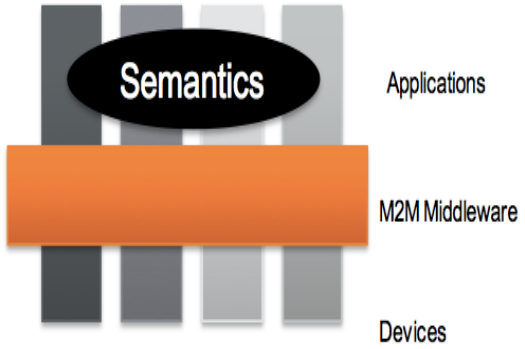
Hanoi University of Science and Technology
School of Information and Communication Technology

Internet of Things: Cloud Computing, Security and Research Area

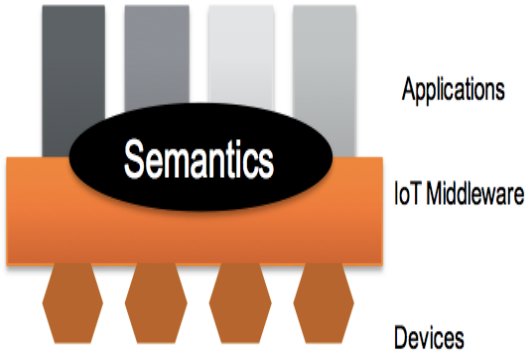
Thu Ngo-Quynh

From M2M towards IoT

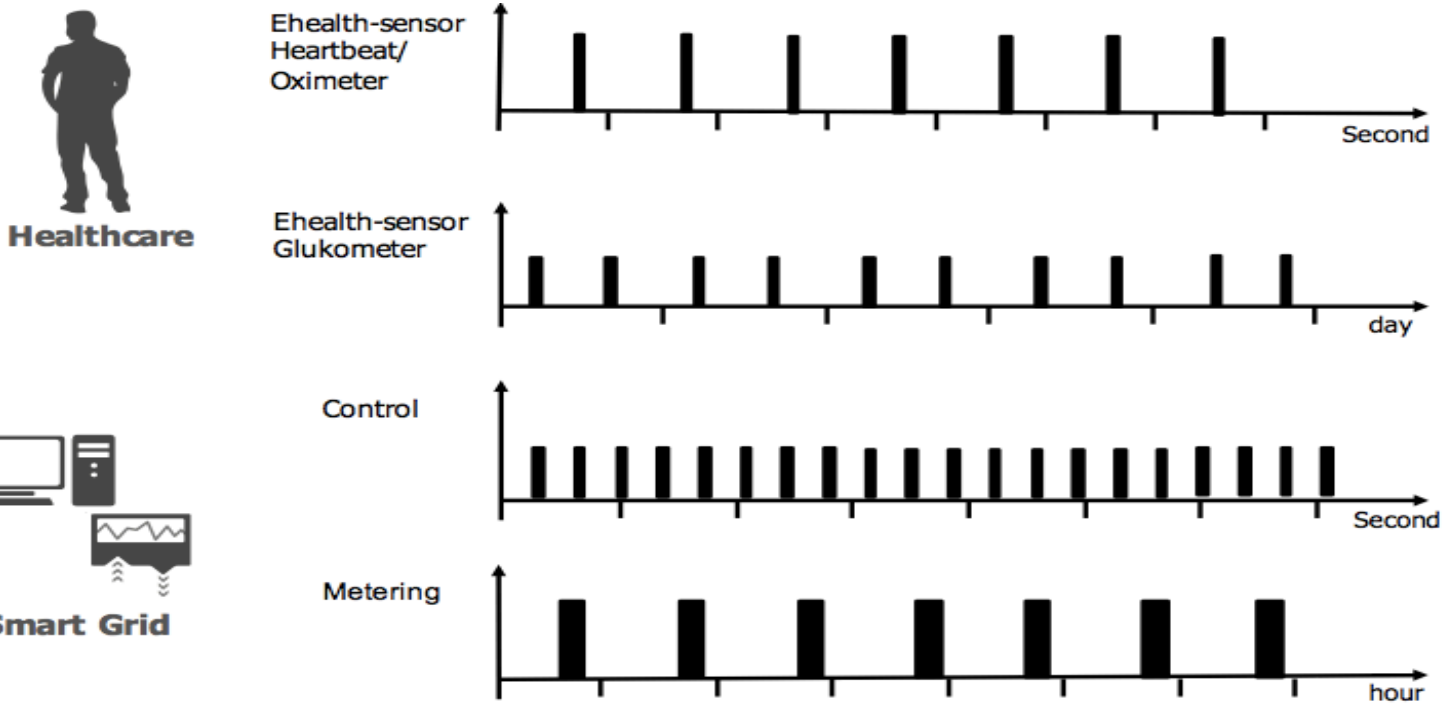
- M2M: Communication is core concept
  - Keep strong/fixed associations between applications and devices
  - Information passed between devices and applications as black box
  - Middleware is not awared of what is being communicated



- IoT: Things are core concept
  - Applications interact on Things level
  - Middleware is aware of Things
  - Requirement of description for association between Things and Higher Level Source
  - Requires functionalities for discovery and processing of information/actuations

