In the Framework of

SESEI | Seconded European Standardisation Expert in India

Enabling Europe-India Cooperation on Standards

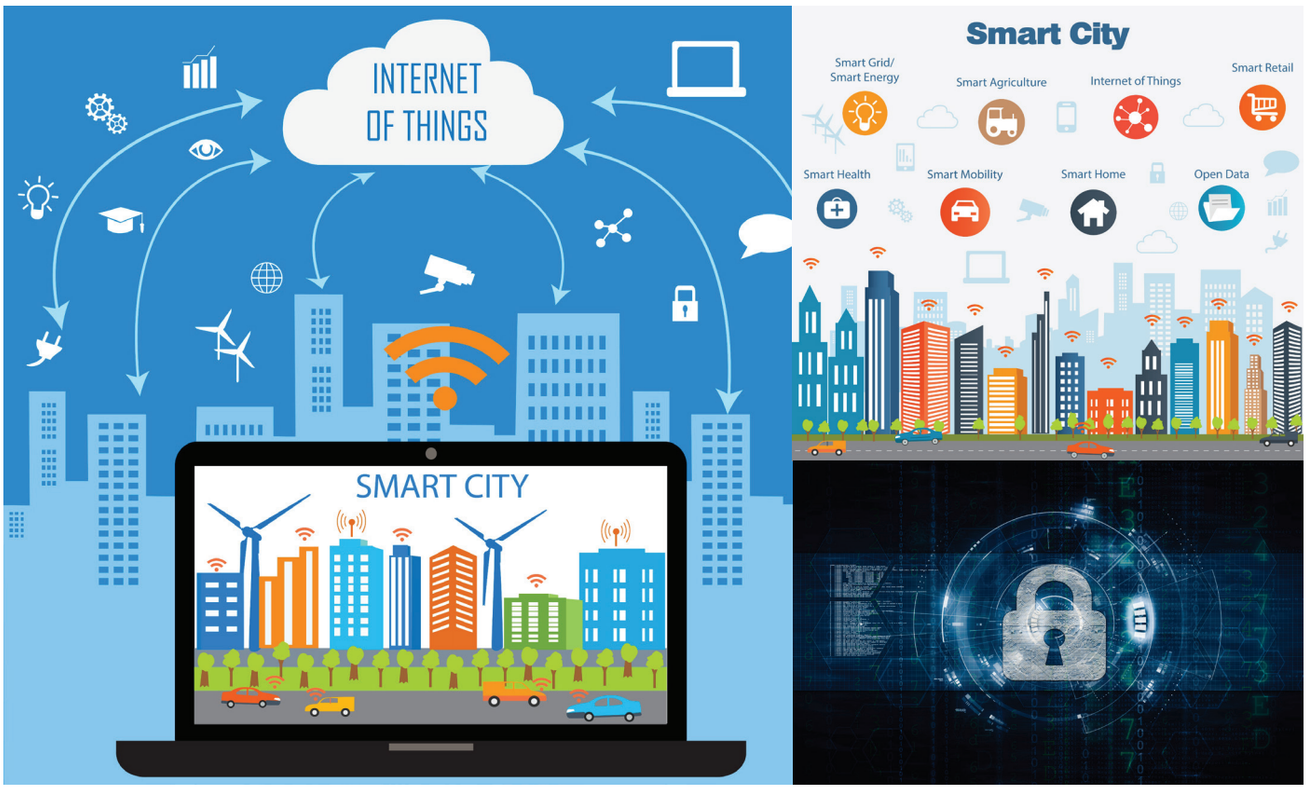
In Association With

Confederation of Indian Industry

Study Report on

Information & Communication Technology (ICT)

"M2M/IoT and its role in Smart City + Cyber Security"



CEN CENELEC ETSI European Commission EFTA

ACKNOWLEDGEMENTS

The study was undertaken under the aegis of EU Project SESEI and is prepared by CII (Confederation of Indian Industry) through research and drafting carried out by Mr. N. Kishor Narang, Mentor & Principal Design Architect, NARNIX TECHNOLABS PVT. LTD. (Lead Consultant & Technical Expert) and George Verghese (Consultant) for CII. Review and additional inputs were also provided by Mr. Dinesh Chand Sharma (SESEI Expert) and Mr Anupam Kaul, Principal & Head- QMS, CII.

TABLE OF CONTENTS

GLOSSARY OF ACRONYMS

- 2G - Second-generation Cellular Technology
- 3G - Third Generation Cellular Technology
- 5G - 5th generation wireless systems
- 6LoWPAN - IPv6 over Low-Power Wireless Personal Area Networks
- AAL - Active Assisted Living
- AMI - Advanced Metering Infrastructure
- AMRUT - Atal Mission for Rejuvenation and Urban Transformation
- BIS - Bureau of Indian Standards
- BTS - Base Transceiver Station
- CDD - Common Data Dictionary
- CDMA - Code Division Multiple Access
- CEN - European Committee for Standardization
- CENELEC - European Committee for Electrotechnical Standardization
- CMTS - Cable Modem Termination System
- CoAP - Constrained Application Protocol
- CPS - Cyber Physical systems
- CVSS - Common Vulnerability Scoring System
- DCU - Data Concentrator Unit
- DoT - Department of Telecommunication, Govt. of India
- DTH - Direct to Home TV Transmission through Satellite
- EC - European Commission
- EDDL - Electronic Device Description Language
- EFTA - European Free Trade Association
- ERNET - National Research and Education Network, India
- ETSI - European Telecommunications Standards Institute
- EU - European Union
- FTA - Free Trade Agreements
- GB - Giga Bytes
- Gbps - Giga Bits per Second
- GOI - Government of India
- GSM - Global System for Mobile communication
- ICT - Information & Communication Technology
- IIC - The Industrial Internet Consortium
- IMT - International Mobile Telecommunications
- IoE - Internet of Everything
- IoT - Internet of Things
- IP - Internet Protocol
- ISP - Internet Service Provider
- IT - Information Technology
- ITS - Intelligent Transport System
- KB - Kilo Bytes
- Kbps - Kilo Bits Per Second
- LITD - Electronics & Information Technology Division
- LPWAN - Low Power Wireless Access Network
- LTE - Long-Term Evolution
- LVDC - Low Voltage Direct Current
- M2M - Machine to Machine

- MB - Mega Byte
- Mbps - Mega Bits Per Second
- MHA - Ministry of Home Affairs, Govt. of India
- MeitY - Ministry of Electronics & Information technology, Govt. of India
- MoHUA - Ministry of Housing & Urban Affairs, Govt. of India
- MSP - M2M Service Provider
- MQTT - MQ Telemetry Transport
- MTC - Machine Type Communications
- MVNO - Mobile Virtual Network Operator
- NASSCOM - National Association of Software and Services Companies, India
- NB-IoT - Narrow Band-Internet of Things
- NFAP - National Frequency Allocation Plan
- NFV - Network Functions Virtualization
- NIST - National Institute of Standards and Technology, USA
- NSGM - National Smart Grid Mission, India
- NTC - National Trust Centre, India
- OASIS - Organization for the Advancement of Structured Information Standards
- OFC - Optical Fibre Cable
- OIC - Open Interconnect Consortium
- OWL - Ontology Web Language
- QoS - Quality of Service
- R&D - Research & Development
- RDF - Resource Description Framework
- REST - REpresentational State Transfer
- RFID - Radio-frequency Identification
- SDN - Software-Defined Network
- SDR - Software-Defined Radio
- SDO - Standards development Organization
- SESEI - Seconded European Standardization Expert in India
- SOAP - Simple Object Access Protocol.
- TBT - Technical Barriers to Trade
- TEC - Telecommunication Engineering Centre, DoT, Govt. of India
- TRAI - Telecom Regulatory Authority of India
- TSDSI - Telecommunication Standards Development Society, India
- TSP - Telecom Service Provider
- UASL - Unified Access Service Licence
- UL - Unified License
- VNO - Virtual Network Operator
- W3C - World Wide Web Consortium
- Wi-Fi - Technology for wireless local area networking with devices based on the IEEE 802.11 standards
- Wi-Max - Worldwide Interoperability for Microwave Access
- WLAN - Wireless Local Area Network
- WPC - Wireless Planning Commission
- WRC - World Radiocommunication Conferences
- WTO - World Trade Organization
- XMPP - Extensible Messaging and Presence Protocol
- ZigBee - An IEEE 802.15.4-based specification for a suite of high-level communication protocols

FOREWORD

The SESEI project (Seconded European Standardization Expert in India) is a project co-funded by five European partners (EC, EFTA, CEN, CENELEC & ETSI), operating from New Delhi, India, with the objective to increase the visibility of European standardization in India and to promote EU/EFTA-India cooperation on standards and related activities.

The SESEI's mission is to enhance the visibility of European standardization activities, increase the cooperation between Indian and European standardization bodies and support European companies facing standardization-related issues hampering market access to India

The project supports the India-Europe cooperation in standardization-related aspects. Ultimately, the SESEI project aims at contributing to the withdrawal of the Technical Barriers to Trade (TBT) both between EU/EFTA and India and globally, thus supporting European and Indian industries by facilitating international trade.

SESEI project through its expert Mr Dinesh Chand Sharma while focusing mainly on the following priority topics, it also keeps a track and extend possible support to both EU/EFTA and India on the topics of WTO-TBT and Market Access, IPR, R&D and Innovation, National Manufacturing Policy: Make in India, EU-INDIA FTAs, Environment (Energy Efficiency) etc.

- Information and communication technology: M2M/IoT, e-Accessibility, Security, 5G, NFV/SDN…
- Electrical Equipment including Consumer Electronics: Smart Grid, Smart Meter, LVDC, Micro Grids…
- Automotive: Connected Cars, e-Mobility, ITS…
- Smart Cities…

This Study Report on 'Information & Communication Technology (ICT) covering M2M/IoT and its role in Smart City + Cyber Security" was commissioned to provide an overview of the sector profile, future developments, challenges & opportunities in India, i.e. the regulatory, policy, technical and technological challenges, limiting the market potential, related opportunities, latest developments and current state of play covering standards development & policy initiatives in India to support the sectorial growth. With this study report and through further deliberation on the matter at the "3rd Indo-European Conference on Standards & Emerging Technology" scheduled for 26th April 2018 at Hotel The Lalit, New Delhi, the SESEI project aims to determine list of actions as a way forward which shall further enable project SESEI and its stakeholders in India and in Europe in achieving its objectives. This will ultimately strengthen the cooperation and collaboration between EU/EFTA and India help in contributing to reduce Technical Barriers to Trade (TBT) and facilitating trade.

EXECUTIVE SUMMARY

"M2M" (Machine to Machine) because of its pervasive nature is now very aptly known by the name "IoT" (Internet of Things). A concept that was once perceived as science fiction is now a reality, and one that is bound to become even more ubiquitous. Promising to be the most disruptive technology since the World Wide Web, the Internet of Things is predicted to result in up to 100 billion Internet-connected objects by 2020. Relying on embedded computing and sensors, and driven by smartphone and tablet adoption, IoT shall witness an explosion of new uses by consumers and enterprises alike. It is believed that the Internet of Things, or the ability for consumer devices and appliances to communicate with one another through telecommunication networks and a complex system of embedded sensors, will enable a wide range of new applications and services while raising many new challenges, not least of which is security.

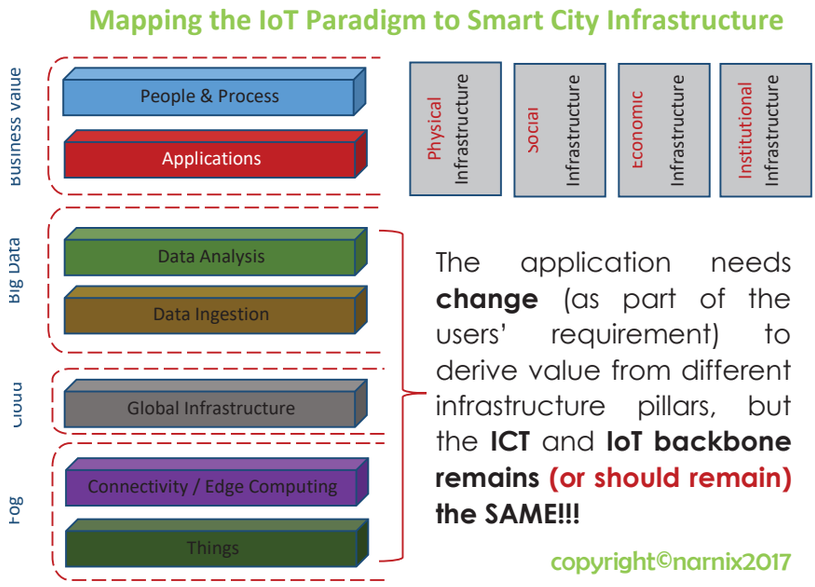
M2M essentially was, and, in the industrial parlance is, still 'application specific' 'Machine to Machine' communication with 'very definite functionality and expectations' with 'controlled mode' of communication; while IoT could be termed as its next generation, yet it is going to see a whole set of new generations in next few years and decades, because IoT is about the 'Connected Intelligence', a sort of 'universal global neural network' in the cloud. The developments in the last few decades in the pervasive embedded processing and revolutions in communication and sensors technologies have catapulted the homogenous M2M networks into heterogeneous global neural networks of 'aware' and interconnected devices with unique IDs, interacting with other machines/objects, infrastructure, and the physical environment. The IoT comprises of smart machines interacting and communicating with other machines, objects, environments and infrastructures.

