IoT and Smart Infrastructure

Standardisation Perspective

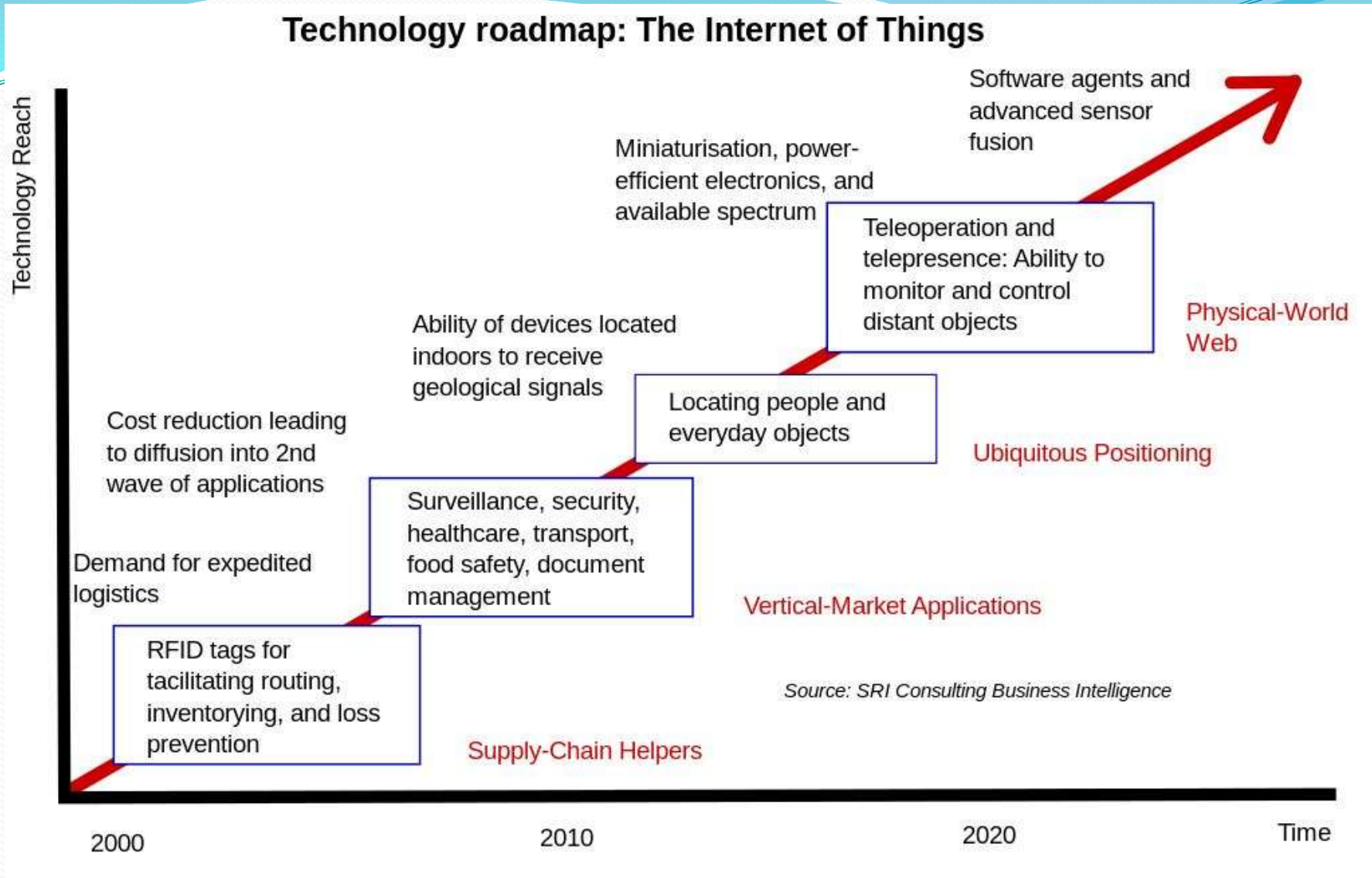
Aurindam Bhattacharya

Centre for Development of Telematics

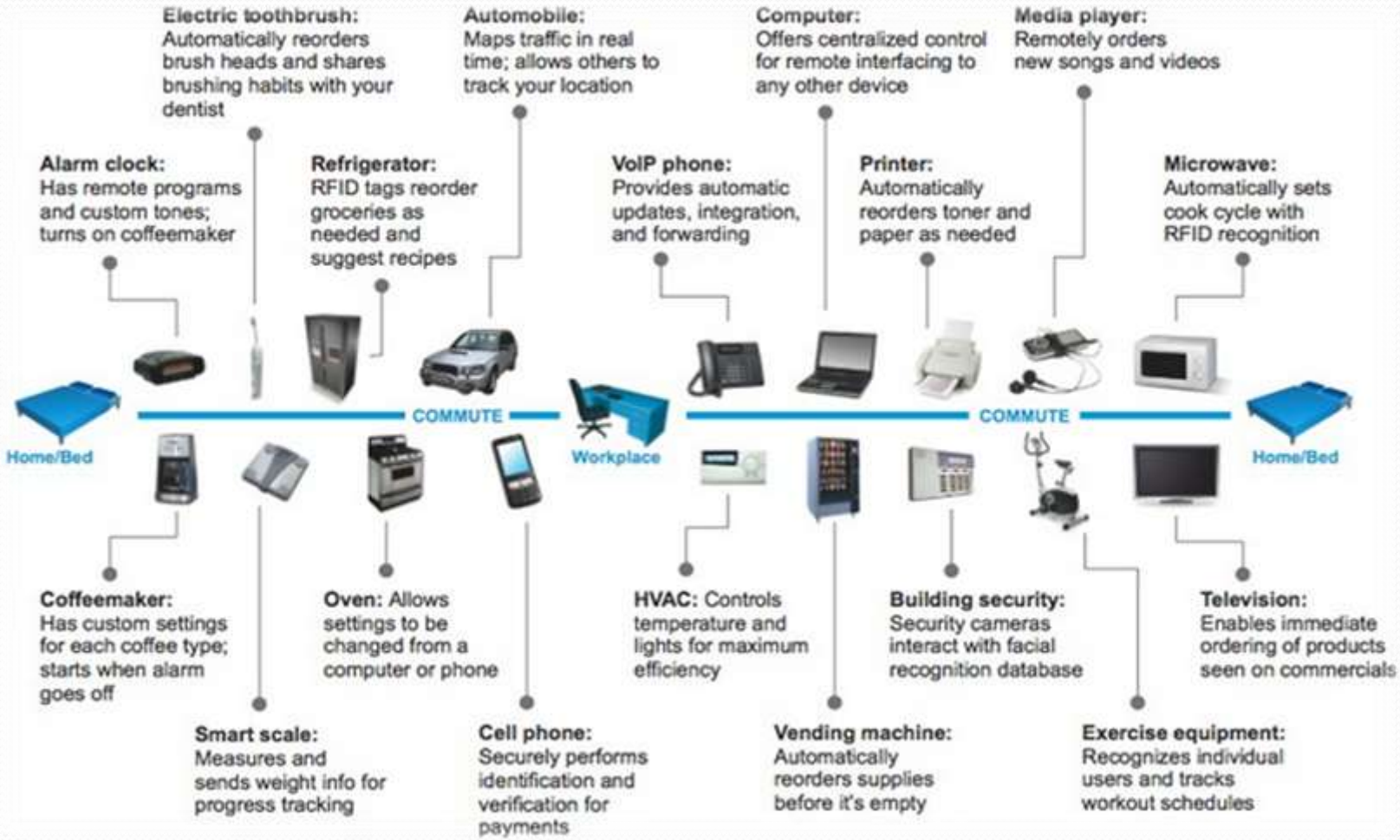
www.cdot.in

IoT- Internet of Things

- The Internet of Things (IoT) is the network of physical objects/devices, vehicles, buildings and other items—embedded with electronics, software, sensors with a network connectivity that enables these objects to collect and exchange data.
- British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto-ID centers, referring to a global network of objects connected to radio-frequency identification, or RFID)
- According to Gartner, The Internet of Things (IoT), would have an installed base that will grow to 26 billion units by 2020.
- ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of Things by 2020.


