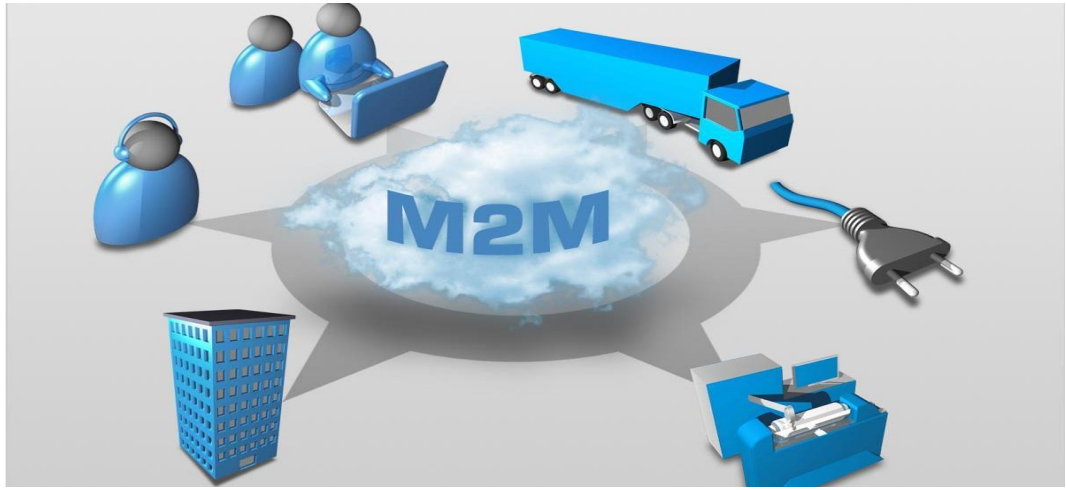
M2M to IOT - An Architectural Overview

Chapter outline

- Building an architecture
- Design Principal and needed capabilities
- An IOT architecture outline
- Standards considerations

M2M Communication

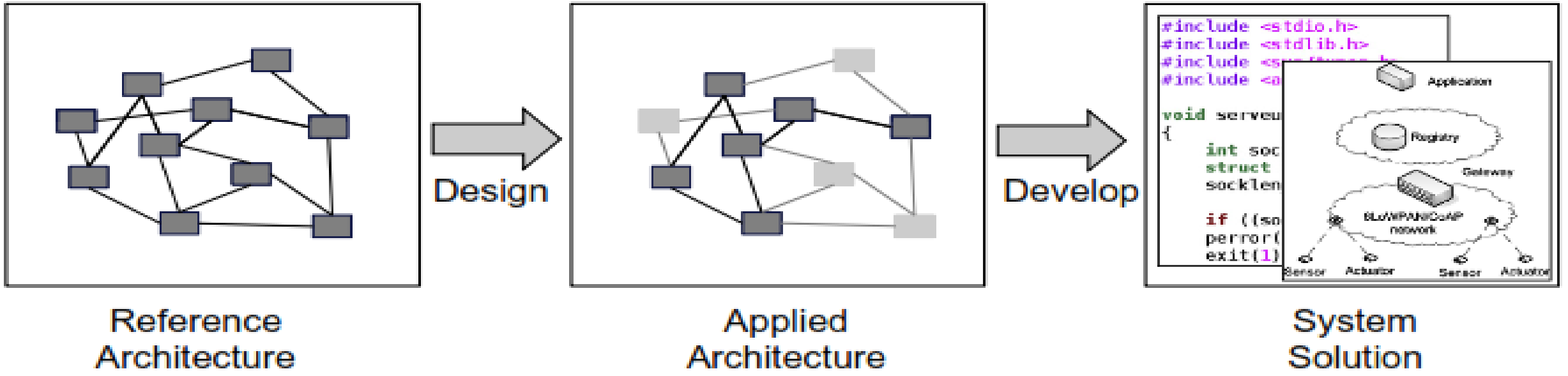
- M2M has recently evolved to where devices can connect and communicate over wired or wireless network with less or without human intervention
- Data are generated, processed and exchanged though a fully automatic fashion.
- M2M is also named as Machine Type Communication (MTC)
- Human Intervention and control is replaced by self-configuration, self-management, self-organization, and self-healing processes from automatize services such as smart home, smart city, smart water, smart transport etc..