As a result, huge volumes of data are being generated, and that data is being processed into useful actions that can "command and control" things to make our lives much easier and safer—and to reduce our impact on the environment. The potential and opportunities of this new era are boundless, with amazing potential to improve our lives as long as the disruption level is kept under control. However, care needs to be taken about protecting privacy of users and confidentiality of the immense amount of data being collected and processed.

Developing as well as developed countries have announced huge investments in terms of billions and trillions of Euros for M2M based services. At present more than 450 mobile operators are offering M2M services across about 200 countries. ITU estimates the market for IoT devices will result in over USD 1.7 trillion in value added to the global economy by 2019.

The enabling technologies for Internet of Things are sensor networks, RFID, M2M, mobile Internet, wired & wireless communication networks, semantic data integration, semantic search etc. In wireless communication Wi-Fi, ZigBee, 6LoWPAN, Bluetooth technologies may be used for short-range connectivity among device(s) to the gateway. Further GSM 2G, 3G, LTE, Wi-Max and NB-IoT or even Fibre may be used depending on the deployment for connecting M2M gateway to the desired server.

Various programs launched by the Indian government, such as "Smart Cities", "Digital India", "Make in India", "AMRUT" and "Startup India" are the key drivers of the growth of the M2M/IoT industry in the country. Further many huge projects undertaken by the Indian government will help in the effective and sustainable utilization of resources by the application of M2M/IoT technology.



Mapping the IoT paradigm to smart city infrastructure

Beyond leveraging M2M/IoT & ICT in the digitization of institutional, economic, social & governance infrastructures of a city, a glimpse into the physical infrastructure brings out a few staggering numbers on the business aspect of this disruptive paradigm.

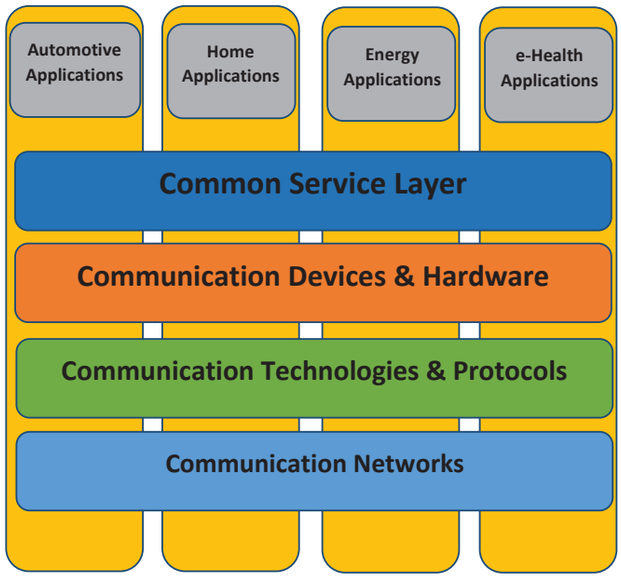
India is going to need a minimum of 4 - 5 billion communication modules to be integrated into the Smart Sensors and Controllers and 10– 50 million gateways that shall be needed to operate and maintain the Nation Wide Critical Infrastructure. And these numbers do not even account for the ever-growing enterprise and consumer applications of M2M/IoT paradigm.

However, because of heterogeneous ecosystem, and lack of interoperability and harmonization, the ecosystem is likely to stay fragmented in near future.

Internet of Things is all about "heterogeneous" and "aware" devices interacting to simplify people's life in some way or the other. Hence, the heterogeneity of the IoT paradigm has made it imperative to have a fresh look at the prevalent architectures & frameworks of the M2M/IoT and/or ICT infrastructures being deployed or being developed.

The IoT value chain is perhaps the most diverse and complicated value chain of any industry that exists in the world. In fact, the gold rush to IoT is so pervasive that if you combine much of the value chain of most industry trade associations, standards bodies, the ecosystem partners of trade associations and standards bodies, and then add in the different technology providers feeding those industries, you get close to understanding the scope of the task. In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major need but also a major challenge.

Bringing the "Internet of Things" to life requires a comprehensive systems approach - inclusive of intelligent processing and sensing technology, connectivity, software and services, along with a leading ecosystem of



Platform based Integration based on open standards

partners. Harmonization in the communication & application protocols, messaging middleware, cloud, big data & data analytics, artificial intelligence shall bring some semblance in this diverse ecosystem.

Platform based integration based on open standards is the key to bringing homogeneity in such scenarios. In the heterogeneous world of M2M/IoT, common service layer brings interoperability by creating a distributed software layer – like operating system- which facilitates the unification by providing a framework for interworking with different technologies to enable re-use of what is already available as much as possible.

The pervasive nature of the M2M/IoT paradigm combined with astounding business potential has brought all the stakeholders on common platforms to address the challenges being faced by the stakeholders, as well as, bridge the gaps in system standards. Extensive collaborative efforts are being undertaken in true earnest to develop standardized frameworks, architectures, platforms, middleware, data models, data exchange formats and APIs etc.

Framework for Interoperability – The variegated nature of IoT environments is reflected in the different types of IoT devices as IoT covers a multitude of industries and deployment scenarios. To create systems that can help ensure that our digital future doesn't become a chaotic dystopia populated with out-of-control objects commanded remotely by "threat actors"—a world in which identities are routinely compromised and stolen? It is imperative to develop/adopt standardized frameworks and architectures to bring comprehensive inter-operability in this heterogeneous, diverse and fragmented ecosystem to enable the users to have wide choice of products for any given requirement without getting concerned about the seamless data/information exchange & interworking diverse products for any given application. It shall also ensure that manufacturers can benefit from the economies of scale that a wider market brings. Interoperability is therefore a crucial factor in the success of modern technologies, and it is market demand that has ensured that interoperability holds a prominent position in standardization.

Comprehensive standardization, harmonization and well defined architectures and interfaces shall go a long

way in bringing the much desired and awaited proliferation and mass acceptance followed by adoption of the IoT paradigm in the society, business and industry.

Security and Privacy - The Internet is an indispensable asset for businesses and consumers to participate in the global sharing economy. Cybersecurity, data security and denial of service protection must be a primary concern as the internet evolves into an industrial internet. And, the IoT is an increasingly attractive attack plane for cybercriminals. Getting security right in the age of the IoT could mean the difference between chaos and order, not just in cyberspace but in the physical world, as well. A successful IoT security requires a multilayered approach. In face of the increased vulnerabilities due to the large Attack Surface Area in the M2M/IoT paradigm it's imperative to move from the "EXTRINSIC SECURITY" (Add on Security) paradigm to an "INTRINSIC SECURITY" (Security by Design) paradigm. The only way is to design new systems based on secure software and architectures.

IoT devices provide significant benefits to individual consumers across different aspects of their lives. Data and especially personal data, underpins and delivers most of these benefits. Consequently, the interaction of IoT devices with individuals would pose ongoing and real time challenges to the privacy of an individual, as they impact lifestyles on a daily basis and permeate into the day to day privacy of the individual. Such interaction with the daily privacy of individuals can lead to potential risks affecting the daily life of people. Hence, it is pertinent to address the challenges created by IoT in the privacy of an individual and confidentiality of the data.

National & Global Coordination & Collaboration - To keep pace with the global developments in technology & standards Indian stakeholders must leverage the initiatives, best practices & work done in global & regional SDOs and collaborate closely to speed up the adoption and implementation of required standards and best practices. However, these shall need to be backed by a national policy on using standards and national coordination to avoid state-specific approaches, or even city-specific approaches in the case of smart cities.

Indian stakeholders should leverage the initiatives by EU: "India-Europe Cooperation on ICT-Related Standardization, Policy and Legislation" and the "Project SESEI" to co-operate and collaborate on areas of mutual interests like M2M/IoT, Security, 5G, NFV/SDN. Also, constitute high level co-ordination groups on important focus areas to harmonize and share the Standardization and other relevant activities in individual national SDO or industry bodies.

BACKGROUND

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

Digitization has accelerated the growth of telecommunications industry and has transformed the fundamentals of conventional network and business architecture with help of technological advancements like big data intelligence, Internet of Everything, Machine-to-Machine Communication.

Nowadays, the Internet of Things (IoT) is widely deployed in several fields including industry, transportation, energy, home & environment monitoring, and healthcare & wellbeing applications. IoT provides an added value service allowing users to easily supervise their environments and helping them make suitable decisions. IoT is likely to improve the quality of people's lives, create new markets and new opportunities, increase economic growth, and be a momentum for competition. The Internet of Things (IoT)/M2M represents a developing field with its own concepts that include sensors, communications in local-area and wide-area, server on premises, local scanning devices, user-facing services, and storage and analytics. Additionally, the technology has leveraged the mobile environment to further improve human and machine communication, including in monitoring systems that collect data and drive decisions. M2M/IoT is also having an impact on the telecommunication industry, helping change how the networks and infrastructure is designed and enable seamless interactions with multitudes of devices.

The IoT ecosystem is heavily dependent on data collection and transmission. Connected sensors collect large amount of data through the Internet, enabling M2M interaction and processing of the data for particular services. Different types of data are transmitted and processed within the IoT ecosystem. The data primarily includes personal data and sensitive personal information such as financial information, location, health related information, etc.

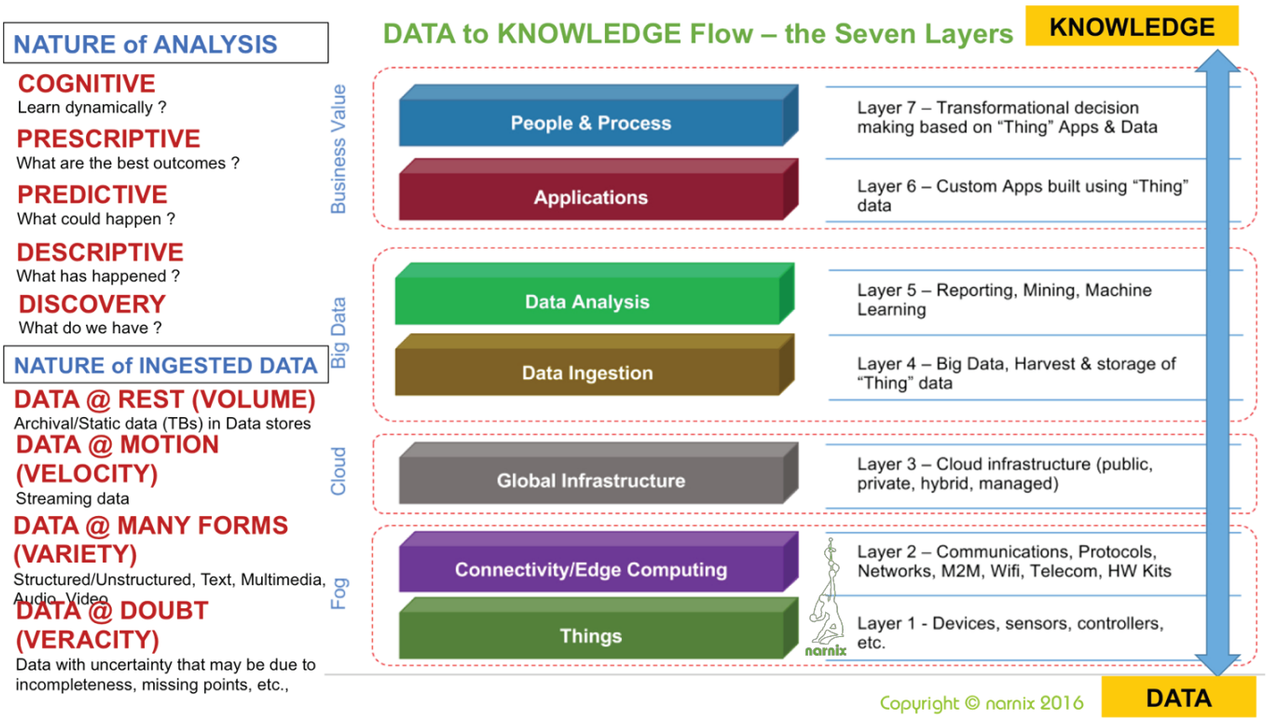
With IoT – sensors, cameras, huge volume of data gathering, analytics, dynamic systems and automation, we are constantly redefining how the cyber world meets and influences the physical world and this is now touching the core of our cities' infrastructure also. We are at the crux of a cyber-physical metamorphosis of cities and the infrastructure that enable any city to breathe. Its blending or merging with advances in computing/ communicating/electronics and how we leverage it will truly define the way we, as a nation, transform our infrastructures at every level.

The new thought processes have combined all the key four elements i.e. People, Infrastructure, Processes and Data to create an end-to-end digital ecosystem supported by reliable and sustainable ICT infrastructure.

M2M/IoT Eco-System, Market Dynamics & Potential

M2M/IoT paradigm is quite diverse, heterogeneous & fragmented. Some define it as a vague and generalized glossy scenario of smart buildings, smart city, smart lighting, smart grid, smart health and industrial automation systems and solutions. Some others define IoT as telemetry-like services over cellular network. Another group defines at as a 'One Box Solution' for each home.