Technology roadmap: The Internet of Things
Technology Reach
Software agents and advanced sensor fusion
Miniaturisation, power-efficient electronics, and available spectrum
Teleoperation and telepresence: Ability to monitor and control distant objects
Physical-World Web
Ability of devices located indoors to receive geological signals
Locating people and everyday objects
Ubiquitous Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
Demand for expedited logistics
RFID tags for tacilitating routing, inventorying, and loss prevention
Supply-Chain Helpers
Source: SRI Consulting Business Intelligence
2000
2010
2020
Time

So What does Smart Infrastructure Mean to us

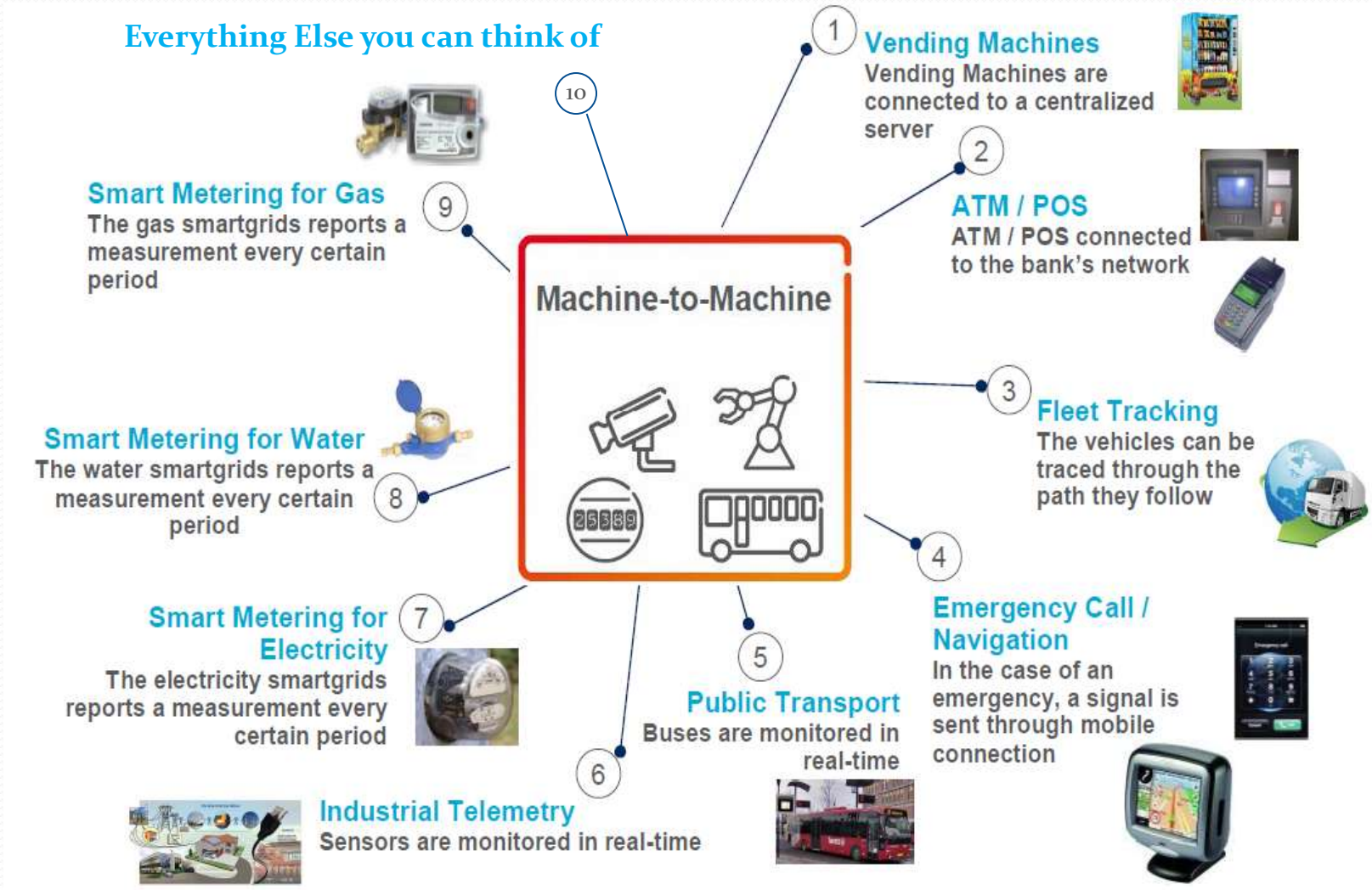


More Devices than people

- Smart phones 
- Smart Tablets 
- Smart desktops and Laptops 
- Data-enabled phones 
- Smart Consumer appliances 
- Embedded systems
- Sensors 

- RFID 

Potential Smart Infrastructure services



View Of 2020 and Beyond : EVERYTHING connected

Drivers

- Entertainment, security, healthcare,
- Productivity, new revenue streams
- Sustainability and regulation

Devices connecting the masses, such as Consumer Electronics and Home Automation

Specialized IoT/M2M applications across all government, industry & society

Enablers

- Ubiquity of Broadband
- Declining cost of connectivity
- Propagation of embedded IoT/M2M Devices

Technology Trends

- Field Domain
  - Sensor Technologies –Long (endless!) battery life, Self healing, Secure, Adaptive
  - Wireless Technologies like Sensor Networks, Wi-Fi, Zigbee, 6 LowPAN , LoRa etc.
- Infrastructure Domain
  - Evolving (It has to change significantly in order to cater to the needs of the huge explosion of IoT)
- Head End
  - Cloud, Big Data, New Age Analytics

Trends envisaged for IoT/M2M Technologies

- Towards 2020, technological development will be shaped by the force-multiplying effects of:
  - The convergence of nanotechnology, biotechnology, materials technology, and information and communications technology.
  - The acceleration of technological development.
  - Growing information exchange between developed and developing countries.
  - Developing countries participating in technology development

Towards 2020 we expect to see major progress in intelligent technology, such as

- Nearfield communication (NFC) sensors,
- smart surveillance and security applications and
- Smart robots,

which will enable automation of more activities. Technology will take over more domains and functions as robot technology improves in quality and stability and prices for advanced technologies decline and labour costs increase.

Consequences of IoT Innovation for the industry

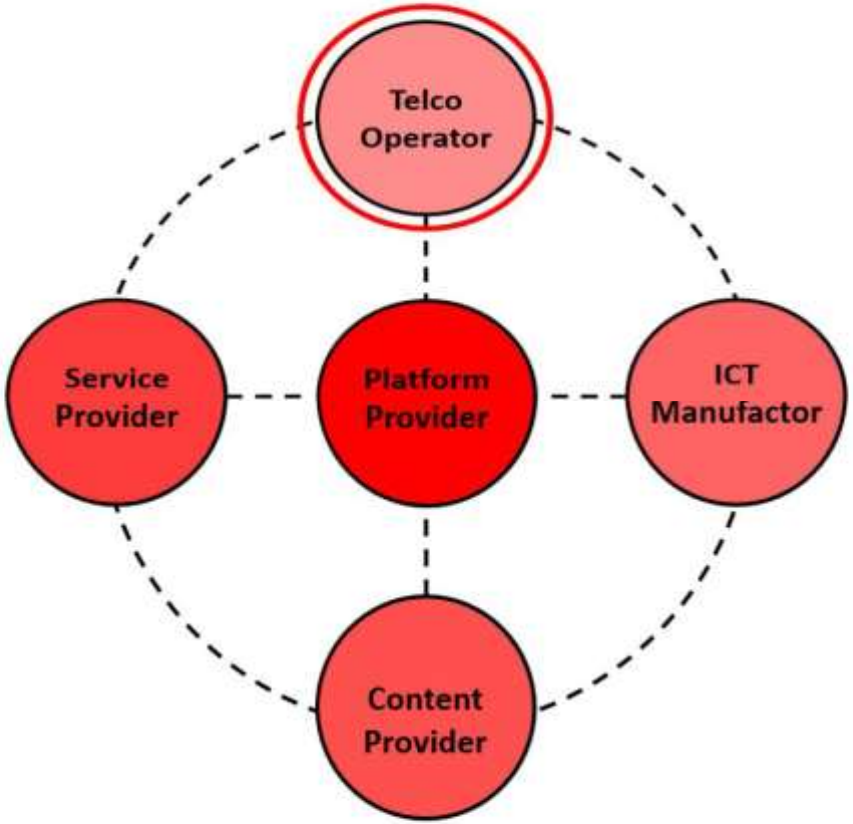
The development of the Internet of Things and ambient intelligence will allow managers to develop a much better understanding of how people are using buildings, cars, wearable devices etc. leading to new maintenance approaches, better designs, and more productive and cost effective technologies.