Building an architecture

- The term Architecture has many interpretations.
- *Architecture refers to the description of the main conceptual elements, the actual elements of a target system, how they related to each other, and principles for the design of the architecture*
- A conceptual element refers to an intended function, a piece of data, or a service.
- An actual element, meanwhile, refers to a technology building block or a protocol.
- The term "reference architecture" relates to a generalized model that contains the richest set of elements and relations that are of relevance to the domain "Internet of Things."
- When looking at solving a particular problem or designing a target application the reference architecture is to be used as an aid to design an applied architecture.
- The applied architecture is then the blueprint used to develop the actual system solution

Building an architecture



Reference Architecture

Applied Architecture

System Solution

Fig. Reference architecture to a system solution

Building an architecture

- When creating a model for the reference architecture, one needs to establish overall objectives for the architecture as well as design principles that come from understanding some of the desired major features of the resulting system solution.
- For instance, an overall objective might be to decouple application logic from communication mechanisms, and typical design principles might then be to design for protocol interoperability and to design for encapsulated service descriptions.
- These objectives and principles have to be derived from a deeper understanding of the actual problem domain, and is typically done by identifying recurring problems or type solutions, and thus by that, extracting common design patterns.
- The problem domain establishes the foundation for the subsequent solutions.
- It is common to partition the architecture work and solution work into two domains, each focusing on specific issues of relevance at the different levels of abstraction

Building an architecture

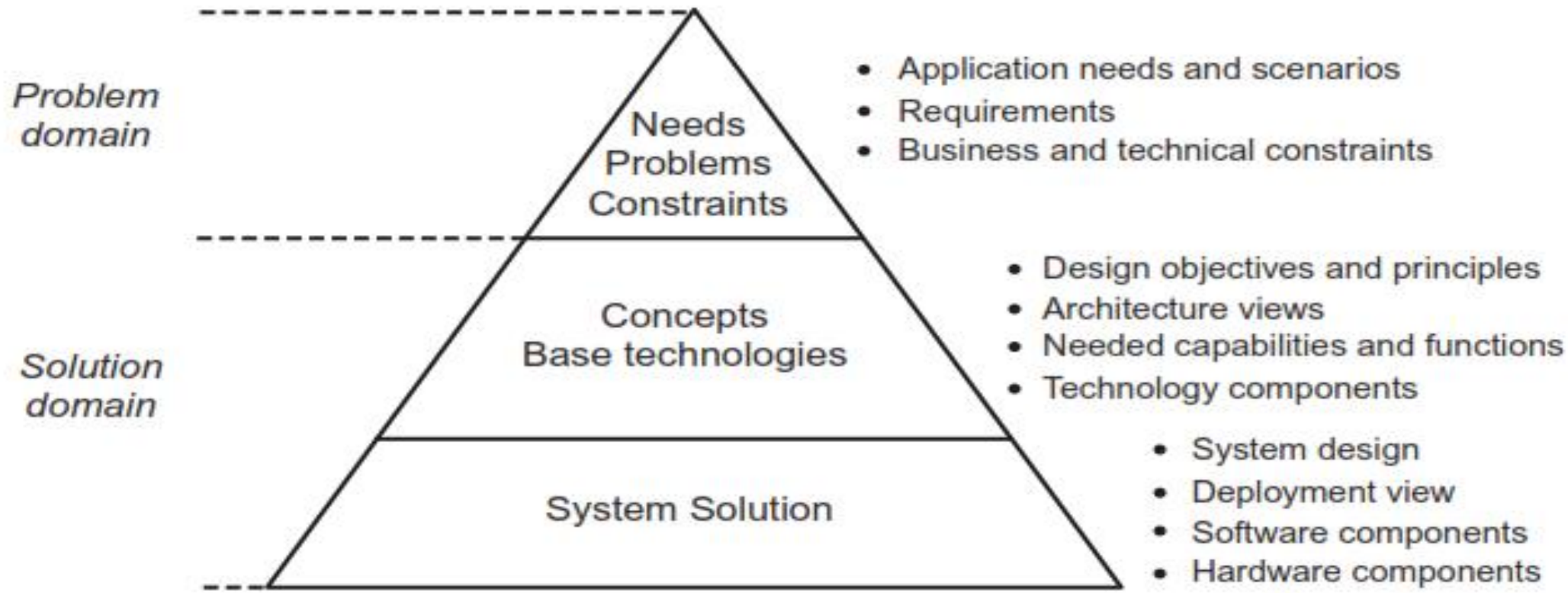


Fig. Problem and Solution domain partitioning

Building an architecture

- Where design objectives and principles are established, conceptual views are refined, required functions are identified, and where logical partitions of functionality and information are described.
- Often this is where a logical architecture is defined, or network architecture in the form of a network topology diagram is produced.
- It is also common to identify suitable technology components such as operating systems and protocols or protocol stacks at this level.
- The actual system solution is finally captured by a system design that typically results in actual software and hardware components, as well as information on how these are to be configured, deployed, and provisioned.

