IoT
Internet of Things Egypt

Internet of Things Egypt Forum

Meeting-01 22-01-2015

Content

1 Overview & Scope

2 Infrastructure & Technologies

3 Governance & Legislation

4 Business Models & Applications

IoT

Internet of Things Egypt

IoT Infrastructure

Requirements & Technologies

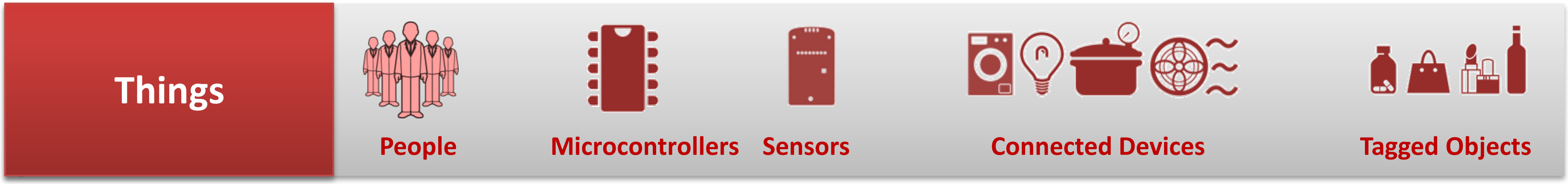
IoT Infrastructure Main Components

Applications	Social Media, Web, Mobile, Enterprise, Industrial
Services	Cloud Services Security
Middleware	Data management, Context Management
Connectivity	Protocols Telecom
Things	People Microcontrollers Sensors Connected Devices Tagged Objects