This development will also lead to a number of ethical and security challenges, for which industry should develop contingency plans.

For example:

i. Which data are you permitted to store, and for how long?
ii. Who owns the data collected from individuals?
iii. Who is responsible for securing and protecting these data?

Stakeholders of IoT/M2M



The Actual Scenario

All are hidden behind the wall and the users are without any choice

IoT/M2M Service Recipient

IoT/M2M Service Provider

Platform Provider

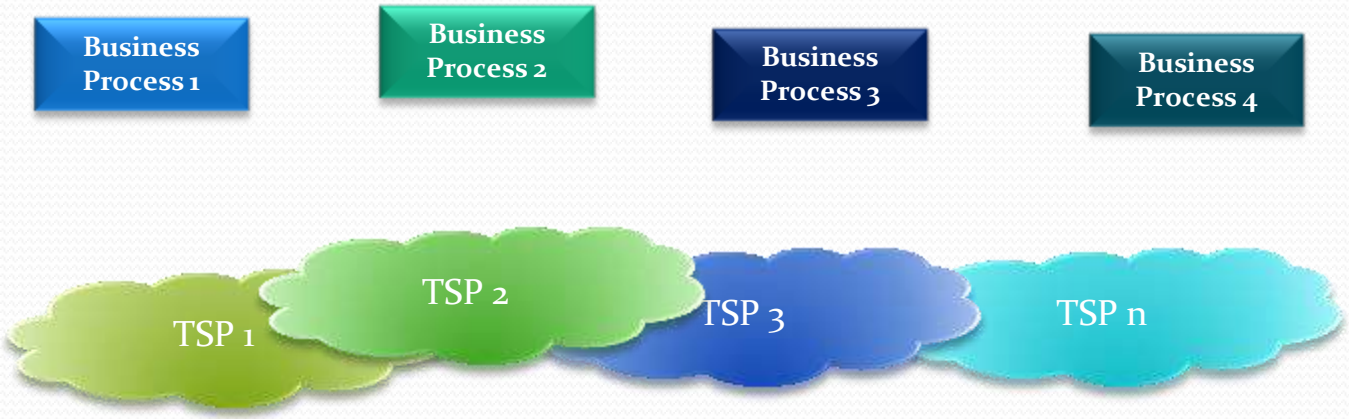
Device Manufacturer

Application Provider

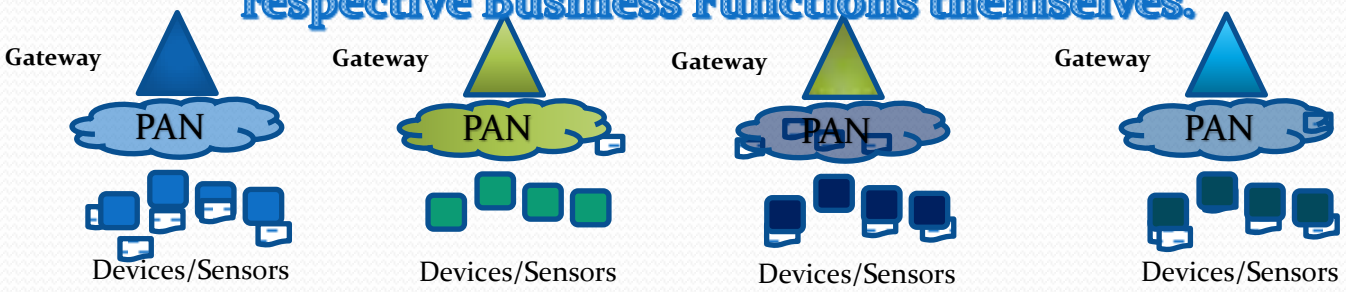
Telecom Service Provider

Present Landscape of Non-standardised M2M/IOT Deployment

A lot of traffic (upload) gets generated in proprietary manner from the sensors to the respective Servers running the business process.
Here the TSPs/ISPs networks are used as mere transport.

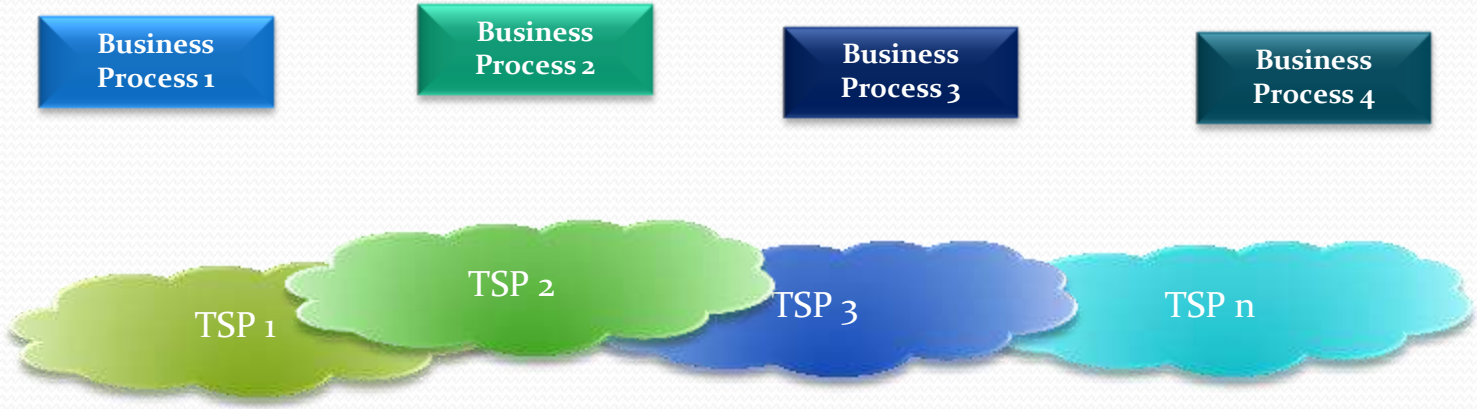


No interoperability....No Common Service Function
The registration, discovery, security etc are taken care of by the respective Business Functions themselves.

