmware Update & Patch Update	X	√	√	√	√
	Software Assets Protection & Response	X	X	√	√	√
	Vulnerability Management & Response	X	√	√	√	√
	Security Policy Update & Response	X	X	X	√	√
Authentication/ Authorization	Biometrics	X	X	X	X	√
	User Authentication	X	√	√	√	√
	Data Authentication	X	X	√	√	√
	Password Management	X	√	√	√	√
	Access Control	√	√	√	√	√
	Device ID Verification	X	X	√	√	√

Security Assement and standard	Level-0	Level-1	Level-2	Level-3	Level-4
Meet Baseline Security Requirement					
Adherence to cyber security based on International Standards					
Adherence to the principles of Security by Design, and absence of known common software vulnerabilities					
Resistance against common cyber-attack and undergo for penetration testing					

Steps taken for boosting Satellite IoT

- Enhanced the scope of license(s) to enable satellite-based M2M/IoT devices.
- VSAT terminal may be used to aggregate the traffic from M2M/IoT devices as long as the CUG nature of the network in not violated.
- M2M/IoT devices, used in any architecture (including Direct-to-Satellite or in aggregator mode), shall not be treated as VSAT for the purpose of levy of license fee.
- The enablement paves way for the introduction of satellite-based IoT devices in the sectors like logistics, industrial automation, railways, agriculture, disaster management etc.
- Emphasis to be on Make-In-India for hardware and software in satellite communication system to make satellite connectivity more cost effective and facilitate holistic standardised development.

Security Aspects in Satellite-Based IoT

Every constellations poses different vulnerability-

- LEO satellites, with their low-latency and frequent handovers between satellites, are highly susceptible to spoofing attacks, unauthorized roaming and global mobility-based misuse.
- MEO systems, primarily responsible for navigation and timing, are sensitive to interference and signal disruption, potentially impacting public utilities, transport and defence networks.
- GEO satellites, with their persistent and wide-area coverage, are at risk of signal spillover, trans-border misuse and jurisdictional enforcement difficulties.

Strong security frameworks are essential to protect digital airwaves and ensure strategic control over satellite-enabled IoT services. As IoT expands across sectors, secure and compliant communication is vital for national sovereignty.

Security Aspects in Satellite-Based IoT ..contd.

- Unavailabilty of real-time geolocation enforcement and mandatory terminal location disclosure, which limits the ability to track or regulate cross-border device usage.

- Security objectives must include:
  - Enforcing geofencing policies.
  - Detecting and neutralizing unauthorized or spoofed IoT nodes.
  - Preventing signal intrusion from adjacent regions.
  - Regulating cross-border satellite connectivity in alignment with domestic laws and ITU standards.

Mandatory Testing & Certification of Telecom Equipment

- Essential Requirements (ERs) of following IoT devices/ Gateways have been prepared and being revised time to time under Mandatory Testing & Certification of Telecom Equipment (MTCTE) regime of Government of India and are available on MTCTE portal (https://www.mtcte.tec.gov.in/)-

  - IoT Gateway
  - Feedback device
  - Tracking device
  - Smart Electricity Meter
  - End Point Device for Environmental Monitoring

Non-Terrestrial Network (NTN) devices

- IoT devices will be tested as per Essential Requirements (ERs) under MTCTE having testing specifications related to EMC, Safety, communication interfaces, IP, SAR and Security. Security specifications being prepared in the form of **ITSARs (Indian Telecom Security Assurance Requirements)** by NCCS Bengaluru are also the part of ERs. ITSARs for Smart Electricity Meter, Tracking device and Feedback device have been published by NCCS but they are yet to be notified.

Working Group (WG) on 'Satellite based IoT solutions':

Terms of Reference (ToR) of the Working Group includes;

1. To study IoT based standards/ specifications/ guidelines for the Satellite based solutions and recommending potential adaptations of global standards to ensure interoperability and optimal performance.
2. To consult all the stakeholders to envisage requirements of telecom/ IoT in Satellite based solutions.
3. To study national and international best practices, benchmarks, policies being adopted for Satellite based IoT solutions.
4. To study global regulatory framework including telecom security conditions and other related aspects.
5. To study and compile diverse use cases related to Satellite based IoT solutions.
6. To study the challenges being faced in implementation of 'Satellite based IoT solutions' and proposed solutions.

Contact- ddgsd.tec@gov.in