Internet of Things Egypt

Software Engineering Competence Center

IoT Infrastructure Main Components - Things



Things

People

Microcontrollers

Sensors

Connected Devices

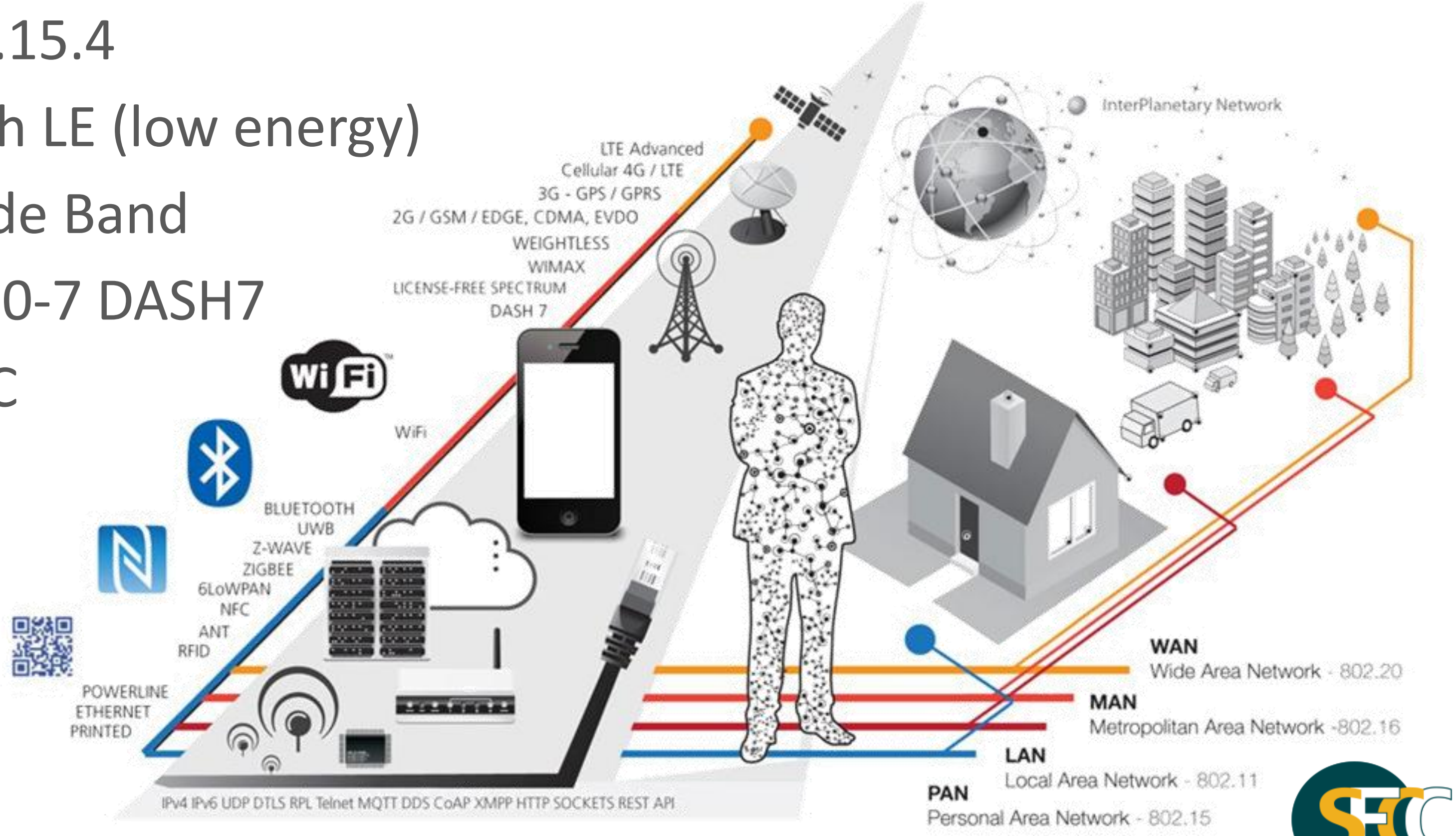
Tagged Objects

- □ Embedded Systems
- □ Wireless Sensor Networks
- □ Smart Objects
  - Tagged objects (NFC / RFID)
  - Sensor Enabled Devices
- □ Micro and Nano electronics
- □ Photonics
- □ Biotechnology
- □ Advanced Materials
- □ Advanced Manufacturing Systems

IoT Infrastructure Main Components - Connectivity

Connectivity | **Protocols Telecom**

- Main concern is low power communication
  - IEEE 802.15.4
  - Bluetooth LE (low energy)
  - Ultra Wide Band
  - ISO 18000-7 DASH7
  - RFID/NFC


InterPlanetary Network
LTE Advanced
Cellular 4G / LTE
3G - GPS / GPRS
2G / GSM / EDGE, CDMA, EVDO
WEIGHTLESS
WIMAX
LICENSE-FREE SPECTRUM
DASH 7
Wi Fi
WiFi
BLUETOOTH
UWB
Z-WAVE
ZIGBEE
6LoWPAN
NFC
ANT
RFID
POWERLINE
ETHERNET
PRINTED
IPv4 IPv6 UDP DTLS RPL Telnet MQTT DDS CoAP XMPP HTTP SOCKETS REST API
WAN
Wide Area Network - 802.20
MAN
Metropolitan Area Network -802.16
LAN
Local Area Network - 802.11
PAN
Personal Area Network - 802.15

IoT Infrastructure Main Components - Middleware

Middleware

Data management, Context Management

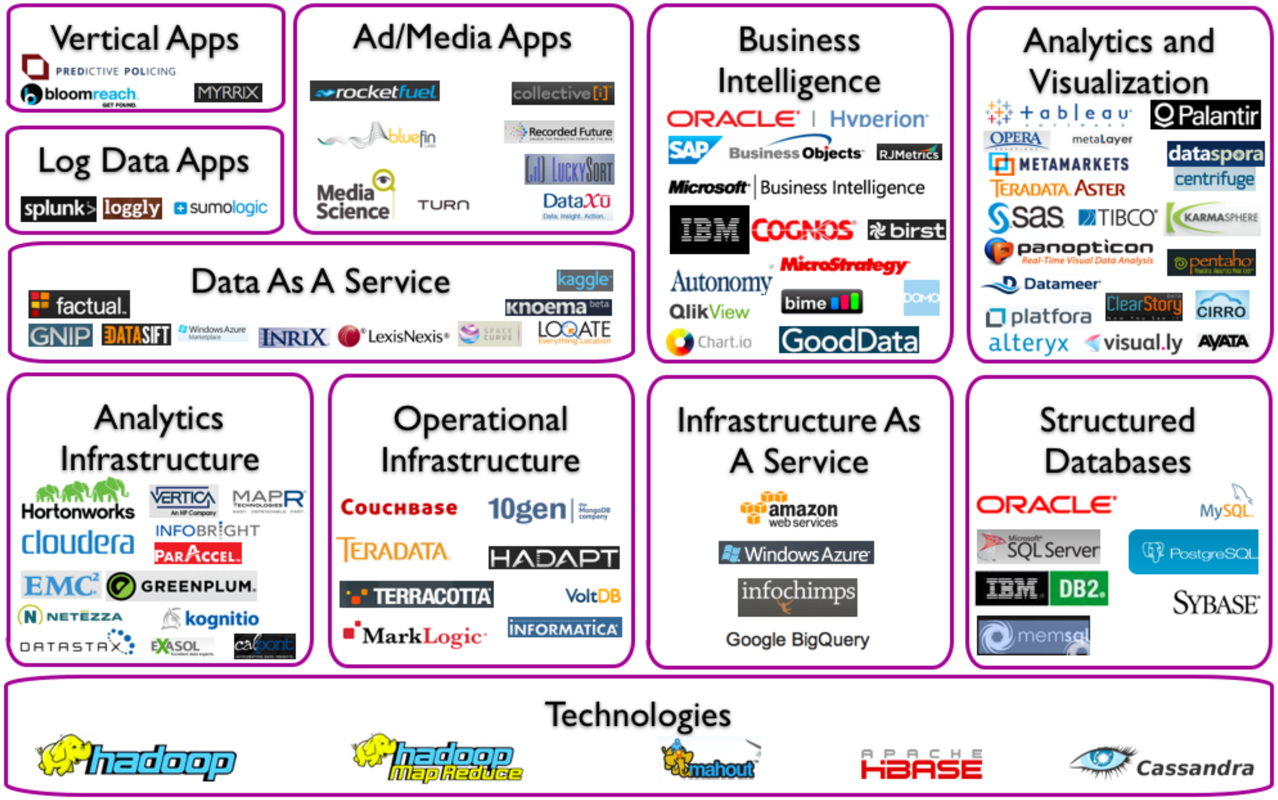
- Middleware Requirements:
  - Hide low-level sensing details
  - Device virtualization
  - Decouple producer and consumer of M2M device data
  - Extendibility & Scalability
  - Interoperability
  - Multiple remote access
  - Appropriate protocols (MQTT, CoAP, RESTful HTTP, XMPP)
  - Big data management