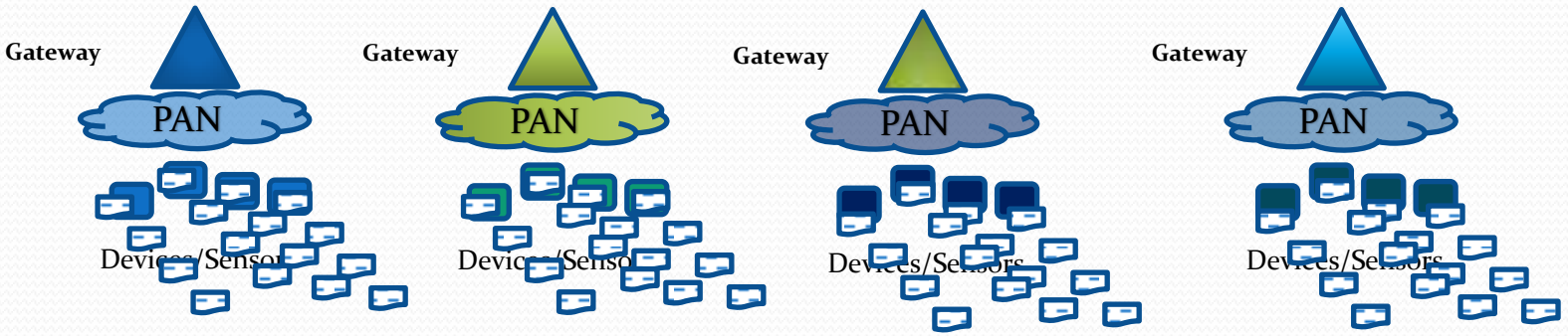


Present Landscape of Non-standardised M2M/IOT Deployment

Now imagine the data being shared between multiple business processes



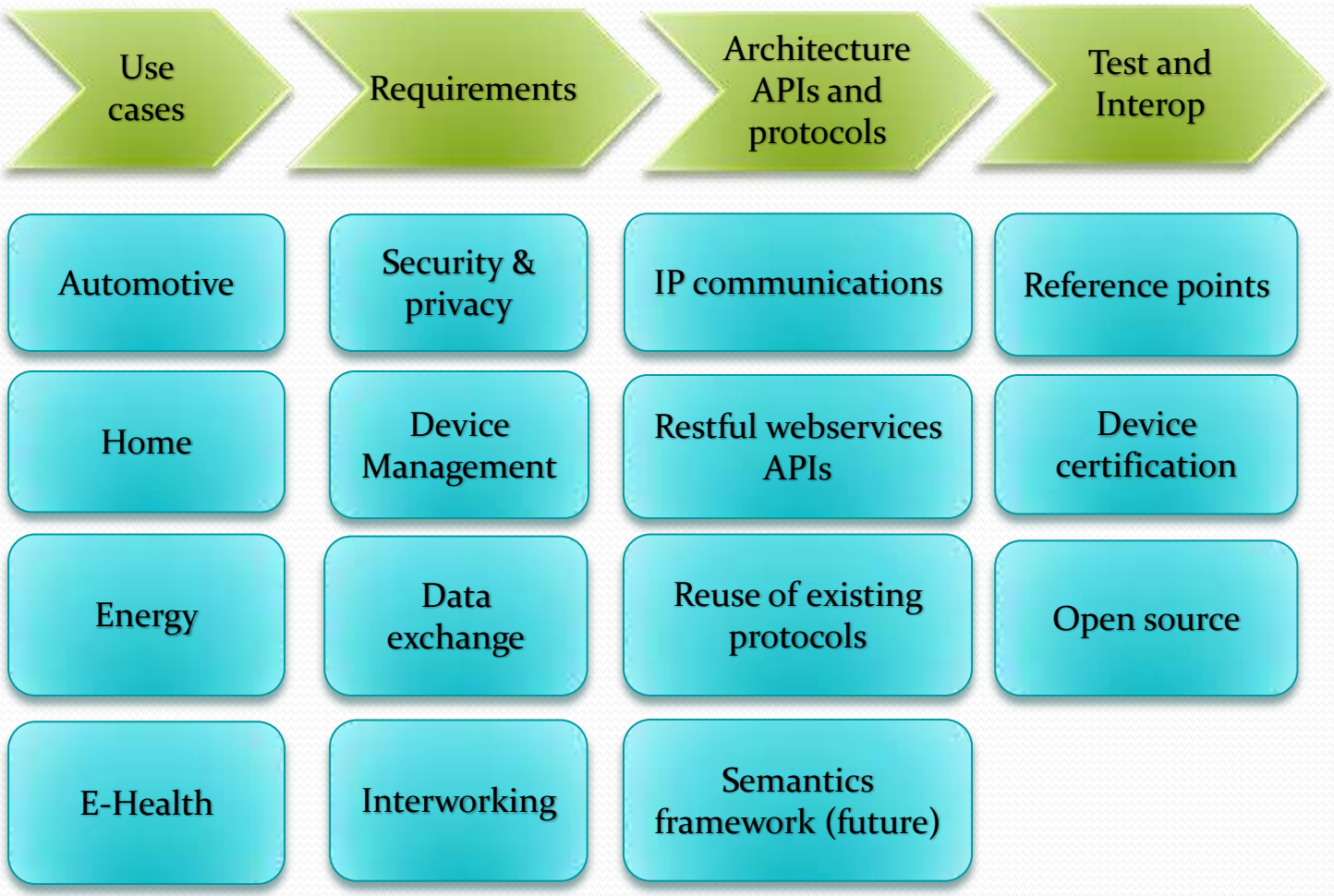
And there are billions of these devices…!!



Need For Standardisation

- So far the IoT/M2M industry is vertical Centric and the Telecom Network is merely used as a transport. However, these networks may need to be optimised to cater for these new solutions which have very different behaviour from what is currently prevailing.
- Standardization is required in order to deliver cost-effective IoT/M2M solutions, and allow this market to take off.
- Many component-level standards already exist, addressing various radio interfaces, different meshed or routed networking choices, or offering a choice of identity schemes. Each is optimised for a particular application scenario and there is therefore a degree of fragmentation.
- Now, efforts are being made by SDOs like OneM2M to bring all these pieces together, and identify the standardization gaps which exist.