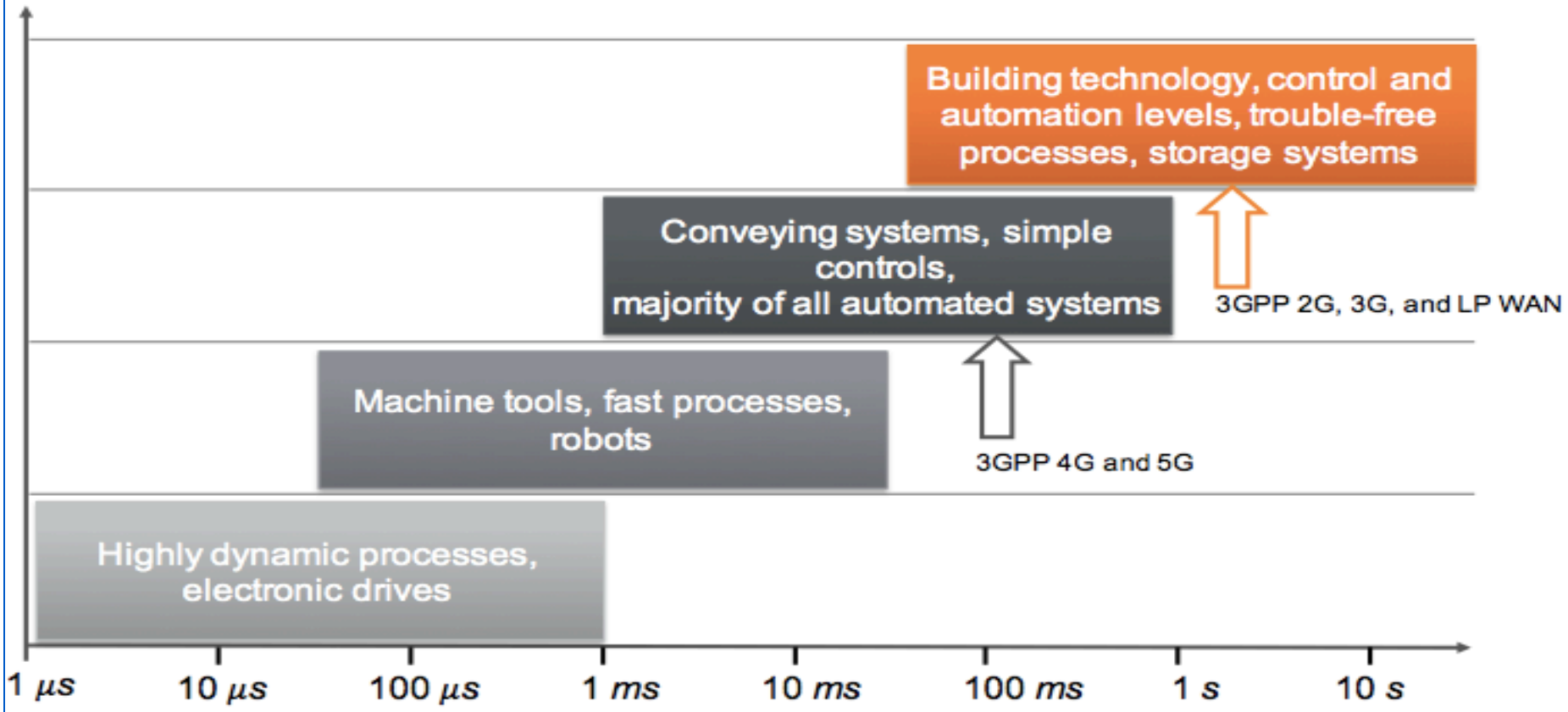


Technical Challenges



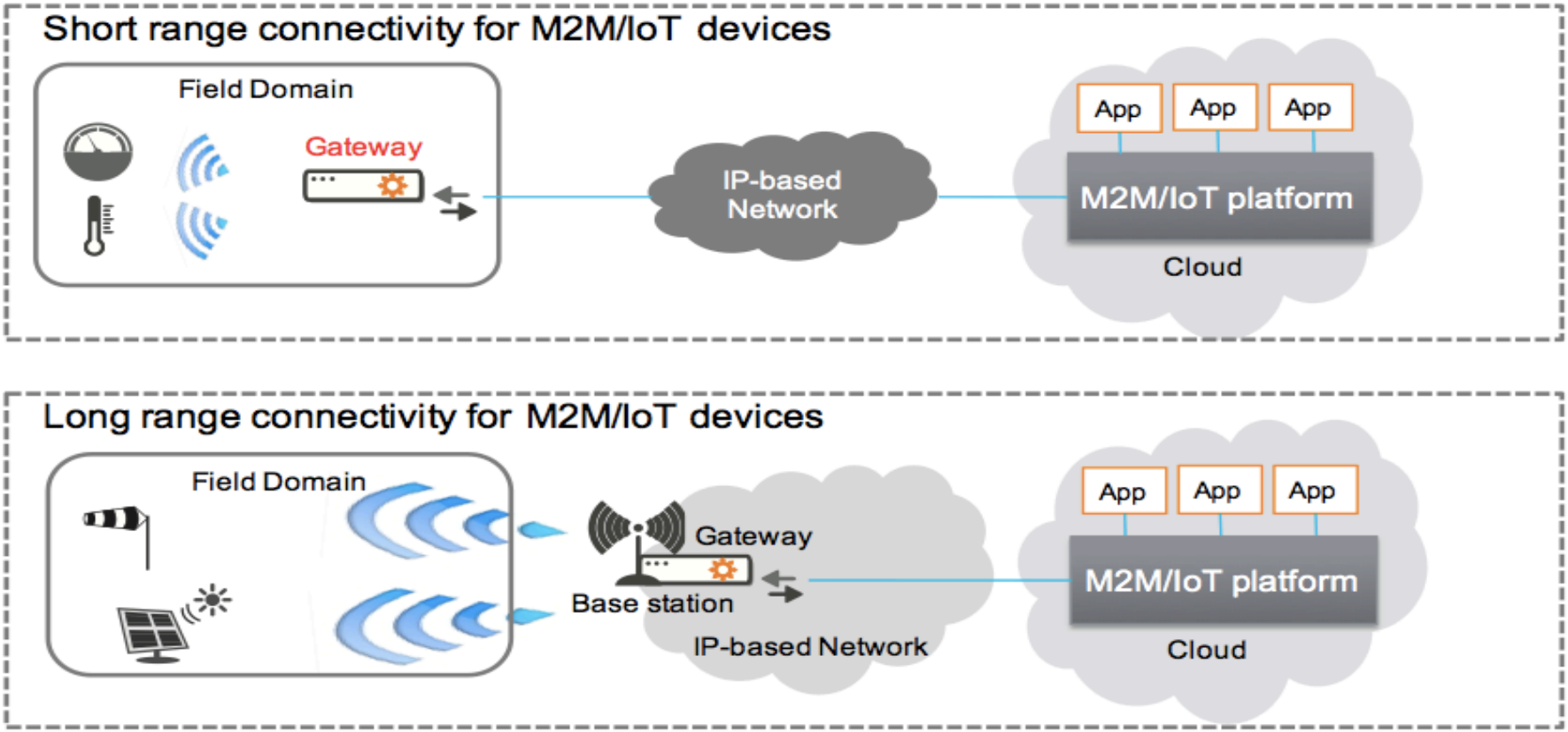
- Support of more than one communication type
  - From Second Scale to day/hour scale
  - Of different applications: Healthcare and SmartGrid

