Applying the Internet of Things and Internet of People paradigms to the urban context

Ph.D. Dissertation of: Alexandru Serbanati

Advisor: Prof. Gianluigi Mondaini
Prof. Stefano Panunzi

Curriculum supervisor: Prof. Stefano Lenci

XI edition - new series
Acknowledgements

This work involved years of research and is the result of a long process with many actors and many factors. Through this long process, which is a piece of my life, there have been some actors that influenced very positively the process. First of all a big thank you to my tutors, prof. Stefano Panunzi and prof. Gianluigi Mondaini, who believed in me even when I didn’t. Many thanks to my friend and boss prof. Carlo Medaglia, who gave me the chance to take the path which I’m walking now and without whom I would have never been able to aim so high in many aspects of my academic life. A warm thank you also goes to the partners of the IoT-A project, from whom I borrowed a large part of my current knowledge in the field of Internet of Things. I would also like to thank to all those that volunteered to answer the survey and generally provide constructive input for this thesis. Last but not least a big thank you to my parents. Getting to the finish line is not only an academic issue. Thank you for always being there when the need arose.
Abstract

Urban systems host a large amount of processes that are relevant to the everyday life of its citizens, to the economy to the industry or to the city administration. Albeit the importance of these processes, currently we are not able to have enough information about them or even to monitor them at all.

This work proposes the use of the Internet of Thing and People (IoTP) as the paradigm for the information systems controlling the different domains and sub-systems of urban systems which would allow to monitor the physical and social part of urban processes. The adoption of IoTP will improve our knowledge and allow to increase the efficiency of processes, identify social issues and improve the effectiveness of urban planning.

In this work, the design of urban systems is analysed and linked to the benefits of using IoTP-based information systems. Then, key elements of the IoTP reference architecture, such as the domain model, the interaction model, the resource model and the functional model, are provided.
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Concept and motivation</td>
<td>1</td>
</tr>
<tr>
<td>1.1.1</td>
<td>The context</td>
<td>1</td>
</tr>
<tr>
<td>1.1.2</td>
<td>The motivation</td>
<td>1</td>
</tr>
<tr>
<td>1.1.3</td>
<td>The concept</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>Interdisciplinary approach</td>
<td>4</td>
</tr>
<tr>
<td>1.3</td>
<td>Structure of the Document</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Modelling the city system</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>Engineering urban systems</td>
<td>6</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Complex systems</td>
<td>6</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Conceptual Modelling in Systems Engineering</td>
<td>8</td>
</tr>
<tr>
<td>2.1.3</td>
<td>Modelling systems in the Information Era</td>
<td>8</td>
</tr>
<tr>
<td>2.1.4</td>
<td>Information system analysis and design</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>Conceptual modelling of urban processes</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>IoTP State of the Art</td>
<td>15</td>
</tr>
<tr>
<td>3.1</td>
<td>Internet of Things</td>
<td>15</td>
</tr>
<tr>
<td>3.1.1</td>
<td>History of the Internet of Things</td>
<td>15</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Technological background</td>
<td>17</td>
</tr>
<tr>
<td>3.1.3</td>
<td>A look into IoT protocols</td>
<td>18</td>
</tr>
<tr>
<td>3.1.4</td>
<td>The IoT-A Architectural Reference Model for the IoT</td>
<td>19</td>
</tr>
<tr>
<td>3.1.4.1</td>
<td>The IoT-A Domain Model</td>
<td>21</td>
</tr>
<tr>
<td>3.2</td>
<td>Internet of People</td>
<td>23</td>
</tr>
<tr>
<td>3.2.1</td>
<td>History of the Internet of People</td>
<td>23</td>
</tr>
<tr>
<td>3.2.2</td>
<td>IoP Application classes</td>
<td>25</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Architecting the Internet of People</td>
<td>26</td>
</tr>
<tr>
<td>3.2.4</td>
<td>Adding Intelligence to the Context</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>Relevance of Future Internet</td>
<td>28</td>
</tr>
<tr>
<td>4.1</td>
<td>Bringing the “smart” to “Smart Cities”</td>
<td>28</td>
</tr>
<tr>
<td>4.2</td>
<td>The Internet of (urban) Things</td>
<td>29</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Application fields</td>
<td>29</td>
</tr>
<tr>
<td>4.3</td>
<td>Urban IoT: see through the citizen’s eyes</td>
<td>30</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Participatory Sensing</td>
<td>30</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Datamining</td>
<td>31</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Application fields</td>
<td>31</td>
</tr>
<tr>
<td>4.4</td>
<td>Bringing the Internet of Things and People to life</td>
<td>32</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Cross-domain synergies and business opportunities</td>
<td>32</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Interoperability is the key</td>
<td>33</td>
</tr>
<tr>
<td>4.5</td>
<td>Information quality</td>
<td>34</td>
</tr>
<tr>
<td>5</td>
<td>Building blocks of the Urban IoTP Reference Architecture</td>
<td>36</td>
</tr>
<tr>
<td>5.1</td>
<td>A generic architecture of urban IoTP applications</td>
<td>36</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Methodology</td>
<td>36</td>
</tr>
<tr>
<td>5.2</td>
<td>A comprehensive Domain Model</td>
<td>37</td>
</tr>
</tbody>
</table>
5.3. Interaction model of the IoTP ................................................................. 43
5.4. Resource Model .............................................................................. 44
5.5. The Functional Model .................................................................... 46
  5.5.1 Use Cases .................................................................................. 47
  5.5.2 Resource Lookup ....................................................................... 47
  5.5.3 Interest Subscription ................................................................. 48
  5.5.4 Security .................................................................................... 49
5.6. IoTP functional architecture ............................................................ 50

Chapter 6. Concluding Remarks .............................................................. 53
  6.1. Conclusions .................................................................................. 53
  6.2. Challenges ................................................................................... 53
  6.3. Future Work ................................................................................ 54

References ............................................................................................ 57

Appendices .......................................................................................... 62
  A. Requirement gathering for IoT ....................................................... 62
List of Figures

Figure 1. Hierarchical decomposition of a complex system such as a generic Urban System .......................................................... 7
Figure 2: Real world and its models ................................................................................................................. 8
Figure 3: Generic simplified model of a process .................................................................................................. 11
Figure 4: A generic model of urban process ...................................................................................................... 12
Figure 5: Visual representation of the IoT paradigm ............................................................................................... 17
Figure 6: The process of deriving a specific system architecture from the Architectural Reference Model ......................................................................................................................... 20
Figure 7: The IoT-A Domain Model as depicted in [36] ......................................................................................... 22
Figure 8: Future Internet overview, taken from [44] ............................................................................................. 24
Figure 9: Possible new business segmentation and the relative location in the IoTP ........................................ 33
Figure 10: The process of creating a Reference Architecture ............................................................................. 37
Figure 11: Fundamental abstraction of the real-world interaction that IoTP-based information systems must carry out in the digital world ................................................................. 38
Figure 12: An EoI can be a Physical Entity, a Social Entity or a composition of both .................................. 39
Figure 13: Resources Provide the capability of interacting with an EoI .............................................................. 39
Figure 14: Adapters translate and transfer information from one domain to another ........................................ 40
Figure 15: Adapter class and its specializations .................................................................................................. 41
Figure 16: The structure of a complex EoI can be reproduced in a complex VE ............................................. 42
Figure 17: The high-level picture of the IoTP domain model ......................................................................... 43
Figure 18: Service invocation. The resource access is transparent to the User .................................................. 47
Figure 19: Resource lookup use case .................................................................................................................. 48
Figure 20: Interest subscription usecase ............................................................................................................ 49
Figure 21: Example of the functional components the IoTP Infrastructure ...................................................... 50
Figure 22: Description of the process of deriving a reference model of IoTP ................................................... 54
List of Tables

Table 1: Supported communication modes in IoP applications related to the number of peers and source authentication requirements........................................................................17
<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAC</td>
<td>Authentication Based Access Control</td>
</tr>
<tr>
<td>autoID</td>
<td>Automatic Identification</td>
</tr>
<tr>
<td>CASAGRAS</td>
<td>Coordination and Support Action for Global RFID-related Activities and Standardisation</td>
</tr>
<tr>
<td>DM</td>
<td>Domain Model</td>
</tr>
<tr>
<td>HIP</td>
<td>Host Identity Protocol</td>
</tr>
<tr>
<td>IM</td>
<td>Information Model</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoT-P</td>
<td>Internet of Things and People</td>
</tr>
<tr>
<td>IoT-A</td>
<td>Internet of Things Architecture (project)</td>
</tr>
<tr>
<td>LR-WPAN</td>
<td>Low Rate Wireless Personal Area Network</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control protocol layer</td>
</tr>
<tr>
<td>MBP</td>
<td>Micro Blogging Platform</td>
</tr>
<tr>
<td>NWK</td>
<td>Network protocol layer</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>SAN</td>
<td>Sensor and Actuator Network</td>
</tr>
<tr>
<td>SN</td>
<td>Social Network</td>
</tr>
<tr>
<td>SNS</td>
<td>Social Network Site</td>
</tr>
<tr>
<td>SRA</td>
<td>Software Reference Architecture</td>
</tr>
<tr>
<td>TRA</td>
<td>Transport protocol layer</td>
</tr>
<tr>
<td>UWAD</td>
<td>Urban Web-Aided Design</td>
</tr>
<tr>
<td>WSAN</td>
<td>Wireless Sensor and Actuator Network</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction

1.1. Concept and motivation

1.1.1 The context

The pace of our evolution has been accelerating in the last century. Cities are not immune to these trends and evolve under the pressure of several drivers that might or might not be evident.

As confirmed by the United Nations Population Fund reports from since 2007 [1], such drivers can be, either directly or indirectly, the global population increase, increasing lack of resources, shift of population from rural to urban areas and consequent population density increase. The latter in particular threatens to bring the urban infrastructure (energy distribution, transportation, waste management and supply distribution) to a collapse.

Climate change [2], on the other hand, demands to take into account sustainability of urban processes. In order to address this issue, many municipalities are reviewing their approach to governance, focusing in first place on the opportunity provided by ICT to increase the efficiency and effectiveness of urban processes [3].

In this rushing pace, all the actors of the urban scenario, from municipalities to private companies, need to introduce constructive drivers that can orientate the evolution of cities in directions that improve the sustainability of urban systems and processes.

Currently, ICT in its many declinations is one of the most effective tools for what concerns improving the quality and efficiency of services, and of processes in general. It can provide automation and almost instantaneous transfer of information, regardless of the distance between the physical location of the source and of the consumer of the information.

1.1.2 The motivation

In [4] Alexander Christopher introduces, with regard to towns, the “idea of a growing whole” with these words:

“When we say that something grows as a whole, we mean that its own wholeness is the birthplace, the origin, and the continuous creator of its ongoing growth. That its new growth emerges from specific, peculiar structural nature of its past. That is an autonomous whole, whose internal laws, and whose emergence, govern its continuation.”

There is a background idea of causality and consequentiality in this paragraph: the evolution is influenced by the past. The knowledge of previous conditions is essential to understand a system and its evolution. This is also the basic assumption for making forecasts.

Until now, it seems that an efficient and integrated approach to urban monitoring – let alone control or forecasting – is missing. The processes that exist and occur in cities cannot be
monitored in a suitable way due to the lack of procedures, high costs, scale of phenomena and so on.

The monitoring of urban-related variables is generally made by public personnel that carry out direct or indirect measurements. This process is very costly and doesn’t scale well with the ever-increasing size of urban entities. As a consequence, the data collected is few and has a low quality. Moreover, it has a very low time- and spatial-density compared both to other fields of measurement and to the needs of urban management.

With this data, the visibility of urban variables is incomplete, shallow, vague and delayed. This means that the processes taking place in the urban context, which affect and are affected by these variables, are difficult to understand, easy to misunderstand or, even worse maybe, completely invisible.

This situation must change if we want to understand the mechanisms of our urban systems. And understanding the processes behind the (urban) curtains is necessary if we want that the cities of the future to be sustainable from an environmental, social and economic point of view.

This PhD work starts from the realization that more data is needed in order to understand the urban processes.

The initial idea was to address the issue thorough the application of the Internet of Things, an ICT paradigm that was the topic of my previous research and that preaches the pervasive distribution of communicating embedded devices in the environment. This could indeed solve the need of high resolution data for the monitoring of the physical part of urban processes.