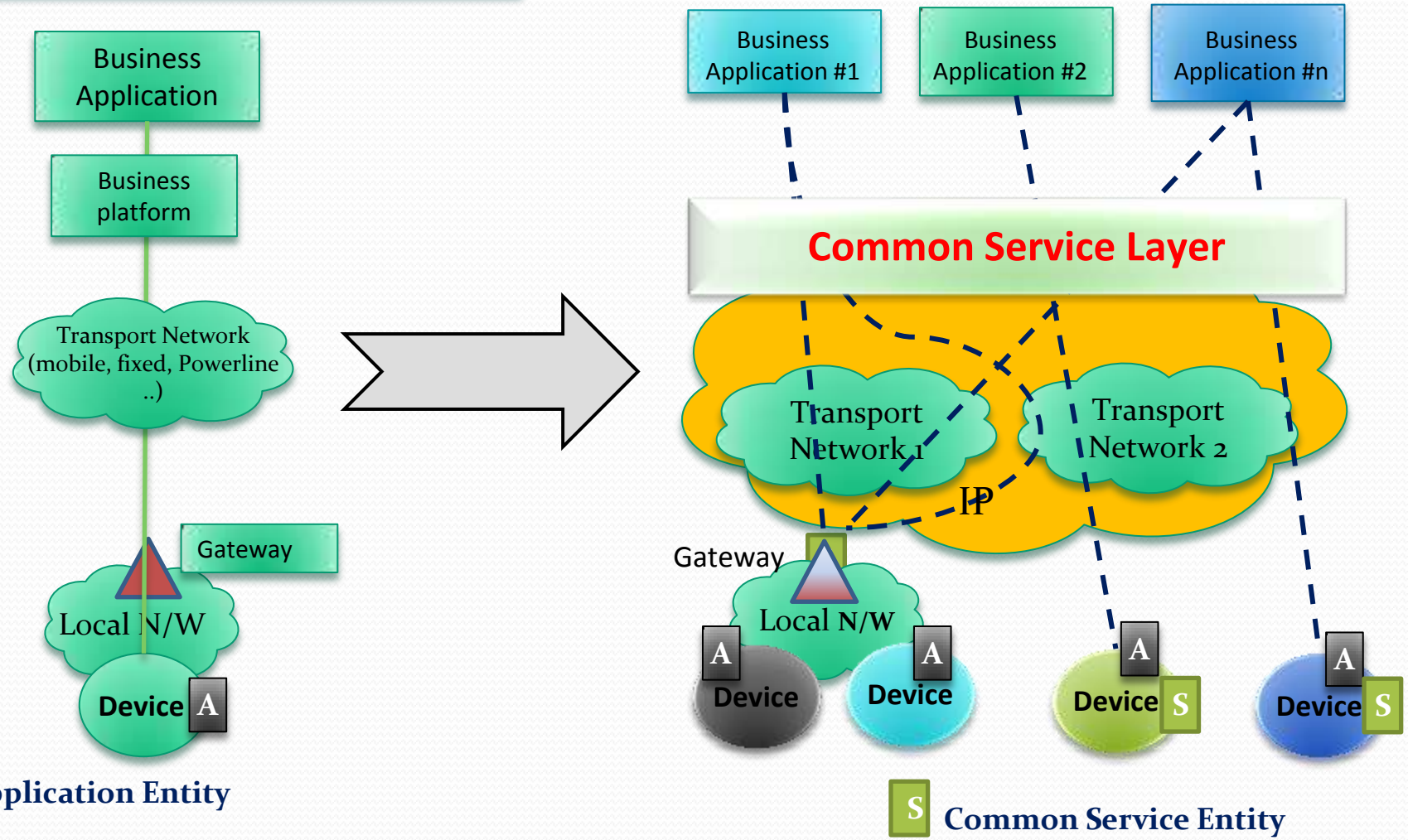
Standardization approach



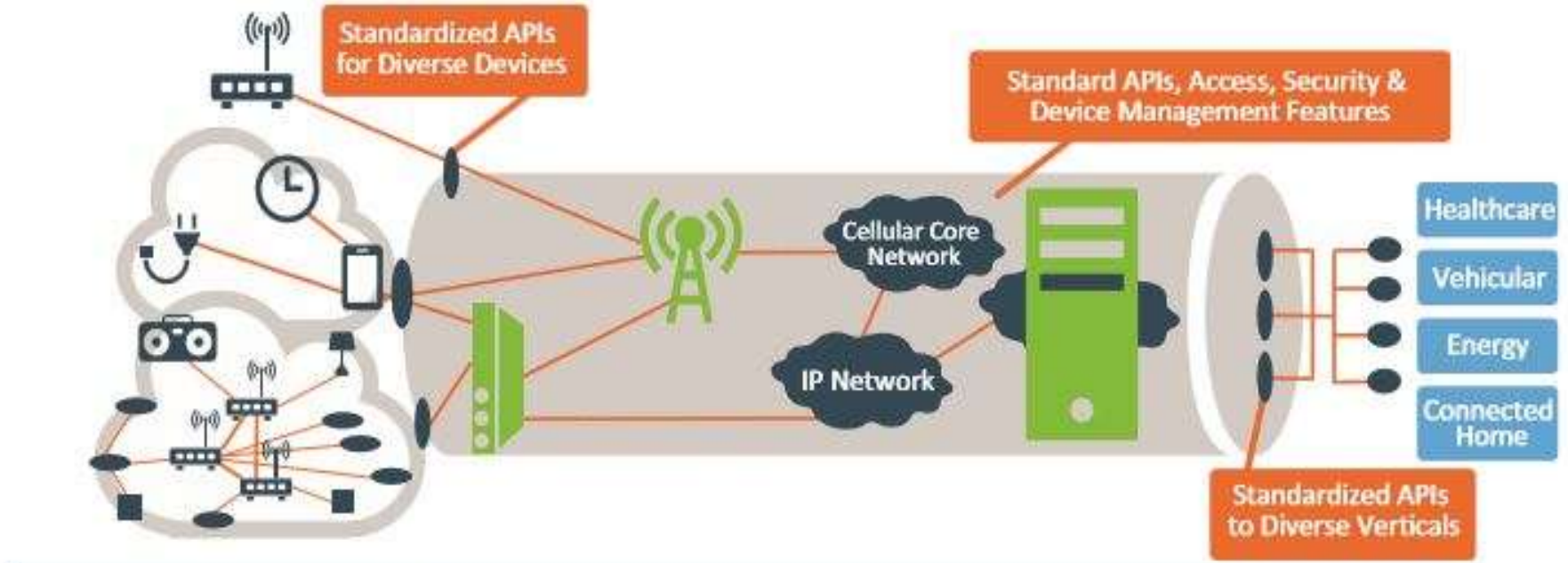
Landscape of IoT/M2M Architecture

Pipe (vertical):
1 Application, 1 NW,
1 (or few) type of Device

Horizontal (based on common Layer)
Applications share common infrastructure, environments, network elements & data



Standard End to End IoT/M2M Solution



M2M Devices

Cellular, WLAN, WPAN (Zigbee, 6LoWPAN, Bluetooth), Wireline

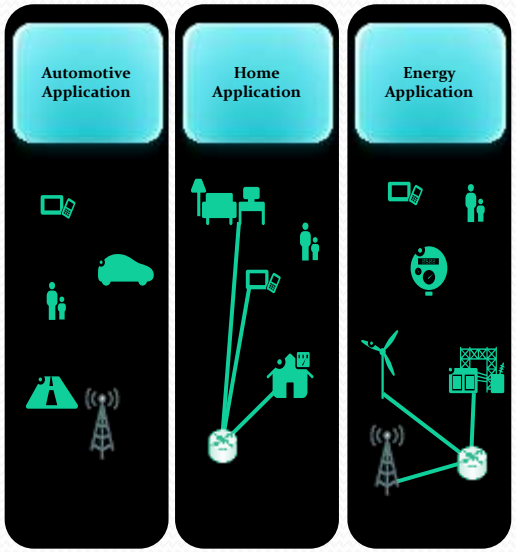
M2M Gateway

Enables cellular & non-cellular M2M devices to communicate through operator networks. Provides localized Service Capabilities to offload network

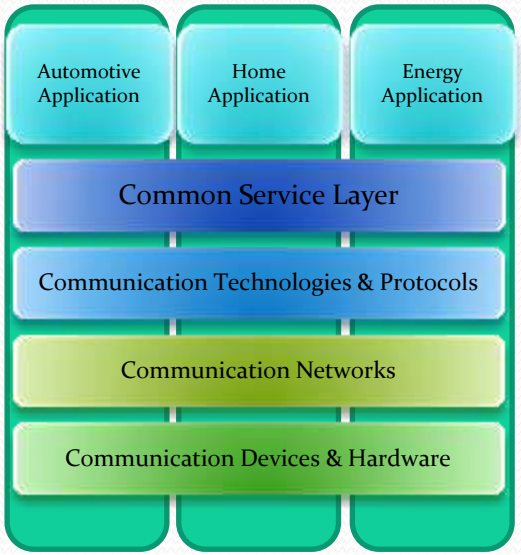
M2M Server

Service Provider's M2M Service Platform, offering Service Capabilities to Diverse M2M Verticals (Device/Data Access, Device Managment, Security, Billing, Service Discovery, etc.)

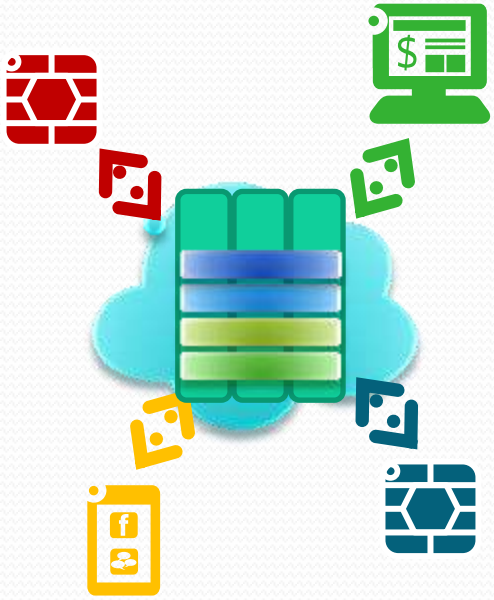
Standard Based Architecture approach



Currently developed solutions are similar are vertically integrated, with limited integration of data models (Zigbee, DLMS for smart meters, etc.).



Horizontal framework, Restful API
Objects represented as resource
Access control policy to access resource



IoT will be based on ontologies (formal description of concepts and relationships, e.g. W3C Semantic Sensor Network) as well as big data frameworks

TOMORROW

IoT ready

IoT enabled

What is oneM2M ?

