

# *ASTAP-36*

*Session: oneM2M development and use cases/ applications in India*

**21<sup>st</sup> May 2024**

*Sushil Kumar*

Additional Director General Telecom

Department of Telecommunications

Government of India

## Five main challenges have to be overcome for IoT



**Robust connectivity:**  
Latency, availability, coverage, cost

1

**Standardization:**  
Standard connectivity for billions of things

2

3

**Interoperability and open interfaces:**  
Enabling platforms to talk with each other

5

**Domain knowledge:**  
Deep, vertical-specific insights

4

**Privacy and security:**  
Prevent malware injection and data misuse

# Introduction on ITU-T



Operational aspects	SG2	SG12	Performance, QoS and QoE
Economic and policy issues	SG3	SG13	Future networks ( & cloud)
Environment and circular economy	SG5	SG15	Transport, Access and Home
Broadband cable and TV	SG9	SG16	Multimedia
Protocols and test specifications	SG11	SG17	Security
		SG20	IoT, smart cities and communities

ITU-T



# ITU-T initiatives on IoT and Smart Cities



- **ITU-T Study Group -20:** Development & implementation of International Standards
  - ITU-T SG-20 has released a large range of standards on Devices / Sensors, Gateways, Platforms, Big data, Open data, Smart data Governance, Frontier technologies, Use cases, Key performance indicators (KPIs), city planning, stakeholder's engagement etc. and the work is in progress to develop more standards.
  - **Adopted oneM2M Release 2 Standards as ITU Standards**
- ITU-T SG-20 Focus Group (FG) AI4A : Artificial intelligence and IoT for Digital Agriculture – In progress from March 2022
- **IoT4SDGs:** Considers the importance of IoT to contribute towards achieving the Sustainable Development Goals for 2030.

# Smart Cities as super application domain of IoT

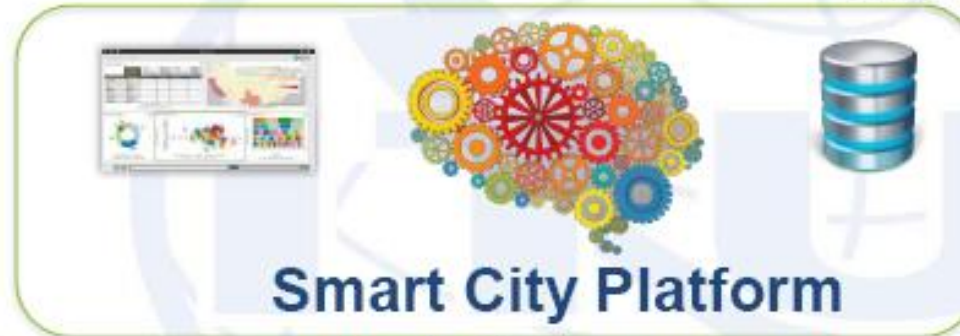


*Integration of  
multiple verticals*



*Still a number of  
technical challenges,  
incl. interoperability,  
scalability, dynamicity,  
security and privacy*