IoT Infrastructure Main Components - Middleware

Middleware

Data management, Context Management

- Big Data



Copyright © 2012 Dave Feinleib dave@vcdave.com blogs.forbes.com/davefeinleib

IoT Infrastructure Main Components - Middleware

Middleware

Data management, Context Management

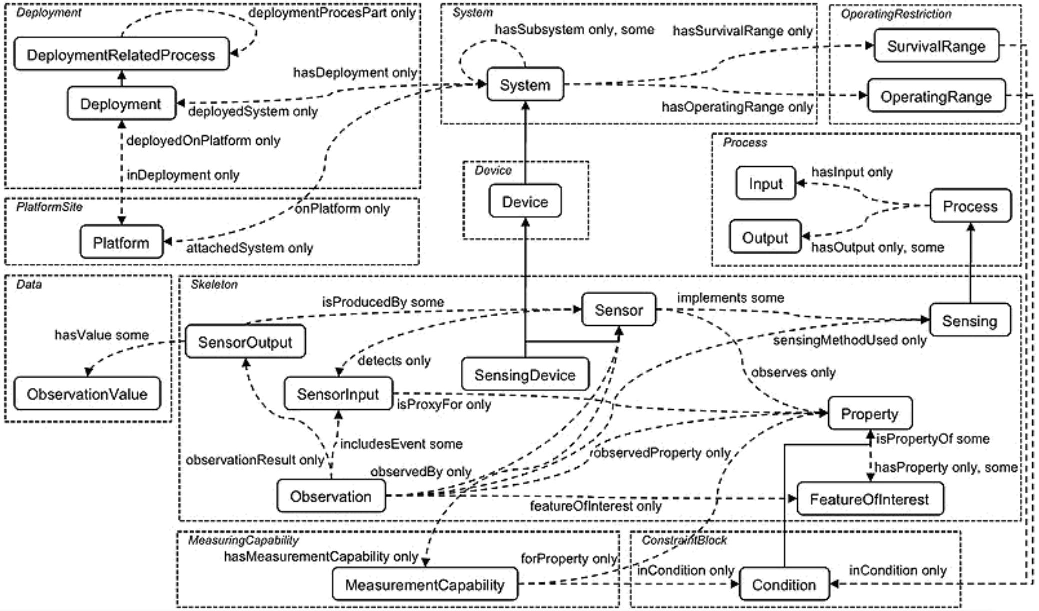
- Protocols (beside well known JMS,REST)
  - MQTT: Message Queue Telemetry Transport
    - Transfer messages via central broker
  - CoAP: Constrained Application Protocol
    - Client/server protocol like HTTP but for constrained devices
  - AMQP: Advanced Message Queuing Protocol
    - Application level message-centric brokered protocol
  - DDS: Data Distribution Service
    - Data-centric middleware language
  - XMPP: Extensible Messaging and Presence Protocol
    - XML based messaging protocol

IoT Infrastructure Main Components - Middleware

Middleware

Data management,
Context Management

- Semantic Sensor Networks & Semantic Annotation of Data
  - Use semantic technologies to annotate sensors with spatial, temporal semantic metadata
  - W3C Semantic Sensor Network Incubator Group is developing sensor ontology



