Azadi Ka Amrit Mahotsav

ISO 9001:2015

TSDSI workshop- oneM2M Stakeholder’s day

Session: Initiatives in IoT standardisation in India

Feb 24, 2023

Sushil Kumar
Deputy Director General
Telecommunication Engineering Center
Department of Telecommunications
Government of India

Telecommunication Engineering Centre (TEC)

ISO 9001:2015

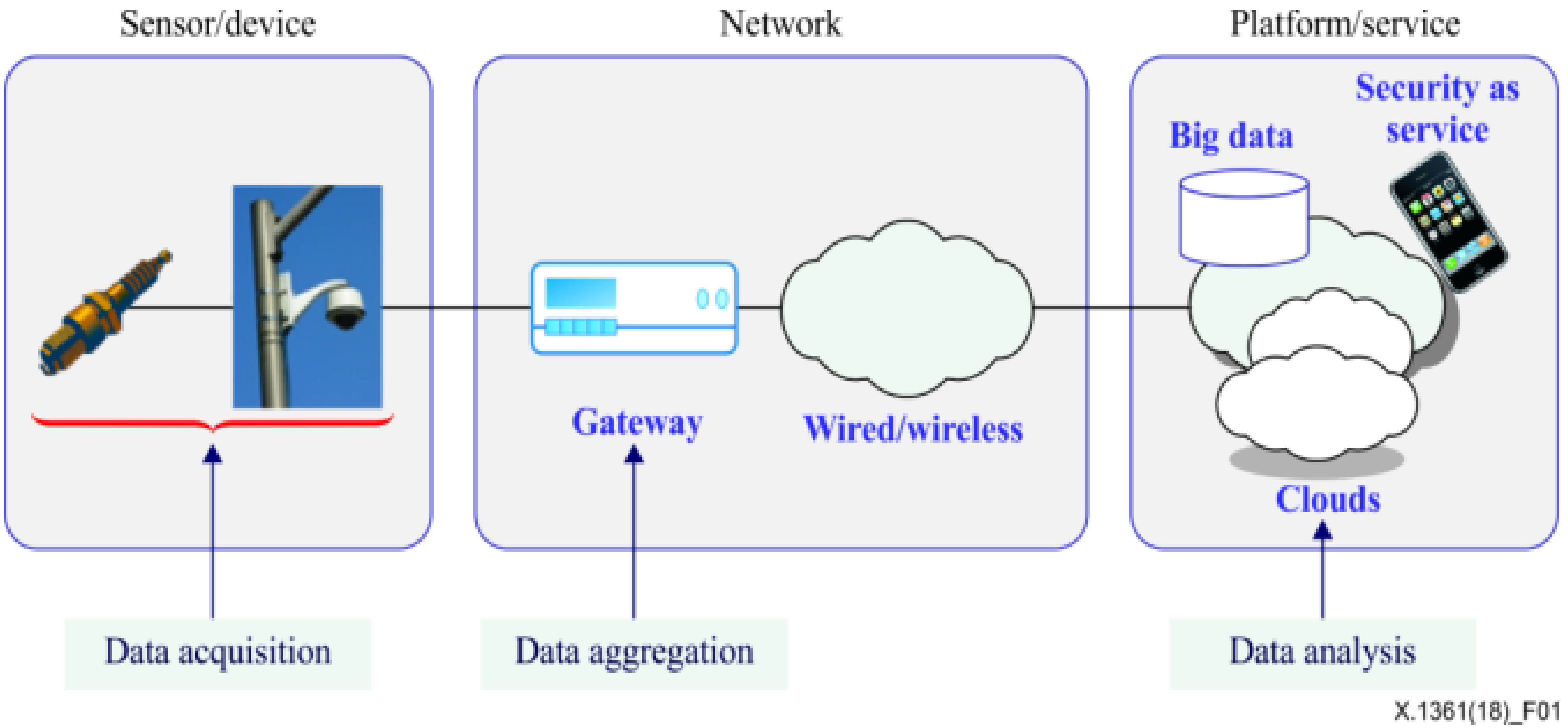
- National Standards Body (NSB) for Telecom & related ICT sector
- Designated National Enquiry point for WTO –TBT (Technical Barrier to Trade) for telecom sector.
- Mandated to coordinate with ITU-T and having National Working Groups (NWGs) in line with ITU-T Study Groups. DoT is the nodal agency for coordinating with ITU from India.
- Designated authority to implement Mandatory Testing & Certification of Telecom Equipment (MTCTE)
- Designated authority to accredit the CABs