The brain of  
the city



Data collection, analysis,  
knowledge, planning,  
action

The senses of  
the city

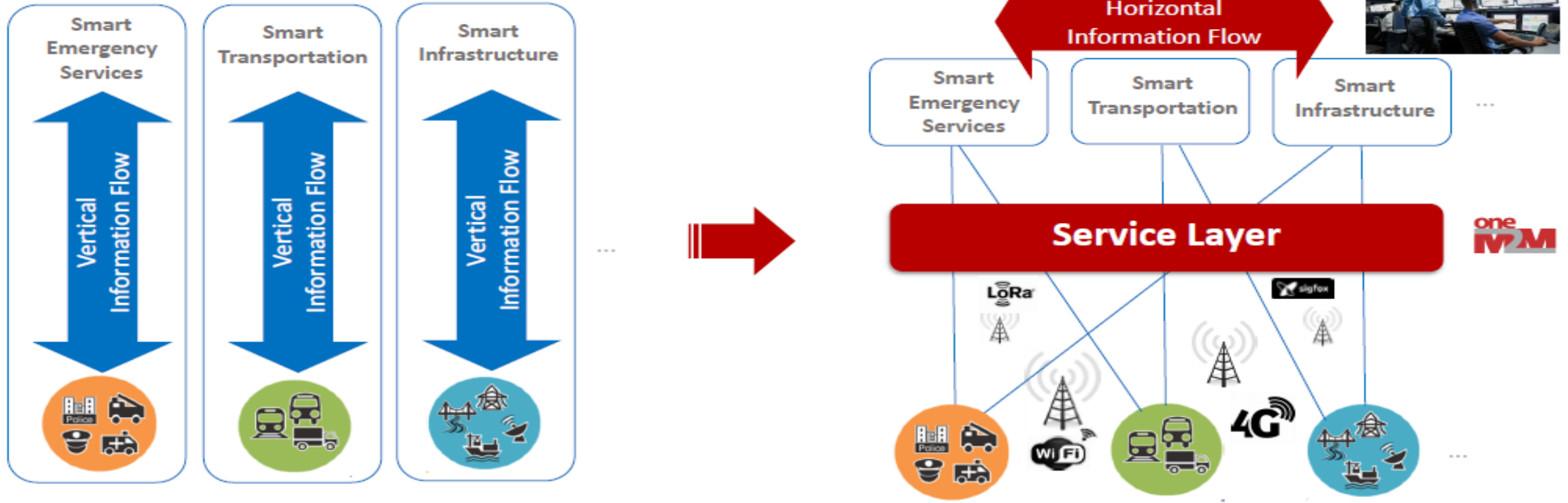


Source: Dr. Levent Gürgen



- ETSI (Europe), TTC (Japan), ARIB (Japan), ATIS(USA), TTA (USA), TTA (Korea) CCSA (China) had come together and created a partnership project oneM2M in 2012, to avoid creation of competing M2M standards. Later, TSDSI ( India) had joined as a partner member in oneM2M. They are working to **create standards for the common service layer**.
- oneM2M has released first set of specifications in Jan 2015 and its second set in March 2016, 3<sup>rd</sup> in Dec 2018.
- work is already in progress on Release 4 and Release 5.
- Specifications are backward compatible just like 3GPP.

# oneM2M Breaks Down the Silos



# Policy initiatives on M2M/ IoT & 5G in India



## 1. Important policy points released by Department of Telecom (DoT)

- **National Digital Communication Policy (NDCP)-2018** released in 2018 having salient features:
  - **Secure & Sustainable** eco-system development for massive scale of **5 billion connected devices**,
  - Simplifying licensing and regulatory framework whilst ensuring appropriate ***security framework for IoT/ M2M/ future services and network elements incorporating international best practices.***
  - ***Developing framework for accelerated deployment of M2M services while safeguarding security and interception for M2M devices.***
  - Creating a roadmap for emerging technologies and its use in the communications sector, such as **5G, Artificial Intelligence, Robotics, Internet of Things, Cloud Computing and M2M**
  - Establish a multi-stakeholder led collaborative mechanism for coordinating transition to **Industry 4.0**
  - Developing market for IoT/ M2M connectivity services in sectors including **Agriculture, Smart Cities, Intelligent Transport Networks, Multimodal Logistics, Smart Electricity Meter, Consumer Durables** etc. incorporating international best practices



# Policy initiatives on M2M/ IoT & 5G in India

- Promoting research & development in Digital Communication Technologies by creating a framework for testing and certification of new products and services
- National Telecom M2M Roadmap released in 2015.
- M2M Service provider registration policy released in Feb 2022: M2M/ IoT Service providers should register on DoT portal.
- Production Linked Incentive (PLI) scheme for Promoting Telecom & Networking Products Manufacturing in India
- Telecom Technology development fund (TTDF) launched for indigenous development of technologies.
- 100 5G Use case Labs are being provided in technical institutions for R&D, Innovations, Start Ups and MSMEs.
- Bharat 6G Alliance launched recently.