Technical Challenges



- Response time/jitter varies from ms to s

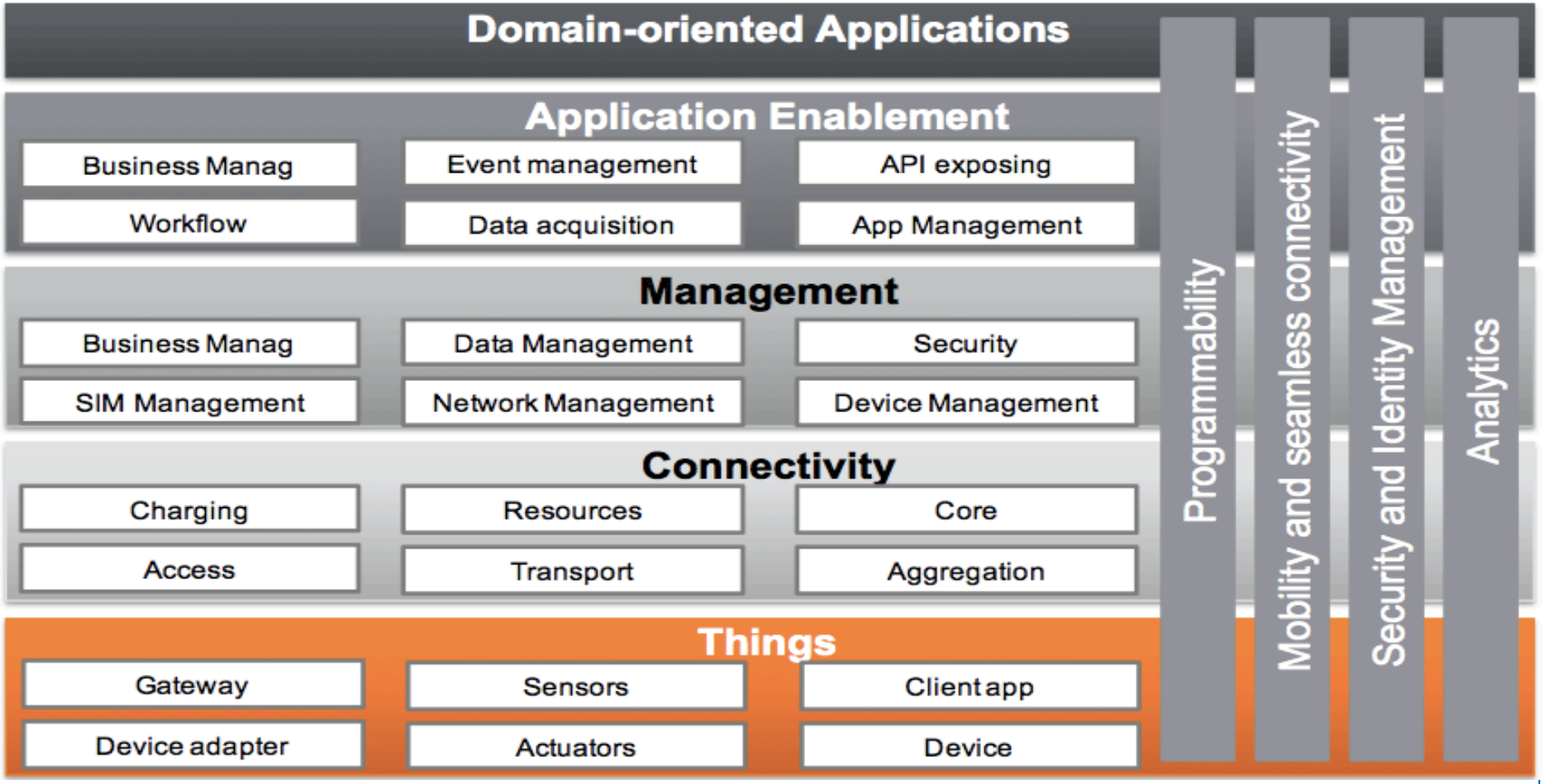
Technical Challenges



- Mesh Networks are not available

Access Technology and Edge Computing

M2M/IoT Reference Model



Characteristics of Access Technologies

	Short Range				Long Range	
Features	**Bluetooth**	**802.11 (Wi-Fi)**	**802.15.4 (ZigBee/6LoWPAN)**	**RFID**	**LPWAN**	**Cellular**
security	64/128bit AES CCM	256 bits AES encryption	128 bit, AES	Low	Low	confidentiality
Latency	100ms/ <3ms (LE)	1.5ms	20ms			~90ms
Mobility	fixed	nomadic subnet roaming	Yes	Fixed	Yes	seamless global roaming
Range	10-100 meters	50-100 meters	10-200 meters	<3m	<10k	>1000m
Power Consumption	Medium Low (LE)	High	Low	Low	Very low	Medium
Battery life	Days years (LE)	Hours	Years	Years	>5	days
Max data rate	3 Mb/s 1 Mb/s (basic or LE)	22 Mb/s (802.11 g) 144 Mb/2 (802.11 n)	250Kb/s	Varies	<100 pbs	12Mb/s (4G LTE)

M2M/IoT Protocols

Protocol	HTTP/1.1	HTTP/2.0	MQTT	AMQP	CoAP
Standards	IETF RFC2616	IETF RFC 7540	Proposed OASIS standard MQTT	OASIS AMQP	IETF RFC 7252
Architecture Style	Client/server model RESTful	Client/servers model	Brokered style	Brokered style	Client/server model RESTful
Transport	TCP	TCP	TCP	TCP	UDP
Messaging	Request/Response	Supports multiplexing of request/response	Publish/Subscribe	Publish/Subscribe (P2P or Brokered)	Request/Response
Service levels (QoS)	All messages get the same level of service	Priority mechanism of streams	Three quality of service settings	Different 3 QoS levels	Confirmable or non-confirmable messages
Data distribution	One-to-one	One-to-one , and one-to-many	One-to-one , and one-to-many	One-to-one , and one-to-many	One-to-one
Security	Typically based on SSL or TLS	Requires TLS version 1.2 or higher	Simple Username/Password Authentication, SSL for data encryption	SASL authentication, TLS for data encryption	Typically based on SSL or TLS
Header	Text-based	Binary (header compression)	Fixed-length header of 2 bytes	Header 8 bytes	4 Bytes binary–based
Message size	Configurable by server, recommended to be less than 8KB	Configurable by server	Up to 256 MB	Unlimited	Small to fit in single IP datagram (1500Byte).

Mobile Edge Computing

- According to ETSI, Mobile Edge Computing:
  - is characterized by ultra-low latency and high bandwidth as well as real-time
  - the evolution of mobile base stations and the convergence of IT and
  - alleviates mobile core networks of further congestion and efficiently serves local purposes
  - will enable new vertical business segments and services, where use cases include:
    - video analytics
    - location services
    - Internet-of-Things (IoT)
    - augmented reality
    - optimized local content distribution and
    - data caching