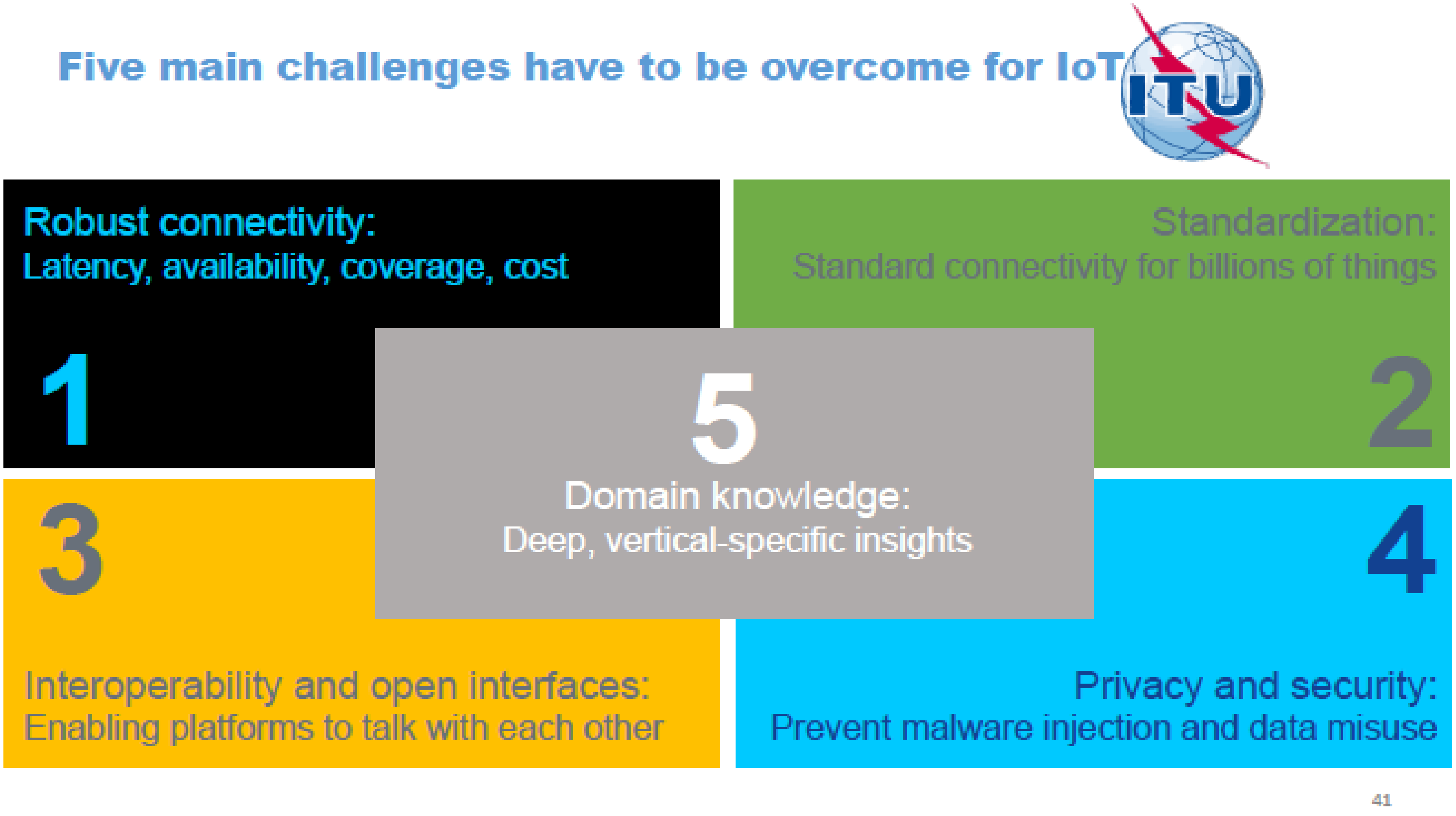
- **Related to IoT and Smart City Standardisation activities**

  Participating in Standardisation activities of ITU-T SG-20, SG-17, ITU-R WP 5D, ITU-T FG AI4A, ISO/ IEC JTC1 SC41, ETSI Security weeks, oneM2M, 3GPP, NIST etc. at international level; and

  in BIS & TSDSI at National level.

IoT functional architecture





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

4

Privacy and security:
Prevent malware injection and data misuse

5

Domain knowledge:
Deep, vertical-specific insights

IoT standardization activities and progress, ITU, Oct 2017

International organizations working on Standards

IoT interoperability and the role of Standardization

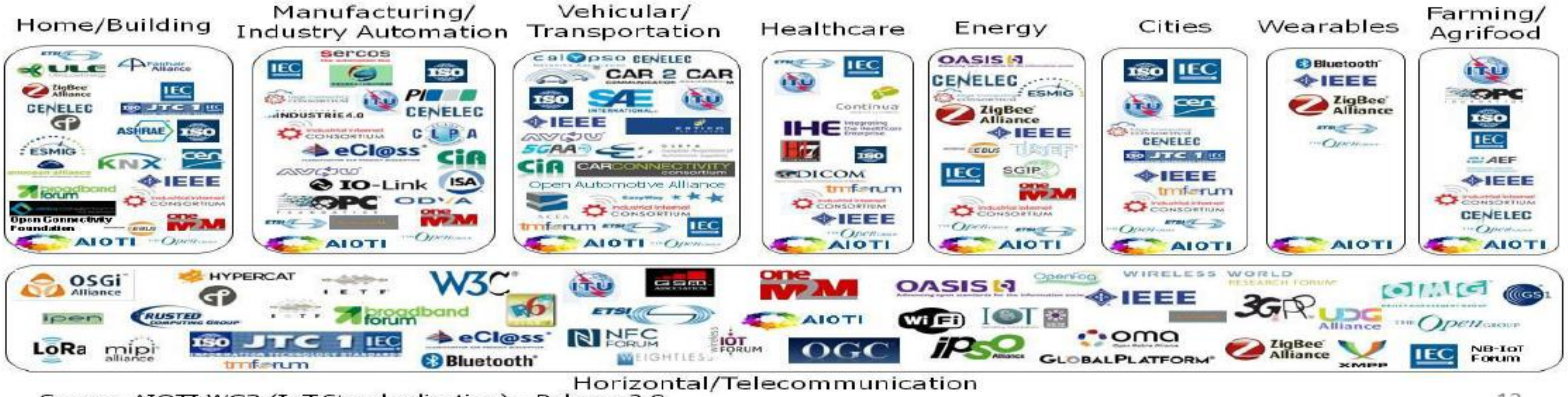
Market research: “nearly 40% of economic impact of the IoT requires interoperability between IoT systems”

IoT value will come solving interoperability issues within/across IoT domains (different interoperability dimensions)

Key issue with IoT interoperability is current diversity =>> the key role of international SDOs in standards convergence/harmonization (ITU-T as key actor)

Open innovation systems move fast =>> Standardization needs to cope - process, collaboration

IoT SDOs and Alliances Landscape (Vertical and Horizontal Domains)


Home/Building
Manufacturing/ Industry Automation
Vehicular/ Transportation
Healthcare
Energy
Cities
Wearables
Farming/ Agrifood
Horizontal/Telecommunication

Source: AIOTI WG3 (IoT Standardisation) – Release 2.8

Introduction on ITU-T

ITU-T

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

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.