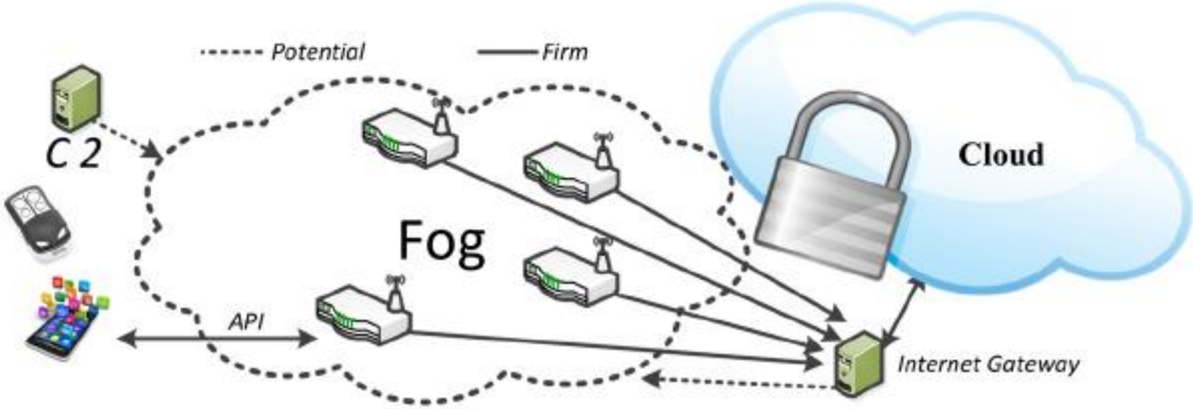
IoT Infrastructure Main Components - Services

Services

Cloud Services
Security

Cloud Services

- Emerging Services: Sensing-as-a-service & Object-as-a-service
- Moving towards Fog Computing Paradigm to cope with the need for mobility, geo-distribution, context awareness and low latency



IoT Infrastructure Main Components - Services

Services

Cloud Services

Security

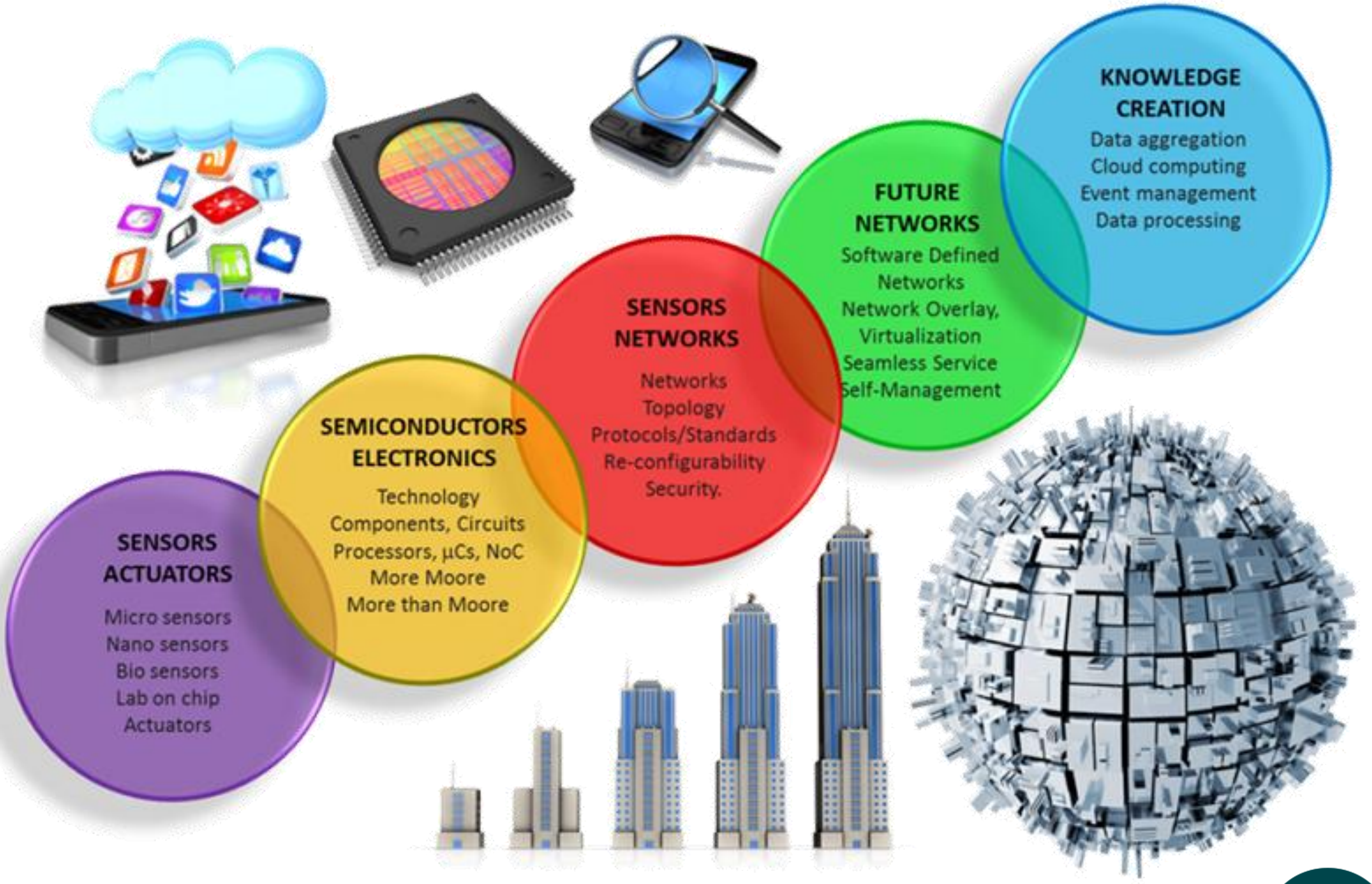
- Trust, Security & Privacy
  - Shifting towards cyber-physical systems will infer security vulnerabilities and threats that require light-weight scalable solutions
  - Trust: Light-weight Public Key Infrastructure and Management systems and Access Control
  - Security: Cyber-Situation awareness
  - Privacy: Cryptographic techniques, fine-grain & self configuring access control mechanisms

