




ISTITUTO SUPERIORE MARIO BOELLA

INTERNET OF THINGS ISSUES AND CHALLENGES

MIRKO FRANCESCHINIS

Workshop on Scientific Applications
for the Internet of Things (IoT)
16-27 March 2015, ICTP – Trieste

ISMB
Istituto Superiore Mario Boella

Pervasive Technologies

ABOUT ME

- 2000 – Telecommunication Engineering Master Degree at Politecnico di Torino
- 2003 – Communication Engineering PhD Degree at Politecnico di Torino
- 2004 – Research Grant on Wireless Networks at Politecnico di Torino
- [2005 - Today] – Researcher @ ISMB in the Pervasive Technologies (PerT) Area, mainly working on low-power wireless networks
- ISMB PerT Area
  - IoT Objects and Platforms
  - Pervasive Secure Networks
  - IoT Service Management

OUTLINE

- Part I – Energy Harvesting for IoT devices
- Part II – The Middleware
- Part III – Security and Privacy Issues
- Part IV – Architectures and Standardization Efforts

PART I

ENERGY HARVESTING FOR IOT DEVICES

SMART OBJECTS DEVELOPMENT

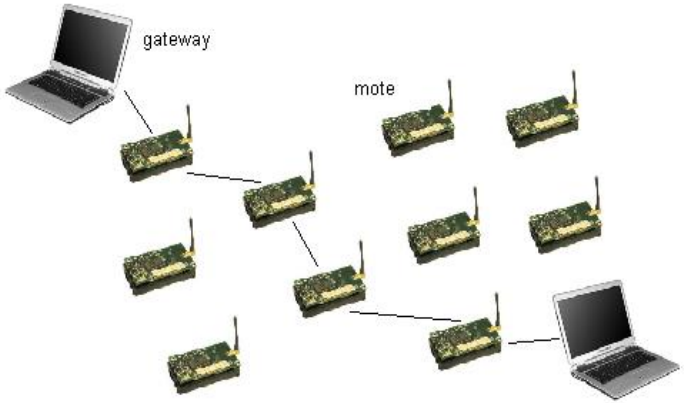
- We are in the domain of the "object-oriented" vision of the IoT
- Energy harvesting is just one of the main challenges for the design of embedded systems for IoT
- Others are, e.g.
  - Energy consumption
  - Device miniaturization
  - Device weight
  - Device integration
- Wireless technologies for IoT all interested by energy harvesting
- WSN suitable case study due to typical applications in harsh environments

ENERGY FOR POWERING OBJECTS

- Sensors need to be self-sustaining
  - Changing batteries in billions of devices deployed across the planet is not feasible
- Sensors need a way to generate electricity from the environment
  - Vibrations
  - Light
  - Temperature gradients
  - Airflow
  - …
- A commercially viable example: nanogenerator, flexible chip using body movements such as the pinch of a finger to generate electricity

DESIGN CHALLENGES IN WSN

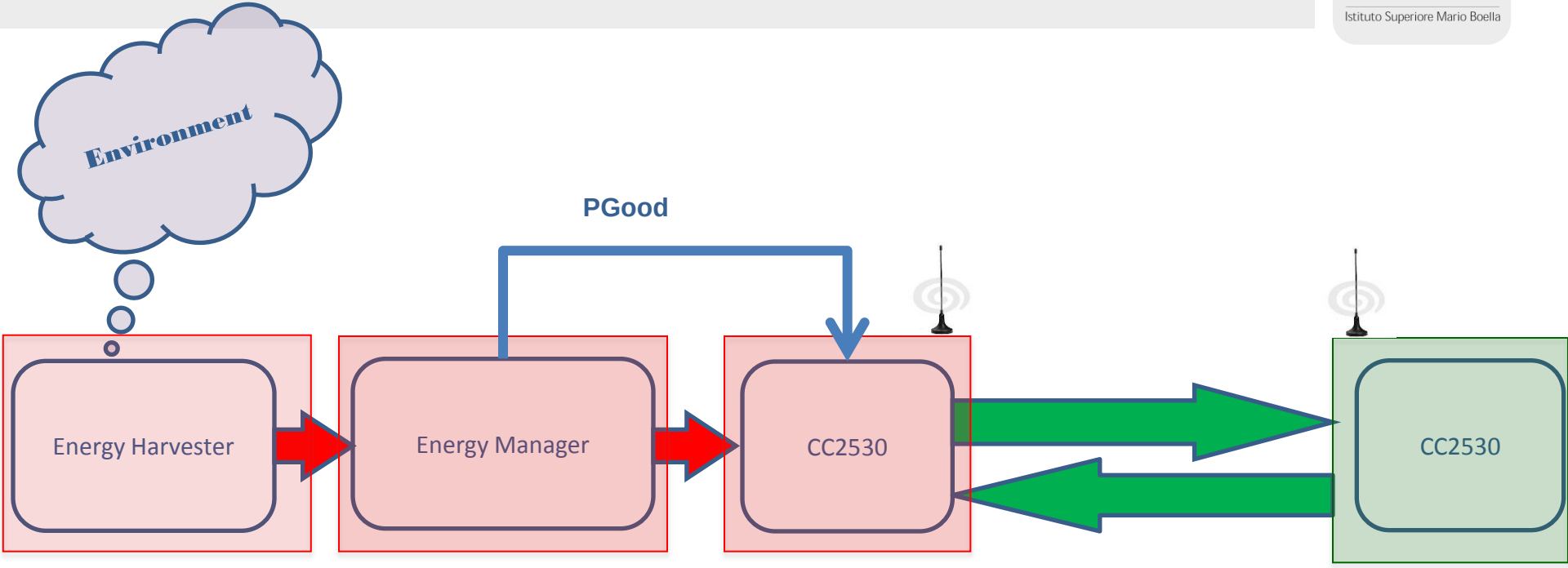
- Hard to replace/recharge batteries in nodes once deployed
- Deployed in large areas and difficult locations
- Human intervention may interrupt nodes operations
- Higher performance requirements demand more energy supply



ENERGY HARVESTING IN WSN

- Energy harvesting/scavenging process
  - To capture ambient energy (in many different forms), and
  - To convert it into usable electrical energy
- WSNs can operate in very low duty cycle, depending on the application
  - Moderate power consumption in (short) active mode
  - Very low power consumption in (long) sleep mode
- Batteries or capacitors can be charged in sensor nodes
- Aims
  - To prolong WSN operational lifetime
  - To enhance system reliability