But then a huge and relevant part of the drivers and impacts of urban processes was still missing: the social one. It was straightforward then that the huge amount of data published or exchanged through the different types of social networks (portals, blogs and microblog messaging) could be a valuable aid. Hence it was decided to include in the scope of this research the Internet of People.

This paradigm proposes and supports new ways of interaction among social entities, which, in the urban context, means that urban actors are more aware of the social aspects in their environment and the processes of urban systems can be monitored also from their social point of view.

1.1.3 The concept

There are though many local, vertical solutions based on real-time Sensor and Actuation Networks (SAN) which improve the efficiency of specific systems. At the same time, social networks collect and transfer a huge amount of information about people. These two tools can be used to identify, analyze and even influence the drivers that affect the processes and the evolution of a city.

While the previous statement is valid in many application fields, the most relevant is probably the urban one. In this context, the potential that could be leveraged, yet still unused, is huge. Until now, automatic data collection – and even less context-awareness and actuation – has only been used in limited contexts, generally related to vertical and closed applications. With the wider and more pervasive adoption of ICT-intensive solutions, the scientific community began to conceive a world of pervasive networks of people and devices that could monitor or even control different aspects of the physical
world. This is the beginning of the adoption of the aforementioned ICT paradigm called Internet of Things and People (IoTP).

The most suited environment for the flourishing of the IoTP are urban areas because they provide some key elements that can favour the advent of this new paradigm:

- an existing, pervasive communication infrastructure based on wired (xDSL and optical fibre) as well as wireless solutions (WiMax, HSPDA/LTE, ...) [5],
- a set of vertical, already existing and working applications which though are isolated and not interoperating, and which are thus not leveraging the possible synergies between different data-collection systems,
- a set of existing data collection processes that could but are not yet (or not fully) managed by ICT solutions.

As stated in the previous section, there is also a clear need for more efficient data collection processes in order to improve our knowledge regarding processes in urban areas to a global perspective.

So why aren’t we already living in the IoTP world?

One of the reasons lies in the fact that the best practices in the system architecture design demand to capture and then maximize the reuse of existing knowledge base, shared best practices and experience, possibly integrating it in systems as modular components.

Currently, the design and development of ICT systems relies on a huge base of existing assets which allows architects to reuse them and design from scratch only a very small part of the system. In other words, designers leverage the existence of several reference architectures.

In literature the concept of reference architecture captures the invariant architectural aspects of a given set of architectures that were conceived for systems operating in a common context. Mastering the reference architecture, cost and time for discussing about the design of basic functions or components is saved, thus reducing time-to-market, allowing focus on more important aspects and generally increasing the competitiveness of the design process [6].

This is not possible for IoTP systems, which are based on an innovative paradigm. This work aims at providing some essential building blocks of a Software Reference Architecture (SRA) for supporting the process of designing IoTP-based urban systems, thus improving its efficiency as well as the basic interoperability feature of resulting systems. Moreover, the reference architecture can also be viewed as a knowledge base for understanding basic principles and concepts of urban systems and discussing about them.

Until now, ICT systems managed internally almost the whole data chain: from data collection, to aggregation, filtering, management, interpretation and use. In this process, stakeholders were users, acquirers, developers or maintainers of the system. The reference architecture was a key tool for having a common understanding of basic principles and concepts of the system among system architects, development teams and stakeholders. In addition to this, with the advent of the IoT mainly, but also of the IoP, the reference architecture will be needed by system architects as a common knowledge base to understand the other systems their own ones have to cooperate and integrate with. I.e. the IoTP reference architecture for urban systems will provide the guidelines for information systems (see section 2.1.3) to interoperate. It is not so different from what happens today when a big enterprise (i.e. the stakeholder) asks a specialized software house to develop and integrate their specific component in a larger application, with the noteworthy exception
that instead of one stakeholder there are several, too many to even hope to interact with. Thus, it is necessary that all the ICT systems operating in the same context are based upon common concepts and principles and system designers are well aware of them.

1.2. Interdisciplinary approach

This PhD thesis was born from the experience I’ve gained in years of research activity in the IoT domain working in projects at national and European level and from the intuition of prof. Stefano Panunzi about what he defined as Urban Web-Aided Design (UWAD). This work integrates two very different approaches: Software Engineering and Urban Engineering, to which IoT and IoP paradigms are applied. Software engineering is the branch of computer science that creates practical, cost-effective solutions to computing and information processing problems, preferentially by applying scientific knowledge, developing software systems in the service of mankind [7]. In [8] Urban Engineering is defined as “the art of conceiving, undertaking, managing and coordinating the technical aspects of urban systems. The term ‘urban technical systems’ has two meanings: the first conveys the ‘physical’ dimension of an infrastructural ‘support’ network, while the second can be construed as a supporting ‘services’ network”. An important phase in the life cycle of Urban Engineering products is Urban Design. UWAD is an advanced method of planning and designing the evolution of cities, towns and villages using web technologies to support the design activity. UWAD is a peculiar branch of Urban Design which delivers innovative solutions to this branch of engineering, aiming to improve the functionality, attractiveness and sustainability of urban areas though the use of Internet-based technologies. Due to the innovation it delivers, it is closely related to what is called Urban Re-Engineering. As it will be detailed in Chapter 2, Urban Design relates to a large number of domains and involves many branches of Engineering, and thus it is managed with the typical tools of Systems Engineering. In this work, though, focus will be placed only on Software Engineering, and specifically Software Architecture Design principles, which will be applied and extended from an IoTP perspective.

1.3. Structure of the Document

This work is structured as follows. In the following part of this section, the need for this work will be discussed and the main concepts will be explained. In Chapter 2 an introduction to the design of urban systems is provided. The analysis of the state of the art
for the Internet of Things and the Internet of People is then provided in Chapter 3 with particular attention to architectural and design aspects. In Chapter 4 a discourse on the smartness of future cities along with a detailed analysis of the benefits of applying the IoTP paradigm to urban systems to improve their efficiency is provided. This accessory knowledge base is completed by a discourse on the benefits of interoperability and the need for information quality. Chapter 5 is specifically aimed to those stakeholders involved in the process of designing urban systems and in particular, in the design or re-engineering of the information systems supporting urban (sub-)systems. Finally, Chapter 6 provides an outlook on the challenges for adopting IoTP in urban scenario and describes the future steps that are needed for a practical and wide adoption of this paradigm.
Chapter 2. Modelling the city system

2.1. Engineering urban systems

To better understand how IoT can help in re-engineering Urban Systems, a look at the larger picture can help. A brief reminder of how the design process is approached at a higher level, in Systems Engineering, is thus provided in the following.

2.1.1 Complex systems

Systems Engineering is an interdisciplinary field of engineering which investigates how the design, development and management of complex system—in our case urban systems—projects should be approached and organized. A complex system is a system composed of several interconnected parts that as a whole exhibit properties or behaviours not obvious from the properties of the individual parts. That is the whole is greater than the sum of its parts. There are two categories of complex systems:

- Complex organized systems are systems that, though complex, can be analyzed, synthesized, and investigated using engineering techniques.
- Complex unorganized (or disorganized) systems are those that are so complex that they can only be studied by averages, aggregates, and statistical methods.

Any complex system is composed of components, themselves systems. This is why any complex system has a hierarchical decomposition where each level in the hierarchy is a set of interrelated systems. In Figure 1 our approach to the decomposition of Urban Systems is shown.

According to Systems Engineering, a complex system is composed of matter, energy and information. For instance, a social organisation such as an enterprise processes:

- matter: transformation of raw materials into finished products—goods and services,
- energy: fuel and electricity are needed to operate machines and heat buildings,
- information: strategies, plans, budgets, personnel records, customer orders, advertising messages, and financial records are all information.

Systems that are functionally related or simply use to interact in order to accomplish common tasks and/or share common resources can also be treated as a complex system. This is the case of Urban Systems which, depending on the resolution with which they are analysed, can be the container of thousands to billions of processes.

In analysing as well as in designing such systems, more layers of classification must be used. Generally different domains are identified in complex systems and each Domain

---

3 In many systems matter and energy are so closely related that they are often treated as one entity.
contains a still large set of systems called Domain Elements. In the case of Urban Systems, domains could be for example Transportation, Health, Culture, Economy, City Administration, Utilities, Social Care, Public Safety, Education, etc. [9].

Figure 1: Hierarchical decomposition of a complex system such as a generic Urban System

Cities, as generally all artificial systems with a high degree of complexity, involve many domains, each domain, in turn, involving different containing elements (i.e. systems) belonging to different branches of engineering. This is one of the possible intermediate views introduced between the complex system and the atomic composing systems in order to allow a better modelling of the system itself. For instance, Transportation is an important urban domain that provides for the safe and efficient movement of people and goods in an environmentally responsible manner. It includes several subsystems according to the perspective we study transportation in the city: rail, water or road transport systems, passenger or freight transport systems, electrical- or fuel-based transport systems, public or private transport systems, etc. Such a subsystem is in turn composed by elements that can themselves be more or less complex systems: road or railway network, stations, transportation users as cars, buses, trucks, pedestrians, tramways or trains, dispatchers, coordination centres, etc. Moreover, such a system is so complex that information systems are needed to monitor and coordinate transport processes in each subsystem.
2.1.2 Conceptual Modelling in Systems Engineering

In order to manage the complexity, Systems Engineering is based on a modelling process: in order to analyse or design a complex system a model (or set of models) of the system is needed.

In our approach a model is an abstraction highlighting only some aspects of real-world systems in order to depict those aspects more clearly. Abstract models reduce the complexity of the real world to digestible chunks that are simpler to understand. Models are representations of a system, either an existent one or one to be implemented. In the first case we have models to better understand or analyse the system, in the second case we have models for system design.

![Image of Real world and its models](image.png)

**Figure 2 Real world and its models**

Usually a model has: an **objective** (the question we want it to answer) and a **viewpoint** (the point of view with which one or more stakeholders of the system – e.g. users, developers, etc. – approach the system). Some systems are better perceived as physical (matter/energy) models: a car, an electric engine or transformer. Others are better understood as information models: the human hormonal system or hereditary mechanism, a computer system, a controller incorporated in a microwave or the decision system in an enterprise.

The advantage of using models can be resumed in the following two aspects:

- Models allow to reason on key features of a real system and from specific points of view which can reduce the complexity of a system. They increase our understanding of the problem and help identify solutions.
- Models are the vehicles for communication between the various parties interested in the system (stakeholders, mainly users and developers).

2.1.3 Modelling systems in the Information Era

In particular, emphasizing information aspects in nowadays artificial systems is particularly interesting in order to develop information systems that support the information flows in the systems.

Currently, Information Systems are very important because they are an efficient and effective tool for (at least partially) organizing, coordinating and managing complex systems. Generally speaking, all domains belonging to a complex system that should be organized should have an information system able to support internal information flows and exchange information with the information systems of other domains.
When developing information systems, the first and one of the most important steps is represented by the Information Model (IM) development, a documentation that models reality through information, capturing from a system in the real world all the relevant information about how information is measured/collected, transferred, stored, processed, and finally used in the system to be analysed or designed. IM consists of a (partial) description of the reality in which aspects concerning substance (mass, size, colour, position) and energy (energy loads and flows, light intensity, mechanical, magnetic, or electric forces) are transformed in information and represented only if they are relevant for the study of the reality.

2.1.4 Information system analysis and design

IMs are used as a blueprint for information systems, essential components to almost all complex organized, artificial systems. Nowadays, considering a generic complex system, many Domain Views include information systems, which is also the way by which many composing systems interact. The development of an information system begins with the capture of user requirements from interviews with the system stakeholders. Requirements Engineering provides the appropriate knowledge and conceptual tools for understanding what the customer wants, analyzing need, assessing feasibility, negotiating a reasonable solution, specifying the solution unambiguously, validating the specification, and managing the requirements as they are transformed into an operational system. The analysis of these requirements has as result a high level model of the system. A model of a non-trivial system is usually composed of more sub-models closely related and interdependent. Each sub-model emphasizes a certain aspect of the system: for example a model should emphasize the system structure, other models the system interactions with the environment or the system dynamics. The IM is used in the system design to first define an architecture for the future system. In this architecture the system components and their interfaces are emphasized.

The IM is also used to define specific requirements for the system components. Each component, if complex, should have subcomponents which must be also specified with their requirements. This process of component refinement ends when the component is itself a system that belongs to specialized, technical domains (for instance a mechanical, electronic or software component). This recursive approach can be used for the projection of requirements on each domain element which, in turn, can be viewed as a system itself or, even at a lower level, on its subsystems until the systems of the technical view. It also works with or, better, it best suits the development of Information Systems.

