A set of Good Practices
and
Recommendations for Smart City Resilience Engineering and Evaluation

Published by AIIC
February 2019

AIIC

A set of Good Practices and Recommendations for Smart City Resilience Engineering and Evaluation

Published by AIIC February 2019

This document is the result of a joint project coordinated by Sandro Bologna and implemented with contributes of (in alphabetical order) Glauco Bertocchi, Sandro Bologna, Luigi Carrozzi, Donato Di Ludovico, Donatella Dominici, Priscilla Inzerilli, Luisa Franchina, Alberto Traballesi.

Acknowledgment: The authors would like to thank the Italian Association of Critical Infrastructures' Experts (AIIC) for its support and stimulus.

Disclaimer: The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of their respective employers.

The present version of the Recommendations represents the state of the work at the date of the publication.

Table of content

Document Scope

Aim of this document is to report the scouting activities performed by some AIIC Members, addressing the state of the art in the area of Smart City Resilience, with a special emphasis on the relation between “smartness” and “resilience”. The problem is well illustrated by the following figure, taken from the web.

IS YOUR SMART CITY A RESILIENT CITY?
Adding environmental and natural hazard risk data into the smart city mix would add some much-needed context and reality to this brave new technical world.
oasis HUB

The justification for a Document dealing with urban resilience and smartness is clear: urban areas, the engines of economic growth, are projected to provide the living and work environment for two-thirds of the global population of close to 10 billion by 2050. The concepts of Smart City and Resilient City go hand in hand with each other and thus are interrelated.

This document is primarily intended for use by organizations with responsibility for urban governance. However, it is equally applicable to all types and sizes of organizations that represent the community of stakeholders, and those organizations that have a role in urban planning, development and management processes in urban areas around the world.

This document describes a framework and principles that want to be coherent with the entire UN Agenda 2030, to goal 11 Sustainable Cities and Communities, to make cities and human settlements inclusive, safe, resilient and sustainable.

To avoid repetitions, the content of the present document is coherent and heavily based on the content of the previous AIIC Reports, referred here following:

Guidelines for Critical Infrastructures Resilience Evaluation[1]

Guidelines for Community Resilience Evaluation[2]

Good Practices and Recommendations on the use of Big Data Analytics for Critical Infrastructure Resilience[3]

Cyber-Insurance: Analisi e metodologia per la valutazione dei rischi residui[4]

The proposed framework would complement the already extensive Reports produced by AIIC and fill the gaps, with specific reference to Smart and Resilient City.

In order to more effectively understand and contextualize this proposal, it is vital to acknowledge the work in progress, at the date of publication, on this topic inside *ISO/TR WD 22370:2019 – WD 2*, from which we fully endorsed the following principles:

Principle 1: Dynamic nature of urban resilience
Resilience is not a condition but a state that cannot be sustained unless the system evolves, transforms and adapts to current and future circumstances and changes. Therefore, building resilience requires the implementation of context-specific and flexible plans and actions that can be adjusted to the dynamic nature of risk and resilience.
Principle 2: Systemic approach
Recognizing that urban areas are comprised of systems interconnected through complex networks and that changes in one part have the potential to propagate through the whole network, building resilience requires a broad and holistic approach that takes into account these interdependencies when the urban system is exposed to disturbances.
Principle 3: Promote participation in planning and governance
A resilient system ensures the preservation of life, limitation of injury, and enhancement of the 'prosperity' of its inhabitants by promoting inclusiveness and fostering comprehensive and meaningful participation of all, particularly those in vulnerable situations, in planning and various governance processes. Such an approach can ensure sense of ownership, thus achieving successful implementation of plans and actions.
Principle 4: Multi-stakeholder engagement
A resilient system should ensure the continuity of governance, economy, commerce and other functions and flows upon which its inhabitants rely. This necessitates promoting open communication and facilitating integrative collaborations between a broad array of stakeholders ranging from public entities, private sector, civil society organizations, and academia to all inhabitants.
Principle 5: Strive towards development goals
Resilience building should drive towards, safeguard and sustain development goals. Approaches to resilience should ensure that efforts to reduce risk and alleviate certain vulnerabilities does not generate or increase others. It must guarantee that human rights are fulfilled, respected and protected of under any circumstances.

[1] http://www.infrastrutturecritiche.it/media-files/2017/03/RESILIENCE_Guidelines_AIIC.pdf

[2] http://www.infrastrutturecritiche.it/media-files /2017/03/COMMUNITY_Resilience_AIIC.pdf

[3] http://www.infrastrutturecritiche.it/ media-files /2018/04/AIIC_BigDataCIPR_FINALE.pdf

[4] https://www.infrastrutturecritiche.it/cyber-insurance-analisi-metodologia-per-la-valutazione-dei-rischi/ (in italian)

Preface *(Sandro Bologna)*

There have been numerous studies attempting to define the Smart City concept, but it is still a difficult challenge to tackle. It is a multidisciplinary concept and to define '*Smart*' is difficult. The first attempts to define the concept were focused on the smartness provided by information technology for managing various city functions. Lately the studies have widened their scope to include the outcome of the Smart City such as sustainability, quality of life, and services to the citizens.

A good conceptualization of Smart City is represented by Figure 1.

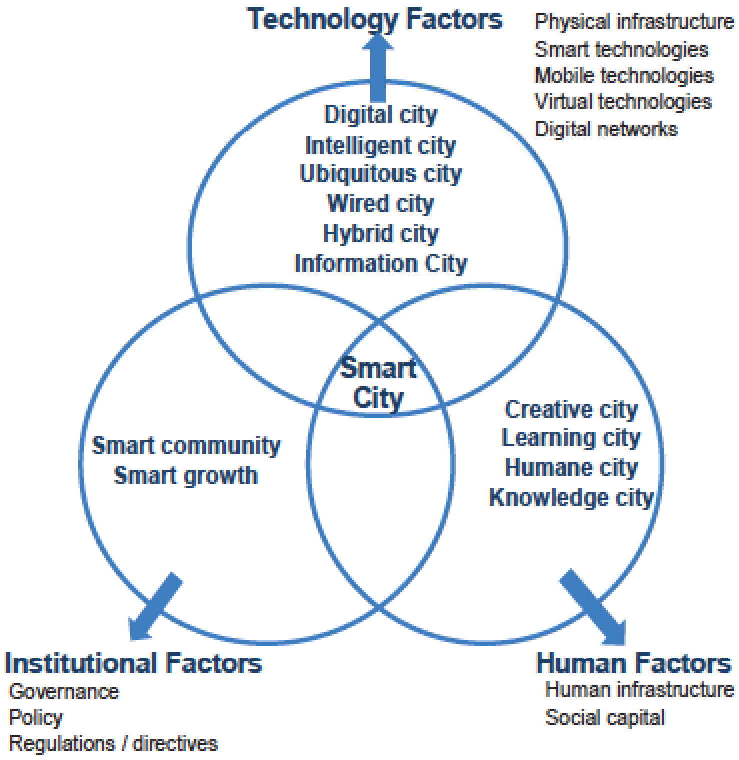


Figure 1. Conceptualization of Smart City

(*Source: Towards Smart and Resilient City: A Conceptual Model Y Arafah et al 2018 IOP Conf. Ser.: Earth Environ. Sci.* ***158*** *012045*)[5]

The first appearance of the concept *resilience* in connection with urban policy dates to 2002. However, only not earlier than 2012 the frequency of searches in Google for Resilient City started to boom[6]. For the cities of the future to be smart, urban resilience must first be achieved.

In contrast with Smart City, the number of definitions of Resilient City is limited. Cities who call themselves resilient, like Rotterdam and The Hague in The Netherlands, claim to build capacity within individuals, communities, institutions, businesses, and systems to survive, adapt, and grow; no matter what kinds of chronic stresses and acute shocks they experience.

[5] http://iopscience.iop.org/article/10.1088/1755-1315/158/1/012045/meta

[6] http://smartcityhub.com/collaborative-city/smart-cities-resilient-cities-make-difference/

While transforming urban areas into better place to live in by increasing smartness, resilience would support the improvement of their capacities to prepare, respond and recover from all potential shocks, stresses and challenges, leading them towards sustainability.

The first difficulty in meeting this demand was the development of a universal approach, a robust model together with characteristics, to understanding and evaluating resilience, in any human settlement or Community, in any circumstance or context.

The concepts Smart and Resilient City have different roots. Large technology companies, like Cisco, IBM, Siemens, Philips started promoting to become a Smart City expert ten years ago during the economic crisis as part of their strategy to find new markets and to attract new customers.

The use of the concept is promoted by international organizations and associations of cities in order to improve city's capabilities to deal with hazards like the hurricanes Katarina in the New Orleans region (2005) and Sandy along the east coast of North America (2012).

The concept of Smart Cities should not be discarded, but it should be embedded within a broader framework of Resilient Cities. In fact, smart technologies are instrumental in the development of resilience.

Resilient Cities are those in which their citizens, businesses, and infrastructures have the capacity to withstand, adapt, and recover in a timely manner from any kind of hazards they face, either planned or unplanned.

Resilience is an important factor as we are facing rapidly changing natural and social conditions, which require cities to be more resilient. The resilience concept in the context of a city refers to the city's ability to absorb, adapt, and respond to any changes in urban system. Therefore, a Resilient City is able to withstand the impact of shocks, hazards, and pressures through adaptability or transformation to ensure the long-term sustainability, basic functions, characteristics and the structure of a city (UNISDR, *How To Make Cities More Resilient A Handbook For Local Government Leaders*. Geneva: United Nations, 2012)[7]. Resilience cannot be reached in one step, it is a new approach to city design and implementation[8].

The implementation of the concept of Smart City Resilience will benefit of the two most disruptive technologies of these last years:
Internet of Things: Interconnection and permanent information of each point of the city.
Big Data: Permanent interpretation of data for the evaluation and evolution of the state of the city.

The concepts of Smart City and Resilient City are concepts that goes hand in hand and have a close relationship and linkage. The best representation we know is from the paper "*Towards a Smart and Resilient City: A conceptual model*"[9]. The proposed model tries to combine the components and character of Smart City and Resilient City into a new, integrated concept: the "Smart and Resilient City". It is still a recommendation that requires more in-depth research, exploration, and model testing.

[7] https://www.unisdr.org/files/26462_handbookfinalonlineversion.pdf

[8] https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-city-resilience-digitally-empowering-cities-to-survive-adapt-and-thrive

[9] http://iopscience.iop.org/article/10.1088/1755-1315/158/1/012045/meta

1 Introduction *(Sandro Bologna)*

Over 50 percent of the global population now live in urban areas, and it is projected that by 2050, more than two thirds of the world's population will reside in an urban setting[10]. This growth trajectory means that cities will face increasing challenges in all aspects of their operations. Cities are particularly vulnerable to problems such as social imbalances, traffic congestion, pollution and strain on resources. It is recognized by Mayors around the globe that deployment of sustainability strategies and becoming technologically smarter is necessary to improve quality of life in cities. In addition, it is understood that embracing advanced technologies will enable smart growth strategies which in turn leads to investment attraction and growth in cities.

Smart Cities increasingly incorporate computer-enabled networks, sensors, and software into buildings and infrastructure, where citizens and municipalities can control lighting, heating, and air conditioning. Sensor technologies can collect information in real time to manage traffic flow and energy use, and critical information can be deployed to do everything from reducing consumption of natural resources to empowering citizens to communicate more readily with first responders and with one another during an emergency.

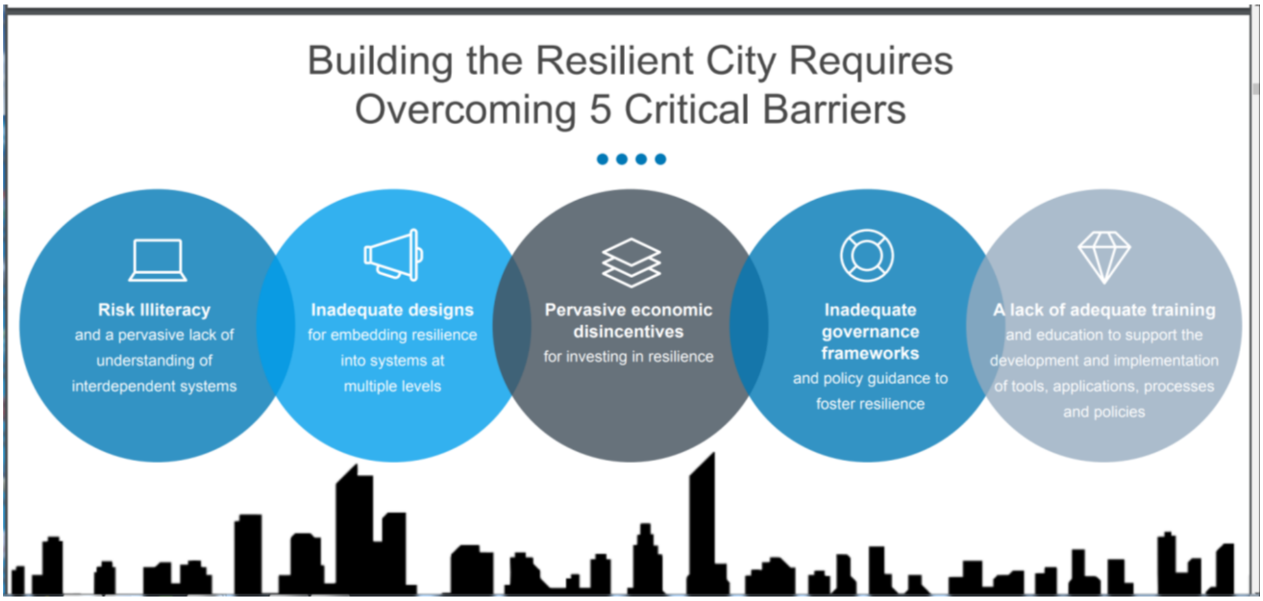
Smart Cities are powered by networks. Devices, people, businesses, and governments must all be able to connect securely, reliably, and quickly in order to share data to improve how people live, work, and manage their daily activities. Even while adopting the most current state of the art telecommunications and network technologies, a meaningful “Smart Cities” strategy must also pave the way for the integration of the next generation of wireless networks and services. This will have to occur not only in the telecommunications companies themselves but in all participating sectors of the economy. Additionally, inherent to any interconnected ecosystem, there are security challenges and altered expectations of privacy[11].

A Smart City approach must ensure that the increase in smart technology is accompanied by strategies to enhance cyber and physical security. As with any complex project, security and privacy must be baked in. That's especially so when a government agency and/or public institution works with vendors and contractors to get the work done - and usually, they do. Having a third party involved raises another level of security awareness to any IT project, even the most trivial. It opens the network to whatever malware infections the contractor brings-in, whether it's cash registers or smart streetlights. Adding the IoT, sensors, GPS, and lots of new stuff is the rule. That type of infrastructure is especially vulnerable to hacking, due to ill-thought-out IoT security. That's because there's been a big push to do IoT cheap and get Internet-enabled devices to market quickly. Developers rely on specific functions in open Source code to do that.

These sensors and smart devices can allow government agencies to not only capture data through IoT-enabled sensors, but to deliver that data to an Intelligent Infrastructure Management (IIM) system. This system performs real-time monitoring of the condition of assets, as well as predicts their condition over time, by applying algorithms that make use of Artificial Intelligence and Big Data Analytics. Armed with this real-time and predictive data, government officials can take immediate action, such as dispatching road maintenance crews, rerouting traffic or deciding whether to repair something, tear it down or invest in new assets.

[10] AIIC “Guidelines for Community Resilience Evaluation” 2017 http://www.infrastrutturecritiche.it/new/media-files/2017/03/COMMUNITY_Resilience_AIIC.pdf

[11] Clinton A. Vince and Jennifer Morrissey “Smart Cities – Modernizing Our Infrastructure as a Platform for Exciting Technology” IEEE Smart Grid Newsletter, March 2018


Building the Resilient City Requires Overcoming 5 Critical Barriers
Risk Illiteracy and a pervasive lack of understanding of interdependent systems
Inadequate designs for embedding resilience into systems at multiple levels
Pervasive economic disincentives for investing in resilience
Inadequate governance frameworks and policy guidance to foster resilience
A lack of adequate training and education to support the development and implementation of tools, applications, processes and policies

source: Prof. Stephen E. Flynn – Northeastern University

Figure 2. Critical barriers for Smart City Resilience

(Source prof. Stephen E. Flynn – Northeastern University)

Most Smart City research has been conducted on large cities, leaving the much larger number of smaller cities left with trying to decide what parts of the larger city projects can be done with the resources smaller cities have available. What about cities with fewer than 100,000 in population? We believe it is easier for large cities (with greater resources) to scale up a framework that succeeds in a small city context than it is for a small city (with fewer resources) to scale down a framework developed in a large city context. The paper "*A Systems Approach to Smart City Infrastructure: A Small City Perspective (2016)*"[12] uses a design science methodology to bring together the common themes in many definitions of Smart Cities to create a framework that establishes a broad and robust definition of a Smart City. Further, it identifies the requirements and measures needed to assess the "smartness" of a city. While many papers identify technologies that can be used to build Smart Cities, none provide a comprehensive basis for comparing two or more Smart Cities with respect to their "smartness". Additionally, the lack of a comprehensive framework leaves practitioners with no guidance on how to make it all work. The framework developed in this paper considers the limited budgets and limited technical resources owned by smaller cities. A special section of our Report is devoted to the experience gained with the city of Aquila, where the concepts of smart, resilience and safety have been used to drive the rebuilding after the earthquake.

1.1 Benefits of Smart Cities

Five factors are driving a greater interest in intelligent infrastructure[13].

[12] http://iot-smartcities.lero.ie/wp-content/uploads/2016/12/A-Systems-Approach-to-Smart-City-Infrastructure-A-Small-City-Perspective.pdf

[13] Forbes insights "Intelligent Infrastructures: How sensor-enabled devices, data streams and robust management systems can build a low-cost smart city network"

Safety: Deficiencies in aging bridge systems are one of the key contributors to life-threatening road conditions for drivers. Fortunately, smart sensors can significantly reduce the risk and improve capacity monitoring and planning by identifying bridges failures before disaster strikes. This not only protects motorists but minimizes occupational hazards for city workers. By gathering real-time data, smart technologies can prevent emergencies that require multiple teams to work under some of the most dangerous conditions.

Resilience: There are more than 120 definitions of resilience, most of them are qualitative. AIIC has published two Guidelines on the subject, also referred at the beginning of this Report. The essence and components of city resilience consists of working to 1) prevent any potential threat; 2) withstand any impact caused; 3) react to the crises derived from the impact; 4) recover the city's functionalities; 5) learn from the experience.

Speed: The ability to act fast is another advantage of analyzing sensor data. Rather than rely on third-party reporting of an asset's condition, cities can receive real-time alerts and issue work orders automatically to expedite the resolution of any problems with critical infrastructure assets. In addition to automating the appropriate business workflow, such as dispatching a maintenance crew, an Intelligent Infrastructure Management system can specify job requirements, such as whether an issue involves high-voltage electricity, or if an excavation team is needed on site. By providing these details, dispatchers can ensure "the right people get to the right place at the right time" for first-time resolution of a problem.

Cost savings: The Global Infrastructure Hub estimates that $15 trillion will be required over the next 20 years to support the world's growing infrastructure needs[14]. Funding this demand will not only require designing and building new infrastructure but extending the life cycle of existing assets. Fortunately, smart devices can help by gathering data directly from an asset, analyzing it to detect anomalies and predicting maintenance issues before they emerge. For example, a bridge may show changes in curvature - an early warning sign of damage. By identifying these changes, cities can take corrective action long before they would normally detect a problem and at a fraction of the cost of having to rebuild a collapsed bridge.

Quality of living: Predictive capabilities can also have a direct impact on quality of life. A smart traffic light control system, for example, can work dynamically - changing street lights from red to green - based on the number of vehicles in a specific location. Other applications include parking identification systems that use spatial sensors to direct drivers to empty parking spaces. These tools improve the daily commute of citizens and enhance safety on the streets – factors that are critical to quality of life.

1.2 Smart City Security and Privacy Concerns

The basic ideas in the behavior of complex systems are always the same, especially when dealing with collapses: complex systems are complex because they are dominated by the mechanism we call "feedback". Because of feedback effects, a large structure may collapse when just one of the elements that compose them fails. That may lead to the failure of the elements that surround it. These, in turn, cause the failure of other elements of the system, and so it goes. The result is what we call an "avalanche" and, as Seneca said, "ruin is rapid".

[14] Global Infrastructure Outlook https://outlook.gihub.org/

Smart City technologies also open new vulnerabilities. Cyber-attacks can bring these thriving Smart Cities to a standstill and create total chaos. Ensuring cyber-physical security against local and foreign adversaries is the new challenge for today's city planners. However, some of the smart devices used for implementing Smart City cyber-physical solutions are not sophisticated and they lack basic security safeguards. Cybercriminals are aware of the various weak points and they are ready to exploit the weaknesses.

Naturally, urban planners and Smart City governments are proactively seeking ways to make their cities infrastructure and their Industrial Control Systems (ICS) safe from potential threats. Smart cities must look at their security needs both at the macro and the micro levels. Here are some things to consider[15]:

Implement Cyber-Physical Security

Smart city technologies occupy both the physical and digital worlds. So, the cities need to address both spaces. Most IT solutions only try to secure the digital component. In a Smart City environment, it's necessary to find solutions that will prevent attacks in the Operational Technology (OT) domain too. So, a comprehensive cyber-physical security solution is a necessity for today's Smart Cities.

Use Secure Mesh Networks and Wireless Integration

High-performance mesh networks and wireless technologies are the building blocks of a Smart City grid. But it's important to use mesh network and WiFi solutions that can provide robust security for a vast range of network topographies and applications. The solutions need to have various levels of authentication mechanisms to allow more secure communication between various components.

Provide Better Perimeter Management

ICS systems that support Smart Cities must deal with a lot of complexity. So, automation through centralized management should be an integral part of the system. It will allow cities to ensure security for large areas and key infrastructure without the need for increasing manpower. Automated entry-control systems for building gates and doors can provide better perimeter control for crucial infrastructures.

Emphasize Intrusion Detection

Most IoT end-point devices like cameras and sensors don't have the necessary security capabilities. As these connected devices are increasing in Smart Cities, city planners need to upgrade to better Intrusion Detection Systems (IDS). Better IDS will prevent hackers from easily infiltrating Smart City central systems by exploiting end-point vulnerabilities.

In the rush to deploy Internet of Things (IoT) or Industrial Internet of Things (IIoT) Smart City technology, security of the devices really come into play.

Three security professionals – Daniel Crowley, research baron at IBM X-Force Red, Jennifer Savage, security researcher for Threat care, and Mauro Paredes, managing consultant at IBM X-Force Red – took a sampling of Smart City devices in use today and discussed just how

[15] Automation, September 24, 2018: How ICS Security Attacks can Cripple Smart Cities

vulnerable they were during a presentation entitled, "*Outsmarting the Smart City*," at Black Hat USA 2018 in Las Vegas[16].
Crowley mentioned what makes a Smart City smart: IIoT, Urban automation, Public safety / emergency management, Intelligent transportation systems, Metropolitan communication systems, etc. In a smart city, however, there is limited citizen privacy and risk management options, so to eliminate those issues, Savage said residents would need to make sure they have: no smart TV, no smartphone, own a very old car, or just move into a "not Smart City". "You just don't have a choice in Smart Cities," she said.

As result in a Smart City there are plenty of devices deployed that have multiple vulnerabilities and some of them are with SCADA systems. In addition, in Smart Cities, it is easier for connected vehicles communicate with each other. In some Smart Cities, folks are beginning to install smart street lights with cameras. "In Singapore, they want to put facial recognition in all street lights," Crowley said.

There are no doubt Smart Cities are the wave of the future, but in their rush to become smart, cities need to think about a total security program and ensure security is built into devices.

The paper "*Cyber security challenges in Smart Cities: Safety, security and privacy*"[17] examines two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go together with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. The interactions between person, servers and things are the major element in the Smart City and their interactions are what we need to protect.

The security and privacy of information in a Smart City has been interest of researchers. The reason behind it is that, in order to ensure the continuity of critical services like health care, governance and energy/utility issues in a Smart City, the information security must be fool proof. The factors that are taken under consideration in order to identify the issues in information security in a Smart City include governance factors, social/economic factors and most importantly economic factors. These factors are elaborated in the paper "*Smart Cities: A Survey on Security Concern*"[18]. In our Report, we have specific sections dealing with security and privacy, also in the light of using new technology solutions like Artificial Intelligence.

1.3 Different views from Smart Cities Resilience Projects

This paragraph intends only to mention different initiatives and research projects relevant for the purpose of this Document.

IMPROVER[19]

The overall objective of IMPROVER is to improve European critical infrastructure resilience to crises and disasters through the implementation of resilience concepts to real life examples of pan-European significance, including cross-border examples.

[16] http://www.isssource.com/black-hat-not-so-secure-smart-cities/

[17] https://www.sciencedirect.com/science/article/pii/S2090123214000290

[18] http://thesai.org/Downloads/Volume7No2/Paper_77-Smart_Cities_A_Survey_on_Security_Concerns.pdf

[19] http://improverproject.eu/

DARWIN[20]
The project is focused on improving responses to expected and unexpected crises affecting critical societal structures during natural disasters (e.g. flooding, earthquakes) and man-made disasters (e.g. cyber-attacks).

SMR[21]
Smart Mature Resilience (SMR) aims to develop and validate Resilience Management Guidelines, using three pilot projects covering different CI security sectors, as well as climate change and social dynamics. With the participation of Roma Capitale.

RESILENS[22]
RESILENS will develop a European Resilience Management Guideline (ERMG) to support the practical application of resilience to all CI sectors.

RESOLUTE[23]
The project recognizes foremost the ongoing profound transformation of urban environments in view of ecological, human and overall safety and security needs, as well as the growing importance of mobility within every human activity. Sustainability is rapidly becoming an imperative need across all economic and social domains. With the participation of City of Florence.

SMARTRESILIENCE[24]
SmartResilience aims to provide an innovative "holistic" methodology for assessing "*resilience*" that is based on resilience indicators.

Video with highlights from the DRS-7 Critical Infrastructure Resilience event[25], where IMPROVER, together with the four projects DARWIN, SMR, RESILENS and RESOLUTE, presented recommendations on how to align European Resilience Management Guidelines.

100 Resilient Cities[26]
Pioneered by The Rockefeller Foundation (100RC) is dedicated to helping cities around the world become more resilient to the physical, social and economic challenges that are a growing part of the 21st century.

Just to give an example of industrial proposals, Bechtel suggest "*How to transform your city with smart, resilient infrastructure"*[27] This guide provides ideas on how to use smart, resilient infrastructure to help tackle the new and emerging challenges facing cities. It shows how solar energy, fuel cells, smart grids, green infrastructure and more can help to decentralize essential services, to offer the flexibility and adaptability so vital to cities.

[20] https://h2020darwin.eu/about/
[21] https://cordis.europa.eu/project/rcn/194885_en.html
[22] http://resilens.eu/
[23] http://www.resolute-eu.org/index.php/2015-07-16-15-29-03
[24] http://www.smartresilience.eu-vri.eu/
[25] http://improverproject.eu/2018/09/25/highlights-video-from-drs-7-critical-infrastructure-resilience/
[26] http://www.100resilientcities.org/
[27] https://www.bechtel.com/smart-cities/

2 How to model a Smart City as a complex System-of-Systems *(Sandro Bologna)*

A Smart City constitutes a “System of Systems” and a set of private and public systems that the city integrates for good governance and to achieve better services for citizens. Further, as being key criteria of ideal system all major components of Smart City i.e. education, transportation, energy and water, healthcare, other ICT systems must be planned and completed simultaneously as each element of process does not appear feasible when considered separately but becomes feasible when considered collectively (*Smart City – A System of Systems*)[28]. Seen in the wider context, the concept of Smart City explains how the Information Communication Technology (ICT) plays an important role in the development of a smart system. See Figure 3 and Figure 4.

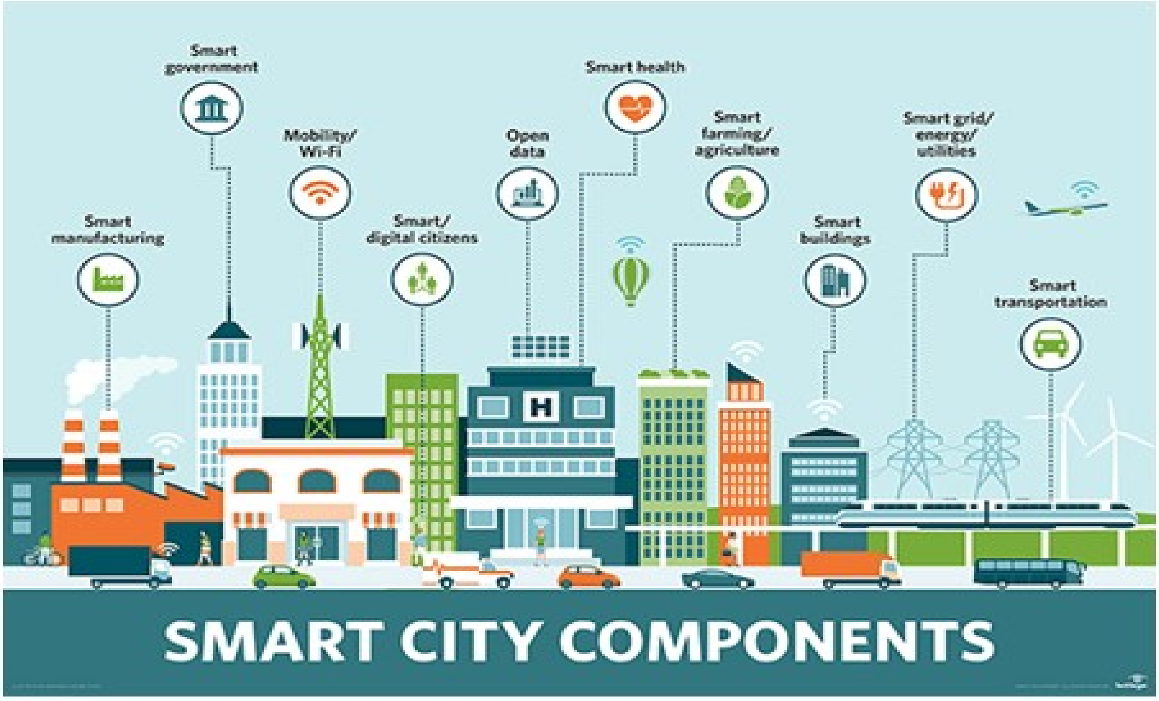


Figure 3. Smart City Components
(Source WEB)

[28] http://www.diva-portal.org/smash/get/diva2:831525/FULLTEXT01.pdf

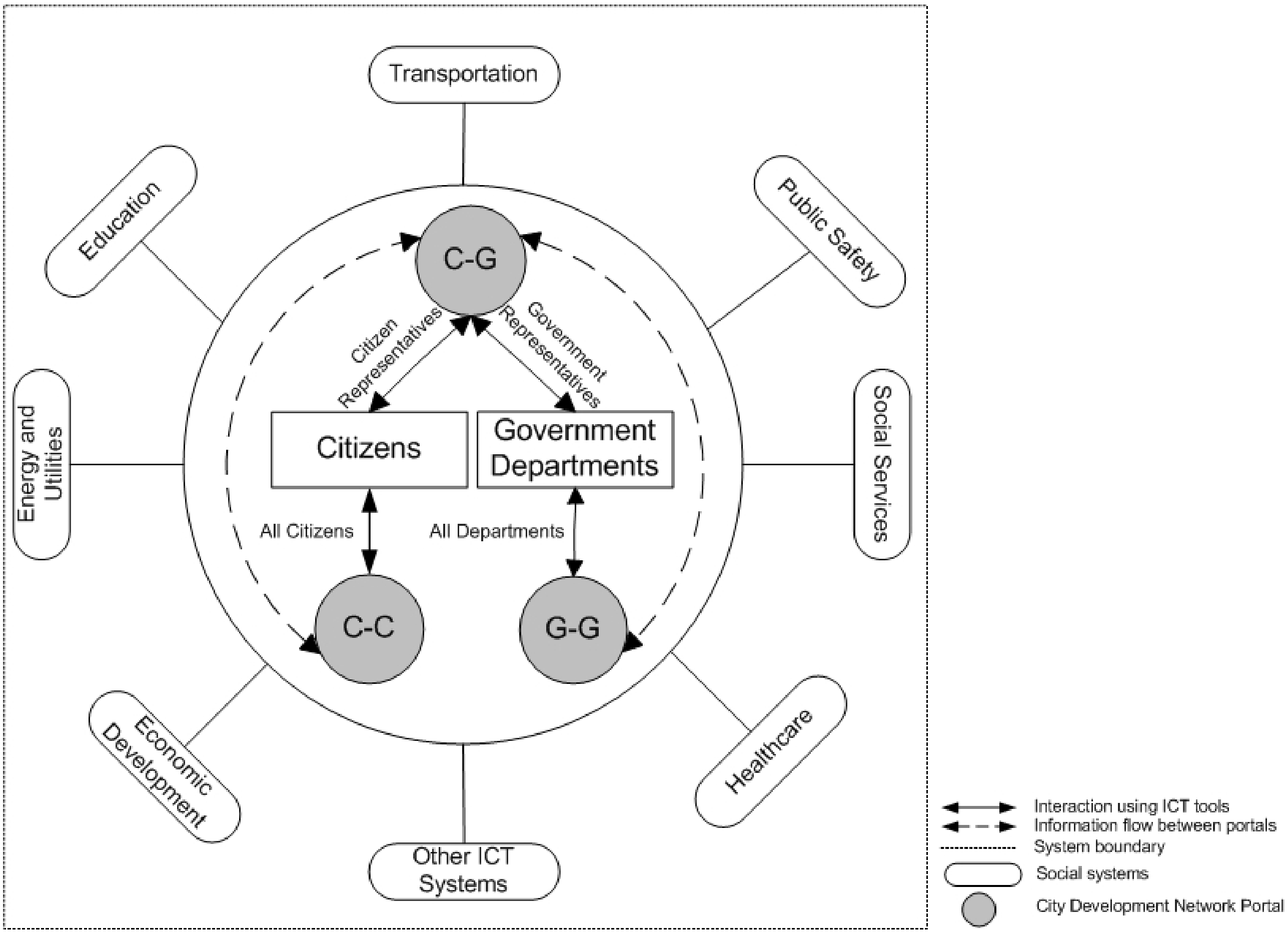


Figure 4. Idealized Smart City Interaction Model

(Source: Smarter City- A System to Systems)[29]

A different view of Smart City is presented in the paper "*Conceptualizing Smart City with Dimensions of Technology, People, and Institutions*"[30]. A set of the common multidimensional components underlying the Smart City concept and the core factors for a successful Smart City initiative is identified by exploring current working definitions of Smart City and a diversity of various conceptual relatives like Smart City, see Figure 5.