BASIC SYSTEM MODEL



- Solar panel
- Thermoelectric generator (TEG)
- Piezoelectric material

WSN Node

WSN Coordinator

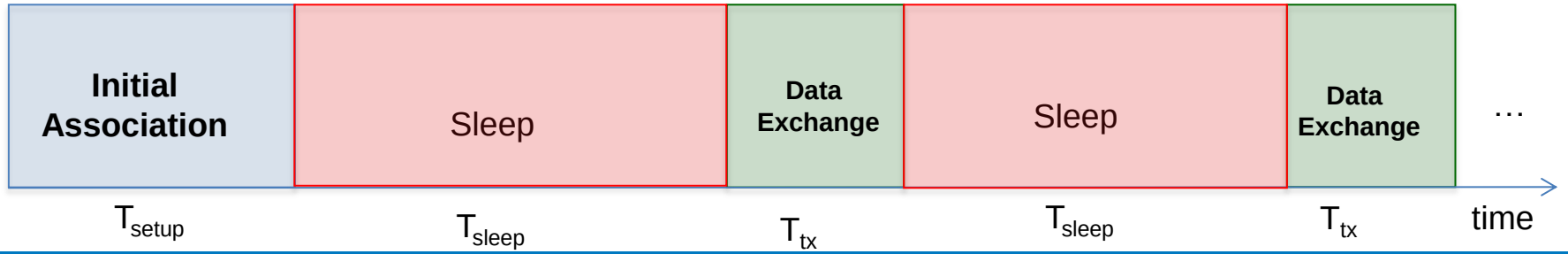
ENERGY AND TIME VALUES FOR CC2530

- System-on-chip that integrates: transceiver, microcontroller and peripherals
- Three energy consumption modes
  - Initial association phase: I = 27mA (T_{setup} = 680ms)
  - Sleeping Mode: I = 1μA (T_{sleep} = 5s)
  - Transmission cycle: I = 27mA (T_{tx} = 28ms)