ITU-T initiatives on IoT and Smart Cities

- **U4SSC**: ITU is the founding member of U4SSC (***United for Smart sustainable cities***), an initiative supported by 16 other UN partners with the aim of achieving SDG goal 11(make cities inclusive, safe, resilient and sustainable).

  - U4SSC developed key performance indicators (KPIs) **for Smart Sustainable cities based on ITU standards.**

  - More than 150 cities across the globe are evaluating their progress towards Smart Sustainable Cities objective and SDGs using these KPIs..(e.g.Dubai, Singapore, Wuxi (China), Moscow (Russia), Valencia (Spain), Pully (Switzerland) etc.)

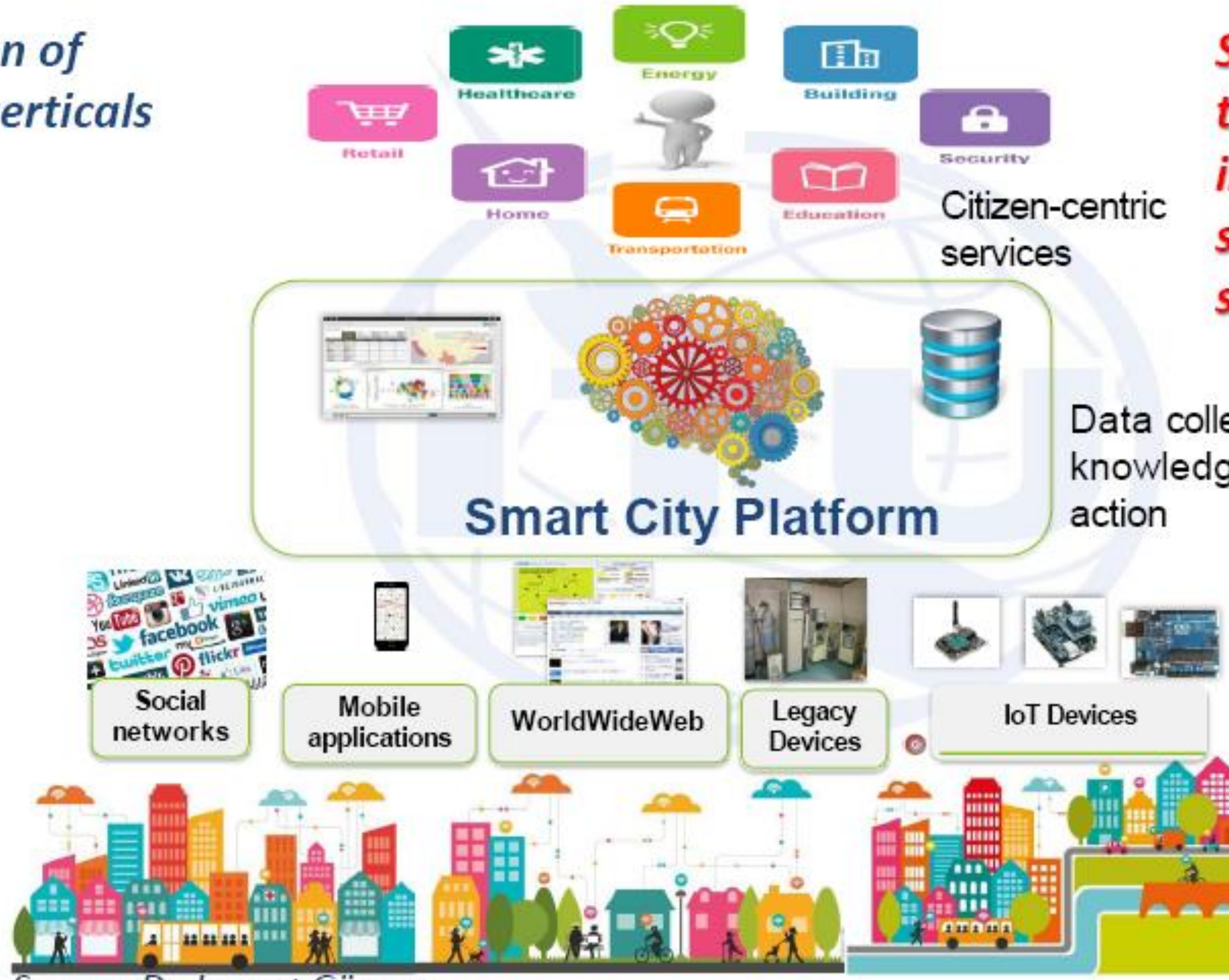
- **Joint Smart Cities taskforce:** ITU, ISO and IEC have established a Joint Task Force to coordinate international standardization for smart cities and communities to build synergies in the ongoing work.
  - This task force represents an integrated response towards achieving UN SDG11 ‘Make cities inclusive, safe, resilient and sustainable goals.

oneM2M

- ETSI (Europe), TTC (Japan), ARIB (Japan), ATIS(USA), TIA (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 also 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, 3rd in Dec 2018.
- work is already in progress on Release 4 and Release 5.
- Specifications are backward compatible just like 3GPP.