- A global partnership among Standards Defining Organizations (SDOs) and Industry Associations like :

  ARIB (Association of Radio Industries and Businesses, Japan), ATIS (Advancing Transformation of the ICT Industry, America), CCSA (China Communications Standards Association, China), ETSI (European Telecommunications Standards Institute, Europe), TIA (Telecommunication Industries Association, America), TSDSI (Telecommunications Standards Development Society, India), TTA (Telecommunications Technology Association, Korea), and TTC (Telecommunications Technology Committee, Japan).

  Additional partners contributing to the oneM2M work include: the BBF (Broadband Forum), Continua, GlobalPlatform, HGI (Home Gateway Initiative), the New Generation M2M Consortium - Japan, and OMA (Open Mobile Alliance).

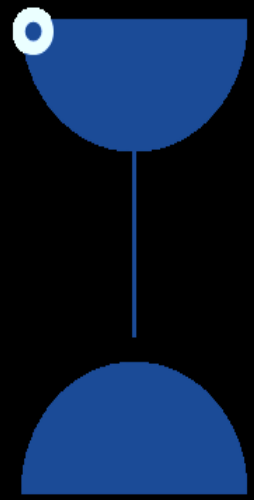
  [C-DOT is also partner Type I (through TSDSI) contributing to the standards]

- In simple terms the main goal to develop technical specifications for an IoT/M2M Service Layer
  - A software platform to make IoT/M2M devices/applications communicate with each other in a secure and efficient manner

"ANY APP"

"ANY NETWORK"

"ANY DEVICE"



application creation & analytics

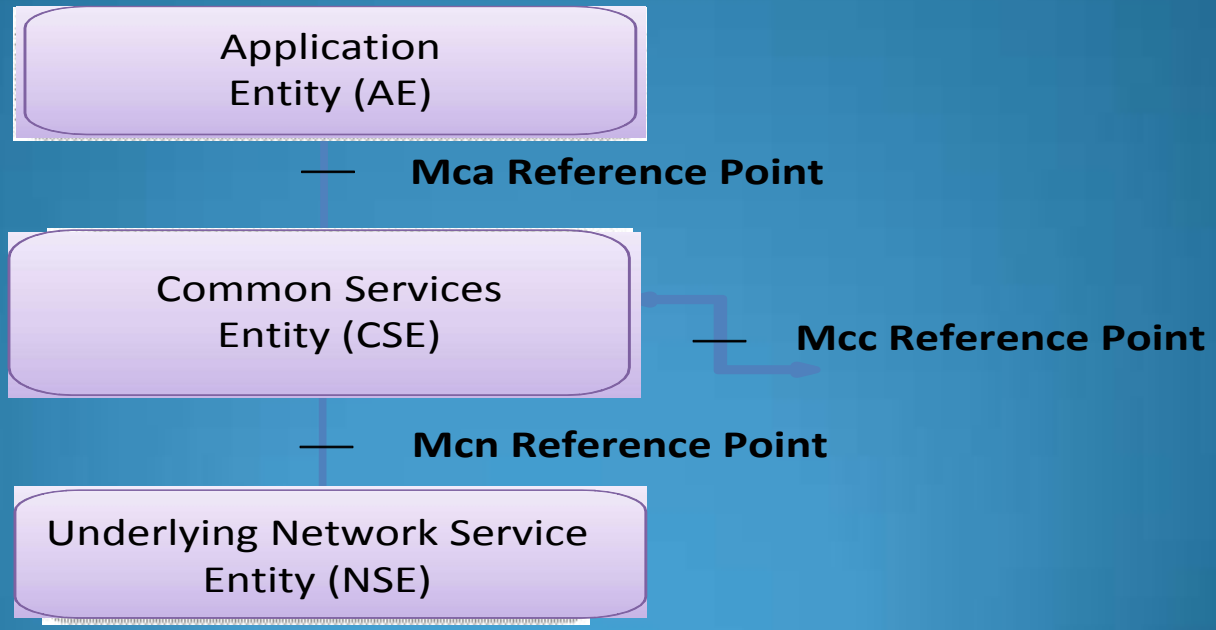
connectivity, onboarding, AAA, management, security, ...