➔ E_{setup} = 57mJ

➔ E_{sleep} = 15μJ

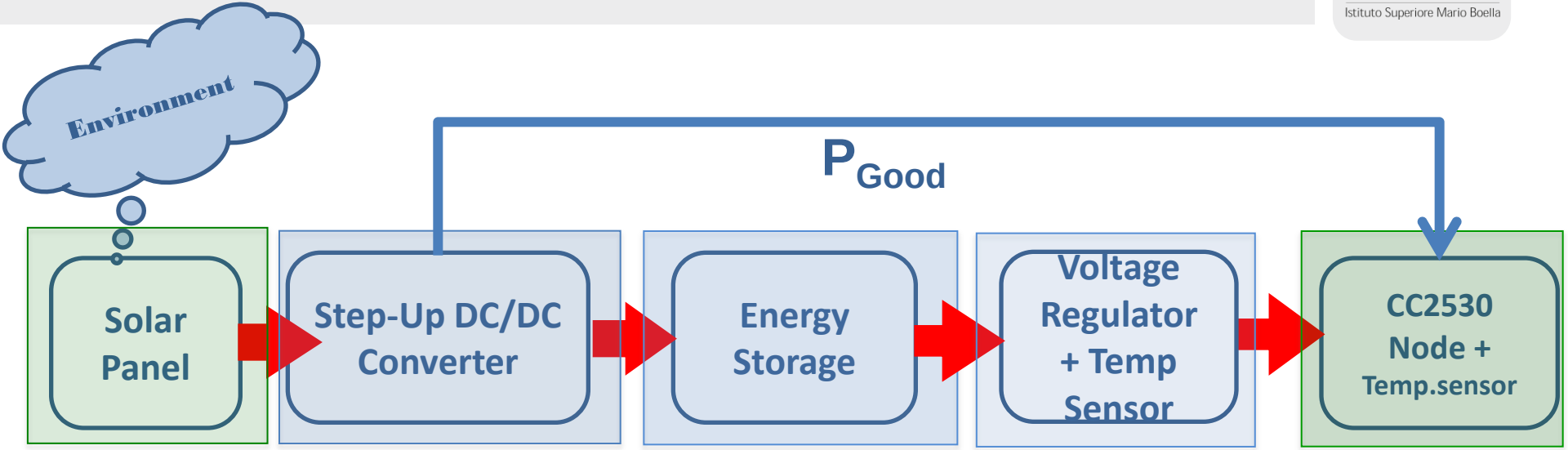
➔ E_{tx} = 2.27mJ



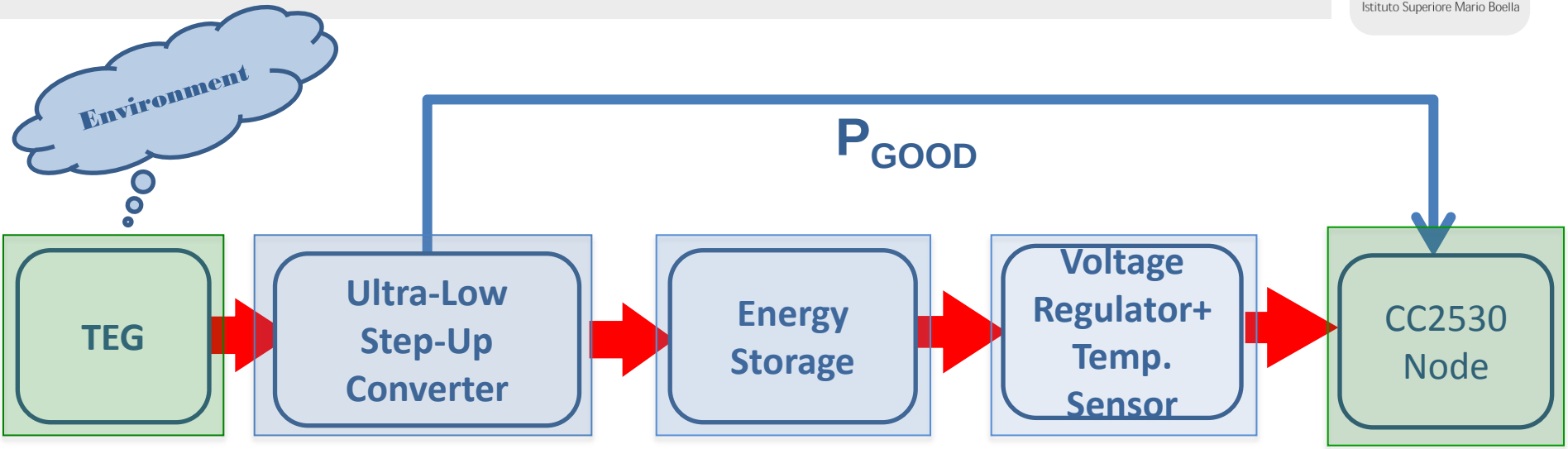
ENERGY HARVESTERS COMPARISON

Energy Harvesters	Efficiency	Harvested Power	Energy Management Circuit	Start up Voltage	Stability Time
SOLAR PANEL	10-24%	100's of mW/cm^2	Voltage Step up regulator, Storage element, Voltage regulator, Li-ion battery charger	250mV	1.5ms
TEG	0.5-3%	10's of mW/cm^2	Ultralow Voltage Step up converter, 1:100 Transformer, Voltage regulator, Li-ion battery charger	20mV	4.5ms
PIEZO MATERIAL	25-50%	100's of $\mu W/cm^2$	Diode bridge rectifier integrated with step down regulator, Voltage regulator, Li-ion battery charger	8Vpp	5.2ms