However, simply put IoT Systems essentially comprise of: sensing nodes, local embedded processing nodes, connectivity nodes, software to automate tasks and enable new "classes of services" remote embedded processing nodes, and last but not the least 'Full Security' across the 'Signal Path'. It needs a unique yet all-encompassing understanding of the technological aspects of designing any and all kinds of IoT devices, products, systems, solutions, software stacks, platforms and even frameworks for diverse use cases, be it consumer, industrial, enterprise or even critical and/or smart infrastructure. And, their use cases include: Machine-to-Machine communication, Machine-to-infrastructure communication, Machine to environment communications, Tele-health (remote or real-time pervasive monitoring of patients, diagnosis and drug delivery), continuous monitoring of, and firmware upgrades for, vehicles, Asset tracking of goods on the move, Automatic traffic management, Remote security and control, Environmental monitoring and control, Home and industrial building automation, "Smart" applications, including cities, water, agriculture, buildings, grid, meters, broadband, cars, appliances, tags, animal farming and the environment, to name a few...



The IoT Paradigm - Seven Layers of Information Flow – from Data to Knowledge

Huge volumes of data are being generated, and that data is being processed into useful actions that can "command and control" things to make our lives much easier and safer—and to reduce our impact on the environment.

With the all-pervasive and all-encompassing nature of the computing and communication technologies today, they have invaded every aspect of our life and each strata of the society: be it the consumers, the commerce, the industry, the governments or even the infrastructure. It seems like a paradox, but it will soon become reality: The rate at which computers disappear will be matched by the rate at which information technology will increasingly permeate our environment and determine our lives. This clearly demonstrates that computers have become very significant in our lives and will influence a wide range of physical and social activities of our lives. However, bringing the "Internet of Things" to life requires a comprehensive systems approach, inclusive of intelligent processing and sensing technology, connectivity, software and services, along with a leading ecosystem of partners. Yet many technological hurdles must be passed before this vision becomes a reality. New types of sensors, new ways of connecting devices, and new strategies for embedded computing must be rolled out to bring IoT's vision to the forefront.

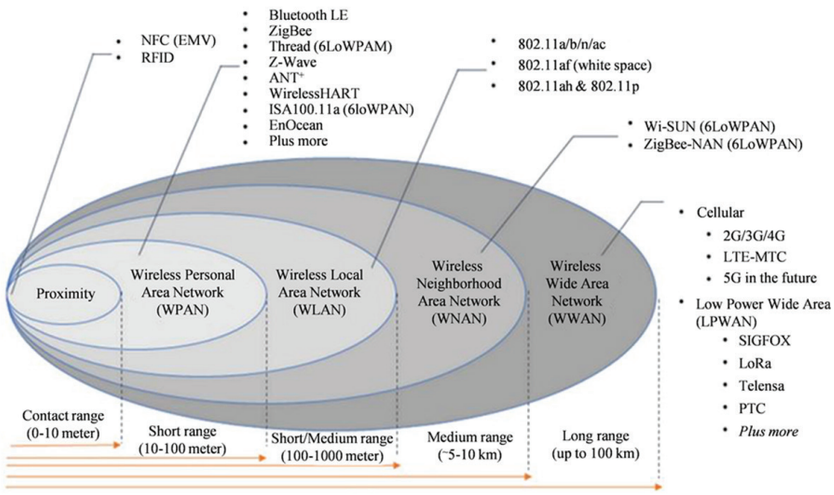
All kinds of M2M services can be efficiently and economically made available to consumers if they are configured on common communication network, which is open, scalable and standards based. However different kinds of M2M services have varying network requirements broadly categorized as under:

- Very low Bandwidth < 1Kbps (Monthly usage 10KB to 1MB) e.g. Remote sensors
- Low Bandwidth < 1Kbps to 10Kbps (Monthly usage 1MB to 10MB) e.g. utility, health security monitoring
- Medium Bandwidth < 50Kbps to 1Mbps (Monthly usage 10MB to 300MB) e.g. retail, ticketing, inventory control, gaming, digital picture frames.
- High Bandwidth, in Mbps (monthly usage from 300MB to 90GB) e.g. digital signage, video surveillance.

Connectivity & M2M/IoT:

Connectivity is the key to any digitization approach. It is the enabler for IoT, cloud and data analytics as it provides the connection between the things and the control, operations, analytics and business applications. While connectivity is one of its major components, IoT is much more about providing the services and semantic extensions to enrich data to valuable information that can be interpreted and understood by all applications and allow them to build up own knowledge. The IoT sub section focuses on these parts of IoT beyond connectivity.

Various communication technologies will be used to connect the machines, sensors, actors, basically any kind of device with each other and with the applications locally, remote or in the cloud. Based on the specific requirements of the various application areas concerning for example bandwidth, reach, quality of service,



latency and available resources different protocols will be used at the different layers of the communication stacks developed for the multitude of communication technologies and network architectures.

The wide variety of communication technologies, protocols and standards developed in last few decades, be it wired or wireless, address all kind of use cases in communication requirements with appropriate architectures and network topologies required for M2M/IoT applications. In wireless communication Wi-Fi, ZigBee, 6LoWPAN, Bluetooth technologies may be used for short-range connectivity among device(s) to the gateway; while GSM 2G, 3G, LTE and Wi-Max or even Fibre may be used depending on the deployment for connecting the M2M/IoT gateway to the desired server.

IPv6 will be the common denominator at the network layer; still some other network layer protocols might be used in limited scale for example for constraint devices and networks. IPv6 standardization is already mature, but the adoption by the market is slow. Nevertheless, application area specific communication standards have to be IPv6 ready and especially existing standards have to be checked and extended as needed to be IPv6 compliant. New approaches to network routing like Software Defined Networking (SDN) have to be taken into account to provide the necessary quality of service for our applications. Wireless technologies will play an ever-growing role in order to connect the increasing amount of things in the industrial environment.

Within the IoT paradigm, we have multiple categories of stakeholders – Consumers, Enterprise, Industrial, Infrastructure. Each category's constraints and requirements are quite diverse and different from others, which make the IoT paradigm one of the most complex and heterogeneous.

In general, we have the trend to use commercially wide available, off the shelf technologies like Ethernet and Wireless LAN also for industrial applications. In the latter context, care shall be taken to ensure that the specific requirements of the industrial applications concerning for example latency and availability are supported.
Especially the role and needs of wireless communication technologies in the industrial environment and related standardization activities have to be further elaborated. This includes especially the use of LTE and future 5G mobile networks and of Software Defined Radio (SDR) as a technology to increase the flexibility of radio equipment.

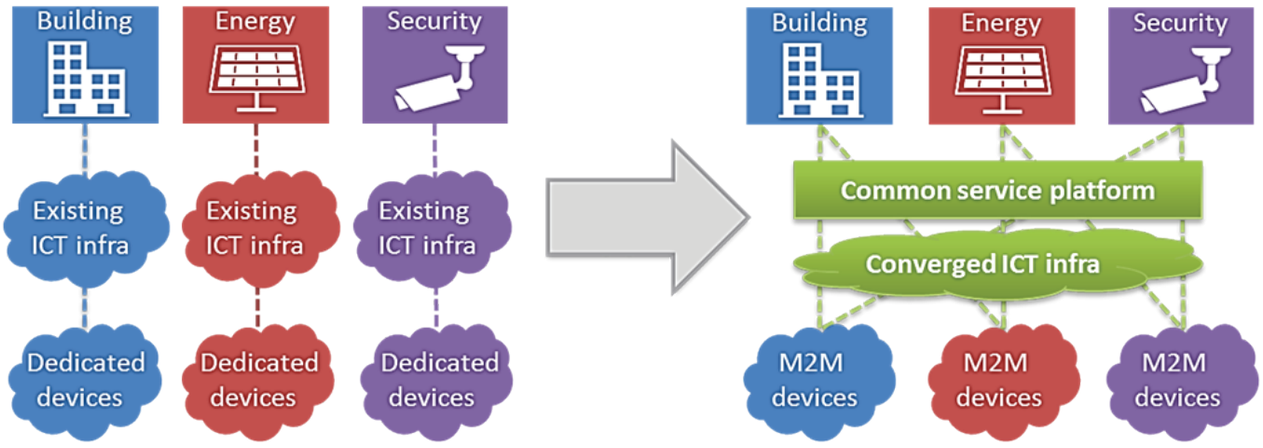
M2M/IoT & Roll Out of 5G Networks

With a promise of 10Gbps speed, less than 1ms latency and 90% reduction in network energy utilization, 5G will spur the next round of telecom infrastructure investments across the globe. The sharp hike in consumer data and the proliferation of IoT devices will fuel the growth of 5G.

A key requirement for 5G-network roll out is availability of a strong reliable backhaul, which is non-existent in India at present. As 5G networks will have to support Bursty data from emerging applications like IoT, smart cities, requirement of a strong and reliable backhaul (from cell tower to network operators Point of Presence) becomes a critical concern. Further to support 5G requirement for latency reduction (from 50ms to 1ms) and speed from 100 Mbps to 10Gbps, the fibre deployment in India needs to be increased from current market of 16-18 million fibre km per year to at least 2-3x per year. 5G will also require a multi-fold increase in small cells deployment, with each small cell having backhaul on fibre. The percentage of tower backhaul on fibre for the operators will need to increase significantly from 20% to 70-80% levels.

Common Service Layer

In the heterogeneous world of M2M/IoT, Common Service Layer brings interoperability by creating a distributed software layer – like operating system- which facilitates the unification by providing a framework for interworking with different technologies to enable re-use of what is already available as much as possible.



M2M Evolution: oneM2M Architecture Approach

Application Protocols and Messaging Middleware

Application protocols and messaging middleware are responsible for the information exchange above the transport layer. Several protocols like SOAP, REST and XMPP already exist. They were developed for specific Internet applications (e.g. XMPP for chat message exchange) but are now used also in various industrial application areas. Specifically, for communication with constrained devices and in constrained networks new protocols like COAP and MQTT have been developed. It has to be ensured that the protocols can cope with the requirements of the different industrial application areas like scalability, processing efficiency, high reliability and low latency.

Cloud

Cloud processing (e.g. computing, storage) allows flexible use of centralized computational resources. For industrial applications cloud solutions like software or platform as a service will play an important role for example for preventive maintenance based on data analytics, enterprise management, product development and engineering tasks. Still for the production process local processing will be more suitable to support for example timing and safety critical functions. Security issues have to be taken into account, not only in case the cloud is located remotely and at 3rd parties. Recently edge or fog clouds have been introduced which are located at the borders between the access and backbone networks. They move the computational resources closer to the machines/things in an attempt to overcome some of the issues with clouds in the backbone like increased latency.

Big Data & Analytics

Data analytics, smart or big data is concerned with handling and analysis of large sets of data. This includes efficient storage, search and visualization. Predictive maintenance, process optimization, supply planning and product quality control are examples for the use of data analytics. The input will be the data from the process and supply chains, product lifecycle information and simulation data from the development and engineering processes.

The IOT ecosystem is heavily dependent on data collection and transmission. Connected sensors collect large amount of data through the Internet, enabling M2M interaction and processing of the data for particular services. Different types of data are transmitted and processed within the IOT ecosystem. The data primarily includes personal data and sensitive personal data such as financial information, location, health related information, etc., that is attributed to an individual.

The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services. Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

M2M/IoT Networks – Security:

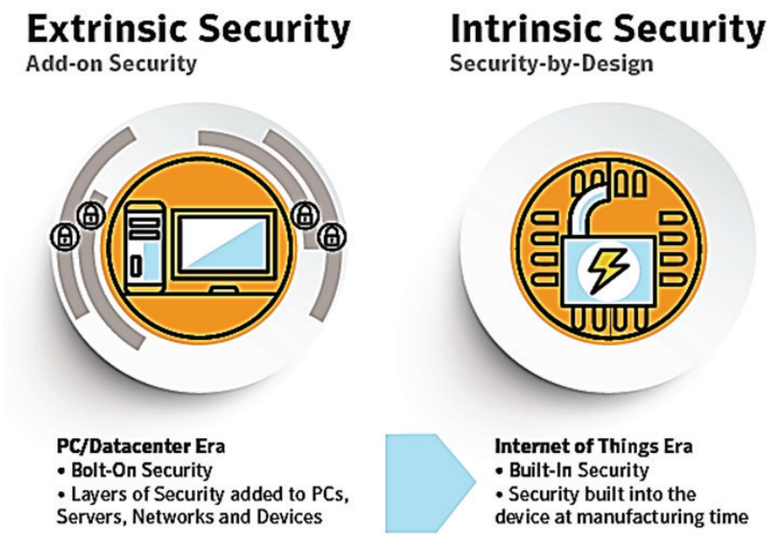
In this next generation technology world, the virtual will have control over the physical world. Take the example of key utility infrastructure, such as power and water. Getting security right in the age of the IoT could mean the difference between chaos and order, not just in cyberspace but in the physical world. The digital world is unique in that there is a “fine line” between productivity and chaos, and that “trust” is the issue which will determine success and failure in the digital future.

The M2M devices will be generating huge amount of data, at times data that are personal in nature, during its life cycle. One of the points where data security can be compromised is at the device layer itself. Hence, to ensure data protection, “Security by design” principle should be implemented or at the very least “Integrity by design”, within the limits of physics. M2M device manufacturer should also be regulated by rules of product safety where applicable.

While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber-attack and expose user data to theft by leaving data streams inadequately protected. The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.