Main Design Principles and Needed capabilities

- There are three primary sources identified for designing architecture of IOT and M2M
  - Larger European 7th Framework Program research projects, SENSEI (2013)
  - IoT-A and
  - ETSI

SENSEI

- The approach taken in SENSEI was to develop an architecture and technology building blocks that enable a "Real World integration in a future Internet."
- Key features include the definition of a real world services interface and the integration of numerous Wireless Sensor and Actuator Network deployments into a common services infrastructure on a global scale.
- The service infrastructure provides a set of services that are common to a vast range of application services and is separated from any underlying communication network for which the only assumption made was that it should be based on Internet Protocol (IP).

Main Design Principles and Needed capabilities

SENSEI

- The architecture relies on the separation of resources providing sensing and actuation from the actual devices, a set of contextual and real world entity-centric services, and the users of the services.
- SENSEI further relies on an open ended constellation of providers and users, and also provides a reference model for different business roles.
- A number of design principles and guidelines are identified, and so is a set of requirements.
- Finally, the architecture itself contains a set of key functional capabilities.

Main Design Principles and Needed capabilities

ETSI

- The telecommunications industry, meanwhile, has focused on defining a common service core for supporting various M2M applications, and that is agnostic to underlying networks in ETSI TC M2M.
- The approach taken has been to analyze a set of M2M use cases, derive a set of M2M service requirements, and then to specify an architecture as well as a set of supporting system interfaces.
- Similar to SENSEI, there was a clear approach towards a horizontal system with separation of devices, gateways, communications networks, and the creation of a common service core and a set of applications, all separated by defined reference points.

Main Design Principles and Needed capabilities

IOT-A

- Approach taken in IoT-A differs from the SENSAI and ETSI approaches in the sense that instead of defining a single architecture, a reference architecture is created, captured in what the IoT-A refers to as the Architectural Reference Model (ARM).
- The vision of IoT-A is, via the ARM, to establish a means to achieve a high degree of interoperability between different IoT solutions at the different system levels of communication, service, and information.
- IoT-A provides a set of different architectural views, establishes a proposed terminology and a set of Unified Requirements (IoT-A UNI 2013).
- Furthermore, IoT-A proposes a methodology for how to arrive at a concrete architecture based on use cases and requirements.

Main Design Principles and Needed capabilities

SENSAI,ETSI and IOT-A

- Comparing these different approaches, a common feature is the focus on a horizontal system approach.
- There is a clear separation of the underlying communication networks and related technologies from capabilities that enable services.
- There is a clear desire to define uniform interfaces towards the devices that provide sensing and actuation, including abstraction of services the devices provide.
- Desire to separate logic that is highly application-specific from logic that is common across a large set of applications.

Main Design Principles and Needed capabilities

- Identified the need for a horizontal approach from a set of different perspectives
- need for horizontal integration across value chains at different levels
- need to integrate multiple infrastructures;
- the need to reuse existing deployments, to name a few.
- Taking other key identified features into consideration as well, such as being able to support openended service development and providing security and being reliable.

Main Design Principles and Needed capabilities

The overall design objective of IoT architecture shall be to target a horizontal system of real-world services that are open, service-oriented, secure, and offer trust.

- Further analyzing both the referenced existing work on both needed capabilities and direct IoT implications, we can also derive a set of supporting design principles that target different means to fulfill the overall architecture objective.

- These design principles have a set of interpretations and further expectations on needed technology solutions.

Main Design Principles and Needed capabilities

Design for reuse of deployed IoT resources across application domains

- Deployed IoT resources shall be able to be used in a vast range of different applications.
- This implies that devices shall be made application independent and that the basic and atomic services they expose in terms of sensing and actuation shall be done in a (to the greatest extent possible) uniform way.
- A system design will benefit from providing an abstracted view of these basic underlying services that also are decoupled from the devices that provide the services.