An Information System is mainly composed by ICT systems and human agents that execute manual procedures and access the ICT systems by Human-Machine interfaces. An ICT system can be mainly divided in Software and Hardware systems. The IM is a good tool for the design and analysis of all Information system components. In particular the ICT systems can be very well described by an IM because they do not involve humans in their processes or, in other words, they are deterministic systems.

---

4 While humans generally interact with ICT systems (providing input or collecting output) they are not considered as a part of ICT systems.
The IM of Information Systems includes at least a Domain Model, a Context Model and an Interaction Model.

The domain model introduces all the concepts related to the specific problem the information system should resolve. It classifies various entities related to the problem in concepts with their attributes, roles, and relationships, plus the constraints that govern the problem domain. The domain model is used to provide us the vocabulary and key concepts of the problem domain. In the object-oriented approach to systems analysis the domain model is introduced with class diagrams.

The context model gives the system boundaries by delimiting the system of all external entities interacting with it. It also provides basic assumptions of how the system interacts with other systems of the same or of different domain elements.

The interaction model describes the collaboration between the system components in order to respond to external stimuli (events). The model is composed of interaction scenarios that are chronological sequences of interactions which involve components of the system and external entities.

The IM of software systems will contain the same components.

2.2. Conceptual modelling of urban processes

Urban systems are dynamic and open, complex artificial ecosystems [53]. They host a large number of urban processes by which life in urban areas is operated and managed. Being open and dynamic also means that urban systems interact with their close environment and that their evolution and the processes carried out within are influenced by urban phenomena, i.e. internal and external events or conditions, which can be viewed as stimuli for the urban system from its environmental context. For instance weather, national or regional economic and social conditions (external stimuli), as well as urban growth or traffic congestion (internal stimuli) are urban phenomena that can affect some urban processes.

On the other hand, urban phenomena, which can involve different time, geographical and social scales, can be produced – as direct- or side-effect – by urban processes. For instance changes in the morphologic configuration, industrialization or tertiarization in urban areas are urban phenomena resulting from specific urban processes as city planning and management.

For the purpose of this work, the urban system is defined as an open system which includes all the physical features, functional infrastructures, living beings, the society as well as the administration of the city itself. Physically, the boundaries of the system overlap with those of the city although external factors and actors can influence the urban system. The term “actor”⁵ is used for identifying entities that hold a role in the scenario⁶, i.e. in the urban environment.

---

⁵ For clarity’s sake, no terminology distinction is made between actors internal to the system, often called agents in software engineering, and external actors.

⁶ Sometimes an entity can have different roles in different processes, i.e. different aims and the capability to operate to pursue them. When modelling such scenarios, these are modelled as different use cases, each with its own primary actor (the actor triggering the use case). In some cases though
Urban processes can be influenced by many factors (e.g. weather conditions, social habits, welfare, etc.) and actors (citizens, private companies, municipalities, etc.). Generally speaking, urban actors are active entities which can start processes that, in turn, might influence (directly or indirectly, intentionally or unintentionally) urban processes, while urban factors are pre-existent or uncontrollable factors that constrain by their simple existence the occurrence or evolution of urban processes. Alongside urban factors, urban phenomena can also influence urban processes as boundary constraints. While it is very difficult to control all these actors and factors, it is paramount to monitor all sources that can affect urban processes; gathering correct and relevant data is fundamental for making right decisions — and eventually influencing the same urban processes — both in the short and in the long term.

Different kinds of actors (secondary actors) can participate and some entities can have more than one relevant role in the use case.
Figure 4: A generic model of urban process. Main categories of urban actors and urban factors are represented. Urban phenomena can potentially impact all processes that and thus, indirectly, all urban actors and urban factors, as well as other urban phenomena.

We have identified 6 categories of entities of the urban system which mainly affect urban processes:

1. **Environmental factors**: they represent the environment and its evolution. The environment here is not only the urban environment but also that of the region around the city. They can range from climate and current weather conditions to the fertility of the soil and the susceptibility to extreme weather events or disasters. They impact on urban processes only in the short term, but some of these factors (e.g. the availability of prime resources – such as water, food and energy) should be taken into account in long-term urban planning. Urban processes also influence environmental phenomena or conditions such as water, soil and air pollution or even weather [54].

2. **Social factors**: they account for education, social trends and relevant one-time events. Currently, this kind of factors is really difficult to model due to the lack of structured data that could be used as input. A good example of how social events could impact city processes is finally described in MIT’s Currentcity project [55].

3. **Built base**: along with infrastructure and geo-morphology, these factors are modelled as constraints in the short term and can be generally defined in a static
way. Urban processes usually don’t affect them, yet in the long term changes might be relevant in some cases. For the modelling purposes we consider this factor to be only a constraint to urban processes and reverse impact is not taken into account. While it might seem similar to the environmental factors, this component is different because a) it only takes into account static (or very slowly varying) factors and b) it includes the buildings and other physical changes that are due to urbanization and are already affecting an area.

4. **Administration**: it should be able to monitor and control the urban processes in the most efficient and effective way. For example, urban planning interacts with urban processes at all scales: it is very important for designing a good development plan to understand which zones of the city are movement sources and which are peaks, which city services are used systematically and which are used asystematically, as well as which is the capacity of urban infrastructures, when related to their current use.

5. **Citizens**: they are influenced and influence urban processes unintentionally. Individuals (the inhabitants of the city as well tourists) as well as groups want to know what is happening in the city, or what other people think about a monument, a place, an event or a service. The goals of single citizen actors range from the avoidance/mitigation of negative impacts to the planning and optimization or activities, while groups of citizens can use IoP to get together and coordinate their activities or even their interaction with the public in the management of the city. In the last years though, citizens are moving from the role of passive users of the city’s services to active figures that want to be in control of what is happening in their environment. This urban actor group involves citizens both as individuals and as groups.

6. **Generic actors**: these urban actors represent systems whose processes coexist with urban processes. For example, while industry and education are considered relevant domains of the urban system actors, we are currently unable to monitor, and thus model them in an abstract and satisfactory way. We acknowledge the importance of these actors, but in the frame of this work they will be disregarded because the focus is on the use of IoT and IoP in a generic urban context. Also, in the future, IoT will allow to monitor city-wide industrial processes, such as the supply chain and even international logistics.

7. **Urban processes**: finally, because the subsystems of the urban system are interconnected, urban processes often affect other urban processes. This can happen either directly or indirectly through the urban phenomena. Private transportation (a subsystem in the transportation domain) is a typical example: it can create traffic congestions (urban phenomena) which in turn can affect again public and private transportation processes but also, other processes (e.g. resource distribution) or factors (e.g. local climate or houses value in the area).

The model proposed in this section is intended as a generic model that could be used to understand the potential of IoT and IoP for urban re-engineering purposes. It is not meant to model all interactions in urban systems nor it is claimed that the interaction between entities is always direct. This model shows only the most relevant interactions for the generic urban process and its elements are chosen for the aforementioned purposes.
As a usage example, one could think about the case in which the municipality decides to close an area of the city to traffic because of too high levels of air pollution. This external event stimulates the urban system to react with an appropriate, previously planned, urban process in order to mitigate threatening of the excessive level of air pollution. For this Administration (an agent in the urban system) decides to trigger a urban function (denying access to a specific area), which generates a urban phenomenon (i.e. the lack of private circulation in the given area) which then has consequences on citizens (who have to change their daily transportation processes) and on urban phenomenon (i.e., hopefully, on the air pollution). The urban process triggered by the excessive level of air pollution ends when the pollution level diminishes at acceptable levels. It is important to stress that the actual mechanism though sees the Administration starting a urban regulation process that interacts with the private-and public-transportation related urban processes which should produce less pollution (urban phenomenon) in the given area. Many of these interactions cannot be controlled and some are even difficult to monitor. Currently the monitoring of the environment and of the physical part of urban processes provides data that has a low spatial resolution. For what concerns the social factors, their monitoring has never been performed in an automatic way to the best of our knowledge. Information about social factors and the social dimension of urban processes is gathered directly only through surveys. Such information though has a very low resolution (both in time and in space) and its quality is affected by subjectivity issues. This paper only focuses on the environmental and social factors as well as on the social and physical part of existing urban processes because these can be monitored thanks to IoT and IoP. In the Chapter 4 an explanation about how IoT and IoP can become relevant tools for efficient administration is provided.
Chapter 3. IoTP State of the Art

In this chapter a detailed view of the current state of the art regarding the IoT and IoP paradigms individually is provided. Because this work is mainly focused on architectural aspects, the discussion will also adopt this point of view.

3.1. Internet of Things

While a shared definition of the Internet of Things is still missing in the scientific community, it is clear that this concept is related to the trend of embedding communicating devices in and providing digitally-mediated interaction with physically objects and environments. The introduction of communication capabilities and the moving of processing capabilities to the peripheral part of the networks will also slowly move the use of Internet from human-oriented to scenarios where the main users will be machines (i.e. computing devices).

Due to its pervasiveness in the everyday environment and the impact on all fields of human activity, the advent of IoT will unavoidably also raise social, administration, privacy and security issues. In order to understand the potential of IoT the current state of the art in this domain will be discussed. A good, general overview can be found in [11].

3.1.1 History of the Internet of Things

This futuristic vision of pervasive, embedded devices has its bases in the established RFID technology which for the first time allowed real-world objects to be represented in the digital world. During the last ten years, many definitions of IoT have been given, extending the original vision [12], which dates back to 2004, of

“Giving everyday objects the ability to connect to a data network”.

In the final report of the Coordination and Support Action for Global RFID-related Activities and Standardisation project [13] the reader can find a compiled list of definitions which capture different aspects of and meanings given to the concept of Internet of Things. In the document, a first technical, consolidated definition of Internet of Things is provided by prof. Anthony Furness from the European Centre of Excellence for AIDC

“A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability”
The CASAGRAS definition was given in the first part of year 2009, and was then confirmed in the final report of the project in 2011. This definition gives to the IoT term the meaning of a network infrastructure. This is coherent with the semantic meaning of the phrase which assumes that the IoT builds upon the existing Internet communication infrastructure. The rest of the work though is less focused on Internet-based communication of devices and the technical relevance of the project itself lays in the RFID-related standardisation activities.

In the same document another definition, later formalized in [14], is provided by an (at that time) SAP system architect, Stephan Haller:

“A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.”

It is worth noting that in this definition the focus is on the physical objects, also called “things” elsewhere, which are in the centre of the attention as main participants of the IoT. These things are described as active participants in the business processes, which for the first time, would point towards the support of Machine-to-Machine (M2M) communication in IoT. Besides, the IoT here is more a vision than a global network, as the word “world” would suggest. Also the idea of using services as communication interfaces for IoT is introduced for the first time and will be later investigated as a means to provide application level interoperability. Security and privacy, though not related to the definition of IoT, are also recalled as critical issues. In time these issues were given more and more importance by governance, research and industry actors, and all approaches to IoT currently involve privacy and security aspects.

In 2009 the European Commission also supported a workshop on the IoT, which provided other interesting definitions [15][16], such as the following:

“a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols.”

“Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts.”

The Future Internet Assembly also provided a definition of IoT in its Real World Internet position paper [17]. It encompasses many aspects of the previous ones and emphasizes the dual aspect of IoT: the communicating devices and the vision about integrating the real world into the Internet

“The IoT concept was initially based around enabling technologies such as Radio Frequency Identification (RFID) or Wireless Sensor and Actuator Networks (WSAN), but nowadays spawns a wide variety of devices with different computing and communication capabilities – generically termed networked embedded devices (NED). [...] More recent ideas have driven the IoT towards an all encompassing vision to integrate the real world into the Internet [...]”
“The Internet of Things is a technological revolution that represents the future of computing and communications” which aims at “making the physical world and information world together” [18]

In conclusion, we can thus identify two different meanings (and thus definitions) of Internet of Things: IoT as a network (of networks) and IoT as an ICT paradigm in which physical and digital entities interact in an augmented world, as described in Figure 5. Taking from the literal meaning, the Internet of Things is a global network, an extension of the current Internet to new types of embedded devices that will enable the identification or interaction with physical objects. IoT also refers to the vision where the digital and the physical world overlap pervasively in a new augmented continuum where users could choose whether to interact physically or digitally with physical objects and things could have goals to achieve and can interact with other things in order to realize them.

![Figure 5: visual representation of the IoT paradigm: the evolution from the current context, where the digital and the physical environment are uncoupled (a), to one where they can interact (b) and, finally, to one where an augmented world seamlessly merges the physical and digital environments (c).]