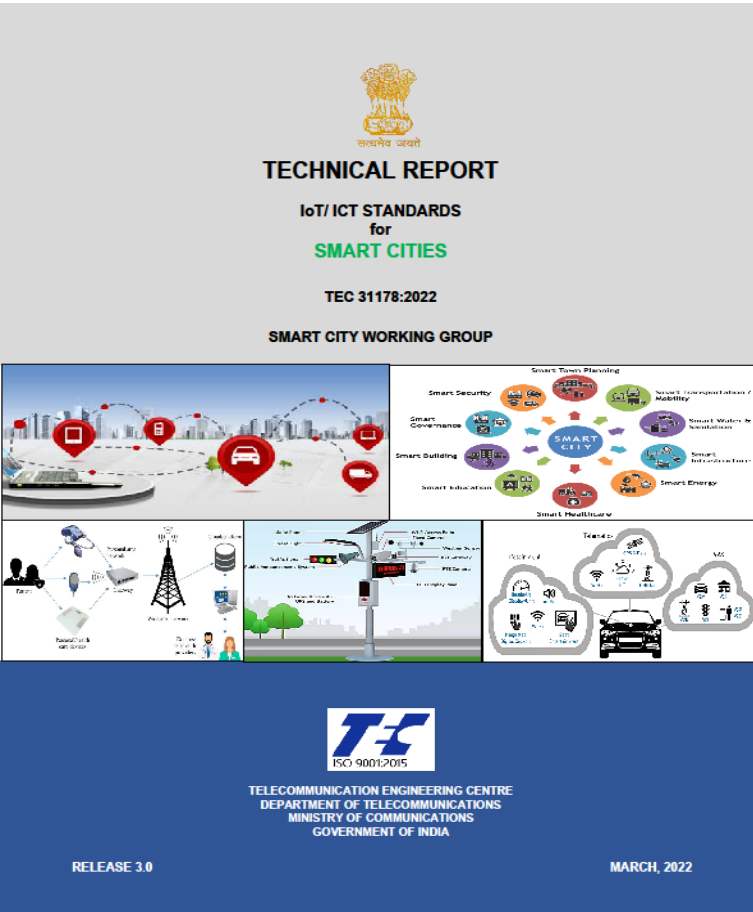
**2. Ministry of Electronics & information technology (MeitY) released the policies on semiconductor development, electronics manufacturing etc.**

- While working in TEC (2013- Oct 2023), created a frame work for developing specifications with multi stake holders and also in sync with global SDOs such as ITU, ISO/ IEC, ETSI, oneM2M, 3GPP, NIST etc.
- released twenty one technical reports in M2M/ IoT domain covering various verticals, communication technologies, EMF radiation from IoT devices and IoT Security with the outcome intended to be used in policies/ standards policies/ standards



1. M2M Enablement in **Power Sector**
2. M2M Enablement in **Intelligent Transport System**
3. M2M Enablement in **Remote Health Management**
4. M2M Enablement in **Safety & Surveillance Systems**
5. **M2M Gateway & Architecture**
6. M2M **Number resource requirement** and options
7. **V2V / V2I Radio Communication** and **Embedded SIM**
8. **Spectrum requirements for PLC** and **Low Power RF Communications**.
9. ICT Deployments and strategies for India's **Smart Cities**: A curtain raiser

# DoT/ TEC initiatives in M2M/ IoT domain



10. M2M/ IoT Enablement in **Smart Homes**
11. **Communication Technologies** in M2M / IoT domain
12. Design and Planning **Smart Cities** with IoT/ ICT
13. M2M/ IoT **Security**
14. IoT/ICT Enablement in **Smart Village & Agriculture**
15. Code of practice for **Securing Consumer IoT**
16. **Emerging Communication Technologies** and Use cases in IoT domain
17. **IoT/ ICT Standards for Smart Cities**
18. Framework of **National Trust Centre for M2M/IoT Devices and Applications**
19. **Security by design for IoT device manufacturers**
20. **EMF radiation from IoT/ M2M devices**
21. **Technologies and Standards for Intelligent Transport System,**