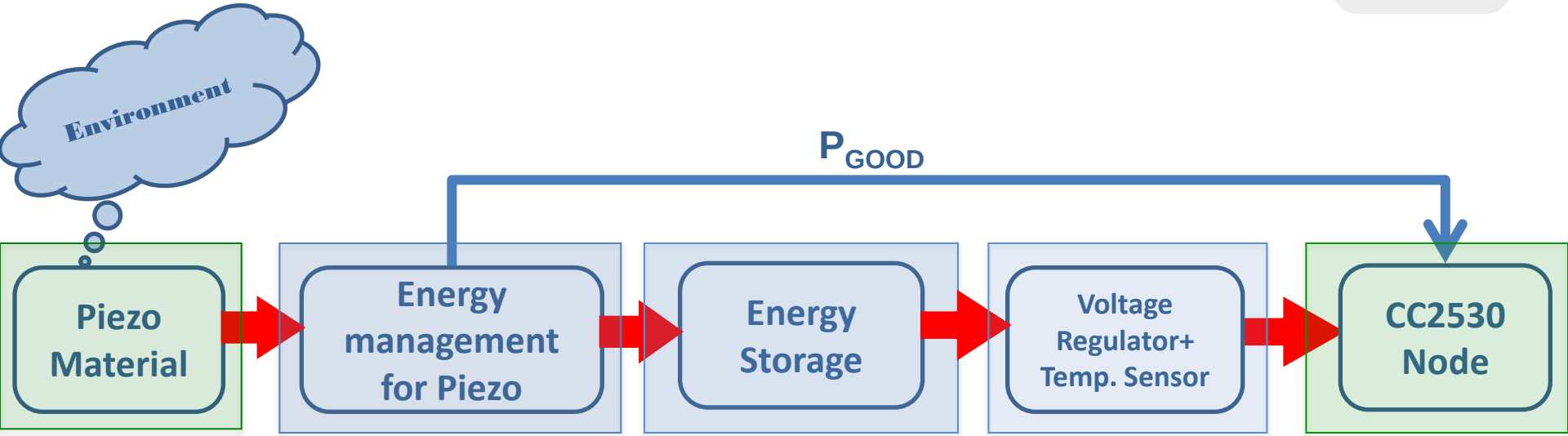
SOLAR PANEL: ENERGY MANAGEMENT CIRCUIT



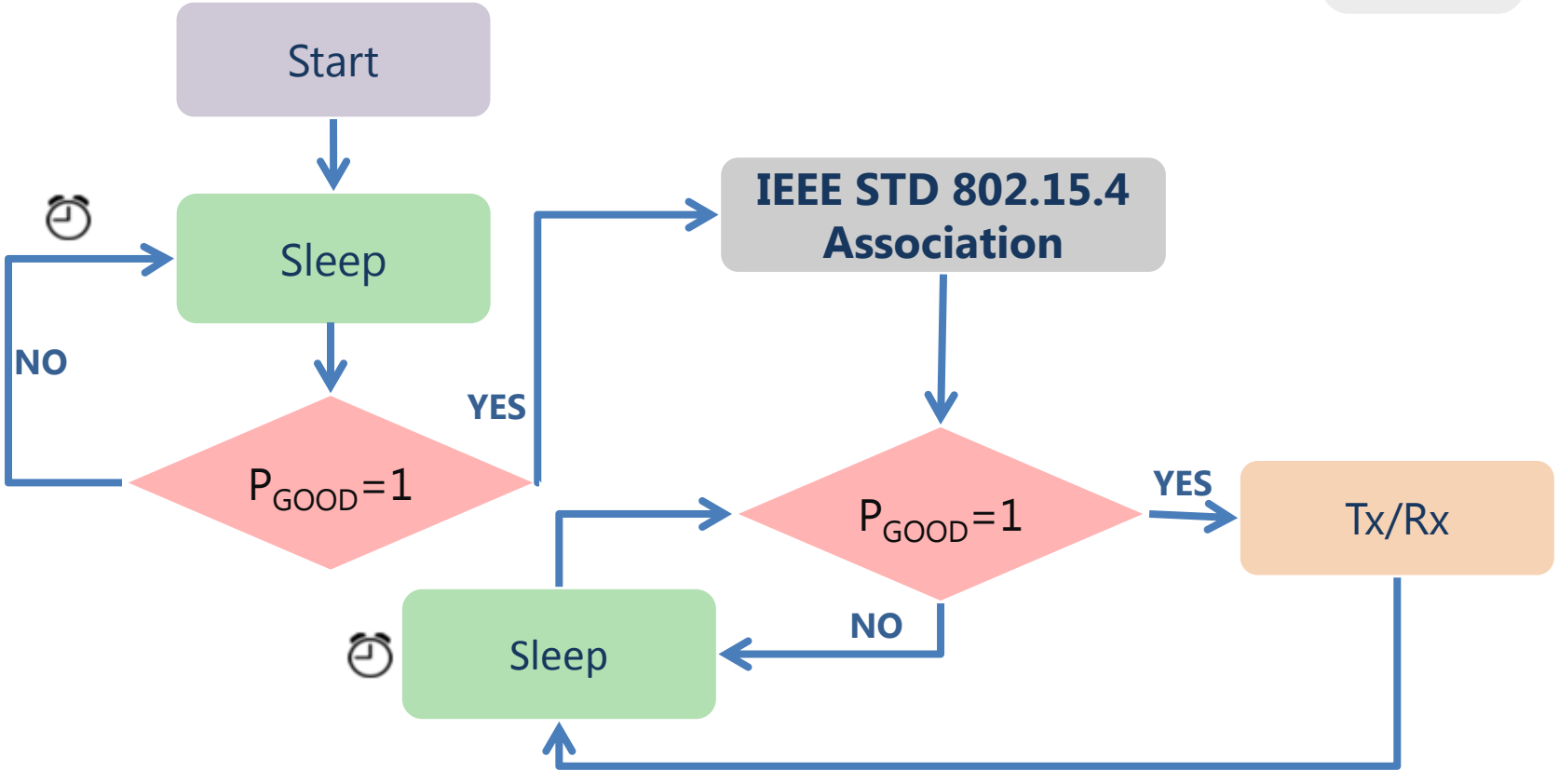
TEG: ENERGY MANAGEMENT CIRCUIT



PIEZO: ENERGY MANAGEMENT CIRCUIT



FIRMWARE FLOW CHART



PART II

THE MIDDLEWARE

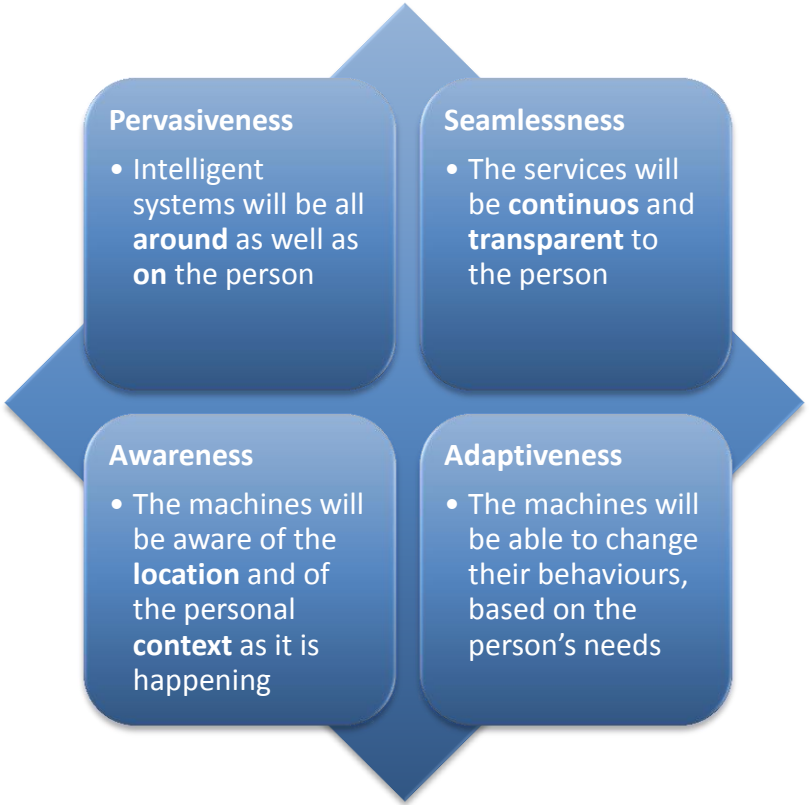
WHAT IS THE MIDDLEWARE

- The concept of **Middleware** has existed since the **'80s**, the term was born in the **software community**
- **Middleware** syntactically means **software in the middle**
- A **software layer of «interconnection»**, composed of **several services**
- At the same time, a **development environment**
  - For **distributed applications**
  - Addressed to the **communication among multiple entities** (processes, objects,…)
- Realized with a **modular architecture**, where **modules** are **software components** able to perform specific functionalities