It is clear that the two definitions are very tightly related, with the first one (extension of the Internet) defining a tool for the realization of the second (the vision).

3.1.2 Technological background

So the IoT can be viewed as a pervasive extension of the Internet to everyday objects. In the frame of this work the IoT is mainly related to Sensor and Actuator Networks (SAN) more than to RFID because, when it comes to data collection or command execution, networks provide greater capabilities and more flexible solutions for communication. In time Wireless Sensor and Actuator Networks (WSAN) proved to be a good solution because they don’t rely on a physical infrastructure and thus don’t require a physical setup requiring, in turn, an easier deployment compared to their wired counterpart [19].

Bidirectional communication is also useful for reprogramming devices directly from remote [20].

On the other hand, using a shared medium for communication brings along a large number of security issues as shown in [21].

WSANs are made of a number of network nodes that also host sensors and actuators and can communicate among them using wireless physical layer (PHY). The data transmitted
throughout the network can be either used by other nodes in a Machine-to-Machine approach or routed through a (router) gateway to a server running a central business logic on a higher level network or on the Internet itself. A good overview reference for understanding the basics on WSN design and architecture can be found in [22] or, in much greater detail in [23].

WSNs are the technological base for many data collection systems in many applications fields in industry, agriculture or services domain. The wide public also came in touch with these technologies in home automation applications. Currently though these are closed applications, which are specialized for a very specific context and use specific, generally different, protocols. Using a metaphor coined by Alessandro Bassi, these applications are closed silos [24], meaning that they can’t use the sensor base of other applications and do not exchange information, i.e. they are not interoperable.

Many researches on the IoT topic nowadays focus on hardware and software issues such as energy harvesting, efficient cryptography, interoperability, communication protocols and semantics.

3.1.3 A look into IoT protocols

Yet, the synergy among systems of the same domain used in different deployments (e.g. deployed by different organizations) or of the applications belonging to different domains would produce a great added value. One of the goals of IoT was to break the walls between the different deployment silos and to make all these systems communicate. It was obvious then to think of the existing Internet as a means to connect these networks of devices, but WSNs generally didn’t rely on the Internet Protocol (IP) as Network layer (NWK) protocol.

As the IP protocol is the cornerstone of the Internet communication, providing identification and routing, the IoT, as an extension of the current Internet, had to be based on it too. In a domain characterized by heterogeneity at all the different layers, a common NWK layer represented a narrow-waist to the complete set of IoT-capable protocol stacks [25]. In particular, the industrial and scientific community identified in Internet Protocol version 6 (IPv6) this common NWK layer protocol because it was capable of supporting a very large number of endpoints. Indeed, the perspective of having 50 to 100 billion Internet-capable devices by 2020 [26] can be even viewed as one of the drivers of the adoption of the IPv6.

But not all these devices are natively capable of using a full-fledged Internet stack. Embedded devices actually are generally very constrained computational-and communication-wise. In this context, the work of the 6LoWPAN7 group [27] in providing an adaptation layer between IPv6 NWK layer and the MAC layer of widely used IEEE 802.15.4 [28] is worth mentioning. The adaptation was needed because of the different purposes of the IPv6 and of the IEEE 802.15.4 standard for Low Rate WPANs (LR-

76LoWPAN means IPv6-based LoWPAN, where LoWPAN (an acronym for Low power Wireless Personal Area Networks) is a simple low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. It typically includes devices that work together to connect the physical environment to mainly wireless sensor applications.
WPANs). The former was based on the existing features of IPv4, and was designed for the Internet while, at design time, LR-WPANs were required to optimize energy consumption. Thus the work had to deal with the typical limitations of constrained devices.

One of the greatest issues was that the LR-WPAN PHY layer packet length of 127 bytes. This forced the workgroup to rely on the compression for the 40 bytes IPv6 header in order to achieve larger application-level payloads and thus greater efficiency in communication, which lead to RFC4944 [29]. The reasons behind this choice can be understood considering that the MAC header has a maximum length of 25-bytes, that the possible overhead due to the MAC layer security can take up to 21 bytes and that fragmentation support in upper layers can reduce even more the actual application payload.

The potential of having small – though constrained devices – to the Internet has been readily perceived by the actors of the embedded devices market. For example, alongside the interest focused from the academic environment, it is relevant that all embedded platforms previously cited already provide support to 6LoWPAN, Contiki, Tiny OS and RTOS, three of the major operating systems for embedded devices, also provide software modules for 6LoWPAN.

Above the NWK layer as a Transport (TRA) layer protocol TCP [30] is generally used on unconstrained devices and UDP [31] on constrained ones. Relative security extensions, TLS [32] and DTLS [33] respectively, are employed for securing the communication channel.

Above the TRA layer HTTP is used as REST protocol on unconstrained devices. The need to use a REST architecture is related to the fact that this is an established use in the current web-based design. Indeed this approach led many to identify the IoT with the Web of Things, identifying the concept of resource with the one used in web applications [34].

On the other hand, a specific REST protocol for the use on constrained devices has been designed. This lightweight protocol, called Constrained Application Protocol (CoAP) [35], is under development in the Internet Engineering Task Force (IETF) can easily be interfaced with HTTP and is tailored for the requirements of constrained networks, i.e. with low data-rate, high latency.

3.1.4 The IoT-A Architectural Reference Model for the IoT

In Section 3.1.1 the Internet of Things was defined with a dual meaning of paradigm and global network. A reference architecture for the Internet of Things is still missing at the moment. The task of developing such an architecture that could embrace all the different architectural designs of systems that are involved in the IoT, which, by definition, is made of heterogeneous systems, is a difficult feat.

As we pointed out in Section 1.1.3, the concept of reference architecture - as it is consolidated in Software - is a framework that captures the invariant architectural aspects of a given set of architectures that were conceived for systems operating in a common context, usually a particular domain. It acts as template that is composed from some invariable parts and a set of slots where variable solutions can be adapted to the problem particular context. However, because IoT is a paradigm which crosses many application domains, it is too generic to be described by one reference architecture.
The Internet of Things Architecture\(^8\) (IoT-A) project tried to extend this concept which became part of a larger design framework called Architectural Reference Model (ARM) [36]. The IoT-A ARM provides a common cognitive ground (concepts, terminology, abstract models), for system architects and software designers working in the IoT domain, regardless of the application domain (eHealth, smart cities, retail, defence, etc.). The ARM is a high level design tool mainly composed by a Reference Model (RM) a Reference Architecture Guidelines, and Best Practices. The RM contains very abstract concepts about the IoT domain, communication, functional and information aspects. The Reference Architecture Guidelines provide theoretical support for the design of Reference Architectures in specific domains. It is important to note that currently there are no IoT RAs for any domain.

**Figure 6**: The process of deriving a specific system architecture from the Architectural Reference Model (on red background). Multiple, domain-specific, RAs can be derived from the RM. Multiple system architectures can then be derived from one RA thanks to the ARM guidelines and specific system requirements

In the IoT-A view, based on the OASIS reference model definition [38], the RM provides the highest abstraction, promotes a common understanding of the IoT domain and collects the high-level functionalities of IoT systems. Based on the RM, IoT (reference) architectures can be designed for specific domains. The IoT-A RM includes:

- a general discourse on the IoT domain,
- an IoT Domain Model as a top-level description of entities and relationships,
- an Information Model explaining how IoT knowledge is going to be modelled and
- an IoT Communication Model in order to provide the basis for understanding how to achieve communication interoperability between many heterogeneous IoT devices.

A RA is the reference for building IoT compliant architectures for a specific domain. The IoT-A RA provides views and perspectives on architectural aspects that are of concern to

\(^8\) http://www.iot-a.eu
the stakeholders of the given domain in accordance to [39]. The development of an IoT RA for a given application domain focuses on abstract sets of mechanisms rather than concrete application architectures. It is driven by a set of requirements that are shared by all the applications belonging to a given domain.

Multiple Reference Architectures could be derived from the same Reference Model following the guidance provided in the IoT-A Architectural Reference Model.

For a complete and deeper understanding it is advisable to read the latest version of the IoT-A Architectural Reference Model [36] and the other deliverables of the IoT-A project.

3.1.4.1 The IoT-A Domain Model

As introduced in Chapter 2.1.3, the DM is an important model used for developing information systems architectures: it describes the key concepts and relations of an area of interest (domain) that the specific architecture addresses and how they relate and interact. The DM is not meant as a description of the components of the system we want to design, but as a description of the context in which the system will be part of. It specifies the knowledge the system must have about all external entities the system interacts with. In the following only the features of the DM which are central to this work will be discussed. A complete analysis, along with examples, is provided in [11].

For describing the IoT DM, we have proposed the first approach in [40]. The same approach has also been used in the frame of the IoT-A project that has also improved and consolidated it in the IoT-A Domain Model, which has received positive feedback from the scientific and industrial community and is currently the state of the art.

In Section 3.1.1, the IoT was defined as a means to make the digital and the physical world overlap pervasively in a new augmented continuum where users could choose whether to interact physically or digitally with physical objects.

Figure 7 presents the IoT-A Domain Model as a UML class diagram.
The basic assumption of the IoT is that all the objects of the physical world called Physical Entities have a digital (i.e., software, or Digital Artefact) counterpart called Virtual Entity which represents them in the digital world. The Virtual Entity must show and provide all the relevant features of the Physical Entity in the digital world as Resources. Resources must be tightly linked to the physical features so that changes in Resources are reflected in state changes of the physical object and vice versa. For this reason, the physical objects will need to have attached or embedded Devices that could allow ICT systems to identify them. These devices can be simple (passive or active) RFID or more complex (W)SAN devices that could provide real-time information about (or actuation on) the Physical Entities. Resources are conceived in the IoT DM as low-level software components, generally

For correctness sake, it has to be pointed that only physical objects that can be useful to include in digital processes are considered Physical Entities and will have an associated Virtual Entity because only these objects will have an attached or embedded Device.
developed for the specific hardware platform they are hosted upon. This platform can be either the Device (in case of On-Board Resources) or some server in the Internet cloud (as in the case of Network Resources such as database entries).

Due to the great heterogeneity of the Devices and thus of the Resources, a Service component was introduced in order to provide a standardized interface for accessing Resources.

Figure 7 explains how the semantic associations between a User\textsuperscript{10} and a Physical Entity are motivated by not only physical interaction, but also interactions in the digital world, i.e. leveraging the potential of the IoT.

At this point, we can easily explain how, instead of resorting to physical interaction (observation, moving, rotating, etc.) the User can leverage the alternate, IoT-based, association to interact with the Physical Entity. The User invokes a Service, which accesses a Resource. In case it is a Network Resource, this stores and can provide up-to-date information about the Physical Entity. In the case of On-Board Resources, this will use the device it is hosted on in order to actuate on or measure relevant status parameters of the Physical Entity.

One last comment about the IoT domain model is that it supports Machine to Machine (M2M) interaction. Indeed, the Virtual Entity can be either a Passive Digital Artefact (i.e. passive software elements such as RFID-stored, data-base entries or other digital representations of the Physical Entity) or Active Digital Artefacts (i.e. agents or other running software that has a business-logic, governs the behaviour of the Augmented Entity and can access other Services in order to achieve its goal).

3.2. Internet of People

In the age of information, social interaction is carried out ever more through digital means and, specifically, Internet-based communication. This phenomenon has its roots back in the 90s with Bulletin Board Systems (BBS), Multiple User Dungeons (MUDs)\cite{41}. It has then evolved in online chat rooms, instant messaging programs, forums, Social Network Sites (SNS)\cite{42}\cite{43} and finally what has been defined as Social Web.

Interaction can either be synchronous as in the case of instant messaging as well as voice and video communication or asynchronous as in the case of content generation on social networks.

3.2.1 History of the Internet of People

The first use of a concept similar to the IoP as defined in this work can be traced back to the “Internet by and for the People” pillar of the Future Internet as defined in\cite{44}. In this document, a group of experts identified the key pillars of the Future Internet along with the

\textsuperscript{10} From here on, \textit{italics} will be used to identify Domain Model components. In this chapter they are IoT Domain model components while elsewhere they will be IoTP Domain Model components. For example Service is referred to the common meaning of the word in Software Engineering, while Service is the Somain model component that provides access to a Resource etc.
key technological challenges and milestones for obtaining a sustainable Future Networked Society.