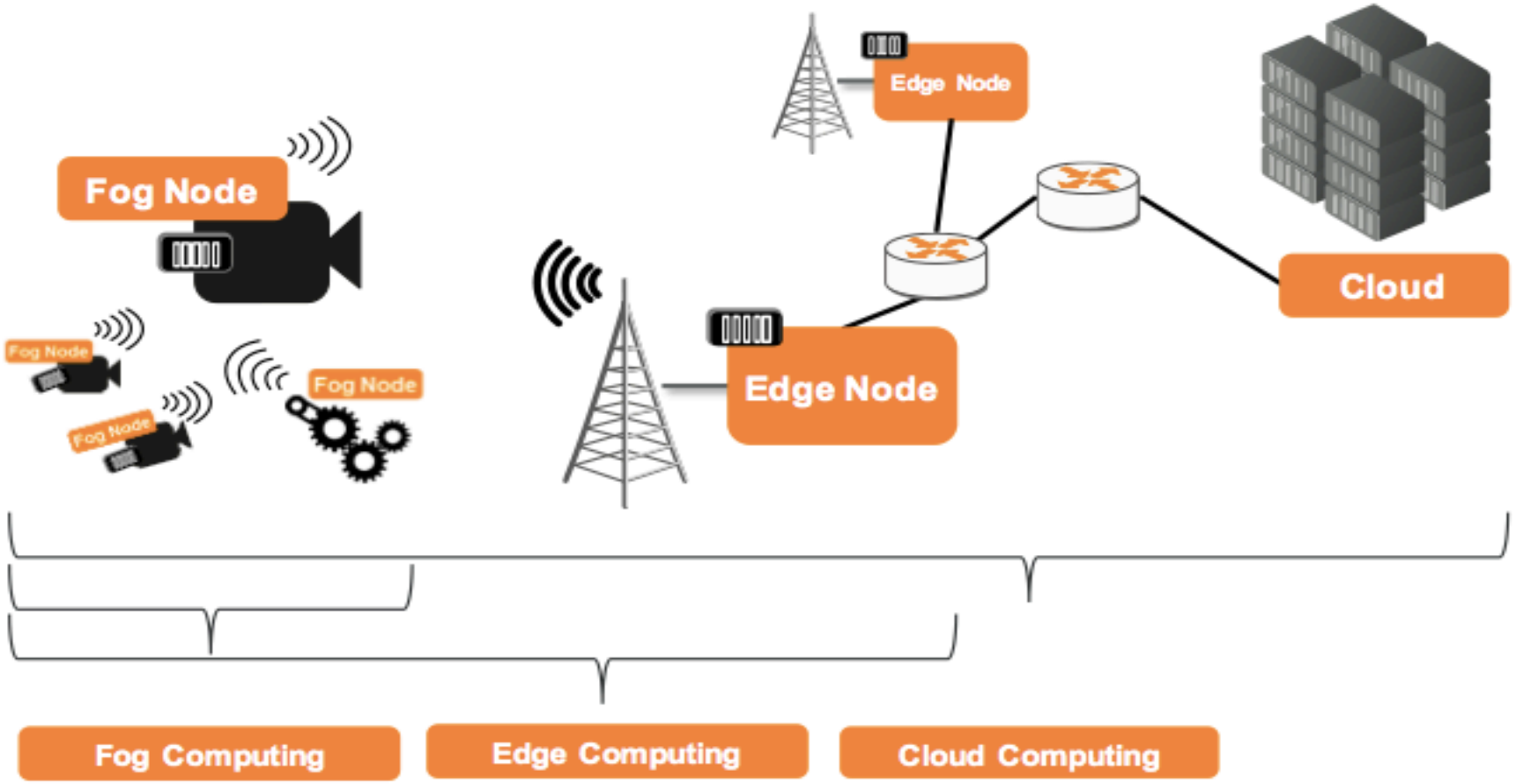
FOG Computing – A Definition

- Fog Computing:
  - Low latency and location awareness
  - Wide-spread geographical distribution
  - Mobility
  - Very large number of nodes
  - Predominant role of wireless access
  - Strong presence of streaming and real time applications
  - Heterogeneity
- Fog nodes provide localization (enabling low latency and context awareness and the Cloud provides global centralization (particularly for analytics and big data)