[29] *http://www.diva-portal.org/smash/get/diva2:831525/FULLTEXT01.pdf*

[30] https://inta-aivn.org/images/cc/Urbanism/background%20documents/dgo_2011_smartcity.pdf

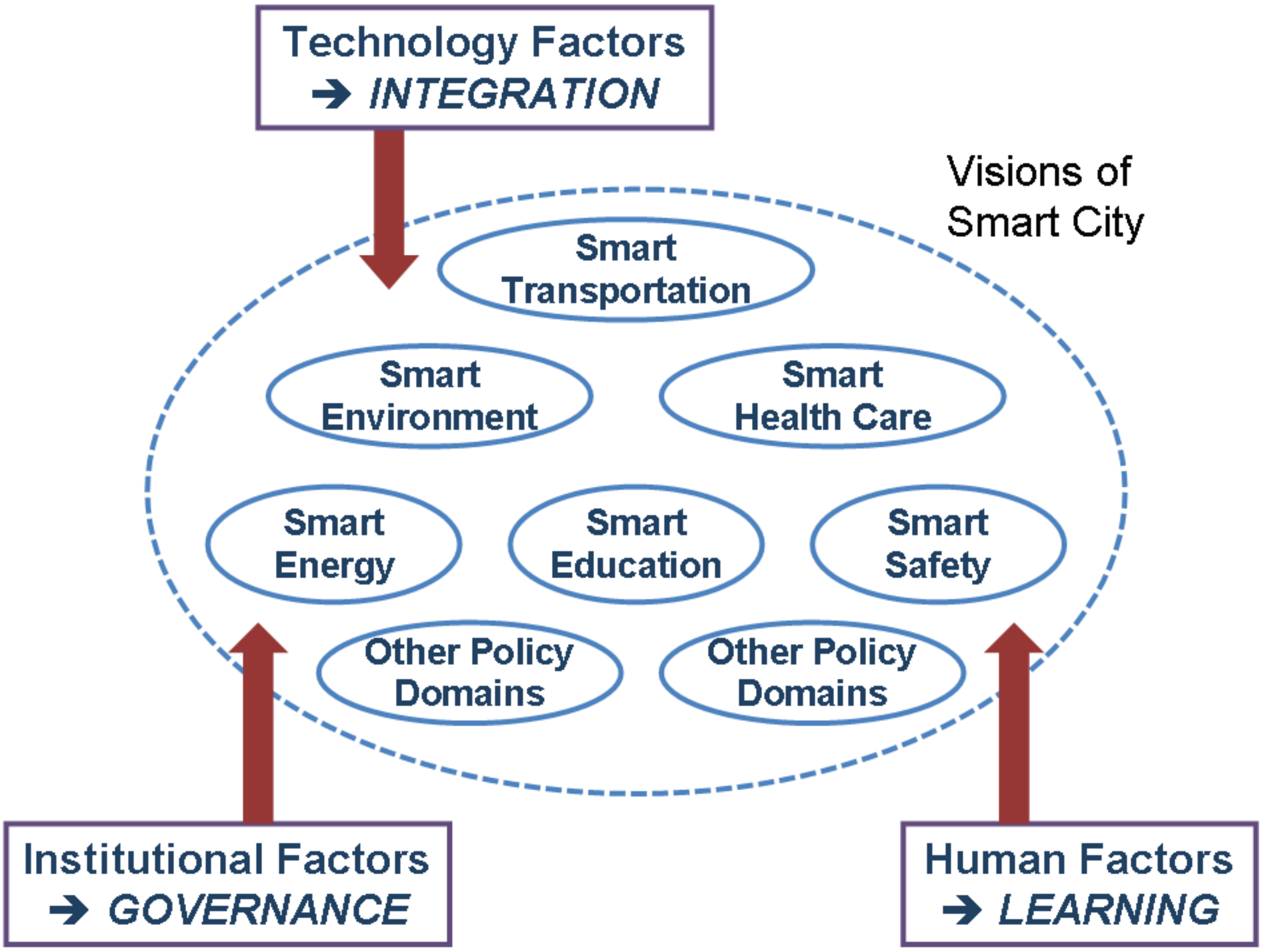


Figure 5. Conceptualization of Smart City

(Source: Conceptualizing Smart City with Dimensions of Technology, People, and Institutions)

To date, systems in Smart Cities have been often developed and deployed in significant fragmentation and isolation, each one responsible for tackling specific areas, concerns, and problems in the city. This might be explained by the fact that these systems are often complex enough in their own right, even before starting the exploration on how they can interact with each other in the daily life of a city. As a result, some implementations of the Smart City concept in urban agglomerations around the world have been done in a bottom-up approach. In this sense, cities would become smarter through decentralized initiatives and gradual implementation of successive projects, each one focusing on a specific objective. Although these applications and systems may be relatively mature in some specific fields, it is easy to observe that collaboration and coordination among them are missing. This type of situation may lead to an unmanageable and unsustainable sea of systems, thus preventing solutions of becoming more efficient, scalable, and suitable to support new generations of systems and services that are not envisaged yet (*Challenges to the Development of Smart City Systems: A System-of-Systems View*)[31]. These are some important issues begging attention, see Figure 6 and Figure 7.

[31] http://www.dimap.ufrn.br/~everton/publications/2017-SBES.pdf

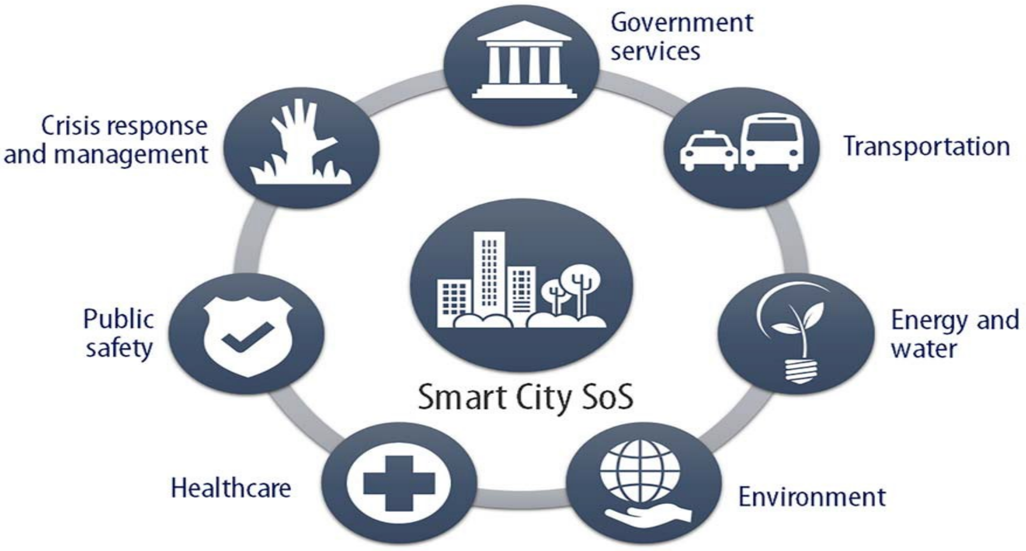


Figure 6. A Smart City SoS can integrate both public and private heterogeneous, independent systems across different domains
(Source: Challenges to the Development of Smart City Systems: A System-of-Systems View)

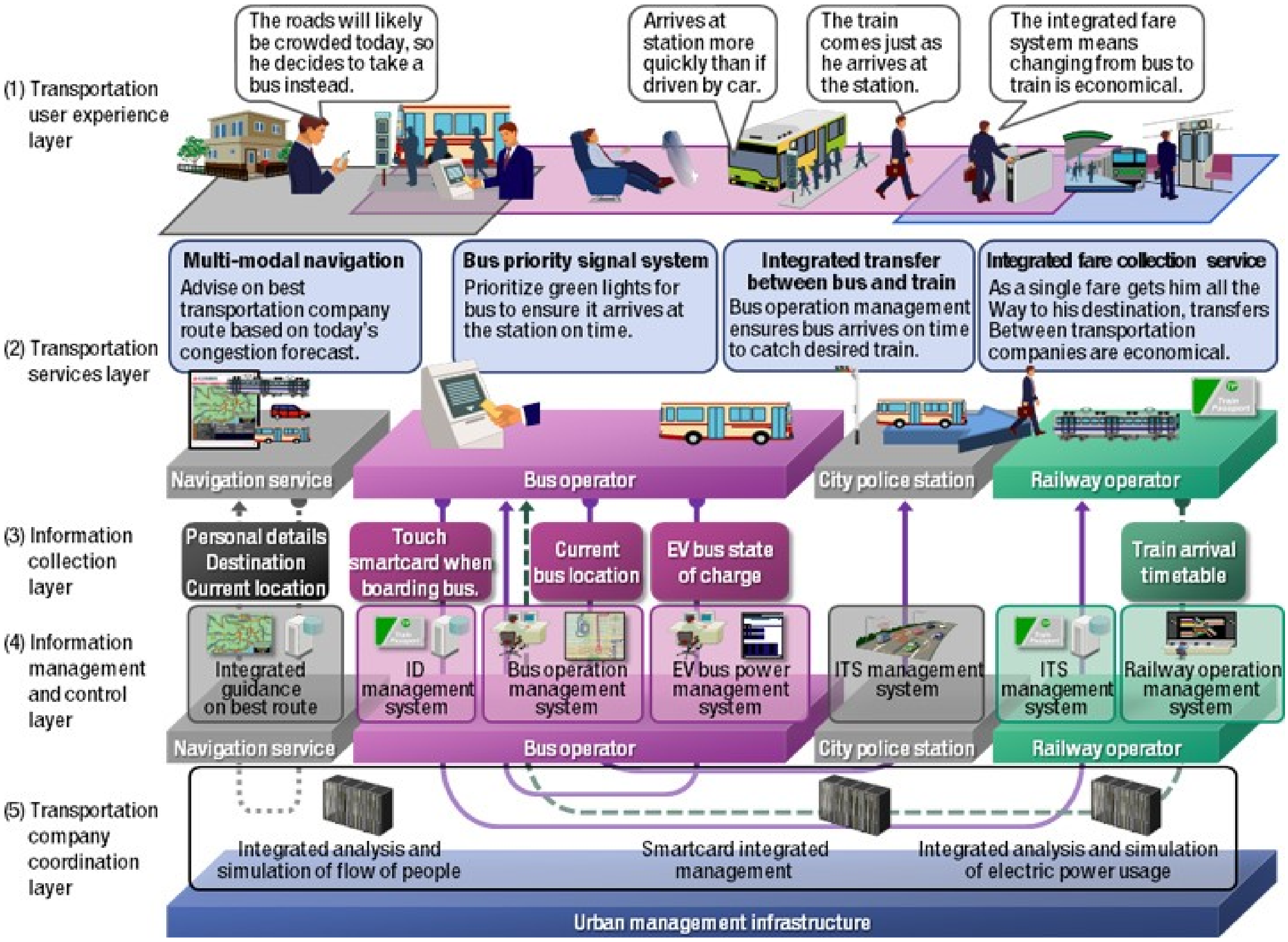

(1) Transportation user experience layer
The roads will likely be crowded today, so he decides to take a bus instead.
Arrives at station more quickly than if driven by car.
The train comes just as he arrives at the station.
The integrated fare system means changing from bus to train is economical.
(2) Transportation services layer
Multi-modal navigation
Advise on best transportation company route based on today's congestion forecast.
Bus priority signal system
Prioritize green lights for bus to ensure it arrives at the station on time.
Integrated transfer between bus and train
Bus operation management ensures bus arrives on time to catch desired train.
Integrated fare collection service
As a single fare gets him all the Way to his destination, transfers Between transportation companies are economical.
Navigation service
Bus operator
City police station
Railway operator
(3) Information collection layer
Personal details
Destination
Current location
Touch smartcard when boarding bus.
Current bus location
EV bus state of charge
Train arrival timetable
(4) Information management and control layer
Integrated guidance on best route
ID management system
Bus operation management system
EV bus power management system
ITS management system
ITS management system
Railway operation management system
Navigation service
Bus operator
City police station
Railway operator
(5) Transportation company coordination layer
Integrated analysis and simulation of flow of people
Smartcard integrated management
Integrated analysis and simulation of electric power usage
Urban management infrastructure

Figure 7. Different layers in a Smart City Transportation System: one of the heterogeneous, independent systems making Figure 7 (*Source WEB*)

A simple view of Figures 6 and 7 should give an idea of the challenges to deal with the System-of-Systems making a Smart City.

Figure 8 gives an idea of the interconnection and permanent information of each point of the city thanks to **Internet of Things** and the need of permanent interpretation of data for the evaluation and evolution of the state of the city making **Big Data Analytics** essential.

For a comprehensive presentation about the different Systems making a Smart City, the reader can refer to "*IEEE 9th International System of Systems Engineering Conference - John Fennell Lead, Smarter Cities IBM ANZ – 2014*"[32]. The presentation gives a bright view of the different Systems making a Smart City a System-of-Systems

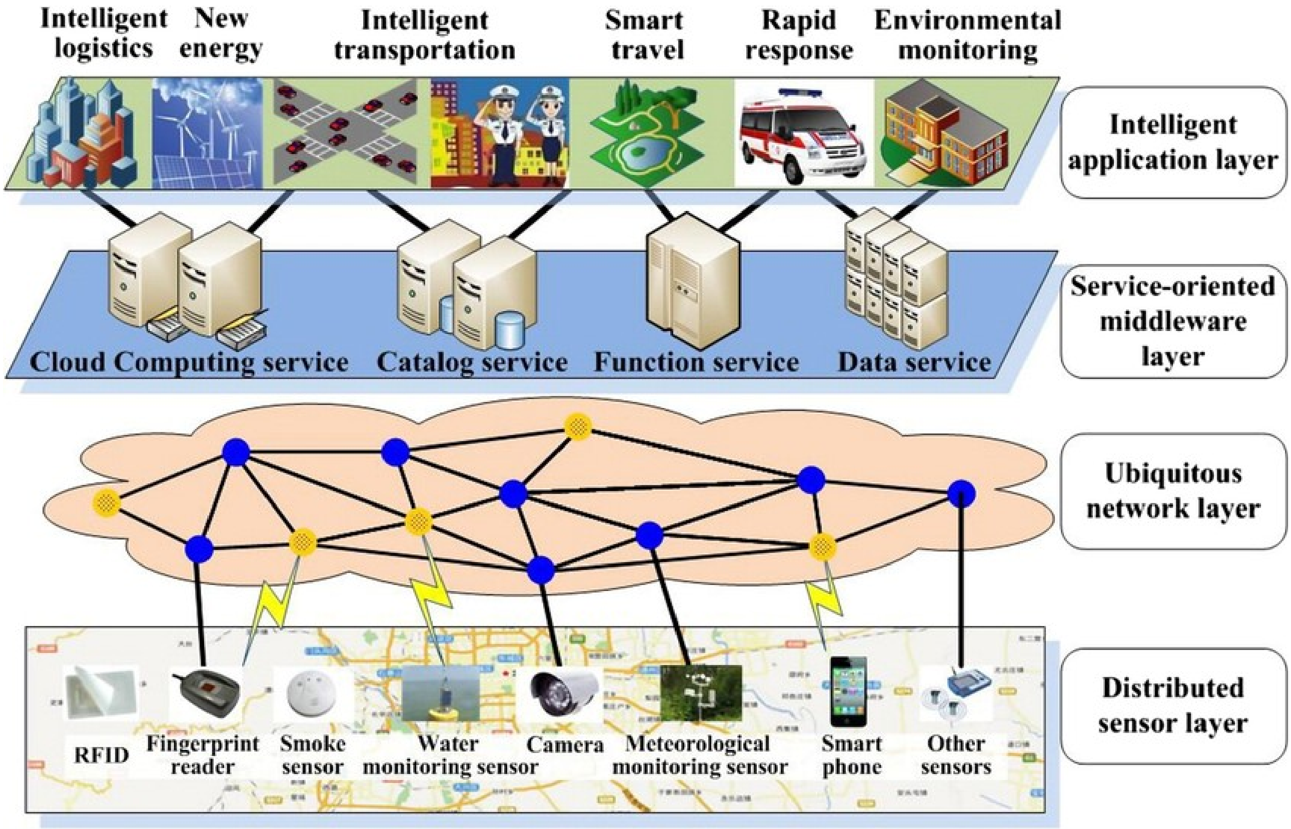


Figure 8. Smart City Layers – How difficult will be to manage a Smart City
(*Source WEB*)

The issue of how to model interdependency among different infrastructures is very challenging. In literature, different techniques are available for modeling lifelines interdependencies, see Eusgeld et al. 2011[33], Figure 9. They essentially fall into two paradigms: the integrated and the coupled approaches. The main distinctions between these two paradigms are related to the scale at which interdependency is modeled and at the stage at which interdependencies are considered in the analysis. The paper *Modeling Electric and Water Distribution Systems Interdependences in Urban Area Risk Analysis*[34] reports about a practical

[32]http://sosengineering.org/2014/wp-content/uploads/2014/05/Smarter-Cities-System-of-Systems-Fennell.pdf
[33] http://webarchiv.ethz.ch/lsa/people/phd/cnan/sos.pdf
[34] https://www.cowm.eu/en/cowm2018-programme.pdf

application of the model, with specific reference to the integrated approach. The specific interdependent elements have been identified and represented in a network model (e.g. the connection between the pumping station and the substation on which it is reliant for power supply) Figure 10. In this way an interface between the two systems has been specified integrating them into one single system, within which each lifeline is just a sub-system. Figure 10 is just a pictorial representation of how modeling interdependency between Electric and Water Infrastructure. As the base of the simulation approach, a hydraulic model for the pilot water distribution network has been preliminarily set up, where the main characteristics of junctions (diameters, length, roughness), nodes (topographic elevation, water demands) and reservoirs (hydraulic heads) have been accounted for. Additionally, the existence of water pumping stations and the urban areas requiring their operation for domestic water supply have been identified.

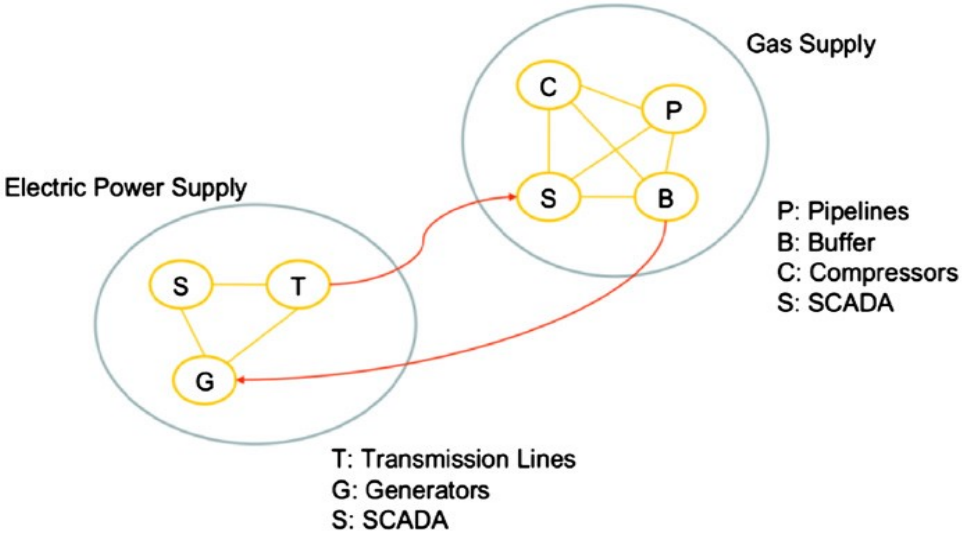


Figure 9. Example of the coupling between the electric power system and the gas transportation network

(Source: "System-of-Systems" approach for interdependent critical infrastructures)[35]

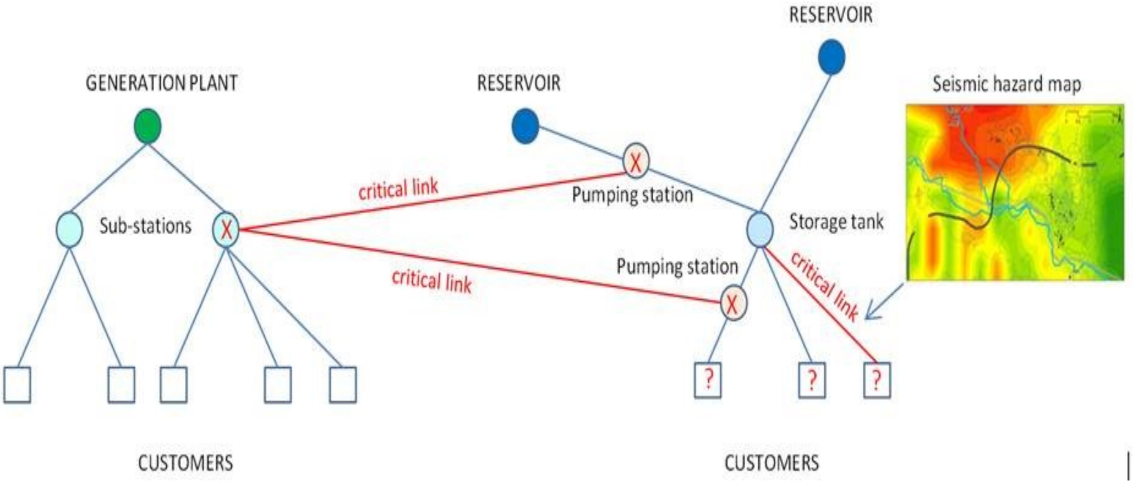


Figure 10. Example of modeling interdependency between electric and water infrastructure

(Source: Modeling Electric and Water Distribution Systems Interdependences in Urban Area Risk Analysis)[36]

[35] http://webarchiv.ethz.ch/lsa/people/phd/cnan/sos.pdf

[36] https://www.cowm.eu/en/cowm2018-programme.pdf

3 How to take advantage of the previous Guidelines produced by AIIC to secure a Community Resilience (*Sandro Bologna*)

Before getting into the understanding of how the previous Resilience Guidelines produced by AIIC can be used, in this chapter we look to what has been proposed by different institutions.

United Nations Office for Disaster Risk Reduction (UNISDR) has the Program "Making Cities Resilient". The Report titled *"From Smart City to Resilient City"*[37] is focused on the topic we are addressing in the present document.

Resilience refers to the adaptability of cities to survive and thrive regardless of shocks and stresses they may face, creating safer, and more sustainable and more Resilient City.

Cities are economic, political, and administrative hubs. They bring together millions of people, businesses, ideas, and foster innovation. Over 50% of the world's population currently lives in cities, and this urbanization will only intensify in the coming decades. It is expected – as already highlighted (at page 9) – that by 2050, around two-thirds of the world's population will live in cities, and cities will become ever larger. Increased urbanization may bring opportunities, but it also brings risks.

Cities will face greater challenges in the upcoming decades due to population growth, climate change, and resource scarcity. They must be able to effectively respond to these challenges, while simultaneously ensuring the well-being of their citizens, economic growth, and sustainability. To be able to meet the challenges of the future, cities have begun focusing on 'smart strategies', merging urban infrastructure and digital technology. These 'Smart Cities' rely on the Internet of Things and data analytics to develop solutions to urban problems, increase the efficiency of infrastructure and services, and improve citizens' quality of life. For instance, sensors can be deployed throughout cities, collecting a variety of data, such as air pollution levels or water levels. Cloud computing allows large quantities of data to be stored, which can then be analyzed with data analytics. Consequently, apps can be used to transmit this information to the general public, also allowing feedback. The collected data and feedback should be considered for future policies and urban designs that improve the quality of life of citizens. While the development of Smart Cities is a step in the right direction, it is necessary to go further than that, and to embrace resilience.

From Smart to Resilient: Harnessing Smart Strategies for Resilient Cities

Resilience is defined by the United Nations (UN) as "the ability to resist, absorb and accommodate to the effects of a hazard, in a timely and efficient manner". Thus, resilient cities are those in which their citizens, businesses, and infrastructures have the capacity to withstand, adapt, and recover in a timely manner from any kind of hazards they face, either planned or unplanned. Resilience strategies do not focus on individual and isolated risks, but rather adopt a comprehensive approach that focuses on all types of risks, from chronic stresses such as unemployment and endemic violence, to acute shocks such as natural disasters and terrorist attacks. They focus on anticipating risks and developing pragmatic and localized solutions that can best manage these risks. In this manner, cities can continue effectively performing their functions in both normal and

[37] https://resiliencepoort.nl/from-smart-cities-to-resilient-cities/

difficult times. The key aspect to the development of resilience cities is the need to involve local society. Citizens should be included not only in decision-making processes, but their quality of life should be at the center of all strategies developed.

The concept of Smart Cities should not be discarded, but it should be embedded within a broader framework of Resilient City. In fact, smart technologies are instrumental in the development of resilience. New and innovative solutions may lie in the technology embedded in Smart Cities. For instance, sensors deployed around cities can be used to maintain databases on vulnerabilities which in turn can be used to develop warning and management systems. Cybersecurity is also another vital aspect underpinning resilience, due to the increasing digitalization of critical infrastructures. Cities that effectively use new technologies, and successfully imbed them into urban planning and design will be more resilient to future challenges. This can also contribute to economic development due to increased productivity and continued economic activity, even in the case of disasters.

Fortunately, there exist recent initiatives aimed at promoting the concept of Resilient City. One of them is the Rockefeller Foundation's 100 Resilient Cities programme[38], which is designed to advance urban resilience by awarding grants to cities that show commitment to building up their resilience. Another one is the "Making Cities Resilient" campaign spearheaded by the United Nations Office for Disaster Risk Reduction (UNISDR)[39]. Initiatives like these should be encouraged, and the shift to resiliency should be embraced. With the future being progressively more urban, cities should take responsibility for ensuring a sustainable, safe, and more livable habitat for their citizens.

How can I measure the "smartness" of Smart Cities?

The question *"How can I measure the 'smartness' of smart cities?"* is not new. Tianzhen Hong, a Staff Scientist and Deputy Head of Building Technology Department of Lawrence Berkeley National Laboratory raised the question more than three years ago[40]. The United States White House announced the Smart Cities Initiative on September 14, 2015[41]. Smart Cities, with various definitions, usually include key elements of smart things: buildings, infrastructure, transportation, energy and water utilities, waste services, governance, healthcare, education, and of course citizens. Can we measure 'smartness' of a Smart City? What metrics and methods do we use? What data do we need? He got many different suggestions, interested readers are invited to go to the link mentioned above.

Cyber risk in Smart Cities

Cities will never be 100 percent "secure," nor can they avoid danger entirely. But they can be resilient in the face of a wide range of stresses and shocks by making the right investments, in both the physical and cyber domains, to prepare for crises, react to restore normalcy, and learn from and adapt to the new status quo. While city leaders tend to have a solid understanding of the physical threats facing them - from earthquakes to terrorism - their understanding of how to mitigate against cyber risk is often spottier. In the McKinsey publication "*Smart city resilience: Digitally empowering cities to survive,*

[38] http://www.100resilientcities.org/

[39] https://www.unisdr.org/we/campaign/cities

[40]https://www.researchgate.net/post/How_can_I_measure_the_smartness_of_smart_cities

[41] https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help

adapt, and thrive"[42] January 2018, it is clearly stated that cyber resilience requires a profound shift in the way cyber threats are dealt with and assets protected - from focusing on breach prevention to understanding that cyber security failures will happen and that quick and efficient recovery capabilities are needed.

Cyber security plays a critical role in mitigating shocks and stresses by protecting the confidentiality, integrity, and availability of data and data-enabled infrastructure. However, security alone is not enough. *Cyber resilience* goes a step further by ensuring that ICT systems continue delivering services in the event of a security breach. For cities, cyber resilience can be understood through their capacity for readiness, response, and reinvention. Efforts to build cyber resilience are critical to both surviving and potentially even thriving in the face of cyber-attacks or physical disasters.

3.1 AIIC Community Resilience Model

AIIC Community Resilience Model is based on the following three assumptions:

- A Community is made of people, technological key infrastructures and organizations supported and regulated by processes. Any Resilience Evaluation activity must take in consideration all these components, including cultural background, in view to be complete and successful. (Figure 11).

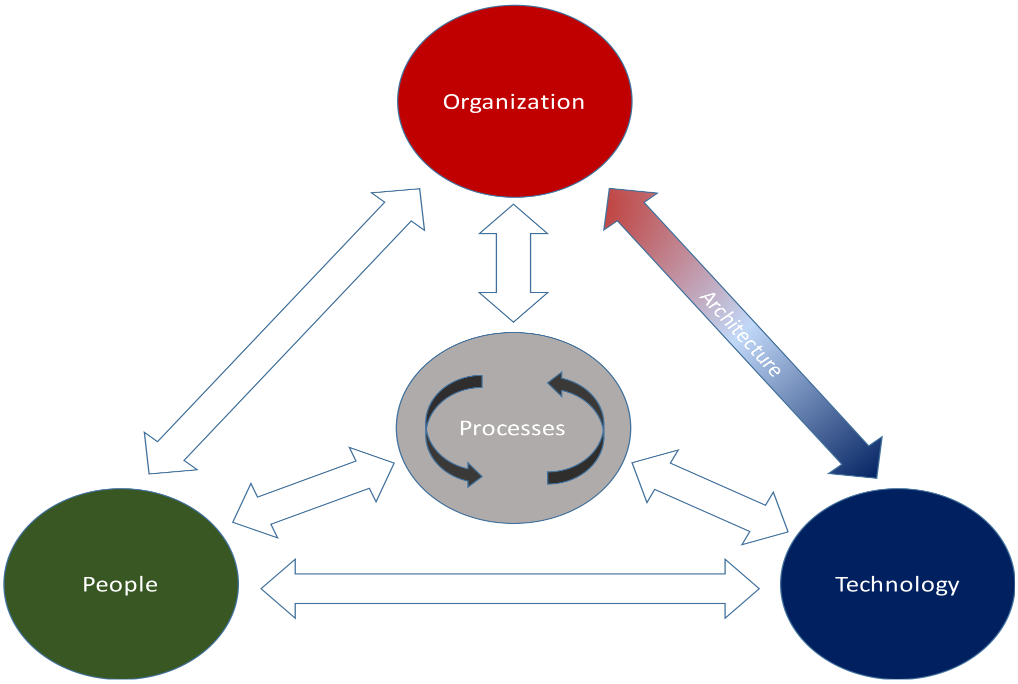


Figure 11. Basic components of a complex systems

(Source: AIIC Guidelines for Community Resilience Evaluation – adapted from USC Marshall School of Business Institute for Critical Information Infrastructure Protection)

- A Community Environment referred in the NIST SP1190 with the term "*built environment*", is made of *Community Key Infrastructures*, *Community Key Functions*, *Community Key Organization's*

[42] https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-city-resilience-digitally-empowering-cities-to-survive-adapt-and-thrive

Capacities. The full meaning of these three Community Elements that contribute to Community Resilience will be cleared in the AIIC Community Resilience Model. Figure 12[43] gives a pictorial representation of the Community Elements that contribute to Community Resilience. The built environment in any community includes its buildings and infrastructure systems. When a hazard event occurs, damage to the built environment can make it difficult for a community's institutions to function and meet members' needs. While some social institutions rely more heavily on the built environment than others, there are linkages between the social and built environments that need to remain strong for a community to thrive. This Guide is based upon the foundation that *the community key functions and the community key organization's capacities drive the requirements of the community key infrastructures*, based on their importance in supporting key functions and key organization's capacities in the community.

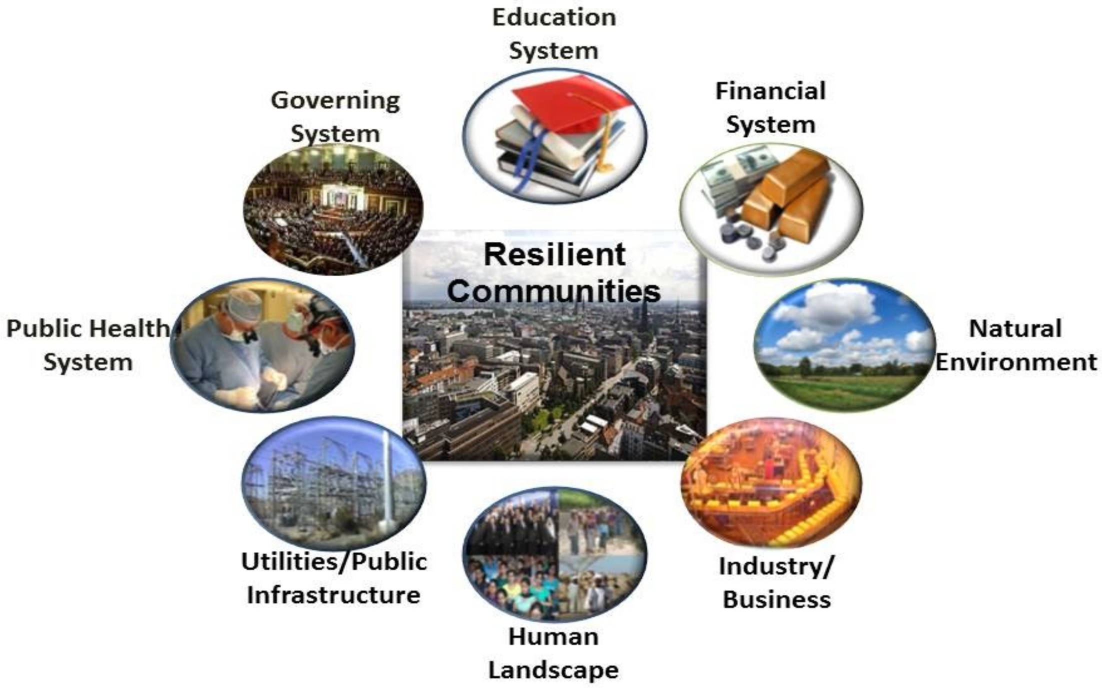


Figure 12. System Elements that contribute to Community Resilience

(source: "The Human Landscape – The Functional Bridge between the Physical, Economic, and Social Elements of Community Resilience" The CIP Report, George mason University, November 2016)

- AIIC Community Resilience Model is built by grouping all the *item to be measured* (Features) with the *indicative measurements* (Resilience Indicators) into four community resilience dimensions: Technical Dimension (Infrastructure & Environment), Organizational Dimension (Leadership & Strategy), Cooperative & Societal Dimension (including Health & Wellbeing), Economic Dimension, and it is represented by the following Figure 13.