<https://tec.gov.in/M2M-IoT-technical-reports>

➤ **TEC Initiatives in M2M/ IoT Domain- An overview**

- **Important outcomes of these technical reports** are the part of policies/ standard. Few are as listed below:
- 13 digit numbering scheme for SIM based devices/ Gateways developed in 2016 in TEC.
  - Embedded SIM: It is based on GSMA specifications. It is in the form of IC and in solderable form factor, therefore temper proof & quite suitable for Automotive and industrial applications. It has been adopted in AIS 140/ IS 16833.
  - IPv6 or dual stack for all devices/ gateways to be connected directly to PSTN/ PLMN. It has been mandated by BIS in IS 16444 (Smart electricity meter on cellular technology)
  - **Common service layer: adopted oneM2M Release 2 and Release 3 as National standards, transposed by TSDSI.**
  - Spectrum for low power wireless communication technologies,
  - Spectrum for C-V2X : spectrum in 5.9 GHz band allocated
  - IoT Security etc.

- Adopted oneM2M Release 2 in 2018 and Release 3 in 2020 as well as 3GPP Release (10 to 16) Specifications as National Standards.
  - Bureau of Indian Standards (BIS) adopted TEC National standards (oneM2M Rel 2) as normative and informative references in its standard released as BIS IoT Reference Architecture i.e. BIS IoT RA - IS 18004 (Part 1): 2021
  - Ministry of Housing and Urban Affairs (MoHUA) India, referred the BIS IoT RA - IS 18004 (Part 1): 2021 in its RFP and issued advisory to Smart City managements responsible for the development of smart cities.
- TEC/ DoT referred U4SSC (United for sustainable smart cities) KPIs (Key performance indicators) for Smart Cities to MoHUA and NITI Aayog for further consideration and use in Smart cities.

NITI Aayog mapped the existing KPIs of MoHUA with U4SSC KPIs and proposed creation of two new categories namely **Quality of Life ICT Infrastructure** and **Service Disaster Management**.
- TEC is having IoT Experience Centre for showcasing the IoT Use cases working on various communication technologies.



# oneM2M based development in Indian Industries



- **Centre for development of Telematics (C-DOT)** developed oneM2M Rel 3 based platform named **CCSP (C-DOT common Service Platform)** and opened it for Start ups, innovators and industries for hosting their applications. Around 140 organizations were shortlisted. Out of these 30 have already tested their devices with the platform and using the platform and the work is in progress for other organizations. Applications pertaining to a number of verticals are being hosted through this platforms, namely a few

- Smart Metering
- Rural Water Supply Monitoring System
- Smart Home
- Smart Poultry solution
- Smart Street Light
- Environment Monitoring
- Surveillance - Torch based identification, Forest Surveillance
- Fire Safety and Security
- Energy Management
- Transport (V2V & V2X)
- Smart Water Management
- Smart Agriculture
- Asset Monitoring, .

# oneM2M based development in Indian Industries



- **Indian Institute for information technology (IIIT) Hyderabad** is having oneM2M Rel 2 based Smart City Living Lab. This lab is being used for connecting various IoT devices & hosting related applications related to the use cases for monitoring Air quality, Water quality, Solar energy management, Surveillance etc. for the IIIT campus.
- **Centre for development of advanced Computing (CDAC)** is having oneM2M Rel 2 based platform. Use case on Adaptive Traffic Signaling is being tested and the use cases on Air quality monitoring have been deployed. CDAC is also working for deployment of platforms in Smart cities.
- oneM2M based development are in progress in various universities and smart cities.