It is imperative to ensure integrity as well as confidentiality of the message/data/information in the IoT networks. This is because, a network may be able to provide integrity of a message without confidentiality or vice-versa.

While Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it; Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). From a user safety standpoint, integrity is critical and privacy of user data and fraud prevention may require confidentiality and additional mechanisms. Hence, as a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues.



Fortunately, IoT security can be covered with four cornerstones:

- Protecting Communications
- Protecting Devices,
- Managing Devices, and
- Understanding Your System

These cornerstones can be combined to form powerful and easy-to-deploy foundations of security architectures to mitigate the vast majority of security threats to the Internet of Things, including advanced and sophisticated threats.

M2M/IoT in Smart Cities & Smart Infrastructure

The new paradigm of smart grid, smart home, smart building, smart city, further complicated by the 'Internet of Things' and Internet of 'Everything' bring a whole new set of challenges for the Security and Security Evaluation Methodologies for complex nature and architectures of IT and communication networks evolving to meet these rising needs of the society. On one hand, we have the highly protected Networks for the 'Critical Information Infrastructures'; on the other, these very 'highly protected networks' need to give access to the consumers for Consumer Engagement and Participation in these Smart Infrastructures to meet the true drivers of setting them up. These large Smart Networks are actually highly complex 'Systems of Systems' and 'Networks of Networks', and thus create new challenges in the security paradigm and development of protection profiles.

Smart Cities being the convergence of IT, communication and diverse engineering technologies designed to cater to a nation's integrated critical infrastructure requirements comprehensively, is a mission critical deployment needing the highest possible grade of security. This is because, once these Smart Infrastructure Deployments are complete, one would simply need a few good hackers who could penetrate through any vulnerable IoT Node into the Smart Cities/Infrastructure network of a nation and shut down the communications and/or the power to the nation.

All the ecosystems, be it Smart Cities, Smart Grid, Smart Buildings or Smart Factories now find themselves making three classes of transformations:

- Improvement of infrastructure – to make it resilient & sustainable;
- Addition of the digital layer- which is the essence of the smart paradigm; and
- Business process transformation - necessary to capitalize on the investments in smart technology.

All Smart City programmes and projects pursue many common goals including sustainable development, better efficiency, resilience, safety and wider support for citizen's engagement and participation. However, each individual city tends to follow its own approach in smart cities programmes and projects. This creates a risk of large-scale fragmentation and it is not surprising that the numerous technology activists are very vocal on various Smart Cities forums even though cities cannot be reduced to just "Big Data" and "IoT".

Fast, secure, reliable and cost-effective communications are critical for the 'Smart Cities', with an entire interconnected network of interactive smart devices. However, a major disconnect which has recently become apparent is: the technological trends in 'Smart Homes', 'Smart Buildings', 'Smart Cities' and 'Smart Grid' are being considered and pursued in isolation from each other with 'silo' approach, by the respective stakeholders. In reality, they form a very tightly interwoven and homogenous confluence of similar technologies being applied in different domains for a common cause of making our planet earth 'smart, green and secure'.

M2M/IoT Industry Growth in India - Key Drivers

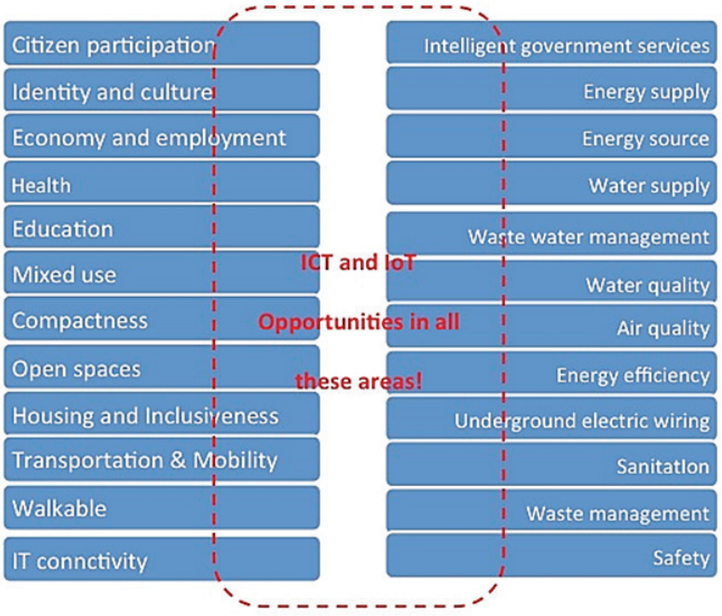
Different agencies have projected huge growth (albeit different numbers in different time scales) for the M2M/IoT devices, deployments and business in the next decade. The sheer wide spectrum of applications of this paradigm be it consumer, enterprise, industrial, commercial, infrastructure somehow ensure that the buzz does not die down, in spite of non (or very slow) proliferation of the paradigm on ground.

However, beyond leveraging M2M/IoT & ICT in the digitization of Institutional, Economic, Social & Governance Infrastructures of a city, a glimpse into the physical infrastructure brings out a few staggering numbers on the business aspect of this disruptive paradigm. The scenario in India is projected as follows:

- In next five years, more than 250 million Smart Electricity Meters are going to be procured & deployed under the NSGM (National Smart Grid Mission). All these 250 million Smart Meters are going to use Communication Modules and Gateways/DCUs (Data Concentrator Units). At a conservative figure of One DCU/Gateway to 500 Smart Meters, 250 million Communication Modules & 0.5 million DCUs/Gateways shall be needed for the last mile communication in the Smart Metering (AMI) Deployments alone...
- Smart Streetlights in next five years, are going to use more than 100 million Communication Modules and at least half a million of DCUs/Gateways...
- Smart Buildings are going to deploy more than 50 million smart Sensors and at least 300K – 500K DCUs/gateways...
- Similarly, various applications of the Smart Infrastructure paradigm like Smart Water, Smart Gas, Smart

Traffic, Smart Environment, Smart Waste Management, Smart Sewage Disposal etc. are going to use a few billions of Smart Sensors with Communication Modules and DCUs/Gateways correspondingly with at the least worst-case ratio of 1:100 to 1:500

- Even if the unified Communication Infrastructure is deployed, the number of sensor Communication modules is not going to reduce; only the DCUs/Gateways needed shall reduce, but shall need enhanced features and design complexities...



Features of a Smart City: 24 Features identified by MoHUA, GoI.

To summarize, India is going to need a minimum of 4 - 5 billion Communication modules to be integrated into the Smart Sensors and Controllers and 10– 50 million Gateways that shall be needed to operate and maintain the Nation Wide Critical Infrastructure that needs to be deployed to enable and empower the citizens to lead a sustainable, safe and secure life. And these numbers do not even account for the ever growing Enterprise and Consumer applications of M2M/IoT paradigm.

However, because of heterogeneous ecosystem, and lack of interoperability and harmonization, the ecosystem is likely to stay fragmented in near future.

Adoption of M2M/IoT in India

Indian Industries across diversified sectors have already discovered the advantage the M2M/IoT Technologies provide to their products and services. An example of M2M/IoT deployment in Agriculture/Farming Sector, a leading Tractor Manufacturing company is using IoT Devices on its tractors to generate data on need for predictive and preventive maintenance and help farmers. The sensors of these IoT devices track the farmer's vehicle operations on real-time basis and schedule maintenance tasks.

Same way in the manufacturing industry sector, a packaging industry giant is partnering with a Startup that is connecting the entire shop floor, comprising more than 100 machines to plan the movement of materials and coordinate with production. Also, their factories use IoT enabled machines, which can track the failure rate in machines in real time.

And in the Consumer Business, an Indian Retail Giant has embraced new digital strategy and is working closely with Communication Company to connect to the modern consumer in a manner where all formats will play a major role in increasing revenues. They are piloting this to win over the 'consumer of the future', targeting them to remain on a single platform with multiple channels for shopping.

Communication and Network Infrastructure

The spectrum requirement for a M2M/IoT services will be based on the technology through which the particular service is extended. A wide range of existing and emerging technologies can be used to provide M2M services. M2M/IoT can be deployed using a wide range of different protocols, based on their connectivity requirements and resource constraints. It could use both wired and wireless networks. Many of the devices and the services offered through them will require flexibility and mobility and hence would prefer wireless network. These can include short-range radio protocols such as ZigBee, Bluetooth and Wi-Fi; mobile phone data networks, or bespoke networks for M2M like LoRa® etc.

Licensed Access Spectrum

Considering the Indian scenario as well as the global deliberations on the spectrum for International Mobile Telecommunications, IMT-2020, IMT Advanced and Machine Type Communication (MTC), the Telecom Authority (TRAI has taken a view that licensed spectrum available with the telecom service providers as on date (Sep 2017), as well as, the spectrum likely to be made available in the near future is sufficient to meet the requirement of deploying M2M services in India in the near future. Once the global standardization process is completed and spectrum identified for 5G and MTC in WRC-19, the spectrum requirement of access services including MTC, would be revisited in order to achieve global harmonization.

Unlicensed Access Spectrum

In India two bands 2.4 GHz (2.400-2.4835 GHz) and 5.8 GHz (5.8255.875 GHz) have been defined as License-exempt bands for indoor and outdoor applications. In addition, 5.15-5.25 GHz and 5.725-5.825 GHz are also available for indoor uses in unlicensed bands. The Telecom Regulatory Authority of India has recommended to DoT to de-license the V-band (57-64 GHz band) for indoor and outdoor access applications like Wi-Fi hotspots etc. In sub-GHz band 433-434 MHz and 865-867 MHz are license exempt for indoor applications. TRAI has recently recommended (Recommendations_M2M_05092017) to de-license additional 1 MHZ frequency band at 867-868MHz and a chunk of 6MHz in 915-935MHz band.

International Internet Bandwidth

International Internet bandwidth owned by various service providers is reported to be 2,600 Gbps during Q1 2017. Thus, the telecom network infrastructure is ready to be leveraged for providing connectivity and services in M2M. Further the telecom access technologies are rapidly evolving to meet the requirements of M2M communication/IoT. For example, narrowband IoT (NB-IoT), EC-GSM & LTE-M are new cellular access technologies, specifically tailored to form an attractive solution for emerging low power wide area (LPWA) applications. Operation in licensed spectrum also provides predictable and controlled environment, which enables efficient use of the spectrum to support massive volumes of devices. The incumbent telecom operators are natural candidates for providing connectivity and services in M2M sector. The TSPs should harness the ready availability of their networks, all over India, to provide M2M connectivity and services. The telecom operators (ISPs/TSPs) viz. CMTS, UASL and UL holders can either offer customized M2M services on their own or they can lease their resources to resellers. The resellers of telecom services in the country are covered under UL (VNO) licensing regime.

Bharat Net

The Bharat Net initiative has been rolled out to realize major objectives of the Digital India vision. It aims at establishing a highly scalable network infrastructure accessible on a non-discriminatory basis, to provide on-demand, affordable broadband connectivity for all households and on demand capacity to all institutions. It is a three-phased initiative to provide broadband access to 250,000 Gram Panchayats (the Rural/Village Local Bodies) through a network of Optical Fibre Cable (OFC) by December 2018. With the revised budget of USD 1.5 billion, OFC has been laid in 155,000 kilometres and is set to provide broadband connectivity to approximately 150,000 villages by December 2018, of which, connectivity to approximately 50,000 Gram Panchayats has already been provided. The government is also working extensively on providing public Wi-Fi hotspots for affordable access and offloading data from cellular networks. As of now, approximately 2,500 Wi-Fi hotspots have been commissioned in a little over 1,200 locations across the country.

In order to realize the dream of 'Digital India', Government of India (GOI) is fast tracking the implementation of 'Bharat Net' As on Jan 2018, it has achieved the Phase-1 target of connecting 1 Lakh Gram Panchayats (1 01 733 – service ready Gram Panchayats). GOI has set the target date of March 2019 for connecting the remaining 1.5 Lakh Gram Panchayats during Phase II. The aim is to ensure at least 100 Mbps at each Gram Panchayat, using appropriate technology. Currently pilot projects are underway at 3 Blocks each consisting of 58 Gram Panchayats to understand use cases/scenarios.

Mobile Networks

The mobile network has grown exponentially in the country in the last decade. As on May 2017,12 there are 665622 2G BTSs, 27341 CDMA BTSs, 348464 3G NodeBs and 461408 4G/LTE eNodeBs are operational in the country shared amongst 6 major operators. Further high-speed Internet is enabled with increased optical fibre capacity up-gradation.

Private Enterprise

Indian Private Enterprises are actively working towards building network infrastructure in smart cities to enable IoT technologies with the aim of linking intelligence and information with devices.

For example, one company is currently working in building Internet network capacities and system in two smart cities. It is creating networks for applications for e-governance, public safety, traffic and utilities, basically a high-level ICT (information and communication technology) architecture.

Similarly, a MVNO (mobile virtual network operator) specializing in providing connectivity to machines is currently working on Smart City Projects for network infrastructure for IoT, claiming that it currently has 7.5 million connected devices on their platform globally.

M2M/IoT - Technology Innovations

IoT Start Ups

IoT Start Ups in India have grown impressively in a very short time from 123 in 2014 to 275 in 2015 and to 971 in 2017. Many of these Start Ups are actively collaborating with GOI in its Smart City Mission in the areas of: renewable and sustainable energy systems, wastage and spillage.