Main Design Principles and Needed capabilities

Design for a set of support services that provide open service-oriented capabilities and can be used for application development and execution.

- Service layer-oriented M2M standardization in ETSI M2M is the definition of a set of common application independent service capabilities.
- These support services shall in general cater to the typical environment of a stakeholder where IoT applications are to be built, such as an open environment, and shall in particular provide support for a few key service capabilities that are central from an IoT perspective.
- The open environment of IoT will, for instance, require mechanisms for authorized usage of services and resources, authentication, and associated identity management.

Main Design Principles and Needed capabilities

Design for different abstraction levels that hide underlying complexities and heterogeneities

- IoT solutions can involve a large number of different devices and associated sensor modalities, and involve a large set of different actors providing services and information that need to be composed and accessed with different levels of aggregation.
- A system design will greatly benefit from providing the necessary abstractions both of underlying technologies, data and service representation, as well as granularity of information and services.
- hiding device-side technologies and providing simple abstractions of the sensing and actuation services is one aspect
- Another is the means to perform aggregation of information or knowledge representation.
- requirement to have appropriate knowledge management tools and a means to compose complex services as well as decomposition of complex queries and tasks down to individual and atomic actuation tasks

Main Design Principles and Needed capabilities

Design for sensing and actors taking on different roles of providing and using services across different business domains and value chains.

- IoT solutions can be run across a set of departments within an enterprise, or across a set of enterprises in a value system, or even be provided in a truly open environment.
- The business contexts can then be viewed as no market (entirely intra organizational), as closed markets (finite and predetermined set of business actors in a specific value system or value chain), or as open markets (undefined and open-ended number of participants)
- The first thing that needs to be provided is a set of mechanisms that ensure security and trust. Trust and identity management that refer to the different stakeholders is a fundamental requirement.
- Authentication and authorization of access to use services as well as to be able to provide services is then a second requirement.
- The third requirement is the capability to be able to do auditing and to provide accountability so that stakeholders can enforce liability if the need occurs.

Main Design Principles and Needed capabilities

- The next fundamental requirement is to ensure interoperability. This is needed at different levels across the interaction points between the stakeholders.
- Primary examples are to ensure data and information interoperability on the semantic level, and means to connect business processes across organizational and administrative boundaries.
- The third fundamental requirement is related to the market perspective, whether the markets are closed or fully open. Mechanisms that provide compensation for used services or data between service users and service providers are needed.

Main Design Principles and Needed capabilities

Design for ensuring trust, security, and privacy.

- Trust within IoT often implies reliability, which can be both ensuring the availability of services as well as how dependable the services are, and that data is only used for the purposes the end-user has agreed to. One important aspect of dependability is the accuracy of data or information, as you can have multiple sources of IoT data.
- Concepts like Quality of Information become important, especially considering that a piece of information can very well be accurate enough for one application, but not for another.
- As has been already mentioned, security and privacy are potential barriers for IoT adoption and represent key areas to address when building solutions.
- Privacy needs to be ensured by, for example, anonymization of data, seeing that profiling of individuals is not easily done or even made undoable. Still, it is foreseen that authorities and agencies will require support to get access to data and information for the purpose of national security or public safety.

Main Design Principles and Needed capabilities

Design for scalability, performance, and effectiveness

- IoT deployments will happen on a global scale and are foreseen to involve billions of deployed nodes
- Sensor data will be provided with a wide range of different characteristics. Data may be very infrequent (e.g. alarms or detected abnormal events), or may be coming as real-time data streams, all dependent on the type of data needed or based on application needs.
- Scalability aspects of importance include the large number of devices and amounts of data produced that needs to be processed or stored.
- Performance includes consideration of mission-critical applications such as Supervisory Control And Data Acquisition (SCADA) systems with extreme requirements on latency

Main Design Principles and Needed capabilities

Design for evolvability, heterogeneity, and simplicity of integration

- Technology is constantly changing, and given the nature of IoT deployments where devices and sensor nodes are expected to be operational and in the field for many years, sometimes with lifecycles of over 15 years (e.g. smart meters), IoT solutions must be able to withstand and cater to introduction and use of new technologies as well as handling of legacy deployments.
- Handling heterogeneity is also important since especially device-oriented technologies used across industries are very different.
- Means to integrate legacy devices using many different protocols becomes a necessity, and gateways of different types and with different capabilities will be essential to expose capabilities of legacy devices in a uniform manner.