[43] http://cip.gmu.edu/2016/11/29/human-landscape-functional-bridge-physical-economic-social-elements-community-resilience/

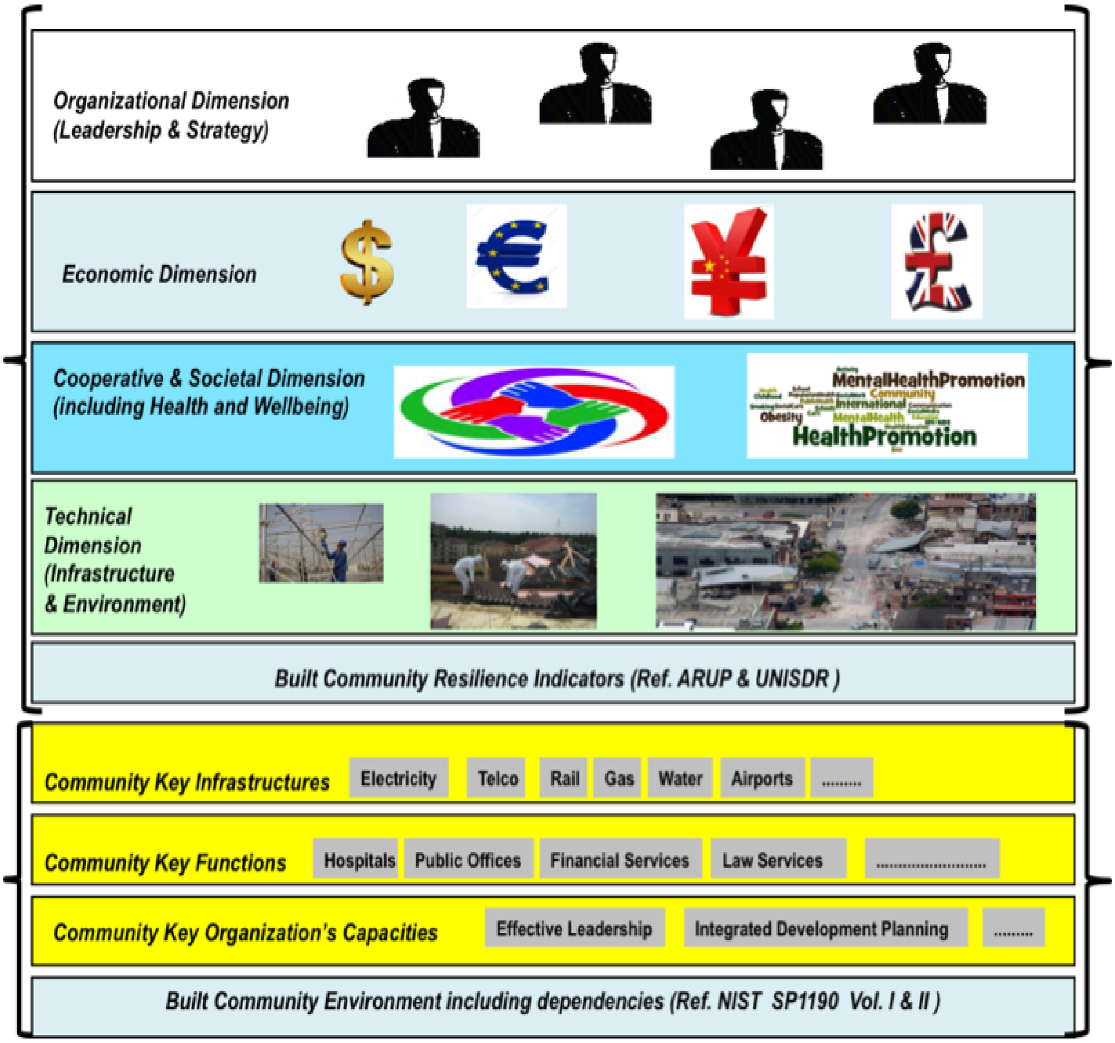


Figure 13. AIIC Community Resilience Model

(Source: AIIC Guidelines for Community Resilience Evaluation)

The AIIC Community Resilience Model starts from the results of the previous Working Group “Guidelines for Critical Infrastructures Resilience Evaluation”, by introducing the concepts of social and economic aspects as well as “dependencies, interdependencies and cascading effects” aimed at identifying dependencies and potential cascading failures among the Infrastructures serving the Community, through the implementation of combinations of societal, organizational and technological resilience concepts. ***Its objective is to allow a territorial Community to understand its standing towards the risk of some specific catastrophic events and its shortcomings, should they exist.***

3.2 The Role of IoT and Big Data in the Smart City Resilience

The implementation of the concept of Smart City Resilience will benefit of the two most disruptive technologies of these last years:

Internet of Things: Interconnection and permanent information of each point of the city.

Big Data: Permanent interpretation of data for the evaluation and evolution of the state of the city.

This is well illustrated in the following Figure 14

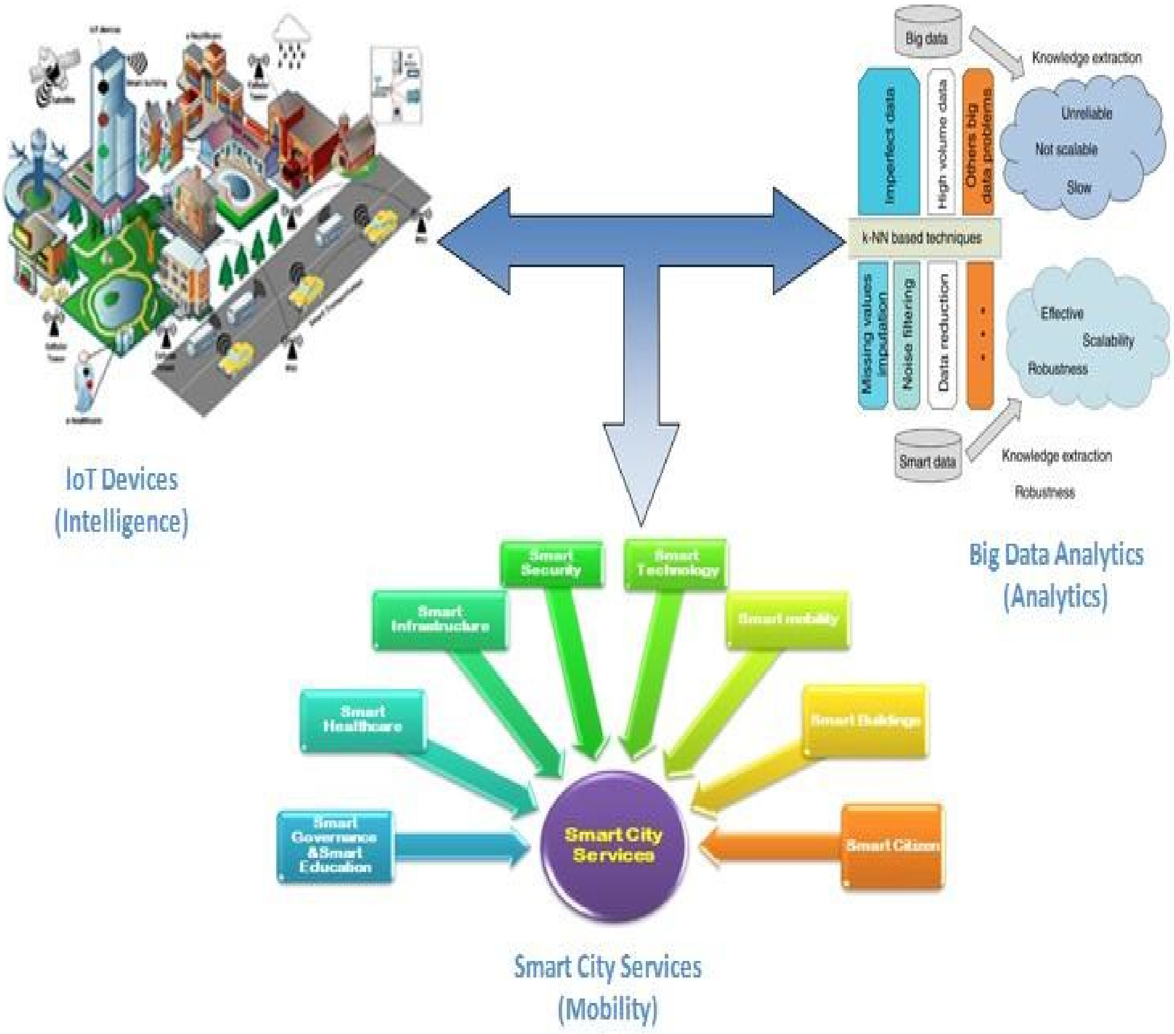


Figure 14. The role of IoT and Big Data Analytics for Smart City Resilience

(Source: Digital Security for Smart Cities in India: Challenges and Opportunities)[44]

AIIC has already investigated this topic in the Report "*Good Practices and Recommendations on the use of Big Data Analytics for Critical Infrastructure Resilience*"[45]. The Report makes a survey of the most appropriate techniques available from the research field and how they can be used with the multiple data Sources from the IT/OT/IoT/IIoT integration, common to critical infrastructures. While surveying different problems and solutions, the Report presents state of the art good practices and recommendations to cope with challenges and issues identified through the surveys.

[44] http://mail.iosrjen.org/Papers/vol9_issue1/Version-3/I0901036371.pdf

[45] http://www.infrastrutturecritiche.it/ new / media-files /2018/04/AIIC_BigDataCIPR_FINALE.pdf

This topic is well covered in Proceedings of the Conference Measuring the Resilience of Cities: The Role of Big Data, 25 October 2013, Edited by Jennifer Cole Conference Report, May 2014[46]

3.3 100 RC - The City Resilience Framework[47]

The Resilient Cities Movement has been boosted in 2014 when the Rockefeller Foundation invested $100 million in the 100 Resilient Cities Challenges[48]. Partly because its institutionalization, the policies of the cities partnering in the 100 Resilient Cities Challenge have more in common than those of the self-appointed Smart Cities. The so-called City Resilience Framework, see Figure 15, plays a key role in each of the participating city's strategy.

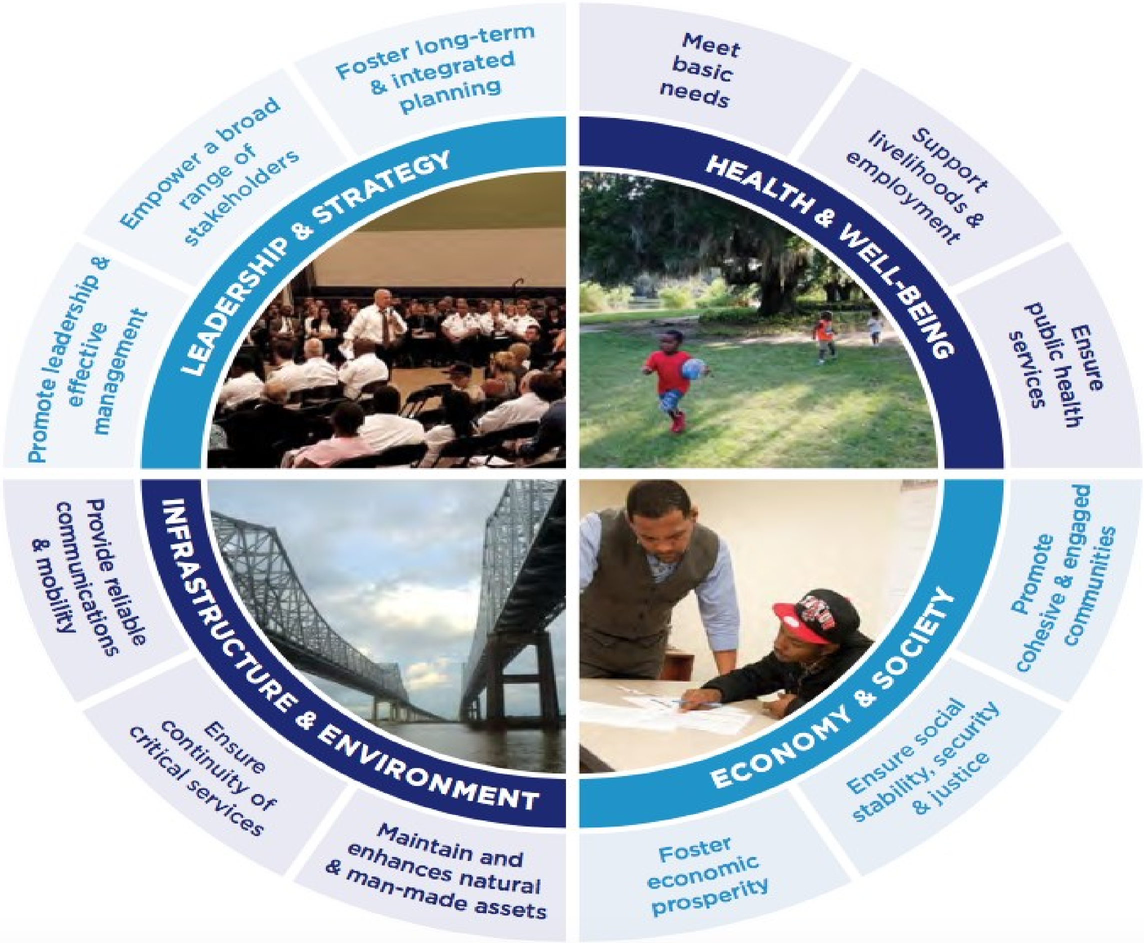

Foster long-term & integrated planning
Meet basic needs
Empower a broad range of stakeholders
LEADERSHIP & STRATEGY
HEALTH & WELL-BEING
Support livelihoods & employment
Promote leadership & effective management
Ensure public health services
Provide reliable communications & mobility
INFRASTRUCTURE & ENVIRONMENT
ECONOMY & SOCIETY
Promote cohesive & engaged communities
Ensure continuity of critical services
Ensure social stability, security & justice
Maintain and enhances natural & man-made assets
Foster economic prosperity

Figure 15. City Resilience Framework developed by ARUP with support from the Rockefeller Foundation

(Source: ARUP City Resilience Framework)

The city Resilience framework

Based upon the framework, an index has been developed. Cities can calculate an indicator of their resilience with respect to the topics mentioned above and subsequently develop a strategy to improve weak points. The result of the analysis made in Rotterdam is indicated below. At this time 30 cities have published strategy reports to increase their resilience in the next decade. Among them are Rotterdam and Athens, a city that came with a brilliantly elaborated action. The report, "*Cities*

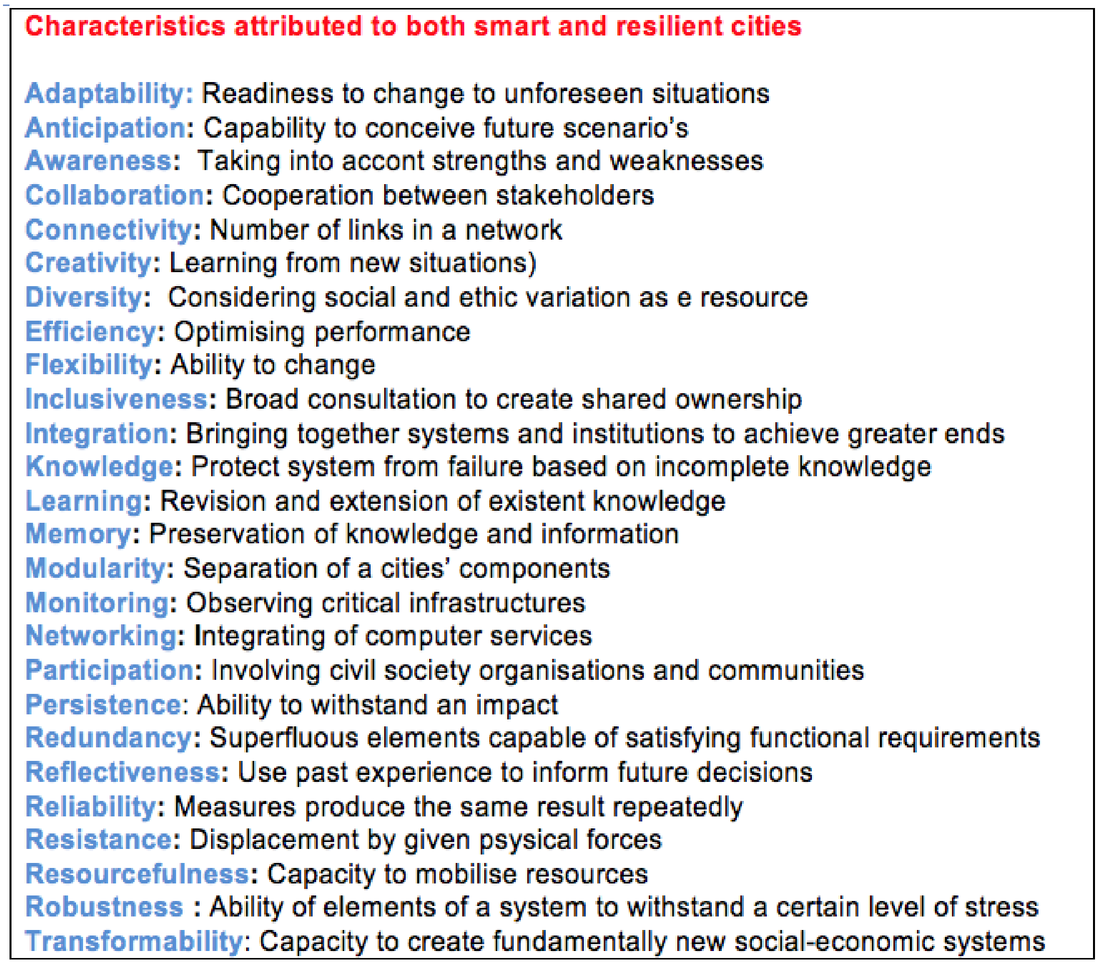
[46] https://rusi.org/sites/default/files/201405_op_resilient_cities.pdf

[47] https://assets.rockefellerfoundation.org/app/uploads/20160105134829/100RC-City-Resilience-Framework.pdf

[48] http://www.100resilientcities.org/

taking Action"[49], written on occasion of the World Summit in July 2017, offers an anthology of what has been reached during the recent past within a selection of the 100 participating cities.

An analysis of definitions of Smart and Resilient City and of characteristics attributed to each of these concepts is revealing a very broad overlap as is demonstrated in the box below.



Characteristics attributed to both smart and resilient cities

Adaptability: Readiness to change to unforeseen situations
Anticipation: Capability to conceive future scenario's
Awareness: Taking into accont strengths and weaknesses
Collaboration: Cooperation between stakeholders
Connectivity: Number of links in a network
Creativity: Learning from new situations)
Diversity: Considering social and ethic variation as e resource
Efficiency: Optimising performance
Flexibility: Ability to change
Inclusiveness: Broad consultation to create shared ownership
Integration: Bringing together systems and institutions to achieve greater ends
Knowledge: Protect system from failure based on incomplete knowledge
Learning: Revision and extension of existent knowledge
Memory: Preservation of knowledge and information
Modularity: Separation of a cities' components
Monitoring: Observing critical infrastructures
Networking: Integrating of computer services
Participation: Involving civil society organisations and communities
Persistence: Ability to withstand an impact
Redundancy: Superfluous elements capable of satisfying functional requirements
Reflectiveness: Use past experience to inform future decisions
Reliability: Measures produce the same result repeatedly
Resistance: Displacement by given psysical forces
Resourcefulness: Capacity to mobilise resources
Robustness : Ability of elements of a system to withstand a certain level of stress
Transformability: Capacity to create fundamentally new social-economic systems

(Source: Herman van den Bosch , JaxStrong http://smartcityhub.com/collaborative-city/smart-cities-resilient-cities-make-difference/

Therefore, some publications consider resilience as a characteristic of Smart Cities. Some observers believe that resilience will replace smart. We are not in favor of the assimilation of one of these terms by the other. Both concepts have their own roots and are on their way to become meaningful for citizens. Therefore, they better can be treated as comparable, as is understood well by one of the platforms. Otherwise, the City Resilience Framework is an extremely useful policy making tool for Smart Cities too because of its high level of elaboration.

Considering the convergence of definitions, both Smart and Resilient Cities are building capabilities to deal with and prevent chronic stress and acute shocks, deploying a broad range of technologies. They enable individuals, communities, institutions and businesses to participate in the definition and execution of policies. They invest in the growth of human and social capital by education, meaningful work, communing, and sharing, and including all of its citizens to live in a decent way.

[49] http://100resilientcities.org/wp-content/uploads/2017/07/WEB_170720_Summit-report_100rc-1.pdf

4. How to take advantage of real-time urban data by exploiting IoT, Big Data Analytics and AI *(Luisa Franchina, Priscilla Inzerilli*)

4.1 Artificial Intelligence (AI) deployment in Smart Cities: challenges and perspectives

In their latest *Smart Cities Spending Guide*[50], IDC estimated that over $81 billion will be spent on Smart City initiatives in 2018 and expect this to grow to $158 billion by 2022. Currently, the Internet of Things (IoT) and Artificial Intelligence (AI) are among emerging key enabler for the new technology-based environment like Smart Cities and they are in the centre of attention among researchers and stakeholders. As the Contexter software company CEO Gabe Batstone said, by incorporating AI into Smart City developments, it is possible to transform the data collected by IoT systems into actionable and intelligent insights.

AI largest current applications in Smart City project globally are prevalent in areas that represent almost 25% of total Smart City spending, like visual surveillance systems, public transit and smart outdoor lighting.

Regarding to some of these applications, like facial recognition applied to public safety, there are some primary challenge to be faced, mainly about privacy and algorithmic bias. Among the 50 billion devices connected by 2020, there will be a billion surveillance cameras, which will send data to artificial intelligence platforms, that would quickly learn our social biases, like racial prejudices, embedding them in the predictive analysis, for example to predict future criminal actions[51].

The successful deployments of the AI-IoT union in Smart Cities environment must consider ethics, privacy, security and legality issues, but also ownership & responsibility ones: which Companies are providing the physical sensors and the computing software? Which Company performs the centralised data management and hosting? Who makes the final decision based on the analytics of the collected data? And if the collected data are personal or sensitive data, are all these activities compliant with GDPR or similar international legislation?[52]

Among all these challenges, it is unquestionable that AI could be used not only for a security purpose, but it can play an important role in many applications within a Smart City environment, like processing traffic data and adjusting the way traffic lights are metered to avoid traffic congestion. The deployment of AI in the Smart City framework could also help improving the capability of autonomous vehicles and other new forms of mobility, like ride sharing (especially ride sharing) and on-demand vehicle hire, that results in a more sustainable form of mobility that would reduce congestion, the likelihood of a road incident and waste of time in searching for a parking space.

[50] *AI in Smart Cities*, Neuromation, 27/11/2018, https://medium.com/neuromation-io-blog/ai-in-smart-cities-dfe2fa7d2829

[51] *How cities are getting smart using artificial intelligence* (Tom Vander Ark), 26/06/2018 https://www.forbes.com/sites/tomvanderark/2018/06/26/how-cities-are-getting-smart-using-artificial-intelligence/

[52] *Urban IoT and AI: How Can Cities Successfully Leverage This Synergy?* (Joseph Bailey and Yalena Coleman), 04/05/2018, https://aibusiness.com/future-cities-iot-aio/

Camera-based AI technology could also aid, for example in the case of an incident or the collapsing of a pedestrian in the street.

There is still much to do on this subject and data collection and process alone is not enough. As the San Francisco-headquartered AI platform "Figure Eight" Chief Marketing Officer Randi Barshack explained, "*AI can do in milliseconds what it might take years for a human to process, but you need to have those data points, and you need to have the theory. AI is not at the point where you can just say: 'make the traffic patterns better'*."[53]

4.2 Multi-level IoT architecture models for a more resilient Smart City

Although there is no standard model for IoT architecture, particularly with respect to network architecture, there are recently published studies in which propose some new IoT model are discussed in their applicability to Smart Cities' resilience. In a context of a (smart) city development, we have to consider the necessity to manage and process thousands and thousands of data generated by various Sources (as shown in Figure 16) through IoT devices interconnecting and communicating with each other in the most efficient way.

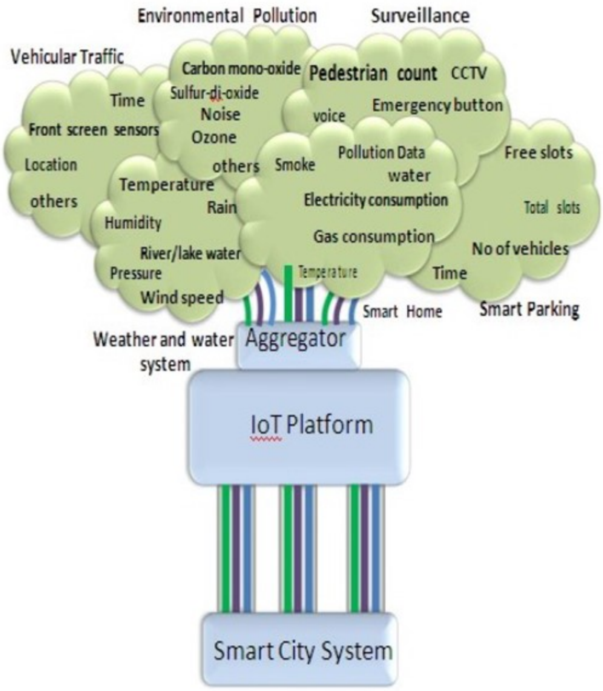


Figure 16. Sensors deployment.
(Source: Development of SMART CITY Using IOT and BIG Data)

One of the simplest models for the IoT is a three-tiered model introduced by IEEE P241 (Institute of Electrical and Electronics Engineers), that works to define a standard of the IoT framework, includes sensing objects in the first level, the entire communication network in the middle level, and application layers at the top level.

[53] *Artificial intelligence in smart cities – what's the link?*, Automotive world, 25/07/2108, https://www.automotiveworld.com/articles/artificial-intelligence-in-smart-cities-whats-the-link/

Another model is the one proposed by ITU Y.2060, which focuses on "physical" and "virtual" objects, and the communication capability, without further deepen the details about the communication network structure, as shown in Figure 17.
Both these models do not provide the details needed for resilience analysis of the smart system.

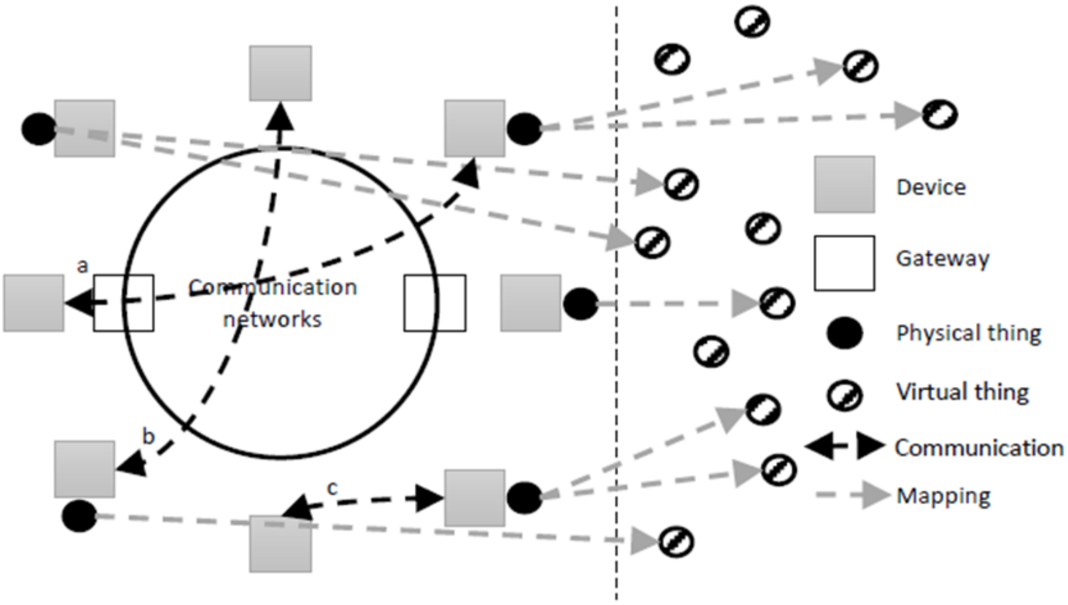


Figure 17. ITU overview of the IoT.
(Source: Multilevel IoT Model for Smart Cities Resilience)

Introducing their *Multilevel IoT Model for Smart Cities Resilience*[54], Modarresi and Sterbenz (University of Kansas) refer to the IoT model proposed by Cisco, in which seven level are considered:

1. physical end devices, including sensors and edge nodes (first and lowest level)
2. network devices and communication systems (second level or connectivity level)
3. local packet-based processing on behalf of simple devices with less processing power, data filtering, and transformation capabilities (third level or computing level)
4. data accumulation for longer storage (fourth level)
5. data integration and aggregation (fifth level or data abstraction level)
6. business analysis and reporting (sixth level or application level)
7. collaboration & processes (seventh and top level)

These seven levels and their related functions can be expressed in the following scheme:

[54] *Multilevel IoT Model for Smart Cities Resilience* (Amir Modarresi James P.G. Sterbenz, University of Kansas) - Conference Paper - June 2017, https://www.researchgate.net/publication/318374739

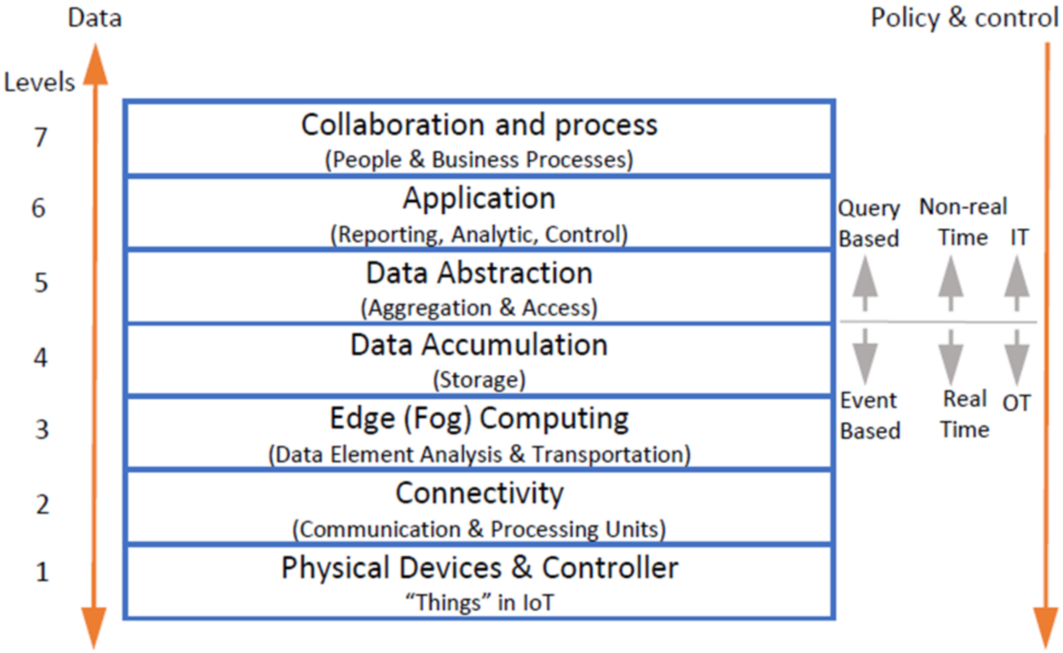


Figure 18. Cisco IoT reference model.
(Source: Multilevel IoT Model for Smart Cities Resilience)

Although it seems to offer greater complexity compared to the two previous models, also in this case the levels of abstraction, according to the authors, "*are not aligned with the physical and logical network structure, nor do they capture the necessary details of diverse network architectures and protocols in use*".

Exposing their Multilevel model, the authors focus on the resilience factor, defining a "ResiliNets" strategy, which consist in two control loops, as shown in Figure19: an inner loop consisting of structural defenses in the middle, and active defenses as part of the control loop; a detection function, a remediation function, and a recovery function.

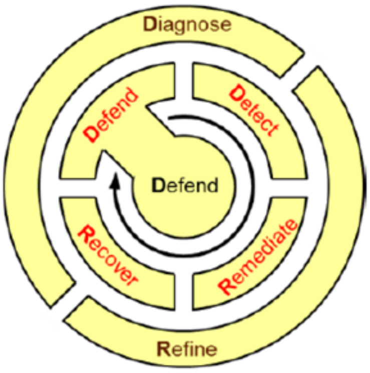


Figure 19. ResiliNets strategy.
(Source: Multilevel IoT Model for Smart Cities Resilience)

In order to design a resilient network, the authors define a set of principles on which the ResiliNets strategy is based; "*including redundancy for fault-tolerance, heterogeneity and diversity for survivability, and self-organizing and adaptable to remediate challenges*":

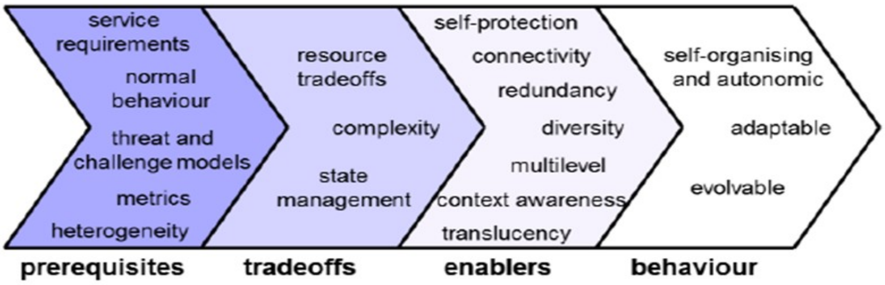


Figure 20. ResiliNets principles.
(Source: Multilevel IoT Model for Smart Cities Resilience)

In the Multi-Level IoT model described by the authors, the architecture can be displayed as shown in Figure 21:

- A lowest layer consisting of device and wire and wireless physical links;
- A logical network path and routing level, in which a migration from IPv4 (that cannot easily scale to the massive increase in addressing) to IPv6 has been proposed to enable the IoT, considering that, according to the authors, ideally all IoT devices in the edge networks should support IP, "*since the dominant networking protocol stack is TCP/UDP/IP with the Internet hourglass waist of IP*".
- A final top layer, including "*the end-to-end flows that things, users, and applications use to communicate on the paths created by the network layer below*".