Centre of Excellence for IoT in India, Bengaluru

The Centre of Excellence for IoT (CoE IoT), at Bangalore, is a Digital India Initiative to jump start the IoT ecosystem

in India taking advantage of India's IT strengths and help country attain a leadership role in the convergent area of hardware and software. It is a joint initiative of MeitY, ERNET, NASSCOM and Government of Karnataka. The main objective of the CoE IoT is to help Indian IoT Startups leverage cutting edge technologies to build market ready product. Through IoT Startups Program, CoE aims to build industry capable talent in an entrepreneurial ecosystem by providing Incubation, Funding, Acceleration, Industry Connect and Mentoring.

C-DOT's Common Service Platform

With the Indian Government focusing on Smart Cities, C-DOT has developed CCSP (C-DOT Common Service Platform), which can be deployed on any off-the-shelf generic server platforms or cloud infrastructure. This platform from C-DOT, which is based on the oneM2M Common Service Layer Standard, will enable the smart cities to reap all the benefits of using a standards compliant horizontal service layer aimed at being more efficient, economical and future proof. This can be seamlessly deployed for any kind of M2M/IoT applications like infrastructure, consumer, enterprise or industrial.

IoT Platform Initiative by a TSP

A leading Indian Telecom Service Provider has launched an IoT platform in April 2017 aiming to provide a common platform for vertical industries such as automation, healthcare, agriculture, financial services and asset tracking. That TSP is continuously developing new IoT use cases for various industries in the Indian market and build them on the IoT Platform, which provides device registration, IoT rules, advanced analytics, visualization, reports and cognitive capabilities for each use case.

M2M/IoT – Readiness of Major Indian Operators

As India has slowly started to emerge as a global destination for many of the IoT technologies, as network connectivity providers, the telecom operators will play a crucial role in in M2M/IoT communication, which would require operators to adopt new communication technologies and processes to ensure seamless connectivity.

According to Deloitte, IoT units in India are expected to see a 31-fold growth to reach 1.9 billion by 2020 owing to advances in reliability, accuracy and technology.

While Indian operators work on creation of 5G infrastructure and deployment, the other stakeholders (GOI, TRAI, TEC etc.) need to address on priority challenges related to telecom and regulatory policies, standards, testing and certification, supporting infrastructure. The status of the major Indian telecom operators with regard to adoption, implementation and introduction of M2M/IoT Communication Networks is as under:

Tata Communications Ltd

Tata Communications along with HPE (Hewlett Packard Enterprise) is deploying LoRa® networks using HPE Universal IoT Platform based on oneM2M interoperability standard to offer massive scale, multi-vendor and multi-network deployments with streamlined interoperability and management of heterogeneous IoT devices and applications that power the intelligent edge.

The deployed networks are low cost, Low Power Wide Area Network (LPWAN), solely dedicated to the Smart City IoT applications, which provide LoRa® powered devices and application development assistance to provide an end to end Smart City solution. Tata Communications IoT network comprises an efficient integrated command centre that displays all data and analysis of the IoT sensors deployed across the city be that in water, electricity, parking, or street lights, which can be monitored and managed in real-time. The results of the citywide LoRa® network has

produced a host of benefits, like:

- 3-fold reduction in cost of the electricity bill for street lighting,
- 30% water saving through automated valves in water network, and
- Improvement of productivity of workforce by 5% (min) & improved efficiency across.

Tata Communications is a member of the LoRa Alliance™, spearheading the adoption of the LoRa® technology and bringing the global ecosystem to India. It plans to extend LoRa® network coverage to all cities with a population greater than 1 million by 2018, and all cities with a population greater than 50,000 by 2019.

Reliance Jio Infocomm:

Reliance Jio Infocomm is gearing up to harness Internet of Things (IoT), focusing first on enterprises and industries followed by the consumer segment. It has started to roll out its IoT networks and launched first commercial pilot on NB-IoT for Smart Metering application. It also plans to roll out home broadband-powered home automation that will allow users to convert basic electronic products into smart products with the installation of six-seven smart plugs. These smart plugs will allow users to control the entire home with the help of smartphones or tablets. Jio is also planning to launch a complete suite of home surveillance comprising smart camera, smart doorbell, smart lock and chime alarm, all of which can be managed from the user's mobile devices.

Bharti Airtel Ltd:

Bharti Airtel is currently setting up a centre of excellence for IoT in Bangalore to develop software platform & communication network to cater to the home automation or smart home segment with its M2M/IoT services, allowing users to control elements such as lighting, heating, air conditioning, music and security systems through smartphones. Bharti intends to leverage on its quad play – broadband, fixed line, wireless, DTH, which has established its presence in millions of homes.

Policy Initiatives & Standardization

The new paradigms like green movement, DC power, renewables, micro-grids, networking devices, smart homes, smart buildings, smart grids and smart cities have given rise to a new much larger paradigm of 'unified and secure' smart infrastructure.

But true convergence is still eluding because of lack of harmonized standards in the respective ecosystems. The smart nodes of one network cannot talk to smart nodes of the other networks. A wide array of 'proprietary systems/solutions', or 'systems/solutions with very limited interoperability' are being deployed in each application areas of home automation, building automation, industrial automation or even the infrastructure automation needs of the society.

To enable smooth roll out of any National Level initiative, the Policies, the Regulations and the Standards play a critical Role. A homogeneous approach among these creates a uniform n robust foundation and framework for harmonized deployment of the various heterogeneous infrastructure components to yield the desired outcomes of the National Initiatives.

The standards in question are related to the communications nodes and the interactions of these nodes at each segment of this system, from the edge nodes, all the way to the cloud. It also would then include service and business models associated with services created. It's a given that ubiquitous access to the cloud, IP and the web paradigm will help hide some of the complexities of the systems for the users, and would allow simpler lower cost solutions down the road.

Government Policies on M2M/IoT- Centre and States:

National Telecom Policy

National Telecom Policy (NTP) 2012, recognized the concept and potential of M2M/IoT. NTP-2012 has mandated to:

(i) Facilitate emergence of new service formats such as Machine-to-Machine (M2M) communications (e.g. remotely operated irrigation pumps, smart grid etc.) through affordable access and efficient service delivery.

(ii) Adopt best practices to address the issues (like encryption, privacy, network security, law enforcement assistance, inter-operability, preservation of cross border data flows etc.) related to cloud services, M2M and other emerging technologies.

National Telecom Policy (NTP) 2018, to be rolled out in next few months is expected to focus on creating an ecosystem using 5G Services, where Internet of Things (IoT) and Artificial Intelligence (AI) are mainstream and connectivity is seamless, designed to improve the quality of e-governance and education, enable financial inclusion, smart cities and an intelligent transportation system, etc.

National Telecom M2M Roadmap

Department of Telecommunications, Ministry of Communications and Information Technology had Published in May 2015 its "National M2M Roadmap" detailing a wide range of aspects including: Spectrum availability for M2M Communications, Role of Bharat Net in enabling M2M reach nation-wide, building M2M network, Certification of M2M products, M2M application in Smart Cities and Road Ahead.

Many of the listed action points have been already addressed by releasing the required guidelines, regulations and policies, and the department is on track to ensure structured and well planned roll out of M2M Services in next few years.

IoT Policy – Centre and States

Ministry of Electronics & Information Technology (MeitY) had published 'Revised Draft IoT Policy' in October 2016 whose stated objectives include:

(i) To create an IoT industry in India of USD 15 billion by 2020. This will also lead to increase in the connected devices from around 200 million to over 2.7 billion by 2020. It is assumed that India's share in global IoT industry would be 5-6%.

(ii) To undertake capacity development (Human and Technology) for IoT specific skill sets for domestic and international markets.

(iii) To develop IoT products specific to Indian needs in the domains of agriculture, health, water quality, natural disasters, transportation, security, automobile, supply chain management, smart cities, automated metering and monitoring of utilities, waste management, Oil & Gas) etc.

The strategy outlined to implement the IoT Policy is through 5 vertical pillars: demonstration of domain-specific applications, incubation & capacity building, R&D and innovation, incentives and engagements, human resource development; and 2 horizontal supports: standards and governance structure.

The initiatives launched for: smart cities, smart water, smart environment, smart health smart waste management, smart agriculture, smart safety, smart supply chain & logistics, smart manufacturing / industrial IoT are part of identification, deployment and demonstration of IoT concepts for solving the nation's challenges and addressing priorities with an inclusive approach.

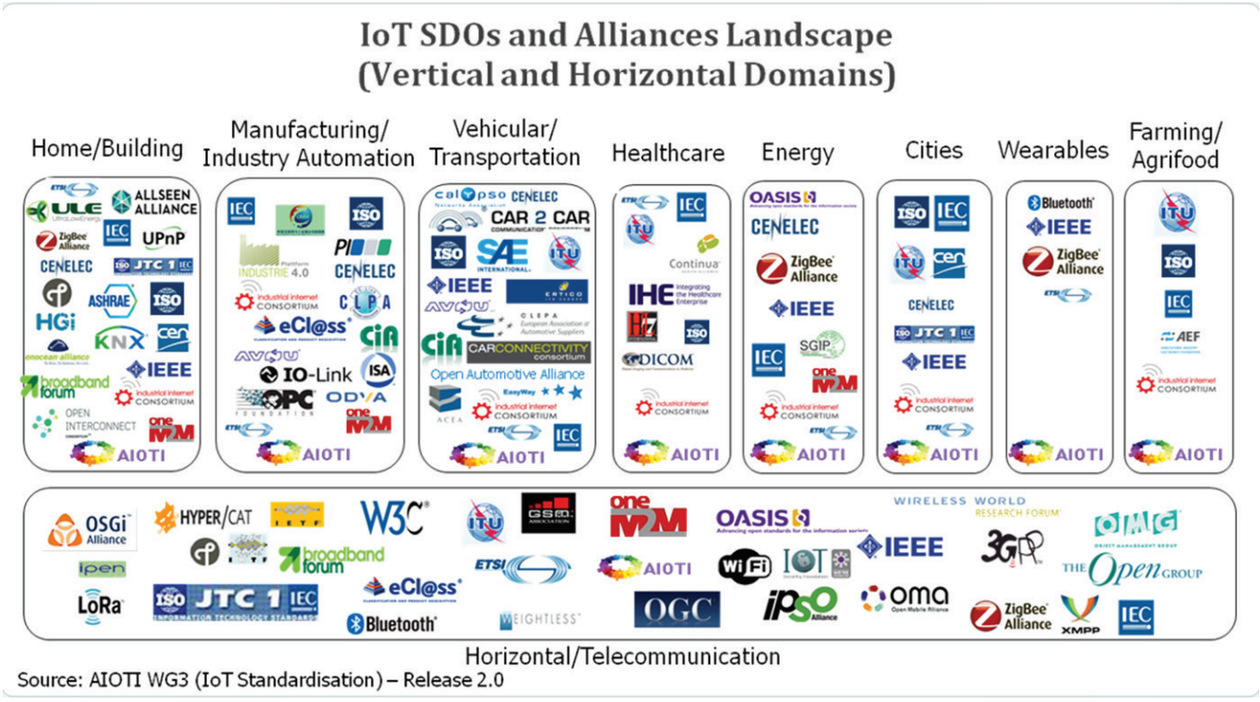
Among the states, Andhra Pradesh has published its IoT Policy (2016-202) on 16 March 2016 and Jharkhand has published Draft IoT Policy 2017.

M2M/IoT standardization

The virtual representation of the physical objects (things) is an important part of all the new "smart" applications that are transforming our industry. The Internet of Things (IoT) is going to provide this in an Internet like structure. IoT covers a wide range of technologies from the lower communication layers to application protocols semantic descriptions of the things and their properties, services and application programming interfaces that allow applications to interact with the things in a standard manner.

The widespread applications of M2M/IoT solutions and services have brought to the forefront the importance of standardization in this ecosystem. Market projections for the growth of Machine-to-Machine (M2M) communications and the Internet of Things (IoT) seem unrealistic without the emergence of a global standardized platforms. In fact, this industry will not take off without significant consolidation and the economies of scale that standardization can bring. Hence Standardization is imperative to deliver/achieve the scalability and flexibility the market requires to maximize the full potential of M2M/ IoT.

Due to this wide variety of technologies and the use of IoT in various application areas with different requirements it can be assumed that no single set of technologies and no single IoT architecture will be standardized and dominate the market. Still it will be useful to have a common architectural framework with common service



definitions as the base for different application domain specific architecture profiles in order to achieve interoperability between these domains at the necessary levels. Coordination between the different domain specific standardization activities and a common IoT architecture framework standardization is needed to achieve that. Application area specific architecture profiles can then be derived from the framework.

Standards and policy are critical elements of IoT and M2M as many heterogeneous devices will be connected with each other to deliver the various services. Standardization is needed in order to deliver the scalability and flexibility the market requires maximizing the potential of IoT and M2M. Standardization enables improved functionality – cost-quality trade-offs to be made, which will deliver faster time-to market for new devices and applications. The dramatic change within short period of time is mainly attributed to development of ICT and Internet.

At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. Attention-grabbing headlines about the hacking of Internet connected devices, surveillance concerns, and privacy fears already have captured public attention. Technical challenges remain and new policy, legal and development challenges are emerging.

With the IoT Architecture Reference Model (IoT-ARM), developed by the EU research project IoT-A (the European Lighthouse Integrated Project) such an architectural and service framework already exists. The IEEE P2413 activity for a Standard for an Architectural Framework for the Internet of Things is leveraging the IoT-ARM for further granular work.