Smart Cities as super application domain of IoT

Integration of multiple verticals



Citizen-centric services

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

City data sources

Source: Dr. Levent Gürgen

DoT policy initiatives on M2M/ IoT & 5G

- **National Digital Communication Policy (NDCP)-2018** released in 2018 having salient features:
  - Secure & Sustainable eco-system is to be developed for massive scale of **5 billion connected devices by 2022.**
  - 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
- National Telecom M2M Roadmap released in 2015.
- M2M Service provider registration policy released in Feb 2022.

TEC initiatives in IoT domain

- TEC started working in M2M/ IoT domain since 2014.
- TEC formed multi-stake holders working groups to study M2M/ IoT domain, having members from academia, start up, industries, SDOs, Government etc. Through these studies, released 18 Technical Reports with the outcome intended to be used in policy/ standards.
- *Total members of all working groups taking together may be around 150.*

TECHNICAL REPORT

M2M GATEWAY & ARCHITECTURE

TEC-TR-S&D-M2M-001-01

M2M GATEWAY & ARCHITECTURE WORKING GROUP

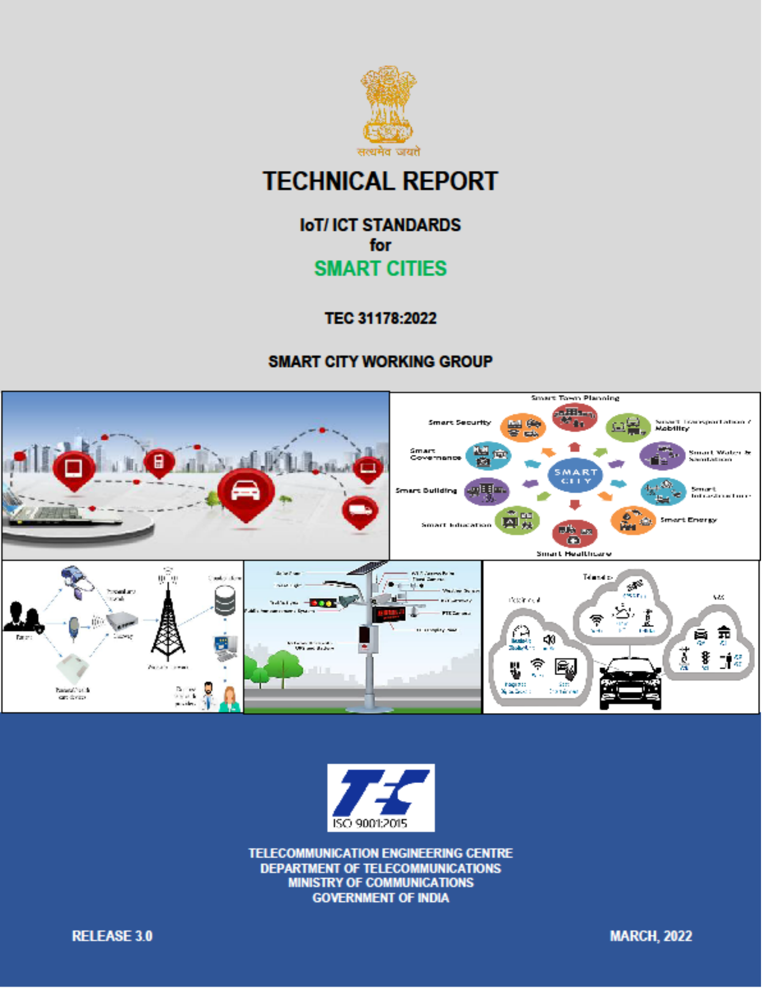
TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

RELEASE 1.0

MAY 2015

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

TEC initiatives in IoT domain



सत्यमेव जयते

TECHNICAL REPORT

IoT/ ICT STANDARDS
for
SMART CITIES

TEC 31178:2022

SMART CITY WORKING GROUP

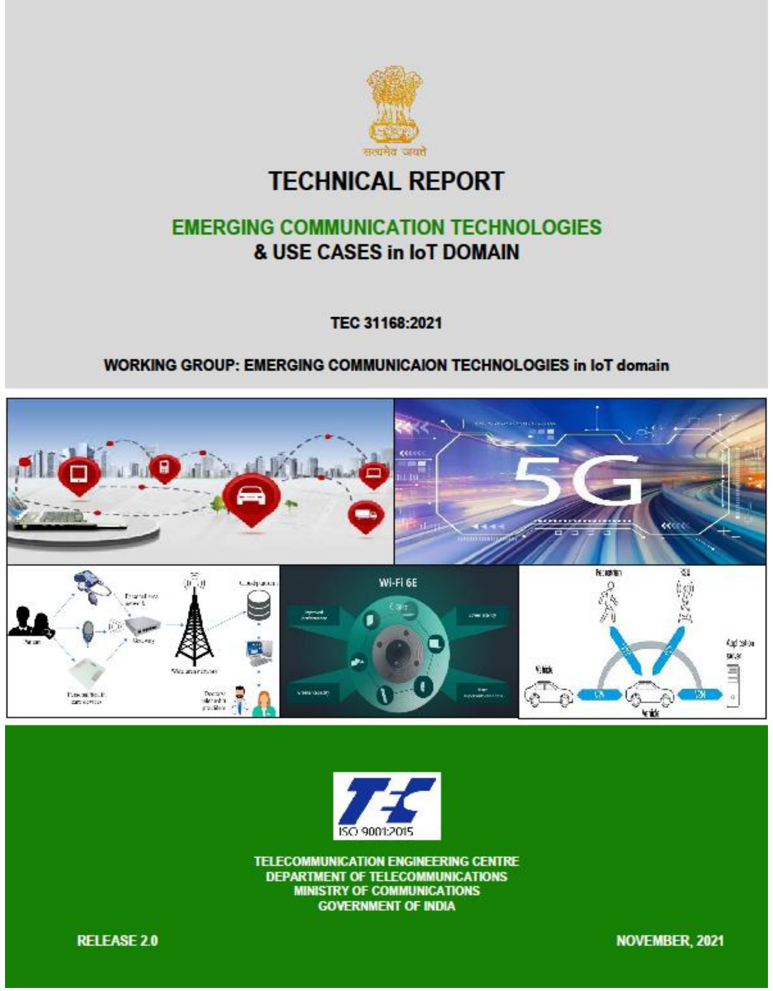
ISO 9001:2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA