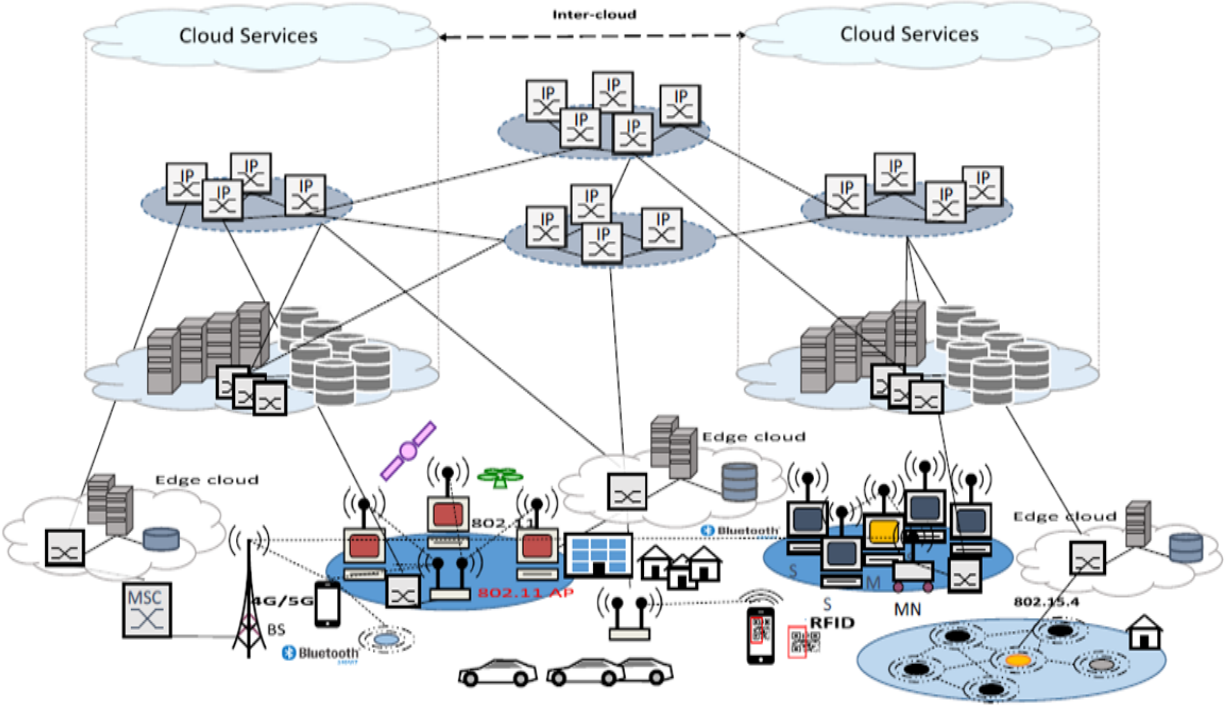


Figure 21. Multilevel IoT model.
(Source: Multilevel IoT Model for Smart Cities Resilience)

The authors of another study, *Development of SMART CITY Using IOT and BIG Data*[55], propose a system based on sensors deployment, including smart home sensors, vehicular networking, weather and water sensors, smart parking sensor, and other surveillance objects. The authors propose a four-tier architecture, as shown in Figure 22:

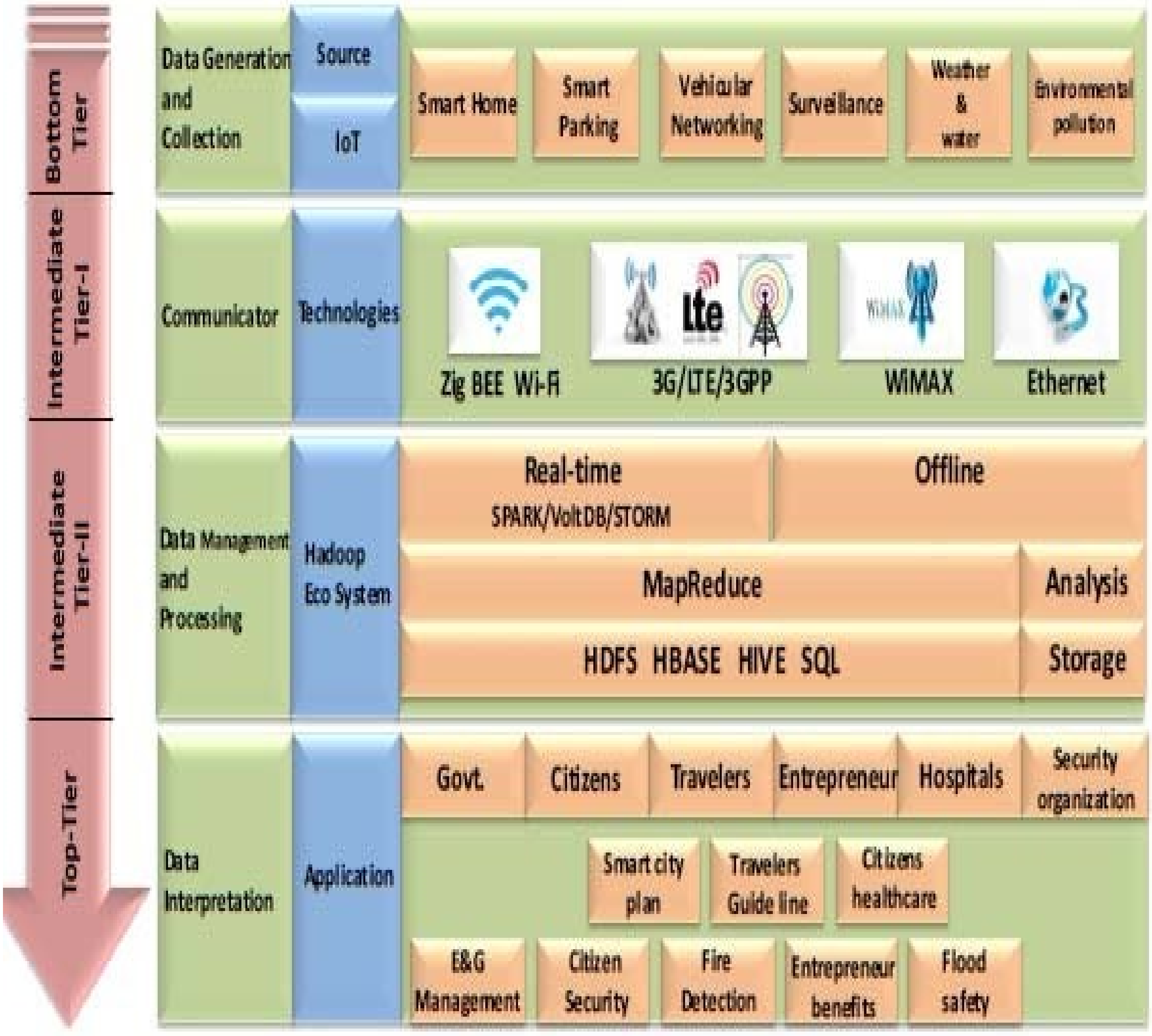


Figure 22. Tier Architecture for IoT Big data analytics for remote Smart City and urban planning.

(Source: Development of SMART CITY Using IOT and BIG Data)

- The Bottom Tier is responsible for IoT Sources, data generations and collections.

- One first Intermediate Tier is responsible for all type of communication between sensors, relays, base stations, the internet, etc., while a second Intermediate Tier is responsible for data management and processing using Hadoop framework.

[55] *Development of SMART CITY Using IOT and BIG Data* (Dr.E.N.Ganesh, ECE, Saveetha Engineering College, and Chennai) - International Journal of Computer Techniques – Volume 4 Issue 1, Jan – Feb 2017, https://www.researchgate.net/publication/314615260

- Finally, the Top tier is responsible for application and usage of the data analysis and results generated.

In the implementation model, shown in Figure 23, the collected data from all smart systems, including smart homes sensor data, smart parking IoT sensor data, weather and pollution sensor data, etc., are filtered and then processed at real-time by using Hadoop ecosystem. All the datasets are replayed to test the real-time efficiency of the system and, through a final process of analysis and interpretation of results, it is possible to define predictive and decision-making processes.

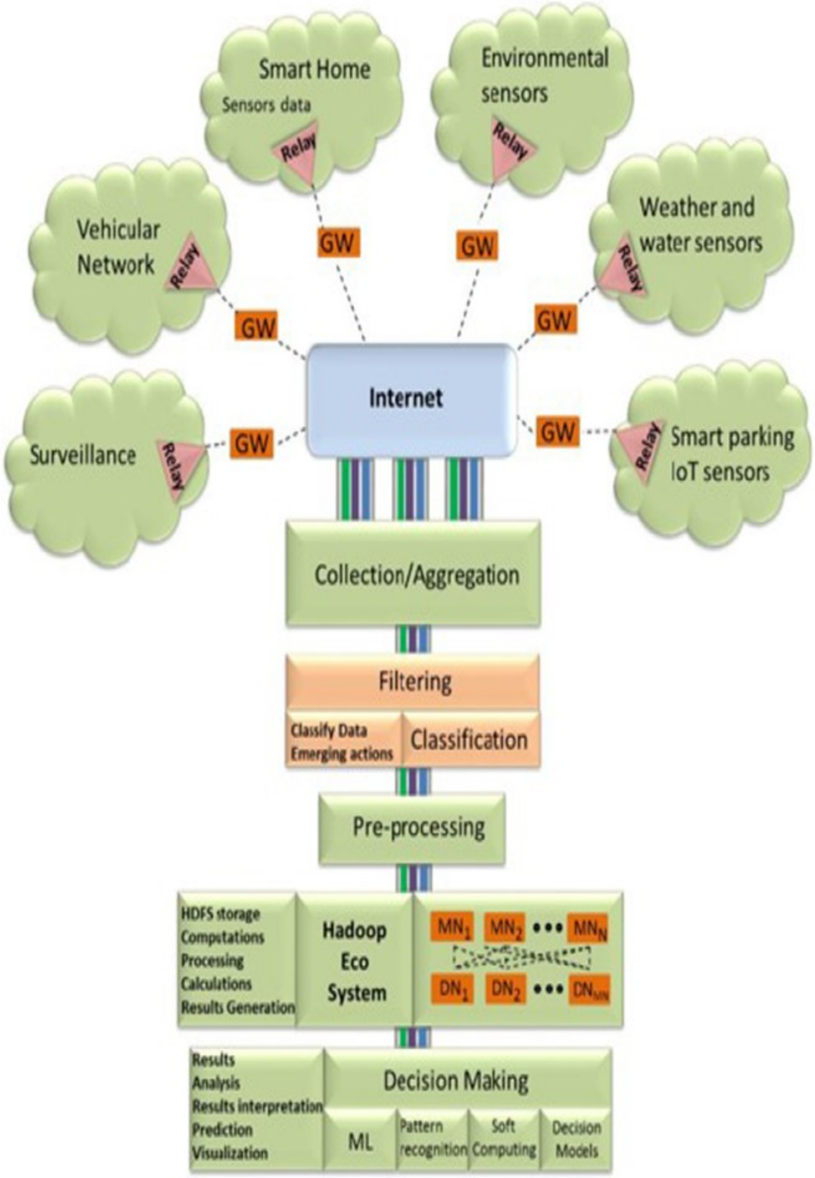


Figure 23. Implementation model.

(Source: Development of SMART CITY Using IOT and BIG Data)

5 How to combine the Smart City and the historic centre: suggestions from a case study. *(Donato Di Ludovico , Donatella Dominici)*

5.1. Introduction

The Italian territory is dotted with about 20,000 historic centres of very diversified size, of which 11,000 are in mountain areas and 1,600 in coastal areas. 19% of these centres are depopulated while 62% are minor historic centres. These are significant numbers that concern practically all the 8,000 Italian municipalities. A study by the ANCSA (National Association of Historic Centre) and CRESME (Centre for Economic, Sociological and Building Market Research) which analysed the dynamics of the 109 historic centres of the Italian provincial capitals, shows that they are faced with a crisis in small-scale retail trade, the entry of new economic players and new tourist uses, the tertiarization of heritage, a major weight of the unoccupied building stock, a rift between those who become the beating heart of the recovery and those who live in abandonment, the absence of adequate investments for the maintenance and management of heritage.

Often these are small settlements where the historical part is predominant, with a strong identity component, with extremely diversified forms and conservation status. In fact, there are ancient settlements, often mountain, abandoned due to geomorphological disruptions, an intervened inaccessibility, unsustainable of healthiness condition, an unacceptable peripherality for contemporary society. There are also ancient settlements of high historic value that, although recovered and restored, are struggling to be dynamic, suffer a continuous decline in population due to the lack of services, with an old age index and a high dependence index and an increase in empty buildings. Finally, there are historic centre, often those of the larger urban centres, which have a population, particularly young people, increasing and therefore positive settlement dynamics, which have an adequate level of services, an adequate level of building heritage in terms of safety, which have all the characters of resilient urban systems.

In the same time the “Smart City” is the new frontier it for the historic centres. The Smart City concept is supported by an organic plan of possible actions to help Italy become “smarter” than it is already today, starting from the assumption that a smarter Country is a forced choice that combines competitivity of the Italian System and citizens wellness. So, we belt in the development of a Digital Smart City, strictly related to the benefits it can bring in terms of improvement of the country and the belt is “how to combine the digital Smart City with the Italian historic centre?”

The experiences on this field, as regards the historic centres, suggest to pursue the resilience strategy, integrating new tools for conservation and building valorisation, such as active conservation, innovative tools of knowledge and urban planning addressed to topics such as new uses, new actors, the tertiarization, the functional housing mix, the relationship between the historical parts and the periphery of the city, the gentrification, but also addressed to the role of new technologies (knowledge / design integration) to improve the quality of life, the safety and resilience of the historic centre.

An example in which the prodromes of a such approach are evident comes from the post-earthquake reconstruction of the City of L'Aquila and its historic centre, which is suffering the lack of urban planning and urban design. Faced with this problem, the acceleration of urban transformation resulting from reconstruction is producing widespread experiments in advanced technologies in the renewal of infrastructures, services and mobility, supported by significant public and private investments. These are innovations that often concern the historic centre and sometimes the periphery, ongoing experiences that invest first the field of knowledge that in L'Aquila assumes a role of absolute importance in relation to the innovation of survey techniques and of investigation that concerned most of the buildings inside the medieval walls. Then there are interventions that can be included in the "Smart" context, such as the Smart Ring, the technological tunnel, the structural monitoring through the sensors, the augmented reality, the 5G for which L'Aquila is one of the cities of experimentation and which will make it possible to significantly improve the capabilities of mobile broadband and to address the new needs of the online society. All these innovations, which concern the context of resilience, are taking place on an urban settlement form deconstructed by the earthquake and reconstruction. The danger is that these technological innovations, particularly aimed at increasing safety and the level of urban services, in the absence of a comprehensive and articulated urban regeneration project that connects them with the reorganization of urban components and their negative dynamics, are likely to have a reduced effectiveness. Among other things, these are innovations disconnected from a coordinated program.

The scientific research of the University of L'Aquila and its Laboratories is addressing these issues, connected to historic contexts, bringing them back within the framework of innovative tools of urban knowledge and urban design oriented towards resilience, a study in which the L'Aquila case is considered paradigmatic.

5.2. Resilient historic center

The concept of resilience is very broad and has been analysed by many authors in many scientific fields. It covers social sciences, environmental sciences, engineering, land-use and spatial planning, urban design, business management, etc[56]. We are interested in the 'urban' meaning of this concept, namely, to define what is a 'Resilient city'[57] and consequently what is a 'Resilient historic centre', a very fragile part of the city. The OECD affirms that "Resilient cities are cities that have the ability to absorb, recover and prepare for future shocks (economic, environmental, social & institutional). Resilient cities promote sustainable development, well-being and inclusive growth"[58]. Therefore, the Resilient city involves several issues, including: Minimal human vulnerability, Social security, Reduced physical exposure, Continuity of critical services, Reliable communications and mobility, Integrated development planning, and more[59].

The experience that we report in this chapter, which concerns a city in reconstruction after a disaster, refers to a shock derived from a natural disaster. In this particular case, Wamsler et alii states that "a disaster Resilient City can be understood as a city that has managed to successfully support measures to strengthen individuals, communities and institutions to: (a) Reduce or avoid current and future hazards; (b) reduce current and future susceptibility to withstand hazards; (c) establish functioning mechanisms and structures for disaster response; and (d) establish functioning mechanisms and structures for disaster recovery"[60].

[56] Fleming J., Ledogar R.J., *Resilience, an Evolving Concept: A Review of Literature Relevant to Aboriginal Research*, Pimatisiwin, No. 6(2), 2018, 7-23.; Bhamra R., Dania S., Burnard K., *Resilience: the concept, a literature review and future directions*, International Journal of Production Research, Vol. 49, No. 18, 2011, 5375-5393, doi: http://dx.doi.org/10.1080/00207543.2011.563826; Haimes Y.Y., *On the Definition of Resilience in Systems*, Risk Analysis, Vol. 29, No. 4, 2009, doi: http://dx.doi.org/10.1111/j.1539-6924.2009.01216.x

[57] Borsekova K., Nijkamp P., Guevara P., *Urban resilience patterns after an external shock: An exploratory study*, International Journal of Disaster Risk Reduction, vol. 31, 2018, 381-392, doi: https://doi.org/10.1016/j.ijdrr.2018.05.012; Zhang X., Lid H., *Urban resilience and urban sustainability: What we know and what do not know?*, Cities, Vol. 72, 2018, 141-148, doi: http://dx.doi.org/10.1016/j.cities.2017.08.009; Meerow S., Newell J.P., Stults M., *Defining urban resilience: A review*, Landscape and Urban Planning, Vol. 147, 2016, 38-49, doi: http://dx.doi.org/10.1016/j.landurbplan.2015.11.011; Patel R., Nosal L., *Defining the Resilient City*, United Nations University Centre for Policy Research, Working Paper 6, 2016, in: https://pdfs.semanticscholar.org/aaec/cdb4b59824958c0442be5af3116003da73fe.pdf, last access: 22.01.2019.

[58] Si veda http://www.oecd.org/cfe/regional-policy/resilient-cities.htm

[59] Patel R., Nosal L., *Defining the Resilient City*, United Nations University Centre for Policy Research, Working Paper 6, 2016, in: https://pdfs.semanticscholar.org/aaec/cdb4b59824958c0442be5af3116003da73fe.pdf, last access: 22.01.2019

[60] Wamsler C., Brink E., Rivera C., *Planning for climate change in urban areas: from theory to practice*, Journal of Cleaner Production, Vol. 50, 2013, 68-81, doi: http://dx.doi.org/10.1016/j.jclepro.2012.12.008.

This definition recalls the theme of technologies and therefore of the ‘smart’ components of urban systems. The next paragraphs will address them in relation to the city of L'Aquila, and to its historic centre under reconstruction for 10 years and in which very rapid changes are taking place following the financing and implementation of projects based on the development of networks and digital services, ICT and other innovative technologies. To date, however, it is not clear what the impact of these changes will be on the historic centre, because there is not an overall Smart City project that coordinates and integrates the strategic development factors with technological advancement, but above all is not still sufficiently developed the issue of conservation of historical-monumental values in relation to the impact of new technologies. Then there is another topic that escapes the government of the city and that concerns the enormous amount of information that the city is taking without real management and without a reflection on their consequence in the transformation process of the city.

5.3. Practices and technologies

We have seen how in our case study the components ‘Smart’ and ‘Resilient’ of the urban transformation of the historic centre recall at least two themes, the knowledge and the technologies with the relative practices. The next sub-sections tackle these topics with the emphasis on new levels of knowledge produced, for example through the geomatic techniques, and on the technologies used in the reconstruction of the historic centre of L'Aquila.

5.3.1 New levels of knowledge for the historic centre

In these last decades, surely, the geomatic techniques have covered a primary role in the heritage and city knowledge and management. The geomatics, combining many techniques and tools of survey, can observe and measure the environment, structures and infrastructures providing certified metric data useful to create a unique database to support the management of a historic centre. In order to define an accurate description of a structure at the time of the survey and consequently to monitor its variations over time[61] new tools have been developed appeared in the last decades including laser scanning, UAV based-imaging, spherical and infrared images, mobile mapping system.

Furthermore, the obtained 3D models, integrated with other information of the structure (structural and seismic analysis, energy systems, etc.) can represent the first informative layer for the innovative BIM systems to analyse the life cycle of the existing structure. The BIM systems are the focus of discussions for their mandatory adoption in public procurement in compliance with European directive and they have been adopted by many European countries.

Geomatic may be considered as a discipline devoted to the knowledge, measurement, monitoring and SMART management of the territory and consequently its structures and infrastructures[62]. Naturally to achieve the mentioned purpose of the discipline, considering the different characteristics of the involved elements, in these years many techniques of survey, instrumentations and measurements analysis have been developed. Table 1 shows how they can be distinguished some important parameters: type of positioning, precision, density (of the measured points) and scale[63].

[61] Dominici D. et alii, *The role of geomatics for civil and environmental monitoring*, Proceedings online 21st Ka and Broadcast Communication conference, Bologna 12-14 October, 2015.

[62] Dominici D. et alii, *Documenting monuments - State of the art geomatic techniques for an accurate and complete documentation of the built heritage*, Coordinates, Vol. IX, Issue 10, 2013.

[63] In geomatics the term small scale refers to a map which covers a relatively large surface of the Earth with the possibility of detecting few details. The term large scale refers to a map with a high level of detail which covers a

Technique		*Type of positioning*	*Precision*	*Density*	*Scale*	*Applications*
Total Station		Local 3D	Millimeter	Single Points	Very large	Monitoring, positioning, mapping
GNSS		Global 3D	Few millimeters	Single Points	Very large to Medium	Monitoring, georeferencing, navigation
Photogrammetry	*Aerial*	Local 3D	Until decimeter	Medium	Large to Medium	Monitoring, DSM, cartography
	UAV	Local 3D	Until few centimeters	High to Really High	Very large to Large	Documentation, Environmental applications, Mapping
	Terrestrial	Local 3D	Until sub-centimeter	High to Really High	Very large	Architectural survey, small objects modelling
Optical Satellite Images		Global 2D	Until few decimeters	Medium	Large to Medium	Change detections, Documentation Mapping
Laser Scanner		Local 3D	Until few millimeters	High to Really High	Very large	Survey, 3D modelling, Documentation
Synthetic Aperture Radar (SAR)		Global 1D (LOS)	Until few millimeters	Low	Large	Monitoring, Change detection
Levelling		Local 1D (Vertical)	Sub-millimeter	Single Points	Very large to Large	Monitoring, control

Table 1. ***Geomatic techniques***

How did the contribution offered by geomatics fit into historic centre? First, it produces documentation, with certified validity, relating to its geometric representation. All the geomatic techniques allows to define the position of points in space (or describing their movements, if a temporal system is also assumed in addition to a spatial referencing system, as in monitoring operations) and describing the outline of surfaces (or their deformations). At the same time, they express how reliable the proposed representations are and are essential in intervention, control, inspection and monitoring phase. The survey of a cultural heritage, for example, has been completely revolutionised. Once the surveyors were equipped with a tape measure and plumb line and the measurements were substantially limited to distances, referred to planes lying in space but that was not simple to put into concrete terms. The revolution in survey introduced by electronic and informatics technologies by laser scanning and by photogrammetry allows to obtain a 3D model georeferenced with deep and metric knowledge.

With the electronic and informatics survey minimal hypotheses are required beforehand, and the interpretative phase can systematically be placed after the measurements stage.
Consequently, increasingly specific technical skills have come to the fore and increasingly high-performance tools have spread and often there is a gap between the geomatic experts who produce the data for the documentation, the survey and preservation and the experts who use these data. There are a lot of research teams as CIPA (international Committee for Documentation of

relatively small portion of the terrestrial surface (Dominici D. et alii, *The role of geomatics for civil and environmental monitoring*, Proceedings online 21st Ka and Broadcast Communication conference, Bologna 12-14 October 2015).

Cultural Heritage) and ICOMOS (International Council on Monuments and Sites) which work to eliminate these difficulties but to a large extent are still open issues[64].

Nowadays, thanks to remote sensing and geomatic techniques giving rise to a tremendous amount of new possibilities that are not possible in the field. In the same time also the geomatic tools in mapping provides good opportunities for the community of the city and historic centre. In fact, the cartography provides a way of presenting information about the physical environment, cultural features, patterns of occupancy, resources and boundaries[65]. The remote sensing, with high resolution satellite images, GNSS, aero and UAV photogrammetry, is expected to offer possibilities for improving incomplete spatial and thematic coverage of current regional and local database.

For example, the handling of photogrammetry high resolution data (ca: 1.5-2.0 cm) allows to obtain different output (Fig.24), from 3D model, to orthophoto and Digital Elevation Model (DEM).

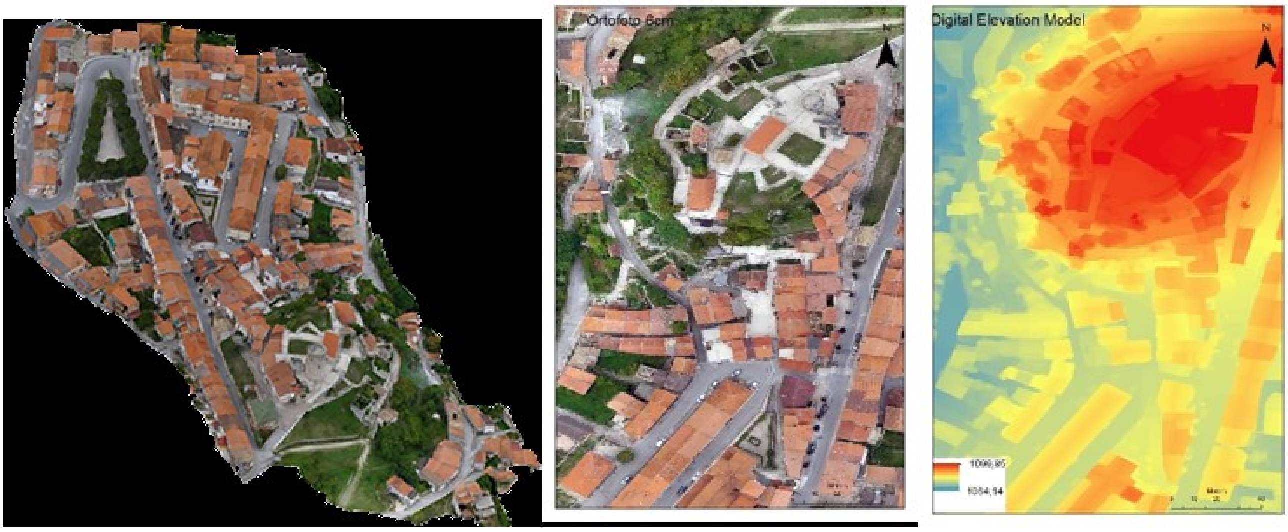


Figure 24. ***a) 3d model; b) ortophoto; c) DEM***

(Source: authors' elaboration)

DEM can be further investigated in the GIS environment to obtain the morphological characterization of the building and a much more advantageous vectorial representation, at the level of information and readability management, of the raster data obtainable from the photogrammetric process. The morphological information (for example slopes and slope exposures) of the buildings can be useful in different fields of application, from sustainable redevelopment where it is possible, for example, to return the photovoltaic potential of the roofs to the realization of snow management plans, in which they can be identified critical points (for example, northern exposures and steep slopes) for optimized planning of interventions[66]. An accurate and multiscale database allows GIS software to make full use of processing enormous amounts of data.

[64] Tucci G., Bonora V., *Geomatics and management of at-risk cultural heritage*, Rendiconti Lincei, Vol. 26, Sup. 1, 2015, 105-114, doi: https://doi.org/10.1007/s12210-015-0427-0.

[65] Gardner-Youden H.L. et alii), *Indigenous mapping technologies: the past, present and future of the collaborative geomatics web-based tool*, Knowledge Management for Development Journal, Vol. 7, Issue 3, 2012, 340-353, doi: https://doi.org/10.1080/19474199.2012.684500.

[66] Dominici D. et alii, *Multiscale documentation and monitoring of L'Aquila historical centre using uav photogrammetry*, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. XLII-5/W1, 2017; Dominici D., Alicandro M., Rosciano E., *Fotogrammetria da UAV per una gestione smart dei centri storici minori*, 11° Workshop Tematico di Telerilevamento | Osservazione della Terra: Georisorse, Risorse Produttive, Geopolitica, Calamità Naturali e Beni Culturali, 2017.

5.3.2 L'Aquila Smart City and the historic centre

The reconstruction of L'Aquila began based on an intentionally ‘ordered’ model, the outcome of a disciplinary rationality substantially restrained to functionalist planning applied to the modern city and of an institutional rationality optimistically projected towards inter-institutional governance, blocked however by a comparison-clash between local powers and central administration. In L'Aquila prevailed a ‘structural’ and static vision of the territory, linked to the great road system, to the geomorphological constraints, to the landscape and historical monumental constraints. But above all, a concept linked to the survival of the two models that have always characterized the territory of L'Aquila, the urban-centred one focusing on the functions of the historic centre, and the polycentric one built on a diversification of the functions of the hamlets. The earthquake not only heavily modified this settlement structure producing new temporary aggregations (CASE Projects, MAP and DCC houses 58/2009) with a substantial consumption of soil but has relocated new centralities and with them has produced a shift of residences and a variation of flows determining in substance a porous and widespread city which corresponds to a new citizenship that manifests predominantly individualistic behaviours.

But if any form of programmatic rationality and urban planning has disappeared, experiments of advanced technologies in the renewal of infrastructures, services and mobility have been widespread, supported by significant public and private investments. These are innovations that almost exclusively concern the historic centre, realizations in progress and rapid evolution that can be summarized with the following points:

- The Smart Tunnel (Figure 25), a tunnel in which the underground networks are housed in a single location under the road surface of the historic centre[67].
- L'Aquila Smart Grids, which empowers technologies and services for the Smart City that arises from an agreement protocol between ENEL (National Electricity Agency) and the Municipality of L'Aquila signed in 2013. It is a series of interventions on the electricity distribution network aimed at implementing capabilities of smart energy networks.
- Structural monitoring, through sensors for assessing the vulnerability of structures and for planning maintenance activities (a University of L'Aquila experimentation[68]).
- Augmented reality (figure 25), through which to represent new levels of information and keep the memory of the reconstruction phases of the city but also of its history (a University of Aquila experimentation[69]).
- The 5G, for which L'Aquila is one of the cities of experimentation and which will greatly improve the capabilities of mobile broadband and address the new needs of the network society, such as Self Driving Car, Work & play in the cloud, Augmented reality, Sensor NW, etc.[70] (University of L'Aquila / ZTE agreement).

[67] Si veda http://www.sottoserviziaq.it/

[68] Potenza F. et alii, *Long-term structural monitoring of the damaged Basilica S. Maria di Collemaggio through a low-cost wireless sensor network*, Journal of Civil Structural Health Monitoring, 2015, 5(5):655-676, doi: https://doi.org/10.1007/s13349-015-0146-3.

[69] Brusaporci S. et alii, *Augmented Reality for Historical Storytelling. The INCIPICT Project for the Reconstruction of Tangible and Intangible Image of L’Aquila Historical Centre*, Proceedings, 1, 1083, 2017, 1-20, doi: https://doi.org/10.3390/proceedings1091083.

[70] IEEE, *ITU-R agrees on key performance requirements for IMT-2020=”5G”*, 2017, in: http://techblog.comsoc.org/2017/03/02/itu-r-agrees-on-key-performance-requirements-for-imt-20205g/, last access: 25.01.2019.

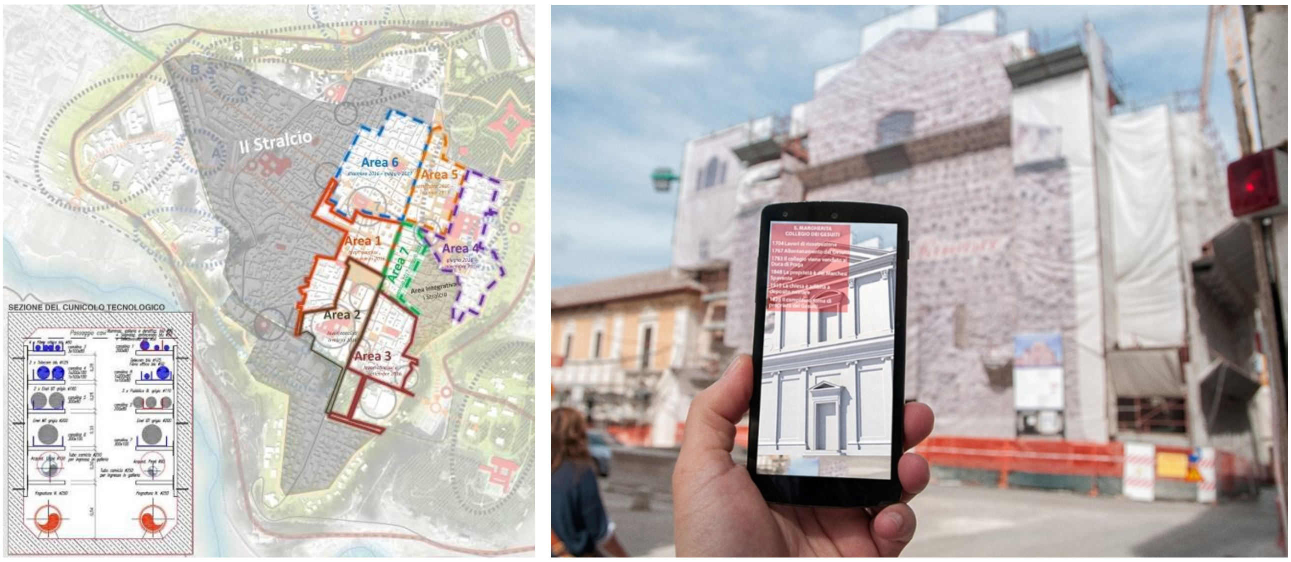

Il Stralcio
Area 6
Area 5
Area 1
Area 4
Area 7
Area 2
Area 3
SEZIONE DEL CUNICOLO TECNOLOGICO
S. MARGHERITA COLLEGIO DEI GESUITI

Figure 25. Historic centre of L'Aquila. On the left the areas where the Smart Tunnel is made. On the right the experimentation of augmented reality on monuments.

(Source: on the left "L'Aquila un centro storico ricostruito smart" - Urbanpromo 2016; on the right[71])

These innovations are taking place on a destructured urban settlement and on a territory that the 2009 earthquake and subsequent reconstruction have radically changed, putting all the urban, social and economic components at stake and therefore presenting a very particular condition in which an acceleration of processes allows to experiment and verify new forms of spatial organization and of their governance. This experimentation, which leads back to the Smart and Resilience principles, allows us to have an idea of what will be the new drivers for the growth of areas of high historical value, with the aim of relaunching urban parts of significant dimensions where today the quality of life has several elements of criticality. However, some open questions remain related to the conservation purpose of historic buildings that, in the historic centre of L'Aquila, for example, did not allow the installation of technological plants to produce energy from renewable Sources[72]. In a historic centre like L'Aquila, 160 hectares large with the potential to house up to 20,000 inhabitants, the theme of clean energy is fundamental and must necessarily be addressed to meet the new needs of the contemporary city.

5.3.2.1 Smart City and Safety

The technological innovations that are modifying the ways of benefiting the city and the rights of citizenship, even the concept of public and private sphere, as we have seen refer to the principles of Smart City and Resilient City, among which urban safety. Some new technologies are in fact oriented to the enhancement and management of urban safety, and not only affect the social but also the physical, connected to catastrophic events. In this last field, some experiments of urban innovation are also developed in the city of L'Aquila and its historic centre.

The first is the structural monitoring, an important tool for assessing the vulnerability of building structures and for planning maintenance activities. This applies to seismic areas with an important monumental heritage, such as L'Aquila. The dynamic and permanent monitoring takes

[71] Brusaporci S. et alii, *Augmented Reality for Historical Storytelling. The INCIPICT Project for the Reconstruction of Tangible and Intangible Image of L'Aquila Historical Centre*, Proceedings, 1, 1083, 2017, 1-20, doi: https://doi.org/10.3390/proceedings1091083.

[72] SBAP, *Prescrizioni per gli interventi nei centri storici di L'Aquila e frazioni*, Comune dell'Aquila, Soprintendenza per i Beni Architettonici e Paesaggistici per l'Abruzzo, 2011, in: http://www.comune.laquila.it/moduli/output_immagine.php?id=1877, last access: 25.01.2019.

place through the installation of wireless sensors (accelerometer, extensometer, inclinometer) in some structural nodes of buildings that produce the data in continuous form to a subject in charge of control in order to have a continuous control on the structural behaviour, for example in relation to micro-earthquakes. In L'Aquila there are some experiences on monitoring, including one on the Basilica of Collemaggio very struck by the 2009 earthquake[73].

A second experimentation that will have enormous repercussions on urban safety concerns the 5G, for which L'Aquila is one of the pilot cities in Italy and is being developed following an agreement between the University of L'Aquila and ZTE. The 5G is a new 5th generation mobile communication standard, at high speed (up to 100 times that of 4G), high bandwidth and very low latency. Figure 26 illustrates some examples of usage scenarios of the 5G envisaged by the International Mobile Telecommunications - IMT for 2020, considering the roles that IMT could play to better meet the needs of the networked society[74]. In particular, the red circles highlight the scenarios that will be tested from the beginning:

- The Self Driving Car, which combined with Car Sharing could significantly reduce the number of cars circulating in urban areas and in particular in the historic centre, and therefore could significantly increase urban safety.
- Augmented reality, which allows to communicate information that may, for example, relate to safety during a disaster emergency. The hypothesis is that the 5G network continues to remain efficient and active even during and after the disaster.
- The Sensor NW, which concerns the sensors connected to home automation, to the measurement of pollution, sound and wind levels, as well as sensors connected to the monitoring of landslides, floods and structural changes in buildings. In this context, the 5G network allows to transfer a huge amount of data in a very short time.