Design for simplicity of management

- IoT adaptation, simplicity of management is an important capability that needs to be properly taken care of when designing IoT solutions.
- Auto-configuration and auto-provisioning are key and well-known means that can ease deployment of IoT devices, and are also very important to lower operating expenditures (OPEX).

Main Design Principles and Needed capabilities

Design for different service delivery models

- Trends to move from product offerings to a more combined product and service offering in a number of industries, for instance, connected vehicles, and Software as a Service (SaaS) as a delivery model.
- IoT with the wide span of possible applications clearly benefit from elasticity in deployment of solutions, all to meet the long-tail aspect. Cloud and virtualization technologies play a key enabler role in delivering future IoT services.

Design for lifecycle support.

- The lifecycle phases are: planning, development, deployment, and execution. Management aspects include deployment efficiency, design time tools, and run-time management.

IOT Architecture

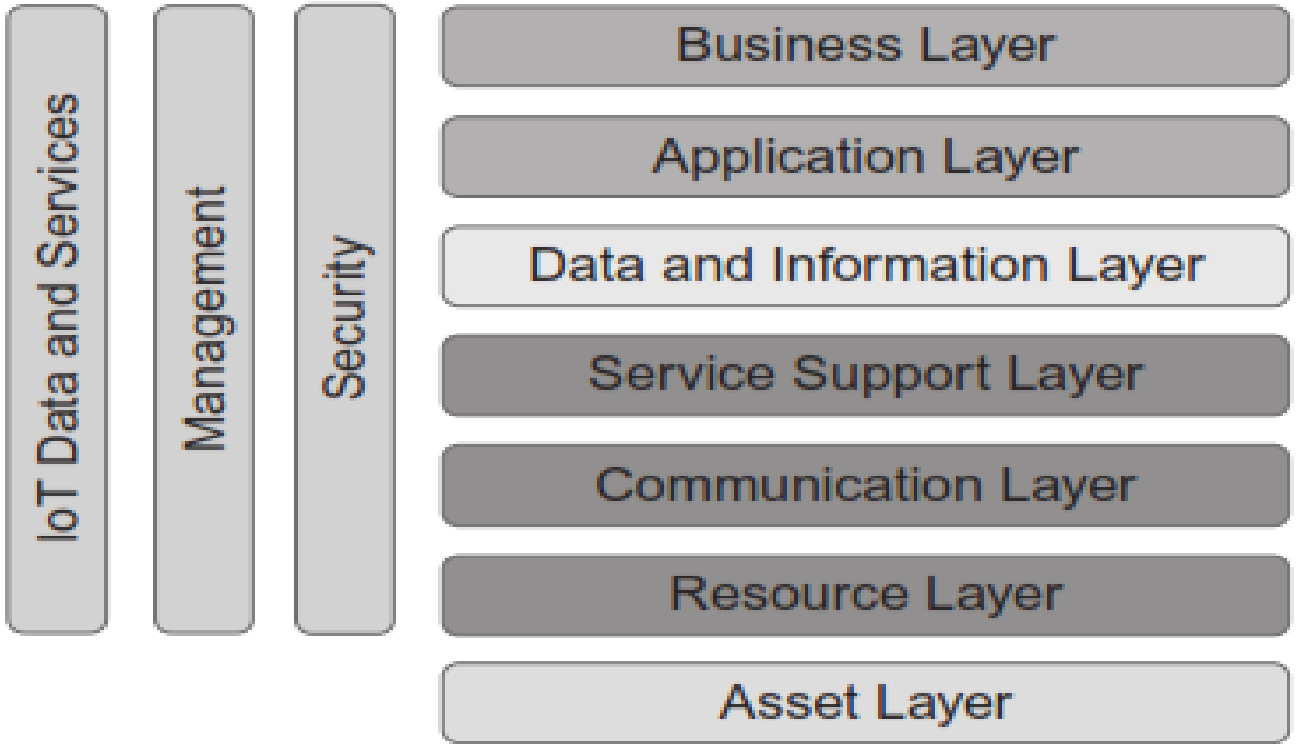


Fig. IOT architecture

IOT Architecture

Asset Layer

- This layer not providing any functionality within a target solution, but represents the most important reason for any IoT application.
- The assets of interest are the real world objects and entities that are subject to being monitored and controlled, as well as having digital representations and identities.
- Assets can also be of a more virtual character, being subjective representations of parts of the real world that are of interest to a person or an organization.
- Assets are instrumented with embedded technologies that bridge the digital realm with the physical world, and that provide the capabilities to monitor and control the assets as well as providing identities to the assets