RELEASE 3.0

MARCH, 2022

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**



सत्यमेव जयते

TECHNICAL REPORT

EMERGING COMMUNICATION TECHNOLOGIES
& USE CASES in IoT DOMAIN

TEC 31168:2021

WORKING GROUP: EMERGING COMMUNICAION TECHNOLOGIES in IoT domain

ISO 9001:2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA

RELEASE 2.0

NOVEMBER, 2021

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

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

TEC Initiatives in M2M/ IoT domain

ISO 9001:2015

➢ **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,
- 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 standards. It is having 14 Common service functions at present.
- Spectrum for low power wireless communication technologies,
- Spectrum for C-V2X : spectrum in 5.9 GHz band allocated
- IoT Security etc.
- …..

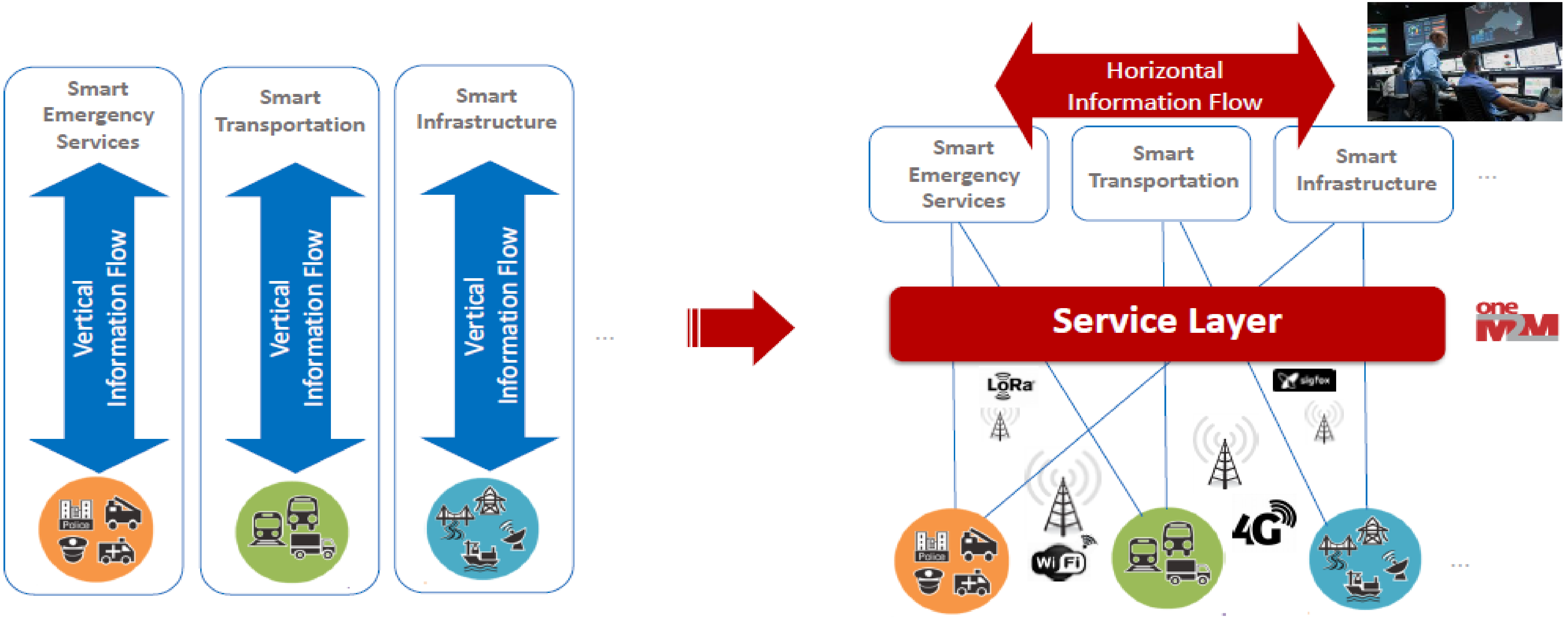
TEC Initiatives in M2M/ IoT domain

- Adopted **oneM2M Release 2 / Release 3** as well as **3GPP Release** (10 to 16) Specifications as National Standards.
- MoHUA referred the BIS IoT RA - IS 18004 (Part 1): 2021 in its RFP and issued advisory to Smart City SPVs. BIS IoT RA is having TEC National standards (oneM2M Rel 2) as normative and informative references.
- 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**.