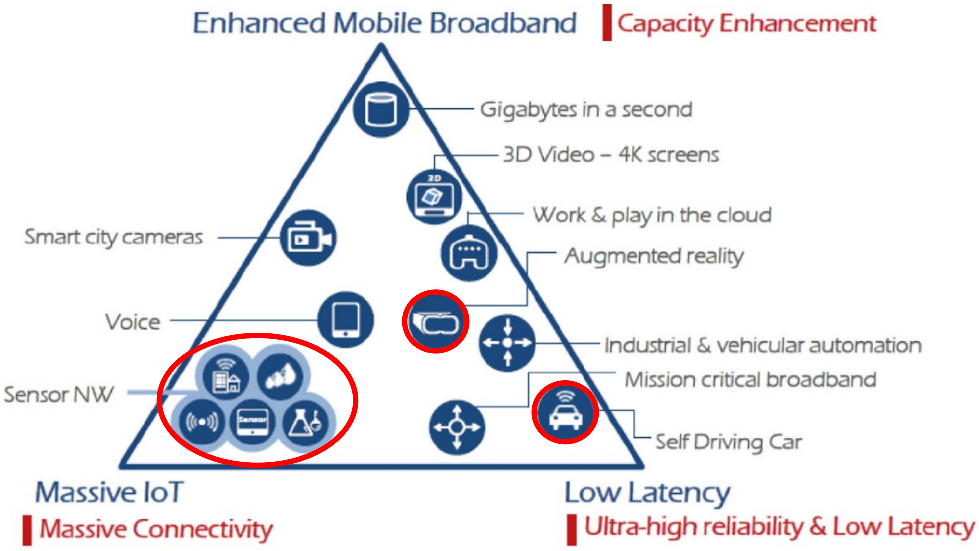


Figure 26. 5G, Usage scenarios.

(Source: ETRI Graphics, from ITU-R IMT 2020 requirements)

Still in the direction of urban safety and resilience, a research by the University of L'Aquila on Clean Mobility systems is organized. This research, for the historic centre a dense-grid of small-sized electric buses, supplied by a hydrogen power unit and characterized by a high transit

[73] Potenza F. et alii, *Long-term structural monitoring of the damaged Basilica S. Maria di Collemaggio through a low-cost wireless sensor network*, Journal of Civil Structural Health Monitoring, 2015, 5(5):655-676, doi: https://doi.org/10.1007/s13349-015-0146-3.

[74] IEEE, *ITU-R agrees on key performance requirements for IMT-2020="5G"*, 2017, in: http://techblog.comsoc.org/2017/03/02/itu-r-agrees-on-key-performance-requirements-for-imt-20205g/, last access: 25.01.2019.

frequency[75]. The goal is to eliminate private transport, at high risk, and introduce public transport with essentially no environmental impact.

The scientific literature deals with the topic of urban risk often in relation to natural disasters and less in anthropic and sustainability terms, placing it in direct relation with resilience and safety[76]. In both cases, however, it affirms that cities must improve their ability to predict risk and adopt new approaches to disaster management that are flexible enough to adapt to an evolving risk environment and to safeguard urban security. This is achieved mainly through new technologies, which simplify and economize data collection and processing.

5.4. A vision for the future of the smart historic centre

For the city, and therefore also the historic centre, being Smart means first having an efficient network infrastructure covered by efficient information services, but it also means:

- Improve urban planning and interventions on historical heritage as it allows new levels of knowledge.
- Improve physical and digital accessibility, also through the creation of services aimed at enhancing the use of zero emission vehicles, with autonomous and shared guidance.
- Realize the continuity of critical services.
- Implement the principles of e-communities / e-societies (blockchain potential[77]) and enhance e-government services.
- Monitor urban safety (social and physical) through a widespread sensor network, also creating a Disaster Risk Management Centre to spread the knowledge produced by reconstruction and to improve human wellbeing in the face of climate change.
- To enrich the sensorial perception of the historic centre, of its monuments but also of its public facilities, by means of a new level of information that can be detected, for example, by the mobile network and its terminals.

These Smart elements, which are already developing autonomously, will characterize the cities and historic centres of the future, permeating new citizenship rights. However, we believe that this development left to the capture of funding, to projects unrelated to a strategic vision, should be traced back to the framework of short and medium-term structural strategies linked to spatial planning and urban design[78] addressed to:

- Strengthening of urban networks with the aim of making sustainable and efficient infrastructures, also in terms of safety.
- Valorisation of the services and facilities system, but also the management of public spaces in relation to the needs of contemporary society.

[75] D'Ovidio G., Di Ludovico D., La Rocca G. L., *Urban Planning and Mobility Critical Issues in Post-Earthquake Configuration: L'Aquila City Case Study*, Procedia Engineering, 161, 2015, 1815-1819, doi: https://doi.org/10.1016/j.proeng.2016.08.670.

[76] Fekete A., Fiedrich F. Eds., *Urban Disaster Resilience and Security. Addressing Risks in Societies*, Spinger international publishing, 2018; Romero-Lankao P. et alii, *Urban Sustainability and Resilience: From Theory to Practice, Sustainability*, 8(12), 1224, 2016, 1-19, doi: https://doi.org/10.3390/su8121224; Prior T., Roth F., *Disaster, Resilience and Security in Global Cities*, Journal of Strategic Security 6, no. 2, 2013, 59-69, doi: http://dx.doi.org/10.5038/1944-0472.6.2.5.

[77] Tapscott D., Tapscott A., *The Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, Portfolio/Penguin, 2018, New York.

[78] Di Ludovico D., *Il Progetto Urbanistico, prove di innovazione per la città del futuro*, Aracne Editrice, 2017, Canterano (Roma); Di Ludovico D., Properzi P., Graziosi F., *From a Smart City to a Smart Up-Country. The New City-Territory of L'Aquila*, Tema, Journal of land use, mobility and environmental, Special issue (june), 2014, 353-364, http://dx.doi.org/10.6092/1970-9870/2482; Di Ludovico D., Properzi P., *Progetti urbani e Progetti urbanistici nel governo dei paesaggi post-urbani*, in (a cura di) Fini G., Caschetto S., Reissner M., L'Urbanistica che cambia. Rischi e valori, Planum, The Journal of Urbanism, n. 25, vol.2, 2012.

- Enhancement of the widespread system of cultural heritage and, more generally, of the urban landscape of historical value.
- Re-planning, based on the new paradigms of contemporary society, of the public city, the residential system and the commercial one.

Today these structural strategies, like the Smart ones, must inevitably be supported by selective injections of public funding that must necessarily respond to a vision of development of the historical nucleuses and the connected suburbs.

5.5. Conclusion

The City of L'Aquila, which can count on the presence of a University that carries out research activities on the themes of the Italian and European digital agenda, covering a large part of the areas of interest, but also of numerous public and private research centres, can and must set ambitious goals on the theme of innovation in the urban context and in particular of its historic centre. It can reasonably aim at least national leadership on how a fragile urban context, such as the historic centre, can best combine innovation, cultural traditions and the quality of life of citizens.

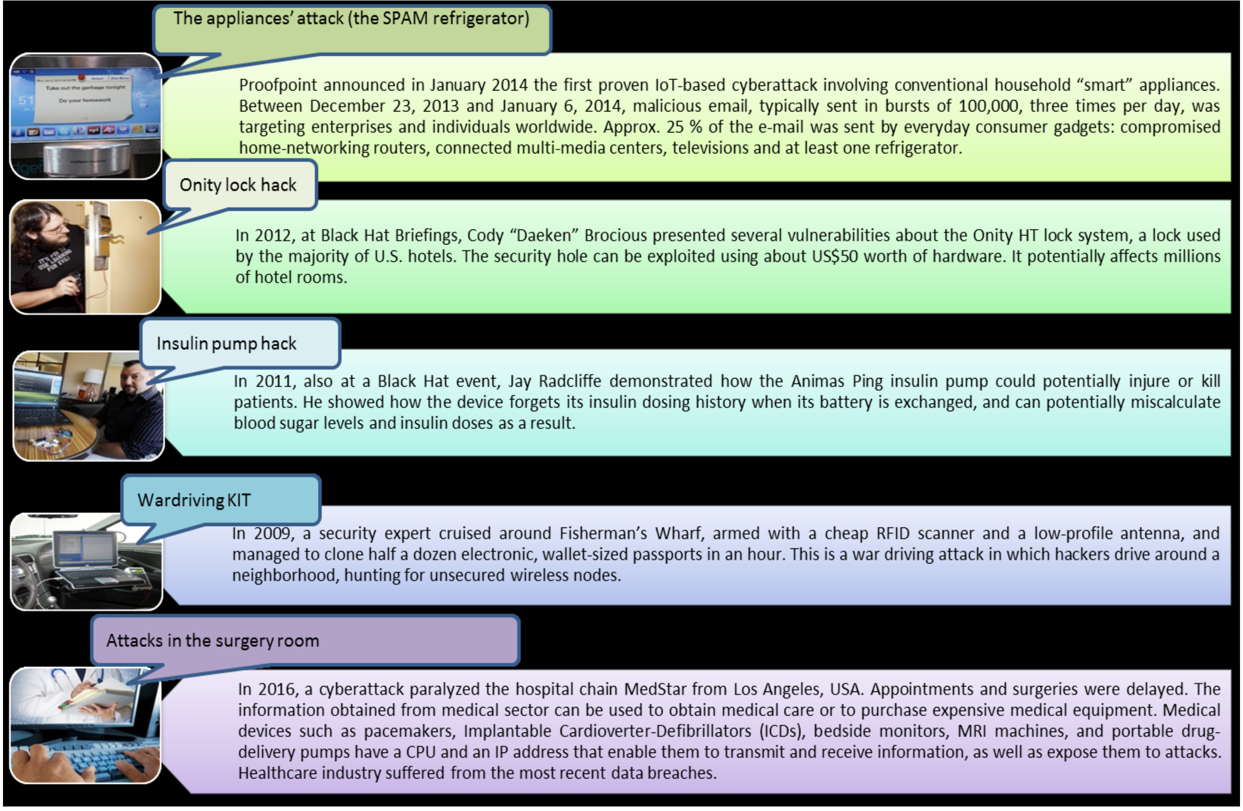
The study prepared by the University of L'Aquila and described in this chapter uses the principles of Smart City to structure a possible new model of development of historic centres, thus hypothesizing a new design path of forms and relationships in a logic of resilience. The *incipit* is the activity of experimentation of innovative technologies for urban development that is affecting the historic centre of L'Aquila in the progress of its post-earthquake reconstruction phase 2009. These are innovative projects detached from a general strategy development of the city which also considers the spatial aspects, and of which the consequence on the urban system is still unclear. It is precisely on this subject that the research is concentrated, that is on the understanding of how the accelerated and autonomous transformations of a historic centre of considerable extension and historical-monumental value, affect its structures and systems, and how much these transformations respond to the new needs of society and the contemporary city. We believe that this combination of innovative principles and tools can develop in an integrated way the new settlement themes in coherence with Smart growth, not only connected to new technologies but also to the effects of climate change and to new urban design and planning applications (new urbanism, tactical urbanism, etc.).

The next steps will extend the analysis to similar cases, including in the context of reconstruction following the 2016-2017 earthquake in central Italy, and international experiences.

6. How to limit the consequence of cyber-attacks on a Smart City Infrastructure, with emphasis to data security *(Alberto Traballesi, Glauco Bertocchi)*

6.1 Security in Smart City and its concerns

Smart City is a complex environment where the interconnected cyber-physical devices and processes generate huge quantities of data, much of them in real-time and very detailed. Consequently, various problems occur in this huge data mechanism: *internal and external parties could not be trustable, new threats that affect data confidentiality, integrity, accessibility, protection and privacy are signalled continuously, smart cities technologies are still in their infancy, there are no standards of use and a lot of technical difficulties need to be defeated .... A large variety of things are used in a Smart City .... all this thing can be very smart in some situations and quite stupid in others. when there is a need to protect them ... These resource-constraints restrict the inclusion of adequate security mechanisms (e.g., cryptography) directly in smart objects. In consequence, designers let the security aside, hoping it could be added later-on, and attack-resistance is usually losing the race against other design-factors, as good performance, small form, and low energy consumption .... Data collected by smart things are at the heart of smart cities. The problem is that they are sensitive data, often gathered without our explicit consent ... .* The consequence of all this is that *in a Smart City the attack surface is an extended one, because of the great number of interconnected cyber-physical things, spaces, infrastructures and users. Violations of data security can provoke the compromising of entire system, and an infection can be easily transmitted between systems.*[79].


Take out the garbage tonight
Do your homework

The appliances' attack (the SPAM refrigerator)

Proofpoint announced in January 2014 the first proven IoT-based cyberattack involving conventional household "smart" appliances. Between December 23, 2013 and January 6, 2014, malicious email, typically sent in bursts of 100,000, three times per day, was targeting enterprises and individuals worldwide. Approx. 25 % of the e-mail was sent by everyday consumer gadgets: compromised home-networking routers, connected multi-media centers, televisions and at least one refrigerator.

Onity lock hack

In 2012, at Black Hat Briefings, Cody "Daeken" Brocious presented several vulnerabilities about the Onity HT lock system, a lock used by the majority of U.S. hotels. The security hole can be exploited using about US$50 worth of hardware. It potentially affects millions of hotel rooms.

Insulin pump hack

In 2011, also at a Black Hat event, Jay Radcliffe demonstrated how the Animas Ping insulin pump could potentially injure or kill patients. He showed how the device forgets its insulin dosing history when its battery is exchanged, and can potentially miscalculate blood sugar levels and insulin doses as a result.

Wardriving KIT

In 2009, a security expert cruised around Fisherman's Wharf, armed with a cheap RFID scanner and a low-profile antenna, and managed to clone half a dozen electronic, wallet-sized passports in an hour. This is a war driving attack in which hackers drive around a neighborhood, hunting for unsecured wireless nodes.

Attacks in the surgery room

In 2016, a cyberattack paralyzed the hospital chain MedStar from Los Angeles, USA. Appointments and surgeries were delayed. The information obtained from medical sector can be used to obtain medical care or to purchase expensive medical equipment. Medical devices such as pacemakers, Implantable Cardioverter-Defibrillators (ICDs), bedside monitors, MRI machines, and portable drug-delivery pumps have a CPU and an IP address that enable them to transmit and receive information, as well as expose them to attacks. Healthcare industry suffered from the most recent data breaches.

Fig. 27. Attacks in a Smart City – some examples

(*Source: Daniela Popescul and Laura-Diana Radu* " *Data Security in Smart Cities: Challenges and Solutions*" *Informatica Economică* vol. 20, no. 1/2016)

[79] Daniela Popescul and Laura-Diana Radu " *Data Security in Smart Cities: Challenges and Solutions*" *Informatica Economică* vol. 20, no. 1/2016.

For these motivations a big, perhaps the biggest, challenge facing Smart Cities progress is the cyber security of systems, this is a critical concern due to the growing potential of cyber-attacks and incidents against critical sectors in a Smart City. Cyber security must take care of intentional attacks, such as from dissatisfied employees, industrial spying, and terrorists, and of involuntary compromises of the information infrastructure due to unpatched vulnerabilities, user errors, equipment failures, and natural disasters. To protect a Smart City in appropriate way, several security problems must be tackled.

Most of these concerns are highlighted in the *Proceedings of Barcelona Smart Cities Congress* of 2011 under the guidance of A. Bartoli[80]:

- *Privacy*: generally, privacy is related to specific aspects of an individual and his right to make his own choices about what he does and to keep certain personal behaviours from being shared with others. An important social necessity is to adapt Smart City services to the specific user expectations and preferences; the knowledge of these preferences means the success or breakdown of a service. So, the great societal challenge for this, and for any service requiring user characterization, is to assure user's privacy and security.
- *Networking connectivity:* keeping the network private would greatly minimize the threats from intruders. But having a separate network is not feasible in today's highly connected world. On the reverse side a minimally secured Internet-connected Smart City approach, as commonly found with commercial networks, opens the door to threats from multiple types of attacks as, for example, cyber-attacks from antagonistic groups with the intention to origin a break of the services. Another type of attack is worm infestations which have proven to negatively impact critical network infrastructures. Such threats have largely been the result of leaving a network vulnerable to threats from the Internet. For example, there have been denial of service ("DoS") attacks on a single network that disrupted all directory name servers, thus prohibiting users from connecting to any of the resources.
- *Complexity*: by interconnecting systems that serve totally different purposes and, in this manner, creating a "system of systems", the complexity of such collaborating systems increases exponentially. As a result, the amount of vulnerabilities in a Smart City system will be significantly higher than that of each of its sub-systems. In addition, the simple interconnection of two systems might open the door to new attacks that have not been considered before. As a result, research into ways of management the growing complexity of distributed systems from the security viewpoint is necessary.
- *Security services*: the Smart City industry requires access to cost-effective, high-performance security services, as well as capabilities in mobility, security, and systems integration. A qualified security services organization would need to provide the following capabilities: demonstrated capability in information security for organizations such as governments, large enterprisers and service providers; holistic security framework that operationalizes security through the people, process, policy and technology foundations of each organization.
- *Sensitive data organization*: the number of users, and the volume and quality of collected data, will also increase with the development of Smart Cities. When personal data is collected by smart meters, smart phones, connected plug-in hybrid electric vehicles, and other types of sensors, attention to the privacy becomes very important. The challenge is, on one side, in the area of identity and privacy management, where, for instance, pseudo-nomination must be applied throughout the whole system, in order to separate the data collected about a user (which is required in order to provide high quality personalized services) from the user's real identity (which is required for purposes such as accounting); this includes that the usage of addressing identifiers, such as IP or MAC addresses, for the purpose of identification should be avoided in future systems.

[80] A. Bartoli and Others "*Security and Privacy in your Smart City*" in Proceedings of Barcelona Smart Cities Congress 2011, 29-2 December 2011, Barcelona (Spain)

On the other hand, privacy technologies must be integrated into all systems, in order to limit and safeguard personal data.

- *Availability*: the availability of services depends on the proper operations of many components and the availability of connectivity between these components. To interrupt a service, an attacker might gain electronic access to a component and configure it incorrectly or to "impersonate" another component and report a false condition or alarm, but one of the simplest types of attacks that an adversary might attempt is the denial of service attack (DoS), where the adversary prevents authorized devices from communicating by consuming excessive resources on one device. Smart City protocol designers must ensure that proper care and attention is given to this threat during protocol development.
- *Emergency plan*: the components, systems, networks, and architecture are all important to the security design and reliability of the Smart City communications solution. But it's inevitable that an incident will occur at some point and one must be prepared with a proper *Incident Response plan*. Response that can be different between commercial providers and private utility systems. A private utility network is likely to provide better consistency of incident response plan in the event of a security incident, assuming that private network is built upon a standardized framework of hardware and software. The speed of the response decreases exponentially as the number of parties involved increases. The rapidity of the response is crucial in emergency situations.
- *Key management*: key management is necessary to provide a reliable crypto security. Smart City will contain millions of devices, spread across hundreds of organizations, the key management systems used must be scalable to extraordinary levels. Further, key management must offer strong security (authentication and authorization), interoperability, and the highest possible levels of efficiency to ensure that unnecessary cost due to overhead, provisioning, and maintenance are minimized.

6.2 Cyber Security and Smart Cities: overview of a possible approach

As already stated in chapter 2, a Smart City can be modelled as system of systems and this consideration can drive a possible approach to cyber security.

We can consider that there are 3 types main components to be considered: 1) the networks that connect the devices and the systems; 2) the systems that provide services used by other systems or by one or more users; 3) the data used by systems to provide services and information to systems and users.

All these types of components must be secured against attacks and/or errors and this goal can be achieved using technical and organizational means that are appropriate to type and relevance of the objects to be protected.

It is beyond our scope and our capabilities, to provide a "complete and exhaustive" review of the very huge landscape of the feasible solutions. Our concern is to focus on some points we consider crucial and suggest a possible approach.

A first general consideration is that a cyber security system must be managed in order to keep the desired level of defence. A security system that is not managed became obsolete or ineffective in a very short time and all previous investments can be voided.

Consequently, you should identify and acquire the resources (financial, human, skills, etc.) needed to keep your security systems up to date and well managed.

A second general consideration is that "human factor" is one of the most relevant weakness in security (not only cyber) systems. People must be informed and trained to be aware of the risks related to cyber world. Users are probably the worst threat and the biggest opportunity; they can "destroy" your systems or help to keep a good level of awareness and security. Involvement of people is a difficult but rewarding task, many situations can be better approached with organizational solutions instead of technical ones and people are the main component of every organization.

Another general consideration is to apply the "defence-in -depth" concept whenever and wherever is possible. In a system of systems this model can be viewed as a distributed defence where each component is protected against threats from "outside". A simple improvement of this model would include protection from "inside" to bound and prevent the spread of menaces to other systems.

Regarding networks one of the main concerns is to keep the bandwidth available, e.g. assurance of effective connections, and avoid the propagation of threats. Segregation of sub-networks can a possible solution that must be balanced with the capability of effective connection among end points in different subnetworks.

Systems that provide services are one of the main targets of threats focused on blocking or altering their functioning. They are also objectives of malware for data exfiltration. Cyber defence against these threats is a difficult and complex task and can be approached using multifaceted solutions (Intrusion Detection Systems on systems and on the network, specialized appliance or programs to identify Advanced Persistent Threats -APT-).

Data are the fundamental component of ICT world and consequently of a Smart City. Without data there are not services (smart or not) and information. Protection of data (confidentiality, integrity, availability) secure access to data is essential to functioning of a Smart City. The following paragraphs are focused on this aspect.

6.3 Passwords and Encryption

Cyber security of a network system or asset is crucial for everyone, especially in a Smart City. Data lost due to disasters such as a flood or fire is devastating but losing it to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners – as affirmed by *Federal Communication Commission (FCC)*[81] .

Most business data are moved and used through the organisation, and every time data moves, it can be exposed to dangers. Generally, access to sensitive data must be restricted, in addition to this safeguard technical protections are fundamental.

The two primary safeguards to protect data are *passwords* and *encryption*. Particularly, when cities are currently using *SCADA (Supervisory Control And Data Acquisition)* systems to control large-scale processes and unify decentralized facilities. In this case if systems are susceptible to be hacked due to the lack of authentication factors and cryptographic security, then there is the consequent possibility that multiple city services are shut down.

User access management is one of the most relevant instruments used to reduce the risk of improper access to systems and data. According to ISO 27001 [82] an access policy to systems and data should be established and maintained; this includes user access rights (which systems and data the user needs to access and for which period) and management of secret authentication information of users. Secret authentication information are means known and available only to the user, they must be kept as secret and not attackable as possible; passwords are the most diffused type of user secret information.

[81] FCC "*Cyber Security Planning Guide*" July 25, 2014, https://transition.fcc.gov/cyber/cyberplanner.pdf

[82] International Standard Organization *ISO-IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements Annex A A.9.2*

Passwords implemented to protect the access to your most sensitive data should be the strongest they can reasonably be. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly and that are closely guarded by those who know them. Employee training on the basics of secure passwords and their importance is a must.

Passwords alone may not be enough to protect the access to the most sensitive data. It's better to adopt two-factor authentication, which often combines the password with another validation element, such as the *PIN (Personal Identification Number)*. Sometimes a stronger authentication factor could be obtained using additional authentication factor like One-Time-Password- (OTP) that are generated on request and have a limited validity (few seconds).

Secrecy of user authentication information is crucial to prevent the possibility of stealing valid credentials (e.g. intercepting authentication data when exchanged with systems to get access) and consequent possible "personification" by an attacker.

Data and information can be stolen, altered, destroyed in many ways. The most used mean against destruction include backup and disaster recovery in their different forms suitable to cope with the needs (time to recover, amount of data to be recovered, etc.) of availability of data.
Stealing and/or alteration of data can be done in many ways (interception on the network, intrusion in systems, malware for data stealing or alteration, etc.) and implies loss of their confidentiality and/or integrity. The most used mean to protect data during their usage, transmission a storage is to encrypt them in a secure way.

With the *encryption* every type of data is converted from a readable form to an encoded version that can be decoded by another user if he has access to a decryption key[83]. *Encryption* is widely used on Internet to protect user information being sent between a browser and a server, including also personal information that should be considered private. The encryption also commonly used to protect sensitive data stored on computers, servers and mobile devices like phones or tablets.

Uncrypted data (*plaintext*) are encrypted employing an encryption algorithm and an encryption key, generating a *ciphertext*. The encryption algorithm can be symmetric or asymmetric depending on the number and type of keys used.

Symmetric key cipher, also named "*secret key*", use a single key. In this case the sender must exchange the key with the receiver to make it capable of deciphering the ciphertext. Exchange of the key can be done in many ways (using a channel of communication separated from the one used to exchange the cyphertext; using a set of keys exchanged in advance, etc.) To allow an automatic exchange of the secret key an asymmetric algorithm is often used to accomplish a secure exchange.

Asymmetric algorithm uses two different mathematically linked keys . This is also called *public key cryptography*, because one of the keys can be given to anyone. The other key must be kept private. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the *public key*. The other key in the pair is kept secret; it is called the *private key*. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

The *RSA*[84] *encryption* algorithm is the most widely used public key algorithm and derives its security from the computational difficulty of factoring large integers that are the product of two large *prime numbers*. Multiplying two large primes is easy, but the difficulty of determining the original numbers from the total assures public key cryptography security. The time it takes to factor

[83] Margaret Rouse "*Encryption*" November, 2017, https://searchsecurity.techtarget.com/definition/encryption

[84] The *RSA* is one of the first *public-key cryptosystems* and the acronym is made of the initial letters of the surnames of *Ron Rivest, Adi Shamir, and Leonard Adleman*, who first publicly described the algorithm in 1978 (Wikipedia)

the product of two sufficiently large primes is beyond the abilities of most hackers, excepting state actors who have access to significant computing capacities[85].

In addition, the *integrity*, *authenticity* and *non-repudiability* of the data may be assured by adding the digital signature, a mathematical technique based on public key cryptography to ensure the authenticity of digital messages or documents[86].

A new emerging encryption methodology is the *quantum cryptography*[87]. Quantum cryptography uses physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages[88]. Quantum cryptography relies more on physics, rather than mathematics, as a key aspect of its security model. Essentially, quantum cryptography is based on the usage of individual particles of light (*photon*) and their intrinsic quantum properties to develop an unbreakable cryptosystem - essentially because it is impossible to analyse the quantum state of any system without interfering with the normal functioning of that system. It is theoretically possible that other particles could be used, but photons offer all the necessary qualities needed, and they are the information carriers in *optical fibre* cables, the most promising medium for extremely high-bandwidth communications. In synthesis the advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state because the act of reading data encoded in a quantum state changes the state. This makes unobserved eavesdropping impossible because it will be quickly detected, thus greatly improving assurance that the communicated data remains private. This could be used also to detect interception attempts in quantum key distribution. The process of developing this cryptography process is underway.

It is important to underline that encryption is an important instrument for protecting data but presently there are some limitations to its general use. Nowadays encryption processing requires time and computing power and these requirements could not always be satisfied in some types of industrial systems like ICS (Industrial Control System) or SCADA and, on the other side of performance, by most of the “small and smart” devices like IOT sensors. Namely industrial systems in general could have timing constrains to manage fast processes that require real time response and encryption could cause an unaffordable overhead. On the other side IOT sensor are in their infancy and encryption is not a priority compared to other features, moreover the cost of “on board encryption” often precludes its implementation for marketing reasons.

A Smart City is a system of systems composed by many different types of elements with different operational requirements and technological capabilities. Consequently, special care must be taken in connecting components (systems, devices, sensors, etc.) to avoid that less secure elements become vehicle for threats.

[85] Margaret Rouse “*Asymmetric cryptography (public key cryptography)*” June 2016, https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

[86] In more details the *digital signature* can provide: Authentication (when a document is digitally signed, the sender can be verified based on its digital signature) - Integrity (a digital signature assures that a document hasn’t be altered during its transfer process) – Non-repudiability (a digital signature is auditable and verifiable, so the sender can’t deny is existence).

[87] Margaret Rouse “*Quantum Cryptography*” September 2005, https://searchsecurity.techtarget.com/definition/quantum-cryptography

[88] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, and Jun Shen ˝*Quantum Cryptography for the Future Internet and the Security Analysis”* 21-january 2018; **https://www.hindawi.com/journals/scn/2018/8214619/**

To bypass the time and CPU power needed to encrypt via software, some devices are built with a firmware encryption. The most widespread of these types of devices is Solid State Drive.

The *solid-state drive (SSD)* is a *solid-state storage device* that uses integrated circuit assemblies as memory to store data persistently (Wikipedia).

SSD or Hard-Drive Encryption is a technology that encrypts the data stored on a hard drive using sophisticated mathematical functions[89]. Data on an encrypted hard drive can be read only by who has access to the right key or password. This can help prevent unauthorized access to data and provides a layer of security against hackers and other online threats. The concept of hard-drive encryption is that when a file is written to the drive, it is automatically encrypted by specialized software. When a file is read from the drive, the firmware automatically decrypts it while leaving all other data on the drive encrypted. The encryption and decryption processes are transparent to all common applications. A computer equipped with hard-drive encryption appears, from the user's point of view, to function as any other computer would.

Solid State Drives or SSDs serve as a convenient method to store data. These devices offer hardware encryption, eliminating the need for encryption software. They are widely used with portable PC and USB storage to prevent data loss in case of theft and the protection offered is considered adequate for data with not high confidentiality. When needed these types of encryption could be complemented with *software ciphering*. In fact, researchers [90]have discovered security flaws in the firmware of some self-encrypting SSDs that could allow an attacker to bypass disk encryption and access the data, without knowing the user-chosen disk encryption password.

For many organizations encryption can be an exacting activity; there are many suggestions to maximize encryption efforts and minimize the impact on productivity and budget. among them a well-known security firm suggests[91] *"to look for the following capabilities when evaluating encryption solutions:*

Centrally Managed Encryption *– You need to be able to easily deploy encryption across your workforce, manage individual and group encryption keys, manage and set encryption policies, and report and audit encryption status. While some solutions might appear to have a free or low- cost benefit, you'll pay much more in time and effort without a centrally managed encryption solution.*

Multiple Key-Recovery Options *– For endpoint encryption, multiple key-recovery options are a must to minimize help desk calls and ensure productivity of your staff and users. This includes local self-recovery for users, whole disk recovery options administrators can provide users to unlock* their *devices, and an Additional Decryption Key (ADK) an organization can apply across its entire encryption implementation for emergency decryption purposes.*

Data Loss Prevention Integration *– Integration between your encryption and data loss prevention solutions can help ensure the encryption of sensitive data before it's transferred via email, shared folders or removable media.*

SSL (Secure Socket Layer) Specific Requirements *– You need to be able to employ SSL encryption throughout your entire process flow. This requires a comprehensive certificate lifecycle management solution to help track and deploy SSL certificates efficiently"*

These suggestions confirm the complexity that encryption can introduce in an organization and the need for a careful design and planning that must also include management[92], this last aspect is essential because cyber security is always moving. As an example of this continuous evolution is

[89] Margaret Rouse "*Hard-drive encryption*" April 2007, https://searchenterprisedesktop.techtarget.com/definition/hard-drive-encryption

[90] Meijer C.- Van Gastel B. "*Self-encrypting deception: weaknesses in the encryption of solid state drives* (SSDs)*" draft ,* November 2018 https://www.schneier.com/blog/archives/2018/11/security_of_sol.html

[91] Symantec "*White Paper: Keeping Your Private Data Secure*"2014 https://www.symantec.com/content/dam/symantec/docs/white-papers/keeping-your-private-data-secure-en.pdf

[92] International Standard Organization *ISO-IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements Annex A A.10 Cryptography*

that the previous suggestion of SSL employment must be updated to TLS (Transport Layer Security) due to increasing of SSL violations.

One of the last evolutions of cryptography is the Attribute Base Encryption scheme that has been proposed, at ITASEC19 conference.[93]

6.4 Intrusion and Detection Systems

With password (and related access controls) and encryption access to data could significantly be reduced and reserved, but to improve the information security we must get also to the security of the system or systems. Intrusions on information systems are a daily occurrence and need for information security grows along with the sophistication of such attacks[94].

An **intrusion** occurs when an attacker attempts to enter or disrupt normal operations of an information system. Even when such attacks are self-propagating, as in the case of *viruses* and *DDOS (Distributed Denial Of Service)* attacks, they are almost always initiated by someone who want to damage an organization. Usually, t different types of intrusion relate to the objectives of attacker: some intruders don't care which organizations they damage and try to remain anonymous, while others search to achieve notoriety.

Intrusion *prevention* consists of activities that deter an intrusion.

Intrusion *detection* consists of procedures and systems that identify system intrusions.

Intrusion *reaction* encompasses the actions an organization takes when an intrusion is detected.

These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible.

Intrusion *correction* activities finalize the restoration of operations to a normal state and seek to identify the Source and method of the intrusion in order to ensure that the same type of attack cannot occur again, starting again from intrusion prevention[95].

An *intrusion detection system* (IDS) is software that automates the intrusion detection process.

An *intrusion prevention system* (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

IDS and IPS technologies offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as IDSs. For brevity the term *intrusion detection and prevention systems* (*IDPS)* is generally used to refer to both IDS and IPS technologies.

A comprehensive approach to intrusion detection and prevention was made by NIST (National Institute of Standards and Technology) [96]. It defines the complex of environments in which IDPS should be deployed.

NIST defines *Intrusion detection* as "*the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices*". While intrusion *prevention* is "*the process of performing intrusion detection and attempting to stop detected possible incidents*". Consequently, *Intrusion detection and Prevention systems (IDPS)* are primarily focused on "*identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators*". In addition, organizations use *IDPSs* for other purposes, such as

[93] /https://whova.com/embedded/subsession/itase_201901/527244/528804/

[94] Michael E. Whitman; Herbert J. Mattord "*Principles of information security*" Cengage Learning, 2011 (Chapter 2).

[95] Idem note n. 7 (Chapter 7)

[96] Karen Scarfone, Peter Mell " *Guide to Intrusion Detection and Prevention Systems (IDPS)*", NIST, february 2007

"*identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies*".

Most ***IDPSs*** use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. The most used detection methodologies are:

Signature-based, which compares known threat signatures to observed events to identify incidents.

Anomaly-based detection, which compares definitions of what activity is considered normal against observed events to identify significant deviations.

Stateful protocol analysis, which compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.

There are many types of *IDPS technologies*, which are differentiated primarily by the types of events that they can recognize and methodologies they use to identify possible incidents.

NIST publication mentions four types of *IDPS technologies,* they define also the environment to be controlled:

Network-Based, which monitors network traffic for network segments or devices and analyses the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

Wireless, which monitors wireless network traffic and analyses its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP – Transmission Control Protocol, UDP – User Data Protocol) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization's wireless network to monitor it but can also be deployed to locations where unauthorized wireless networking could be occurring.

Network Behaviour Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization's internal networks and are also sometimes deployed where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners' networks).

Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

Among others, NIST Guide specifies that most IDPSs can provide a wide variety of security capabilities. Some products offer information gathering capabilities, such as collecting information on hosts or networks from observed activity. IDPSs also typically perform extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDPS and other logging Sources. Generally, logs should be stored both locally and centrally to support the integrity and availability of the data.