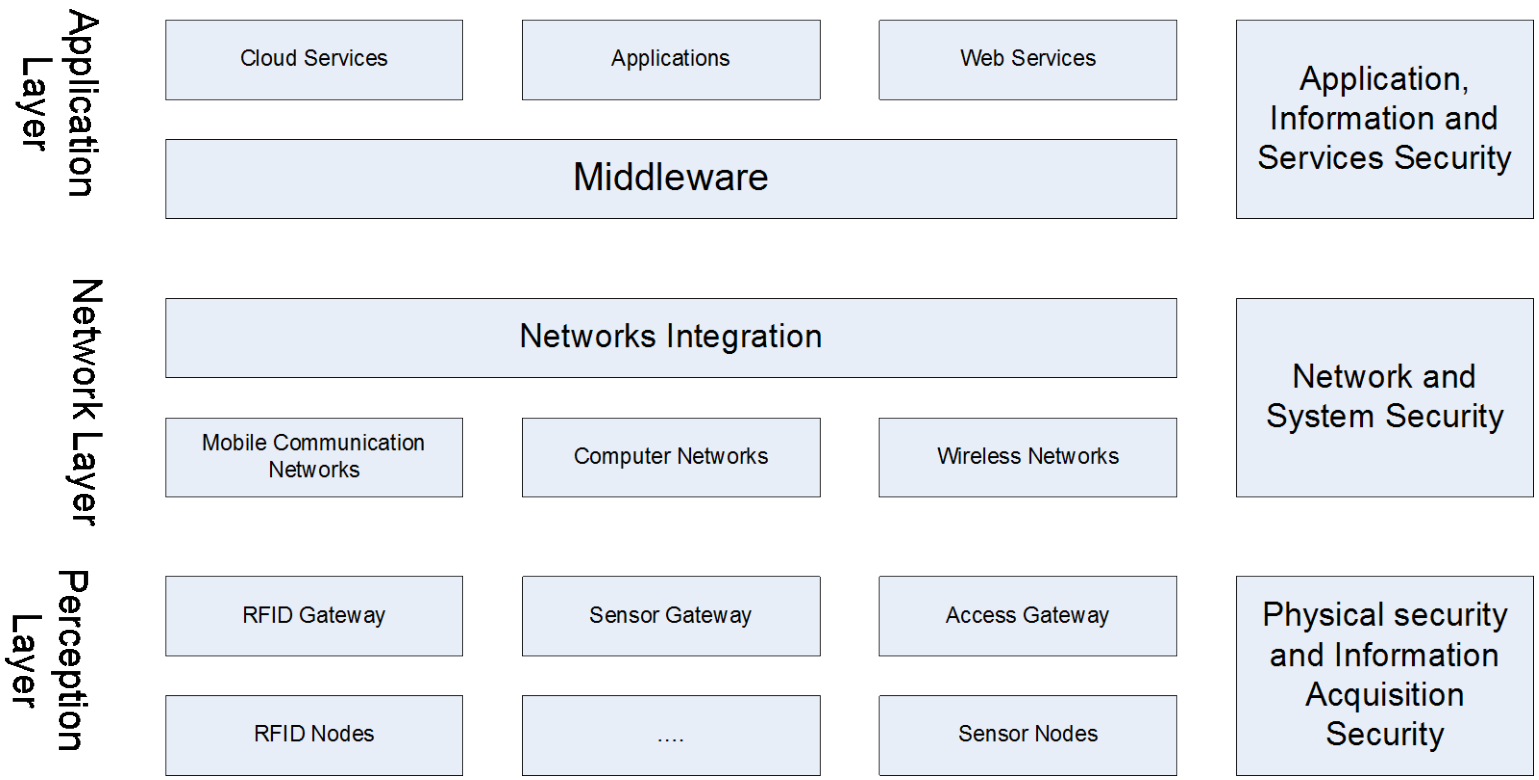
MEG and FOG Computing

- Mobile Edge Computing and Fog Computing share many commonalities
  - ultra-low latency
  - localization and location awareness extension of the cloud
  - distributed analytics
  - pre-dominant role of wireless access
  - enable various IoT scenarios, including M2M
- Fog Computing and Mobile Edge Computing are technologically similar approaches, complementarily enabling mission critical applications for various industrial usage areas (and beyond)