devices & gateways

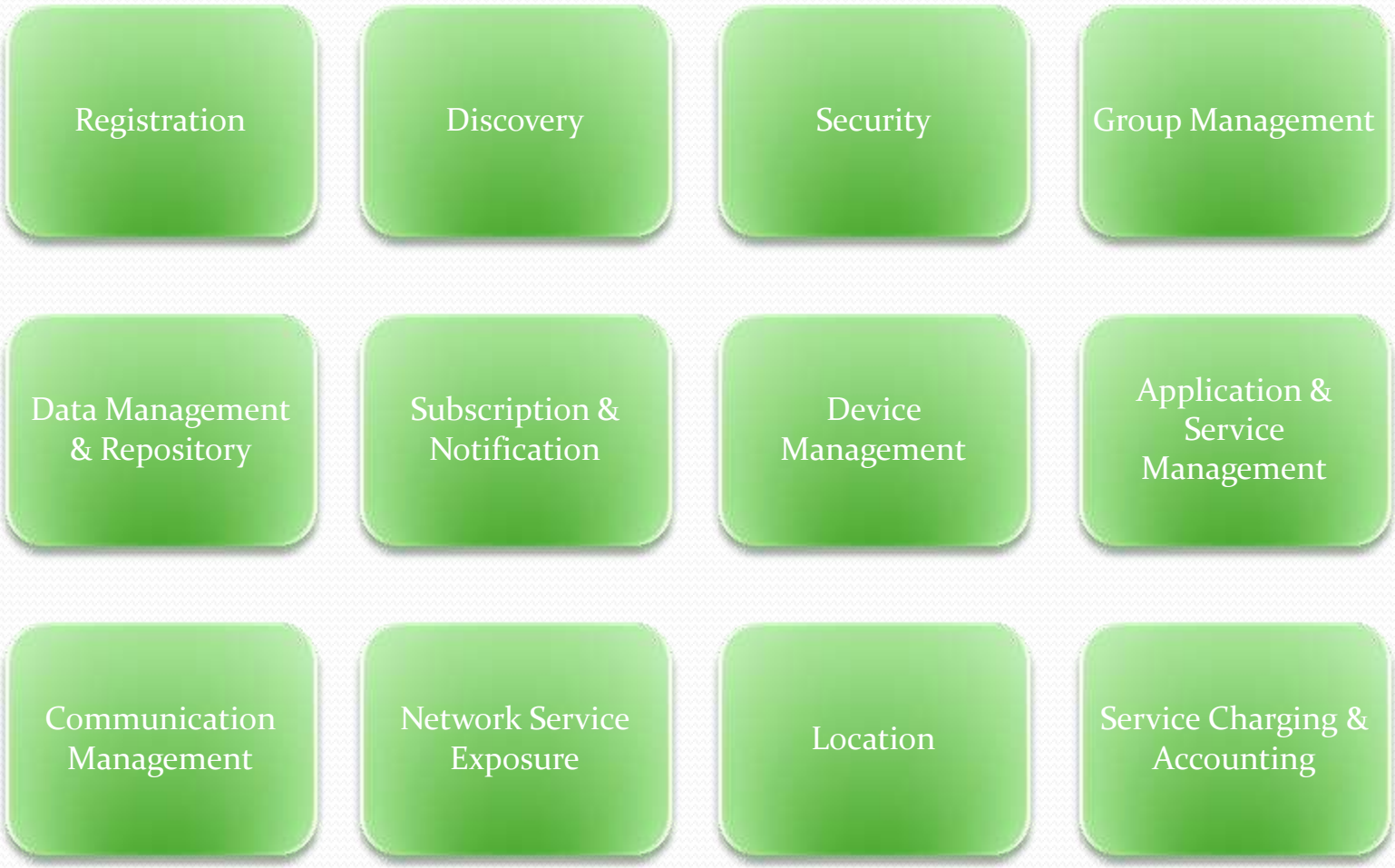
sensors

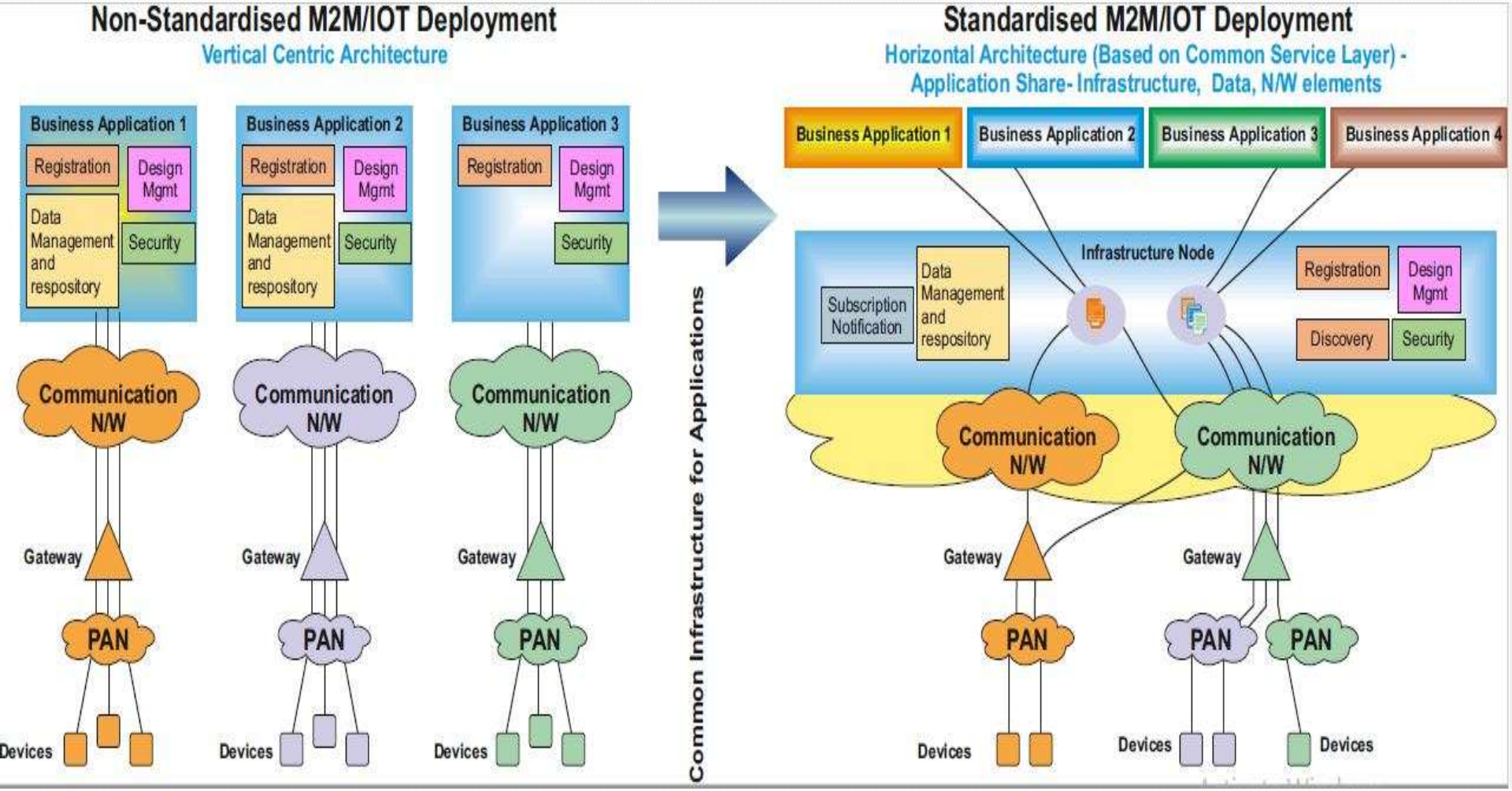
Layered model for high-level architecture of oneM2M

- **CSE (Common Service Entity):**
  - Offer common functionalities exposed through the Reference Points.
  - CSE contains Common Service Function Modules (CSF).
  - CSE and CSF are represented by Restful resource management and message flows.