Figure 28 summarize the main characteristic of these types of technology

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyse the widest range of application protocols; only IDPS that can thoroughly analyse many of them
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically, more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyse activity that was transferred in end-to-end encrypted communications

Figure 28. Comparison of IDPS Technology Types

(*Source: Karen Scarfone, Peter Mell " Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST, 2007*)

These four types of IDPS technologies offer different capabilities. Therefore, according to NIST, institutions should use together more types of IDPS technologies to achieve better accurate detection and prevention of malicious activity.

The picture depicted by NIST is still valid and applicable with considerations of some problems in IDPS management and technological evolutions, like IOT when devices are often less protected against intrusion.

First, an organization that deploys any type of IDPS must operate it, this implies skilled personnel trained to analyse the warnings (true alarm, false negative or false positive, etc.) and tune the system to avoid overwhelming information.

Second, more than one system should be used in a coordinated way to protect all the technological environment, applying a "defence-in-depth" criterion, with a security level appropriate to risks.

The evolution of technology has brought in some new environments to be controlled like the widespread usage of virtualization and of the cloud.

The always changing of threats landscape has also pointed out one of the main problems of IDPS, it is difficult to detect the first appearance of a menace. A lot of investments have been made to improve the capability of detection for anomalies in programs, messages, files, etc. Neural network approach has been devised [97] in 1992 and since then many researches has been done to use AI instruments in IDP and some available products claim to have parts using AI components, mainly deep-learning techniques and Bayesian analysis.

Despite these efforts, IDPS still remains an area where skilled personnel must be employed; "intelligent" IDPS can significantly reduce the amount of meaningless warnings but analysing the alarms coming form an "intelligent" system could require a lot of human expertise and intelligence.

[97] H.DEBAR M. BECKER D. SIBONI *"A Neural Network Component for an Intrusion Detection System"* https://pdfs.semanticscholar.org/9f71/2bd6b2118758152aeace0a0e7a6205325f53.pdf

7. A proposal for exploiting research results, technology advances and the role of governance tools in managing Smart and Resilient City projects. *(Glauco Bertocchi, Alberto Traballesi)*

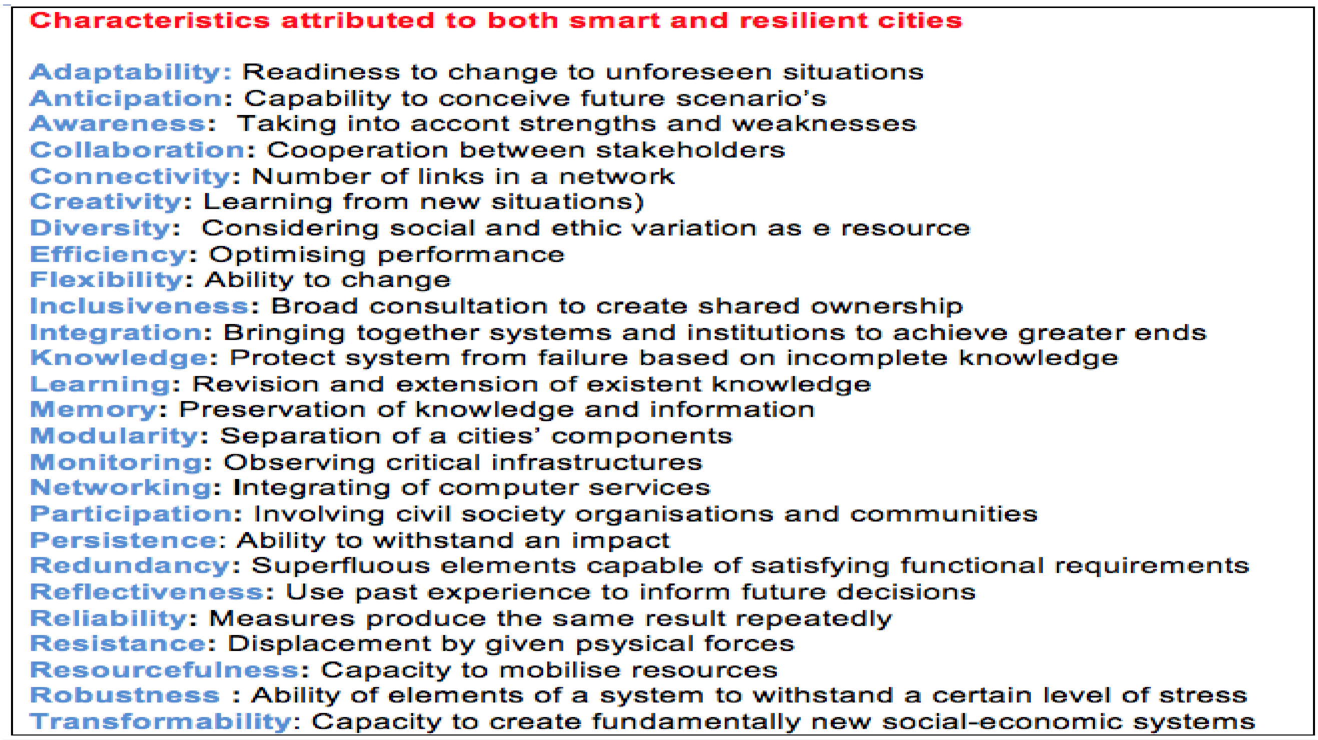
7.1 Foreword

Smart City and Resilient City are concepts that have many different definitions, those in chapter 2 are considered but, whatever is your preferred definition, there is one single point in common: they refer to a process that will take time and resources to be accomplished and very probably will change its targets during the time of accomplishment. More realistically Smart and Resilient Cities are a possible evolution of present cities and Smartness and Resilience are some phases of this evolution focused on some aspects we consider important. In future other aspects will probably emerge and we will possibly define and try to implement Sustainable and/or Livable Cities or other "fashionable" words.

The path to Smart and/or Resilient Cities from present state to a smarter and possibly more resilient condition is slow due to reasons like budget and political constraints, bureaucratic complexities and time needed to accomplish the works and acquire and deploy new technologies.

On other side Smart Cities models and requirements are constantly increasing in number and complexity, moreover technological progress is speeding up and new devices and technologies are available on an almost daily basis.

This "difference of speed" between technological evolution and its real possibility of deployment due to constrains like budget, procurement procedures, installation, is one of the major obstacles and challenge for a coherent and useful transition to Smart and Resilient City environment.



Characteristics attributed to both smart and resilient cities

Adaptability: Readiness to change to unforeseen situations
Anticipation: Capability to conceive future scenario's
Awareness: Taking into accont strengths and weaknesses
Collaboration: Cooperation between stakeholders
Connectivity: Number of links in a network
Creativity: Learning from new situations)
Diversity: Considering social and ethic variation as e resource
Efficiency: Optimising performance
Flexibility: Ability to change
Inclusiveness: Broad consultation to create shared ownership
Integration: Bringing together systems and institutions to achieve greater ends
Knowledge: Protect system from failure based on incomplete knowledge
Learning: Revision and extension of existent knowledge
Memory: Preservation of knowledge and information
Modularity: Separation of a cities' components
Monitoring: Observing critical infrastructures
Networking: Integrating of computer services
Participation: Involving civil society organisations and communities
Persistence: Ability to withstand an impact
Redundancy: Superfluous elements capable of satisfying functional requirements
Reflectiveness: Use past experience to inform future decisions
Reliability: Measures produce the same result repeatedly
Resistance: Displacement by given psysical forces
Resourcefulness: Capacity to mobilise resources
Robustness : Ability of elements of a system to withstand a certain level of stress
Transformability: Capacity to create fundamentally new social-economic systems

(Source: Herman van den Bosch , JaxStrong http://smartcityhub.com/collaborative-city/smart-cities-resilient-cities-make-difference/)

7.2 Main aspects to be considered: Resilience and Smartness

Resilience of a Community (a City is a Community) has been already investigated by our AIIC group among others and some concepts have been recalled in previous chapter 3. It depends on many factors, (see figure 6,7,8 of Guidelines for Community Resilience Evaluation[98]) and is based on a layered model (see figure 11 of chapter 3) that shares, obviously, most of the key infrastructures and functions with a Smart City.

A first question is: which is the most relevant aspect to be considered for a City, Resilience or Smartness?

In our opinion a strong synergy among the two aspects is the most appropriate answer but the two factors are not equivalent.

Smartness, if resilient, can give a big contribution to resilience in terms of communication, emergency management, time for recovery.

Smartness without resilience can worse an emergency making everything more complex due to sudden lack of complex and valuable resources.

In our opinion a Smart City must be designed and built using “smart” solutions that improve or, at least. do not decrease resilience, in fact smartness can improve daily life but resilience is essential to “survive” adverse events.

7.3 A proposal for a pragmatic approach to smartness and resilience of a City

What we consider a pragmatic approach and why suggest adopting it?

First, it is necessary to adopt a point of view. Following there are some brief considerations and the indication for a possible choice.

- Political Administrator. This point of view cannot be chosen due to very different constraints depending on the country and the region considered. Usually political administrators have limited period (4-5 years) and the need to produce visible results; security, safety and emergency management are relevant issues that can be of some interest for them.
- General manager. he/she is not required to be competent for everything but must be capable of organizing complex programs with multi annual evolutions; his/her action can be influenced and limited by political objectives; security, safety and emergency management are mandatory, these topics cannot be avoided.
- Citizens. They are the addressee of city services. They are satisfied by effective, efficient and reliable services; easy access to information and services is required; interconnection among services is really appreciated; security, safety and emergency management are very important; privacy is a relevant issue. Their point of view is relevant in assigning priorities in investments, but it is not relevant for the scope of this paper, except when indicated.

In present paper the point of view of a General City manager has been adopted, his/her daily work is a mix of contingent problems with a part of long and medium planning. A strategy is a must for a City manager, but flexibility and resilience are essential to professional survival. Considering mid and long-term strategies requires preparation to continuous change of all factors that define a City context (e.g. political governance, budget, technological evolution, citizens’ requirements, law and regulatory, etc.). It seems that a pragmatic approach becomes the best possibility, if not the only possible choice.

[98] http://www.infrastrutturecritiche.it/new/media-files/2017/03/COMMUNITY_Resilience_AIIC.pdf

7.3.1 Methodological suggestions for a pragmatic approach

How can we decline a pragmatic approach to a Smart and Resilient City? In [99] there is a similar approach described from the point of view of a Chief Resilience Officer in the 100 Resilient Cities project.

Here are some integrative suggestions:

- **Follow the main research aspects.** Because some of the research results produce applicable technology and, probably more important, organizational aspects and models are often interesting and, using analogies, can suggest some valuable solutions. Some examples of current research projects will be presented in the following.
- **Consider research results that are technologically** available and economically feasible. Large adoption of non-mature technologies can be a dangerous challenge for a City because of costs, reliability, acceptance by the user. On the other side limited experiments of technological novelties can be useful to probe the validity of solutions and help to assess future adoption.
- **Do not bind too much to a short list of technological solutions**, be open to innovation and change. One of the worst problems with technological solutions is their volatility in terms of lifecycle and effectiveness, i.e. you will never know when a new technology will bring your investment in the list of "heritage" solutions. This is a big problem for designers and producers of technologies, but it is also relevant for the administration of a City that uses public funds raised by taxes. Keeping up to date about trend and aware of the risks connected to technology can help.
- **Use what is available now or in the short term.** This an approach that will reduce the technological risk; as a City Manager you are requested to indicate the best available solutions or those reliable answers that will be available in a short time.
- **Keep always in mind that Smart City is a System of Systems** (see chapter 3) and links between systems are fundamental also for resilience and smartness. It is impossible to have all the services of a city at the same level of resilience and smartness; railways have a life cycle of decades whether telecommunication products have a cycle of few years.
- **Focus on interfaces and interoperability** at all levels (from cable to end-user applications) isvital. Interfaces that assure the interoperability among systems for a long period of time (possibly a decade) are the only means to connect different systems with different lifecycle and deployment time.

7.3.2 Some suggestions for essential services

Today's technologies are at very different levels of maturity, but this should not prevent their usage in a scale that should be evaluated based on the previous criteria. Following there are some suggestions of available instruments for some essential services.

- ***Infrastructure (transportation, communication, energy utilities,).*** Each of these sectors has its set of applicable technologies but most of them are in common, mainly those related to the use of ICT, IOT, IIOT, Big Data collection and exploitation, AI usage. All these technologies are used mainly in the Operational Control and Management and they constitute the base for data exchange and services interconnection.

[99] http://www.100resilientcities.org/how-to-develop-a-resilience-strategy/

There is a spread awareness among engineering and construction enterprises about change and integration of infrastructures, in [100] a company proposes a type of infrastructure to transform a city using resilient smart infrastructure. This type of proposals is relevant because it is focused not only on ICT related technologies but includes also building environment, over-ground and underground transport, water management, communications; energy production. The relevant fact is that city resilience and smartness is coming out from the research labs and produces commercial and industrial proposal.

- ***Services (Health care, Education, public safety and security, social services)*** Each of these sectors has its part of smart technologies. Health care benefits of robots for surgery and a lot of new devices for image diagnosis not mentioning the extensive usage of fast communication networks for data transmission. Other sectors have similar enhancements, think for example to advances in video surveillance and face recognition. For these services a secure and reliable communication network is mandatory to obtain the desired results in terms of fast processing of huge amount of data. Other technologies that are of interest for Services are Big Data collection, IIOT, IOT and AI.
- ***Services to citizens (apps and services for a better usage of Services and Infrastructures)*** This is a fast-evolving sector that depends mainly on integration and exchange of information among infrastructures and services. Every city has already its own set of "smart" apps that are useful to track bus or trains arrivals, traffic situation on the route, contact city administrative offices, etc. Reliability and usability of these services depends on the continuous flow of correct and timely information from other providers, reliable and fast transmission networks are essential. Some improvements can derive also from a more intensive and focused usage of Big Data collection and IOT. AI will help the user to orienteering in an overwhelming flow of information.

7.4 Draft Proposal for a possible path to Resilient and Smart City

This draft proposal is based on previous considerations and it lists a set of research projects, methodologies and organizational considerations. It has been drafted to give suggestions and references that could help a City manager to design a strategy, i.e. a path from a current state and a desired one. To transform a strategy in a multi annual plan and to realize it a City Manager would need a governance framework, this specific topic is discussed in following paragraphs.

- **Assessment of current state** (Smartness and Resilience). This is a necessary task to be accomplished. To improve something (service, infrastructure, level of service, etc.) knowledge of current status is mandatory otherwise it is impossible to define improvement. It is a difficult task but some research projects, described in the following, had produced some usable methodologies.

  In chapter 1 some different views of Smart and Resilient City have been introduced using some relevant research projects that are completed in 2018 *IMPROVER, DARWIN, SMR, RESILENS, RESOLUTE, SMARTRESILIENCE*) and *100Cities*, five of them (*IMPROVER, DARWIN, SMR, RESILENS RESOLUTE*) had been coordinated in a common presentation that shows how to improve the European Resilience Management Guidelines

  In the following a synthetic exposure of the main aspects of all these projects with a special focus to methodologies is given.

  IMPROVER[101]

[100] /https://www.bechtel.com/smart-cities/

[101] http://improverproject.eu/

The overall objective of IMPROVER was to improve European critical infrastructure resilience to crises and disasters through the implementation of resilience concepts to real life examples of pan-European significance, including cross-border examples. Some deliverable can be useful for suggestions of methodologies, in particular deliverable 5.1[102] "Framework for implementation of resilience concepts to Critical Infrastructure" is relevant for the definition of resilience. Deliverable 4.5[103] defines a communication strategy that could be useful not only for critical infrastructures but also at city level.

DARWIN[104]

The project was focused on improving responses to expected and unexpected crises affecting critical societal structures during natural disasters (e.g. flooding, earthquakes) and man-made disasters (e.g. cyber-attacks). The main result of this project is[105] "DARWIN RESILIENCE MANAGEMENT GUIDELINES (DRMG Book)" with many useful methodological hints and "DARWIN RESILIENCE MANAGEMENT GUIDELINES" with adaptations for two critical sectors: air traffic management and health care.

SMR[106]

Smart Mature Resilience (SMR) aimed to develop and validate Resilience Management Guidelines, using three pilot projects covering different CI security sectors, as well as climate change and social dynamics. The main result of the project is probably [107] "EUROPEAN RESILIENCE MANAGEMENT GUIDELINE" which has been presented in a coordinated way with (*IMPROVER, DARWIN, RESILENS, RESOLUTE*), this Guideline has also been investigated for standardization at European level.[108]

Among the results [109] "Resilience Maturity Model" is very interesting for current state assessment and it can be downloaded.[110]

RESILENS[111]

This project aimed to develop a European Resilience Management Guideline (ERMG) to support the practical application of resilience to all Critical Infrastructure (CI) sectors. It is CI oriented but the ERMG draft [112]is interesting also for cities.

RESOLUTE[113]

The project was focused on the growing importance of mobility within every human activity and urban transportation in particular. A European Resilience Management Guideline (ERMG) is part of the deliverables[114] as contribution to the general objectives of the five projects already mentioned. A specialized version of the ERMG focused on urban transportation[115] is a relevant result of this project.

[102] http://improverproject.eu/2018/02/16/deliverable-5-1-framework-for-implementation-of-resilience-concepts-to-critical-infrastructure

[103] http://improverproject.eu/2018/08/23/deliverable-4-5-a-communication-strategy-to-build-critical-infrastructure-resilience/

[104] https://h2020darwin.eu/about/

[105] https://h2020darwin.eu/wp-content/uploads/2018/08/DRMG_Book.pdf

[106] http://smr-project.eu/home/

[107] http://smr-project.eu/fileadmin/user_upload/Documents/Resources/WP_5/SMR-EMRG-handbook-WWW_s.pdf

[108] http://smr-project.eu/standards/

[109] http://smr-project.eu/tools/maturity-model-guide/

[110] http://smr-project.eu/fileadmin/user_upload/Documents/Resources/WP_7/SMR-A1-www.pdf

[111] http://resilens.eu/

[112] http://resilens.eu/wp-content/uploads/2017/10/D3.2-Draft-ERMG.pdf

[113] http://www.resolute-eu.org/index.php/2015-07-16-15-29-03

[114] http://www.resolute-eu.org/files/RESOLUTE_D3-6-ERMG-final.pdf

[115] http://www.resolute-eu.org/files/RESOLUTE_D3-8-ERMG_UTS_v2-FULL.pdf

SMARTRESILIENCE[116]

SmartResilience aims to provide an innovative "holistic" methodology for assessing "*resitience*" that is based on resilience indicators. The project was focused on Smart Critical Infrastructures, but its methodology could be helpful also for Smart Cities. One of the relevant results is a [117]"Resilience Tool" that is oriented to help resilience assessment projects at resilience managers and assessors' level. Other interesting deliverables are [118] "Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures" and [119] "Assessing Resilience Level of Smart Critical Infrastructures based on Indicators".

100 Resilient Cities[120]

Pioneered by The Rockefeller Foundation (100RC) is dedicated to helping cities around the world become more resilient to the physical, social and economic challenges that are a growing part of the 21st century. The usefulness and relevance of this project for resilience assessment has been already depicted in chapter 3.

- **Research projects** are eligible for methodologies, research projects usually are not suitable for technology except for indications of future applications. In fact, only very few of the technological results of research projects will reach the market as competitive, reliable and affordable, products.

- **Risk analysis** or more precisely risk management, is the most relevant activity to reduce the elements of risk (impact, likelihood, vulnerabilities) of a system to an acceptable level. A Smart and Resilient City is a system of systems each of them should be designed and implemented in the safest and securest way to obtain a desired level of resilience. Risk management is standardized by standardization bodies (e.g. ISO, NIST). Standard ISO 31000 [121] provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Other ISO standards, like ISO 27005,[122] provide specific adaptation of to specific sector like ICT. NIST recently issued (Dec 2018) a new version of its" SP 800-37 rev.2 Risk Management Framework for Information Systems and Organizations"[123]. Risk management is mandatory at each step and level in pursuing the objective of a Smart and Resilient City. In this activity a standard approach (ISO, NIST), should be used to assure consistency and comparability of assessment.

- **Establish projects with security**, privacy, safety and resilience "by design" and by default". The "by design" approach is recommended by international standards and best practice for reducing the costs of "reshaping" services, applications, systems (also industrial) that were designed and implemented without consideration of resilience, security, privacy and safety. The "by default" approach means that a service, system or application has been devised such as it reaches a "secure" state in case of anomaly or fault.

[116] http://www.smartresilience.eu-vri.eu/

[117] http://www.smartresilience2.eu-vri.eu/RunningApp/RIdb/Welcome.aspx

[118] http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.6.pdf

[119] http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.8.pdf

[120] http://www.100resilientcities.org/

[121] https://www.iso.org/iso-31000-risk-management.html

[122] https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

[123] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

- **Choice of known and available technologies** because devices and systems must be operated and maintained by available and trained resources. This could be a very difficult task because an anomalous dependency can derive when a proprietary product is chosen by a contractor. Moreover, choice of a proprietary technology could imply the impossibility of interfacing and data exchanging with other existent or foreseen technologies used in the city.
  City management should ask for technologies that assure interfaces and data exchange and possibly those with a widespread landscape of suppliers.

- **New and emerging technologies** are important to build up a Smart and Resilient City, they should be adopted gradually and initially for limited projects; general deployment could take place after an appropriate time of positive testing.

- **IOT, IIOT, Big Data and AI** are emerging technologies, they are increasingly involved in many types of services (Energy, transportation, communications, customer services, etc.) they carry some relevant issues for security and privacy that must be addressed.
  IOT security is a relevant problem that has already received some initial answers [124] in terms of structured approach to compliance [125].IEEE has focused some activities on IOT world [126] in order to pursue future standards., the same objective has moved ISO with its Working Document ISO 27030[127] "Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT)". IOT security has already moved to commercial services offered by important companies[128]. Thousands of IOT devices invade the market every year but their security will probably remain a secondary issue respect to cost, features and market visibility.
  IIOT are less common than IOT due to their specific field of application consequently their security issues are less known than IOT but nevertheless there are initiatives like Industrial Internet Consortium that published an [129]Industrial Internet Security Framework with the contribution of many of the most relevant industrial companies. But the IIOT security is still in initial evolution as reported by this [130]review article and by the availability of seminars on the usage and security of IIOT like this seminar[131] issued by one of the biggest actors in industrial automation.
  Big Data security has been object of an ENISA publication [132] and many aspects has been investigated by AIIC Report "*Good Practices and Recommendations on the use of Big Data Analytics for Critical Infrastructure Resilience*"[133] cited in chapter 3. There is not very significant improvement from the situation described in the report; the security issue is still relevant, especially regarding privacy.
  AI security is a very new topic that must be already addressed. NIST [134] has started an initiative that will try to encompass the very broad and still not clear field of AI applications, including its security. The debate on the use of AI has started and is at a very initial state [135] [136] [137] and is

[124] https://www.iotsecurityfoundation.org/

[125] https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

[126] https://standards.ieee.org/initiatives/iot/index.html

[127] https://www.iso.org/standard/44373.html

[128] https://aws.amazon.com/it/iot-device-defender/

[129] https://www.iiconsortium.org/IISF.htm

[130] https://semiengineering.com/toward-iiot-security-standards/

[131] https://www.plm.automation.siemens.com/global/en/webinar/iiot-the-next-big-digital-disruption/31921

[132] https://www.enisa.europa.eu/publications/big-data-security

[133] http://www.infrastrutturecritiche.it/ new / media-files /2018/04/AIIC_BigDataCIPR_FINALE.pdf

[134] https://www.nist.gov/topics/artificial-intelligence

[135] Osonde A. Osoba, William Welser IV *"The Risks of Artificial Intelligence to Security and the Future of Work"* 2017 RAND Corporation%20https:/www.rand.org/pubs/perspectives/PE237.html

mainly focused on the impact that AI will have on human activities especially on employment and on benefits that derive from the use of this technology. As matter of facts there are AI tools already available for anyone like[138] Google tools and platforms[139] that cover most of the requirements for the design and implementation of AI applications.AI tutorials for executives are available in Internet, [140] is an interactive example.
The ethic challenge of AI to personal data protection is discussed in Chapter 9 of present report.

- Services to citizens are very important for the success of Smart City and there are a lot of studies on the subject[141] and service's offers [142] [143] also from "small" nation. Significant factors of success would probably be simplicity of use and device independence.

7.5 Need for Governance framework

The Smart City could be considered as an "enabling platform for the activities that citizens are able to develop, linking those inherited from the past to those that can be realized in the future, so it is not focused on just applications but on the possibility that citizens realize them"[144]
A Smart and Resilient City therefore is a very long, more correctly never ending program, composed by main relevant projects with a duration measured in many years (more than 5 e possibly within 15 years). During this time period many things can change (city political management, budget of the city, technology available, population variation in number and establishment, etc.).

It seems relevant to define what is a program and a project. *"At the most basic level, a project is created to deliver a specified 'deliverable' as efficiently as possible. Programs focus on the coordination of a number of related projects and other activities, over time, to deliver benefits to the organisation* "[145]

It is also useful to define governance in terms of setting strategic goals and monitoring their accomplishment when management is responsible of converting strategic goals in programs and projects and accomplish them in an effective and efficient way. [146]

A more comprehensive definition of Governance framework can be excerpted from Wikipedia:
Governance frameworks are the structure of a government and reflect the interrelated relationships, factors, and other influences upon the institution. Governance structure is often used interchangeably with governance framework as they both refer to the structure of the governance of

[136] https://www.sas.com/sas/offers/18/ai-momentum-maturity-success-models-109926.html?gclid=Cj0KCQiA7briBRD7ARIsABhX8aAPC51381JQ5FR_AdbKX1_YWVRa1T7vvWDV1DYnjMSIQyDfGTokyYoaAghtEALw_wcB

[137] http://www.xorlogics.com/2016/07/31/google-reveals-five-security-issues-concerning-artificial-intelligence/

[138] https://ai.google/tools/

[139] https://www.predictiveanalyticstoday.com/artificial-intelligence-platforms/#topartificialintelligenceplatforms

[140] https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/an-executives-guide-to-ai

[141] E. Dudley, Diaan-Yi Lin, M. Mancini, J. Ng "*Implementing-a-citizen-centric-approach-to-delivering-government-services*" 2015 MCKINSEY https://www.mckinsey.com/industries/public-sector/our-insights/implementing-a-citizen-centric-approach-to-delivering-government-services

[142] https://www.serco.com/sector-expertise/citizen-services

[143] https://www.ttconnect.gov.tt/gortt/portal/ttconnect/!ut/p/a1/jc_dCoJAEAXgZ_EBckaXjbw0UFOD0ChtbkJh2wTbDZO2x0-7q-hn7ga-w5wBghJIVddGVn2jVdWOO033aeYijz2Gqww9dPPYCZCnLEr4AHZPII_CAQTcWaRbhoj_5fHD-D_za6GgAHph7y0e4MuZBEi2uh5eLuZAog-ypRnL-apmMwnUiYPoRGcf9aWH0hhjS61lK-ymh_NpU97iCYXSsu6z9AWx/dl5/d5/L2dBISEvZ0FBIS9nQSEh/

[144] De Biase, L." *L'intelligenza delle Smart Cities (2012)*", http://blog.debiase.com/2012/04/intelligenza-delle-smart-city/

[145] https://mosaicprojects.com.au/WhitePapers/WP1002_Programs.pdf

[146] https://mosaicprojects.com.au/WhitePapers/WP1084_Governance_Systems.pdf

the organization. Governance frameworks structure and delineate power and the governing or management roles in an organization. They also set rules, procedures, and other informational guidelines. In addition, governance frameworks define, guide, and provide for enforcement of these processes. These frameworks are shaped by the goals, strategic mandates, financial incentives, and established power structures and processes of the organization.

A Governance framework is needed to maintain consistency during the time period and make inevitable changes within the objectives. This concept can be passed on different elements, pillars to be organized and linked together[147]. In synthesis they can be summarized in three main pillars, as explained in Fig. 29

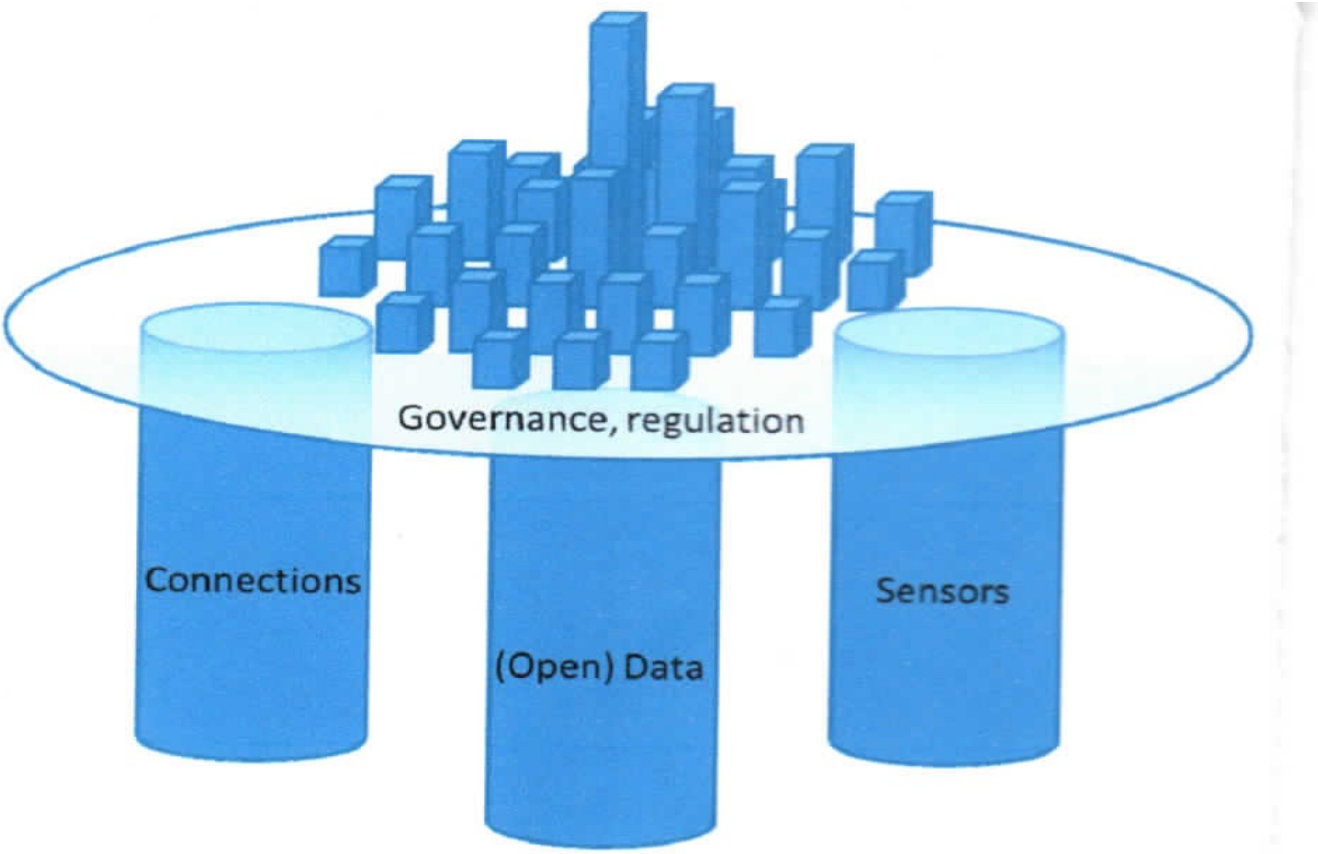


Figure 29. The pillars sustaining the Smart City and its Governance

(Source: Graphical elaboration, after concepts in De Biase, 2012)

These pillars must be combined with a governance able to link them together, giving a direction and a vision to the city.

As a consequence, a Smart City is an environment where a group of elements, as the ones above reported – sensors, data and connections – in combination with a collection of fundamental rules, gives public bodies, citizens, enterprises the possibility of developing applications and solutions able to improve life of the city itself, allowing also to create new markets and solutions also where the public sector is not able to make progress.

To support the city Governance framework a Management system is needed. Executive management is responsible for creating an organisation capable of achieving the objectives defined

[147] Beniamino Murgante1 and Giuseppe Borruso *"Cities and Smartness: A Critical Analysis of Opportunities and Risks"* https://www.academia.edu/people/search?utf8=%E2%9C%93&q=Smartness+and+Italian+Cities.+A+Cluster+Analysis+

by program and projects and capable of providing assurances to the Governance that resources of all types are being effectively and ethically used in accordance with the organisation's policies.

Following there are some indications about well-known systems used for Project Management (PM) or Governance and/or Management. Most of them were conceived for ICT but are also suitable for generic context with extensions or adaptations. They can be used at different levels (governance, management, programs, projects), according to their capabilities and usability, during the transformation to a Smart and Resilient City.

Prince2[148]

PRINCE2 (PRojects IN Controlled Environments) is a structured project management method and a certification program for professionals. PRINCE2 emphasizes the division of projects into manageable and controllable phases. It is adopted in many countries of the world, including the United Kingdom, the countries of Western Europe and Australia. PRINCE2 training is available in many languages. PRINCE2 was developed as a governmental UK standard for information systems projects.
It is suited for projects management.

TOGAF[149]

TOGAF® (The Open Group Architecture Framework) is an Enterprise Architecture Framework, which provides best practices and tools to support the acceptance, production, use and maintenance of a corporate architecture, based on an iterative process model supported by best practices and a reusable set of existing architectural assets. The first version released in 1995 was based on the Technical Architecture Framework for Information Management (TAFIM), developed by the United States Department of Défense. TOGAF® embraces even if it does not strictly adhere to the terminology of ISO / IEC 42010: 2007, where for TOGAF® the concept of "Architecture" has two meanings according to the context:

- A formal description of a system, or a detailed plan of a component-level system to guide it to its implementation;
- The structure of the components, their interrelations and the principles and guidelines that govern their design and evolution over time.

It has been devised as framework and can be used as management and governance system.

AGILE [150]

In software engineering, the expression agile methodology (or agile software development ASD) refers to a set of software development methods that emerged from the early 2000s and are based on a set of common principles, directly or indirectly derived from the principles of the "Manifesto for the agile development of software" (Manifesto for Agile Software Development, improperly also called "Agile Manifesto") published in 2001 by Kent Beck, Robert C. Martin, Martin Fowler and other. Agile methods are opposed to the cascade model and other traditional software processes, proposing a less structured approach focused on the objective of delivering to the customer quickly and frequently (early delivery / frequent delivery), functional and quality software.

[148] https://www.prince2.com/eur

[149] https://www.opengroup.org/togaf

[150] https://www.apm.org.uk/resources/find-a-resource/agile-project-management/w

It is suited for ICT projects.

DEVops [151]

DevOps is a cultural and professional movement that emphasizes communication, collaboration and integration between software developers and IT professionals. The resulting improved workflow gives organizations the flexibility to change and change quickly, without sacrificing the quality and reliability of their IT-based services. The term "DevOps" has been popularized during a series of DevOps Days since 2009 in Belgium. Despite the name, DevOps (DEVelopment and OPerationS) goes beyond software development teams and IT professionals. In general, "Dev" represents all the people involved in the development of software products and services (including company representatives and suppliers) and "Ops" includes all the people involved in the provision and management of these products and services (suppliers included).
It is suited for ICT context and could be used for governance and management

COBIT[152]

In November of 2018, the release of COBIT 2019 has started.
Previous and still relevant version COBIT 5 (Control OBjectives for Information and related Technology) is the only business framework for the governance and management of an IT organization. This evolved version incorporates the latest thinking techniques on the governance and management of organizations, and provides universally accepted principles, practices, analytical tools and models to help increase the credibility and value of information systems. COBIT 5 has been developed, but at the same time extends the concepts of COBIT 4.1 through the integration of the main other frameworks, standards and resources, including IT Risk from ISACA, Information Technology Infrastructure Library (ITIL®) and other standards of the International Organization for Standardization.
It is a powerful instrument for governance and management not only for IT organization because can be easily adapted and extended.