IOT Architecture

Resource Layer

- The Resource Layer provides the main functional capabilities of sensing, actuation, and embedded identities.
- Sensors and actuators in various devices that may be smartphones or Wireless Sensor Actuator Networks (WSANs), M2M devices like smart meters, or other sensor/actuator nodes, deliver these functions.
- This is also where gateways of different types are placed that can provide aggregation or other capabilities that are closely related to these basic resources.
- Identification of assets can be provided by different types of tags; for instance, Radio Frequency Identification(RFID) as in (ISO/IEC RFID 2013), or optical codes like bar codes or Quick Response (QR) codes

IOT Architecture

Communication Layer

- The purpose of the Communication Layer is to provide the means for connectivity between the resources on one end and the different computing infrastructures that host and execute service support logic and application logic on the other end.
- Different types of networks realize the connectivity, and it is customary to differentiate between the notion of a Local Area Network (LAN) and a Wide Area Network (WAN).
- Particularly in the mobile network industry, there are different models for how the communications services are provided that include wholesale of access, and dedicated virtual network operators that focus on managed M2M connectivity offerings without owning licensed mobile spectrum or actual network resources.
- Prominent examples of wireless LAN networking technologies include the (IEEE 802.11 2013) and (IEEE 802.15.4 2013) families, as well as (Bluetooth 2013), which has a recent protocol addition called (Bluetooth Low Energy 2013) that targets typical IoT applications.
- IEEE 802.15.4 is the basis for protocol stacks that target different M2M and IoT applications, for instance, the ZigBee specifications (Zigbee 2013a), the proprietary protocol stack (Z-Wave 2013) for home automation, and ISA100.11a (ISA100 2013) for industry automation

IOT Architecture

Communication Layer

- Many of the existing legacy industry specific LAN protocol stacks do not use IP as the networking protocol, but there is a growing number of examples where the legacy protocol stacks are migrated towards IP, for instance, ZigBee IP, BACnet over IP, and IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) Bluetooth (IETF 6LoWPAN BTLE 2013)
- From a communication layer perspective, gateways are primarily used to do interworking or protocol translation at different levels of the protocol stack

IOT Architecture

Service Support Layer

- Service Support Layer provide service support such as executing in data centers or server farms inside organizations or in a cloud environment.
- These support services can provide uniform handling of the underlying devices and networks, thus hiding complexities in the communications and resource layers.
- *Examples:* include remote device management that can do remote software upgrades, remote diagnostics or recovery, and dynamically reconfigure application processing such as setting event filters.
- Communication-related functions include selection of communication channels if different networks can be used in parallel, for example, for reliability purposes, and publish subscribe and message queue mechanisms.
- Location Based Service (LBS) capabilities and various Geographic Information System (GIS) services are also important for many IoT applications.

IOT Architecture

Data and Information Layer

- Resource, Communication, and Service Support layers have concrete realizations in terms of devices and tags, networks and network nodes, and computer servers, the Data and Information Layer provides a more abstract set of functions as its main purposes are to capture knowledge and provide advanced control logic support
- Knowledge Management Framework (KMF) as a collective term to include data, information, domain-specific knowledge, actionable services descriptions as, for example, represented by single actuators or more complex composite sensing and actuation services, service descriptors, rules, process or workflow descriptions, etc
- The KMF needs to integrate anything from single pieces of data from individual sensors to highly domain-specific expert knowledge into a common knowledge fabric
- Key concepts to construct the KMF include semantic annotation, Linked Data (Bizer et al., 2009), and building different ontologies.
- Knowledge is highly dynamic, and different techniques are used to capture knowledge as insights, as well as consume knowledge to learn, draw conclusions, propose or even make decisions based on past experiences, current knowledge, and predicted outcomes of certain actions.