Figure 8: Future Internet overview, taken from [44]

The fact that the content creation and publication no more requires a professional expertise is acknowledged and a specific objective for the Future Internet to “break the barriers/boundaries between information producer and information consumer” with the help of (what here is called) IoP is set.

The IoP term was also used in [45] in the frame of a larger concept defined as Internet of People, Things and Service.

The term IoP also used in close relation and sometimes as a declination of the IoT. In [46], the authors define the

“Internet of People is envisaged as a world where people equipped with human-implantable RFID tags will become part of the ubiquitous network of networks facilitated by the popularity of social networks.”

The first part of this definition seems to refer to humans as Physical Entities from an IoT point of view, which is already well covered by the IoT paradigm. Reading through the paper one understands that the IoP concept as defined here doesn’t include the social interaction of people, which is instead, the main focus of IoP in this work. More recently, in [47], Robert Van Kranenburg defines the IoP as a practical version of the IoT, actually useful in the very short term to the citizenship.

In the scope of this work, Internet of People is defined as an interaction paradigm which envisages the Internet-based social interaction of people. IoP can be also viewed as the digital projection and extension of real-world social relations: both existing relations can be projected on the IoP and new relations can be born which not necessarily have a real-world correspondence.

It is clear that, in order to use the IoP for interaction, human users need a computing device (with a human-computer interface) as an adapter towards the digital world. These devices must in turn provide the needed hardware and software environment to run specific software, which will be called IoP application, that enables the user to connect to the virtual community of the user and interact with it.
3.2.2 IoP Application classes

In the frame of this work the term IoP Application includes a wide array of applications that can be classified by their communication mode and source authentication requirements. It is important to note that this classification is \textit{a posteriori}, as these application classification is based on the analysis of current solutions, which, generally, are, emulate, extend or improve the features of few successful and really innovative solutions.

<table>
<thead>
<tr>
<th>IoP Application Class</th>
<th>Unicast</th>
<th>Broadcast</th>
<th>Publisher subscriber</th>
<th>Access Control</th>
<th>Authentic.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Network Sites (SNSs)</td>
<td>s\textsuperscript{11}</td>
<td>x</td>
<td>s</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Web-based Forums</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blogs</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSS Feeds</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant Messaging (IM) applications</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Micro Blogging Platforms (MBPs)</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Ad-hoc applications</td>
<td>s</td>
<td>s</td>
<td>s</td>
<td>s</td>
<td>s</td>
</tr>
</tbody>
</table>

\textsuperscript{11} Many SNSs nowadays include IM features

Table 2: Supported communication modes in IoP applications related to the number of peers and source authentication requirements. x = supported/required; s = sometimes, i.e. some implementations provide this mode or require authentication; [blank] = generally not supported/required or not applicable.

The following communication modes have been identified:
- **Unicast**: is a term borrowed from network communication which describes communication where a piece of information is sent from one point to only one other point. Unicast transmission is also referred to as one-to-one nodes and involves two nodes only.
- **Broadcast**: this term also has its roots in network communication and describes a communication from one node to all (or any) other nodes in a given context. We use this term also to identify content that is published to all the audience, without restriction.
- **Publisher/subscriber**: is a messaging pattern where the senders of the messages, called publishers, do not manage nor are aware of the distribution of the messages to the users called subscribers (if any). The messages are only classified upon publication, based on either their origin, the content type or context, and sent directly to the subscribers that registered the call-back for one of the classes of the message. Subscribers register for message classes without knowing when and even if messages for that given class will be published.

The following features are relevant for what concerns the use of IoP applications in the urban context:
• **Access Control:** the content, also provided as resources later on, is only available to users pertaining to a given category. This can be verified either by authenticating the user and verifying that the access policies allow the given user to access the resource (Authentication Based Access Control, ABAC) or by verifying that the user, which could not be authenticated, has the right to use the given resource because of his role in the system (Role Based Access Control, RBAC). This check is performed generally by the user by demonstrating the possession of a certificate. In this context, it is assumed that the access policies are decided by the owner of the content, as this is the most relevant case in IoP, but we acknowledge that this is not the only case.

Access control is relevant because, in a first moment, the takeoff of IoP in urban context is bound to the use of currently existing IoP applications for urban purposes. In order to do so without raising privacy issues, resource providers must be able to set and manage the access policies of the content provided.

• **Authentication:** this is a fundamental feature for making IoP resources trustable. Without it, the content provided could not be traced back to the creator by the managers of the IoP or of the IoP application. This, in turn, would mean both that users that provide low quality data could not be followed (and the associated data excluded from processing) and that, in case of malicious acts, non-repudiability could not be guaranteed.

Among these different types, the only interesting ones are those IoP Application classes that can publish or otherwise provide public content because the aim is to use that content for public purposes without raising privacy issues.

SNSs are probably the most interesting IoP applications for two reasons: first of all they provide the most meaningful content to our aims and, second, they already have access policy management features that are essential could be extended for our use. In [48] a set of common functionalities provided by the top 16 social networks is provided.

### 3.2.3 Architecting the Internet of People

Currently there is no work or ongoing project for what concerns the definition of a common architectural reference model for the Internet of People nor, more specifically, SNSs, blogging, microblogging platforms. The reasons behind this situation are multiple.

1. The prominence of few IoP Applications per IoP application class, each of them generally dominating in only one specific niche domain. There is a wide range of domains including shopping, business and jobs, dating, participatory citizenship.

2. The lack of interest in interoperability. Actually, one could argue that the different IoP applications are ‘fighting’ over the set of common users where this happens to exist.

3. The specialization of social networks on specific topics (business, dating, citizens participation, ...) comes with specific impacts on the functional components of the architecture.
The cases in which some degree of interoperability is provided are generally related to the use of third party applications such as aggregators. Aggregators can be both user-side or centralized.

User-side aggregators are IoT applications that can manage multiple IoT application accounts and multiplex the user commands toward different such applications while integrating the content provided by the different accounts.

Centralized aggregators filter specific content accessed through accounts of various IoT applications and aggregate it according to specific rules. These operations can be performed by human editors or by software agents.

3.2.4 Adding Intelligence to the Context

It is well known that any information entered by a user of a SNS can be empowered if the SNS knows the context of the entering. This context can include information on the user’s behaviour, habits, beliefs, and interests using the user inputs not only from connected home devices like set-top boxes and media gateways but also from the user’s access to SNS. Linking the usage of home devices and the preferred content of SNS with the inserted information can put in evidence new aspects of the communication content. This extended context awareness, if managed in a right way, is a key element in giving intelligence to the environment, city, or house. It represents more than the simple location detection of a mobile user’s applications that discovers and reacts to changes in the environment they are situated in [49].

The social behaviour of the users can be a key driver of content generation and consumption patterns of IoT-based applications.

How can the SN architecture get us this type of information? There are mainly two application categories that enable the context awareness extension and put together human personality and presence of some things in the environment: Social Enabler and Social Watchdog [50]. Such applications can be active in home set-top boxes and media gateways, as well as in the network. Social Enabler is an intermediary between the SN and the user in order to ensure the correct representation of the user across the different devices. It handles the user authentication from the SN and provides the user credentials to crawling applications to retrieve a requested content. Social Watchdogs handle requests as fast as possible by maintaining in a cache memory already authenticated requests and devices for a given period. In this way all requests sent from the same device within this period will be handled faster than those sent by other devices.

Until now, IoT content was only considered as usable by human users. However enabling machines to understand this content would be extremely powerful. First of all, there wouldn’t be the need of human personnel checking all the content (which in some cases might even be impossible) and, second, the monitoring of the social dimension would finally be available to the efficiency improvement related to the use of digital technologies for the processing of information.

Unfortunately, the IoT content is produced for human users. There are two ways to address this issue:

- Asking content providers to provide the content in a machine readable way, i.e. adding context tags to the content itself and
- (only for what concerns textual content) using natural language semantic analysis to infer automatically the meaning of the content [51]

Moreover technical methods for retrieving approximate location information from the network layer protocols can be leveraged to position IoT nodes [52].
Chapter 4. Relevance of Future Internet

The concept of living in a smart city is obviously attractive. But are the current cities smart? This chapter introduces a new concept of smartness for cities and explains why IoT and IoP are key enablers of Smart Cities.

4.1. Bringing the “smart” to “Smart Cities”

In the real-life, smartness is all about making (right) decisions in a given context. In the urban context, regardless of the definition one wants to use for “smart city”, making the right choices for what concerns traffic management or urban planning is fundamental. And, as it happens in real life, correct and good quality information is key to making the right decisions.

Until now, all decision making was responsibility of persons in charge of specific roles, which usually held responsibility for their decisions. Even simple tasks, such as opening a gate, were assigned to persons whose task was as simple as pushing a button whenever a car with a specific ticket entered or left a parking. Yet, computers have demonstrated their computation and decision making capabilities since the late 90s. In [59] there is a very nice and interesting analysis of the evolution of artificial intelligence applied to a specific complex topic: the chess game.

Doubtless, computers had the potential to make right decisions even in complex situations since (at least) year 2000. But what is the difference between playing chess and opening a gate? The difference lies in the (lack of) context awareness. In the case of chess, the game was played in the virtual world, on a virtual chessboard that the computer could control and monitor. Actually, in the first challenges, Mr. Kasparov was moving wooden pieces on a wooden chessboard while an IBM specialist ‘copied’ them as command line input to the pc.

In the case of the gate, the input from the physical world was missing and, regardless of the intelligence of the machines that theoretically could be leveraged in an automation system, the gate could not be monitored or controlled from the digital world.

At least not until the automatic identification (autoID) technologies began to be widely adopted. RFID, WSANs and optical recognition provided the means to include the physical objects inside processes that are controlled digitally. As previously discussed, thanks to the IoT, it will be possible to have a stateful representation of the physical reality.

IoP on the other hand can provide access to data related to the social dimension of the urban processes, factors and phenomena related to the city.

In current days, one of the first goals of a city is to provide a satisfactory environment for the life of its inhabitants. Whether this is achieved or not mainly depends on the population and their opinion. The perception of the quality of life in a urban area is related to many aspects (community, job opportunities, quality of public services, climate, mentality of other people, availability of green areas, population density, and so on). Information about
the perception of these (and other) parameters would be a very useful feedback for adjusting the intervention of public administration.

In this work, the concept of smartness is closely coupled with the concept of context-awareness. The use of IoT for urban purposes serves two main goals:

- to give urban actors the capability to make decisions based on a good (extensive, precise and timely) knowledge of the context,
- to gather large amounts of data that will enable planners to design longer-term and more precise models of the urban (sub-)systems.

4.2. The Internet of (urban) Things

One of the greatest benefits of the IoT lies in the interoperability features it aims to provide. As previously stated, information systems are part of many (if not all) domain views of the urban system. IoT can provide automation to all those domains where information about physical objects (i.e. Physical Entities in IoT-A terminology) is needed. Moreover, applying the IoT paradigm to a large number of domains would enable a cross-domain data exchange. One could also view it as an opportunistic synergy from which different applications operating in different domains can benefit from each other if they are deployed pervasively in the same location or, more generically, in the same context.

4.2.1 Application fields

The main features that IoT can grant are presence/localization, sensor data collection and control through the use of actuators. Many information systems can benefit from these features. Generally, IoT can ease the management and increase the efficiency of systems where the collection of data related to physical objects or their control is needed. As these generally features are provided thanks to RFID tags or embedded devices with short range connectivity and low performances, designers must be aware of the security, and reliability limits of such systems.

Nevertheless, the IoT paradigm has been successfully applied (at least at prototype level) to information systems supporting complex systems in the following fields:

- Intelligent Transportation System (ITS) [60]
  - traffic monitoring and active transport management
  - public transportation monitoring
  - smart and integrated transportation
  - parking (loading/unloading places, places reserved for people with reduced mobility, bus stops)
- Logistics and generic transportation of goods
- Waste management
- Emergency Relief
- Environmental monitoring (meteorological, pollution, safety)
  - Meteorological
  - Precise rainfall measurement
  - Urban Heat Islands
o Pollution (air, water, acoustic, etc.)

- Safety
  o environmental hazards[61]
  o floods
  o earthquakes
  o avalanches
  o wildfires [62]

- Physical Infrastructure monitoring [63]
  o transportation
  o gas and water distribution (dams, pipes, …)
  o energy distribution
  o sewer system
  o street light monitoring and control

- Built base monitoring
  o Structural Health Monitoring (public and private buildings, dams, …)
  o Energy consumption and efficiency
  o Building automation
  o Construction site monitoring

- Urban Web-Aided Design
  o Introducing digital features as requirements in urban planning
  o Providing real-time view of urban development and quality of services to citizens and administration
  o Design of objective and effective Quality of (urban) Service indexes

The Internet of Things paradigm promises to provide a common framework for the integration of these vertical applications. Moreover, by leveraging M2M communication and real-time availability of data, new decentralized, context-aware systems could be designed and developed for a more efficient, autonomous and ultimately smart control of the environment.