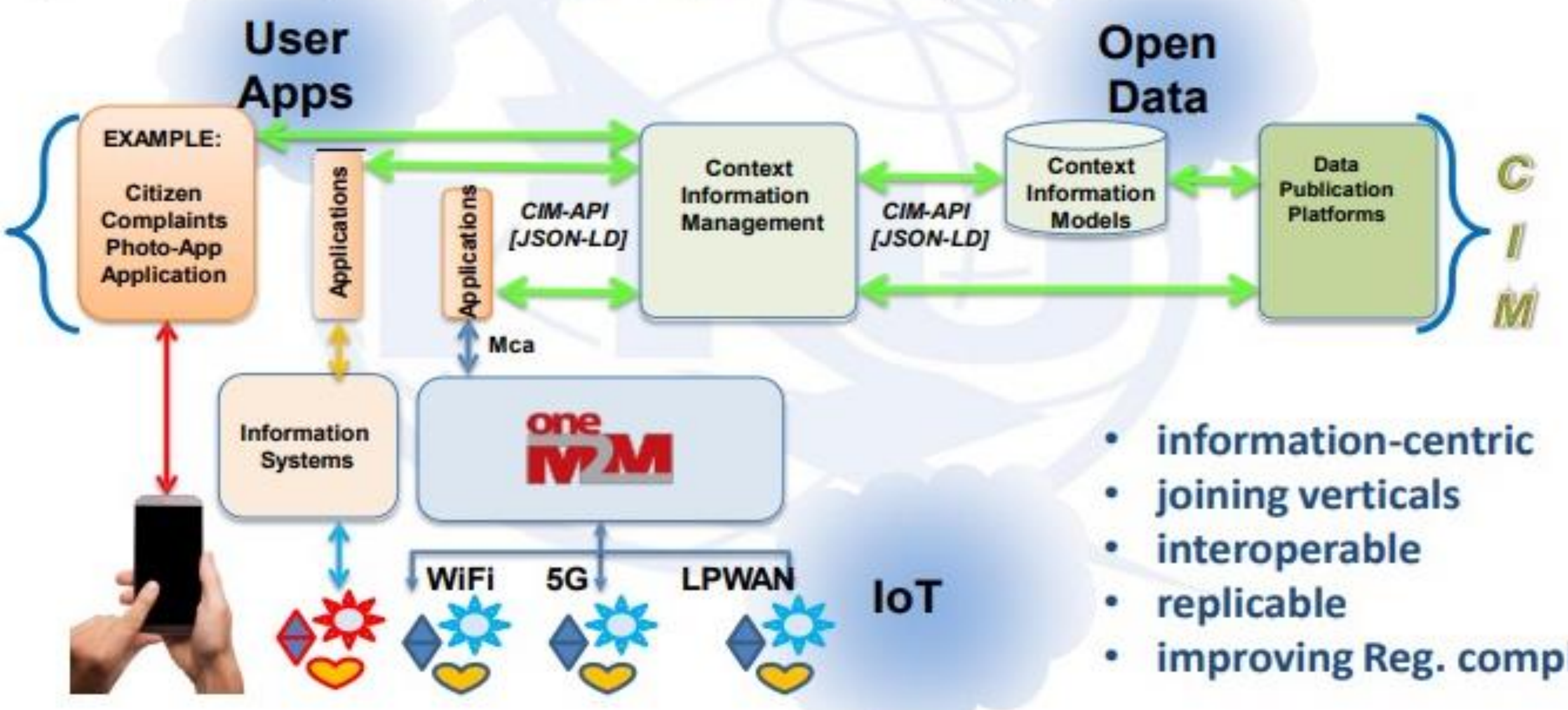
- TEC is having IoT Experience Centre for showcasing the IoT Use cases working on various communication technologies.

oneM2M Breaks Down the Silos



Context Information Management (ETSI ISG CIM)

ETSI ISG CIM has mandate to establish an info-exchange layer
on top of IoT platforms especially targeting Smart City applications



- information-centric
- joining verticals
- interoperable
- replicable
- improving Reg. compliance

Context Information Management Layer - exchanging information between domains

ITU recognition to TEC Technical Reports

- **International Telecommunication Union (ITU)** has posted the following five Technical Reports (released in 2021-22) on its website, recognising as insightful technical resource for the benefit of global community (https://www.itu.int/en/ITU-T/climatechange/resources/Pages/Frontier-technologies.aspx#internetofthings).

  1. Framework of National Trust Centre for M2M/IoT Devices and Applications
  2. IoT/ ICT Standards for Smart Cities
  3. Emerging Communication Technologies & Use Cases in IoT Domain
  4. Code of Practice for Securing Consumer Internet of Things (IoT)
  5. IoT/ ICT Enablement in Smart Village and Agriculture