IOT Architecture

Application Layer

- The Application Layer in turn provides the specific IoT applications.
- There is an open-ended array of different applications, and typical examples include smart metering in the Smart Grid, vehicle tracking, building automation, or participatory sensing (PS)

Business Layer

- Business Layer, which focuses on supporting the core business or operations of any enterprise, organization, or individual that is interested in IoT applications.
- This is where any integration of the IoT applications into business processes and enterprise systems takes place
- The enterprise systems can, for example, be Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), or other Business Support Systems (BSS)

IOT Architecture

Business Layer

- The business layer also provides exposure to APIs for third parties to get access to data and information, and can also contain support for direct access to applications
- by human users; for instance, city portal services for citizens in a smart city context, or providing necessary data visualizations to the human workforce in a particular enterprise. The business layer relies on IoT applications as one set of enablers out of many (e.g. field force automation), and takes care of necessary orchestration and composition to support a business process workflow

IOT Architecture

Management

- Management as the name implies, deals with management of various parts of the system solution related to its operation, maintenance, administration, and provisioning.
- This includes management of devices, communications networks, and the general Information Technology (IT) infrastructure as well as configuration and provisioning data, performance of services delivered, etc

IOT Architecture

Security

- Security is about protection of the system, its information and services, from external threats or any other harm.
- Security measures are usually required across all layers, for instance, providing communication security and information security.
- Trust and identity management, and authentication and authorization, are key capabilities.
- From an IoT perspective, management of privacy via, for example, anonymization, is in many instances a specific requirement

IOT Architecture

IOT data and Services

- Data and Service processing can, from a topological perspective, be done in a very distributed fashion and at different levels of complexity.
- Basic event filtering and simpler aggregation, such as data averaging, can take place in individual sensor nodes in WSANs, contextual metadata such as location and temporal information can be added to sensor readings, and further aggregation can take place higher up in the network topology.
- More advanced processing is, for instance, data mining and data analytics that can be done in near real-time. This functional group thus represents the vertical flow of data into knowledge, the abstraction of data and services in different levels, and the process steps of extracting knowledge.
- *knowledge layer* is focused on the organization and representation of knowledge, this functional group is focused on the different processing steps in the data and services value chain, thus at different levels of granularity and abstraction. Different technologies are used to support the different levels of knowledge extraction, processing, reasoning, and decision-making. Well-known technologies here include stream processing, analytics, machine learning, reasoning, and inferencing.

Standards considerations

- Not to provide an overview of relevant standards, but to provide an overview of the landscape in which various relevant standards are developed
- The primary objective of any technology oriented standardization activity is to provide a set of agreed-upon specifications that typically address issues like achieving interoperability in a market with many actors and suppliers.

