University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Postgraduate Program of Studies
MSc Digital Systems Security

Security and Privacy in future Smart Cities

Master Thesis
of
Iliopoulou Theoni

Supervisor Professor: Gritzalis Stefanos

Piraeus, [July 2022]

Acknowledgments

This project would not have been possible without the support of many people. I would like to say a special thank you to my supervisor Professor Gritzalis Stefanos. His support, guidance and overall insights in the field of privacy and technologies have made this an inspiring experience for me.

I would also like to thank to my family and numerous friends, who endured this long process with me, continuously support and understanding when undertaking my research and writing my project.

Table of Contents

Abstract

In this thesis addresses the issue of security and privacy in future smart cities. In recent years, building smart cities has been a controversial issue for European and non-European countries. In the scope of this thesis, the characteristics of such a city will be analysed in detail, and similar cities worldwide will also be discussed. In addition, fundamental principles of such cities, such as Smart Grid, Micro Grid and the individual potential problems that may arise when using them are mentioned. In conclusion, the definition of privacy, the risks that may arise regarding personal data, and the correlation of GDPR, CCPA, PIPL with smart cities and their requirements are given.

Keywords

Smart cities, security, privacy, internet of thing (IoT), smart energy grid, cybersecurity

Περίληψη

Το παρόν εκπόνημα θίγει το ζήτημα της ασφάλειας και της ιδιωτικότητας στις μελλοντικές έξυπνες πόλεις. Τα τελευταία χρόνια η δόμηση έξυπνων πόλεων, αποτελεί αμφιλεγόμενο ζήτημα για Ευρωπαϊκές και μη χώρες. Στην έκταση της διπλωματικής αυτής εργασίας θα αναλυθούν λεπτομερώς τα χαρακτηριστικά μιας τέτοιας πόλης, ενώ επίσης θα γίνει αναφορά και σε αντίστοιχες πόλεις παγκοσμίως. Επιπλέον, αναφέρονται θεμελιώδεις αρχές αυτών, όπως το Smart Grid, Micro Grid και τα επιμέρους πιθανά προβλήματα που δύναται να προκύψουν κατά τη χρήση αυτών. Ολοκληρώνοντας, δίνεται ο ορισμός της ιδιωτικότητας, τα ρίσκα που πιθανόν να προκύψουν όσον αφορά τα προσωπικά δεδομένα, καθώς και η συσχέτιση GDPR, CCPA, PIPL με τις έξυπνες πόλεις και τις απαιτήσεις τους.

Chapter 1 : Security and Privacy in Smart Cities

1.1 Introduction

The 21st century is the era of urbanisation. Already more than half of the world's population lives in large modern cities, and by the end of the century it is estimated that this percentage will reach over 80%. Quality of life is a key priority for cities worldwide, as is its perpetual improvement. However, living in the age of technology, apart from the amenities it provides, one of which is the smart city, there are many risks associated with the increasing use of its factors.

Smart cities obey the rules of information and communication technologies (ICT) and are called upon to offer solutions and new perspectives based on their positive characteristics. Cities in general should achieve rapid growth in the short term in various areas of life, such as health, education and the economy, with the ultimate aim of ensuring the well-being of citizens and the full satisfaction of their needs. The innovative solutions offered by smart cities are a key tool for achieving this.

Chapter 2 : Smart Cities

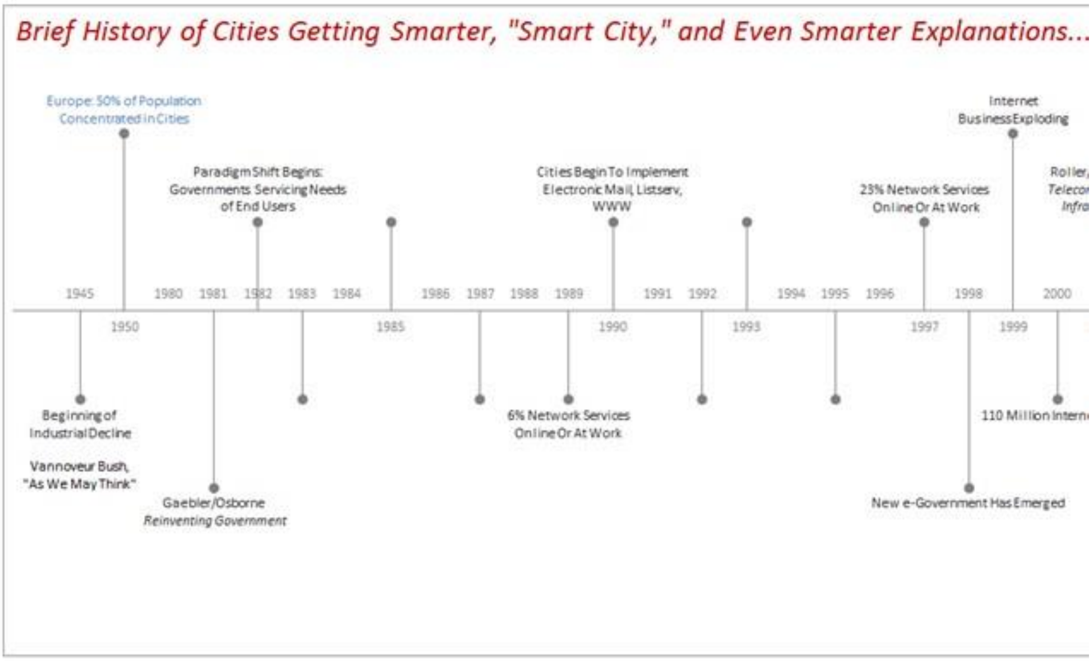
[1]

2.1 Definition of Smart City

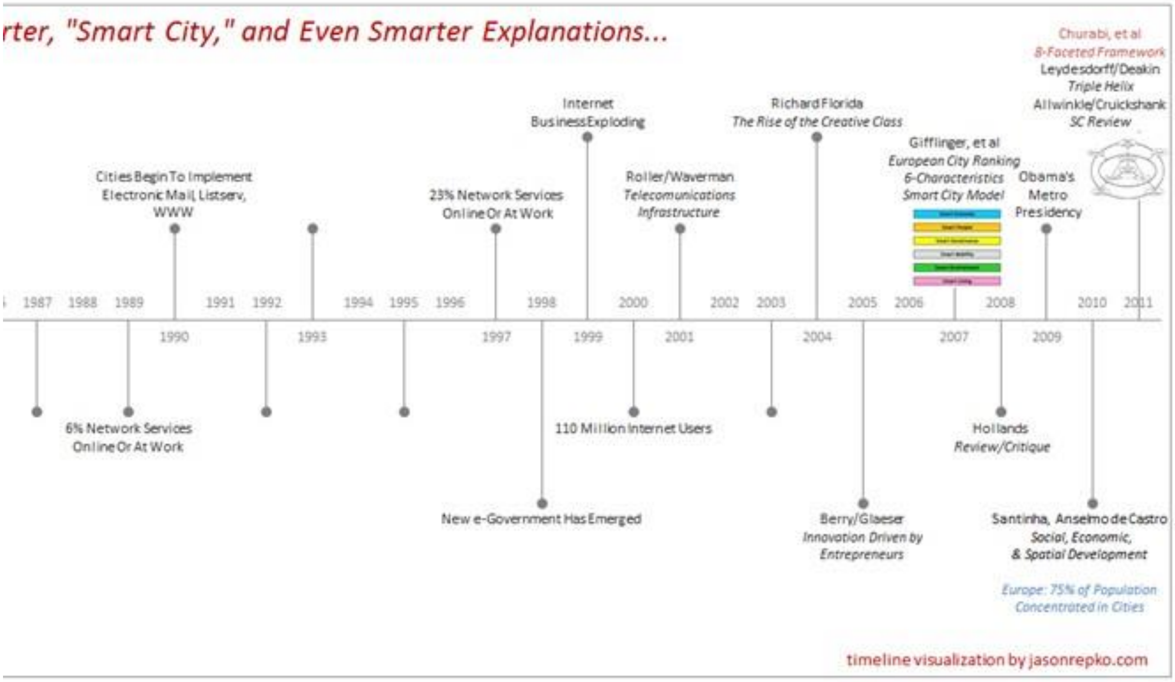
The term "Smart City" is used to describe a city that uses modern technologies to improve the daily lives of its citizens and to enhance their participation in decision-making on issues that concern them. A smart city goes beyond the use of digital technologies to make better use of resources and less emissions. It means smarter urban transport networks, upgraded water and waste disposal services and more efficient ways of lighting and heating buildings. It also means more interactive and responsive city management, safer public spaces and meeting the needs of an ageing population. In practice, this translates into broadband internet connections, interventions to facilitate mobility in the city, reduction of energy consumption and use of environmentally friendly ICT, e-government services, public data open to citizens, so that the basic services of a city are made more accessible and citizens can contribute to identifying and solving problems. The Smart City is a key pillar for the emergence of new and modern forms of governance and the formulation of policies and strategies, with the key objective of achieving sustainable development. [2] [3]

2.2 Historical background – Modern reality

In the 18th century less than 5% of the worlds population lived in large urban centres and the vast majority of the world's population were engaged to the production of the necessary food for survival. Today, more than 50% of the world's population lives in rural areas and probably by the end of this century it is predicted that more than 80% of the world's population will be gathered in large urban areas. [4] Thus, we conclude that cities are the future of humanity. Most of this urbanization is due to people's need for a better life, contributing a key method for saving energy and CO2 emissions proportionally.



This rapid migration of the population to large urban centres poses may challenges for the planning and the development and operation of cities that have the capacity to meet the needs and demands of this population. This is food for researchers and scientists, architects, engineers, planners, etc. Therefore, there is a great need for redesign and change od cities. The most common means of solving problems of urban areas is cooperation between stakeholders, human capital, good communication, creativity and scientific ideas that can be used to solve the problems of urban areas, which can be considered as smart solutions. [5]



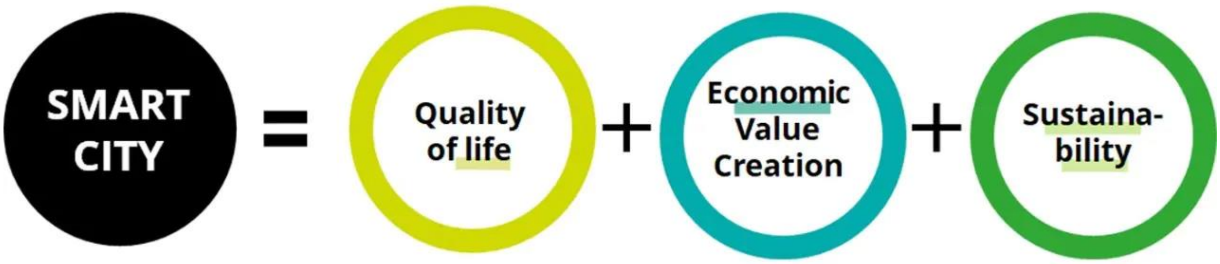
[6]

The concept of smart cities can be traced back to the 1960s and 1970s, when the US Community Analysis Bureau began using databases, aerial photography and cluster analysis to collect data, guide resources and reports in order to direct services, mitigate against disasters and reduce poverty. This led to the birth of the first generation of smart cities. The first generation of smart cities is provided by technology providers to understand the impact of technology on everyday life. This led to the birth of the second generation of smart cities, which looked at how smart technologies and innovations can create integrated municipal solutions. The third generation of smart cities has taken control of technology providers and city leaders, but has created a model that engages the public and enables social inclusion and community participation. Vienna adopted this third generation model and created a partnership with local company Wien Energy to enable citizens to invest in local solar installations and work with the public to address gender equality and affordable housing issues. This adoption is continuing globally, including in Vancouver, where 30.000 people have jointly developed an action plan to make Vancouver a greener city by 2020. [7]

Below a smart city timeline evolution is depicted, starting from the first digital city in Amsterdam.

[8]

The future of smart cities is a simple equation, but as demonstrated by the COVID-19 crisis, cities also need to prepare for the unexpected, building resilient structures able to emerge stronger from difficulties.



- Quality of life: Smart cities are happier cities. A positive quality of life involves improving every aspect of citizens' daily lives. Smart cities use data and digital technology to improve the quality of life of their citizens.
- Economic Value Creation: Smart cities can multiply the value creation of cities. Cities have long been important centres of trade and commerce, taking advantage of the diversity of the citizens to help bloom an innovative economy.
- Sustainability: Smart cities have a key role in sustainability. Each smart city, promotes economic growth and quality of life not just in the short term but for future generations as well. [9]

In Hangzhou, China, a smart technology based on artificial intelligence called "Urban Brain" has helped reduce traffic congestion by 15%. During the pandemic, New York City analyzed data on changes in spending patterns in specific communities to better allocate aid spending and investment priorities. San Diego has been praised for its "citizen-centric focus" approach to urban construction, thanks in part to its use of mobile apps and expansion of open data, as well as its Get It Done reporting tool.

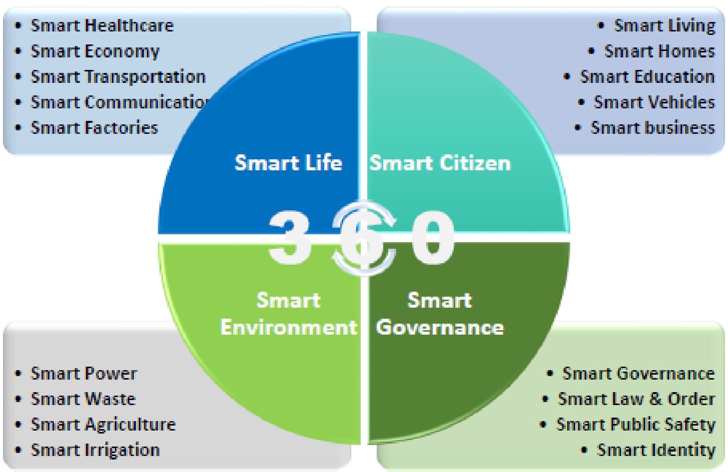
Smart cities have emerged around the world and are fast becoming the standard framework for future-ready urban centers, with the aim of improving the way citizens' data are collected and analyzed. What they have in common is the way they invest resources and time to develop city-centric solutions to address the wide range of urban challenges: waste and water management, public safety, transport, air quality monitoring, transport and parking, public works, municipal Wi-Fi projects, etc. The drivers underpinning the future of cities, especially when they are all recovering from devastating pandemics, are innovations overwhelmed by hundreds of projects designed to answer a key question: how do we use data in smart city technology to help us Digitalization empower cities to adapt and thrive?

Some experts believe that the epidemic has brought some positive aspects regardless of how much damage it has caused to the supply chains of various communities and the closure of businesses. The health care department or state agency has significantly accelerated its data collection strategy. The ongoing trend of using fast and remote interconnected IoT devices has also created interesting connections. According to a report by research firm MSCI, at the national and infrastructure level, with the introduction of pandemic warning and control systems, artificial intelligence and machine learning may combine with the Internet of Things for closer societal monitoring.

With the rapid increase in broadband usage in residential policy for more than a year, 5G networks continue to grow rapidly, even in areas that need to achieve high-quality connections as soon as possible. Building this underlying network is the foundation for the seamless adoption of key technologies in future smart cities. In the future, city planners and developers will use datasets from companies to put various detailed data into heat maps through analytics platforms. Understanding the relationship between income levels and usage rights of certain retail stores (such as grocery stores) or the rapid increase in community traffic density and park usage rights may also be an opportunity for cities to identify community needs and work with developers on new projects. [10]

2.3 Characteristics of Smart Cities

Many characteristics define a smart city; they can vary according to the social context in which the city is located or other variables related to culture. The below 360-degree depicts some of the most important characteristics of a Smart city, which will be described more detailed in the next pages.