4.3. Urban IoP: see through the citizen’s eyes

The IoP transfers a great amount of information relevant to the human users that produce the content. But this information is also useful for understanding some processes of the urban context or, at least, how people participate in and how they view urban phenomena and processes. Indeed, from a very abstract point of view, people could be viewed as social sensors [64].

There are two different approaches to IoP systems which can all be contextualized for the urban setting.

4.3.1 Participatory Sensing

In current days, one of the first goals of a city is to provide a satisfactory environment for the life of its inhabitants. Whether this is achieved or not mainly depends on the population
and their opinion. The perception of the quality of life in an urban area is related to many dimensions (community, job opportunities, quality of public services, climate, mentality of other people, availability of green areas, population density, and so on). Information about the perception of these (and other) parameters would be a very useful feedback for adjusting the intervention of public administration.

In this approach, urban actors participate actively and voluntarily in the process of data collection. This is a spontaneous process in which urban actors use IoP applications to share content that they deem relevant (either for themselves or for the users of IoP applications) as observations.

Participation is expressed through IoP applications that have specific (urban-oriented) themes: business, criminality, entertainment, inclusion, local communities, participation in the transformation of the city, citizen-administration communication, and tourism support.

Here information on events, advice, requests, or opinions is published for the benefit of other users who range from citizens to the city administration. Machine users, i.e., software agents are not used yet; apparently, the reason behind this fact is that the information provided by content creators addresses humans and is human-readable only. However, if content creators provide a semantic-enriched content, this could be made accessible to software agents too. A forerunner of the process of adding a semantic structure can be found in all those social networks that provide support to geotagging. By asking the user to pinpoint a place on the map, the system can actually derive the meaning and value of the position to which content is related to.

4.3.2 Datamining

The second heavily leverages semantic analysis for analysing huge amounts of raw content generated on IoP applications for generating relevant content. Despite IoP apparently targets human users, the advances in semantic technologies and their application to social networks demonstrate that the information submitted to social networks can be interpreted automatically to a certain extent. On the other hand, context-rich information has a great value in urban process analysis as it can be a valid source of machine-readable data. Context can be for example the identity of the user, a location, the timing. In this way, content originally created for human users can become part of automated processes. This information can then be aggregated and used to understand or even predict processes evolution.

Due to the kind of process itself, the resulting content is semantically-enriched from the origin.

4.3.3 Application fields

While IoT can provide a quantitative measurement of physical parameters, IoP can provide information about how citizens perceive the physical reality, what their needs and expectations are, in other words it can sense the social dimension of urban processes and
urban phenomena. This can be useful both to replace and integrate the data collected through the IoT and to evaluate the mood of the citizens. The Web is becoming the digital shadow of our society, so it is the ideal tool to monitor social factors.

- Quality of life
  - Changes in the environment
  - Evidence of decadence and environmental degrade
  - Pollution evidence
  - Criminality
  - Availability of public services
- Early warning [64]
- Identify citizens’ habits (both as individuals and as groups)
- Identify events that might have an impact in the given social scope.

These application fields are only generic and each of them can be further contextualized. Actually, almost every field of human life could be monitored through IoP.

4.4. Bringing the Internet of Things and People to life

4.4.1 Cross-domain synergies and business opportunities

One of the most interesting features of IoTP is the fact that once data is collected for one application, it can be reused in the same domain or, sometimes in completely different ones. For example,

- pollution forecasting can benefit from meteorological sensors
- resource distribution management might benefit from real-time data about resource consumption
- energy distribution management will benefit from the monitoring of home automation appliances.
- urban planning can benefit from the statistic analysis of the archives of transportation system or energy consumption data as well as from the assessment of the citizen’s perception of the new areas, public services, etc.
- transportation system planning can leverage the implicit information about the position of citizens during the day provided by IoP in order to better understand movements and flows

System designers should be aware of this possibility and invest in achieving interoperability with other systems because the precision, reliability or robustness of their IoTP applications could benefit from the data provided by other IoTP systems.

On the other hand, this approach really emphasizes the value of information as a valuable asset. This is an asset that could be easily converted into value. One of the most interesting things that we’ll probably assist to in the next years is the separation of services. While currently all present and foreseeable IoTP applications still have a vertical approach, the deployment of IoT sensors or collection of IoP data will probably become a standalone service that companies working in the data analysis sector could purchase. Finally, after
filtering, integrating and analysing this raw data, these companies could sell the access to the resulting information as a service to the final users, generally social actors. A possible scenario of the information market is presented in Figure 9.

**Figure 9: Possible new business segmentation and the relative location in the IoTP network.**

The carrier service provider market segment already exists and is well developed for what concerns mobile communication. However a significant change might occur with the advent of IoT. Specific communication solutions might be adopted and become relevant to the extent that even the current aspect of this specific market might change or new specific markets could rise.

4.4.2 Interoperability is the key

In the Information Era, accurate and timely information is a valuable asset in many aspects of nowadays society: we have discussed how it enables users (machines or humans) to take the right choices and act with good timing. It has also been emphasized how application from different owners but pertaining to the same vertical domain can support each other. Also cross-domain synergies can develop among systems operating in the same context. The base quality needed for these systems is interoperability, i.e. the capability of different, generally diverse or heterogeneous, systems to work together. In the case of information systems, this means that such systems must be able to exchange information in such ways so that they are able to use it after the exchange has occurred. In the frame of IoTP, the interest is mainly towards M2M communication which is needed for process automation. In this frame, the approach to interoperability is quite different in the IoT and in the IoP. Generally speaking, in M2M communication interoperability is related to three different aspects:
1. Routing, transmission and presentation: how data is divided into packets, how packets are sent and routed through the network and how they are rearranged into coherent messages

2. Syntax: which is related to how the message is structured, i.e. how the sending peer serializes structured data and how the receiving peer rebuilds the structure of the message from a serialized message

3. Semantics: which, in turn, is related to how a peer understands the meaning of the message. Generally, communicating peers need to use the same ontology or to reference it at the beginning of the message in order to understand the content of a message.

The first aspect is the least relevant: both IoT and IoP use IP as network layer and above UDP and TCP protocols are widely used in implementations of both paradigms. The presentation layer is generally HTTP based for IoP while CoAP is used for what concerns IoT. However CoAP-HTTP translation is feasible, and as proposed in [56], this could lead to the use of SOAP in IoT environment.

Syntax and semantics issues are in turn more difficult to address because of many application specific solutions which answer particular requirements of the given application field.

Moreover, IoP applications currently use human input and target human users, which means that any content should be translated/converted before being usable by IoTP software-agent users.

4.5. Information quality

In the Information Era, quality information is a valuable asset in many aspects of nowadays society: we have discussed how it enables users (machines or humans) to take the right choices and act with good timing. Due to the relevance of the topic, research in the information quality field have progressed very much in the last years, to the point that a complete analysis of the state of the art would probably exceed the effort invested in this work itself. For this reason only a brief introduction to the topic will be provided.

By definition, information is the basis of knowledge and hence it is collected in order to enable the understanding of – in our case urban – processes and phenomena. The quality of information is linked to the use that can be made of it and, thus, the need to understand is always related to a given context. This context can be described as a multidimensional domain [57], containing space, time and other dimensions related to the information content but also information quality dimensions which describe the information itself. Beyond the content dimensions, data collected by a given source has an associated information quality domain for each of the information dimensions.

The following dimensions of information quality are fundamental for a solid monitoring of the urban processes and urban phenomena. These dimensions are selected mainly from [58] and customized for the specific purposes of this work:

---

12 Sometimes information dimensions in the context space can even be characterized by qualitative (also known as categorical) variables, i.e. factors that don’t have a metric, such as belonging to or being relevant to a specific entity or group.
• Content-related dimensions: accuracy, completeness, relevancy, precision of the dimensions of the content of the information (space, time, etc.)
• Technical dimensions: reliability, latency, price, confidentiality, non-repudiability, sampling/timeliness
• Intellectual dimensions: believability, reputation/trust, objectivity

So, the concept of information quality is tightly related to the intersection of the information domain with the information quality domain. While this work is not going to delve deep in the topic of information quality, it is important to understand the potential impact of IoT-based information quality on the monitoring of urban processes as well as the availability of meta-data about information quality itself.
Chapter 5. Building blocks of the Urban IoTP Reference Architecture

By definition, a reference architecture must include all the important and recurrent features of the existing architectures of that given type and be able to accommodate all common requirements for systems of that domain.

In this chapter, after briefly describing the methodology that was used, the fundamental components of the urban IoTP RA are described. For information systems, such as the IoTP-based ones this work focuses on, these components are the domain model, the interaction model and the functional model.

5.1. A generic architecture of urban IoTP applications

5.1.1 Methodology

By definition, a reference architecture must include all the important and recurrent features of the existing architectures and be able to accommodate all common requirements for systems of that domain. Thus, the first step was to check the existing architectures of IoT and IoP systems. These two system types have been analysed separately because currently no IoTP system exists.

For what concerns IoT, the deliverables of the IoT-A, which already dealt with the issue of designing a reference architecture, have been used. While I have contributed myself to that project, in this work some changes have been made in order to correct existing issues and to accommodate for the IoP architecture features.

From a practical point of view, existing IoT and IoP architectures have been analyzed. Alongside with the knowledge gathered on IoT requirements in the IoT-A project, a set of interviews has been conducted with possible stakeholders of the IoTP RA coming not only from Italy but from different countries around Europe.

Two main categories of stakeholders\(^{13}\) have been considered: experts of the ICT domain, who would leverage this work to design future applications and Smart Cities experts who could leverage it to understand the potential of IoTP. All the ICT experts involved had at least a basic technical knowledge about IoT and IoP. Smart Cities experts had a basic knowledge of IoT and IoP too, albeit not of technical type. Experts involved were mainly from Italy but also other European experts have been involved. It is theoretically possible

---

\(^{13}\) While writing this document, the hope is that, when it will be ready, also the communication between these two groups during the design process will be benefit from this work, as a common knowledge and terminology background.
though that this choice limits the validity of some of the following considerations when applied to different scenarios. Moreover surveys (see Appendix 1) were submitted to some of the above-mentioned experts for what concerns the identification of use cases for IoP-supported ICT systems.

Figure 10 The process of creating a Reference Architecture. The system architecture and requirements drawn here represent both IoT and IoP ones.

5.2. A comprehensive Domain Model

The Internet of Things has a very generic approach to data collection and actuation. Moreover it is closely related to the IoP because both mediate some kinds of interactions of entities of the physical world through the digital one. We is a high-level conceptual model, defining physical and abstract objects in an area of interest to the Project. In this Section, the same approach adopted in [36] will be followed, paying attention to extend the content provided therein by abstracting the concept only enough to support both IoP and IoT paradigms. A higher degree of abstraction might prove harmful to the understanding of the whole system.
Figure 11: fundamental abstraction of the real-world interaction that IoT-based information systems must carry out in the digital world. Brown arrows are used to show real-world interactions.

In principle, the IoTP is meant to support the interaction between Users and what we call *Entity of Interest (EoI)*\(^{14}\). An *EoI* is a physical or conceptual entity in which the user is interested. Such interest can manifest as a need to know the state of the *EoI* or to change the state of the *EoI*. This representation is the first modelling step for IoT-based systems, which aim to enhance this interaction between the User and the *EoI* by carrying it out through the digital world instead of leaving in the real world.

This means that, for what concerns IoT-based systems, an *EoI* can only be an entity for which a digital representation is available. Such digital representation can already exist or can be created at the moment in which a *Resource* related to that *EoI* is created. A *Resource* is a software entity that is assigned to a process/activity or workflow activity and is accessed at runtime to interact with the physical or social world in order to fulfil the aim of the process/activity.

In an IoT urban system, an *EoI* can thus be either a *Physical Entity* in IoT terms – such as a place, a person (from a physical perspective) or any other object – or a *Social Entity* – such as a concert, a community, a strike – for what concerns the IoP point of view.

---

\(^{14}\) The term was originally used in the SENSEI project [37] and was only related to IoT. Then *Physical Entity* replaced the term in the IoT-A project, again only affecting the IoT domain. As the domain to which this work refers is broader, than the physical one, the original terminology was adopted, albeit with a different meaning.
Figure 12: An EoI can be a Physical Entity, a Social Entity or a composition of both.