Semantic technologies that allow describing the meaning of data and ontologies are important features of such an approach. This goes in hand with the self-description of things as the base for its virtual representation. For the flexible and dynamic nature of IoT it is not possible to agree on all data models beforehand. Instead knowledge about new data elements has to be built up autonomously by the applications based on Ontologies that define the fundamental types and properties of the domains and their relationships and a semantically

enhanced representation of the data. Semantic Web and Ontology protocols like RDF and OWL have been already defined by W3C in order to make the content of web pages machine-readable. For the industrial use cases and requirements extensions of these protocols are needed to support for example real-time, bandwidth and processing requirements. Rules and structures for product properties have been defined by IEC (SC3D) and ISO (TC184) and a Common Data Dictionary for electrical components incl. component, material, feature and geometry descriptions is available from IEC (IEC CDD). Also, an electronic device description language (EDDL) has been defined by IEC. eCl@ss provides a cross sector standard for the classification and distinction description of products and services. Further evaluation on extensions for all relevant application areas and how they fit together with the W3C Semantic Web protocols is needed.

One specific issue for IoT is the unique identification of things, which is a pre-requisite for their virtual representation. This includes for example the identification of the products, the production equipment and all the control and management components. The identification should be independent of specific communication technologies, preferably stay with the things during their whole lifetime and scale with the expected massive growth of connected things. Various methods for identification have been defined so far like barcodes, RFIDs or visual identification. IEC (SC3D) and ISO (TC184) have defined requirements and rules for identification systems that will apply for the industrial automation domain. Alignment/interworking with identification schemas used in the various application domains has to be considered. Mainly being addressed by IEEE P2413, oneM2M, ITU, JTC1 SC41, OIC, AllSeen, W3C, OASIS, NIST CPS, IIC, IEC SC3D(v), IEC TC65(v), eCl@ss, ISO TC184(v)...

Over the last years two major developments are happening in the vertical application areas in relation to ICT:

- The increased use of ICT enables new, often called “Smart“solutions that lead to increased overlap and interaction between the application areas. A Smart Grid interacts with factories, buildings, homes, electrical vehicles and the city infrastructure. E-Health and Active Assisted Living (AAL) applications connect the healthcare sector with the home. Smart City applications interact with the whole city infrastructure, its administration and residents. In addition to product standards, complex systems and their interaction with systems from other application areas have to be considered.
- Vertical application area specific ICT solutions are more and more replaced by horizontal technologies like Ethernet, WLAN, IP and web protocols. These widely used off-the-shelf technologies will decrease development, production and maintenance costs. Standardization of these technologies is done in dedicated ICT standardization organizations like IETF, W3C, OASIS, ETSI and ITU. With the current introduction of the Internet of Things this trend is even increasing.

Convergence of Vertical and Horizontal Standardization

With the increasing importance of horizontal ICT for the new “Smart” vertical solutions like smart grid, smart home, smart manufacturing (Industry 4.0) we see also the establishment of standardization activities that try to cover both horizontal technology and vertical application issues. IoT is a major driver for that development as the vertical solutions are the main application area for IoT. Especially horizontal ICT standardization bodies like oneM2M, ITU, IEEE and OASIS try to cover vertical applications. In addition, many new consortia like OIC, IIC and AllSeen Alliance have been established which cover horizontal and vertical issues. They focus either on specific application areas like the smart home or try to cover larger eco systems like the IIC (industrial), OIC (home + industrial) and oneM2M (home + industrial). Some of them define their own standards (OIC, oneM2M, AllSeen) while others focus on providing interoperability by defining architectures and profiles based on existing standards (IIC) mainly being addressed by - IIC, OIC, oneM2M, JTC1, ITU, AllSeen...

European Telecommunications Standards Institute (ETSI)

ETSI standardization activities are structured as a set of Technology Clusters, and M2M/IoT standardization activities are addressed under the 'Connecting Things Cluster' with focus on integrating objects to create new networked services and the main emphasis on leveraging technologies to enable transparent interaction between people and things.

ETSI Technology Clusters for Standardization

ETSI is addressing the issues raised by connecting potentially billions of smart objects into a communications network, by developing standards for:

- data security
- data management
- data transport
- data processing

to ensure interoperable and cost-effective solutions, open up opportunities in new areas such as eHealth and smart metering, and allow the market to reach its full potential.

Current Policy & Standardization Activities in India

BIS and TSDSI have dedicated working groups for formulating standards specific to M2M/IoT & Smart Infrastructure. TSDSI is an Organizational Partner (OP) of 3GPP and Partner Type1 of oneM2M, and provides all its members with access to these two bodies. BIS is a founder member of International Organization for Standardization (ISO) and member of International Electrotechnical Commission (IEC) since 1949. BIS and TSDSI are also participating and proposing, India specific requirements at global Platforms to address Indian concerns in global standards and facilitate harmonization of Indian M2M/IoT Standards with global standards to reap benefits of compatibility, interoperability, scale and affordability.

The European Union and EFTA perceive India as a very important market for IoT & M2M products and services. Information and communication technology: M2M/IoT, e-Accessibility, Security, 5G, NFV/SDN are the areas of cooperation between India and EU/EFTA in development of emerging standards.

India has many organizations responsible for Standards and Policies in the M2M/IoT domain–DoT/TEC, BIS, TSDSI and MeitY. BIS being the National Standards body, Smart Infrastructure Sectional Committee LITD 28 is continuously ensuring that all the standardization activities within India on similar subjects are comprehensively harmonized by monitoring the work progress in TSDSI, DoT/TEC & MeitY and ensuring close collaboration and coordination. Further BIS LITD 28 continuously maps the work going on in various organizations/forums actively engaged in M2M/IoT Networks promotion to ensure development of Latest, India specific, yet globally harmonized ICT, M2M/IoT, Smart Cities & Cyber Security Standards. BIS LITD 27 on Internet of Things & Related Technologies is the National Mirror Committee of ISO/IEC JTC1/SC41 with the same Title & scope. Recently BIS has constituted LITD 29 on Blockchain & Distributed Ledger Technologies as the National Mirror Committee of ISO/TC 307 with same title & Scope; LITD 30 on Artificial Intelligence as the National Mirror Committee for ISO/IEC JTC1/SC42 with same Title & Scope.

BIS LITD 27:

To develop standards in the field of Internet of Things and related technologies including sensor networks; wearable electronic devices and technologies; and big data. And act as the National Mirror Committee for ISO/IEC JTC 1/SC 41 Internet of Things and related technologies, ISO/IEC JTC 1/WG 9 Big data, IEC/TC Wearable electronic devices. Comprises of Work Groups on IoT Architecture, IoT Interoperability, IoT Applications & Wearable Devices; and Study Groups on IoT Trustworthiness, Wearables, Industrial IoT, Real Time IoT, Industrial IoT & Aspects of IoT Use Cases.

BIS LITD 27 is currently evaluating some ISO Standards developed by JTC1/SC41 to adopt as National Standards.

BIS LITD 28:

Standardization in the field of Smart Cities (Electro-technical and ICT aspects) and related domains including Smart manufacturing & Active assisted living. Current Standards development on the following:

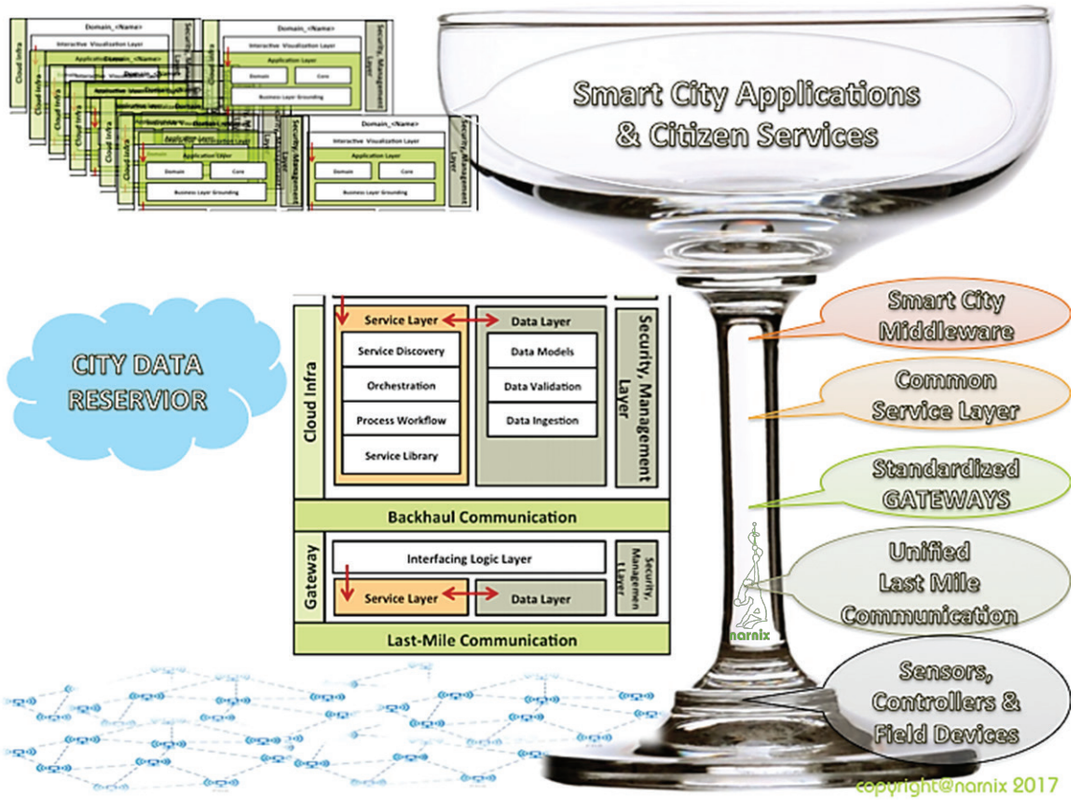
- Reference Architecture for Unified Secure & Resilient ICT Infrastructure for Smart Cities
- Unified Last Mile Communication Architecture & Protocols for Smart Infrastructure
- Common Service Layer for Unified Smart Cities/Infrastructure ICT Architecture
- Unified Data Semantics, Data Models & Ontology in Smart Cities & Smart Infrastructure Paradigm
- Security & Resilience Framework
- Use Cases in Smart Infrastructure Paradigm
- Standards Inventory & Mapping for Smart Infrastructure Paradigm

The BIS Smart Infrastructure Sectional Committee LITD 28 has undertaken an in-depth study on the Spectrum requirements for M2M/IoT applications & Services in the near future, along with comprehensive analysis of Regulatory aspects in this context. This “Study Report on Spectrum Implications” based on “Technical Analysis of RF Spectrum Requirements in Constrained Applications’ Communication Networks for Smart Infrastructure” has been released recently and shall be submitted shortly to the Ministry of Communications and all its relevant Wings & divisions like TEC, WPC & TRAI.

The LITD 28 has also released a Pre-Standardization Study Report on Technical Requirements Analysis of Unified, Secure & Resilient ICT Framework for Smart Infrastructure. It is aimed at providing some critical Actionable Insights for Smart City Planner in context of Unified Secure & Resilient ICT Infrastructure in Smart Cities. As an outcome of the in-depth studies of Indian requirements the report illustrates a new Architecture for Unified & Secure ICT Backbone for Smart Cities leveraging the M2M/IoT technologies in a Standardized &

interoperable framework.

The evolved Comprehensively Unified ICT Architecture can be modelled as a "Classic Saucer Champagne Glass"



Classic Saucer Champagne Glass Architecture

with a wide Flat Bottom Base depicting the multitude of Field Devices & sensors etc. The Saucer Shaped Bowl on the Top depicting being filled with an ever-increasing spectrum of City Applications and Citizens' Services. The Long Stem depicts all the Common Layers viz.: Unified Last Mile Communication, Common Standardized Gateways (application or Vertical Agnostic), Common Service Layer representing the Common Service Functions in the Gateways, as well as, in the Cloud... and the Smart City Middleware & City Data Reservoir in the Cloud.

It is the "Long Stem" of the "Champagne Glass Model" instead of the Short & Narrow Neck in the "Hourglass Model" that brings the comprehensive harmonization, standardization & interoperability in the Architecture leading to optimization in operational efficiency & Life Cycle Cost of the ICT Infrastructure in any Smart City.

LITD 28 has started in true earnest developing the following Standards for the "Unified Secure & Resilient ICT Infrastructure":

- Unified Last Mile Communication Protocols
- Common Service Layer
- Unified & Secure ICT architecture for Smart Infrastructure
- Unified Framework for Data Semantics for Smart Infrastructure

LITD 28 has also constituted a study group on 5G imperatives for Smart Infrastructure to define a smooth migration path from current frameworks and architectures to '5G inclusive' next generation homogeneous architectures.

TSDSI

- Transposition of oneM2M Specifications Rel 2 (comprising 17 specifications and 10 technical reports) into TSDSI Standards. These have been published on TSDSI website.
- Transposition of 295 Specifications of 3GPP (select specifications from Rel 10 to Rel 13) for IMT Advanced (as per ITU-R M.2012-3) into TSDSI Standards.
- TSDSI has been mandated by MoC to develop Standards for Cloud Services Interoperability and adapt 3GPP specifications related to Security.
- MoC has set up a High Level 5G Forum that is expected to formulate strategy for India to take lead on 5G. TSDSI will play the lead role in terms of technical standards for various facets of "5G Systems" (including, but not limited to, radio and core network).