Towards MEG, FOG and Cloud Computing



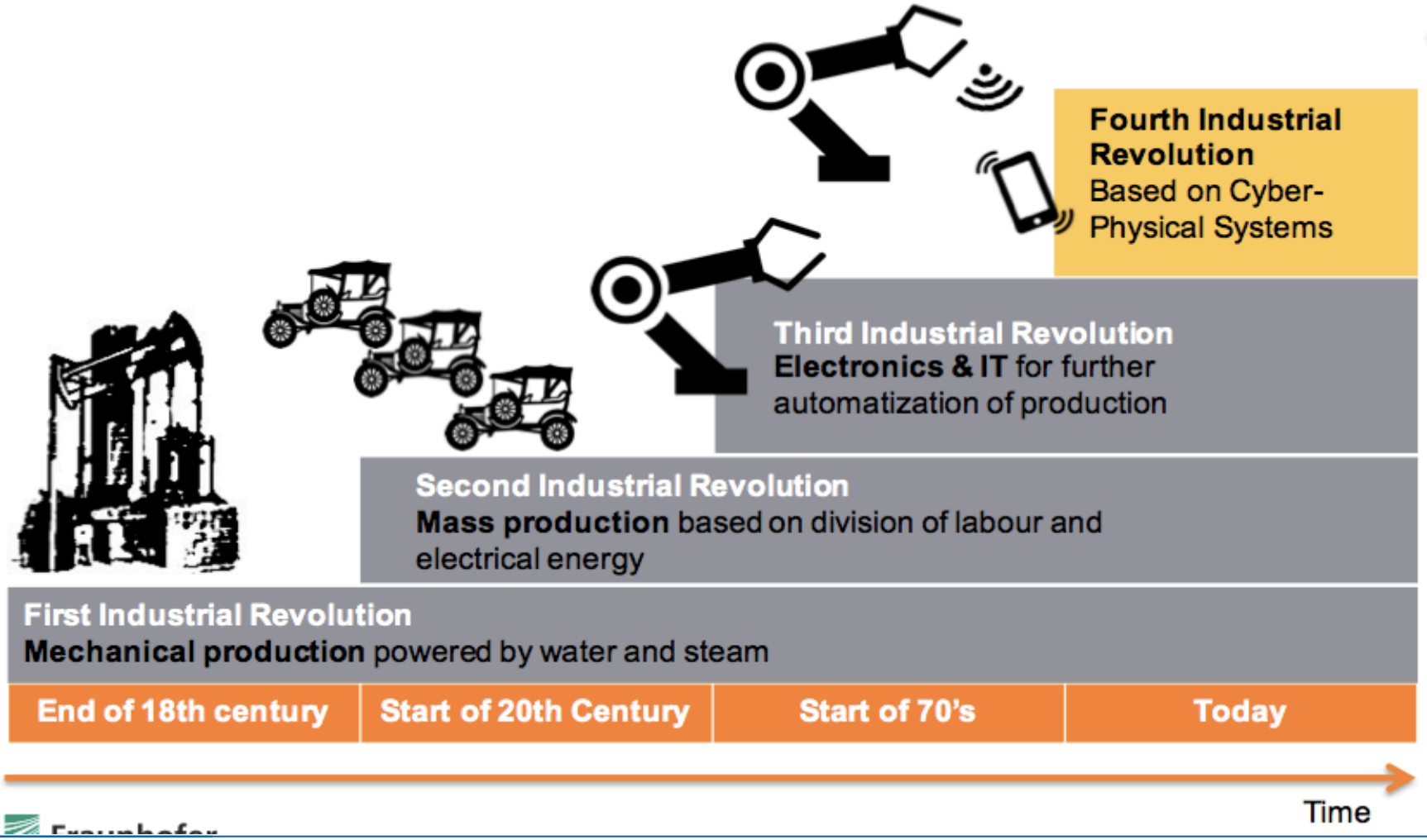
Security Architecture



Security Challenges

- RFID security mechanism
  - Physical methods
  - Code mechanism
- Sensor Technology and Network Security
  - Security framework
  - Encryption – decryption
  - Key management and distribution
  - Secure routing
  - Intrusion detection mechanism
- IoT Gateway security
  - Data processing centers security
  - Identity authentication
  - Data access control
  - Channel encryption
- Information transmission over the Internet of Things Security