2.3.1 Smart Life

Smart Life is segregated into five (5) subdomains as follows:

- Smart Healthcare: This category includes Patient Surveillance (real-time monitoring of patients' condition), Physical Activity Monitoring (body sensors network which records unstoppably), Medical Fridges ("smart" refrigerators that monitor and regulate the cooling conditions of medicines, vaccines and organic items) and Chronic Disease Management (monitoring systems for patients with chronic diseases such as diabetes). [11]
- Smart Economy: An economy driven by technological innovation, resource efficiency, sustainability and high social welfare. It adopts innovative and new business initiatives, with the overall aim of improving the quality of life of all citizens, increasing productivity and competitiveness. [12]
- Smart Transportation: Intelligent Transportation Systems (ITS) apply a variety of technologies to monitor, evaluate and manage transportation systems to improve efficiency and safety. In other words, intelligent transport uses emerging technologies to make moving around cities more comfortable, more efficient (for cities and people) and safer. [13]
- Smart Communication: Information communication, data exchange and connectivity are the keys to future smart cities. Communication technology in smart cities is no longer limited to fixed telephone networks, mobile communications and the Internet. Modern cities are based on a new concept of communication, which combines traditional and unique communication infrastructure - from sensor networks to information networks and mobile communications. [14]
- Smart Factories: Smart factories optimise efficiency and productivity by extending the capabilities of building equipment and personnel. By focusing on creating flexible, iterative production processes through data collection, smart factories can use more powerful data to aid the decision-making process. By continuously improving the productivity of the production process, smart factories can reduce costs, decrease downtime and minimize waste. Identifying and reducing misused or underutilised production capacities means opportunities for growth without investing additional financial and/or physical resources. [15]

2.3.2 Smart Citizen

Smart Citizen is segregated into five (5) subdomains as follows:

- Smart Living: Smart living as a trend involves the rise of standards in all aspects of everyday life, including homes, workplaces and the way people travel in cities. In the context of building construction, this trend can be defined by the increasing availability of innovative, faster, cheaper and more efficient technologies, materials, processes and construction ideas. [16]
- Smart Homes: refers to a convenient home environment in which mobile devices or other network devices can be used to automatically control appliances and electrical

devices remotely from anywhere with an Internet connection. The devices in a smart home are connected to each other via the Internet, allowing users to remotely control functions such as access to home security, temperature, lighting, etc. [17]

- Smart Education: It reflects the way in which advanced technology allows learners to absorb knowledge and skills more efficiently, effectively and comfortably. Smart education is an important part of smart city building. Advantages in basic education, advanced training and certification, universities and community colleges, e-learning infrastructure, lifelong learning, and innovation in educational technology are all part of the definition of smart cities. [18]
- Smart Vehicles: In the coming years, vehicles will be equipped with multi-interface cards and sensors on and off the road. As more and more vehicles are equipped with embedded wireless devices and sensors, efficient transportation and management applications focus on optimizing vehicle flow while reducing travel time and avoiding congestion. [19]
- Smart Business: Refers to the companies, which are able to use digital transformation, know how to manage the data they own, are able to value their assets, can communicate both internally and externally, can easily adapt to market changes and use monitoring systems for supervising IT and analyse their performance. [20]

2.3.3 Smart Environment

Smart Environment is segregated into four (4) subdomains as follows:

- Smart Power: Each smart city aims to reduce pollution footprints, increase public safety, or offer improved services to residents, which are parts of power management. Moore's law has guided successive generations of chip development to provide ever greater functionality in smaller packages that consume less power per operation and cost less per unit. [21]
- Smart Waste: Powered by IoT, smart waste solutions use fill level sensors and dynamic routing to help cities optimize their waste resources so they can collect waste at exactly the right time. Smart waste management uses IoT sensors in bins to automatically send data on fill levels to waste collectors. [22]
- Smart Agriculture: Promoting sustainable agriculture in smart cities, addressing the challenges related to the growing demand for protein-rich foods due to intense urbanisation. It looks at developing the appropriate technologies and optimised infrastructure needed for the massive deployment of smart urban agriculture while enabling circular economy mechanisms to recycle waste into value assets. Data collection, storage and analytics are expected to play a key role for smart agriculture applications. [23]
- Smart Irrigation: A programmable irrigation system, which allows the users to set a time which automatically turns lawn sprinklers an and off. Tests have shown that smart irrigation controllers can save up to 20 percent more water than traditional irrigation controllers. Smart irrigation is also used for agriculture purposes especially in countries where there is no efficient source of water and irrigation system is implemented to provide water to plants according to their moisture level and soil type. [24]

2.3.4 Smart Governance

Smart Governance is segregated into four (4) subdomains as follows:

- Smart Governance: Smart governance is defined as the application of technology and innovation to improve decision-making and planning. It has to do with improving democratic procedures and changing how government services are delivered. The governance process is based on the use of ICT tools and the Internet to provide information and public services, on communication and collaboration between government and citizens, and on good governance principles. [25]
- Smart Law and Order: Smart cities use a range of smart applications, which help to provide a wider range of options for policy and decision makers in managing infrastructure and prioritising urban planning. However, in the absence of appropriate legal and regulatory frameworks, the deployment of smart devices and applications that continue to collect, analyse and share data about people and infrastructure can compromise people's interests and put at risk the national interests of their respective countries. [26]
- Smart Public Safety: Some of the public safety measures already in use by smart cities are smart streetlights (with cameras and microphones and sensors monitoring traffic, accidents and crimes), smart traffic signals (analyse traffic conditions, change their timing and easing congestions), smart intersections (capture and analyse traffic patterns, detect risks, warn against imminent accidents, reduce crashes), smart emergency vehicles (capture and share video, audio, and vehicle telemetry against accidents) and smart buildings (monitor access, review video feeds and run environmental systems). [27]
- Smart Identity: In smart workplaces, smart identity is needed in order to avoid the traffic and help you to get where you need to be. To achieve this level of personalization, connected systems need a way to identify each user and tailor everything to their preferences. With a fingerprint authentication-driven digital identity solution, users can authenticate themselves and connect to systems based on personal information. [28]

2.4 Advantages

The advantages of a Smart City are plenty considering the above characteristics, each Smart City provides. The most important advantage we will meet is the better transportation services. A smart city has the potential to drastically improve the current level of transport across the city. It will have better traffic management, the ability to monitor public transport and better serve its citizens with continuous information and low fares. There is also safer communication as the most technological advances and partnerships with the private sector will benefit society since there will be lesser criminal activity. Additionally, since there is a limited amount of natural resources left to meet the demand of the people, smart cities offer technologies and tools to decrease the usage of natural resources and water waste, electricity, etc. without having to cut down on any factors. Another significant advantage is the reduced environmental footprint. A smart city has thousands of energy-efficient buildings that can improve air quality, use renewable energy sources and reduce reliance on non-renewable energy sources. Each smart city resident, must have access to high speed internet services and affordable prices. This way the smart city offers digital equity to all of its residents. Moreover, smart cities offer improved infrastructure because of the smart technology they make use of, which predicts and identifies the areas that can cause infrastructure failures before it occurs. Investing in smart cities will lead to improving business, since the entire city will have access to an open data platform, information, etc. companies will flourish. As a result economic development and job opportunities are both advantages since each resident of the city will get equal access to basic resources such as internet connection, transportation, etc. Lastly, since the authorities can monitor the dealings of the people closely, due to the new technologies, there will be a reduced amount of crime. [29]

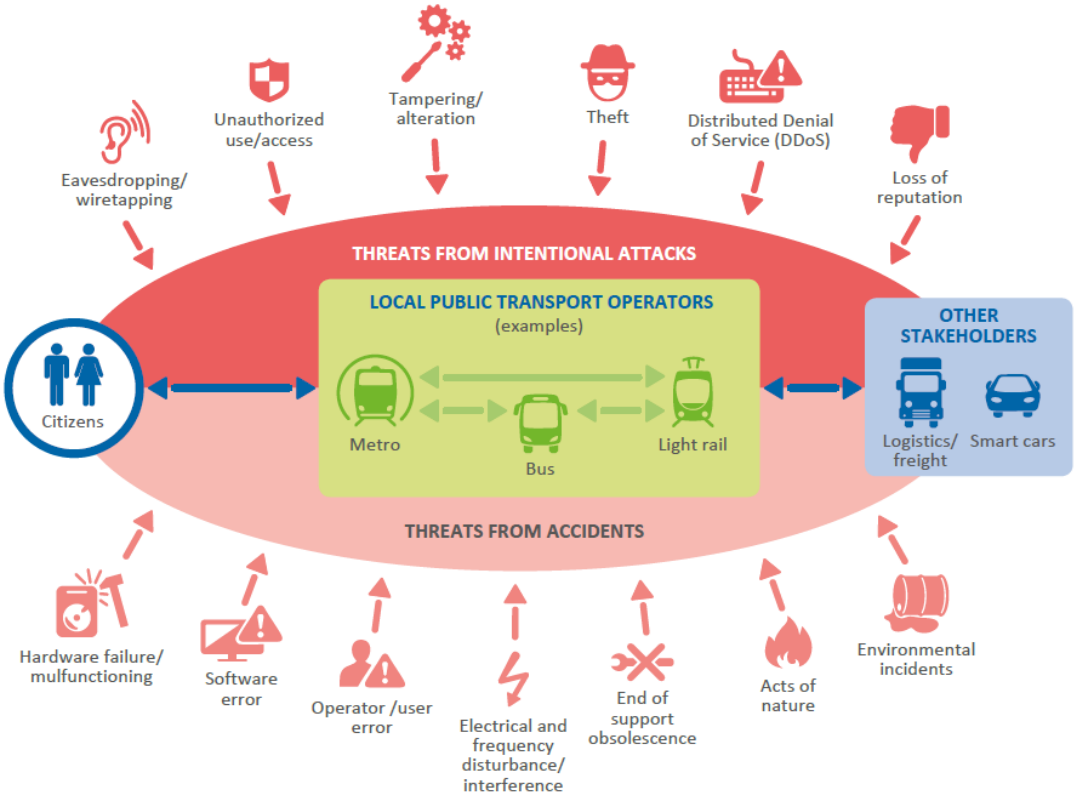
2.5 Troubles & Challenges

The problems associated with smart city solutions usually arise from the following sources:

- The Smart City is not treated as it should be, i.e. a complex system consisting of many parameters, different and competing interests.
- The smart city focuses on the creation of technical and technocratic forms of governance aimed at the interests of large companies or governments, sometimes overlooking citizen-oriented solutions.
- With the creation of technological solutions, cities are treated as markets, providing a specific solution without it being adapted to the needs of each city.
- The technologies used have social, political as well as ethical implications, although new forms of social control and governance are introduced, thus facilitating the violation of privacy.
- The technologies used do not protect user data. Furthermore, dysfunctional devices can cause the creation of vulnerable security systems. [30]

The European Network and Information Security Agency (ENISA) carried out a study on the digital security of public transport in a smart city. According to the study, a smart public transport system is vulnerable to digital malicious attacks. There are two categories of attacks, malicious and accidental. Regarding the malicious attacks, eavesdropping is a program which aims to monitor the network traffic at the IP packet level and reconstruct the messages and thus intercept the passwords. Eavesdropping refers to attacks on the confidentiality of the system. Copper is vulnerable to attacks and the 50 companies are investing in wireless infrastructure to reduce the risk of malicious attack. In addition, the category of malicious attacks also includes unauthorised access through the process of copying, modifying or destroying data and is carried out by violent attacks but also by manipulation and password interception. Finally, there is the coordinated denial of service due to the collapse of a network due to overload.

The other category is random attacks that are not intentional. These are hardware/software failures that may be related to lack of maintenance. In addition, mistakes on the part of the operator made in maintenance or upgrading can damage the data and make it vulnerable. Power outage can affect the availability of a system and make it vulnerable. Finally, natural phenomena such as rain are a reason that may damage the operation of telecommunication networks. [31]



[31]

Chapter 3 : Smart Cities Worldwide

[32]

3.1 Smart Cities in Greece

In Greece, there is a significant mobility in the field of Smart Cities and there is a trend towards networking, with the creation of inter-municipal networks for the exchange of good practices and experience in the management of urban problems. As already mentioned, in Greece, Smart Cities are not the dominant scientific discipline. However, this does not mean that it is absent from the whole of the Greek territory. There are some cities that can be classified as Smart Cities and some examples of cities that are taking significant steps to reach this level of development.

3.1.1 Trikala Smart City

Smart Trikala

[33]

Trikala has the reputation of a Smart City pioneer, as in 2004 it was characterized as the "First digital city in Greece". Toda, under the name "Smart Trikala", the public authorities have developed a wide range of digital solutions that help improve the lives of citizens.

In collaboration with companies such as Cisco and Vodafone, Trikala now hosts innovative services such as an electronic complaints system for residents. Through these smart tools, the city is now also able to gather an increasing amount of data, the authorities are able to gain a greater insight into the functioning of Trikala and how the various public services can be made more efficient and sustainable.

Trikala aims to ensure that it remains at the forefront of new smart digital solutions, helping it to maintain its leadership. Some of the digital solutions the city offers, are the following. [34]

Teleprovision: It is about tele-care and tele-medicine infrastructure to provide support services to vulnerable groups in society. Thus, people with chronic heart failure and other serious problems are monitored and served in a daily basis, in order to reduce the possibility of a critical health issue, as well as the everyday care. However, the most important goal of teleprovision is to avoid the admission of the patient to the hospital or institution. Patients have their biological signals recorded via smart phones and transmitted wired or wirelessly to the tele-care centre or a doctor. [35]

E-dialogos: The ultimate and certainly innovative "tool" of e-government, which every citizen of Trikala – from anywhere in the country or the world – has freely, is e-dialogos. Through the website www.edialogos.gr citizens have the opportunity to actively participate in the decision-making process of the Municipality, using new technologies. Similarly, citizens are able to cooperate with the Municipality of Trikkaion, through electronic polls, where electronic signatures are collected and the citizens can also participate in Electronic Consultations with the ultimate goal of formulating and implementing political actions. [35]

Intelligent transport system: It is a project with direct impact on the daily life of the citizens of Trikala city. Based on the inductive loops, the traffic data of the city is managed, while the fleet and the network of urban buses is monitored as well, thus as a result the citizens are always informed and up to date. Additionally, the smart bus stops offer precise information of the routes, the waiting time until the arrival of each bus with an accuracy of one second. The citizens of Trikala can regulate their time while enjoying "god practices" of a similar size of European cities. [35]

CityMobil2 transport pilot project: The driverless bus was a major innovation in the European CityMobil2 pilot project. In Trikala, the vehicle was driven through the urban fabric and at the control centre, technicians monitored the bus's progress and recorded any problems that may occurred. The connection between the control centre and the pilot was made using optical fibre. The bus had also implemented a safety laser and in case any object or person may detected, it would instantly immobilise the bus. Driverless driving is an important innovation in road transport and will provide positive results in terms of traffic safety. [36]

Trikala is the only city in Greece, which has supplied Lego and Raspberry Pi robotics kits to all its 120 public schools, a move paid by e-Trikala. Over in the echoing corridors of the 7th High School of Trikala, ICT teacher Vassilios Spachos shows off his robotics lab – the first of its size in a Greek public school when it opened in 2015 with a grant from the Stavros Niarchos Foundation and support from the municipality.

Trikala city supports its farmers through tech farming project, which promises to create job opportunities especially for young people, and fight one of the biggest problems in Trikala and Greece: brain drain. For ICT teacher Spachos, creating smarter cities is the key to tackling this problem. "Tech is the only sector that gives young people the tools to succeed in life nowadays, just look at the wealthy people in the world," he says, shaking his head. [37]

3.1.2 Chalkida Smart City

Chalkida is showing the way to the "smart city" as it has been doing more and more on the internet to simplify citizens' lives and those efforts have been recognised. To better and faster service for citizens and work safety for employees, develop, introduce and implement new technologies in its operations, especially interoperability applications (API), and therefore won the Bronze in the Best City 2020 award. The application allows for the interconnection of different databases (public) and the automatic export of data from the property expense management (TAP), municipal tax and municipal expenditure (back-end) applications from the property declaration platform. In this way, citizens visit only one point (where the application is done), which has obvious time and money saving benefits and simplifies the process using new technologies. [38]

Chalkida has already implement smart parking system (Smart Parking), lighting (Smart lighting), a way to measure the environmental parameters (Air Quality Monitoring) and a single management platform has been installed as well. The project is jointly implemented by the OTE Group, Cisco, CAUCASUS and OTS, and has demonstrated in practice how the adoption of smart technology can contribute to improving the quality of life and everyday life of city dwellers.

Smart Parking: The "smart" parking solution combined with mobile apps developed by OTS for Android and iOS devices can tell drivers where free parking spaces are available and how to get there, or directed to another location if the first one is occupied. The app is expected to make a significant contribution to reducing parking time, thereby reducing congestion and emissions. At the same time, it enables the municipality to manage parking spaces more efficiently, having an idea of the parking time of each vehicle and each parking space that violates the traffic code.

Smart Lighting: The Caucasus SSL/LED "smart" lighting system has replaced the traditional lighting system and has contributed more than 60% energy savings. Through their wireless management, they enable remote monitoring and programming of operation and maintenance and dynamic regulation of lighting, with the aim of maximising energy savings, safety and visual comfort for citizens.