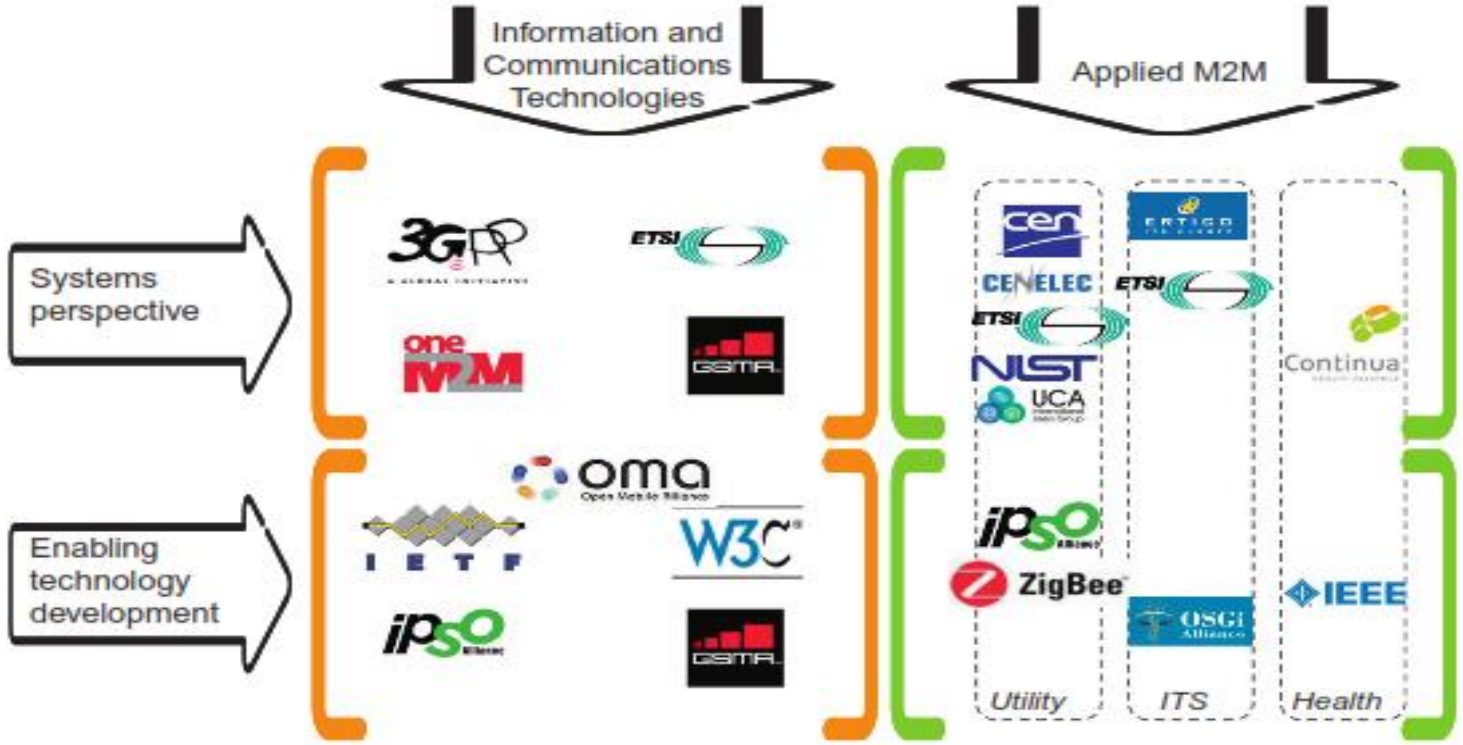


Fig. Landscape of M2M and IoT standardization

Standards considerations

- The first consideration is that standards are developed across a number of different industries. There are a number of standardization organizations and bodies, both proper Standards Development Organizations (SDO) as well as special interest groups and alliances that develop standards specifications.
- Different national and international bodies ratify standards by SDOs, whereas standard specifications developed by special interest groups and alliances are normally agreed-upon and adopted by market actors such as technology manufacturers.
- Examples of international SDOs are the International Telecommunications Union (ITU) and the International Organization for Standardization (ISO), whereas the European Telecommunications Standards Institute (ETSI) and the European Committee for Electrotechnical Standardization (CENELEC) are examples of regional SDOs.
- Other independent international standardization organizations include the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF).

Standards considerations

- From an M2M and IoT perspective, one can make a distinction between standards developed within the Information and Communications Technology (ICT) industry, and standards that are developed within a specific industry segment, such as the Health, Transportation, or Electricity industry segments.
- The ICT industry develops technologies that are targeting use in different other industry segments, and the applied IoT industry segments make use of the ICT standards to varying degrees in developing their standards.
- As all these industries have a long history of providing their own industry specific standards, there is an inheritance and legacy of practices and technologies that continue to develop, but as we see more and more converging interests across industries, standards will have to cater to reducing technology fragmentation.

Standards considerations

- The second consideration is that some standardization activities define entire systems or parts of systems, and other standards organizations target development of specific pieces of technologies, for instance, specific protocols.
- System standards can address a 3G mobile communication network as defined within the 3rd Generation Partnership Project (3GPP) or standards towards the Smart Grid as done by the National Institute of Standards and Technology (NIST). Organizations like the IETF, on the other hand, focus on developing the protocol suite of the Internet without any effort to specify a system standard beyond what is already in existence in a few key IETF Request For Comments (RFC) such as RFC1958, establishing the Architectural Principles of the Internet.
- The natural observation is that system standards rely on the enabling technology components as the foundation, but as there generally are many competing technology components (e.g. protocol stacks), the adoption into a system standard is not a straightforward route

Standards considerations

- The third and final consideration is about the lifecycle process of standards. Many times, standards are emerging as a result of collaborative research involving both academia and industry. In other situations, technology selection for standardization can happen as part of regulatory or legislative processes. Within the European Union, the European Commission has issued so called Mandates that can have a direct impact on the choice of technology, which hence precedes any subsequent standardization activity.
- An example of this is the European Mandate M490 (EC M490 2011) on the Smart Grid that was issued by the European Commission to the European Standardization Organizations to come together to develop and update a set of consistent standards within a common European framework that integrates various ICT and electrical architectures and processes to achieve interoperability for the European Smart Grid.
- As a conclusion, technology selection does not only happen in the process of standardization