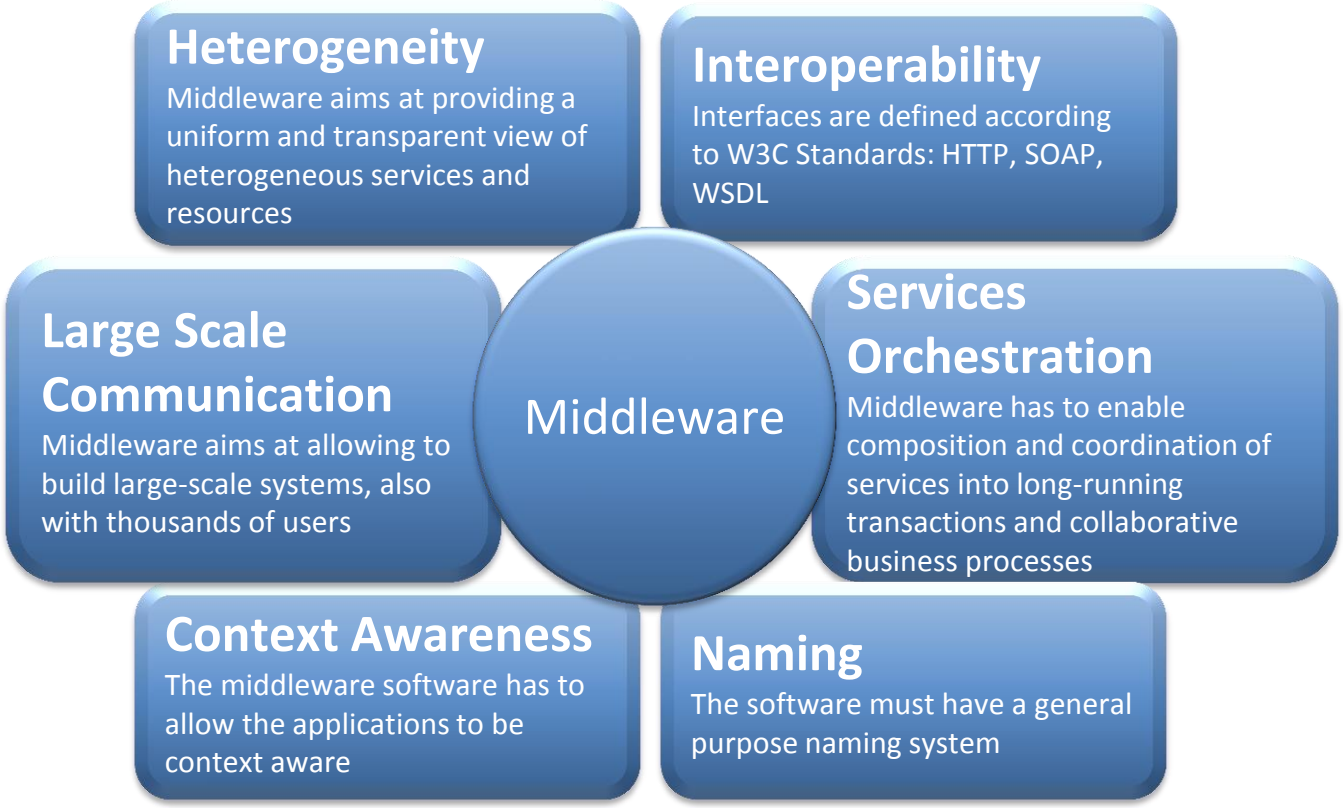
MIDDLEWARE FEATURES

- **Hides** the **details** of **different technologies**
  - For IoT, this means virtualization of physical objects and connection between physical and digital world
- **Simplifies** the **development** of new services
- **Exempts** the programmer from
  - Issues not directly pertinent to her/his focus, which is the development of the specific application
  - The exact knowledge of the variegate set of technologies adopted by the lowest layers

MIDDLEWARE FEATURES



MIDDLEWARE CHALLENGES

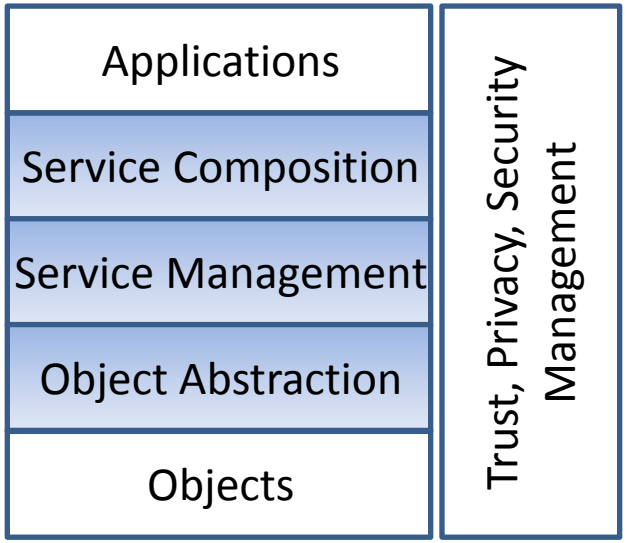


MIDDLEWARE ARCHITECTURES

- Recent **middleware architectures** proposed for **IoT** often follow the **Service oriented Architecture** (SoA) approach
  - Adoption of SoA principles allows for decomposing complex and monolithic systems into simpler applications with well-defined components
  - SoA approach also allows for software and hardware reusing, since no specific technology is imposed for service implementation
- Alternative to the SoA approach: **Data oriented Architecture** (DoA)
  - focus on the data produced, not on the services
- More recently, solutions proposed with a **mixed approach**
  - based on a SoA, but
  - provide also the features to work following an event-driven behavior

MIDDLEWARE ARCHITECTURE FOR IOT

- A **common**ly accepted layered **architecture** is **missing**!
- **Common points** of proposed solutions
  - Face essentially the same problems of **abstracting devices functionalities and capabilities**
  - Provide a common **set of services** and an **environment for service composition**



STATE OF THE ART

Name	Description
Plastic	Enriches the traditional SoA with key features for services to become truly pervasive by taking full benefit of the rich capacities, now embedded in wireless devices
Linksmart	Allows developers to incorporate heterogeneous physical devices into their applications by offering easy-to-use web service interfaces for controlling any type of physical device
SAI middleware	A scalable-grid SoA middleware for distributed heterogeneous data and system integration in context-awareness oriented domains
ASPIRE	Aims at developing and promoting an open-source, lightweight, standards-compliant, scalable, privacy-friendly, and integrated middleware along with several tools for RFID
SOCRADES	Enables enterprise-level applications to interact with and consume data from a wide range of networked devices using a high-level, abstract interface that features web services standards
VIRTUS	General-purpose middleware based on XMPP communication, developed in ISMB
Sensor Andrew	Uses the XMPP protocol to host many different sensors and actuators

LINKSMART MIDDLEWARE

- Open source middleware for intelligent networked embedded systems
- Originally developed in the FP6 EU Hydra project
- Successfully applied in subsequent FP7 and H2020 EU projects
- Main advantages
  - Cost effective development of innovative IoT solutions
  - Low cost for device manufacturers to be part of the IoT
  - Secure and reliable services for end-users