  - Security vulnerabilities
  - Protocols security
  - IPv6
- Information processing security
  - Application security
  - Service security
  - Cloud security
  - Privacy protection

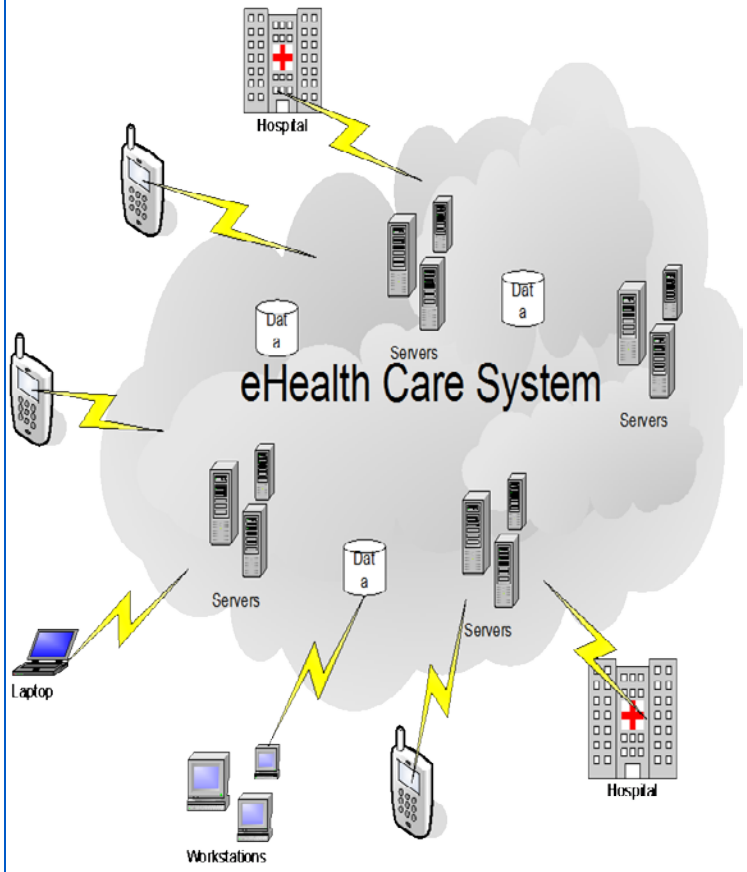
Industry V4.0 Revolution



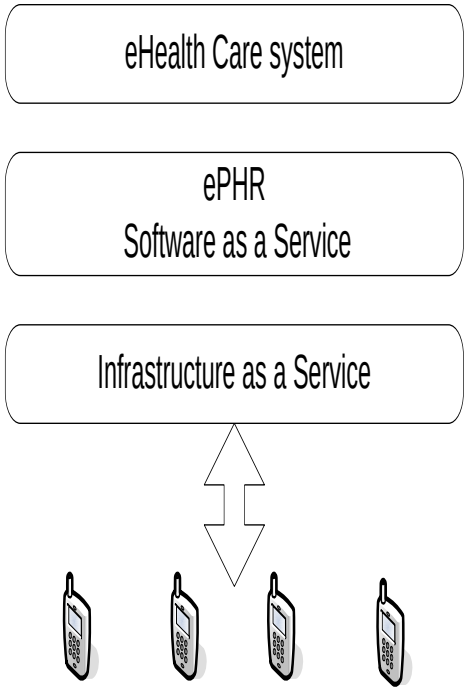
Industrial Internet Domain Sections

Fraunhofer FOKUS

Cloud-centric IoT in eHealth Care system



- Layered Structure of eHealthCare System
  - Mobile devices and medical sensors for collecting health data records
  - Data services infrastructure based on Cloud IaaS and SaaS.