IoT Infrastructure Main Components - Applications

Applications

Social Media, Web, Mobile, Enterprise, Industrial

- Smart Cities
- Smart Transport
- Smart Buildings
- Smart Energy
- Smart Industry
- Smart Health



SENSORS ACTUATORS
Micro sensors
Nano sensors
Bio sensors
Lab on chip
Actuators

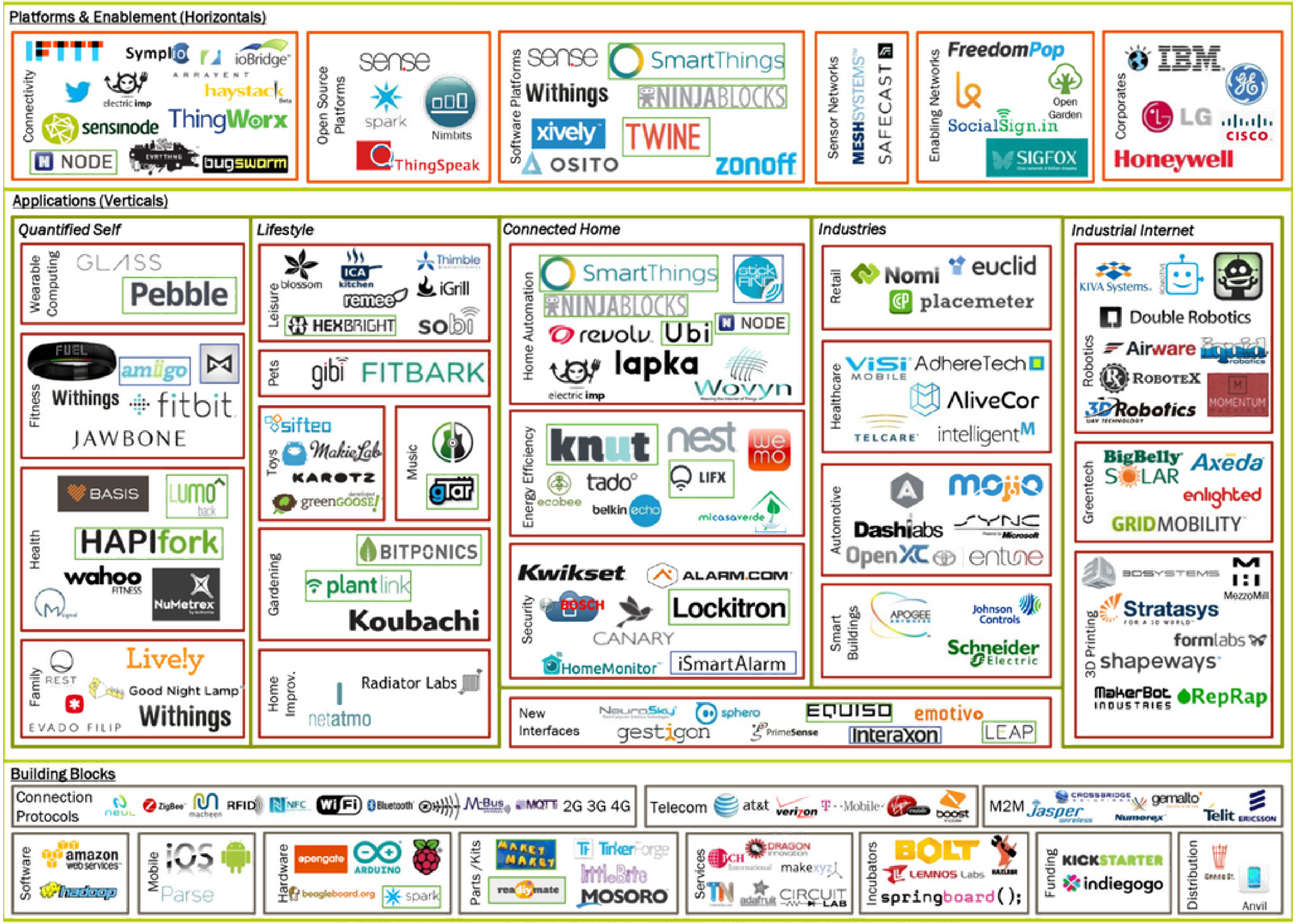
SEMICONDUCTORS ELECTRONICS
Technology
Components, Circuits
Processors, µCs, NoC
More Moore
More than Moore

SENSORS NETWORKS
Networks
Topology
Protocols/Standards
Re-configurability
Security.