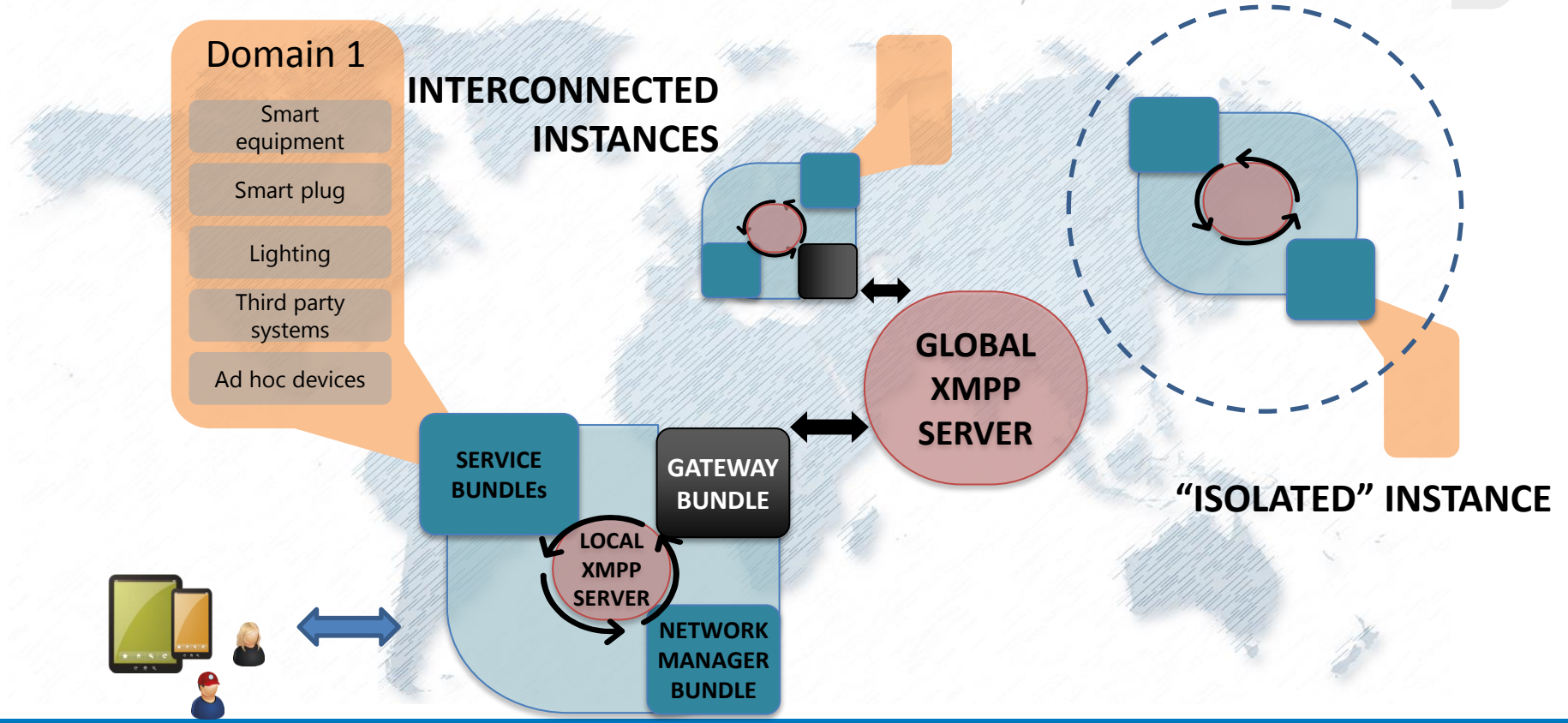
LINKSMART MIDDLEWARE

- Based on SoA approach
- Includes support for
  - Distributed as well as centralized ambient intelligence architectures
  - Reflective properties of the middleware components
  - Security and trust enabling components
- Based on semantic models to
  - allow for a generic, configurable and flexible architecture
  - facilitate automatic generation of code as much as possible
- Supports model-driven development of ambient intelligence applications

LINKSMART TOOLS

- Tools for solutions providers, SDK (Software Development Kit)
  - Easy to integrate and use devices in applications
  - Hide complexity of underlying network and device access protocols
  - Integrated into familiar programming environments
- Tools for device manufacturers, DDK (Device Development Kit)
  - Low cost for networking devices
  - Support for their devices to be part of an intelligent environment

VIRTUS



VIRTUS FEATURES

- **Communication based on XMPP**: Extensible Messaging and Presence Protocol used for entire communication intra and extra domain
- **Portable**: it is based on the Java programming language and, for this reason, it is portable on the operating systems that support a Java Virtual Machine (Windows, Linux, Mac)
- **Modular**: all the components can be installed dynamically, started and removed at runtime, so to use only the useful modules of the domain
- **Configurable**: all the components are configured using a single configuration interface
- **Web 2.0 oriented**: it can support the interaction via chat with other chat services and social networks like Facebook, Twitter, Skype

PART III

SECURITY AND PRIVACY ISSUES

SECURITY OVERVIEW

- **IoT** extremely **vulnerable** to attacks
  - **Unattended components**
  - **Wireless communications**
  - **IoT components** are **energy-constrained** and **lack of computing resources**, cannot implement **complex schemes** supporting **security**
- **Major problems** related to security concern:
  - **Authentication** -> who requests info is really who is expected to be
  - **Data integrity** -> risk of alteration of original contents

AUTHENTICATION

- Proxy attack problem, also known as the **man-in-the-middle attack**
  - Actors
    - **A** = 'good' interrogator – **B** = 'good' queried listener
    - **A'** = 'malicious' interrogator – **B'** = 'malicious' queried listener
  - **Basic idea**: *to make A believe that B' is B, and make B believe that A' is A*
  - **Events**: *B' transmits to A' the query signal received by A. A' transmits it to B. A' receives the reply from B and transmits it to B', that transmits it to A.*
  - This can be **done regardless** of the fact that the **signal** is **encrypted** or not

DATA INTEGRITY

- **Goal**: An adversary cannot modify data in the transaction without the system detecting the change
- **Risks**: Data can be modified by adversaries while they are stored in an unattended node or when they traverse the network
- About solutions
  - **Keys/passwords** in **RFID** too **short** to provide strong levels of protections
  - All the proposed solutions use some **cryptographic methodologies**
  - Cannot be applied to the IoT, **too many resources** (**computation capabilities, energy, communications**) at source/destination **required**
  - **Key management schemes** still at an **early stage** (especially in the case of RFID)

PRIVACY OVERVIEW

- People **concerns** about **privacy** are well **justified** today (**Internet**)
- People **concerns** about **privacy** are even **more justified** tomorrow (**IoT**)
  - The ways in which **data collection**, **mining** and **provisioning** will be accomplished are multiplied and **not controllable**
- Differently from security, in general **privacy problems** can**not** be **solved technical**ly (only) by means of **algorithms** and protocols
- The **less smart** the **object**, the **more complex** is the solution to **privacy respect** (RFID tags less than WSN nodes, less than …)
- New system that **negotiate**s **user privacy** level on the basis of **preferences** set by the **user** itself