ITIL[153]

ITIL, or the Information Technology Infrastructure Library available today in the 2011 Edition, called ITIL 2011, published in July 2011, has completely replaced the previous ITIL v3 edition, and aims to describe the management of IT services (approach to IT service management - ITsm), in order to improve the quality of the Service itself in compliance with the agreed cost objectives and constraints. The life cycle is based on some fundamental concepts as: Value, Service, Service Management. In IT service management, ITIL cannot be considered a standard, but a good/best practice, while the reference standard is ISO / IEC 20000 (part-1).
It is extensively known and adopted in ICT context. It refers also to Prince2 and AGILE

ISO 21500[154]

[151] https://devops.com/

[152] http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx

[153] http://www.itil.co.uk/,

[154] https://www.iso.org/obp/ui/#iso:std:iso:21500:ed-1:v1:en

The ISO 21500 standard "Guidance on project management" It is a guide for project management that can be used by any type of organization, public, private or community, and for any type of project, regardless of complexity, size or duration. The standard presents the concepts and processes considered good practices in project management. In 2011 ISO created the Technical Committee ISO / TC 258 Project, which started the project 21500 for a first international standard on the topic of Project management. ISO 21500 was published for the first time on 3 September 2012.
It is PM (Project Management) oriented but is of generic application

ISO 20000[155]

ISO / IEC 20000 is the first international standard for IT service management. It was developed in 2005 by ISO / IEC JTC1 SC7 and subsequently updated in 2011 and 2018. Formally: ISO / IEC 20000-1: 2018 ('part 1'- service management system requirements) includes "design, transition, delivery and improvement of services that meet service requirements and value for both the customer and the service provider This part of the ISO / IEC 20000 requires an integrated process approach when the service manager plans, defines, implements, manages, monitors, revises, maintains and improves the service management system (SMS). "
It has been devised for IT services and is the reference standard for ITIL

7.6 Examples of Governance and Smart cities

7.6.1 Singapore

Singapore is an important example of effort aimed to transform a city in a Smart City and then in a Smart Nation, thanks to its peculiar characteristic of being a state composed by one city.

At the beginning (2016) Singapore was at its early stage of building their unique version of Smart City. Although several different masterplans in previous years have introduced polices that utilize information technology, the Smart City initiative originated from Smart Nation Vision established in 2014.
The Singapore Smart Nation Initiative has been studied and presented in many occasions; the relation between technology and governance has been investigated by J.J. Woo. [156]

Since then Singapore government had refined and progressed in its very complex program based on the three pillars of Digital Economy, Digital Government and Digital Society [157]

In Transforming Singapore [158] there is a more detailed update of the project that include aspects like: *Open Data; Living Laboratory, Industry and start up ecosystem; Cybersecurity and Data Privacy, Computational Capabilities and Digital Inclusion; Cross-border Collaboration with ASEAN Smart cities network.*

[156] J.J.Woo, “Technology and Governance in Singapore’s Smart Nation Initiative” Harvard Kennedy School 2018 https://ash.harvard.edu/files/ash/files/282181_hvd_ash_paper_jj_woo.pdf

[157] https://www.smartnation.sg/why-Smart-Nation/pillars-of-smart-nation#sthash.OVUZfTc7.dpuf

[158] https://www.smartnation.sg/why-Smart-Nation/transforming-singapore

An updated (December 2018) picture of the project is given in figure 30

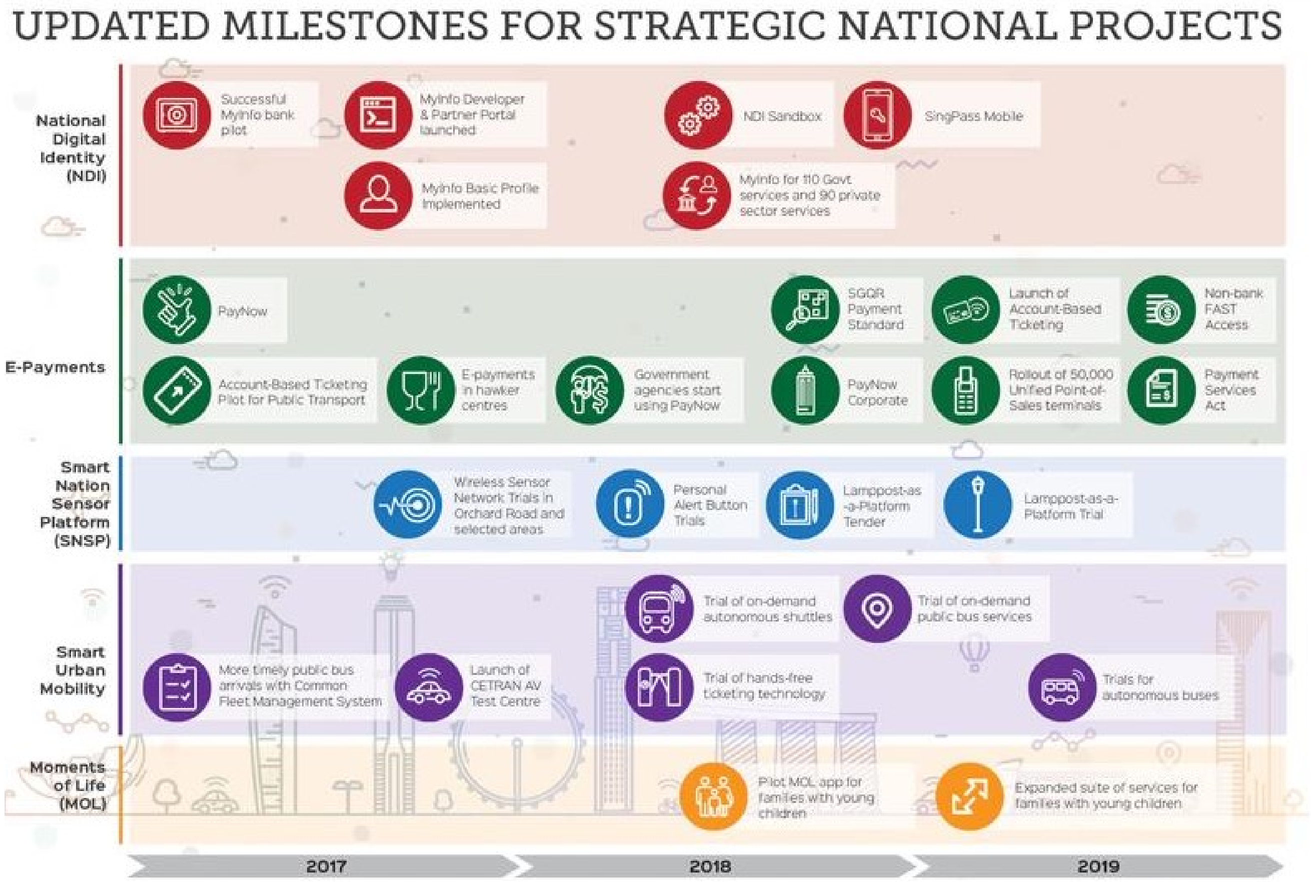

UPDATED MILESTONES FOR STRATEGIC NATIONAL PROJECTS
National Digital Identity (NDI)
Successful MyInfo bank pilot
MyInfo Developer & Partner Portal launched
NDI Sandbox
SingPass Mobile
MyInfo Basic Profile Implemented
MyInfo for 110 Govt services and 90 private sector services
E-Payments
PayNow
SGQR Payment Standard
Launch of Account-Based Ticketing
Non-bank FAST Access
Account-Based Ticketing Pilot for Public Transport
E-payments in hawker centres
Government agencies start using PayNow
PayNow Corporate
Rollout of 50,000 Unified Point-of-Sales terminals
Payment Services Act
Smart Nation Sensor Platform (SNSP)
Wireless Sensor Network Trials in Orchard Road and selected areas
Personal Alert Button Trials
Lamppost-as-a-Platform Tender
Lamppost-as-a-Platform Trial
Smart Urban Mobility
Trial of on-demand autonomous shuttles
Trial of on-demand public bus services
More timely public bus arrivals with Common Fleet Management System
Launch of CETRAN AV Test Centre
Trial of hands-free ticketing technology
Trials for autonomous buses
Moments of Life (MOL)
Pilot MOL app for families with young children
Expanded suite of services for families with young children
2017
2018
2019

Figure 30. Updated schedule of Singapore Smart Nation Project

(Source:https://www.smartnation.sg/why-Smart-Nation/transforming-singapore)

7.6.2 City of Bergamo

An example of initial steps on the way of becoming a Smart City is the small Italian town of Bergamo (Northern Italy). The town started its path to a Smart City with the realization of 7 smart squares and the completion of the city WIFI coverage. The important intervention concerns the construction of 7 smart squares in the suburbs. Digital squares will be areas available to citizens where there will be benches with charging points devices, 153 smart bins, water sensors, environmental and green monitoring sensors, interactive information totems.

The project also includes the extension of the WIFI service and the completion of various city routes that will be covered by the connectivity service: parks, libraries, aggregation centres, pedestrian areas, the entire upper city and Astino[159]. Smart services will be activated through the specialized network LORA that will handle IOT services; this network is already available in main cities of Lombardia (Northern Italy)

[159] http://www.a2asmartcity.io/2018/09/03/bergamo-piazze-smart/

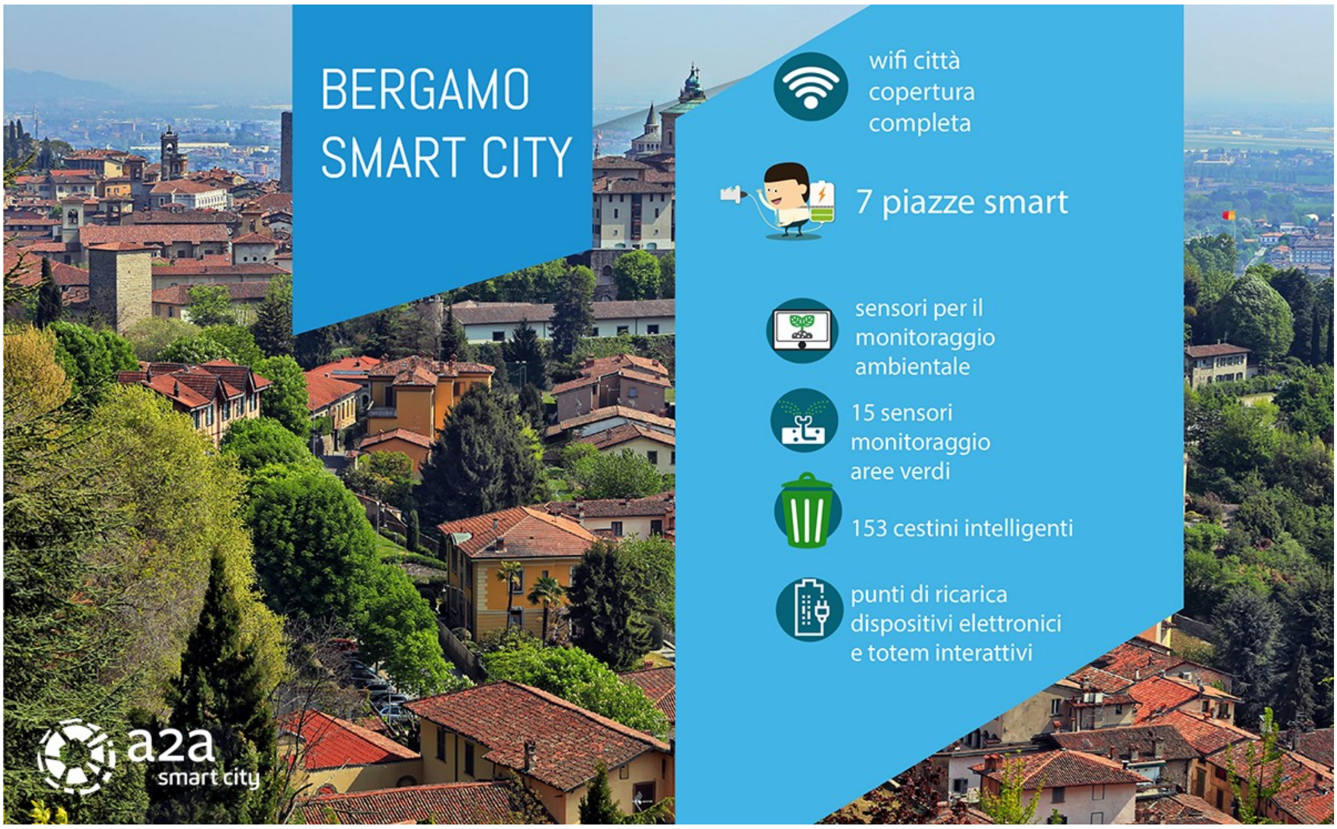

BERGAMO
SMART CITY
wifi città copertura completa
7 piazze smart
sensori per il monitoraggio ambientale
15 sensori monitoraggio aree verdi
153 cestini intelligenti
punti di ricarica dispositivi elettronici e totem interattivi
a2a smart city

Figure 31. City of Bergamo

(Source: A2A Smart City, 2018)

7.6.3 COBIT 5 for Smart City Governance

A demonstrative study on how COBIT5, the governance framework of ISACA can be used for Smart and Sustainable Cities "*Using COBIT 5 to Get and Give Board Support for Revolutionizing Cities* "was published in [160]Isaca Journal n.5 (2018) by Graciela Braga.

The author shows how to integrate COBIT 5 strategic goals with others taken from international organizations like by the International Telecommunication Union (ITU) and the Organisation for Economic Co-operation and Development (OECD) and build up also appropriate metrics. One relevant point is that COBIT 5 goals and metrics are ICT oriented and must be integrated with other focused on social, economic and environmental aspects.

In this way COBIT 5 can be used for the governance of IT aspects of the transition to Smart and Sustainable City and can be also helpful in other sectors.

[160] G. Braga"*Using COBIT 5 to Get and Given Board Support for Revolutionizing Cities*" -2018 ISACA JOURNAL https://www.isaca.org/Journal/archives/2018/Volume-5/Pages/using-cobit-5-to-get-and-give-board-support-for-revolutionizing-cities.aspx

8 Cyber supply chain risk management for Smart Cities' critical information infrastructures (*Luigi Carrozzi*)

8.1 The hyperconnected urban environment of Smart Cities

Today urban areas are evolving in Smart Cities through development of several intelligent services largely based on technical infrastructures that are required to provide highly performant on-demand and reliable services to citizens. If Smart Cities largely depend on critical infrastructures essential services (energy, transportation, water, oil, gas, health, emergency services, etc.) we may assume that the applications that made "smart" such services within the urban circle are also worth, as the same, to be considered as "critical" and hence protected accordingly to the importance they have for that community.

In details the use of last generation networks, the massive use of intelligent devices in public and private infrastructures, the remarkable potential due to the convergence of IOT, Industrial IOT, Big Data, distributed ledger and Artificial intelligence technologies lead to face unprecedented challenges in safety, security and privacy of population. Hugh Boyes, Roy Isbell, and Tim Watson in their paper "*Critical Infrastructure in the Future City - Developing Secure and Resilient Cyber–Physical Systems*"[161] after introducing the concept of Cyber Physical System (CPS) write that:

"*There are a number of definitions of CPS. Common features effectively describe* ***control systems, networked and/or distributed, incorporating a degree of intelligence (adaptive or predictive), and work in real time to influence outcomes in the real world.*** *These definitions point to the diverse nature of CPS found in transportation, utilities, buildings, infrastructures, manufacturing, and health care*"

and point out that:

*"**Critical infrastructure systems are CPS**, whose failure would have economic or social impact. Society expects systems will operate in a safe, secure and consistent manner. In response to environmental, demographic and societal pressures, cities may no longer conduct business as usual. **Traditional city models are no longer appropriate,** as transport and utility infrastructures become unsustainable and require significant investment. **Some cities have embraced the concept of the 'city as a platform', a hyperconnected urban environment that harnesses the network effects, openness, and agility of the real-time web.** The focus has been on access to data, leading to development of smartphone apps and portals allowing citizens to 'connect' with city services and institutions"*

In their work the authors introduce a "Framework for secure and resilient Future Cities" where Cyber security is a primary component of the framework as shown in the following picture.

[161] Critical Infrastructure in the Future City Developing Secure and Resilient Cyber–Physical Systems -Hugh Boyes, Roy Isbell, and Tim Watson - Cyber Security Centre, WMG, University of Warwick, Coventry, UK https://pdfs.semanticscholar.org/2cee/ac14446c06398cdfad176a4e676d5fac7825.pdf?_ga=2.77406805.1360114604.1550667396-200007173.1536666350

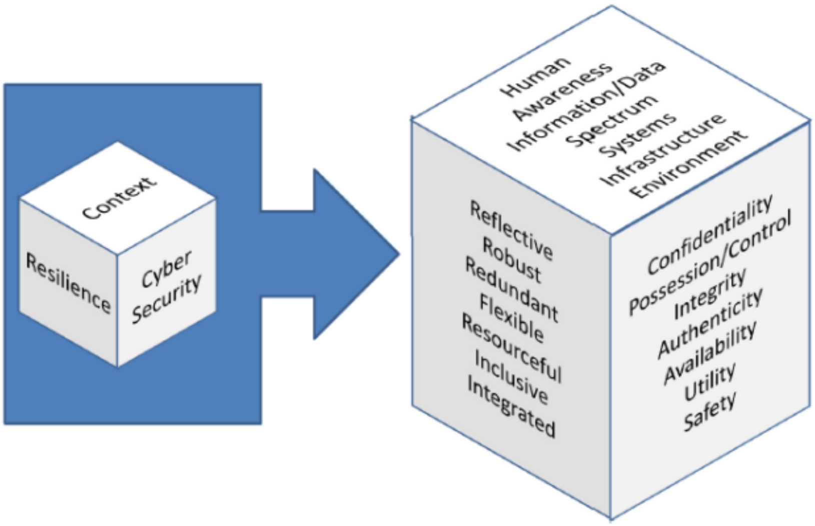


Figure 32. Analysis Framework for secure and resilient Future Cities
(*Source: Hugh Boyes, Roy Isbell, Tim Watson Critical Infrastructure in the Future City - Developing Secure and Resilient Cyber–Physical Systems)*

8.2 Securing supply chains

Evaluating supply chain cyber risk

Supply chain management typically implies a sourcing strategy being aware that a fully integrated lifecycle approach to the product/services is recommended. NIST SP800-53[162] defines Supply Chain as "*Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer*"

In cybersecurity an aspect whose importance is often underestimated is to provide a secure supply chain to systems. There is a large literature on procurement management and supply chains. The design of a product or a service generally implies an adequate overall control of the procurement process, but this becomes essential in case of cyber systems providing critical services for example to a Smart City and the evaluation of the supply chain risk is a primary activity.

[162] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

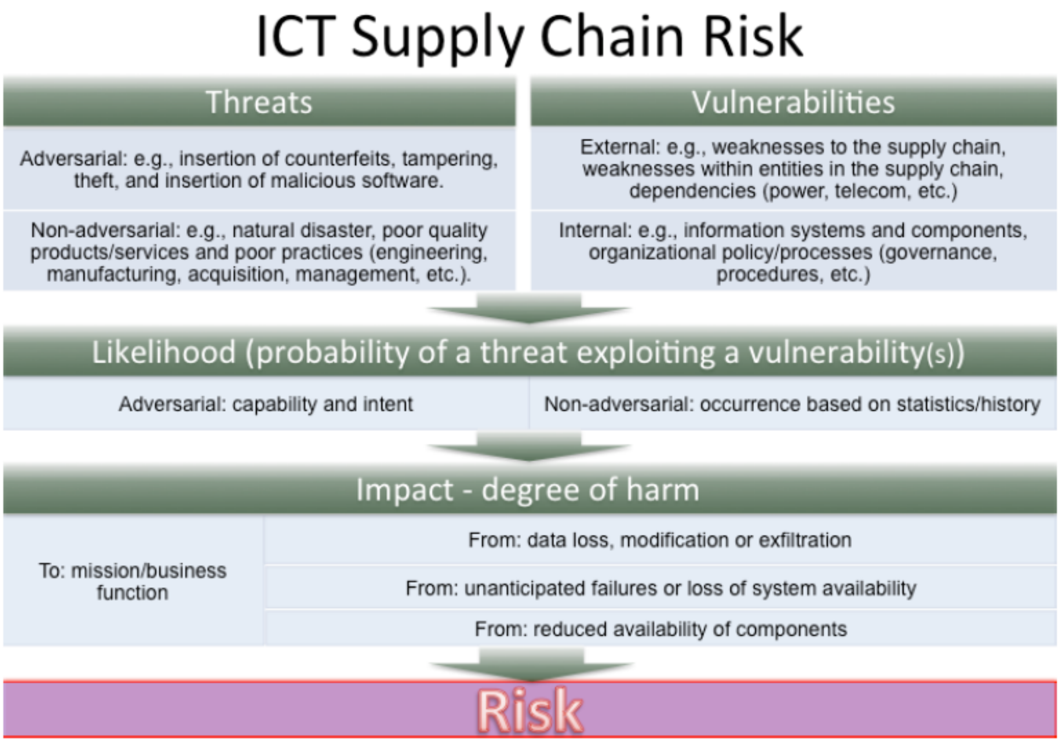

ICT Supply Chain Risk
Threats
Vulnerabilities
Adversarial: e.g., insertion of counterfeits, tampering, theft, and insertion of malicious software.
External: e.g., weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, telecom, etc.)
Non-adversarial: e.g., natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc.).
Internal: e.g., information systems and components, organizational policy/processes (governance, procedures, etc.)
Likelihood (probability of a threat exploiting a vulnerability(s))
Adversarial: capability and intent
Non-adversarial: occurrence based on statistics/history
Impact - degree of harm
To: mission/business function
From: data loss, modification or exfiltration
From: unanticipated failures or loss of system availability
From: reduced availability of components
Risk

Figure 33. ICT Supply Chain Risk

(Source: NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations[163])

According to NIST[164] Cyber supply chain include risks from:

- *third party service providers or vendors - from janitorial services to software engineering - with physical or virtual access to information systems, software code, or IP,*
- *poor information security practices by lower-tier suppliers,*
- *compromised software or hardware purchased from suppliers,*
- *software security vulnerabilities in supply chain management or supplier systems,*
- *counterfeit hardware or hardware with embedded malware,*
- *third party data storage or data aggregators;*

and the best practices adopted by organizations to manage their cyber supply chain risks are the following:

- *Security requirements are included in every RFP and contract.*
- *Once a vendor is accepted in the formal supply chain, a security team works with them on-site to address any vulnerabilities and security gaps.*
- *"One strike and you're out" policies with respect to vendor products that are either counterfeit or do not match specification.*
- *Component purchases are tightly controlled; component purchases from approved vendors are pre-qualified. Parts purchased from other vendors are unpacked, inspected, and x-rayed before being accepted.*

[163] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[164] NIST Best Practices in Cyber Supply Chain Risk Management - Conference Materials – Cyber Supply Chain Best Practices https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

- *Secure Software Lifecycle Development Programs and training for all engineers in The life cycle are established.*
- *Source code is obtained for all purchased software.*
- *Software and hardware have a security handshake; secure booting processes look for authentication codes and the system will not boot if codes are not recognized.*
- *Automation of manufacturing and testing regimes reduces the risk of human intervention.*
- *Track and trace programs establish provenance of all parts, components and systems.*
- *Programs capture "as built" component identity data for each assembly and automatically links the component identity data to sourcing information.*
- *Personnel in charge of supply chain cybersecurity partner with every team that touches any part of the product during its development lifecycle and ensures that cybersecurity is part of suppliers' and developers' employee experience, processes and tools.*
- *Legacy support for end-of-life products and platforms; assure continued supply of authorized IP and parts.*
- *Tight controls on access by service vendors are imposed. Access to software is limited to a very few vendors. Hardware vendors are limited to mechanical systems with no access to control systems. All vendors are authorized and escorted.*
-

It's clear that the higher is the complexity of the system (i.e. of number of providers, supply chain elements, systems architecture characteristics, etc.) the wider is the attack surface of the system and hence the likelihood to suffering a "supply chain attack"[165] that is the attack to the system occurring through a compromised third party involved in the supply chain. The following picture[166] gives a description of such type of attack in case of software supplies.

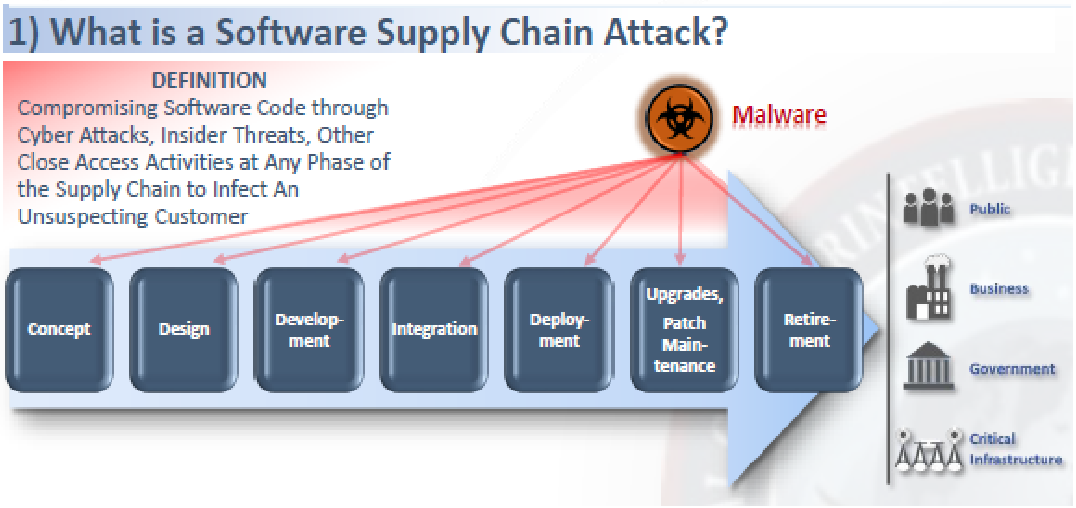

1) What is a Software Supply Chain Attack?
DEFINITION
Compromising Software Code through Cyber Attacks, Insider Threats, Other Close Access Activities at Any Phase of the Supply Chain to Infect An Unsuspecting Customer
Malware
Concept
Design
Develop-ment
Integration
Deploy-ment
Upgrades, Patch Main-tenance
Retire-ment
Public
Business
Government
Critical Infrastructure

Figure 34. Software Supply Chain Attack
(Source NIST-CSRC)

It's also worth of mention that a relevant dimension characterizing the complexity of sourcing activities typical of the hyperconnected context of Smart Cities is related to the involvement of providers and sub-providers of supply chains.

[165] The supply chain attack is also known as "value-chain attack" or "third-party attack"

[166] https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf

As mentioned by NIST[167]:
*"**ICT supply chain risks** are associated **with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed**. They are also associated with the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services"*

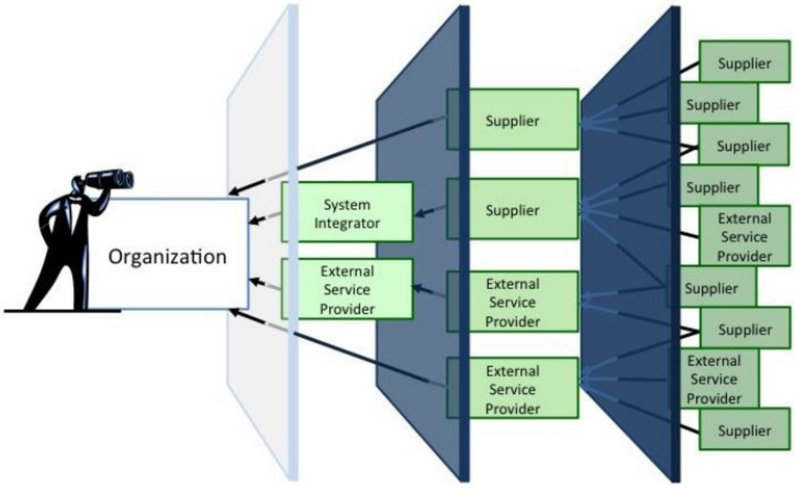

Organization
System Integrator
External Service Provider
Supplier
Supplier
External Service Provider
External Service Provider
Supplier
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
External Service Provider
Supplier

Figure 35 An Organization's Visibility, Understanding, and Control of its ICT Supply Chains
(Source: NIST Special Publication 800-16. Supply Chain Risk Management Practices for Federal Information Systems and Organizations)

Supply chain and personal data protection

As described in the following chapter Smart Cities services may involve massive processing of personal data. In this case GDPR[168] applies and the relations between *Controller*[169] and *Processor*[170] in contract of services are regulated by article 28 – Processor – that in the first three paragraphs provides as follows:

1.Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2.The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

[167] *NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
[168] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[169] Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (GDPR, art. 4)).
[170] Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR, art. 4)).

3.Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [...]

Furthermore Recital 78 provides that:
[...] The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

So, it's clear that in supply chain management compliance to GDPR entails at least: an accurate procurement process by the organization in terms of selection of the service provider (requiring competence and technical capabilities on data protection),

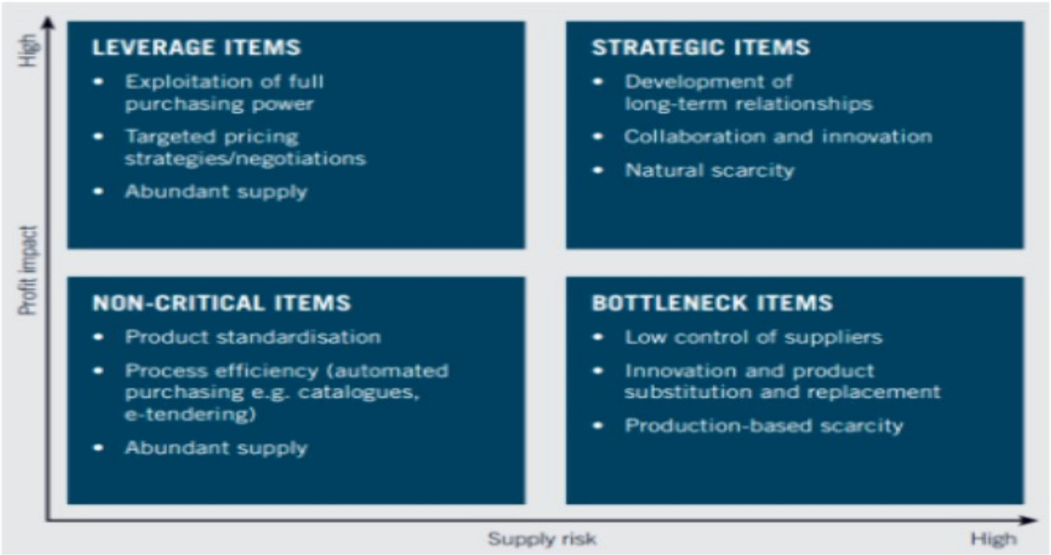
- control (knowledge and authorization) of sub-providers,
- specific data protection contractual clauses,
- requirement of "privacy by design and by default" principle in public tenders

8.3 Critical infrastructures protection: the role of procurement engineering and the supply chain management

Strategic Supplies and Supplier Relationship Management

The Kraljic Matrix is a tool that allows to classify the purchases of a company into four groups, based on the complexity of the supply market (low-high risk) and the importance of purchases determined by the impact in terms of economic returns (low-high profit impact). Based on this pair of variables four classes of supplies are identified:

- **Non-critical supplies**: they are characterized by a low impact on the company and with supplies stable in low-risk markets;
- **Supplies with "leverage effect"**: important for the company, but placed in low-risk markets;
- **Bottleneck supplies**: they are placed in markets with a certain level of risk of supply but with limited business impact;
- **Strategic supplies**: they are very important for the company's survival and market risk is very high.



LEVERAGE ITEMS
- Exploitation of full purchasing power
- Targeted pricing strategies/negotiations
- Abundant supply

STRATEGIC ITEMS
- Development of long-term relationships
- Collaboration and innovation
- Natural scarcity

NON-CRITICAL ITEMS
- Product standardisation
- Process efficiency (automated purchasing e.g. catalogues, e-tendering)
- Abundant supply

BOTTLENECK ITEMS
- Low control of suppliers
- Innovation and product substitution and replacement
- Production-based scarcity

Figure 36. The Kraljic Matrix
(Source: Kraljic Matrix - Harvard Business Review)

In critical infrastructures the production output may have a relevant impact not only on the business for the company but also in terms of interruption or degradation of essential services to the population or to other critical infrastructures dependent by those services (case of interdependent critical infrastructures: e.g. telecommunications industry dependence from energy sector)[171]. Moreover, these infrastructures typically have highly complex supply chains with providers of very specific, high value, and "customized" items that makes them "high risky" supplies. So according to the Kraljic Matrix we may allocate these supplies on the top-right quadrant of "strategic supplies". In this case the development of strategic partnership and long-term relationships with suppliers should be crucial for these companies. A sound suppliers management system is necessary where, among others, performances are measured and evaluated in order to control and report the risks arising from those contracts of product or services. Moreover, a robust "supply incident management" process should be put in place to manage problems that may arise on the supply chain. In the following is introduced a model for the governance of the supply chains.

The supply chain operations reference model (SCOR)

The supply chain operations reference model (SCOR)[172] is a management framework used to take supply chain management decisions within a company and with suppliers and customers of a company. The model describes the business processes along the entire supply chain and provides basis for improve those processes.

SCOR is based on six management processes: Plan, Source, Make, Deliver, Return, and Enable

- ***Plan***– *Processes that balance aggregate demand and supply to develop a course of action which best meets sourcing, production, and delivery requirements.*
- ***Source***– *Processes that procure goods and services to meet planned or actual demand.*
- ***Make***– *Processes that transform product to a finished state to meet planned or actual demand.*
- ***Deliver***– *Processes that provide finished goods and services to meet planned or actual demand, typically including order management, transportation management, and distribution management.*
- ***Return***– *Processes associated with returning or receiving returned products for any reason. These processes extend into post-delivery customer support.*
- ***Enable***– *Processes being associated with the management of the supply chain. These processes include management of business rules, performance, data, resources, facilities, contracts, supply chain network management, managing regulatory compliance and risk management.*

[171] Luigi Carrozzi "*Procurement Management per la protezione delle infrastrutture critiche*" - Università degli studi di Roma Tor Vergata – June 2009

[172] http://www.apics.org/apics-for-business/frameworks/scor

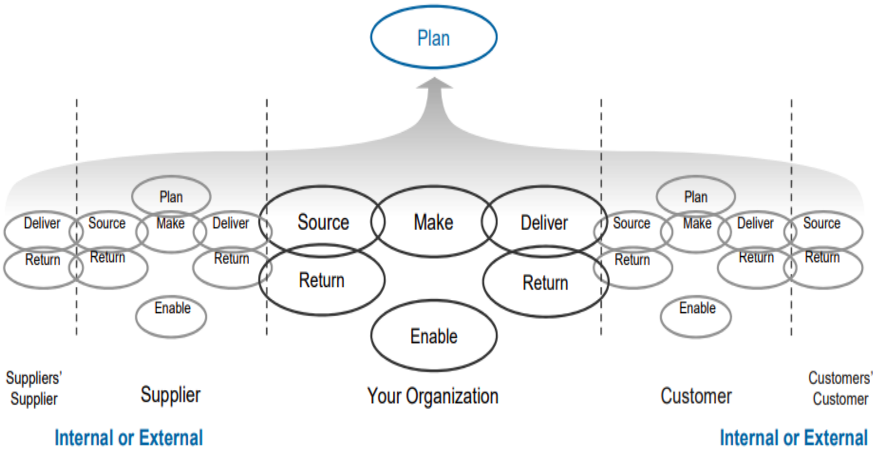


Figure 37. The SCOR Process Model

(Source: Supply Chain Operations Reference Model - Supply Chain Council)

This model may be used to describe supply chain using these processes building blocks and applies both to very simple and very complex supply chains using a common set of definitions. Having a sound model of the supply chain helps organizations to have in depth-knowledge of sourcing processes enabling risk management and optimization of the whole sourcing strategy.