FUTURE NETWORKS
Software Defined Networks
Network Overlay, Virtualization
Seamless Service
Self-Management

KNOWLEDGE CREATION
Data aggregation
Cloud computing
Event management
Data processing

IoT Landscape



© Matt Turck (@mattturck), Sutian Dong (@sutiandong) & FirstMark Capital (@firstmarkcap)

IoT Standardization and Legislation

Outline

- IoT Standardization Activities
  - ITU
  - ISO
  - ISO/IEC
  - IEEE
- IoT Legislation Aspects
  - Europe and U.S efforts in legislation

Internet of Things (IoT)

Standardization Activities

ITU and IoT – Standardization Activities

IoT GSI- IoT Global Standard Initiative

JCA-IoT - Joint Coordination Activity of the IoT

ITU-T Focus Group on the M2M service layer

ITU-T Study Group 2 : Numbering Naming, Addressing

ITU-T Study Group 11 : Testing Architecture for tag-based identification

ITU and IoT

ITU-T Study Group 16 – requirements and architecture for multimedia information access triggered by tag-based identification

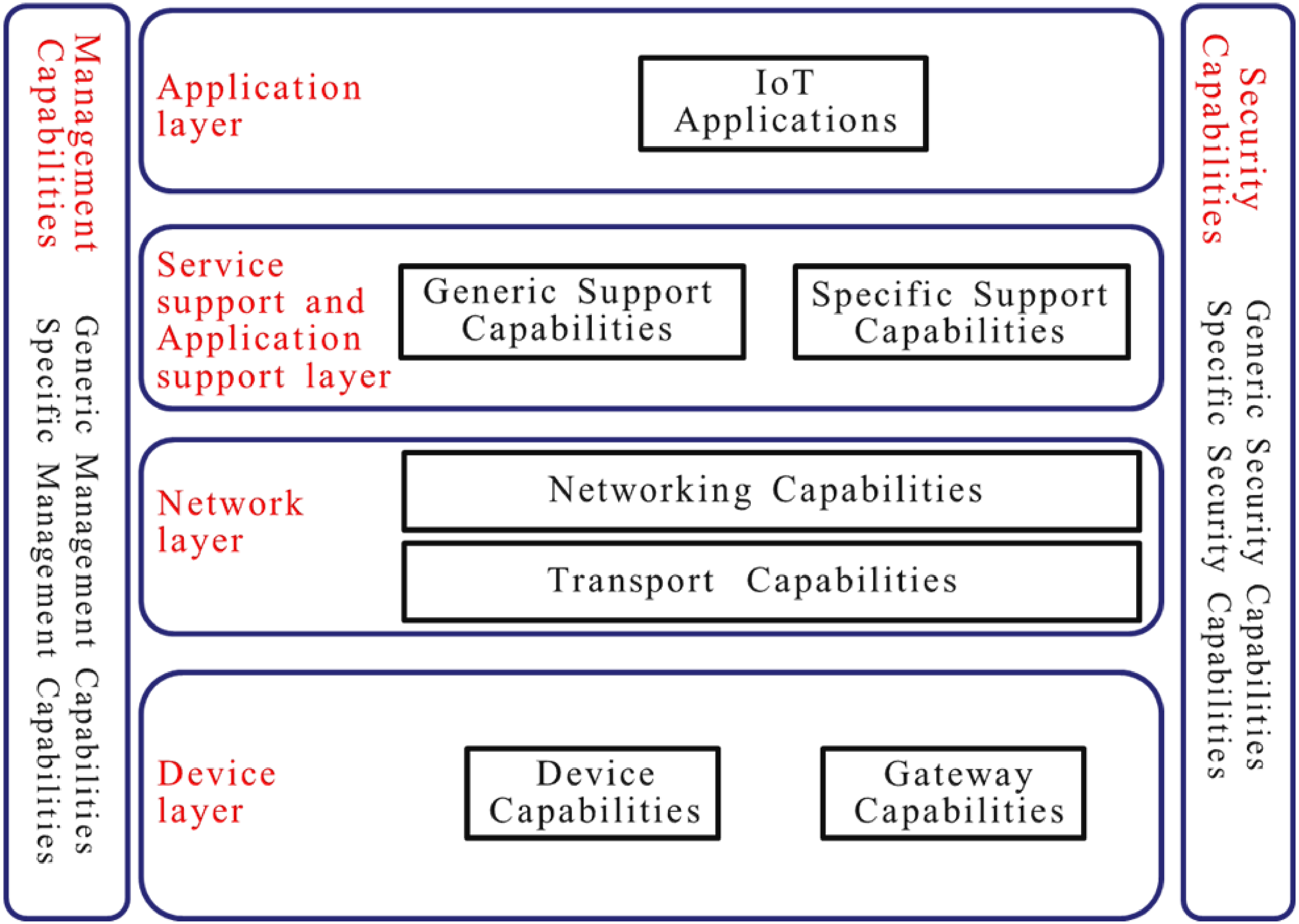
ITU-T Study Group 17 – security and privacy of tag-based applications