Technical Reports available on https://tec.gov.in/M2M-IoT-technical-reports

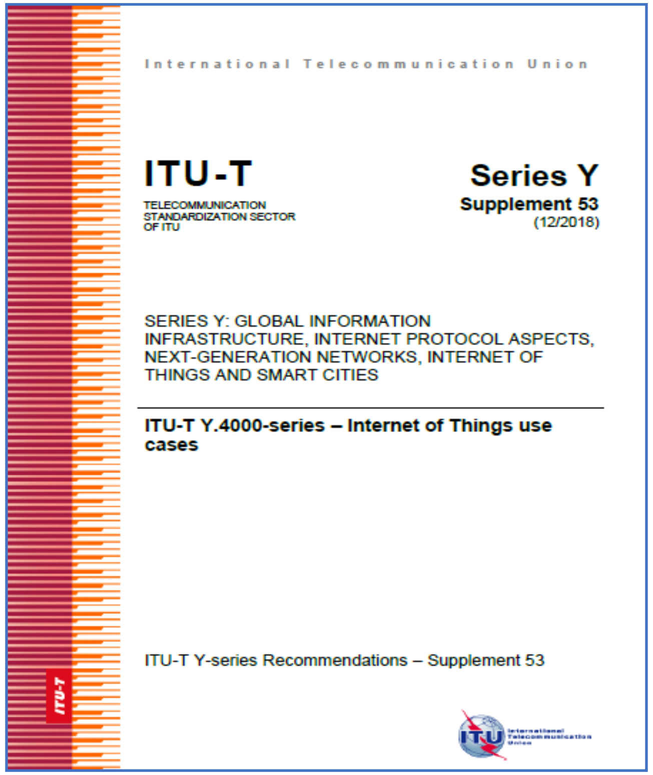
TEC Contributions in ITU-T SG-20 – approved as standard

- Besides working as an editor, significant contributions have been submitted by TEC in the following standards documents:
  - *ITU-T Recommendation Y Suppl. 53 (12/2018)* on IoT Use cases
  - *ITU-T Recommendation Y Suppl. 56 (12/2019)* on Smart City Use cases
  - *ITU-T Recommendation Y .4218 (02/2023)* on IoT and ICT Requirements for deployment of Smart services in rural community

Contributions in ITU-T SG-20 – approved as standard

- ***ITU-T Recommendation Y Suppl. 53 (12/2018) – IoT Use cases***

1. Vehicle emergency call system for automotive road safety
2. Digitization and automation of Vehicle Tracking, Safety, Conformance, Registration and Transfer via the application of e-SIM and Digital Identity
3. Remote monitoring the health of a patient
4. Connected Smart homes.
5. AMI (Advanced metering infrastructure)
6. RFID Based Digital Identification for Vehicle Tracking, Registration, and Data Transfer



International Telecommunication Union

ITU-T
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

Series Y
Supplement 53
(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

ITU-T Y.4000-series – Internet of Things use cases

ITU-T Y-series Recommendations – Supplement 53

- **first five (1 to 5) use cases submitted from India** and one (sl no. 6) from Egypt was approved in SG-20 meeting in Dec 2018.

Mandatory Testing and Certification of Telecom Equipment (MTCTE)

- Gazette notifications issued in Sept. 2017. TEC is responsible for implementing MTCTE scheme.

- Regulatory and legal compliance requirements - Devices with communication facility needs testing and certification against

  - EMC (Electro magnetic compatibility),
  - Safety,
  - Communication interfaces (wireline/ wireless, LPWAN, Low power short range)
  - Others (SAR, IPv6 etc.)
  - Security

- Testing to be done in the accredited labs in India based on minimum Essential Requirements prepared by TEC.

- In case of MRA (Mutual Recognition Arrangement) with other countries, testing may be carried out in the related country and no need of further testing in India and vice versa.

- Being implemented in phased manner wef 1st August 2019. Manufacturer is responsible to get the device model tested and certified.

For more details- https://tec.gov.in/

Some hacking incidences across the globe

1. Puerto Rico (US territory) smart meters were hacked : Cost the Puerto Rican Electric Power Authority as much as $400 million a year.

2. Foscam IP Baby-Cam hijacked : In 2013, hackers hacked a Foscam wireless IP camera that was being used as a baby monitor so he could spy on a two and half year old girl.

3. Connected car Vulnerability : In 2017-18 security researchers discovered 14 vulnerabilities in connected vehicles which could be used to remotely control a number of BMW models.

4. Mirai- DDoS : An IoT botnet was used to execute the worst DDoS attack against Internet performance management services provider Dyn back in October 2016, As a resulting several websites including CNN, Netflix, and Twitter went offline.

   After becoming infected with Mirai malware, computers continuously search the web for susceptible IoT devices before infecting them with malware by logging in using well-known default usernames and passwords.