PART IV

ARCHITECTURES AND STANDARDIZATION EFFORTS

STANDARDIZATION OVERVIEW

- Standardization efforts mainly by:
  - Different sections of the Auto-ID Lab
  - European standards organizations (ETSI -> ETSI-M2M, CEN, CENELEC, etc.)
  - International standards organizations (ISO, ITU)
  - Other standards bodies and consortia (IETF, EPCglobal, OMA, …)
  - …
- Good news: tight collaboration between standardization institutions and other world-wide interest groups and alliances (IPSO, ZigBee Alliance, …)

STANDARDIZATION OVERVIEW

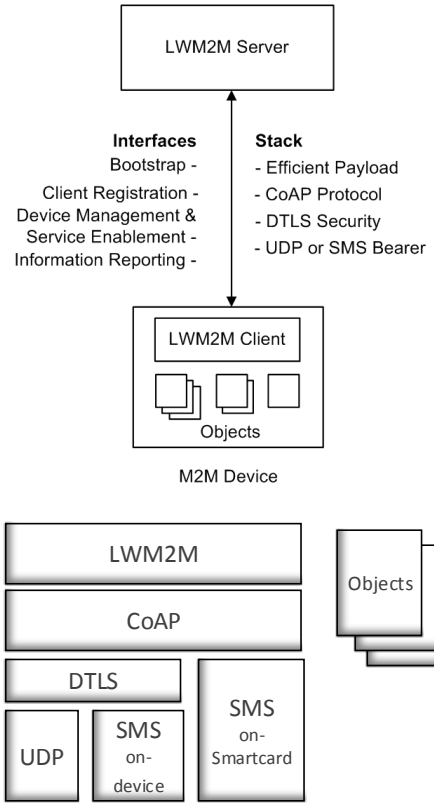
- Emerging idea: to consider the IoT standardization as an integral part of the Future Internet definition and standardization process -> CERP-IoT (Cluster of European R&D Projects)
- Much progress has been made, more is needed, especially in the areas of
  - Security
  - Privacy
  - Communications
  - Architectures

OPEN MOBILE ALLIANCE (OMA)

- Non-profit organization constituted in June 2002 whose members are
  - Mobile operators
  - Device and network suppliers
  - Information technology companies
  - Content and service providers
- Goal: to deliver open specifications for creating interoperable services working across all geographical boundaries
- Specifications support
  - billions of new and existing fixed and mobile terminals
  - a variety of mobile networks, from traditional cellular operator networks to emerging networks supporting M2M communication

OMA LIGHTWEIGHT M2M

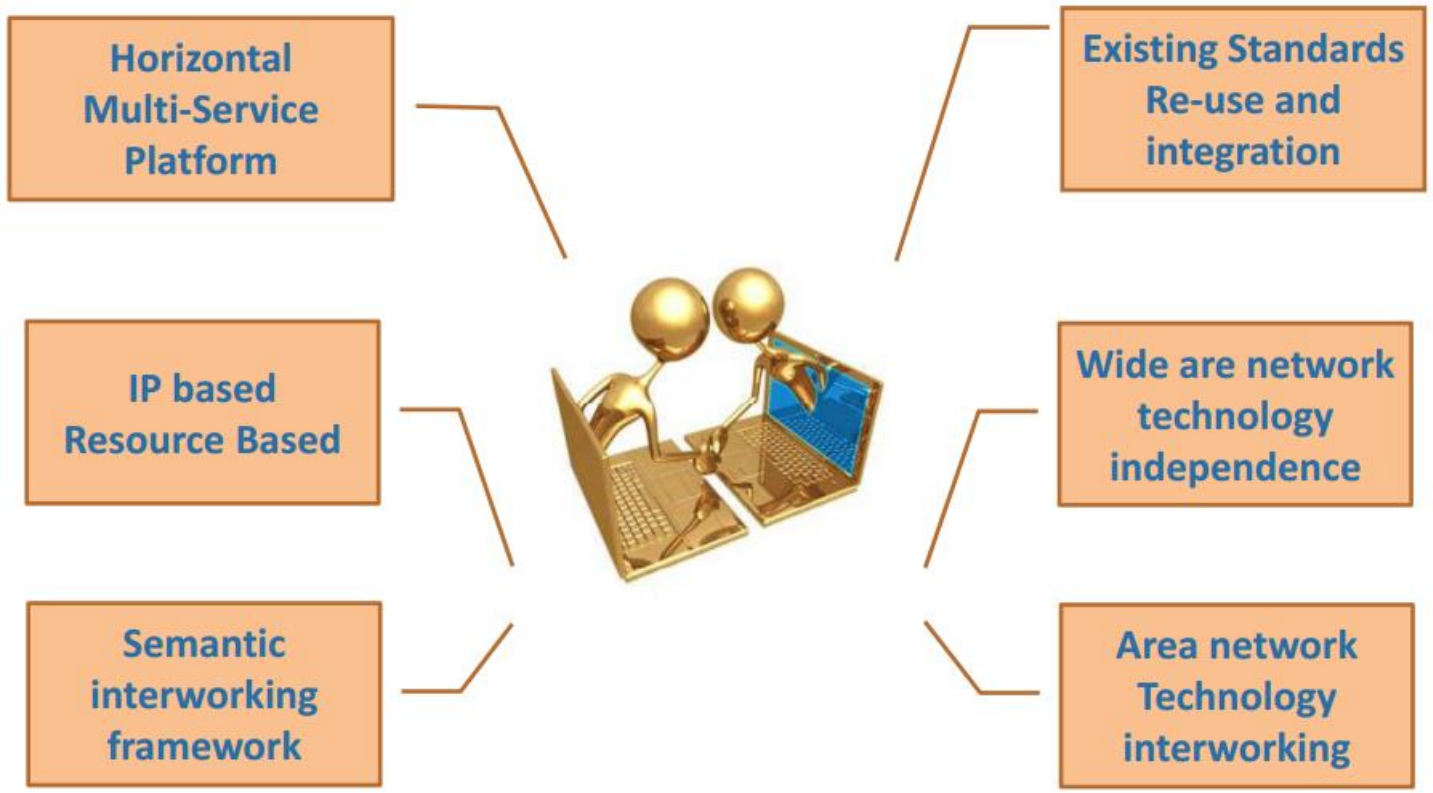
- New and recent standard from OMA focusing on M2M devices
  - Device-Server interface based on open IETF standards (CoAP and DTLS bound for UDP or SMS)
  - The LWM2M Enabler has two components
    - LWM2M Server
    - LWM2M Client
  - Client-Server architecture for the LWM2M Enabler
    - the LWM2M Device acts as a LWM2M Client
    - the M2M service, platform or application acts as the LWM2M Server
  - Multiple Objects, which define Resources, for a Client