The data of the smart parking and lighting solutions is collected, via network infrastructures, in OTE Group’s Cloud infrastructure and is delivered to Cisco's Smart & Connected Digital Platform. The platform manages "smart" solutions through a single dashboard, as well as the integration, storage and viewing of data from applications. The Smart & Connected Digital Platform has the potential for future integration of more smart solutions.

Air Quality Monitoring: The environmental parameter measurement system installed by the OTE Group uses high-quality sensors to detect harmful gases and three types of particles in the atmosphere. It will also measure temperature, humidity and atmospheric pressure. As a result, municipalities will be able to better plan and implement actions to reduce air pollution and improve the quality of life of residents. [39]

3.1.3 Heraklion Smart City

[40]

Heraklion has been included in the list of 100 smart cities in Europe after an evaluation of its digital policy. The evaluation was carried out by the European Commission's Smart City Challenge initiative in 192 cities from 20 European countries, resulting in Heraklion being included in the list of 100 smart cities in Europe. In this list, there are 10 cities with international reputation, 8 mentor cities and 82 other cities with high ratings of their digital policies. It is worth noting that in 2018 the city of Heraklion was included in the list of the 27 most powerful digital cities in Europe after an evaluation by the same initiative. [41]

Heraklion provides a website which describes the city’s vision, the projects, the distinctions and the news to everyone who is interested. The electronic services Heraklion provides to its residents are also provided through the website. Some of them are mentioned below.

Parking Control: Personalised parking system via appropriate sensors in the parking spaces. Through the website, the available parking spots are visible in each parking zone, as well as the occupied parking spots.

Crowd Estimation: Crowd estimation system in central squares of the Municipality of Heraklion. Through the website the user can choose one or more square zones, while there are also two tabs in which the initial and final date of the recording can be filled as well.

Noise Measurements: An Intelligent Noise Platform, combining telecommunications, electronic and information technologies with transport engineering, to record, dynamically process and map noise at specific points of interest. Through the website the user can choose one or more square zones, while there are also two tabs in which the initial and final date of the recording can be filled as well.

Traffic congestion: Intelligent traffic measurement system, for optimal use of road networks and better service, safety and improved efficiency. Through the website, the user can choose the type of the vehicle he chooses as well as the initial and final date. [41]

3.2 Smart Cities Abroad

Smart cities are part of the broader project of Western societies to transition to a knowledge-based society and economy. They describe environments that enhance human capacities for creativity, learning and innovation. They are created by the fusion of local innovation systems operating within cities (technology districts, technology parks, innovation poles, clusters) with digital networks and information society applications. Their value lies in in their ability to bring together and combine three forms of intelligence of the human population of cities, the collective intelligence of innovation institutions, and the artificial intelligence of digital networks and applications. In this section some of the most significant Smart cities all over the world, will be described. [42]

3.2.1 Smart Cities in Europe

[43]

Ancient history is emerging from many European cities. But that doesn't mean they have to lag behind in technology and innovation. Optimising resources and maximising the well-being of citizens has always been at the forefront of the European Community's agenda. Leading in innovation, some cities are perfect examples of modern technology applied to public services. These are the best smart cities in Europe. [44]

1. Paris, France
   Paris is a city with boasts over 400 parks and 300 Metro stations. The Internet of Things can help builders and planners gain better insight into the millions of people who move through cities like Paris every day. There are Bluetooth beacons, which gather data in two simple ways. Either by recording when individuals with Bluetooth enabled phones rest n a bench or visitors and Parisians participate in active data collection. There is also a project named “Paris Smart City 2050” which includes 8 prototypes of energy-plus towers eco-conceived to fight against climate change. The study has been carried out for Paris City Hall by « Vincent Callebaut Architectures » agency. [45] [46]
2. Valencia, Spain
   Valencia has become a benchmark for smart and sustainable cities, and one of the three largest cities in the world with dual certification for measuring progress towards the SDGs and an active participant in various international forums in an effort to make technology a sustainable, prosperous and quality ally for people. Some of the city's innovative technologies include. Smart bins indicate in real time if they are filling up to avoid overflows and optimise collection routes. A computerised system that can speed up help to those most in need, guarantee their well-being and save them time and paperwork. [47]
3. Venice, Italy
   The SmartVenice approach focuses on environmental and social sustainability in the context of innovation - it supports a participatory and co-creation-based research/design approach to propose solutions and services based on human needs and help address discrimination and exclusion. With Horizon 2020 funding, the city has appointed a smart city secretariat responsible for the creation of the Venice smart city and community. The initiative aims to use advanced technology and digital solutions to address the city's various challenges and improve the quality of life of its residents. Venice has also signed a Green Digital Charter, committing the city to achieve climate goals through digital means. [48] [34]
4. Dublin, Ireland
   Dublin is the city where technology providers, academia and citizens collaborate to transform public services and enhance quality of life. The city develops innovative solutions in order to respond effectively in the environment changes, engage with the residents and local government issues, reduce congestion through technological innovations in mobility, improve liveability and competitiveness, make better decisions and deliver better services, bring communities together and improve Dubliner’s wellbeing. [49]
5. Ljubljana, Slovenia
   Ljubljana is the capital and largest city of Slovenia. It is known for its university population and green spaces, while the winding Ljubljanica River separates the old town from the commercial centre. Ljubljana's green credentials are widely recognised and it has been awarded the status of "City of Trees" by the World Tree Project. In 2019, Ljubljana was awarded the title of Earth Friendly City for the eighth consecutive time. In 2017, the city adopted the Integrated Transport Strategy of the City of Ljubljana, a

strategic document with a special focus on promoting sustainable transport. In 2018, the city adopted the Ljubljana Integrated Urban Transport Strategy, which identifies key measures aimed at improving the quality of life of citizens, while focusing on reducing the use of passenger cars and promoting public transport. [34]

6. Gothenburg, Sweden
   Gothenburg is recognised globally as a top-ranking Smart City. Gothenburg is among the world-leading smart cities as it offers numerous innovations. The city bases 60% of its district heating on waste/recycled heat, while 90% of the buildings are using district heating. Additionally, there is a Lighthouse project "IRIS", which consists of three European cities: Utrecht, Nice and Gothenburg. The project is focused on energy-positive areas, smart energy management, smart e-mobility and innovation platform for digital cities and residents. There is also a Smart Map, which encourages citizen engagement by gathering all places available for renting, borrowing, sharing, giving and getting. Lastly, a 3D city model is available to be used by developers, architects and planners to host public consultations, anticipate the impact of future development and make better-informed decisions. [50]
7. Amsterdam, Netherlands
   Amsterdam Smart City is working on the smart, green and healthy future of the Amsterdam Metropolitan Area. By a values first approach ensuring innovations actually contribute to cleaner, greener and happier cities. At Amsterdam Smart City residents and users of the cities become protagonists and the interests are clear: data and tech are used to increase the quality of life. It's all about open and transparent sharing of knowledge. Amsterdam Smart City is that open and safe space for cooperation and innovation. It is about an open platform which is a meeting place and workplace for metropolitan challenges and solutions. Because Amsterdam Smart City is convinced that the challenges for now and the future can only be solved by collaboration, thus a public-private collaboration started. As an urban innovation platform, companies are brought, public institutions and residents together to shape the cities of the future. Via this online platform and various events innovators show each other what is happening in the Amsterdam Metropolitan Area, learn from each other and can get in touch. [51]
8. Copenhagen, Denmark
   Smart City Copenhagen is a living laboratory for testing smart technologies to address the challenges of urbanisation and climate change. Unique access to data and effective public-private partnerships attract many multinational companies. Copenhagen aims to become the world's first carbon-neutral capital by 2025, while Denmark is determined to be completely independent of fossil fuels by 2050. Around 250 companies in the Copenhagen area are involved in smart city operations. Small companies account for two thirds of the smart cities industry, offering attractive investment opportunities. Copenhagen won the Global Smart Cities Award in 2014 for the Copenhagen Connecting project, demonstrating the city's leadership as a smart city. For decades, Danish authorities have been collecting and storing key data on citizens, businesses and real estate in order to digitise services across all administrations and departments. A new government programme provides free access to public data sources to promote innovation in the smart city. [52]
9. Helsinki, Finland
   The Helsinki Smart Region showcases smart expertise in Helsinki-Uusimaa. The Smart Innovation Strategy for the Helsinki-Uusimaa region brings together factors from both

urban and rural areas for research and innovation activities with impact under the overall theme of the Wisdom of Resources. Uusimaa is a driver of economic development and internationalisation in Finland. Uusimaa's three strategic priorities, "Prosperity and competent people", "Successful and responsible enterprises" and "Climate wise and diverse province" coincide with the top themes of Smart Uusimaa: climate neutrality, Renewable industry and innovative services, City of people. At the interfaces of these priorities are multi-thematic entities that offer ample opportunities to develop new types of research and innovation, while supporting industries in their ongoing transformation. [53]

10. London, England

    London is at the top of the overall ranking, given its very high scores in many areas. In digital infrastructure and new technologies, for example, the UK capital is home to more start-ups and developers than almost any other city in the world. It has launched the Smarter London Together project, which aims to be a structured but flexible digital growth plan to make it the smartest city, technologically speaking, in the world. London is described as a kind of global test city for innovation, where the best ideas are developed with the highest standards of privacy and security. Its population has reached 9 million (and is on track to grow to 11 million by 2050). In addition, London is a natural hub for AI, with 750 suppliers working in the field (twice as many as Paris). The intelligent evolution of services and lifestyles in the city is a hallmark of the urban redevelopment plans and sustainable mobility projects launched by the administration in recent years. [54] [55]

3.2.2 Smart Cities in America

[56]

As cities struggle to attract new people or improve the lives of existing residents, they are investing more and more to become smarter. In the U.S., municipalities will invest about $41 trillion over the next 20 years to upgrade their infrastructure to take advantage of the Internet of Things, according to the Presidential Innovation Fellow initiative (Smart America Challenge) launched by the White House to bring together projects from the following industries to take advantage of the Internet of Things Smart Manufacturing, Healthcare, Smart Energy, Smart Transportation and Disaster Response. Not surprisingly, many cities that have invested heavily in smart technology are already known as centres of innovation or academic hubs. These smart cities are going to be analysed in the list below.

1. New York, NY

   As the largest urban area in the United States in terms of population and GDP, New York City has unparalleled investment potential to become a smart city. It proved to be one of only 2 U.S. cities to receive an A rating in the 2020 Global Smart Cities Index (7 cities, all of them outside the U.S., received AAA or AA ratings). According to the Global Smart City Index (GSCI) survey of New York City residents and more than 100 other major cities around the world, New York is one of the best cities for Internet speed and reliability, congestion information, and cultural events.

Best Smart Initiative: the city recently launched a pilot project that installed hundreds of smart sensors for monitoring. In a separate pilot project, it has 5 municipal fleets equipped with solar energy sensors to collect and compare air quality data in different neighbourhoods in the South Bronx.

2. Washington, DC

   It is the only US city to receive an A rating in the 2020 Global Smart Cities Index. According to respondents, information on local government decisions is readily available, online platforms where residents can find ideas in order to improve city life as well as cultural events dates, which are among the best in the world.

   Best Smart Programme: DC uses video sensors to classify and measure urban traffic to gauge traffic and flow in key economic development corridors and event locations. The primary goal is to provide "traffic analytics" to improve city operations, economic planning efforts, and other ways to understand and improve cities.

3. Boston, MA

   According to QS Top Universities, Boston has 2 of the top 3 best universities in the world. With such an abundance of human capital, it's no surprise that Boston is one of the top smart cities in the United States. Boston received a BBB rating in the 2020 Global Smart Cities Index. Residents declare that the internet speed and medical services are above-average.

   Best smart initiative: The BOS:311 app, previously called Citizens Connect, through which the residents can report an issue like paddles or graffiti. These reports are imported simultaneously into the city’s work order system, where they are tracked and assigned to service teams.

4. San Francisco, CA

   As a gateway to Silicon Valley and a city that attracts billions of dollars in tech investment each year, it's no surprise that San Francisco tops the list of smart cities, providing feedback on local government programs. The city received a BBB rating from the Global Smart City Index 2020.Like New York, Washington, D.C., and Boston, people in San Francisco consider it a world leader in cultural events.

   Best smart initiative: Although it was launched in 2011, the SFpark smart parking system deserves to mention here. Through sensors placed on the asphalt, data is fed to smart parking meters that change prices based on availability and time of day. The aim of the system is to reduce the time and fuel wasted by drivers looking for a parking space.

5. Seattle, WA

   Seattle is a place where numerous tech companies like Amazon, Microsoft, etc. are hosted and was yet another city to receive a BBB rating from a Global Smart City Index 2020. Residents are able to navigate through employment-finding services and can easily provide feedback on local government projects. Seattle ranks well above the global average for cultural activities.

   Best smart initiative: The Food Rescue Innovation Labs, an initiative of Seattle Pacific University supported by the City of Seattle’s Innovation Advisory Council, is developing software to provide real-time, open-access information about surplus food, transportation options, and other food rescue logistics.

6. Denver, CO

   Denver is another city received a BBB rating from Global Smart City Index 2020. Residents of the city mention that Denver stands out for online purchasing of tickets to shows and museums, ease of online voting, and ready availability of employment services. Denver is a city well above the global average for cultural activities.

   Best smart initiative: The Colorado Smart Cities Alliance’s Love My Air program, in partnership with Denver Public Schools, is creating a citywide air-quality (AQ) monitoring network to provide real-time AQ data–utilizing low-cost cutting-edge air pollution sensor technology, redeveloped with solar, battery storage and data connectivity to make it useful for wide scale deployment and replicable in any municipality.

7. Los Angeles, CA

   USA’s second largest urban centre by population and GDP had to appear somewhere on this list. LA received a BBB rating from the Global Smart City Index 2020 as well. Residents, were impressed with the recent online voting pilot which was run in 10 neighbourhood councils, including Downtown LA, in 2019, according to the GSCI survey.

   Best smart initiative: In 2019, LA was the first U.S. city to launch an earthquake early warning app to the public. Through a network of seismic sensors, which were installed in the greater Los Angeles region, ShakeAlertLA triggers in case of an earthquake of magnitude 5.0 or larger and sends an alert to its users.

8. Columbus, OH

   Columbus won the U.S. Department of Transportation’s inaugural Smart City Challenge, as it proposed an integrated plan addressing challenges in residential, commercial, freight, and downtown districts using numerous latest technologies, including connected infrastructure, electric vehicle charging infrastructure, an integrated data platform, autonomous vehicles, and more. Columbus goals for the future is to work closely with residents, community, business leaders and technical experts in order to implement successfully its’ plan.

   Best smart initiative: Columbus is working to empower residents through responsive, innovative and safe mobility solutions. Columbus wants to become a leader in EV markets in United States, regarding the electric vehicles.

9. Austin, TX

   Austin is known for being one of the fastest-growing as well as fast-growing centre for hi-tech in America. The University of Texas at Austin’s world-class engineering and computer science programs supports the idea and constantly provides new talents from abroad or internally.

   Best smart initiative: Austin Water is conducting a pilot installation of thousands of smart water meters in various neighbourhoods. The meters transmit consumption data electronically, enabling the utility to predict and respond to conditions and improve engagement with customers.