5. Camera of a Smart TV is vulnerable. - FBI

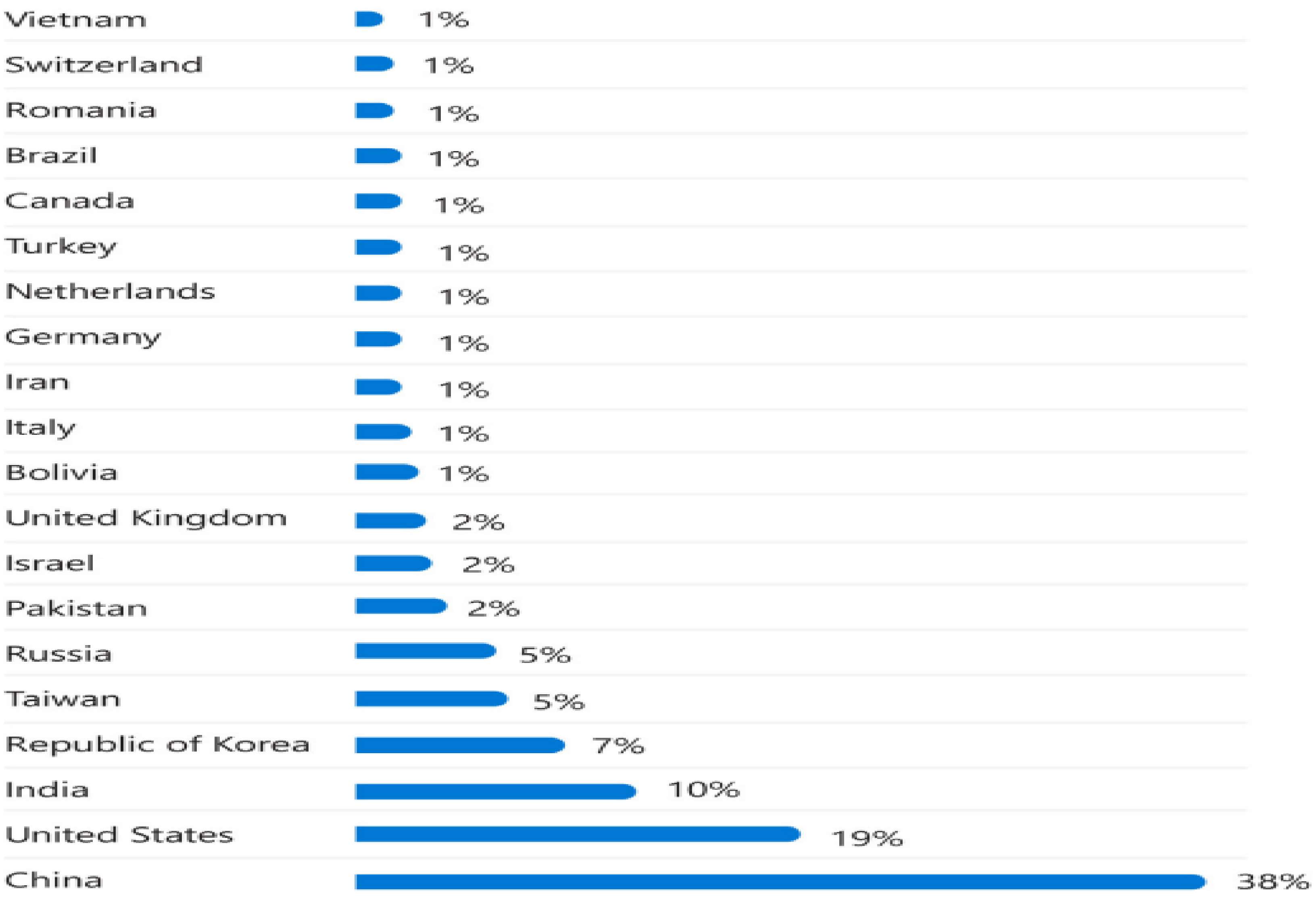
Some hacking incidences across the globe

5. Camera of a Smart TV is vulnerable. – FBI

6. Server of All India Institute of Medical Science (AIIMS), Delhi was hacked in Dec 2022 causing disruption in services and compromise of data as reported by Mint. Cause of disruption is said to be the malware infection.

7. Some computers in DoT-Controller of Communication Accounts (CCA), Vijayawada, India came under suspected ransomware attack in Jan 2023.

Top countries originating IoT malware infection during 2022



Source: Cyber signals, Dec 2022

TEC Initiatives in M2M/ IoT domain - Security

- Out of eighteen, three technical reports are related to M2M/ IoT Security:

  i. ***Framework for National Trust Center for testing of M2M Devices and Applications***, released in March 2022.

  ii. ***Code of practice for Securing Consumer IoT***, released in August 2021

  iii. ***M2M/ IoT Security***, released in 2019

  First two technical reports are the part of study of TRAI work items.

- The Department of Telecommunications (DoT) has issued the Office Memorandum(OM) in July 2022 to all the ministries of Government of India, DRDO and telecom service providers with the request for wider circulation of TEC technical report on ***Code of practice for Securing Consumer IoT*** to all related stakeholders (IoT device manufacturers, IoT service providers System integrators, Application developers etc.) for voluntary adoption of the guidelines available in this document and provide feedback.

Important works in progress in M2M/ IoT domain in TEC

- **Study is in progress**
  1. TRAI work item- *Device manufacturers should be mandated to implement "Security by design" principle in M2M devices manufacturing so that end to end encryption can be achieved*
  2. *EMF exposure from IoT devices*
  3. *Emerging technologies & standards for Intelligent Transport System.*
  4. *IoT and 5G Use cases in Agriculture*
  5. *IoT and 5G Use cases in Smart Grid*

- Development of *National Trust Center* portal *by C-DOT* based on *TEC Technical report on NTC*

Some Recommendations

1. Platform specifications should have more security features such as detecting vulnerable devices.

2. 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.

3. First three guidelines available in TEC Technical Report ***Code of practice for securing consumer IoT*** may be adopted on priority as a baseline requirements for all related stakeholders:

   (a). No universal default passwords i.e. Ban default password.

   (b). Implement a means to manage reports of vulnerabilities. (c). Keep software updated

4. Secure on boarding of IoT devices at the platform preferably using ITU-T X.509 standard for digital certificates.

Some Recommendations…

5. Vulnerabilities management should be a part of policy and mandated for IoT Device manufacturers.

6. IoT device manufacturer should test the devices against known vulnerabilities before release. To begin with critical devices and network elements such as IoT Gateway, Smart Camera, Wi-Fi routers, ONT etc. may be taken.

7. Consumer awareness regarding Vulnerabilities / security of IoT products.

8. Every consumer device should have a forced mechanism for changing the password by the user prior to its first use.

9. Life expired devices or the devices not getting updates may be highly vulnerable and threat to the network.

Open standards and Interoperability

are the key to

Resilience, Sustainable and Scalable growth of

IoT verticals / Smart infrastructure

THANKS

Sushil Kumar
Dy. Director General (IoT)
Telecommunication Engineering Center(TEC)
+919868131551
ddgsd.tec@gov.in
sushil.k.123@gmail.com