ETSI AND ETSI M2M

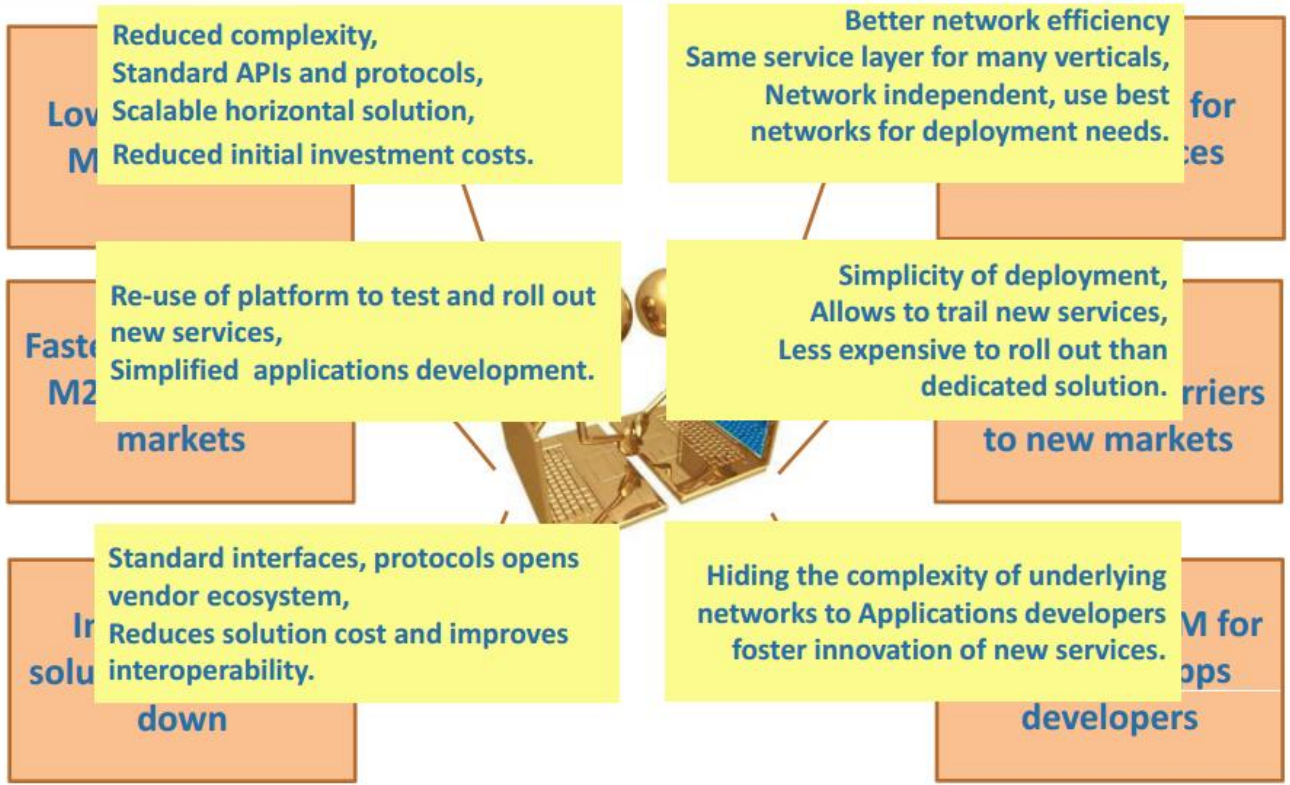
- European Telecommunications Standards Institute
- Not-for-profit organization
  - Over 750 ETSI member organizations, 64 countries, 5 continents
- Produces globally-applicable standards for ICT covering every related technology
- Proposed ETSI M2M aiming at
  - Conducting standardization activities relevant to M2M systems and sensor networks at architecture level
  - Developing and maintaining an end-to-end architecture for M2M with end-to-end IP philosophy behind it

THE ETSI M2M SOLUTION



Source: ETSI

THE ETSI M2M SOLUTION



Source: ETSI

ONEM2M

- Leading global standardization body for M2M and the IoT
- Formed and founded in 2012
  - Seven leading ICT standards development organisations, **ETSI included**
  - Five industry consortia, **OMA included**
- Establishment to develop a **single horizontal platform** for the exchange and sharing of data among all applications
- Release 1 (January 2015): set of 10 specifications
  - covering requirements, architecture, API specifications, security solutions
  - mapping to common industry protocols such as CoAP, MQTT and HTTP
  - making use of OMA and BBF (Broadband Forum) specifications for Device Management capabilities

OM2M AND ONEM2M: THE DIFFERENCE?

- OM2M based on ETSI standard for M2M, now called smartM2M
- ETSI also among the founders of the OneM2M initiative
- Therefore ideas and principles of smartM2M are inside OneM2M
- So OM2M is not far away from OneM2M

IOT ARCHITECTURES

- Large number of schemes, strategies, approaches to enable communication among heterogeneous devices
- Many architectures have been proposed to meet vertical IoT scenarios (e.g., Smart City, Smart Home, Smart Health, …)
- Definitively, a definitive and unique IoT Reference Architecture does not exist
- Some recent EU projects have been trying to define reference IoT architectures
- IoT-A is an example, which subsequently inspired other projects

INTERNET OF THINGS – ARCHITECTURES

- IoT – A project lasted 3 years
- Proposed an architectural reference model and the definition of an initial set of key building blocks
- Detailed results
  - Architectural reference model for the interoperability of IoT systems
  - Principles/guidelines for technical design of its protocols, interfaces and algorithms
  - Mechanism for its efficient integration into the Future Internet service layer
  - Scalable look up and discovery of Internet-of-Things resources
  - Novel platform components

THANKS FOR YOUR ATTENTION !

Mirko Franceschinis

Researcher

Pervasive Technologies (PerT) Reasearch Area

+39 011 227615

franceschinis@ismb.it