10. Pittsburgh, PA

    Pittsburgh’s Carnegie Mellon University in collaboration with the city of Pittsburgh, Allegheny Country and other government agencies have developed a program named Metro 2021:Smart Cities Institute, which aims to use technology in order to improve

quality of life in metropolitan areas. For this reason, Pittsburgh earns a place on our list of top 10 smart cities.
Best smart initiative: One of the projects run by Metro 21 is an artificial light survey of night-time Pittsburgh at resolutions finer than can be done by open satellite surveys. Camera and spectrometer-enhanced drone flights assemble a high-resolution map of Pittsburgh at night. The data is used for scientific studies of light pollution and its effects to identify the major light polluters in the city. [57]

3.2.3 Smart Cities in Asia

[58]

Currently, most of the growth of smart cities is taking place in the Asia-Pacific region. People are flocking to cities, and more and more are moving to the ASPAC. Today, the region is home to 60% of the world's cities and is expected to rise to 62% by 2030. In addition, 1.2 billion new residents are expected to move to AAC between 2019 and 2050. As big cities grow, it is essential to build better, cleaner and safer cities. By integrating new technologies such as the Internet of Things (IoT) and 5G, businesses and smart city service providers can overcome security challenges and increase efficiency. To address the urban challenges posed by population growth, local governments are turning to technology and digital solutions that can improve public safety, environmental monitoring, water treatment, transportation, and energy production and consumption. Some of the most known smart cities in Asia will be presented below: [59]

1. Kuala Lumpur (Malaysia)
   Kuala Lumpur, known by its inhabitants as KL, is the capital of Malaysia and one of the most important cities in the region. Like many Asian smart cities, Kuala Lumpur is also developing a "City Brain" smart city initiative using Alibaba Cloud computing systems. This "brain" works by using IoT sensors and data analytics to help solve urban challenges. The most notable application of this technology is the city's recent adoption of a smart traffic management system in partnership with Alibaba Cloud and Sena Traffic Systems Sdn Bhd. The project aims to streamline travel and significantly reduce traffic congestion. Other smart projects in the region include the creation of special

national key economic areas and other government initiatives that will support the city's smart revolution and help accelerate the country's digital transformation by focusing on education and promoting cloud technologies and artificial intelligence. [60]

2. Seoul (North Korean)
   South Korea's capital, Seoul, has consistently topped Asia's smart city lists, and for good reason. As one of the largest cities in the region, with a population of more than 10 million and nearly 15 million in the greater metropolitan area, the city has risen to the challenge. From pollution to traffic congestion, from a lack of affordable housing to an exponentially growing population, Seoul has no challenges it hasn't faced. Smart mobility solutions like the Hope Seoul Surveillance System that helps prevent congestion by monitoring vehicular and pedestrian traffic throughout the city, free public bicycle programs, attractive public transportation services and more are helping Seoul develop a car-free city. The goal is for the city to no longer have private cars by 2030. Mobility is a small part of the city’s ambitious plans. Using a variety of smart open data platforms, sustainability projects, and a variety of public-private partnerships, Seoul is rapidly turning into one of the most advanced smart cities in the world. [60]
3. Shanghai (China)
   Juniper Research has ranked Shanghai as the world's first smart city for 2022, following an assessment that included aspects such as transport and infrastructure, energy and lighting, city management, technology and urban connectivity. The survey particularly praises Shanghai's Citizen Cloud as a one-stop shop for more than 1,000 different services for city residents. 2022 kicked off with a series of smart city technology developments around the world. As part of its plans to become a smart city, the Swedish municipality of Borås Stad has hired Extreme Networks, in partnership with NetNordic, to create what is claimed to be one of the largest cloud-managed network infrastructures. The new infrastructure in Borås Stad is designed to provide faster and more advanced connectivity, extending secure public Wi-Fi for citizens, local government, schools and services, while automating and simplifying network management for the IT team. The transition to a smart city also aims to provide more sustainable resources to residents while improving quality of life and fuelling business innovation. [61]
4. Abu Dhabi (United Arab Emirates)
   The recent McKinsey report saw Abu Dhabi narrowly beat Dubai in terms of the strength of its respective smart city technology base (18.4 to 17.3), demonstrating that the UAE capital certainly has the potential to lead the country and indeed the region in the race to achieve sustainable urban smart growth. In October last year, Abu Dhabi's Department of Urban Planning and Municipalities launched the pilot phase of the Zayed Smart City Project: a five-year plan to promote the development of smart city technologies powered largely by AI. While the pilot project of test-use technologies is focused on Abu Dhabi's 'Corniche area', the spread of smart services through IoT and AI platforms will spread across the city from now until the end of 2022. Alongside the ongoing development of smart mobility solutions similar to Dubai, Abu Dhabi is also implementing smart projects that will fully rebalance the equation of urban living, which is so often associated with waste and environmental damage. Just last month, for example, Abu Dhabi's Masdar City unveiled a demonstration of smart home farming called "Bustani" in one of its original eco-villas. This annual open exhibition reveals 15 distinct technological innovations that will enable Abu Dhabi citizens to grow their own

food sustainably at home, turning consumers into producers and radically improving the food security of the city and the region. [62]

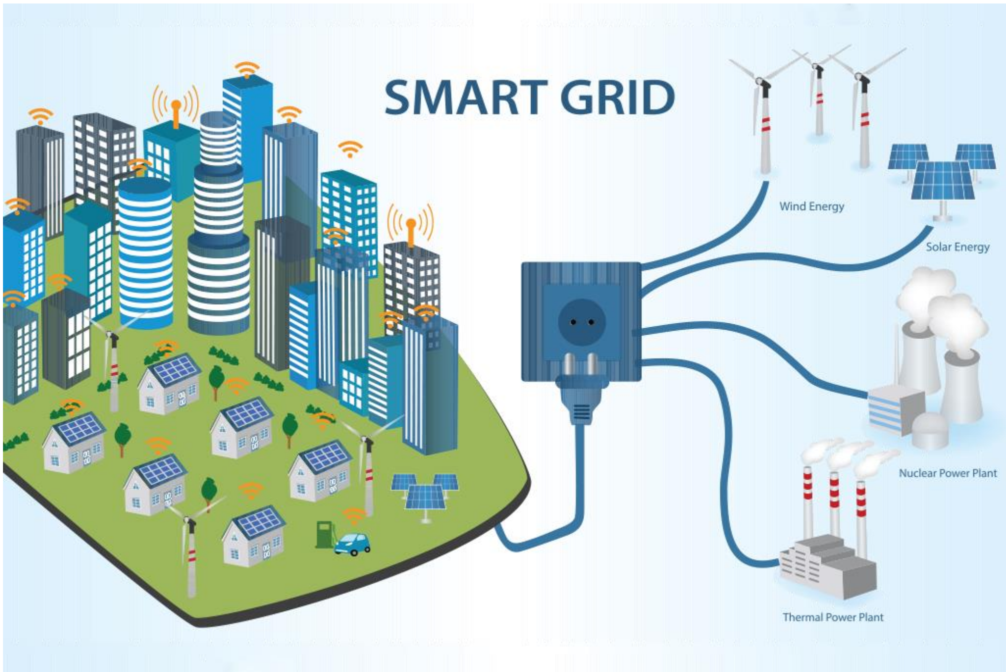
5. Manila (Philippines)
   There have also been restoration projects in the Manila Bay area in the past, such as the current Aseana City development, but the option of restoration as a land bank remains on the developers' radar. The New Manila Bay Pearl City is a redevelopment project that is expected to be developed in the coming years. The 407.42-hectare rehabilitation project will be financed and developed by a consortium led by local company UAA Kinming Group Development Corp. With global partners from Hong Kong, mainland China, Southeast Asia, Europe and other regions. New Manila Bay will also have a central business district that will offer other services such as housing, retail, entertainment, infrastructure, medical, education, sports and other ancillary facilities. [63]
6. Bangkok (Thailand)
   As part of its Smart City Action Plan, Bangkok is focusing on building infrastructure and achieving a quality environment that could ease its transport problems. There are plans to develop Bangkok's still nascent public transport network so that 60% of the city's residents can rely on public transport for their daily commute, as opposed to the 40% that currently do. The express rail network in Greater Bangkok is also to be extended to more than 500 kilometres by 2029. In terms of sustainable living conditions, the One Bangkok "city within a city" area will be an integral part of the smart city development. It will be guided by IoT data and cover an area of 16.7 hectares. With eight hectares dedicated to green and open spaces, the project is set to be a prime example of human-centric and environmentally sustainable living in the smart city. In terms of energy-efficient buildings, Bangkok is home to Park Ventures Ecoplex, which houses the Okura Prestige Hotel in the capital's central business district. The hotel is the first building in the city to be awarded a LEED (Leadership in Energy and Environmental Design) platinum rating. [64]
7. Tabuk (Saudi Arabia)
   NEOM is a smart city under development in Tabuk. The original plans were for a city with artificial intelligence, flying taxis and an artificial moon. In January 2021, this plan became more concrete and tangible when Prince Mohammed bin Salman unveiled The Line, a 170-kilometre-long linear urban community development connected by an underground public transport network. It will connect the Red Sea coastline with the mountains and valleys of northeastern Saudi Arabia. It will be the cornerstone of Saudi Arabia's Vision 2030 and an economic engine for the Kingdom, as it will promote diversification and aims to contribute 380,000 jobs and $48 billion to domestic GDP by 2030. NEOM, presented as a "living laboratory" consisting of towns and cities, ports and business zones, research centres, sports and leisure venues and tourist destinations. It will include a range of innovations based on sustainability and technology, as outlined below:
   Solar energy, wind energy... Solar energy, wind power, wind energy, wind energy, wind power, and green hydrogen. NEOM will be one of the world's leading producers of green hydrogen, as it is one of the few places in the world where it can be produced competitively and in large quantities. NEOM's water distribution network will be fully connected through an advanced Internet of Water infrastructure, providing high quality drinking water and recycled water throughout the network, while removing wastewater.

Finally, thanks to Artificial Intelligence (AI), 90% of the data collected will allow for improved infrastructure capabilities beyond the 1% used by existing smart cities. [65]

8. DKI Jakarta (Indonesia)
   As part of its smart city development, Jakarta launched Qlue - "the app for the smart city". Qlue is a social networking app with artificial intelligence that allows users to report problems directly to local government and businesses, as well as share information with other citizens. The local government receives an average of 1,400 messages a day through the app. In addition, Jakarta residents send an average of 130 SMS messages a day to the governor's mobile phone and many more via social media and email. Qlue promotes citizen participation and bottom-up engagement by encouraging citizens to complain about poor or incomplete services, make suggestions or share data through various platforms such as Smart Government Dashboard, Smart Environment, Smart Mobility, Smart Media Analysis or Smart Safety. Other smart city applications used in Jakarta include iJakarta, a public digital library, and the Jakarta Smart City Portal (JSC), a portal with city data and information accessible to the general public. For example, users can access footage from the 7,300 CCTV cameras installed throughout the city to monitor crime, traffic congestion, flooding and waste problems. The JSC is one of the government's efforts to improve transparency by centralising and integrating all the data in one place. [64]
9. Hanoi (Vietnam)
   Hanoi has been working on the smart city design since 2016. With a population of 7.6 million, the Vietnamese capital aspires to become a green, culturally rich, urban and modern city with sustainable development to create a better life for its residents by 2030. On the technology front, that the country will adopt 5G within two years, which will give a huge boost to the development of Hanoi's smart city infrastructure. The action plan for Hanoi's smart city includes the establishment of a smart business centre, which will include a number of functional nodes, including a support centre for the city's IT staff, a data analysis centre and a centre for traffic supervision, traffic control and crime prevention. In the education sector, 2,700 schools and universities are being integrated into an electronic system where school reports and enrolment data will be easily accessible electronically by students and teachers. And in terms of transport, the city is working on a digital traffic map to ease traffic congestion. Hanoi, along with Ho Chi Minh City, is using the iParking app in some districts. Thanks to this app, drivers can find free parking spaces and pay from their smartphones easier and faster. [64]
10. Tokyo (Japan)
    The Tokyo Smart City Initiative is an international collaboration from 2016 to 2020 between the Eco-City Laboratory of School of Urban Planning and Regional Planning and the Georgia Institute of Technology School of Architecture, the Global Carbon Project (GCP), the National Institute for Environmental Research, Japan and the Department of Civil Engineering, University of Tokyo. Tokyo provides a living urban laboratory for the accumulation of complex urban layouts, physical, cultural and technological systems. Tokyo Smart City Studio will explore Shinagawa and surrounding areas in the Tokyo Bay area in spring 2020 as part of the development of the new Maglev train station area, one of the city's largest urban developments in the next ten years. The opening of the new Maglev HSR station in 2030 will make Shinagawa the new 70-70 gateway, 70 minutes from Tokyo to Osaka for a region with a population of 70 million. The new infrastructure will compress the concepts of space

and time, changing the relationship between cities. The future vision of the city will have a profound impact on urban form, function and experience. The project aims to develop an urban design test bed to show how Japan can design, evaluate and implement smart communities by integrating government agencies, stakeholders and communities, with a focus on urban planning and modelling, big data urban analytics; Internet of Things (IoT), smart transportation and eco-city performance evaluation. [66]

Chapter 4 : Smart Energy Grid



[67]

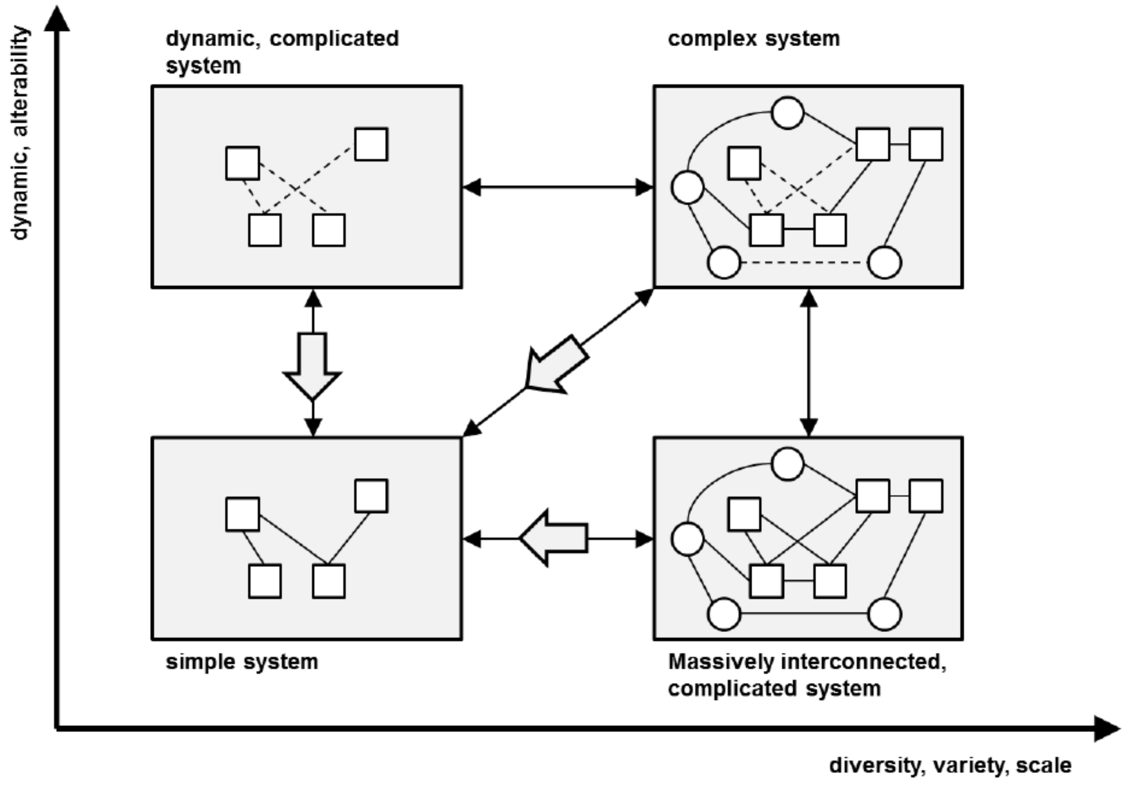
4.1 Definition of Smart Grid

A smart grid is a power grid that enables the two-way flow of power and data through digital communications technology, enabling detection, response and proactive measures to changes in usage and multiple problems. Smart grids are self-healing, making electricity customers active participants. Big data analytics and IoT technologies are important technology drivers in the smart grid, where analytics are moving to the edges, such as peak computing. Smart grids use more technology, but not just computing or even technology. Smart grids have multiple uses and the transition from traditional grids to smart grids is due to many factors, such as the liberalization of energy markets, developments in metering, changes in the level of power generation, decentralization (distributed energy), the advent of the involved 'prosumer', changing regulations, the rise of microgeneration and (isolated) microgrids, renewable energy mandates with more energy sources and new points where and purposes for which electricity is needed (e.g. electrical vehicle charging points). [68]

4.2 Smart Grid Architecture Model

The original scope of the SGAM was created in the M/490 mandate of the European Commission (EC) to the European standardization bodies CEN (Comité Européen de Normalisation), CENELEC (European Committee for Electrotechnical Standardization), and ETSI (European Telecommunications Standards Institute) with the focus on finding existing technical standards applicable to Smart Grids as well as identifying gaps in state-of-the-art and standardization.

Looking at an intelligent network from a systems engineering perspective, it can be classified as a complex system. More specifically, it can be said that the network evolves from a massively interconnected complex system to a complex system. As shown in the figure below, such a system is characterized by the subsystems that constitute it and reflect a degree of diversity/variety/scale on the one hand, whose structure is governed by, while on the other hand, a certain dynamic/volatility.