Also an EoI can be an aggregation of more EoIs.

On the other hand, a Resource is defined as a software that provides the capability to interact with an EoI. Such interaction can be of two kinds: sensing and actuation. Sensing refers to the capability to have quantitative or qualitative information about an EoI (either a Physical Entity or a Social Entity). Actuation instead refers to the capability to change the status of the EoI.

Figure 13: Resources Provide the capability of interacting with (i.e. sensing or actuating on) an EoI.

As the Resource is a software entity, in order to provide interaction with an EoI which is not a software entity, the Resource needs an adapter who can transport the information to or from the digital domain. In the IoT DM this function was carried out by the Device component, which was generally identified as a hardware component.
In the IoTP DM, we define an Adapter as a component that lies on the border between the digital domain and another domain, i.e. and the physical or the social domain. Currently the adapter can be of two logical types: Sensors and Actuators. Sensors monitor the social and/or physical dimensions of EoIs, i.e. they transform characteristics of other domains in digital information. On the other hand, Actuators transform digital commands into changes of states of the EoI they act on. For obvious reasons there cannot be Social Actuators.

---

15 The term domain here is used as a more specific synonym of “world”. It is not related to the meaning of domain as in “the domain views in which a system is divided”.

40
Figure 15: Adapter class and its specializations

Each Adapter can be associated to one or more EoIs. For example a mobile temperature sensor will be associated to different places during its movement, but, as long as it is active, it will always be associated to at least one EoI.

From another perspective, it is worth mentioning that, for IoT systems, EoIs are relevant if they have a unique digital (i.e. software) representation called Virtual Entity (VE). In order to qualify as a VE, the representation of the EoI must be meaningful, i.e. the relevant state of the EoI must be correctly represented and updated if it changes. For what concerns Social Entities, the challenge is to identify at the moment a Resource is created the time-span for which it can be considered a relevant updated for the Virtual Entity it is associated to.
Moreover, as both IoT and IoP EoIs can have an internal structure (for example as a community can have members or a building can have rooms), so can VE s. In this case, each component of the EoI can have an associated VE and the EoI resulting from the aggregation of composing EoIs will have an associated VE that results from the aggregation of the composing VEs. Any VE must be associated to at least one Resource, and thus there must be at least one Adapter capable of realising the interaction with the associated EoI at any given time. In this way, the requirement of having in the VE a meaningful representation of the EoI is satisfied. This is a requirement for supporting any system with IoTP. The association between VEs and Resources is stored in an infrastructural component of the IoTP called Look-up Service (see Chapter 5.5), according to its functional definition. IoTP Resources are by definition heterogeneous. This heterogeneity depends on the software environment where they are deployed, the specific procedures used to interface with the User, and the different capabilities they provide. The last element that must be introduced in order to close the loop and enable the execution of User-EoI interaction through the digital world is a communication interface that will provide abstraction from the heterogeneity of Resources. This component is called Service because, indeed, from the user point of view, disregarding its background behaviour, this entity provides a service to the User.

Finally, in Figure 17, we can draw a complete view of the IoTP-based ICT systems.
Figure 17: The high-level picture of the IoTP domain model. Brown arrows are used to show real-world interactions, which are mediated through the digital world (black arrows).

5.3. Interaction model of the IoTP

IoTP inherits the interaction patterns from both IoT and IoP. After analysing these patterns three main types of interaction have been:

- **Synchronous request**: the *User* requests the use of the *Resource* in real-time and waits for the response (the “call-reply” pattern). In IoT this can be the request to read the sensor data in that specific moment or to use an actuator upon receiving a command. In IoP generally this kind of interaction is not available because Social Sensors are not available all the time.

- **Asynchronous request**: the *User* requests the use of a *Storage Resource* with archive capabilities or requests the activation of a *Resource* without waiting for response. The *User* will wait for the response to be sent later. For example, in IoT, a *User* can look-up and request sensor data which was previously collected and stored in an archive or request an actuation in the future. In IoP a *User* could look-
up a Resource according to specific criteria (geofencing, identity or semantic tags, or other kinds of context) that was previously created.

- Event-driven interaction: the User subscribes alerts for a given context. Any event (external or internal, of the physical, the social or the digital world) related to that context will launch a call-back from the Service to the User.

5.4. Resource Model

Albeit invisible to the User, Resources are one of the most important components when designing IoTP systems. They represent an abstraction of the information class that is envisioned in the IM of an IoTP-based information system. This Resource is a super-class of the IoT-A Resource which can also be specialized as an IoP Resource (Figure 7).

In the following a rather extended structure of an IoTP Resource is provided. This structure hosts many parameters, most of which optional, that help in providing the context and added-value to the raw information transported within. Some of these are created at collection time by Sensors, while others must be filled out by the Service or the real-world owner of the Resource.

- **Resource Type**: this field describes the type of the Resource. The description has an internal structure related to the capabilities it provides.
  - **Sensor**: identifies the resource as a sensor Resource, and describe its characteristics as a sensor
    - **isPhysical**: this Resource uses an IoT Sensor
    - **isSocial**: this Resource uses an IoP Sensor
    - **hasQuantitativeData**: this field identifies the Sensor as one providing quantitative data and specifies the metadata needed to use it:
      - **Measurable**: the physical quality that is measured by the sensor
      - **Presence**: indicates that the Adapter only senses the presence of a Virtual Entity. This is generally associated to autoID –based Adapters
      - **Unit**: indicates the measurement unit in which the value is expressed
      - **Time**: indicates if the availability of the Resource for what concerns time
        - **Real-Time**: these Resources can be accessed at any time in the future and provide a value measured in the specific moment. For what concerns IoP this option can be found only on Resources derived from datamining and from crowd-sourcing. Participatory sensing cannot provide real-time data
- Archive: if the Resource stores past values sensed by the Sensor associated to this Resource
- Delayed: if the Adapter is not always connected and only provides data once, at given (or unpredictable) times

- Technical Information Quality\(^{16}\): precision, reliability, latency, are all relevant parameters to be taken into account
- hasQualitativeData:
  - Type: Qualitative data can have a structure and contain more than one type of data
    - Text
    - Picture
    - Video
    - Audio
    - Structured data
    - Annotations/tags

- Actuator: only available for the physical environment, i.e. in an IoT sub-system
  - Type: identifies the type of actuator (mechanical, lighting, temperature, etc.)
  - Range: describes the range of commands that can be used to command the actuator.
  - Syntax: identifies the syntax that must be used to command the actuator.
  - Time: indicates if the availability of the Resource for what concerns time
    - Real-Time: these Resources can be accessed at any time in the future and provide a value measured in the specific moment. For what concerns IoP this option can be found only on Resources derived from datamining and from crowd-sourcing. Participatory sensing cannot provide real-time data
    - Archive: if the past values sensed by the Adapter associated to this Resource have been recorded and can be accessed
    - Delayed: if the Actuator is not always connected and accept commands to be executed in the future at its first connection or at scheduled times

- Associated Adapter: identifies the instance of the Adapter associated to the Resource. This can be used for reputation evaluation and trust metering.
- Associated VE\(s\): identifies the Virtual Entity or Entities associated to the Resource. For each of these entities the indication if the association is persistent or not

\(^{16}\) See Chapter 4.5
should be available. For example an IoP Resource is created by a citizen providing content

- **Associated Service**: includes all the information needed for contacting the Service providing access to the Resource
  - **Access Methods**: describes how to access the Service, i.e. what communication protocol, what authentication method, what security features are supported or required for accessing the Service
  - **Service Locator**: it is assumed that the network uses the IP protocol, so the locator of the service could be an IP address. However if an ID/locator split approach is applied, the ID of the service could be enough

- **Location**: the geographic location of the Adapter or of the Virtual Entity it is associated to. The location can be a point, an area or a volume and can be expressed either in coordinates or as a name pointing to a geographic location [70]
  - **Coordinates**
    - **Point**
    - **Area**
    - **Volume**
  - **Names**

While the concept of Resource that needs to be looked up can vary between the two paradigms, both IoT and IoP provide their users the ability to search Resources. As it was shown in the previous section, Resources should have an associated description in order to enable their identification among the complete set of available Resources and enable syntactic and semantic interoperability. Indeed, almost all fields of the aforementioned description are mandatory when using an M2M approach because the basic assumption of IoTP is that these paradigms connect heterogeneous systems, which are not aware of how other systems communicate.

From a practical point of view, this information could be described in RDF, or better RDFS, in order to be managed by the infrastructural services that provide lookup functionalities. However, other descriptive languages – or even specific ontologies – could theoretically be used as well.

### 5.5. The Functional Model

The functional model of a system or real-world area is a structured specification of the functions within the modelled system or area. The main concept in this modelling perspective is the process; this could be a function calculation, transformation, activity, action, task etc. A functional modelling perspective is a process-oriented view on the system or area. Other possible perspectives in system modelling are: behavioural, informational, and eventually organisational (for business systems).

System functional model representation promotes functional decomposition, that is the process of partitioning a function in its constituent parts in such a way that the original function can be reconstructed from those parts by functional composition.

To represent functional models UML introduces use cases and activity diagrams, and the structured analysis and design methods introduce data flow diagrams. In the following a set
of reference use cases will be provided. These have been derived from interviews with experts in the field of IoT and of urban planning as well as from the surveys on IoP.

5.5.1 Use Cases

The simplest scenario that can be conceived is when a user needs to access a Service it has already identified as providing access to a Resource he needs.

![Diagram](uc UC0
User
Invoke Service
Access Resource
Distributed Environment)

**Figure 18: Service invocation. The resource access is transparent to the User.**

For example, a citizen could need to know the temperature at home or at his working place (an IoT Resource he already knows and of which he knows the Service needed to access it) or a comment thread he previously accessed (an IoP Resource of which he knows the Service needed to access it). We will use this use case as a basis and gradually add different degrees of complexity to it.

5.5.2 Resource Lookup

In the previous case it was supposed that the Service needed to access the Resource was already known. But this is a rather unlikely cause in an environment that will include a huge amount of Resources. In this case, the Resource has to be identified according to some criteria provided by the User. Such criteria can be based on association to a given EoI (i.e. VE in the digital world), position, time, type of data, etc. The process is very similar to what happens today when a human user looks up for a given content on a search engine. As its counterpart in the example, the function will return a set of ranked results according a criterion. However, as the result of the lookup cannot be processed by a human but, instead, is subject to choice from a User that can be either a human or a machine, this result must be machine-readable, i.e. semantically described.
In future, such criteria could probably be set by the User himself during the query, however, in this use case we suppose that the User will autonomously verify the relevance of the results querying looking up details about the information quality of the single results. In the IoT-A project, such description is provided as a result of the initial lookup query, however, we advice against such practice due to the large overhead concerning both server-side processing and client-side communication, especially in the case of embedded (IoT) devices acting as Users.

5.5.3 Interest Subscription

Another, slightly more complex case is that of a User that might want to subscribe a call-back for a specific event. Examples of such events can be: pollution above a given threshold, local administration takes decisions concerning a given area, citizens report crime activity or dissatisfaction when a Resource responding to a given criterion is available.

The subscription can be performed with a specific Service providing such a feature or with an infrastructural component called Watchdog. The difference is that in the first case a Resource has already been identified, while in the second, only a generic criterion will be provided to the Watchdog, which will send a call-back when a Resource satisfying that criterion will become available. The call-back will include the description of the Service providing the Resource.
5.5.4 Access Asynchronous Resource use case

Most of the current, vertical IoT scenarios and most IoP one partially implement a centralized architecture where data is mandatorily stored by a centralized component (called data sink) and then provided to Users. In some cases, this centralized component is used to provide a IoT-like behaviour, by emulating the existence of real, always connected Resources. In this case the service invocation behaves in the same way as in the previous use cases but, instead of accessing directly the Resource, the Service accesses the data sink to which the Resource previously updated the value.

![Diagram of Interest subscription use case](image)

**Figure 20: Interest subscription use case**

5.5.5 Security

The security and privacy of IoT and IoP are also similar and both, although with different meanings, employ functionalities such as authentication, authorization and reputation metering. A good knowledge base including terminology and further information about the setup of security and privacy in the IoT environment can be found in [71]. Due to the similar abstractions, security principles and architecture adopted, a large part of those architectural considerations can be applied to IoP as well.