ITU-R : Global management of the radio frequency spectrum

ITU-T Study Group 13: NGN requirements and architecture for applications and services Using tag-based identification

ITU-T Study Group 13: NGN requirements and architecture for applications and services Using tag-based identification

IoT Reference Model


Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application layer
IoT Applications
Service support and Application support layer
Generic Support Capabilities
Specific Support Capabilities
Network layer
Networking Capabilities
Transport Capabilities
Device layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Security Capabilities
Specific Security Capabilities

(Source: ITU-T Y.2060)

ISO/IEC JTC 1/SWG 5 Internet of Things (IoT)

ISO/IEC JTC 1/SWG 5 Internet of Things (IoT)

- A standardization special working group (SWG) of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Develops and facilitates the development of standards for Internet of Things (IoT).
- Established in 2012 as a result of growing interest in the field of IoT by other standards organizations

- Examples of standards:
  - ISO/IEC NP 19654: Internet of Things Reference Architecture (IoT RA)
  - ISO/AWI 18575: Internet of Things (IoT) in the supply chain - Products & product packages
  - ISO/IEC JTC 1/SC 6: Telecommunications and information exchange between systems
  - ISO/IEC JTC 1 Information technology

IEEE Standards Association (IEEE-SA)

- Develops a variety of standards for IoT including:
  - IEEE 754™-2008 - IEEE Standard for Floating-Point Arithmetic
  - IEEE 802.11™-2012 - IEEE Standard for Information Technology Telecommunications and information exchange between systems
  - IEEE 1609.2™-2013 - IEEE Standard for Wireless Access in Vehicular Environments
  - IEEE 1905.1™-2013 - IEEE Draft Standard for a Convergent Digital Home Network for Heterogeneous Technologies
- The complete list of standards in this link: http://standards.ieee.org/innovate/iot/stds.html

IoT Legislation aspects

Need for a legal revolution

Internet of Things Egypt

Software Engineering Competence Center

From definition to legislation

A. "Connected“ objects

- Setting up a network of sensors and RFID chips will certainly raise a variety of issues:
  - Public health issue about the levels of exposure to Electro-Magnetic Field (EMF)
    - **Regulations** must be able to ensure that all devices and systems will respect the safety and health needs of the population in the future
  - The connections can be established in restricted areas or made publicly accessible
  - Liability for things
    - Numerous legislations recognize "liability for things“ as the liability of the owner in case of harm caused by things
    - What is new with IoT is that harm does not depend on things itself, but on the way that things will interpret, process and return the data received. The problem is that all these functions depend on settings on which the thing owner has no control.

From definition to legislation- *Identity of the thing*

B. Identity of the thing

- IoT requires that each object is uniquely and certainly identified and identifiable inside the network
  - Today, the elements connected to the network have three identifiers:
    - MAC address
    - a product identifier (e.g. a bar code)
    - a digital identifier (e.g. IP address).
- What will happen tomorrow when each thing will have an identity?

From definition to legislation- *Identity of the thing*

- Legal and regulatory questions raised about The ownership of the future new addressing system
  - Ex: The French Commission for the Liberalization of Growth initiated by former French President Nicolas Sarkozy urged the French government to ensure the **independence** and **confidentiality** of the operator managing the identities of the Internet of Things (radio frequency identification–RFID) as it will offer the possibility to trace identities and flows of transactions

From definition to legislation- *smart objects*

c. Smart objects: when the object is in charge

- □ A smart object would have two new functions
  - help the decision-making process
  - take decision for the human
- □ This will raise a lot of questions about the **liability**

In USA, the state of Nevada legalized self-driving cars in 2011 and in May 2012 granted America's first self-driven car license to a Google car. In the event of an accident, law-enforcement authorities and insurers will have to decide who will be held liable: the car manufacturer, the "smart“ car...? And this is just the beginning as other U.S. states are also considering the legalization of self-driving cars

Internet of Things Egypt

Software Engineering Competence Center

From definition to legislation- *privacy*

D. Privacy

- □ The most obvious legal issues in IoT **concern privacy and security**.
- □ IoT has the potential to generate large amounts of personal information that has serious implications for consumers.
  - ▣ IoT data may include an individual's identity, location, medical issues, sexual orientation, socioeconomics or political profile.
  - ▣ It might include a live video feed, or report whether doors and windows are locked.
- □ It would not be sufficient to penalize illegal access to personally-identifiable data as it is the case today.