Cloud-centric IoT in eHealth Care system

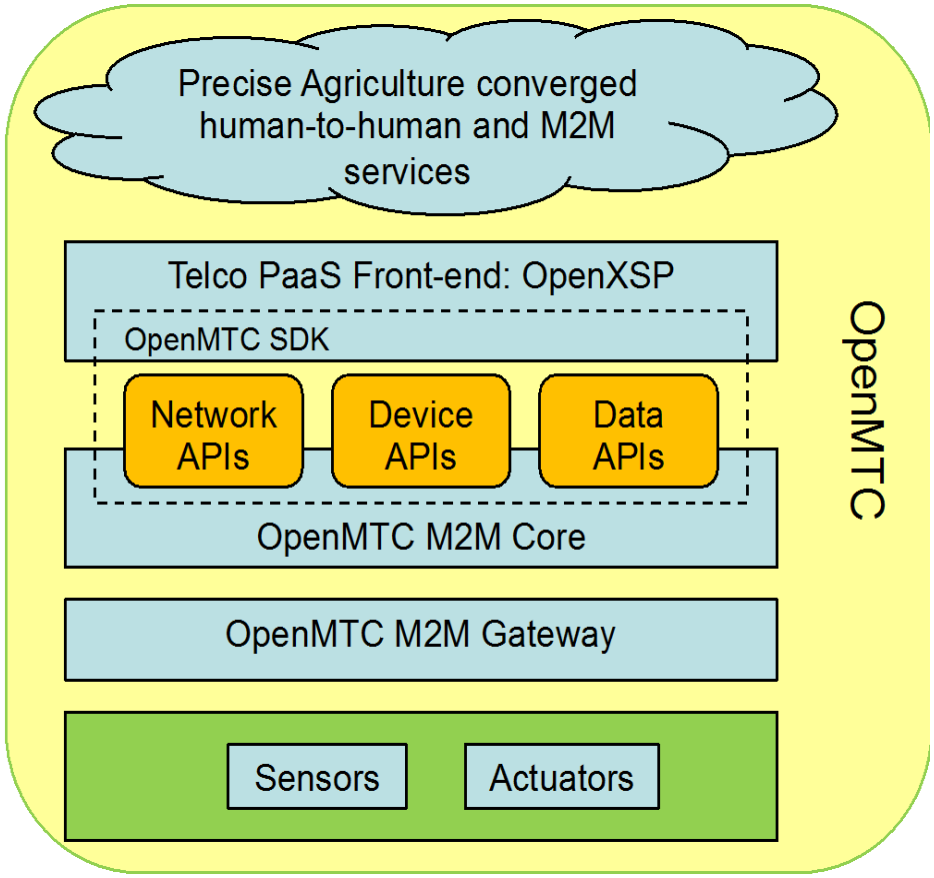
- Security Challenges:
  - Multi domain Access control to eHealth Cloud;
  - Privacy of medical data stored in the eHealth Cloud;
  - Privacy of medical data collected by mobile devices and medical sensors and transmitted over the Internet of Things;

IoT and Networking for Precise Agriculture

1. App: a simple environment monitoring application
2. Transport: UDP – does not require complex mechanism
3. Network: IPv6 along with RPL
4. IPv6 Adaption: a header compression to adapt IPv6
5. MAC: perform carrier sense multiple access
6. RDC: perform transmission, periodically reception CCA
7. Framer: to extract bit from package object
8. cc2420 simulation
   - Propagation model
   - Energy consumption model

IoT	My benchmark	OMNeT++ Module
Application	Application	Server Client
Transport	Transport	UDP
Network	Network	IPv6, RPL
IPv6 Adaption	IPv6 Adaption	6LoWPAN
Data Link	MAC	Un-slotted CSMA
	RDC	ContikiMAC
Physical	Framer	Framer 802.15.4
	Transceiver driver	cc2420 driver

IoT and Networking for Precise Agriculture



- Backend
  - Real-time data aggregation and processing
  - Open and standardized APIs to apps
  - Support various deployment scenarios
    - Tightly or loosely coupled from the core cloud deployments
  - Device management and discovery
  - Integrate H2M communication based on IMS
  - Enable the development of M2M and H2M applications over a common platform
- Frontend
  - Support different sensors and actuators
    - FS20, ZigBee, Bluetooth, etc.
    - Integrate multiple sensors
  - Various gateways
    - Android-based and Linux-based
    - Embedded hardware (Arduino and Raspberry Pi)
  - SDK and scenarios as reference implementation
- M2M communication
  - Support open REST APIs
  - Support different protocols and interaction models
    - HTTP, CoAP, MQTT
    - pull, push, Pub/Sub, etc.
    - store&forward
  - Heterogeneous wireless access
    - 4G, 3G, 2G and WiFi
  - QoS and mobility enforcement through 3GPP EPC interfaces
- Comformant
  - Aligned with the standards like ETSI M2M and oneM2M
  - All functional elements available individually
  - Any functionality combination feasible due to software modularity
  - Source code available