However, in the recent past, a subset of complex systems has been identified as a System-of-Systems (SoS), characterized by at least eight criteria supported by Maier and DeLaurentis:

1. Operational Independence of Elements

2. Managerial Independence of Elements

3. Evolutionary Development

4. Emergent Behavior

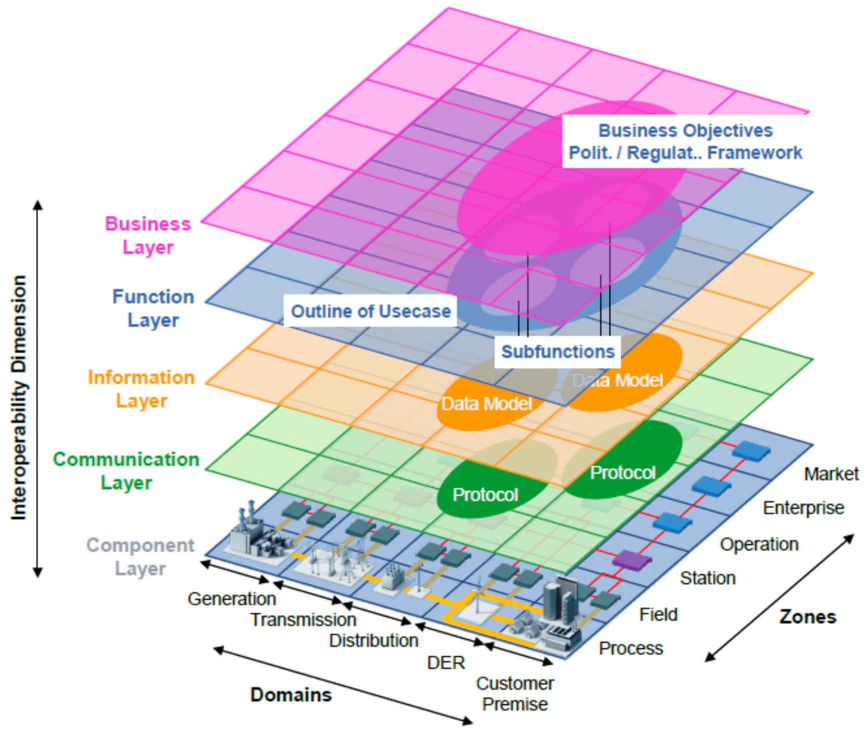
5. Geographical Distribution of Elements

6. Interdisciplinary Study

7. Heterogeneity of Systems

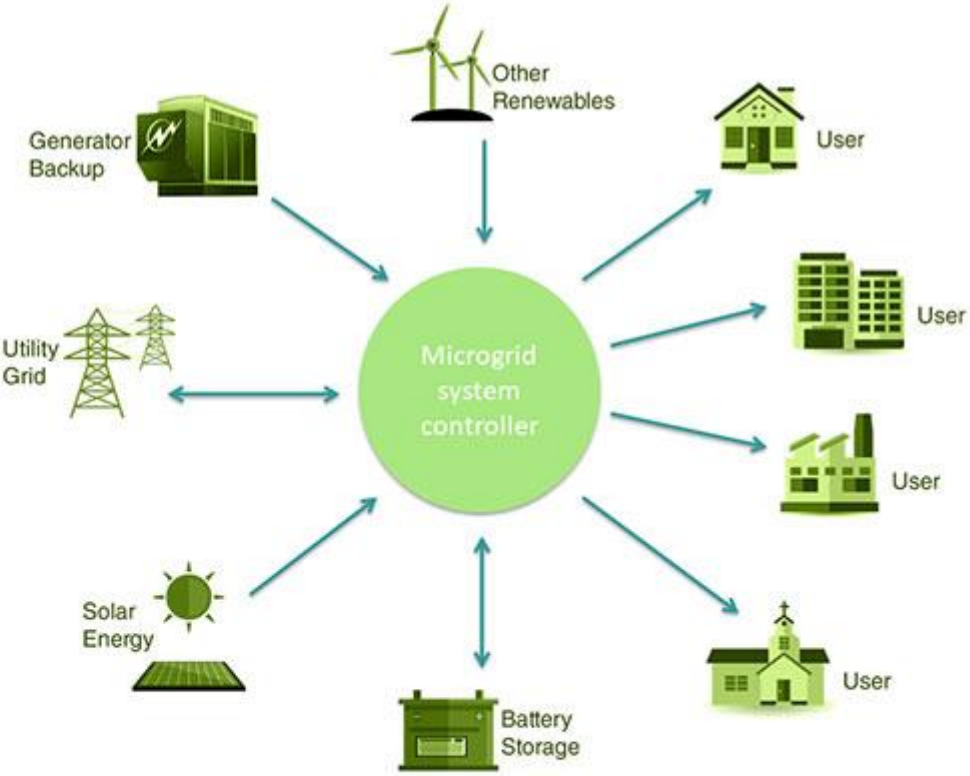
8. Networks of Systems

The SoS perspective is important for considering interoperability between component systems. This challenge has been identified mainly as a standardisation issue. It is clear that integration cost drivers are mainly derived from incompatible technical models and semantics. To address these issues, standardisation bodies are publishing work on reference architectures and corresponding roadmaps. This work serves as an initial focus for fundamental methods engineering research on how to model and document smart grid architectures using standard, prescriptive methods. In addition to IEC 62559 use case standards and methods to document essential blueprint solutions, for Smart Grid systems of systems to be implemented, the SGAM has been created for the purpose of identifying gaps in existing and future standardization. The SGAM acts as a reference designation system, providing three main axis for the dimensions of: (i) value creations chain ("Domains"); (ii) automation pyramid ("Zones"); and (iii) interoperability ("Interoperability Layer").



[69]

4.3 Micro Grid



For decades, most countries have relied on large grids to meet their electricity needs. However, with the rapid development of technology, mini-grids around the world have made significant contributions in recent years, especially in meeting the needs of remote mini-grids, including microgrids, microgrids and nano-grids.

A minigrid is a utility that is smaller in capacity and geographic scope or may be a specific set of microgrids. A microgrid system is a small power supply system consisting of loads and distributed energy resources (DER) such as renewable energy sources (RES), cogeneration, combined heat and power (CHP), fuel cells and energy storage systems. Nano-grids are individual power domains; individual physical layers of power distribution, reliability, quality, capacity, price and management.

They achieve specific local goals, such as reliability, carbon reduction, energy diversification and cost reduction, defined by the communities they serve. Like large-scale grids, smart grids generate, distribute and regulate the electricity that flows to consumers, but locally. Smart microgrids are an ideal way to integrate renewable resources at the community level and allow customers to participate in the electricity business. They are the building blocks of the Perfect Electricity System. [70]

4.4 Cybersecurity issues in Smart Grid

Due to the heterogeneous communication architecture of the smart grid, the challenge is to design complex and robust security mechanisms that can be easily deployed to secure the communications between the different layers of the smart grid infrastructure. The traditional grid is now moving towards a smart grid. Smart grids combine traditional power grids with information and communication technology (ICT). This integration enables electricity suppliers and consumers to improve the efficiency and availability of electricity systems while continuously monitoring, controlling and managing customer demand.

A smart grid system must have several main security objectives:

- Uninterrupted power supply can be provided according to user requirements,
- Integrity of the information communicated.
- Confidentiality of user data. We need to focus on the major vulnerabilities in the network, the different attackers and the types of attacks they can carry out, as well as the necessary security solutions.
- Predictive analysis, passive security with intrusion control and mitigation are not sufficient for critical CPS and similar smart grids. Unlike traditional computer systems, the impact of an attack on critical infrastructure can be devastating in terms of damage and consequences. Therefore, it is necessary to prevent the identification of potential threads in order to reduce the attack area of smart grids and avoid harmful consequences.
- Security analysis of automated large-scale and hybrid systems such as smart grids. The smart grid security guidelines developed by NIST are very detailed.
- Dynamic security measures are the ability to provide security and resilience in smart grids by introducing flexibility in system properties.

In this section the security risks in Smart Grid will be reviewed as well as discussions on some possible attacks on Smart Grids and possible security solutions.

These suggestions are potential common threats that could pose an effective threat to the smart grid. Smart grids can take on many risks that affect not only organizations but also ordinary customers. These risks can pose a significant threat to personal privacy, such as sensitive customer information, the risk of information theft or business termination. These risks do not only exist when using the Internet, but also affect customers at home and competitors may collect personal information.

- Phising: Phising can be the first step to compromising customers and organizations because the process is so easy to perform.
- Denial of service: Denial of service (DoS) is a strategic attack and any attack on availability is part of a DoS attack. On the smart grid side, all leading smart grid services are available, which means that smart grids are more vulnerable to denial of service attacks. Smart grid connection links need to be secure and reliable. The reason the connection link must be reliable and secure is because the smart grid uses a distributed architecture system to distribute the connection to countless devices in a larger area. If there is an attack (Dos) on the smart grid, it will suffer huge losses.
- Malware spreading: The most significant threat an intelligent network can face is the spread of malware, which is the biggest concern. Attackers can develop malware that can infect an organization's servers and devices.
- Eavesdropping and traffic analysis: Eavesdropping and traffic analysis are types of eavesdropping attacks. Attackers can obtain sensitive information by monitoring network traffic. A smart grid will face this risk because the network it contains is large, the smart grid contains many network nodes and it is difficult to keep devices connected to the larger network. [71]

4.4.1 Cybersecurity issues in devices – Attack in devices

The security of IoT devices has long been an issue and inevitably leads to small and large-scale attacks. Most of these attacks stem from simple security issues, such as maintaining default passwords for telnet services. Below we will analyse some of the most important cybersecurity issues.

1. Incorrect access control
   Services provided by IoT devices should be accessible only by the owner and those in the immediate environment they trust. However, device security systems are often inadequate to meet this requirement and IoT devices can trust the local network without further authentication or authorization. Any other device connected to the same network is also trusted.
2. Overly large attack surface
   Each connection that can be made to a system presents an attacker with a new set of opportunities to discover and exploit vulnerabilities. The more services a device provides over the Internet, the more services can be attacked. This is called surface area. Reducing the attack surface is the first step in securing your system.
3. Outdated software
   As software vulnerabilities are identified and resolved, it is important to distribute vulnerability updates, any known vulnerabilities after device deployment. For example, the malware Linux. Darlloz was first discovered late 2013 and worked by exploiting a bug reported and fixed more than a year earlier.

4. Lack of encryption
   When devices communicate in plain text, all information exchanged with a client device or support service can be retrieved by an intermediary (Man-In-The-Middle). Network traffic may be monitored and sensitive data, such as login credentials, may be obtained. Even if the data is encrypted, vulnerabilities may exist if the encryption is incomplete or incorrectly configured. For example, a device may not be able to verify the authenticity of the other party even if the connection is encrypted, it may be intercepted by a MITM attacker, and sensitive data stored on the device should also be encrypted. The downside is that Lack of encryption stores API commands in plain text on the device, cards or credentials.
5. Application vulnerabilities
   Recognizing that software contains vulnerabilities from the beginning is an important step in securing IoT devices. Software vulnerabilities can enable functions on a device that developers don't want, which in some cases could allow an attacker to execute their own code on the device, allowing sensitive information to be extracted or elsewhere.
6. Lack of Trusted Execution Environment
   Most IoT devices are essentially general-purpose computers that can run specific software. This allows attackers to install their own software with functions that are not part of the normal operation of the device. For example, attackers can install software that performs DDoS attacks. By limiting the capabilities of the device and the software it can run, the possibility of misuse of the device is reduced. To limit the software a device can run, code is typically signed with a cryptographic hash. Since only the vendor has the key to sign the software, the device will only run software distributed by the vendor. This way, an attacker can no longer run arbitrary code on a device.
7. Vendor security posture
   When a vulnerability is discovered, the vendor's response largely determines the impact. Vendors can play a role in receiving information about potential vulnerabilities, developing mitigation measures, and updating field devices. A vendor's attitude towards security often depends on whether the vendor has a process in place to adequately address security issues.
8. Insufficient privacy protection
   Consumer devices often store sensitive information. Devices deployed on a wireless network store passwords for that network. Cameras can provide video and audio recordings of the homes in which they are deployed. If an intruder could access this information, it would constitute a serious breach of privacy. IoT devices and related services should only handle sensitive information properly and securely with the consent of the end user of the device.
9. Intrusion ignorance
   When a device is compromised, it generally continues to function normally from the user's perspective. Usually no additional bandwidth or power consumption is detected. Most devices do not have logging or alerting capabilities to notify users of any security issues. If present, they can be replaced or disabled when the equipment is damaged. The result is that users rarely find their devices compromised or tampered with, preventing them from taking mitigation measures.
10. Insufficient physical security
    If an attacker has physical access to the device, they can open the device and attack the hardware. For example, any protection software can be bypassed by directly reading the

contents of the memory component. In addition, the device may have debugging contacts that can be accessed after the device has been switched on, providing the attacker with additional functionality. Physical attacks have an impact on a single device and require physical interaction. Since it not possible to perform these attacks en-masse from the Internet, we do not recognize this as one of the biggest security problems, but it is nevertheless included.

11. User interaction
    Suppliers can encourage the secure development of their devices by promoting their secure configuration. By paying close attention to usability, design and documentation, you can drive users to secure configurations. There is some overlap between this category and the other categories above. For example, the inappropriate access control issues listed above include the use of insecure or default passwords. One way to overcome this is to have the user interact with the device to make it very easy or even mandatory to configure a secure password. For most of the above security categories, it is difficult for non-technical users to assess whether a device meets the requirements. [72]

This type of attack is capable of disrupting IoT devices. The primary goal of the attacker is to compromise critical system architectural functions (depending on the devices involved). In an RFID-based inventory control system, a successful attacker can "take down" the entire network (for example, when the target is a server). In a Neighborhood Area Network (NAN), an attack on one device can affect the resilience of the network, in extreme cases leading to a distributed denial of service attack across the network. Device attacks can be caused by IP misconfiguration, memory corruption, and malicious code execution in the device's operating system at the middleware level. [73]

4.4.2 Cybersecurity issues in network – Attack in network

The potential networking problems in Smart Grid are mainly focused on internet, wireless networks and sensor networks. Just like the Internet, multiple networking technologies can be used for SG including fiber optics, Land Mobile Radio (LMR), 3G/4G (WiMax - Worldwide Interoperability Microwave Access), RS-232/RS-485 serial communications, WiFi wireless networking technology, and others. Which one to use depends on the requirements of the network environment and is an open issue in the development of new SG communication standards. [74]

For wired networks, passive Ethernet passive optical networks (EPON) could be a promising solution for Smart Grid broadband access networks due to the following characteristics: 1) backward compatibility, 2) low fiber usage and maintenance costs, and 3) minimal network protocol overhead. EPON has also been designated as the next generation Gigabit-Ethernet by the IEEE 802.3ah standard. However, EPON can easily become vulnerable to denial-of-service, spoofing, and eavesdropping attacks. [75]

For wireless networks, radio waves could be potential vulnerabilities against attackers. In particular, such an unprotected physical medium could reveal energy consumption data and thus cause an intrusion of personal data. NIST claims that the IEEE 802.11i wireless local area network security standard can help secure wireless network deployment in the Smart Grid. Other research argues that Smart Grid wireless networks can be made more secure using existing standards such as IEEE 802.16e (Mobile WiMax), and the cutting-edge 3GPP LTE technology. Possible technologies used for security in wireless networks are EAP (Extensible Authentication Protocol), 4-way handshake, AES-CCMP (AES-Counter Mode CBC-MAC Protocol), CBCMAC (Cipher Block Chaining Message Authentication Code), PKMv2 (Privacy and Key Management version 2), 128 group encryption key algorithms, 3DES (Triple Data Encryption Standard), RSA acknowledgement message and others. However, their applicability to the Smart Grid has not been further analysed. [74] [76]

For sensor networks, to date, researchers have reached a consensus that wireless mesh networks should be used in the AMI infrastructure. The main reason for this is that mesh networks can overcome bad nodes by using redundant communication paths. However, the IT industry has documented a number of attacks against wireless mesh network technologies such as cross-layer traffic injection, node impersonation, route injection, message modification and others. Most existing routing protocols do not have specific strategies to secure paths and data due to their inherent allocation characteristics. Without routing security, traffic in the AMI network is not reliable. Table 5 summarizes the potential problems of the internet, wireless network and sensor network in the Smart Grid. [74] [76]