- Significant contributions in the following Standards of ITU-T SG-20
  1. ITU-T Y Suppl. 53 (12/2018) on IoT Use cases
  2. ITU-T Y Suppl. 56 (12/2019) on Smart City Use cases
  3. ITU-T Y. 4218 (05/2023) on IoT and ICT Requirements for deployment of Smart services in rural community.
  4. ITU-T Y Suppl. 76 (09/2023) Use cases of IoT based Smart agriculture
- Following contributions have been submitted in FG AI4A meetings and presented
  - a. *Applications of Drones, AI and IoT in Cashewnuts farming*
  - b. *IoT based Farmland Surveillance System with Disease Detection in Paddy Crops*
  - c. *Artificial Intelligence-based Disease Identification in Wheat Crops*

Use cases at (a) & (b) above are based on the projects carried out in VIT Chennai and ( C) in ICAR Delhi.

All the three use cases have been approved by the Focus group and included in its document

# M2M/ IoT – need of Cyber security



- IoT / M2M technology is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety, Surveillance, Health care, Agriculture, Smart homes, and Smart cities etc.
- World Economic Forum (WEF) in its report titled Future of Connected World released in June 2022 mentioned that
  - there was an increase in Cyber attacks by 31% in 2021 as compared to 2020.
  - IoT device attacks became double in the first half of 2022 as compared to 2021.
  - US \$ 1.85 Million average recovery cost for mid sized companies to recover from cyber attacks
- Security of the IoT domain, from devices to the applications becomes a matter of paramount importance as hacking of the devices / network being used in daily life will harm companies, organisations, nations and more importantly people

1. Technical Report ***Security by design for IoT Device Manufacturers*** released in March 2023, highlights various threats and challenges related to IoT device security; includes study of national/ international standards (by ITU, ISO/ IEC, ETSI, ENISA, IoTSF, NIST, GSMA, 3GPP etc.), best practices and guidelines (UK DCMS, CSA Singapore, WEF, STQC etc.) to mitigate these challenges. This report also provides recommendations for IoT device manufacturers and related stakeholders including policy makers, which will help in securing IoT ecosystem.

Cyber Security labeling scheme is an important outcome of this technical report.

Recommendations are being included in the security requirements being developed for testing & certification of the products.

2. The technical report on ***Framework of National Trust Centre (NTC) for M2M/ IoT Devices and Applications*** released in March 2022 visualizes the implementation of national trust centre in a phased manner for managing/ addressing the vulnerability related issues of the IoT devices reported by IoT/ Smart city platforms working in the network.

This project is being developed and expected to be implemented in near future..



# Proposed IoT devices classification for India

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						

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

### ➤ 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.



## Takeaways



- Standardisation is a collaborative efforts at national as well as global level.
- oneM2M is a global standard having interoperability and interworking with a number of standards and technologies.
- Use of interoperable standards provides economies of scale and the infrastructure developed so will be sustainable for a long time.
- Interoperability testing and Conformance testing as well as test lab eco system based on Rel 2/ 3 is required to be deployed.
- Platform / National Trust Center is expected to analyse
  - Average response time / patch release time for critical vulnerabilities by product
  - Percent/ number of products no longer receiving security updates in operation.
- Secure on boarding of IoT devices at the platform preferably using ITU-T X.509 standard for digital certificates.

Open standards and Interoperability  
are the key to  
Resilience, Sustainable and Scalable growth of  
IoT verticals / Smart infrastructure

# THANKS

For detail, pl. see the Technical Reports in M2M/ IoT domain, available on  
[www.tec.gov.in/technical-reports/](http://www.tec.gov.in/technical-reports/)

**Sushil Kumar**  
**Additional Director General Telecom,**  
**Department of Telecommunications,**

+919868131551

[Sushil.kumar20@gov.in](mailto:Sushil.kumar20@gov.in)

[sushil.k.123@gmail.com](mailto:sushil.k.123@gmail.com)

[in.linkedin.com/in/sushil-kumar-98895560](https://in.linkedin.com/in/sushil-kumar-98895560)