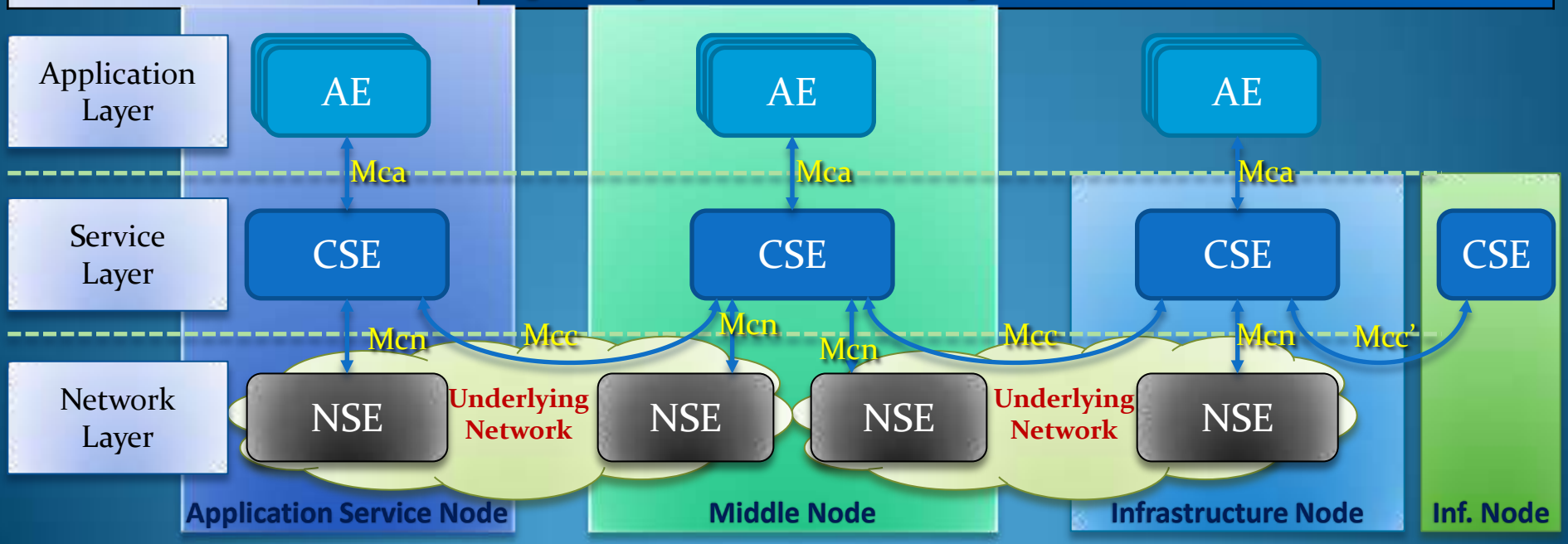
Common Service Functions



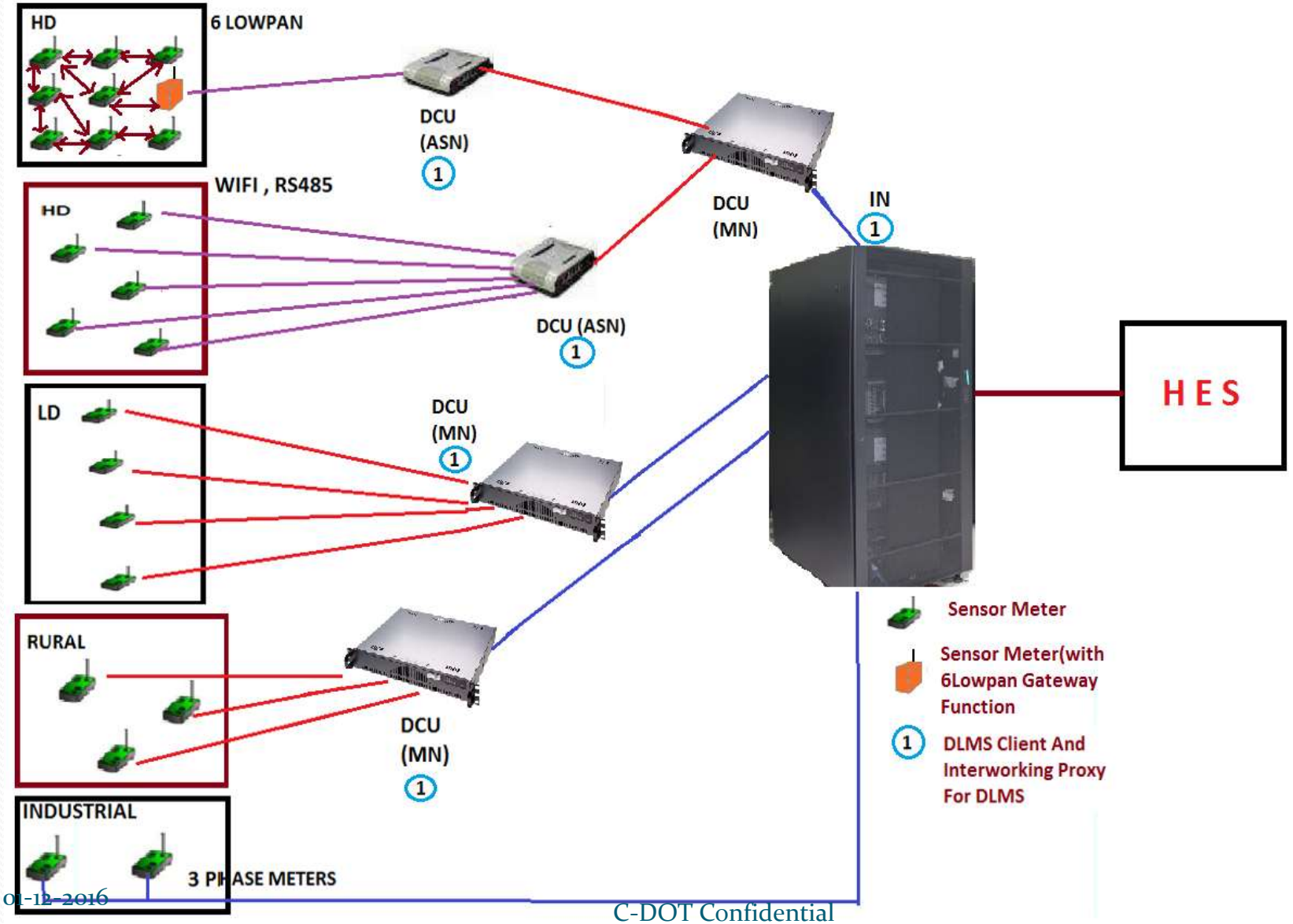

Non-Standardised M2M/IOT Deployment
Vertical Centric Architecture
Business Application 1
Registration
Design Mgmt
Data Management and respository
Security
Business Application 2
Registration
Design Mgmt
Data Management and respository
Security
Business Application 3
Registration
Design Mgmt
Security
Communication N/W
Communication N/W
Communication N/W
Gateway
Gateway
Gateway
PAN
PAN
PAN
Devices
Devices
Devices
Common Infrastructure for Applications
Standardised M2M/IOT Deployment
Horizontal Architecture (Based on Common Service Layer) -
Application Share- Infrastructure, Data, N/W elements
Business Application 1
Business Application 2
Business Application 3
Business Application 4
Infrastructure Node
Subscription Notification
Data Management and respository
Registration
Design Mgmt
Discovery
Security
Communication N/W
Communication N/W
Gateway
Gateway
PAN
PAN
PAN
Devices
Devices
Devices

Architecture

Reference Point	One or more interfaces - Mca, Mcn, Mcc and Mcc' (between 2 service providers)
Common Services Entity	Provides the set of "service functions" that are common to the IoT/M2M environments
Application Entity	Provides application logic for the end-to-end IoT/M2M solutions
Network Services Entity	Provides services to the CSEs besides the pure data transport
Node	Logical equivalent of a physical (or possibly virtualized, especially on the server side) device



Typical IoT/M2M use case in Power Sector using C-DOT IoT/M2M Solutions



C-DOT's IoT/M2M Offering

- A Standard based IoT/M2M Platform
  - Middle Node (Gateway in the Device Domain)
  - Infrastructure Node (in Infrastructure Domain)

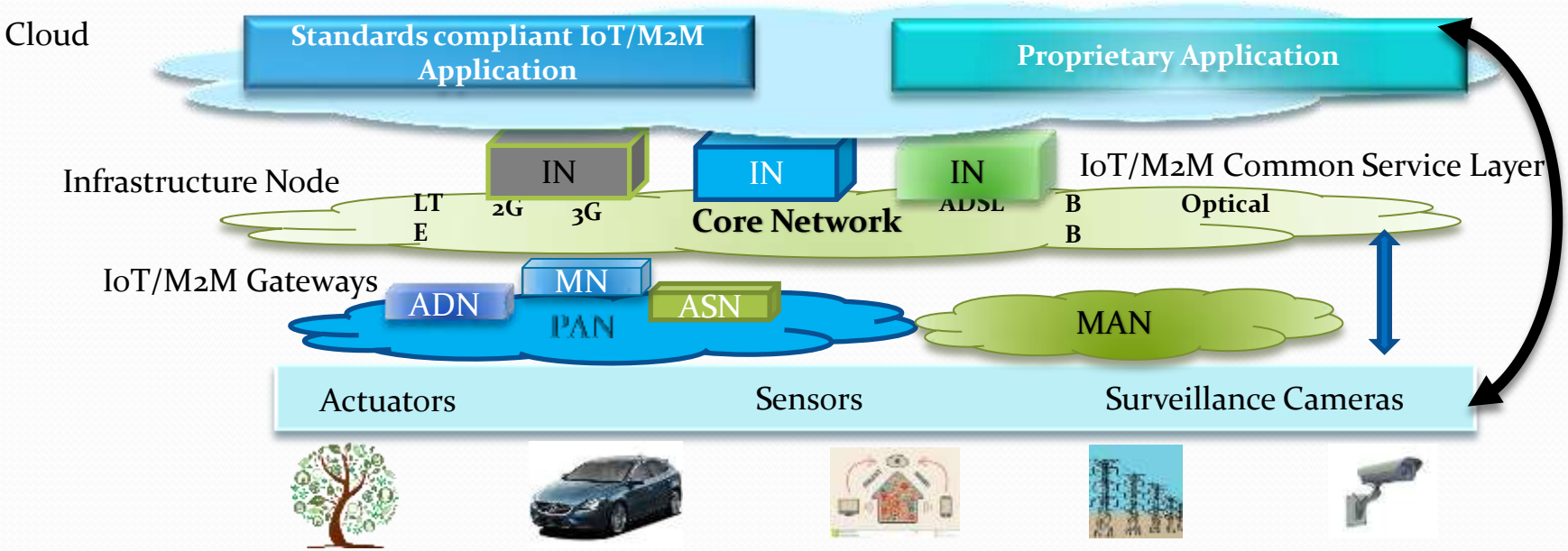
  Having the Common Service Entity (Common Service Layer) providing the Common Service Functions described above.

  It would enable the industry to develop Standard based Applications which would reduce the development, test and deployment lifecycles

Advantages of C-DOT IoT/M2M Platform

Combat fragmentation	• Healthy eco-system with economies of scale • More partnering choices and opportunities for M2M/IOT industry stakeholders
Lower CAPEX	• Standardized protocols / APIs -> simplifies application development/deployment • Cross-vertical standards -> same devices and back-ends in different industries
Lower OPEX	• Standard features to use networks more efficiently -> get better tariffs • Flexibility for verticals -> utilize best transport network meeting business needs
Time to Market	• Reduced development, test and deployment lifecycles through focusing on core business (application logic)

Typical Standards' Compliant Smart City Architecture



Thank You