One big difference concerns the creation of Resources which, for IoT, is delegated to machines which, generally, have preset access policies that associate to the Resources they provide. On the other hand, the content of IoP is created by humans and regards social
entities and they might have privacy or safety concerns and they might want to actively set and manage the access policies to the content they create in order to limit its availability to specific groups.

5.6. IoTP functional architecture

While we have introduced IoP and IoT as paradigms for global, pervasive, distributed data collection, it is clear that due to the very large number of Resources, Users will never be able to manage locally information about all the available Services. If we take as given that machines will be Users in the IoTP paradigm, we will have what the IoT-A project suggested since its beginning: each Device (or Adapter in IoTP terminology) can also be a User. For a completely distributed paradigm that would mean, if there only were globally \( n=10^{20} \) Users, each of them should need to store \( n \) descriptions. It simply doesn’t scale. Infrastructure services address exactly this issue: they provide the functionality of storing, organizing and managing the auxiliary information related to:

- the identification and authentication of Services and Users,
- the location of (i.e. routing to) Services on the network,
- the creation and management of Service descriptions and their association to Services and VEs, as well as the creation of the latter.
- billing and access policies for Services,
- guaranteeing security and privacy of the data collected.

In Figure 22 a layout of some basic functional components is shown.

![Figure 22: Example of the functional components the IoTP Infrastructure will need to support](image-url)
In detail, the proposed functional components can be divided into User Services, which are accessible to Users and Core Registries which are internal components accessible only to User Services and store information about the Services.

The Core Registries store critical data used and managed solely by the User Services and specifically:

- **User Registry**: securely stores the Identifier and the security material used for authentication purposes.
- **Access List Registry**: stores access policies for *Services*.
- **Billing**: stores information about the use of User Services for billing purposes.
- **Data Registry**: stores information used and managed solely by User Services and specifically:
  - **User Registry**: securely stores the Identifier and the security material used for authentication purposes.
  - **Access List Registry**: stores access policies for *Services*.
  - **Billing**: stores information about the use of User Services for billing purposes.
  - **Data Registry**: stores information about *Services*, including the description of the *Resources* associated to the *Service*.

On the other hand, the User Services provide the following functionalities:

- **Watchdog**: this component is in charge of firing a call-back to the User when the event for which the User subscribed an interest occurred. The Watchdog component can poll the Resource Registry in order to identify new, relevant *Resources*. It must also monitor the Data Registries – where these are available – to check the values collected by Sensors. However, in a completely distributed environment, Data Registries don’t exist and call-back functionality must be implemented directly by the *Services* in case of a completely distributed approach. This component leverages the Data and Service Registries components.
- **Service Manager**: it allows the registration of new *Services*. It provides an interface for the registration and updating of the auxiliary information related to *Services* (e.g., IP address, description of associated *Resources*, supported protocols, etc.). According to the functionality requested, the Service Manager can read or write data to the Service Registry and can remove policies from the Access List Registries.
- **Service Resolution**: it provides *Users* with information about the network location of the *Services*. This function is similar to that of current DNS services. It is used for retrieving the network address (i.e., locator) of a Service, given its identifier. The functionality is mainly aimed to support mobile *Services* which change address, in case mobility is not directly supported by the NWK layer protocol of the stack (e.g., mobileIP [72]) or a specific ID layer, implementing the ID/locator split, is used (see HIP [73]). This component uses mainly the Service Registry.
- **Service Lookup**: this component searches in the Service Registry for *Services* that comply with a set of given criteria provided by the *User* in the frame of a lookup query. Specifications should be provided for what concerns the ontology and semantics used in the queries for interoperability purposes. While generally, the lookup process involves the description of *Resources*, the functionality and the component is related to the *Service*, because, from a use case point of view, *Resources* are invisible to *Users*.
- **Security and Privacy Services**: provides authentication of *Users* and *Services*, authorization access features, support to privacy protection through
pseudonimization, and the management for the security features themselves (i.e. registration of new Users, Services, creation and modification of access policies, etc) and so on. Again, for further reading the initial chapters of [71] are suggested. The component also is manages the interaction between different functional components for what concerns security. For example Users that are not entitled to access a Service are also denied access to their description and will not receive that Service as a result in queries. In this sense, this component filters the interaction between all User Services and Core Services.

Note that, even at infrastructure level, Resources do not appear explicitly because they are meant to implement capabilities that can only be accessed by Services and which are provided to the IoTP domain only through the Services themselves. It is important to understand that the infrastructure services are not meant to be centralized. The scalability issues that were the reason for their adoption would make them unusable too. It is out of the scope of this work to investigate the best way to geographically distribute and deploy the instances of the IoTP infrastructure. However it is relevant to note that the adoption of the IoTP probably will not be a global, uniformly distributed process. It will probably start in the background, from key, business-driven domains. In this stage, due to the huge potential in increasing the efficiency of processes, the optimal technological environment, urban IoTP-based systems will probably be the pioneers of the IoTP advent. This might well mean that the infrastructure services might initially be themed on urban processes and might need to address scalability issues typical to urban distributed ICT systems.
Chapter 6. Concluding Remarks

6.1. Conclusions

During this PhD work I have gradually started to understand the depth of the potential of applying IoT and IoP paradigm to human life processes. In particular a conspicuous number of applications – i.e. processes of the urban system – could benefit from applying the IoTP paradigm for two main reasons: extending and improving the automation of same processes (and thus their efficiency), and having a more complete and systematic view of the urban processes in both their physical and social dimensions in order to allow their optimization, innovation or re-structuring. These changes are very important for the sustainability of the same processes from the environmental, cost and social impact point of view. In order to enable the efficient adoption of IoTP as the main paradigm for information systems in urban environment, a reference architecture for these systems is needed.

In this work, an abstract model of urban processes is for the first time provided and used in a holistic approach to urban design that views the city as a complex system. This model was developed because such systematic approach to systems engineering in a urban context was missing and still I felt that was needed to provide the logical glue between the high level systems design and the specific design of information systems. Finally, I have extended the IoT reference architecture as developed in the frame of the IoT-A project to the IoP domain. In this thesis, the basis for such IoTP reference architecture has been set. The hope is that the different stakeholders of urban systems have been provided with the conceptual tools needed to understand the problem and participate effectively in the design process by “talking the same language”.

The intended audience, who would most benefit from this reading, is made of software engineers, urban planners, and administration personnel. Here they could find:

- A general approach to the analysis and design of urban systems
- An analysis of the current IoT and IoP architectures
- An explanation of the benefits of adopting the IoTP paradigm for information systems in the urban context and
- The basic models for the IoTP reference architecture (the Domain Model, the Interaction Model, the Resource Model and the Functional Model) along with some methodology background

6.2. Challenges

While the benefits provided by IoT and IoP are clear, their true potential has yet to be explored. As with all innovative paradigms, there are several challenges.
One of the key concepts of IoTP is that applications that until now were closed and vertical can use resources provided by different applications. This raises a host of interoperability issues, which have different declinations in IoT, where the constraints of device processing and communication is the main limit, and IoP, where the lack of interoperability is related to a lack of unsupportive business models. Solutions to these issues range from power-efficiency increase in IoT nodes to using open-source semantic frameworks for the description of services, resources and processes. Yet interoperability is a key concept that must be addressed in the frame of the IoTP reference architecture and guidelines for achieving this essential quality must be provided.

6.3. Future Work

While this work starts the process of defining the IoTP reference architecture, it is clear that this is subject to improvement and expansion. The reference architecture, in its current status, is only a knowledge base. However, a reference architecture should also include tools for developing and implementing architectures, such as design guidelines and architectural patterns and styles, etc. The reference architecture moreover, although is based on high level abstractions and is used for creating new implemented architectures, is still subject to evolution due to the evolution of the underlying and generic ICT technologies, built from the abstraction of existing architecture.

Moreover, in second stance, the reference architecture for the IoTP in urban context could be used as one of the reference architectures from which to abstract the domain-independent Reference Model of the IoTP.

Figure 23: Description of the process of deriving a reference model of IoTP
From another point of view the generalization of the IoT paradigm is very attractive. Currently the *things* are physical objects. There are parts of the scientific community though that would like to interpret the term “things” as any …thing. While conceptually attractive, I personally fail to understand the benefit of generalizing to this extent the IoT concept. However there are some other very interesting interpretations of Internet of * concept. In the years when I attended university, I was already astonished by the similarities between living and ICT systems. Now I could say (joking) that both systems have an information system. From Ageno’s definition of living system, to the fact that DNA has error correction features, or to that that cells communicate through molecules dispersed in blood, there are many analogies. The last one is particularly interesting from my point of view.

It is clear that cells have a communication protocol. We don’t know yet the syntax and semantics of its “payload”, but one day we might understand it. In that moment M2M communication will hold a completely new meaning. There are already ideas of using injected nanomachines for medical reasons. Well, supposing that these nanomachines could sense the communication of cells, they would become the smallest, yet more revolutionary, *Adapter* of all Internet of *. Gateways could be developed and new layers of network miniaturization would be developed.

Maybe we will be soon working on an Internet of Plants [74] reference architecture soon, or maybe IoTTP-based systems will evolve to digital ecosystems similar to living ecosystems. Who knows?
References


[52] Takhteyev, Y., Gruzd, A., and Wellman, G., Geography of Twitter networks, Social Networks, vol 34, no.10, pp. 73-81, Jan 2012, Elsevier


[56] Castellani, A.P., Gheda, M., Bui, N., Rossi, and M., Zorzi, M., Web Services for the Internet of Things through CoAP and EXI, Communications Workshops (ICC), 2011 IEEE International Conference on, 5-8 Jun 2011, Kyoto, Japan


[63] Al-Hader, M., Rodzi, A., Sharif, A. R., Ahmad, N., Smart City Components Architecture, in Computational Intelligence Modelling and Simulation, 2009 International Conference on, (ICCIMS), 7-9 Sep 2009, Brno, Czech Republic


Appendices

A. Requirement gathering for IoP

A.1. English version

This document aims to support the process of identifying the requirements for the application of the Internet of People (IoP) in the urban sector. You receive this document because you have agreed to contribute to the process of gathering requirements for the design of a reference architecture for IoP systems in urban areas.

IoP is a paradigm of interaction between people who envisages them as nodes of a global and pervasive communication network that transfers information using the Internet infrastructure and ICT technologies. The IoP projects in digital world some of the relationships and of the interactions that exist between people in a given context (social, occupational, communities of practice, etc.). In the future, however, the data transmitted through IoP could be used also by software agents employed for the monitoring and control of phenomena and urban processes of various kinds in physical reality.

Social networks are increasingly cited as a participatory tool in urban areas. However, the IoP is not limited to social networks, but also includes Microblogging platforms, forums and Instant Messaging. We assume that people have an ICT device that works as user interface (hardware and software) and allows citizens to enter and use the information provided by IoP Services to interact with the IoP.

1. How do you evaluate your expertise and knowledge of the problems and issues of Smart Cities? If you work in this field, are you specialized in a specific field?
1.1. In which of the following field do you have experience? [Multiple choices allowed]:
• Architecture and city planning
• Civil Engineering
• ICT, Computer Engineering, System Engineering and Process Engineering
• Other (please specify)
2. What kind of information transmitted through the IoP can be useful in a urban context?
3. Elaborate briefly on whether and how the following IoP Application classes could be used in a urban context:

17 An Italian version was also used but has been omitted being a simple translation of the present one.
3.1. Generic Social Network Sites (Facebook, Myspace e 4Square) and specific ones (such as Youtown, EveryBlock, Giropasta, …): list which could be the aims and their ways of use, clearly identifying who are the users and which the other stakeholders. Feel free to split the answer in two or more use case scenarios.

3.2. Microblogging platforms (e.g. Twitter): list which could be the aims and their ways of use, clearly identifying who are the users and which the other stakeholders. Feel free to split the answer in two or more use case scenarios.

3.3. Instant Messaging platforms (e.g. Messenger, gChat, Skype, …): list which could be the aims and their ways of use, clearly identifying who are the users and which the other stakeholders. Feel free to split the answer in two or more use case scenarios.

3.4. Altre piattaforme di condivisione (es. flickr, Picasa, LinkedIN, …): list which could be the aims and their ways of use, clearly identifying who are the users and which the other stakeholders. Feel free to split the answer in two or more use case scenarios.

4. Suppose that software agent could autonomously understand the meaning of the data transferred through IoP, briefly describe how you imagine a use case scenario that uses this capability.

Thank you for your availability. It will be my pleasure to send you an electronic copy of the work you have contributed to, once it is finished.