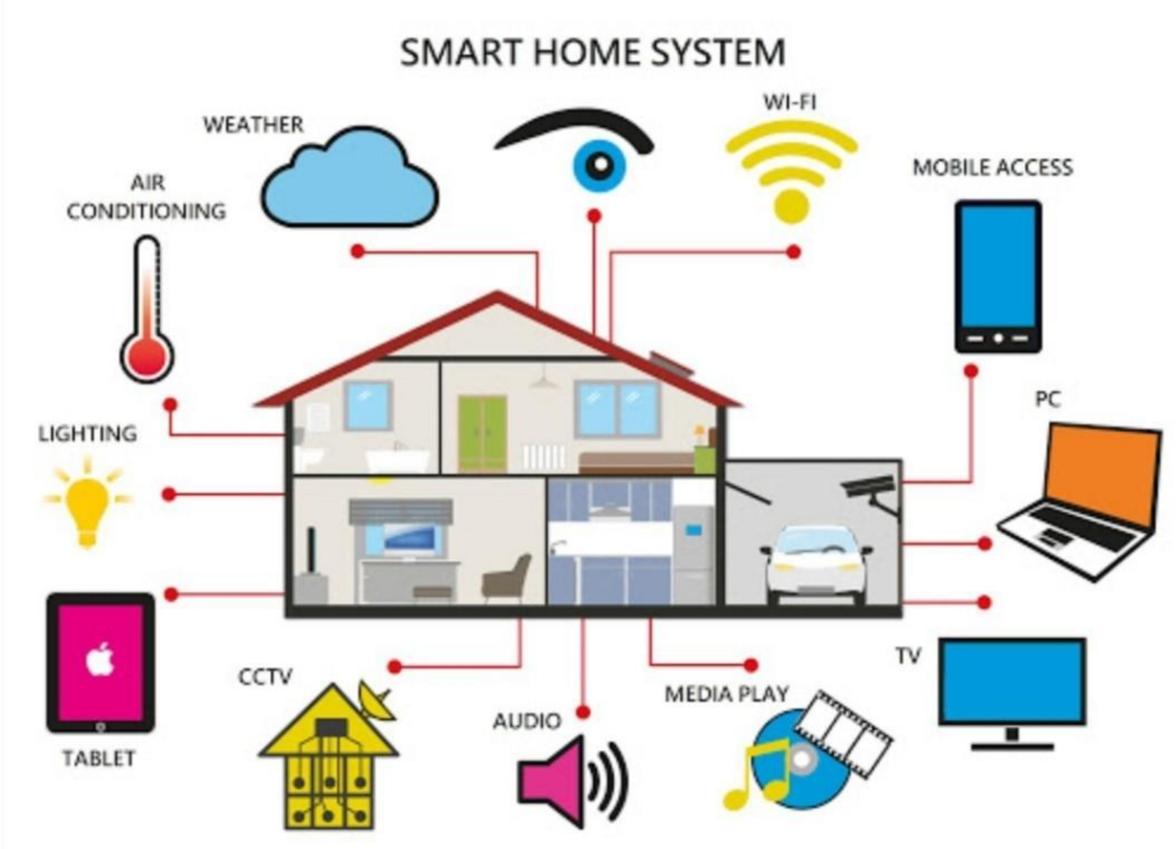
This is an attack that aims to compromise communication between devices, either by delaying forwarding messages or by losing messages. Network attacks may destroy computational processes within IoT systems. In home area networks (HANs) this type of attack is aimed at destroying the functionality of monitoring or interfacing devices. Similarly, in a neighbourhood area network (NAN) this type of attack, could deny connected devices access to vital information from neighbouring devices, and also impede the ability to exchange messages from neighbouring devices. Causes of such attacks include SQL code injection, DoS and code execution. [77]

4.4.3 Anomaly detection issues

Reliable Smart Grid operations require accurate and timely detection of abnormal and unexpected events. The ways of detecting faults and faults in the power grid need to be reviewed and studied in a model that includes including systematic malicious manipulation. [75]

To meet the criteria for automated fault analysis in the Smart Grid, several studies have been conducted, many of which are still ongoing. These include: 1) a plan to detect, categorize and mitigate a series of events in the intercom data at the local level and system-wide, 2) implementation of an optimal fault location algorithm using data from substation IDEs devices, as well as data from the SCADA PI and simulation data from short circuit analysis programs, 3) development of a risk-based asset management methodology for maintenance planning that takes into account data collected from substation IEDs, 4) proposal of a smart processor with a risk signal to exploit enhanced data protection by interpreting the cause and effect relationship between signals, 5) a protective relaying system based on a neural network allowing simultaneous improvements in reliability and security of transmission line protection. [78]

4.5 How to attack a Smart Home



A smart home is made up of a number of different devices connected to the internet of things (IoT), each with a specific set of functions. No matter how different these devices are from one another, they have the shared goal of streamlining the tasks and simplifying the lives of their users. Together they paint an enticing image of comfort and convenience. However, just as these devices have revolutionized home living, they have also given rise to new complications for home security.

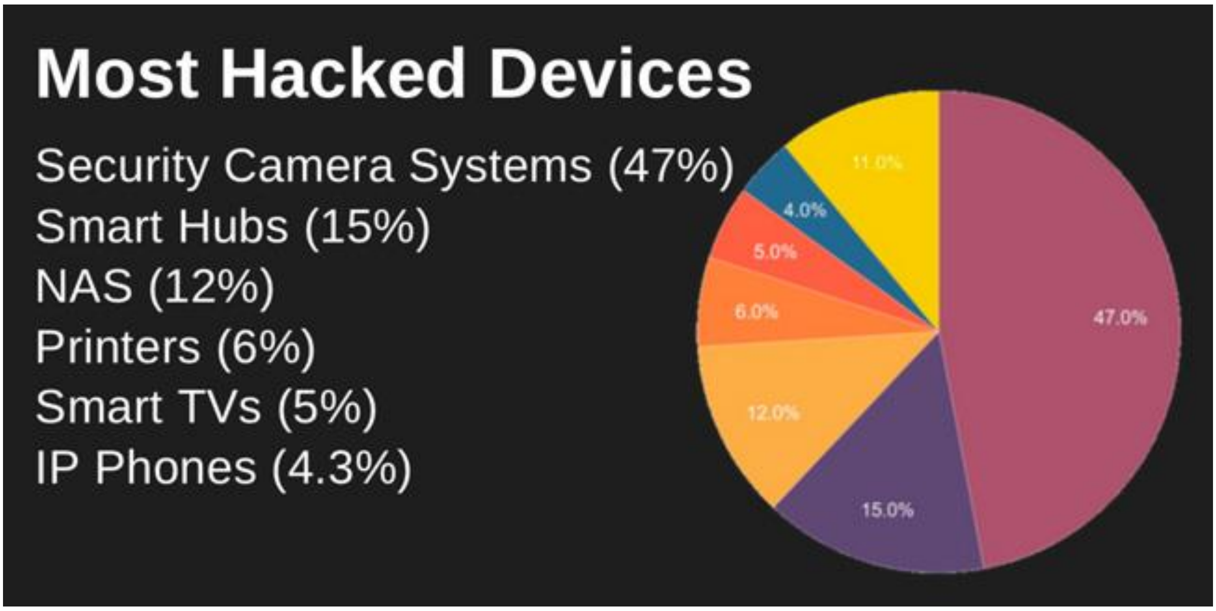
4.5.1 Attack Scenarios

Many of the individual attacks made on IoT devices can be ignored by their users as harmless. However, once a device or system has been compromised, attackers can use this as the starting point to carry out a combination of actions to escalate their attacks, under the impression that they will cause harmful consequences. In this section we will describe two scenarios that can result from a breach of a smart robot vacuum cleaner inside a smart home.

The owner of the smart home believing that the device is only connected to the home network does not fear exposure from a malicious intruder. But in reality, the UPnP (University plug play) function of the device automatically connects to the home router, thus exposing it to the internet. If there are no security measures in this exposure attackers are free to compromise the device as part of their attack.

Once the device is compromised the attackers use it to familiarize themselves with the "layout" of the home. They then move through the home's network to compromise other devices. Using a combination of different actions and compromised devices within the smart home, attackers can plan various attacks, two of which we describe below. [79]

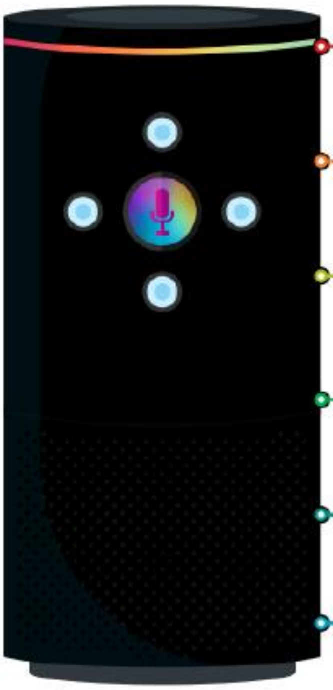
4.5.2 Break-in a Smart Home



[80]

Attackers can monitor residents using IP cameras installed in the house, so using a clever plan they can lure residents into a room or away from the entrances of the house. The attackers will then open the necessary smart locks in order for a partner/burglar to enter, while disabling the alarm system to avoid alerting neighbours and authorities. While the partner/burglar is inside the house, the attackers can additionally disable IP cameras or any other photo or video recording media in order to conceal the partner/burglar. Once the partner/burglar exits the house the attackers can control the smart locks to give the partner/burglar the necessary time to escape. [79]

4.5.3 Levels of Attack



Attack layer	Security issues	Risks
Hardware	› Ease in being dismantled and further examined › Existing debug port	› Hackers can connect to the JTAG UART, I2C, and SPI of the system without any security limitations.
Firmware	› Credential issues › Backdoor issues › Unpatched firmware › Buffer overflow issues › Privilege escalation	› Hackers can use the default and hard-coded passwords in the firmware. › Hackers can easily predict these passwords and access the system easily.
Operating system and application	› Unpatched operating system › Buffer overflow issues › Privilege escalation › Possibility of man-in-the-middle (MitM) attacks	› Buffer overflow (stack, heap, and integer) can allow hackers to gain privilege or control over the system
Web interface	› SQL injection › Directory traversal › Buffer overflow issues › Cross-site scripting (XSS) › Cross-site request forgery (CSRF) › Use of default or sample pages › Privilege escalation issues › Other OWASP issues	› Hackers can gain access to the system without the need for a password. › Hackers can get information that the web interface should not provide (e.g., internal IP address, system structure, directory name, and database configuration).
Protocol	› DoS or DDoS › Session hijacking › Authentication bypass › Media access control (MAC) spoofing attacks › PIN cracking attacks › MitM attacks › Hard-coded key attacks › Replay attacks	› Hackers can disable the device function by flooding the connection bandwidth. › Hackers can initiate hijacking sessions to send forged data. › Hackers can steal data or credentials through MitM attacks. › Hackers can replay stolen data to bypass authentication.
Policy	› Misconfigured policies › Policy violations	› Hackers can leak sensitive data, such as credentials, connection strings, IP addresses, and internal network topology. › Hackers can gain unlimited access to the system. › Unknown exposure outside the network through settings like enabled UPnP in devices.[2]

[79]

Some of the questions that need to be answered are what are the factors that allow attackers to compromise IoT devices. One factor is that, there is no security from the design phase in the set of IoT devices in the market. Another factor is the poor configuration of many IoT devices, which are configured according to what is convenient for users rather than what is secure. Lack of security by design can lead to more vulnerabilities. Also, poor configuration can lead to inability to certify security. Not eliminating these two factors exacerbates the problem because many attackers are determined to find vulnerabilities in IoT devices.

Attackers can start at the deepest layer of an IoT device, the physical motherboard. There they can find the hardware debug port or communication port, e.g. JTAG UART, I2C and SPI. From there they can look for passwords using code, hidden doors in hardware or software and vulnerabilities in firmware. They can also search for entry points in the form of operating systems and application bugs. They can also be directed to the device's web interface to look for web bugs. In addition, they can try to look for vulnerabilities in communication protocols, e.g. Bluetooth, Zigbee, Z-Wave, NFC, 4G, 5G and IEEE 802.1x. Attackers can also follow policies, which may contain sensitive information or maintain settings that may expose the device outside the home network. In Figure 7 we show the attack levels on an IoT device. [79]

4.5.4 Protection against Attacks

The fact that attacks are possible within the confines of the home makes it critical to secure IoT devices against them. With this in mind, here are some questions for users to consider in relation to the relevant indicators, with the aim of helping to improve the security of smart homes. [79]

1. What devices are used in the smart home?

The first thing users should do is to look at all their devices. This way users can assess the security risks their home may face based on the complete list of connected devices.

2. How many vulnerable devices are there?

Having compiled a list of their smart home devices, users can begin to assess the number of known vulnerabilities each device may have using a security scanning app. They can also search for vulnerabilities in the Common Vulnerability and Exposure (CVE) database using the names and versions of the devices. This information can help in assessing security ratings and severity ratings of vulnerabilities faced by users. Creating a list of vulnerabilities, CVE information, device names and versions can be a good reference point for users.

3. Which vulnerable devices can be easily hacked?

Users can refer to the list they have created to find and download the necessary "patches" from the official websites of the respective vendors. This step is called vulnerability management. At this point users should have some idea of the risks against the home security environment.

4. How much information do users possess?

To really answer this question users need to take a deeper look at their devices. This means reading the device manuals and checking the settings of each device. Although the information gathered from this question is important, it is not enough to fully assess the security risk of the home environment. This is because users do not yet know the configuration of the device, including its security credentials. Users will now have to study each device manually and carefully, even consulting its packaging and manual. They should note and take seriously all warning messages, if of course they exist. They should also change all default passwords to strong, unique and secure ones.

5. How many devices can be protected using a security gateway?

Overlaying a device can cause problems in some cases. A code update can either cause the device to become unusable or fail to perform its original functions. A good option is to run a virtual patch from the gateway. This means that users will not have to patch the actual device, but block attacks from the gateway.

6. How long will it take to replace or remove the dangerous devices?

At this point users should have all the information they need to know the security risks their home is vulnerable to. The next step is to assess the time it will take to replace or remove vulnerable devices that can no longer be fixed or protected. This assessment is the beginning of a process called risk management.

7. What should users do?

Based on the information users have gathered from the questions above, they should be able to identify their home's weak points and consider possible solutions. These steps are simplified into the following three:

- Vulnerability partitioning: timely code and firmware updates are two initial actions users can take, since updates are usually related to security issues. Users can choose to enable the automatic update feature on supported devices to ensure that updates are applied as soon as they become available.
- Changing default password settings: when users go through the settings of their devices one by one, they can take the opportunity to make the necessary modifications to make the devices more secure. They should immediately change the default or easy-to-use passwords and use unique and strong passwords for multiple accounts. When configuring devices, users should avoid using PII, especially with router settings.
- Device isolation: users should consider implementing home network segmentation for certain devices and isolating them from the entire home network. This is necessary especially for vulnerable devices that cannot be fixed, but on the other hand cannot be replaced or removed by users for any reason. [79]

Chapter 5 : Privacy

[81]

5.1 Definition of Privacy

There is no universal, internationally accepted definition of "privacy" as it can mean many different things to different people. Originally the first definition given by Samuel D. Warren and Louis D. Brandeis defined privacy as ¨the right to be alone¨. Privacy is not a clearly defined concept and is not just the standards provided by laws and regulations. Moreover, privacy should not be confused, as is often the case, with confidentiality and personal information with confidential information. Confidential information is information to which access should be specified only to those with a business need to know and could result in the compromise of the system, data, applications or other business functions if disclosed to others.

In addition, privacy can often be confused with security, which although there may be overlap between the two, are also separate concepts. There can be security without privacy, but there cannot be privacy without security: it is a part of privacy. Security involves ensuring the integrity, confidentiality and availability of data. However, privacy protection goes beyond proper authentication and similar security protections. It also addresses needs such as ensuring that data is used only for the purpose for which it was collected and is properly disposed of when it is no longer needed to achieve that purpose.

It is important to understand that considering privacy in relation to SG involves consideration of the rights, values and interests of individuals: it includes the relevant characteristics, descriptive information and identifications, activities and opinions of individuals. Privacy is affected by the practices of the customers who provide and the entities that collect or manage this data. [76] [82]

As a broader interpretation, privacy concerns the integrity of the individual and therefore covers all aspects of his or her social needs. For example, privacy can be divided into four categories as follows:

1) **Privacy of personal information**: This is the most common category. Personal information is any information about an individual that can be identified, directly or indirectly, from that information and in particular it may refer to a personal identification number (PIN) or one or more particular features of his or her physical, mental, cultural, economic, geographical or social identity. Privacy of personal information includes the right to control where, when, how, to whom, and to what extent an individual shares his or her own personal information, as well as the right to access, correct, and ensure the protection of personal information provided to others.

2) **Privacy of the individual**: This is the right to control bodily integrity. It covers things like physical requirements, health problems and required medical devices.