9 Personal data protection and the ethic challenge of Artificial Intelligence systems *(Luigi Carrozzi)*

9.1 Personal data protection: a citizen's right

In a previous publication of AIIC[173] we introduced the matter of personal data protection when processing BIG data Analytics. IoT and IIOT (Industrial IOT) are potential massive sources of personal data. When we use a sport tracker App, drive a car, interact with smart devices at home, use healthcare, energy or transportation services, some information about us may be made available, collected and processed for different purposes (provide the services itself, enhance their quality, deal with customer preferences through profiling, manage faults and security of infrastructures, etc.) obtaining detailed high value information, analytics and insights using the processing power of Big data technology. IOT, IIOT and Big Data may be considered "enabling technologies" for a large variety of Smart Cities application from general municipal services, public safety, security and crime prevention to any potential "smart" service deployable in almost all sectors of city life (energy, transportation, road traffic, buildings, etc.). When designing Smart Cities services, it's necessary to be aware that if any personal data processing may occur, specific and adequate safeguards are to be implemented in order to protect identity, dignity, freedom and self-determination of the of individuals involved, compliantly to the applicable legislation.

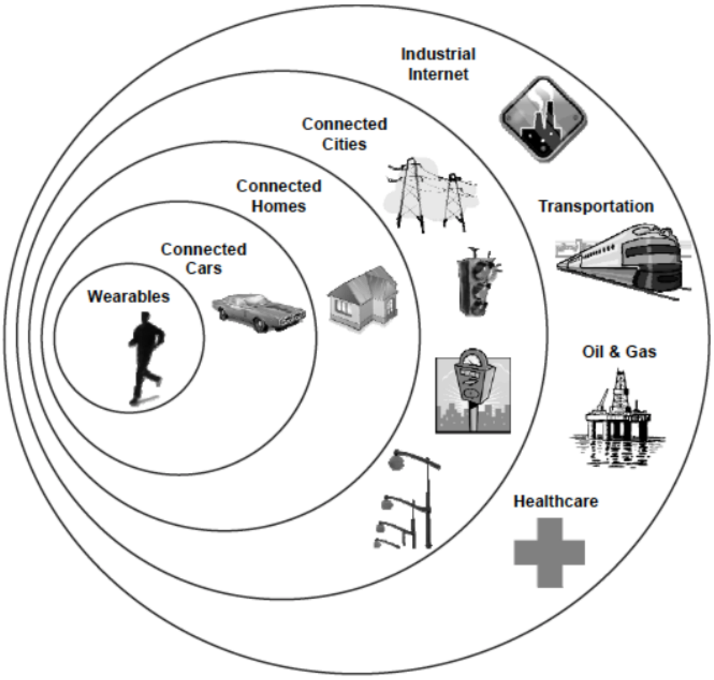


Figure 38. The IoT landscape

(Source: Goldman Sachs - The Internet of Things: Making sense of the next mega-trend)

[173] AIIC- *Good Practices and Recommendations on the use of Big Data Analytics for Critical Infrastructure Resilience*. http://www.infrastrutturecritiche.it/new/media-files/2018/04/AIIC_BigDataCIPR_FINALE.pdf

According to the EU General Data Protection Regulation (GDPR)[174] personal data defined as "any information relating to an identified or identifiable natural person"[175] are to be suitably protected in order to respect freedom and rights of individuals. Since data are considered the new oil of the economy[176] it's important to strike the balance between the free flow of personal data and their protection. On this point Recital 6 of GDPR states:

"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data".

The "high level of protection" is required to counterweight the risks for natural persons that occur when their personal data are processed.

GDPR at article 5 states the "Principles" relating to the processing of personal data:

- **lawfulness, fairness and transparency** - personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data;
- **purpose limitation** - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- **data minimization** - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **accuracy -** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- **storage limitation** - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- **integrity and confidentiality** - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Furthermore, the same article introduces the principle of "Accountability"[177], that is the Controller shall be responsible for, and be able to demonstrate compliance with those principles. The accountability implies that organizations are not only required to adhere to the above-mentioned principles but must also demonstrate compliance. This means to adopt a proper personal data protection management system to implement appropriate and effective technical and

[174] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[175] "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person ((GDPR, art. 4)).

[176] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[177] GDPR at art. 24 envisages the "Responsibility of the Controller"

organizational measures based on a sound risk analysis for rights and freedom of natural persons and other specific measures explicitly provided by GDPR such as, among others, provide documented processes and policies, carry out a Data Protection Impact Assessments (DPIA), Data Protection by Design and by Default, designate the Data Protection Officer (DPO), maintain a Records of processing activities, manage personal Data Breaches under GDPR provisions.

In details GDPR at article 32 provides prescriptions for the "Security of processing". The Controller and the Processor should perform a risk assessment for rights and freedoms of natural persons and implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In performing risk assessment it's recommended to take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed; GDPR Recital 75 provides a description of major impacts on natural persons:
"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects".

9.2 Cities made smarter by the use of Artificial Intelligence: the "win- win" approach with personal data protection

Artificial Intelligence (AI) systems are designed to improve efficiency, enable new business opportunities, enhance capabilities to generate value in all sectors of the economy and improve the quality of life of citizens. Smart Cities may take significate advantages from this technology in several critical city-life applications[178]. As a matter of fact, there is a remarkable growth of "intelligent systems" developed to support fundamental services such as transportation, mobility management, traffic control, public safety, energy systems and other relevant city management functions.

At the same time high concerns rise on protection of rights, dignity, self-determination and freedom of people. It's important to be aware of such relevant threats in order to identify possible solutions able to prevent harms to individuals thus adopting that "win-win" approach able to combine AI based Smart City applications and personal data protection.

All the potential provided by any AI system must be exploited in order to get beneficial output for individuals and society minimizing the drawbacks such as discrimination, unfairness, inaccuracy and bias when processing personal data. AI applications for Smart Cities may be able to combine IoT and IIOT, big data, geographic information system, video and other sources of information.

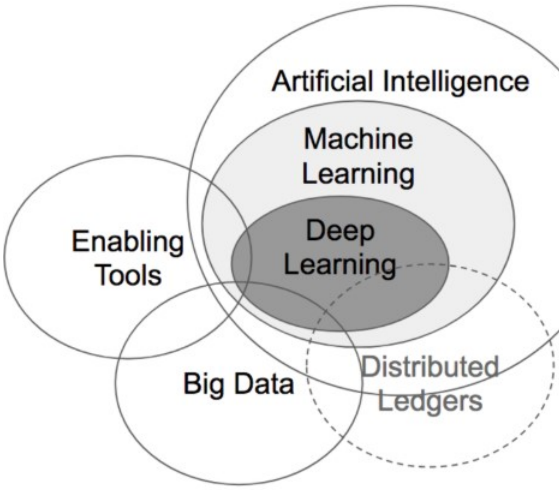


Figure 39. How AI is helping Cities get smarter

(Source: Tom Vander Ark: How Cities Are Getting Smart Using Artificial Intelligence[179])

Intelligent systems may process and correlate biometric data, position data, characteristics of services usage and other relevant data that may profile personal preferences and habits of citizens. AI applications of video surveillance may enable facial recognition and human behavior understanding. The role to form judgment and take consequent decisions to support human activities may be given. to artificial intelligence and autonomous systems, powered by machine learning and deep learning capabilities and fed from large sets of input data.

It's important to be aware that if AI based applications may provide very remarkable value to citizens, local authorities and city managers, at the same time they shall not be harmful to people.

[178] Examples of application of AI in smart cities can be found in the following links:
https://emerj.com/ai-sector-overviews/smart-city-artificial-intelligence-applications-trends/
https://www.automotiveworld.com/articles/artificial-intelligence-in-smart-cities-whats-the-link/

[179] https://www.forbes.com/sites/tomvanderark/2018/06/26/how-cities-are-getting-smart-using-artificial-intelligence/#1bfcf2d93803

Let's see in the following what are the main risks for individuals and how GDPR may apply to AI systems.

- AI applications may collect and process personal data only for specified, explicit and legitimate purposes and not further processes in a manner that is incompatible with those purposes. As provided by Recital 50 of GDPR, "*the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected*." Do not comply to those provisions means infringe the GDPR principle of "purpose limitation".
- Artificial intelligence systems may require collection and processing of huge amounts of personal data not necessary for the application's specific purposes. This may expose data subjects to undue personal data processing and infringe the principle "data minimization". And if those data are stored for an undue period the "storage limitation" principle is also violated.
- AI applications providing profiling and automated decision-making may be biased, unfair, discriminatory for individuals and groups and induce in judgment or actions deemed "faulty" due, for example, to an incorrect algorithmic design. On this issue it's worth to mention that GDPR article 22 provides specific limitations in case of automated individual decision-making, including profiling: at paragraph 1, it provides that *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".*
- Machine learning applications need large amounts of data "to train" the algorithms; concerns in this case rise for the quality of training data: any inaccuracy of the input data may induce distortion in the AI system outputs and in case of personal data this may infringe the principle of data "accuracy".
- The inner logic of algorithms processing personal data may be opaque to individual. "Black boxes" are not acceptable according to the principle of "transparency". Data subjects should have the right to know the logic applied in processing personal data, and that those data shall be processed "lawfully" and "fairly".

Cybersecurity is a key issue for AI systems. Integrity, availability, confidentiality and resilience of artificial intelligence and autonomous systems are to be provided according to specific risk for everyone, group and the whole community involved. The provisions of article 32 "Security of Processing" and article 25 "Data protection by design and by default" need to become solid engineering best practices. The compliance to GDPR provisions which implies deploying safe and secure systems provides also the opportunity to seize business opportunities and to serve properly our communities with best-in-class technologies, respectful of human rights.

The Council of Europe[180] (CoE) is the continent's leading human rights organization that includes 47-member states, 28 of which are members of the European Union. It's worth of note that on 28 January 2019 the Consultative Committee of the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108) of CoE has published "*Guidelines on Artificial Intelligence and Data Protection*"[181]. The guidelines aim to assist policy makers, artificial intelligence developers, manufacturers and service providers in ensuring that AI applications do not undermine the right to data protection.

[180] https://www.coe.int/en/

[181] https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

9.3 Embedding Ethics and data protection in Artificial intelligence and autonomous system

Taking decisions on what is good and bad for humans implies aligning to a system of moral principles. Artificial intelligence and autonomous systems need to embed ethics to be fully supportive to human being. Several initiatives have recently flourished on the issue of ethics in artificial intelligence trying to identify principles and recommendations for development of AI respectful of human beings. Here follows some of these initiatives whose results should be carefully considered both by designers and policy makers in developing AI based Smart Cities services.

9.3.1 The AI4Peoples's core opportunities and risk of AI and the five ethical principles

AI4People, an Atomium - European Institute for Science, Media and Democracy initiative[182], designed to lay the foundations for a "Good AI Society" in his White Paper[183] introduces:

- the core opportunities and risks of AI for society,
- five ethical principles as a framework,
- recommendations, including 20 action points for a "Good Society".

Let's consider the following table:

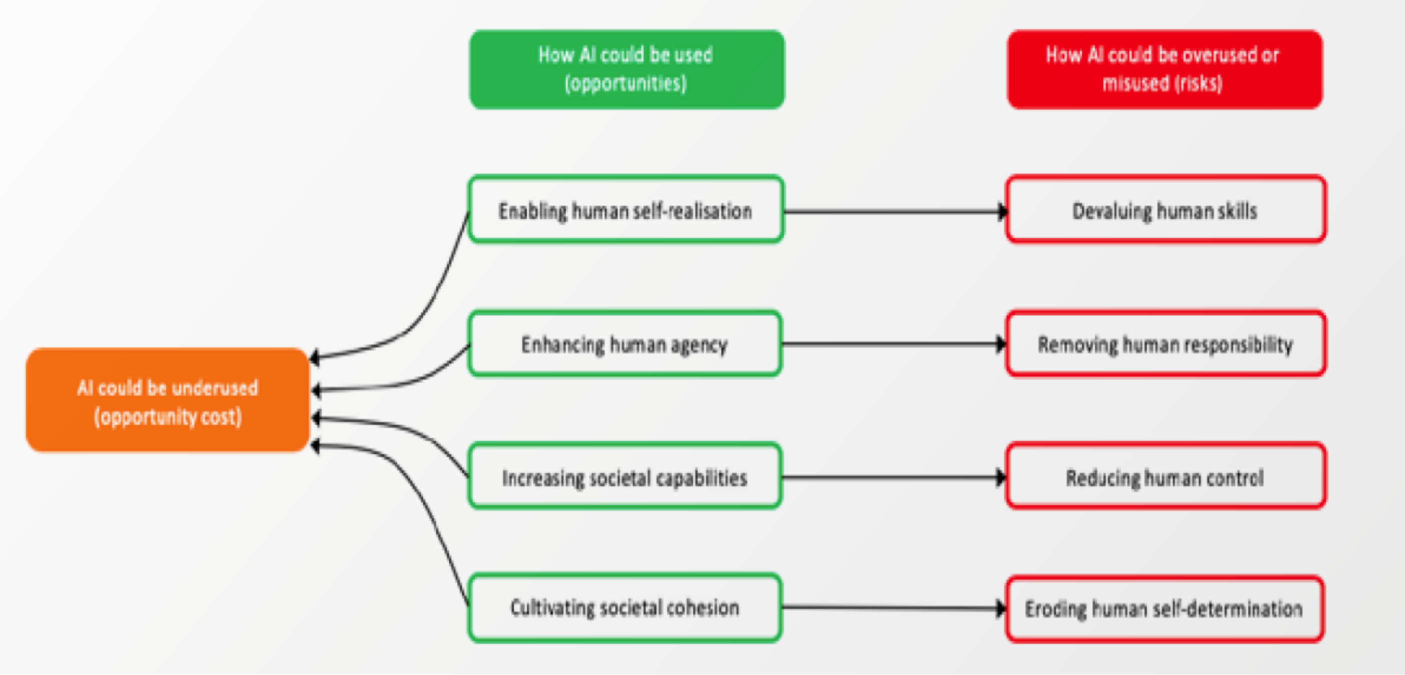

How AI could be used (opportunities)
How AI could be overused or misused (risks)
Enabling human self-realisation
Devaluing human skills
Enhancing human agency
Removing human responsibility
Increasing societal capabilities
Reducing human control
Cultivating societal cohesion
Eroding human self-determination
AI could be underused (opportunity cost)

Figure 40. Opportunities and Risks of AI for Society

(Source: AI 4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations)

[182] Atomium European Institute - http://www.eismd.eu/

[183] "AI 4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations" http://www.eismd.eu/wp-content/uploads/2019/02/Ethical-Framework-for-a-Good-AI-Society.pdf

Opportunities and risks, as here exposed, lead to the consideration that once identified the beneficial outputs and appropriately estimate related risks, AI systems developers should recognize the “Privacy and Ethics by Design” as the leading approach to deploy, on a global scale, beneficial AI applications. AI industry is expected to put in place an aware, preventive approach embedding ethics and data protection since from the design phase to fully exploit benefits of such technology, minimizing the risk and enabling the necessary trust of users’ community.

AI4People identifies the “ethical framework for a Good IA Society” based on the following Principles:

- **Beneficence**: promoting well-being, preserving dignity, and sustaining the planet
- **Non-maleficence**: privacy, security and “capability caution”
- **Autonomy**: the power to decide (whether to decide)
- **Justice**: promoting prosperity and preserving solidarity
- **Explicability:** enabling the other principles through intelligibility and accountability

These are to be considered tightly concurrent principles explicating how to design beneficial AI system maximizing user value while limiting the risks of drawbacks.

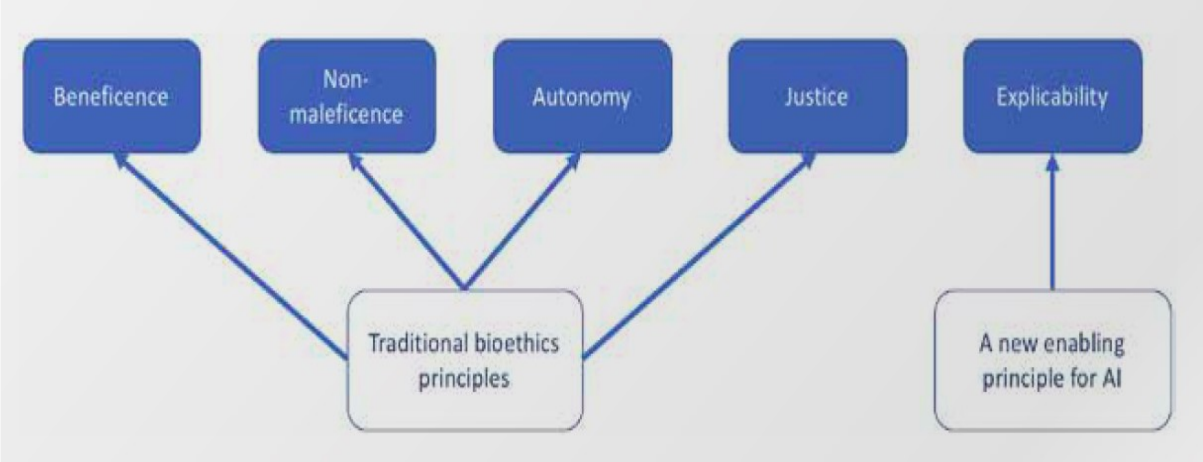

Beneficence
Non-maleficence
Autonomy
Justice
Explicability
Traditional bioethics principles
A new enabling principle for AI

Figure 41. An Ethical Framework for AI

Source: AI 4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations

And here follows the 20 action points.

Assessment

1. Assess the capacity of existing institutions, such as national civil courts, to redress the mistakes made or harms inflicted by AI systems.
2. Assess which tasks and decision-making functionalities should not be delegated to AI systems.

3. Assess whether current regulations are sufficiently grounded in ethics to provide a legislative framework that can keep pace with technological developments.

Development

4. Develop a framework to enhance the explicability of AI systems which make socially significant decisions.
5. Develop appropriate legal procedures and improve the IT infrastructure of the justice system to permit the scrutiny of algorithmic decisions in court.
6. Develop auditing mechanisms for AI systems to identify unwanted consequences, such as unfair bias, and (for instance, in cooperation with the insurance sector) a solidarity mechanism to deal with severe risks in AI intensive sectors.
7. Develop a redress process or mechanism to remedy or compensate for a wrong or grievance caused by AI.
8. Develop agreed-upon metrics for the trustworthiness of AI products and services, to be undertaken either by a new organisation, or by a suitable existing organisation. These metrics would serve as the basis for a system that enables the user-driven benchmarking of all marketed AI offerings.
9. Develop a new EU oversight agency responsible for the protection of public welfare through the scientific evaluation and supervision of AI products, software, systems or services.
10. Develop a European observatory for AI.
11. Develop legal instruments and contractual templates to lay the foundation for a smooth and rewarding human-machine collaboration in the work environment.

Incentivisation

12. Incentivise financially, at the EU level, the development and use of AI technologies within the EU that are socially preferable (not merely acceptable) and environmentally friendly (not merely sustainable but favourable to the environment).
13. Incentivise financially a sustained, increased and coherent European research effort.
14. Incentivise financially cross-disciplinary and cross-sectoral cooperation and debate concerning the intersections between technology, social issues, legal studies, and ethics.
15. Incentivise financially the inclusion of ethical, legal and social considerations in AI research projects. In parallel, incentivise regular reviews of legislation to test the extent to which it fosters socially positive innovation.
16. Incentivise financially the development and use of lawfully de-regulated special zones within the EU for the empirical testing and development of AI systems.
17. Incentivise financially research about public perception and understanding of AI and its applications, and the implementation of structured public consultation mechanisms to design policies and rules related to AI.

Support

18. Support the development of self-regulatory codes of conduct for data and AI related professions, with specific ethical duties.
19. Support the capacity of corporate boards of directors to take responsibility for the ethical implications of companies' AI technologies.
20. Support the creation of educational curricula and public awareness activities around the societal, legal, and ethical impact of Artificial Intelligence.

9.3.2 The Asilomar Principles – Future of Life institute

The Future of Life Institute[184] has his mission in "*catalyze and support research and initiatives for safeguarding life and developing optimistic visions of the future, including positive ways for humanity to steer its own course considering new technologies and challenges*".

Among the 23 principles on Artificial Intelligence[185] developed in conjunction with the 2017 Asilomar conference in order "*to empower people in decades and centuries ahead*", in relation to "Ethics and Values", are mentioned the following principles:

- ***Safety****: AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.*
- ***Failure Transparency****: If an AI system causes harm, it should be possible to ascertain why.*
- ***Judicial Transparency****: Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.*
- ***Responsibility****: Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.*
- ***Value Alignment****: Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.*
- ***Human Values****: AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.*
- ***Personal Privacy****: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.*
- ***Liberty and Privacy****: The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.*
- ***Shared Benefit****: AI technologies should benefit and empower as many people as possible.*
- ***Shared Prosperity****: The economic prosperity created by AI should be shared broadly, to benefit all of humanity.*
- ***Human Control****: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.*
- ***Non-subversion****: The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.*
- ***AI Arms Race****: An arms race in lethal autonomous weapons should be avoided.*

9.3.3 The IEEE Standards Association "Ethically Aligned Design"

IEEE, the Institute of Electrical and Electronic Engineers[186] is recognized as "the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity with over 420.000 members in more than 160 countries".

[184] https://futureoflife.org/

[185] https://futureoflife.org/ai-principles/

[186] https://www.ieee.org/

IEEE launched the “Global Initiative on Ethics of Autonomous and Intelligent Systems” and published the second version of “*Ethically aligned design - A vision for prioritizing human well-being with autonomous and intelligent systems*”[187]

The mission of this IEEE initiative is:
“To ensure every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained, and empowered to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity”
where “stakeholder” is
“anyone involved in the research, design, manufacture, or messaging around intelligent and autonomous systems, including universities, organizations, governments, and corporations making these technologies a reality for society”

The ethical design, development, and implementation of these technologies should be guided by the following general principles:

- ***Human Rights***: *Ensure they do not infringe on internationally recognized human rights*
- ***Well-being***: *Prioritize metrics of well-being in their design and use*
- ***Accountability***: *Ensure that their designers and operators are responsible and accountable*

pursuing the following objectives:

- *Personal Data Rights and Individual Access Control*
- *Well-being Promoted by Economic Effects*
- *Legal Frameworks for Accountability*
- *Transparency and Individual Rights*
- *Policies for Education and Awareness*

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems reflects the inputs from 13 expert committees:

1. *General Principles*
2. *Embedding Values into Autonomous Intelligent Systems*
3. *Methodologies to Guide Ethical Research and Design*
4. *Safety and Beneficence of Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI)*
5. *Personal Data and Individual Access Control*
6. *Reframing Autonomous Weapons Systems*
7. *Economics/Humanitarian Issues*
8. *Law*
9. *Affective Computing*
10. *Policy*
11. *Classical Ethics in Autonomous and Intelligent Systems*
12. *Mixed Reality*
13. *Well-being*

[187] Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2. IEEE, 2017. http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.

9.3.4 The International Conference of Data Protection and Privacy Commissioners - "*Declaration on Ethics and Data Protection in Artificial Intelligence*"

The International Conference of Data Protection and Privacy Commissioners (ICDPPC)[188] has the objective to provide leadership at international level in data protection and privacy connecting the efforts of 122 privacy and data protection authorities from across the globe.
The 40th International Conference of Data Protection and Privacy Commissioners "*considers that any creation, development and use of artificial intelligence systems shall fully respect human rights, particularly the rights to the protection of personal data and to privacy, as well as human dignity, non-discrimination and fundamental values, and shall provide solutions to allow individuals to maintain control and understanding of artificial intelligence systems*"

On 23rd October 2018 ICDPPC adopted the "*Declaration on Ethics and Data Protection in Artificial Intelligence*"[189] endorsing six guiding principles, as core values to preserve human rights in the development of artificial intelligence, which can be summarized as:

1. *Fairness*
2. *Continued Attention and Vigilance as well as Accountability*
3. *Systems Transparency and Intelligibility*
4. *Privacy by Design & by Default for a Responsible Design and Development*
5. *Empowerment of Every Individual*
6. *Reduce and Mitigate Bias and Discrimination*

Based on these principles, the 40th International Conference of Data Protection and Privacy Commissioners
"*calls for common governance principles on artificial intelligence to be established, fostering concerted international efforts in this field, in order to ensure that its development and use take place in accordance with ethics and human values, and respect human dignity. These common governance principles must be able to tackle the challenges raised by the rapid evolutions of artificial intelligence technologies, on the basis of a multi-stakeholder approach in order to address all cross-sectoral issues at stake. They must take place at an international level since the development of artificial intelligence is a transborder phenomenon and may affect all humanity. The Conference should be involved in this international effort, working with and supporting general and sectoral authorities in other fields such as competition, market and consumer regulation*".

9.3.5 European Group on Ethics in Science and New Technologies

The European Group on Ethics in Science and New Technologies (EGE), is an independent advisory body of the President of the European Commission and provides the Commission with independent advice on ethical aspects of science and new technologies in relation to EU legislation or policies. EGE published a "*Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*" [190] endorsing the following "ethical principles and democratic prerequisites"

(a) Human dignity
(b) Autonomy

[188] https://icdppc.org/
[189] https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
[190] http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

(c) *Responsibility*
(d) *Justice, equity, and solidarity*
(e) *Democracy*
(f) *Rule of law and accountability*
(g) *Security, safety, bodily and mental integrity*
(h) *Data protection and privacy*
(i) *Sustainability*

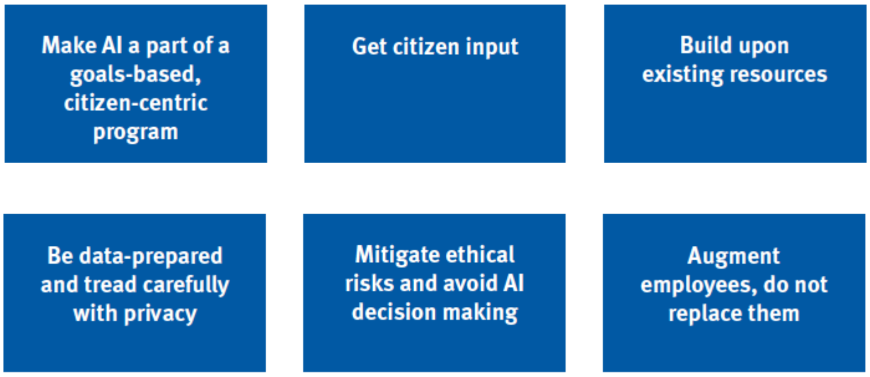
9.4 Sustainable development of AI based Smart Cities respectful of individuals

The keyword for a sustainable artificial intelligence system development is the "Human Centered design". This means that when developing systems and services based on somewhat "intelligent function" that may infringe the rights and freedom of natural persons, a robust, preventive, risk management to avoid material and non-material damages to individuals should be put in place. Both private and public sector should design and deploy AI systems and application respectful of dignity, rights and freedom of each citizen. Algorithmic bias, discrimination, non-transparent and non-intelligible logic of algorithms and of the overall purpose of the system, undue profiling and performance non-aligned with the expected behavior by end user, are obstacles to overcome towards an "ethically sustainable" AI systems design. These topics need to forge a new mindset of industry, technology providers, as well as community managers and local authorities in order to drive Smart Cities in the right direction where the primacy of the well-being of population is recognized and every technology becomes an instrument for the achievement of this primary objective.

On these issues Hile Mehr in his paper "*Artificial Intelligence for Citizen Services and Government*"[191] writes about the important role that AI can play in delivering high value services to citizens and calls on government agencies to consider six strategies for applying AI to their work:

1. *Make AI a part of a goals-based, citizen-centric program*
2. *Get citizen input*
3. *Build upon existing resources*
4. *Be data-prepared and tread carefully with privacy*
5. *Mitigate ethical risks and avoid AI decision making*
6. *Augment employees, do not replace them*

[191] Hila Mehr : Artificial Intelligence for Citizen Services and Government - Harvard Ash Center Technology & Democracy Fellow - https://ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf



Make AI a part of a goals-based, citizen-centric program

Get citizen input

Build upon existing resources

Be data-prepared and tread carefully with privacy

Mitigate ethical risks and avoid AI decision making

Augment employees, do not replace them

Figure 42. Navigating AI in Government

(Source: Ash Center for Democratic Governance and Innovation - Harvard Kennedy School)

As we already mentioned, at home, workplaces, streets and spaces citizens have the opportunity to be increasingly connected and to interact with private and public services AI based. Looking ahead, it's worth to mention the Japan's model "Society 5.0"[192]. As shown in the following picture, this model seems to make possible also the rise of "super-Smart Cities" where, again, the *human centered approach* is probably the only one able to combine economic growth and well-being of population.

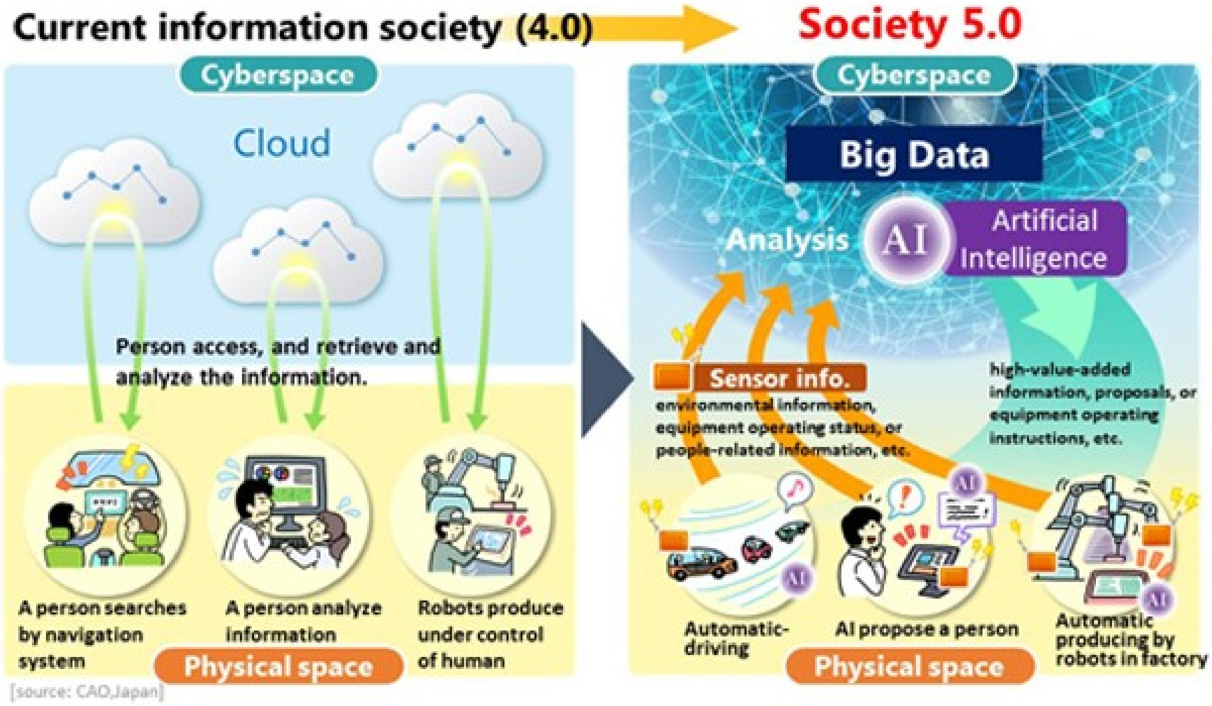

Current information society (4.0)
Society 5.0
Cyberspace
Cloud
Person access, and retrieve and analyze the information.
A person searches by navigation system
A person analyze information
Robots produce under control of human
Physical space
[source: CAO,Japan]
Cyberspace
Big Data
Analysis
AI
Artificial Intelligence
Sensor info.
environmental information, equipment operating status, or people-related information, etc.
high-value-added information, proposals, or equipment operating instructions, etc.
AI
Automatic-driving
AI propose a person
Automatic producing by robots in factory
Physical space

Figure 43. How Society 5.0 Works

(*Source: Government of Japan– Cabinet Office*)

[192] https://www8.cao.go.jp/cstp/english/society5_0/index.html

CONTRIBUTORS (*in alphabetical order*)

Glauco Bertocchi

Graduated in physics from Rome University. More than 40 years of experience in Informatics and Security within Universities and National Institutions. CISM and 27001 LA certified. Present research activity deals with Critical Infrastructure Protection and Resilience.

Sandro Bologna

Graduated in physics from Rome University. Main research activity deals with Critical Infrastructure Protection and Resilience, with a special emphasis to vulnerability and interdependencies modelling, simulation and analysis.

Luigi Carrozzi

(CGEIT, CRISC, Auditor L.A. ISMS, ISMS Senior Manager, Privacy Officer) over 30 years of ICT management experience in Governance, Risk management and Compliance for primary private and public organizations

Donato Di Ludovico

PhD, researcher of Urban and territorial planning and design, Urban design adjunct professor at the University of L'Aquila (Engineering). He carries out scientific research activities within the new forms of Spatial and Strategic planning, Urban planning and design security oriented, knowledge and assessment systems (SEA).

Donatella Dominici

Associate Professor at the Faculty of Engineering of the University of L'Aquila, with a PhD in Geodetic and Topographic Sciences at Faculty of Engineering of Bologna. Her scientific career has developed on issues related to the control and monitoring of the territory using GNSS techniques and remote sensing.

Luisa Franchina

Has been General Manager of the Secretariat for Critical Infrastructures (Presidency of the Council of Ministers 2010-2013). She published a great number of articles and books on safety and critical infrastructures protection.

Priscilla Inzerilli

Open Source intelligence analyst and consultant. She taught cyber security, risk management, Osint and Socmint at various companies and institutes, like SIOI – Society for International Organization, Link Campus University and La Sapienza University of Rome.

Alberto Traballesi

In service in the Italian Air Force from 1958 to 1995, left with the rank of Air Brigade General. Up to 2013 serviced as expert in the Presidency of Council of Ministers. Graduated in mathematics, electronic engineering and aeronautical sciences. He is currently involved in research on the protection of ICs and space policy issues.