It would be required to punish the action of placing connectors and other chips without giving prior information about and the capacity to disable such connectors

From definition to legislation- *security*

E. Security

- Security of information systems and the handling of cybercrime are already of high priority in the agenda of the Internet community.
- In IoT the nature and consequences of security threats will change:
  - Identity theft will no longer target the identity of an individual but the identity of the machine, with the objective to retrieve information by misleading one or more machines.
  - The security breaches will not be concerned with personal data but also other data generated that might be of crucial importance for businesses.

From definition to legislation- *security*

- The Internet of Things will necessarily lead to review IT criminal law around two concepts:
  - The protection of identity, as generalized and extended to objects and
  - The protection of information.
  - The theft of data and the protection of the sensitive information capital (business secret) will also need to be recognized

European and U.S Legislation Activities

European Legislation Activities

- □ The European ministerial meeting held on 6 and 7 October 2008 was focused on the Internet of the Future with emphasis on the Internet of Things and the European Commission drafted in 2009 an important Communication on the Internet of Things
- □ This Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled ***"Internet of Things: an action plan for Europe", lays down 14 lines of action***

European Legislation Activities *(cont'd)*

- Two lines of action are more interesting from a **legal perspective**:
  - Line of action 2: It talks about the necessity for a continuous monitoring of the privacy and the protection of personal data
  - Line of action 3: It underlines the need to be able to disconnect from the networked environment, i.e. achieve the silence of the chips or the management of chips
- The EU Commissioner's report recommended that IoT should be designed from the start to guarantee for users the right of deletion, right to be forgotten, data portability, privacy and data protection principles.

Lawmakers and Regulators

The IoT has captured the attention of regulators and lawmakers across the world.

The OECD
In January 2012, the OECD published a report called Machine-to-Machine Communications: Connecting Billions of Devices. The report considered what governments can do to promote the IoT as a new source of economic growth.

The US FTC
In November 2013, the US Federal Trade Commission (FTC) looked at the IoT and put forward a case for targeted regulation to help the industry to develop.

BEREC

BEREC, the European regulatory body for electronic communications, undertook a similar exercise to the FTC and came to similar conclusions.

Ofcom
In July 2014, Ofcom, the UK communications regulator, called for inputs on the promotion of investment and innovation in the IoT. The consultation followed an Ofcom-commissioned report on the future demand for IoT applications and their likely spectrum requirements.

US Legislation Activities *(cont'd)*

- US has also addressed particular IoT concerns with legislation.
- Currently, no federal law expressly and comprehensively governs privacy and security of personal information but at least 14 states have proposed legislation on the 2014 docket that is intended to increase privacy protection for consumers and limit both government and private sector surveillance via the IoT.
  - "We Are Watching You Act" currently with Congress
    - Regulate monitoring of surveillance by video devices in homes
  - "Black Box Privacy Protection Act" with the House of Representatives.
    - Prohibit the sale of automobiles equipped with event data recorders- unless the consumer can control the recording of information.

Other US Regulations of IOT Privacy and Security Issues

- Other federal regulators are also considering privacy and security concerns related to the IOT.
  - The U.S. Department of Energy has led multiparty discussions on smart-grid privacy and security issues.
  - The U.S. Department of Transportation's National Highway Traffic Safety Administration has initiated cybersecurity research for motor vehicles.
  - The U.S. Food and Drug Administration has published guidance concerning cybersecurity of networked medical devices.
  - Federal Communications Commission enforces rules concerning the confidentiality of customer use information collected by wireless network carriers

Additional Legal Concerns

The FDA has published a range of guidance concerning IoT medical products, on topics including wireless technology, software and machine-readable drug packaging.

The NHTSA is researching vehicle-to-vehicle and vehicle-to-infrastructure communication platforms designed to help avoid or mitigate crashes

The Department Of Energy (DOE) also has broad interests in the IoT. Its mission includes researching and developing smart-grid technologies, developing standards and protocols, and relating smart-grid technologies and practices to electric utility regulation

Internet of Things Egypt

IoT Business and Applications

IoT Business Models

- □ Existing business models are not suitable for IoT business domain.

- □ Requires the mind shift from a firm Business model to an ecosystem business model

- □ **Government** has an essential role in creating and the business ecosystem for IoT.

Internet of Things Egypt

Software Engineering Competence Center

Role of IOT in Enhancing Business Model Components

- Enhance Digitally Charged Products' Business Models.

- The components to be enhanced include:
  - Physical Freemium
  - Digital Add-On
  - Digital Lock-In
  - Product as Point of Sales
  - Object Self Service
  - Remote Usage and Condition Monitoring
  - Sensor as a Service

Capabilities of IoT Applications

- Location sensing and location info sharing
  - Mobile asset tracking
  - Fleet management system
  - Traffic information system

- Environment sensing
  - Environment detection
  - Remote medical monitoring

Capabilities of IoT Applications Cont’d

- Remote controlling
  - Appliance control
  - Disaster recovery
- Ad Hoc networking
- Secure communication