3) **Privacy of personal conduct**: This is the right of individuals to retain any knowledge of their activities and choices without sharing them with others.

4) **Privacy of personal communications**: This is the right to communicate without excessive surveillance, monitoring or censorship by other individuals or organizations. [83]

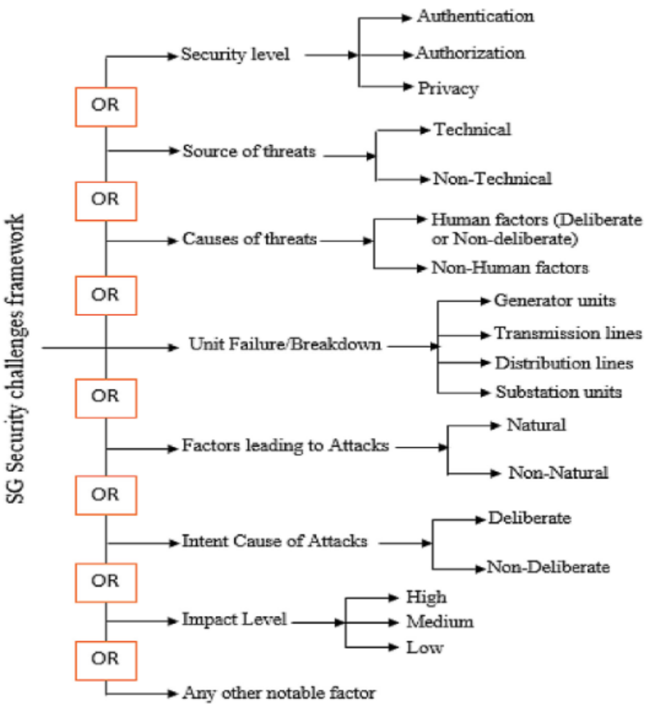
New data on energy consumption collected outside of smart meters, such as home energy management systems, is also generated through applications of smart grid technologies. As this data becomes more specific and available to additional individuals, the complexity associated with privacy issues increases. The identification of these issues in the Smart Grid, as well as opportunities and recommendations for mitigating them, was assigned to the Privacy Subgroup of the Cyber Security Working Group. In addition, this group sought to clarify expectations, practices and rights related to privacy in the Smart Grid. [84]

5.2 Risks in Smart Grid

The Smart Grid architecture and infrastructure face countless security threats and challenges, such as theft, cyber attacks, terrorism, natural disasters and many more. If a Smart Grid fails due to any threat, the potential consequences include system outages (small and large) such as IT infrastructure failure, misrepresentation of the true state of the system, chain failure, disruption of consumer devices, disruption of energy markets , human safety risks, etc.

Various security threats and challenges for smart grids have been identified in the past including the risk of large amounts of sensitive customer information being leaked by intruders - theft, destruction of physical assets, spread of malware in cyber systems, transient system failures - vulnerabilities of distributed control equipment - lack of physical protection such as natural disasters or the environment, fire , tsunami, explosions, landslides, dangerous radioactive leaks, pollutants, dust corrosion, inadequate control mechanisms in conventional systems that do not take into account cyber threats - trade-off between security and infrastructure performance as most facilities were built decades ago - industrial difficulty, device replication complexity etc. etc. As a result, various sectors become vulnerable to these threats and challenges.

Given the interconnection and interdependence of infrastructure, the requirement for a reliable and robust power system is critical and must be well structured for safe and efficient power supply. Therefore, well-designed security targets are often considered essential to ensure efficient and reliable operation. These objectives should cover all possible expansion and improvement plans for future networks. Therefore, a secure smart grid should be authentic, accessible and confidential, with a high level of integrity and efficiency, with a high level of certification, acceptance, reliability, robustness, flexibility, resilience (self-healing) and serve mature electricity markets.



[85]

5.3 Personal data in Smart Grid

Under the PIA process, energy data and personal information can reveal something specific in a direct or indirect way about individuals, groups of individuals or the activities of those individuals. SG data such as energy consumption measurements combined with the increased frequency of usage reporting, energy production data and the use of household appliances and devices capable of recording consumption create new sources of personal information.

The direct information traditionally collected by electricity companies can be used to identify individuals through data such as the home number and/or address, the name of the owner of the house or the person living there, the date of birth and some digits of the social security number.

There are potential unintended consequences of collecting, storing, and linking the seemingly anonymous SG data. While current privacy anonymization practices tend to focus on removing specific elements of personal information, studies reported in this area indicate that re-identification and linkage to an individual can occur. This issue, of data re-identification becomes more important as the amount and level of detail of data collected during operations increases with the development of more SG applications. It then becomes important, from a privacy perspective, for electricity companies and third-party entities participating in SG to determine which data elements they will remove the ability to link to specific addresses or individuals when performing data anonymization activities. [86]

5.4 Privacy issues in Smart Grid

There is a wide range of privacy issues in Smart Grid that need to be addressed. These may have an impact on the implementation of Smart Grid systems or their effectiveness. For example, lack of consumer confidence in the security and privacy of their energy usage data can lead to a lack of consumer acceptance and participation, if not litigation. In general, issues related to privacy in Smart Grid fall into one of two broad categories:

Category 1: Personal information not previously available

Category 2: Mechanisms not previously available to obtain personal information

Examples of the first category include detailed information on the devices and equipment used at a given location, including the use of specific medical and other electronic devices indicating personal data and schedules of legal or potentially illegal actions at that location, as well as detailed temporal data on energy consumption at metering sites and individual household appliances.

The second category includes cases where personal information is available from other sources and SG may present a new source for the same information. For example, the physical location of an individual today can be traced from the use of a credit card or mobile phone. Electric vehicle (PEV) charging points increase the ability to track physical location through new energy consumption data.

Activities within a home or building can be detailed from the characteristics of electrical equipment and their time pattern. These can form the basis for drawing conclusions about the activities of people in the house or building (for example, whether the premises are empty).

Although direct communication technology already exists for appliances and other energy consumption data, the implementation of SG can create additional incentives for their use. Appliances equipped with such equipment can transmit energy consumption information to both owners and managers and external parties.

The table below presents some of the possible privacy-related issue areas and provides some breakdown of the nature of the issues according to the categories mentioned above. [86]

PRIVACY ISSUES	***DESCRIPTION***	***CLASSIFICATION***
Disclosure of personal data	Unauthorised disclosure of energy consumption or other personal information.	Category 2: The traditional method of reading consumption meters (either manually or electronically via remote meter reading systems) may allow less potential for manipulation or disclosure of data without the consent of the staff who manage them.
Identifying patterns of personal behaviour/devices used	Smart meters combined with home automation networks or other technologies can detect the use of specific appliances. Access to usage data that can reveal specific temporal and local characteristics of electricity use in specific areas of the home can also reveal the	Category 1: The type of data available from the Smart Grid application can have more detail and availability on a larger scale.

	types of activities and/or appliances being used. Possible uses for this information include: • Reliability and product warranty purposes of appliance manufacturers • Targeted marketing	
Perform real-time remote surveillance	Access to energy use data at the time they occur can potentially reveal things like whether there are people on the premises, what they are doing, when they wake up and when they sleep, where and how many people are in the house/building.	Category 2: There are many real-time surveillance methods. The availability of computerized real-time data would create another way in which such surveillance could be conducted.
Commercial off-network data uses	Storing data on customer energy consumption can reveal information about the customer's lifestyle, which could be exploited by many entities including sellers of a wide range of products and services. Vendors can obtain attribute lists for targeted sales and marketing campaigns that may not be acceptable to some. The data can also be used for insurance purposes.	Category 2: Under existing metering and billing systems, the meter data do not have enough detail in most cases to reveal things about the activities. However, with smart meters, time of use, demand rates and direct load control can generate detailed data that could be sold and used for energy management and peer comparison analyses. As long as this information is useful to external entities, educating consumers on how to protect this data has significant positive effects.

5.5 GDPR and Smart Cities

The General Data Protection Regulation (GDPR) is the EU law (regulation) on the protection of personal data. The GDPR defines personal data as any information relating to an identified or identifiable natural person known as a data subject. This means that the data subject is a natural person (living person) whose data is managed by the data controller.

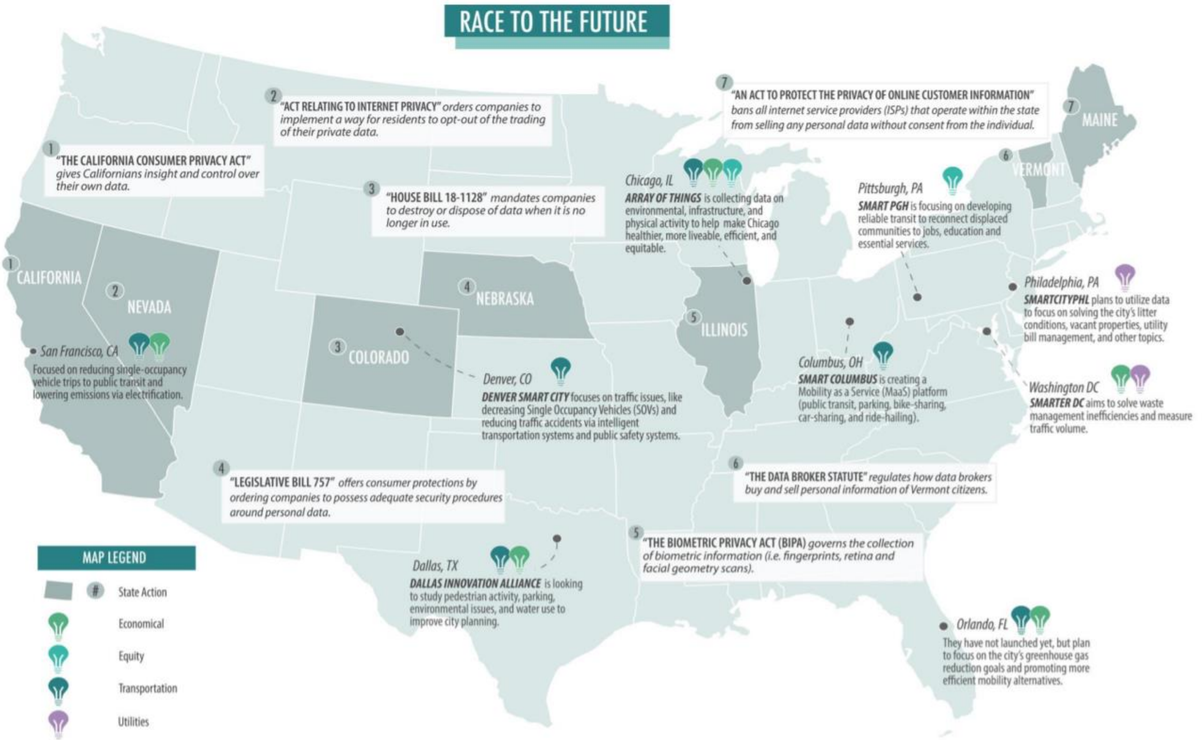
The Regulation applies to the processing of personal data, whether automated (or even partially automated), and sets out the following requirements and principles:

- Transparency - i.e. data processing must be fair, lawful and transparent;
- Purposes - i.e., data should only be collected for determined, explicit and legitimate purposes, and should not be processed later for other purposes;
- Minimization - i.e., the data processed must be relevant, adequate and limited to what is necessary in view of the purposes for which they are processed;
- Accuracy - i.e., the data processed must be accurate and up-to-date regularly;
- Retention - i.e., the data must be deleted after a limited period;
- Subject explicit consent - i.e., the data may be collected and processed only if the data subject gives his explicit consent.

Therefore, the introduction of GDPR in Smart Cities means not only preventing the vulnerabilities that can cause various cyber-attacks, but also addressing the data privacy concerns of people migrating to Smart Cities and using its services. Recently, several proposals have been made to change the architecture of Smart Cities safe while maintaining privacy. They can be roughly divided into the following categories:

- Proposals providing supporting facilities for transforming the GDPR's text into executable access control policies. In this case, the policies are either systematically derived from the GDPR,
- Proposals easily enforceable into the Smart ICT Systems architectures. They can be divided into: (i) those using access control mechanisms for the protection of personal data within Smart ICT Systems perimeters; (ii) those using Smart ICT Systems users location information for authenticating the customer and managing his/her data; and (iii) those exploiting specific security attributes for assuring the GDPR compliance. [87]

5.6 CCPA and Smart Cities



With the growing number of data breaches, lawmakers are taking action to protect their constituents. On June 28, 2018, California passed the Consumer Privacy Act, the most comprehensive consumer privacy law in the United States today. California Consumer Policy Act 2018 (CCPA). The law went into effect on January 1, 2020 and is expected to take effect on July 1 of this year. It shares similarities with the EU's CCPA, which came into force on 25 May 2018, and expands on a previous set of guidelines and directives to provide individuals with certain rights in relation to their personal data. In particular, six states began seeking similar legislation in 2019, while many others are already pursuing a tangential set of legislation. The CCPA may push for federal privacy protections.

The huge amount of data collected seems to be used to optimise operations and smart partitions are no exception, which can include any number of software-supported connected devices on the drive and possibly a common area. Smart apartments are being installed in both new developments and retrofits in existing buildings, not without controversy. It is estimated that one in four new developments in the US in 2019 included some form of smart appliance with associated software. That number is expected to increase in 2020. In addition, diversifying efforts to attract and retain residents as new developments rapidly compete with existing multifamily stock has resulted in more equipment and more data.

Applied to smart cities, the CCPA has far-reaching implications. Owners and managers, property management software (PMS) providers, software and hardware providers, and their hybrids are all responsible for minimal business. The CCPA applies to all personal information, sometimes referred to as PII (Personally Identifiable Information), that is directly or indirectly related, described, associated, or likely reasonably associated with a consumer or household.

California consumers have the right to request the deletion of data collected from consumers at any level of collection (but not from third parties). There are many exceptions, some of which align directly with the stated intent of the smart apartment provider, such as tracking security incidents.

Finally, organizations are required to provide the consumers the appropriate information as to the categories and purposes of the data collected at or before collection and give consumers the right to receive their information upon request. While consumers have a right to opt out of having their data sold, CCPA does not go so far as to allow the opt out of collection. For smart apartment providers, these shouldn’t create onerous burdens, as end user license agreements, terms of service, and privacy agreements are made available in app opt-in. To best serve wary residents, multiple opt-out options (some required by CCPA) and darkened data for occupied units are absolute necessities, if a step beyond. [88]

5.7 PIPL and Smart Cities

China's Personal Information Protection Law (PIPL) is now in force, which sets out the basic rules on how data is collected, used and stored. It also outlines data processing requirements for companies outside China, including security assessments by government authorities.

According to PIPL, multinational companies that transfer personal information overseas should also obtain data protection certification from professional bodies. The legislation was passed in August after several revisions since it was first introduced in October last year. The

Chinese government had said at the time that the new law, which will come into force on November 1, was necessary to address the "data chaos" created by internet platforms collecting too much personal data.

The PIPL also applies to foreign organizations that process personal data overseas for purposes including providing products and services to Chinese consumers and analyzing the behavior of Chinese consumers. A designated agency or representative should also be established in China to be responsible for matters related to the protection of personal data.

According to the Office of the Hong Kong Privacy Commissioner (PCPD), the new legislation includes a chapter dedicated to cross-border data transfers, which states that companies that need to transfer personal information outside of China must first conduct a "personal information protection impact assessment." information."

They must also obtain the individual's consent to the transfer of their personal data and meet one of several conditions. These include agreeing to "standard contracts" issued by authorities that regulate cyber cases and meet the requirements outlined in other laws and regulations issued by the authorities, the PCPD said. These multinational companies should also take the necessary steps to ensure that other foreign parties involved in data processing comply with the data security standards set out in the PIPL. [89]

Chapter 6 : Conclusion

In conclusion, based on the above, it is clear that smart cities and their technological achievements have come to make our lives easier, encouraging us to adopt greener habits. Changes in technology are necessary, and with them come the countervailing risks to the security and privacy of users. We must keep up with these changes and evolve.

Moreover, it is important in this context to protect the principles of privacy and to implement the necessary measures to this end. The implementation of GDPR, CCPA and PIPL are an essential step in the protection of personal data, although the complexity of the systems may make it difficult to use them at times. Nevertheless, if new technologies and privacy principles are properly combined, the way of life of people worldwide will be improved to the maximum.