MoC/TEC

The Department of Telecommunications, Ministry of Communications, and Government of India vide Gazette Notification No. G.S.R. 1131(E) dated 5th September, 2017 has amended the Indian Telegraph Rules, 1951 (Amendment 2017) to introduce Mandatory Testing & Certification of Telecom Equipment.

These rules shall come into effect from October 1st, 2018. TEC is implementing Mandatory Testing & Certification of Telecom Equipment in India. For the compliance of these rules, testing and certification of the telecommunication equipments shall be done with the respective Essential Requirements (ER) documents to be framed by TEC. TEC is in the process of formulation of ERs for the Mandatory Testing and Certification of Telecom Equipment.

TEC in DoT has been entrusted the Framing of ERs (Essential Requirements) for Testing and Certification of Smart Devices in M2M/IoT domain. Comprehensive consultations with all the ecosystem stakeholders are being undertaken by IEC senior officials to ensure smooth implementation of the Testing & Certification processes. Essential Requirements will have requirements mainly related to safety, security, technical and functional parameters.

The Security Division of Telecommunication Engineering Centre (TEC), Department of Telecommunications, shall be responsible for activities related to the telecom network security under the overall policy on the cyber security and telecom security.

The focus areas of Security Division are:

- Contribute in defining the Security framework for ICT network, including security objectives, threats and vulnerabilities, management strategies and challenges associated with it;
- Contribute in defining the Security indexing guidelines for telecom equipment in line with ITU-T recommendations X.1521 on CVSS i.e. Common Vulnerability Scoring System;
- Defining security auditing guidelines specific to telecom Service providers in accordance with ISO 27001;
- Co-ordinate with DoT, MHA and other cyber security agencies.

Since 2015, TEC has been regularly releasing study reports on various topics in M2M/IoT domain.

MoC/WPC

Wireless Planning & Coordination Wing under the MoC has begun the preparatory work on the new NFAP – National Frequency Allocation Plan.

Ministry of Communications

Ministry of Communications is in the process of formulating the New Telecom Policy, targeted to be released in 2018, after holding wide range of consultations with various stakeholders. The Policy shall be governed by key guiding principle of alignment with National Vision. The major themes that new Telecom Policy shall try to address include, Regulatory & Licensing frameworks impacting the sector, Connectivity for All, Quality of Services, Ease of Doing Business and Absorption of New Technologies including 5G and IoT. The draft of the Policy shall be put up on the Ministry's Portal shortly for Comments.

TRAI

TRAI recommends that

- Device manufacturers should be mandated to implement "Security by design" principle in M2M device manufacturing so that end-to-end encryption can be achieved.
- The government should provide comprehensive guidelines for manufacturing/ importing of M2M devices in India.
- A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software).

TRAI Recommendations on M2M– September 2017:

Telecom Regulatory Authority of India (TRAI) has published it's "Recommendations on Spectrum, Roaming, QoS Requirements in Machine-to-Machine (M2M) Communications" on 05 Sep 2017. The recommendations are based on the analysis of responses received on the Consultation Paper (CP) from various stakeholders. The recommendations cover:

- Regulatory Framework for M2M Service Providers (MSP)
- Regulatory Framework for Device manufacturers
- Regulatory Framework for M2M Connectivity Providers – Licensed Spectrum
- Regulatory Framework for M2M Connectivity Providers – Unlicensed Spectrum
- Spectrum, Roaming and QoS Requirements for M2M Communications

TRAI Recommendations on NTP- March 2018:

TRAI has recently proposed very progressive norms for the National Telecom Policy(NTP) 2018. TRAI has recommended to enable access for wireless broadband services at affordable prices, including through satellites to 90 per cent population by 2022. It also aims to achieve 900 million broadband subscriptions and deploy five million public WLAN including Wi-Fi hotspots by 2022. In order to ramp up internet connectivity, TRAI has identified a need to review National Building Code of India to mandate city developers and builders to have properly demarcated space for housing communication infrastructure in buildings.

The new NTP will address the challenges the telecom sector faces today and pave the growth path for it. The regulatory body has also laid down strategies to realise the recommended objectives. It emphasised the requirement of huge amount of private investment in the communication infrastructure and networks and the need to unleashing the power of entrepreneurship for investment, innovation, inclusive development to meet the desired results. TRAI also recommended to put in place an ombudsman based consumer grievance redressal mechanism by end of 2018. The other major recommendation TRAI has made is to simplify licensing and regulatory frameworks, rationalise taxes, levies and related compliances by 2019. It also suggested to have an online platform for all government to business (G2B) activities and establish a policy framework for facilitating setting up of data centres by 2019.

MeitY

MeitY is continuously working on identifying and developing standards in the domains of e-Governance and Information Security.

MeitY has released the following e-Governance Standards recently:

- E-Governance Service maturity Model
- Framework for Adoption of Open Source Software in e-Governance Systems
- Framework Document for e-Authentication: ePramaan
- Framework for Mobile Governance

Interoperability Framework for e-Governance

- Code Directories of Generic Data Elements
- XML Schema for Generic Data Elements

MeitY is currently working on:

- India Enterprise Architecture Framework
- India Enterprise Architecture Adoption Guide A Method Based Approach
- Adoption of Mobile AppSec Verification Standard (MASVS)

MeitY is working on the New Electronics Policy...

Testing and Certification

Testing and certifications of various technologies and devices is required to ensure the reliability and the quality of M2M/IoT service across large number of devices and network. TEC is working on establishing device certification and responsibility centres for M2M/IoT domain, in India.

In December 2017, ETSI in cooperation with C-DOT, TEC, TSDSI, and COAI organized a symposium in India on Achieving Interoperability. The event focused on the promotion of best practices in standardization and the awareness of the importance of validation and testing. The attendees to the symposium were provided with insights into how 'Standardization Best Practices' can:

- produce standards of high quality
- support the incubation of new eco-systems
- reduce costs to market
- create economies of scales
- include Open Source contributions in the Standards Making Process
- be relevant to certification

The symposium also provided special focus on how to run Interoperability events and manage the Conformance Testing projects.

Gaps & Challenges

The extensive work done by various global SDOs has very comprehensively defined the frameworks and roadmap for future ICT Infrastructure, except that all that is available still allows for a very fragmented market. Further, the new paradigm of "Internet of Things" has given rise to a new aspect of the way human, machines and things are going to communicate with each other in the very near future.

The heterogeneity of the IoT paradigm has fragmented the market and somehow created unique challenges in reaping the benefits from this paradigm for the society. This heterogeneity and fragmentation has made it imperative to have a fresh look at the prevalent architectures and frameworks of the ICT infrastructure being deployed or being developed.

Hence, true convergence is still eluding the evolved citizens of today's super industrial society, because of lack of harmonized standards in the respective ecosystems of Smart Homes, Smart Buildings, Smart Grid and Smart Cities. The smart nodes of one network cannot talk to smart nodes of the other networks. Multitude of 'proprietary systems/solutions', or 'systems/solutions with very limited interoperability' are being deployed in each application areas for today's Home Automation, Building Automation, Industrial Automation or even the Infrastructure Automation needs of the society. This is certainly leading to a situation where we will not be able to derive the maximum benefits of these technologies unless a very strong push is made and sustained at the highest level for interoperable standards.

Recently such pushes are becoming quite frequent. One such strong push was apparent at the workshop on "Future Proof Smart Cities with a Common Service Layer: A Standards Driven Approach" under India-EU ICT Standardization Collaboration in April 2017.

Problem Statement

We are witnessing an exponential growth in consumer-facing application, and hence M2M/IoT applications are poised to explode. They will drive order-of-magnitude increases in bandwidth consumption and provisioning and control actions. However even today, many applications are poorly adapted for the constraints posed by wireless networks. But wireless is essential in bridging the digital divide especially in rural areas. Protocols that manage the services and devices efficiently are essential if the promise of untethered applications is to be fulfilled. Another challenge is: how do mobile operators deploy networks that efficiently serve populated areas with their onslaught of M2M devices as well as rural areas that need both high speed data and M2M services?

IoT Paradigm & Challenges

The IoT paradigm is expected to be a solution for all the problems and expected to have the characteristics of a Homogeneous Network of Heterogeneous Devices... it is expected to address applications in multiple diverse domains like Industrial, Consumer, Infrastructure, Enterprise, Buildings, Homes and Cities seamlessly. While it is expected to cater to a wide spectrum of applications and deliver multitude of services, it needs to be secure from End-to-End in the entire Signal path and Value chain. Hence, it's imperative for it to be a homogeneous & secure paradigm for heterogeneous devices, systems & solutions.

Challenges in fast growth of IoT:

The IoT value chain is perhaps the most diverse and complicated value chain of any industry or consortium that

exists in the world. While, standardization is needed in order to deliver the scalability and flexibility the market requires to maximize the potential of IoT and M2M because standardization enables improved functionality – cost-quality trade-offs to be made, which will deliver faster time-to market for new devices and applications.

The standards in question relate to communications nodes and the interactions of these nodes at each segment of this system, from the edge nodes, all the way to the cloud. The other hurdle is: viable and acceptable business models of services based on the IoT. It is a given that ubiquitous access to the cloud, IP and the web paradigm will help hide some of the complexities of the systems for the users and would allow simpler lower cost solutions down the road.

At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. Attention-grabbing headlines about the hacking of Internet connected devices, surveillance concerns, and privacy fears already have captured public attention. Technical challenges remain and new policy, legal and development challenges are emerging.

The challenges that inhibit the IoT-related standards and hence robust rollouts of IoT services are:

- Security and Privacy issues;
- Endless IoT applications;
- Endless potential types of edge node technologies, and the interface to the communication nodes (e.g. Sensors and use cases integration into Telco services);
- High fragmentation of today's IoT connectivity solutions;
- Lots of legacy systems that will now be a part of IPv6 network, with no (or minimal) existing "co-existence" and interoperability plans;
- Partnerships, between heterogeneous and diverse industries, and defining the associated business models involving multiple stakeholders and service providers of some of those legacy systems in number;
- Management and provisioning of the various networked devices, applications, and services, and the network capacity planning that comes with it;
- Regulatory issues that will hinder deployments on a worldwide basis;
- Special needs of "industrial grade" product rollouts, with long lasting requirements in the field, that require future proofing of any standard recommended;
- Slow development of the IoT services market, partially due to lack of future proof standards etc.

In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major need but also a major challenge.

Service provider challenges

- A complex and fragmented value chain: IOT / M2M value chain is expected to be complex and fragmented into various niche applications, devices, modules, vertical markets and services. It will include product, system and content providers and solution integrators. Because no single company can provide all components of a complete solution, it is not clear who will play what role. Partnership can help.
- Network requirements: Network challenges result from increasing network traffic, caused by an extremely high number of short messages (SMS) with high signaling overhead.
- Availability: Connectivity will be required in locations not yet considered in current networks.

- Reliability: If networks are critical parts of the business, they must be as reliable as any other critical equipment.
- Scalability: Service providers must manage the significant additional traffic load of the Internet of Things and ensure that each application's (voice, video, data, IOT) communication requirements and service level agreements are met.
- Flexibility: With the varied needs of different applications, enterprises will demand real time reconfiguration of networks and allocation of resources that match their network utilization and also needs flexible pricing schemes.
- Security: Lack of security could derail Internet of Things applications. Devices provide access to a network with applications and data; all of them including the communication have to be secured.
- Response Time/Latency: Service providers need the ability to define flexible priorities for services with different response times, ranging from real-time responses to uncritical long delays

The Security aspect of the IoT

The security aspect of the IoT ecosystem must be given some serious thought and is unfortunately often under-estimated. Creating a secure public applications platform, which will facilitate the IoT ecosystem that consists of partners, carriers and application developers, is a must.

- Security and control of identified devices are key aspects in a universe teeming with privacy concerns, insufficient authorization, lack of transport encryption, insecure web interface and inadequate software protection. This gets all the more critical considering that consumer and industrial applications are increasingly interwoven and acknowledging that awareness of security practices and behaviors is not to be expected from regular consumers.
- With smartphones posing as a key component of IoT, there is a need to look at the complete lifecycle of the mobile security architecture - from design and implementing products and technologies to managing the architecture over time. A key element of security is encryption technology, which is critical to protecting the confidentiality and integrity of a digital transaction between two end points, such as a mobile device and a car or central house automation system. Naturally, that technology will only work as intended if it is used in a carefully designed product or service. As usual the less secured part of a product or service dictates the overall security level.
- The importance of security for IoT infrastructure and platforms cannot be overemphasized. Rather than specific products or services, the next important developments in IoT should be overarching standards, policies, security frameworks and infrastructures. It is critical that the need for security is understood by all, and that security is not seen only as an additional cost in markets with sometimes extremely low revenue per device/user.
- A stable secure technology platform with proven security standards will be imperative for IoT proliferation. This isn't only about the protection of individuals and their privacy but about safeguarding any nation's digital ecosystem and the economy therein.

In Smart Cities, a unified ICT backbone paradigm and a common infrastructure pool enable the creation of an interconnected and truly homogenous system with seamless communication between devices and services. Coordination, collaboration and harmonization can be better implemented by the effective use of standards-based, open, common and shareable, information and communication technologies. The disconnect amongst technological trends being pursued by the stakeholders of the now homogenous smart infrastructure needs to be bridged without any further delay to maintain the Lifecycle Cost or TCO (total cost of ownership) of these individual components within viable economic thresholds.