Chapter 7 : References

[1]	“What is smart city,” [Online]. Available: https://cscl.co.in/what-is-smart-city.
[2]	Ο. Α. Τεχνολογιών, «Ανοιχτές Τεχνολογίες για τη Σύγχρονη Πόλη,» ΕΕΛ/ΛΑΚ , [Ηλεκτρονικό]. Available: https://smartcities.ellak.gr/anichtes-technologies-gia-ti-sigchroni-poli/.
[3]	Μ. Σ. Α. κ. Σ. Γ. Παναγιωτοπούλου, “Έξυπνη πόλη,” 09 Ιούλιος 2021. [Online]. Available: https://el.wikipedia.org/wiki/%CE%88%CE%BE%CF%85%CF%80%CE%BD%CE%B7_%CF%80%CF%8C%CE%BB%CE%B7.
[4]	T. A. P. Taewoo Nam, “Smart city as urban innovation: Focusing on management, policy, and context,” Center for Technology in Government, New York, U.S, 2011.
[5]	C. D. B. P. N. Andrea Caragliu, “Smart cities in Europe,” 3rd Central European Conference in Regional Science – CERS, 2009.
[6]	C. Turner, “SMART CITIES Traveling the timeline Traversing the future,” 2012. [Online]. Available: https://slideplayer.com/slide/4464706/.
[7]	twi.co.uk, “WHAT IS A SMART CITY? – DEFINITION AND EXAMPLES,” twi-global.com, [Online]. Available: https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city#SmartCityDefinition.
[8]	L. G. Anthopoulos, The Rise of the Smart City, Thessaly: University of Thessaly, 2017.
[9]	M. E. Antunes, “Smart Cities of the Future,” Deloitte, [Online]. Available: https://www2.deloitte.com/global/en/pages/public-sector/solutions/gx-smart-cities-of-the-future.html.
[10]	S. Maffey, “Smart Cities of the Future Rely on Innovation, Critical Discussions,” 13 September 2021. [Online]. Available: https://www.globaltrademag.com/smart-cities-of-the-future-rely-on-innovation-critical-discussions/.
[11]	Π. Αθανάσιος, «Η ΥΓΕΙΟΝΟΜΙΚΗ ΠΕΡΙΘΑΛΨΗ ΣΤΗΝ ΨΗΦΙΑΚΗ,» ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ, Καρλόβασι, Σάμος, 2019.
[12]	E. F. a. G. A. Fernández-Montesinos, Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies, Spain: Universidad CEU San Pablo, 2020.
[13]	S. Mazur, “An Introduction to Smart Transportation: Benefits and Examples,” Digi, 09 December 2020. [Online]. Available: https://www.digi.com/blog/post/introduction-to-smart-transportation-benefits.
[14]	fokus.fraunhofer, “Smart Cities and Communities Lab,” Fraunhofer fokus, [Online]. Available: https://www.fokus.fraunhofer.de/en/fokus/smart_cities_lab/topics/communication.
[15]	Tulip, “What Is A Smart Factory? (And What It Means For You),” Somerville, MA.
[16]	E. M. L. F. D. C. P. L. Laurent Probst, “Smart construction products and processes,” European Union, European Union, 2014.
[17]	A. HAYES, “Smart Home,” Investopedia, 10 January 2022. [Online]. Available: https://www.investopedia.com/terms/s/smart-home.asp.
[18]	J. Glasco, “SMART EDUCATION FOR SMART CITIES: VISUAL, COLLABORATIVE & INTERACTIVE,” bee smart city, 27 February 2019. [Online]. Available: https://hub.beesmart.city/en/solutions/smart-people/smart-education/viewsonic-smart-education-for-smart-cities. [Accessed 2019].
[19]	M. B. R. C. Anna Maria Vegni, Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks, Rome: IntechOpen, 2013.
[20]	L. Cano, “What is a smart business? Is yours?,” pandorafms, 27 August 2021. [Online]. Available: https://pandorafms.com/blog/smart-business/.
[21]	B. C. Marc Cram, “Smart cities run on smart power,” Raritan, 2021.

[22]	Scott, “IoT Waste Management In Smart Cities,” wellthatsinteresting.tech, Belgium, 2020.
[23]	M. C. N. D. B. L. Ghadah Al-Dabbagh, “Promoting sustainable agriculture in smart cities,” September 2021. [Online]. Available: https://www.g20-insights.org/wp-content/uploads/2021/09/TF2-PROMOTING-SUSTAINABLE-AGRICULTURE-IN-SMART-CITIES.pdf.
[24]	N. Himasailaja.V, “SMART IRRIGATION FOR SMART CITIES A SYSTEM,” Chennai, Deemed University, 2018, pp. 253-262.
[25]	A. C. Pego, Smart Cities, Citizen Welfare, and the Implementation of Sustainable Development Goals, Portugal, 2021.
[26]	A. Badran, “Developing Smart Cities: Regulatory and Policy Implications for the State of Qatar,” 01 December 2021.
[27]	Intel, “Emerging Public Safety Technology Leveraging IoT,” Intel, [Online]. Available: https://www.intel.com/content/www/us/en/internet-of-things/smart-cities-public-safety.html.
[28]	D. Orme, “The city built for you: how biometric identity will drive personal security in smart cities,” Technative, 02 March 2020. [Online]. Available: https://technative.io/the-city-built-for-you-how-biometric-identity-will-drive-personal-security-in-smart-cities/.
[29]	Prasanna, “Smart City Advantages and Disadvantages | List of All Benefits and Drawbacks of Smart Cities,” aplustopper, 16 January 2022. [Online]. Available: https://www.aplustopper.com/smart-city-advantages-and-disadvantages/.
[30]	N. M. U. Rob Kitchin, “Getting smarter about smart cities: Improving data privacy and data security,” Department of the Taoiseach on behalf of the Government Data Forum, Dublin, 2016.
[31]	M. E. D. Dr. Cédric LÉVY-BENCHETON, “Cyber security for Smart Cities An architecture model for public transport,” December 2015. [Online]. Available: https://www.enisa.europa.eu/publications/smart-cities-architecture-model.
[32]	U. o. Salamanca, “Worldwide Ranking of Smart Cities,” [Online]. Available: https://bisite.usal.es/en/blog/formation/20/10/30/worldwide-ranking-smart-cities-BISITE.
[33]	“Smart Trikala,” [Online]. Available: https://trikalacity.gr/smart-trikala/.
[34]	E. Commission, “100 Intelligent Cities Challenge,” [Online]. Available: https://www.intelligentcitieschallenge.eu/cities/trikala.
[35]	“e-trikala,” [Online]. Available: https://www.e-trikala.gr/projects-services-2/.
[36]	Α. Κασσίμη, «Στα Τρίκαλα η πιο επιτυχημένη στον κόσμο πιλοτική χρήση λεωφορείων χωρίς οδηγό,» *Η ΚΑΘΗΜΕΡΙΝΗ ,* 2016.
[37]	V. Rainey, “Inside Greece's first smart city: 'Now you don't need to know a politician to get something done',” *The Guardian ,* 2018.
[38]	Unknown, «Η ΧΑΛΚΙΔΑ ΒΡΑΒΕΥΕΤΑΙ ΩΣ ΜΙΑ ΕΞΥΠΝΗ ΠΟΛΗ,» *Ευβοϊκός Τύπος,* 2021.
[39]	Unknown, «Η Χαλκίδα απέκτησε εφαρμογές Smart City,» *Πρώτο Θέμα,* 2017.
[40]	«Έρευνα του Δήμου Ηρακλείου για σύστημα Smart Parking (έξυπνης ελεγχόμενης στάθμευσης),» 17 July 2018. [Ηλεκτρονικό]. Available: https://smartcity.heraklion.gr/el/ereyna-toy-dimoy-irakleioy-gia-systima-smart-parking-exypnis-elegchomenis-stathmeysis/.
[41]	Unknown, “Το Ηράκλειο στις 100 «Εξυπνες Πόλεις» της Ευρώπης,” *Η Καθημερινή ,* 2020.
[42]	“Intelligent Cities - Smart Cities – Innovation Ecosystems,” Urenio , [Online]. Available: https://www.urenio.org/wp-content/uploads/2008/11/2006-ceadcebecf85cf80cebdceb5cf82-cf80cf8ccebbceb5ceb9cf82-ceb1cf81cf87ceb9cf84ceadcebacf84cebfcebdceb5cf82-1.pdf.

[43]	Unknown, “SECOND FIA SMART CITIES EFORUM SEASON 5 FOCUSES ON EUROPE,” 01 July 2021. [Online]. Available: https://www.fiasmartcities.com/news/second-fia-smart-cities-eforum-season-5-focuses-europe.
[44]	E. Commission, “Winners of the 2022 European Capitals of Smart Tourism Competition,” 16 November 2022. [Online]. Available: https://smart-tourism-capital.ec.europa.eu/cities_da.
[45]	M. Benoliel, “Is Paris the City of the Future?,” 23 January 2020. [Online]. Available: https://www.iotforall.com/paris-smart-city.
[46]	Unknown, “Paris Smart City 2050 by Vincent Callebaut Architectures,” 2020. [Online]. Available: https://amazingarchitecture.com/futuristic/paris-smart-city-2050-by-vincent-callebaut-architectures.
[47]	Unknown, “Working for a smart and sustainable València,” 2022. [Online]. Available: https://smartcity.valencia.es/en/.
[48]	Unknown, “Smart Venice RESEARCH, PROJECTS AND INNOVATIONS FOR SUSTAINABLE AND INCLUSIVE COMMUNITIES,” [Online]. Available: https://smartvenice.org/lagunalibre_an-urban-regeneration-project-in-venice/.
[49]	Unknown, “Smart Dublin brings together technology providers, academia and citizens to transform public services and enhance quality of life,” [Online]. Available: https://smartdublin.ie/about/.
[50]	Unknown, “Gothenburg, it’s a Smart City,” 2021. [Online]. Available: https://www.thisisgothenburg.com/smart-city.
[51]	L. v. d. Beuken, “Amsterdam Smart City,” [Online]. Available: https://amsterdamsmartcity.com/about.
[52]	A. S. Nielsen, “Smart City in Greater Copenhagen,” 2017. [Online]. Available: https://www.copcap.com/set-up-a-business/key-sectors/smart-city.
[53]	V. Virkamäki, “Smart City + Smart Countryside = Smart Region,” [Online]. Available: https://helsinkismart.fi/.
[54]	S. Angieri, “Smart cities: London,” 04 June 2021. [Online]. Available: https://www.eni.com/en-IT/low-carbon/smart-cities-london.html.
[55]	Uknown, “Hi-tech London, or the making of a smart city,” 05 01 2022. [Online]. Available: https://www.webuildvalue.com/en/megatrends/smart-city-london.html.
[56]	Uknown, “SMARTAMERICA EXPO,” [Online]. Available: https://smartamerica.org/.
[57]	N. Shemer, “Top 10 Smart Cities in America for 2022: Which Should You Move To?,” 25 January 2022. [Online]. Available: https://www.top10.com/moving-companies/top-10-smart-cities-in-america.
[58]	Uknown, “SMART CITY ASIA Ho Chi Minh City,” 2021. [Online]. Available: https://www.tradefairdates.com/SMART-CITY-ASIA-M13708/Ho-Chi-Minh-City.html.
[59]	G. Lim, “The Development of Smart Cities in Asia,” 14 July 2021. [Online]. Available: https://www.jumpstartmag.com/the-development-of-smart-cities-in-asia/.
[60]	J. Appleton, “THE TOP 10 SMART CITIES IN ASIA (UPDATED 2021),” 26 August 2021. [Online]. Available: https://hub.beesmart.city/en/strategy/top-10-smart-cities-in-asia.
[61]	J. O'Halloran, “Shanghai rated world’s number-one smart city for 2022,” 24 January 2022. [Online]. Available: https://www.computerweekly.com/news/252512366/Shanghai-rated-worlds-number-one-smart-city-for-2022.
[62]	Unknown, “Abu Dhabi and Dubai expand their smart city horizons this year,” world future energy summit , [Online]. Available: https://www.worldfutureenergysummit.com/en-gb/future-insights-blog/abu-dhabi-and-dubai-expand-their-smart-city-horizons-this-year.html.
[63]	C. Talavera, “World’s biggest ‘smart city’ to rise in Philippines,” The Philippine Star, 06 July 2017. [Online]. Available: https://www.philstar.com/business/real-estate/2017/07/06/1717043/worlds-biggest-smart-city-rise-philippines.

[64]	C. Lago, "Top 10 Smart Cities in ASEAN," 25 February 2020. [Online]. Available: https://www.idginsiderpro.com/article/3315258/top-10-smart-cities-in-asean.html.
[65]	Uknown, "THE LINE," 2021. [Online]. Available: https://www.neom.com/en-us/regions/whatistheline.
[66]	C. L. B. W. M. C. R. L. O.-c. N. P. D. J. S. Z. W. Z. S. B. A. S. B. V. F. B. D. L. D. A. V. D. G. P. D. A. Barnum, "Tokyo Smart City Design at Shinagawa," May 2020. [Online]. Available: https://smartech.gatech.edu/handle/1853/63476.
[67]	B. C. R. C. A. B. M. Pilkington, "The Smart Grid and Renewable Energy," 2019. [Online]. Available: https://innovationatwork.ieee.org/smart-grid-transforming-renewable-energy/.
[68]	Uknown, "Smart grids: electricity networks and the grid in evolution," [Online]. Available: https://www.i-scoop.eu/industry-4-0/smart-grids-electrical-grid/.
[69]	S. R. C. N. F. P. A. J. V. C. S. V. E. G. M. S. H. H. B. T. I. S. Mathias Uslar, "Applying the Smart Grid Architecture Model for Designing and Validating System-of-Systems in the Power and Energy Domain: A European Perspective," mdpi, 2019.
[70]	A. D. Pranadi, "Micrograds and Smart Grids in Definition," 21 July 2016. [Online]. Available: https://aseanenergy.org/microgrids-and-smart-grids-in-definition/.
[71]	N. C. V. S. K. O. L. M. Dharmesh Faquir, "Cybersecurity in smart grids, challenges and solutions," 12 January 2021. [Online]. Available: https://www.aimspress.com/article/doi/10.3934/electreng.2021002?viewType=HTML.
[72]	S. Langkemper, "The Most Important Security Problems with IoT Devices," [Online]. Available: https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices/.
[73]	M. Gloukhovtsev, "IOT SECURITY: CHALLENGES, SOLUTIONS & FUTURE PROSPECTS," Dell.inc, 2018.
[74]	A. R. M. a. R. L. Ekl, "Security Technology for Smart Grid Networks," 2010.
[75]	H. S. M. Y. S. F. Sun Zhongwei, "Security Mechanism For Smart Distribution Grid," Beijing, China, 2010.
[76]	N. I. o. S. a. Technology, "Guidelines for Smart Grid Cybersecurity," 2014.
[77]	K. E. S. R. T. Samuel Tweneboah-Koduah, "Cyber Security Threats to IoT Applications and Service Domains," Springer, 2017.
[78]	F. I. M. Kezunovic, "Automated Fault Analysis in a Smart Grid".
[79]	Z. Chang, "IoT Device Security Locking Out Risks and Threats to Smart Homes," Trend Micro Research.
[80]	Uknown, "Smart home security devices most at risk in IoT-targeted cyber attacks," 13 June 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/06/13/iot-targeted-cyber-attacks/.
[81]	G. Nanni, "ITU Workshop on Shaping Smart Sustainable Cities SCC," 05 December 2013. [Online]. Available: https://present5.com/itu-workshop-on-shaping-smart-sustainable-cities-scc/.
[82]	s. d. w. a. l. d. brandeis, "harvard law review: the right to privacy," 1890.
[83]	R. Clarke, "What's Privacy," 2006.
[84]	S. Z. C. A. S. G. F. Siddiqui, "Smart Grid Privacy: Issues and Solutions," 2012.
[85]	M. W. M. R. M. L. Abdulrahaman Okino Otuoze, "Smart grids security challenges: Classification by sources of threats," Elsevier B.V. on behalf of Electronics Research Institute (ERI), 07 February 2018. [Online]. Available: https://reader.elsevier.com/reader/sd/pii/S2314717218300163?token=329B53D8A1BA20D18DB76E2F3C530BAF196952EE22D4CA3763041874A9BB5484012B2FA5B741B50A30CFFB5416C57164&originRegion=eu-west-1&originCreation=20220502124443.

[86]	N. I. o. S. a. Technology, “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0,” 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pdf..
[87]	E. M. V. S. J. B. B. J. G.-R. R. T. M. J. A. M. a. A. F. S. Said Daoudagh, “Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal,” *sensors,* 28 October 2021.
[88]	F. Moorman, “A New Firewall – Multifamily Data Privacy and Security in the Age of Smart,” *CPO Magazine,* 09 April 2020.