Current Challenges Smart Cities including Smart Infrastructure

The current state of Smart Cities Challenge Proposals has several gaps that need to be addressed:

- Closed Solutions: Available solutions are extremely closed with an ecosystem that is highly locked-in by vendors i.e., a single vendor owns the vertical application, platform, communication, services, and data. While convergence of technology, unified standard, interoperability, etc., are necessary to ensure customer-centric systems, open markets are essential for competitive, affordable and sustainable solutions. The existing ecosystem allows minimal or no flexibility. This leads to a high risk of a large-scale fragmentation, undermining the country's ambitious goals.
- Force-Fitting Solutions developed for Mature Markets: There is a natural tendency to force-fit existing solutions developed for other cities such as Madrid, Barcelona, etc., to the proposed smart cities in India. This may not be the right approach given the requirements, constraints and challenges in India. India specific needs should be factored-in upfront in the architecture of these solutions.
- Inappropriate Last Mile Solutions: Existing last mile technology for wireless sensor networks are undergoing rapid change to meet radical lower levels of capital and operation cost and much higher levels of reliability for mass usage in smart cities. We may need to contract wisely to encourage experimentation and migration to successful new approaches rather than get locked into a high cost solution such as the Dabhol Power Station.
- Deployment Diversity: Under the Smart City Mission, different cities are expected to contract separately but we need an approach to benefit from some commonality and State-to-State arrangements.
- Non-Standard Disharmony: There is no common framework and architecture defined for the various physical infrastructures to be deployed in the proposed smart cities to work in an integrated, harmonized and optimized manner.
- Dichotomy: There is a dichotomy between, on the one hand, the need for investment in R&D for new products, systems and solutions based on an integrated and secure System Architecture when there is little awareness about the problem among stakeholders, and on the other hand, the creation of a unified System Architecture and Framework where there is no demand due to ignorance about the problem at hand.

Other important Smart City issues

- Smart cities development & deployments are announced without any groundwork on preparedness of the stakeholders and the ecosystem...
- In a smart city, multiple utilities are going to leverage and deploy similar technologies & solutions to improve the operational efficiency
- The technological trends in "smart Homes", "Smart Buildings", "Smart Grid" "Smart Water" "Smart Transport" and "Smart Cities" are being considered and pursued in isolation from each other, by the respective stakeholders. This is in spite of the fact that they form a very tightly interwoven and homogenous confluence of similar technologies being applied in different domains.
- Since, there is no standardization or Harmonization groundwork undertaken to cater to the physical infrastructure's comprehensive and heterogeneous needs of the smart cities, most of the systems & solutions deployed shall have to be procured based on respective vendors' proprietary technologies with limited or NO interoperability with system/solution components from other vendors.
- Each city shall always be dependent on the respective vendors throughout the lifecycle of such systems/solutions for their Operation & Maintenance, and more so for their up-gradation...
- Lack of harmonized standards in the respective "SILO" ecosystems of the Smart Infrastructure shall imply that the smart nodes of one network cannot talk to smart nodes of the other networks. Thus, Data sharing amongst the multiple stakeholders of a smart city shall be a major challenge.

In fact, there is a recursive cycle to the data in a Smart City. Information that is generated is information that is consumed which in turn adds to the information generated and the cycle repeats.

Standardization Imperatives

Each application ecosystem like smart home, smart building, smart street lighting and smart grid have, over the years, developed their own respective sets of standards and last mile communication protocols. In fact, some ecosystems like smart grid, smart building and smart home have multiple sets of standards and protocols being advocated as the most appropriate for their respective applications. Unfortunately, all these initiatives, protocols and standards go against the tenet of the unified and harmonized paradigm of the smart infrastructure.

Architectures and framework designs provide umbrella guidelines to the stakeholders of respective components and layers of the overall smart infrastructure paradigm. However, it is imperative to work on sufficiently fine granularity of each component and layer for standardization, as well as, harmonization, for ensuring the interoperability among various similar components addressing different applications at semantic as well as syntactic levels. Further, the standards being adopted for the smart homes or smart buildings deployments must be harmonized with standards in all other relevant ecosystems and integrated smart infrastructure paradigms. Last, a special effort shall be needed to develop standards for conformance and interoperability testing.

oneM2M is one such initiative that is attempting to address this problem. However, their efforts are limited to the Common Service Layer only. its philosophy keeps the upper and lower layers of the comprehensive communication network in any infrastructure at a very abstract level, which on the other hand brings the benefit of technology agnosticism. The user and/or web interfaces are defined relatively in an explicit manner in line with the WEB Paradigm under constrained environment. But, on the sensor or field devices side of the network, interfaces are defined on the API (Application Programming Interface) paradigm, which apparently seem quite logical and appropriate; yet during implementation on diverse sensors or field devices from different vendors even for the same applications/use cases, challenges of API based approach of Interoperability come to the fore. In the API based interoperability scenario, to ensure true interoperability, each API needs to be tested against the respective API's Compliance Test Tools (which also need to be first developed and accepted by the respective stakeholders) for each use case and/or application, which in most cases turns out to be more cumbersome than defining an end to end protocol.

Conclusions and Recommendation

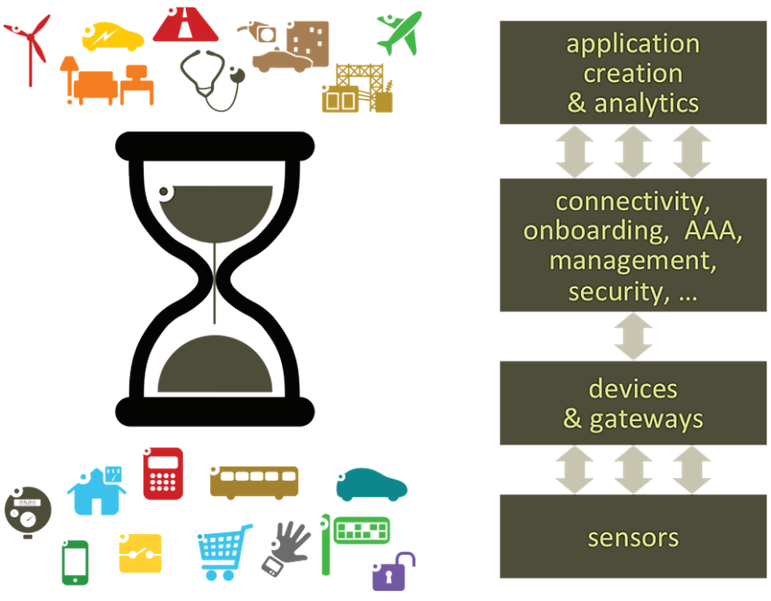
Convergence of the multitude of stakeholders of the IoT ecosystem to common standards is essential for the wide acceptance of the IoT wave by the masses. We should expect to see acceleration and a maturing of common standards, more cross-sector collaboration and creative approaches to business models.

Framework for Interoperability

There is an immediate need to develop/adopt standardized frameworks and architectures to bring comprehensive inter-operability in this heterogeneous, diverse and fragmented ecosystem to enable stakeholders monetize their respective resources and investments that shall further encourage them to offer more solutions and services to the society, business, industry and infrastructure. There is also a need to create and suggest frameworks to achieve the Interoperability among all the devices & layers at every interface in the networks, be it a smart home network, a smart building network, a smart city/community network or the smart grid network that shall enable the stakeholders to prepare a set of detailed standards-based specifications to cater to specific/defined/fixed use cases followed by development of a Compliance & Interoperability Testing Framework.

Common Service Layer Standardization:

It is imperative to standardize a Common Service Layer in the heterogeneous world of M2M/IoT to bring interoperability by creating a distributed software layer – like operating system- which shall facilitate the unification by providing a framework for interworking with different technologies to enable re-use of what is already available as much as possible.



Typical illustration of Common Service Layer

The key to unified smart infrastructure adoption by the diverse stakeholders shall also lie in the design of the Standards based Gateways (or Data Concentrator Units) with Standardized Common Service Functions like Device Management, Registration, Discovery, Communication Management & delivery Handling, Data Management and Repository, Security etc. Only if all the smart devices are easy to install and use, require little or no maintenance activity, and provide useful services, will stakeholders readily adopt them.

Security Framework for Infrastructure

There is a need for defining a security Framework for Telecom Infrastructure assets such as Fibre & Telecom Towers deployed across the country. This framework should allow the assets to be treated as essential infrastructure, which enables telecom connectivity and provision of Internet services to the public and stringent penal provisions should be in place to mitigate risk of damage to these assets.

The IoT is an increasingly attractive attack plane for cybercriminals. Hence, getting security right in the age of the IoT could mean the difference between chaos and order, not just in cyberspace but in the physical world, as well. In face of the increased vulnerabilities due to the large Attack Surface Area in the M2M/IoT paradigm it's imperative to move from the "EXTRINSIC SECURITY" (Add on Security) paradigm to an "INTRINSIC SECURITY" (Security by Design) paradigm. A successful IoT security shall require a multilayered approach to design new systems based on secure software and architectures.

It would be critical to comprehensively address the challenges created by IoT in the integrity & confidentiality of the data and privacy of an individual.

Awareness on Standards

As things stand, Standards & even SDOs are not at the forefront of city planners', utilities', service providers or users' minds. There are misconceptions on what standards are for, and, the case for use of standards has not been made. A key imperative is creating standards awareness among policy makers, planners, utility suppliers and service providers.

National & Global Co-ordination & Collaboration

To keep pace with the global developments in Technology & Standards Indian Stakeholders must leverage the initiatives, best practices & work done in Global & Regional SDOs and collaborate closely to speed up the adoption and implementation of required Standards and best practices. A few initiatives that could be taken up without any complications and delays could be:

- BIS to keep close tab on and adopt (without much delay) the relevant standards from ISO, IEC, ISO/IEC JTC1 & IEEE to speed up proliferation of standards based Interoperable M2M/IoT deployments.
- TSDSI to maintain close co-ordination with 3GPP, oneM2M, ETSI and other global & regional SDOs in the domain to understand, participate and contribute with relevant Indian perspective, as well develop National Standards concurrently to keep pace with global technological advancements...
- BIS and TSDSI to work in close collaboration and synchronizatioin; and BIS to adopt the relevant TSDSI deliverables as National Standards.
- MoC and all its wings to monitor and sync up with activities in ITU and encourage & enable harmonization of Indian telecom policies and other activities...
- MoC, MeitY, TSDSI, BIS and all other ecosystem stakeholders to leverage the initiatives by EU viz.: "India-EU Cooperation on ICT-Related Standardization, Policy and Legislation" and the "Project SESEI" to co-operate and collaborate on areas of mutual interests like M2M/IoT, Security, 5G, NFV/SDN and ensure that Indian stakeholders are technologically at par with global technology advancements.
- Learn from best practices in Standardization, Policies & Regulations from European Union initiatives; and emulate them by constituting High Level Co-ordination groups on important focus areas to harmonize and share the Standardization and other relevant activities in individual National SDO or Industry Bodies.

REFERENCES

- Ministry of Housing and Urban Affairs, Government of India - http://moud.gov.in/
- SMART CITIES MISSION, Government of India - http://smartcities.gov.in/content/
- National Institute of Urban Affairs - https://www.niua.org/
- Smartnet - https://smartnet.niua.org/
- Ministry of Electronics & Information Technology - http://meity.gov.in/#
- Ministry of Telecommunication - http://www.dot.gov.in/
- Telecom Engineering Centre, DoT - http://www.tec.gov.in/
- EU Project SESEI - http://sesei.eu/
- India-EU ICT Standardization - http://www.indiaeu-ictstandards.in/
- http://tec.gov.in/pdf/M2M/Spectrum%20requirements%20%20for%20PLC%20and%20Low%20power%20RF%20communications.pdf
- http://www.trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf
- http://www.bis.org.in/other/USR_ICT_FSI_V_1_0.pdf
- http://meity.gov.in/content/guidelines-0
- NIST: www.nist.gov
- IEEE: www.ieee.org
- IETF: www.ietf.org
- IEC: www.iec.ch
- ISO: www.iso.org
- TIA: www.tiaonline.org
- BIS: www.bis.org.in
- ITU: www.itu.int
- CEN: www.cen.eu
- CENELEC: www.cenelec.eu
- ETSI: www.etsi.org
- OMA: www.openmobilealliance.org
- 3GPP: www.3gpp.org
- GSMA: www.gsma.com
- oneM2M: www.onem2m.org
- OASIS: www.oasis-open.org
- TSDSI: www.tsdsi.org
- ISA: www.isa.org

Bringing the "Internet of Things" to life requires a comprehensive systems approach - inclusive of intelligent processing and sensing technology, connectivity, software and services, standardized & harmonized architectures and frameworks along with a leading ecosystem of partners.

CEN - **European Committee for Standardization**

CENELEC – European Committee for Electrotechnical Standardization

ETSI - European Telecommunications Standards Institute

EC - European Commission

EFTA – European Free Trade Association

SESEI

C/o EBTC, DLTA Complex, 1st Floor, 1, Africa Avenue, New Delhi 110029

Tel: +91 11 33521525, Fax: +91 11 33521501,

www.sesei.eu