APPROVED

INTERNET OF THINGS DEVELOPMENT POLICY OF VILNIUS CITY

BUILDING INTELLIGENT
Vilnius City Brain

Document version

Document date and version, list of amendments.

Document date	Version	Description of amendments
29 05 2020	V1.0	First release.
14 01 2021	V1.1	1. Added additional requirements into the chapter IT INFRASTRUCTURE Connectivity regarding alternative communications technologies application pages 10 and 11. 2. Added second paragraph into the chapter ARCHITECTURE OF INTERNET OF THINGS. 3. Chapter 7 point 3 the last sentence has been changed. 4. Added an amended Annex No. 1 “TABLE OF APPLICATION OF Internet of things TECHNOLOGY “. 5. Added Annex No. 2 “GUIDELINES FOR ENSURING COMMUNICATION SERVICES”.

CONTENT

1. GENERAL PROVISIONS

The Internet of Things (IoT) Development Policy of Vilnius City has been drafted taking into account the Strategic Plan of Vilnius for 2020 - 2030 and other normative legal documents governing the activities of the City of Vilnius and its subsidiaries. This policy complements the existing legal acts and helps to pursue the priorities of the City of Vilnius, creating and implementing strategic vision of the city, providing quality services to residents, attracting investments to the city, acting transparently, promptly and being open to residents, guests and investors.

The Internet of Things Development Policy of Vilnius City must be implemented in accordance with best practices and the Smart Cities Initiative of the European Commission – the European Innovation Partnership for Smart Cities and Communities (EIP-SCC), which brings together cities, industries, small businesses, banks, research and others. The EIP-SCC aims to improve urban life through more sustainable integrated solutions and to address specific challenges of cities in different policies in such areas as energy, mobility, transport and the development of information and communication technologies. The EIP-SCC is based on the involvement of society, industry and other stakeholders in the development of innovative solutions and participation in the management of the city.

The Internet of Things Development Policy of Vilnius City lays down the goals and tasks for this area, the main areas of implementation of the policy, defining the content and benefit of requirements of the policy, its stakeholders, their role and responsibilities as well as the course and sequence of monitoring of its implementation.

The City of Vilnius, its subordinate enterprises and institutions, natural and legal persons (including research and development companies, innovation developers, developers of advanced technologies and investors) planning to conduct or conducting their business in Vilnius and residents of the city are subject to the *Internet of Things Development Policy of Vilnius*.

Employees of the City of Vilnius and its group of companies have developed the *Internet of Things Development Policy of Vilnius City* taking into account areas of application of the Internet of Things and focusing on the development and integrity of a smart city and a smart society. The City of Vilnius, its subordinate companies and institutions are responsible for proper implementation of the policy and the cases when it applies to natural and legal persons operating in Vilnius.

2. CONCEPTS, DEFINITIONS AND ABBEVIATIONS

The following are the key concepts and abbreviations used in the *Internet of Things Development Policy of Vilnius City.*

Seq. No.	Concept	Definitions
1	**IOT**	Internet of Things
2	**Internet of Things Categories**	Defines 3 (three) categories: intelligent metering; intelligent video surveillance and intelligent operation. The areas of application of the Internet of Things fall within these categories
3	**Internet of Things Application Areas**	Defines 10 intelligent metering areas, 3 intelligent video surveillance areas and 5 intelligent operation areas
4	**Internet of Things Use Case Groups**	Groups of cases of use of Internet of Things, which specify the cases when this policy applies, belong to each areas of application of Internet of Things
5	**Stakeholder**	Any person or organization interested in the implementation of a policy or those, who are affected by policy-making and the relevant regulatory documents, is a stakeholder
6	**EIP-SCC**	Smart Cities Initiative supported by the European Commission - European Innovation Partnership for Smart Cities and Communities

Table No.1

3. KEY GOALS AND TASKS OF THE POLICY

The Internet of Things Development Policy of Vilnius City (hereinafter – the Policy) is aimed to "Build Intelligent Vilnius City Brain" – an advanced and sustainable ecosystem where everything is interrelated, also at creating conditions for a sustainable development of urban and industrial digitization, increasing the level of integration of technologies and urbanization. The implementation of the policy will help the city of Vilnius to focus on the development of a smooth city, the needs and expectations of residents and guests of the city, create conditions for being mobile, responding faster to changes in the environment, increasing the efficiency of services in both public and private sectors.

MAIN GOALS OF THE *INTERNET OF THINGS DEVELOPMENT POLICY OF VILNIUS CITY*

- To ensure full integration of information and urbanization.
- To expand possibilities and perception of management of the city and entities operating in it.
- To develop innovative business environment and open win-win new intelligent city, a new smart city.
- To create a safer and friendlier environment in Vilnius, to increase added value for residents of the city.
- To seek for a more efficient use of energy resources of the city and municipality-owned resources.
- To increase efficiency in the areas of operation of the City of Vilnius, its subordinate enterprises and institutions.
- To successfully implement cooperation between the public and the private sector for practical application of the policy.

MAIN TASKS OF THE *INTERNET OF THINGS DEVELOPMENT POLICY OF VILNIUS CITY*

- To set requirements for the development of the Internet of Things technology and advanced digital solutions in Vilnius.
- To ensure the validity of a uniform and clear regulation on the Internet of Things technology and the development of advanced digital solutions in Vilnius and compliance therewith by stakeholders, also defining their responsibilities.
- To respectively revise and supplement valid and newly drafted normative legal acts of the City of Vilnius, its subordinate enterprises and institutions with new provisions, conditions and requirements to ensure the implementation of the Policy.
- To ensure consistent development of advanced and digital solutions in Vilnius and a sustainable interoperability of technological components, which would best meet the needs of the society and the city.
- To draft methodological instructions and rules in separate areas of the implementation of the Policy.
- To create ecosystem of innovative services of Vilnius controlled by ar*tificial intelligence*, which would be able to independently (automatically) monitor, analyse and manage the condition of the city.

4. KEY ELEMENTS OF VALUE AND REQUIREMENTS OF THE IMPLEMENTATION OF THE POLICY

CONSTITUENT ELEMENTS OF VALUE AND COMPONENTS OF THE INTERNET OF THINGS

The constituent parts of the implementation of a sustainable Internet of Things, which must be assessed when implementing and developing the Internet of Things technology and advanced digital solutions are laid down in Figure 1. This means that the value of each constituent element when implementing and developing the technology of the Internet of Things and advanced digital solutions shall be properly assessed and prepared both functionally and organizationally, with the approval of stakeholders overseeing the respective constituent part or component.

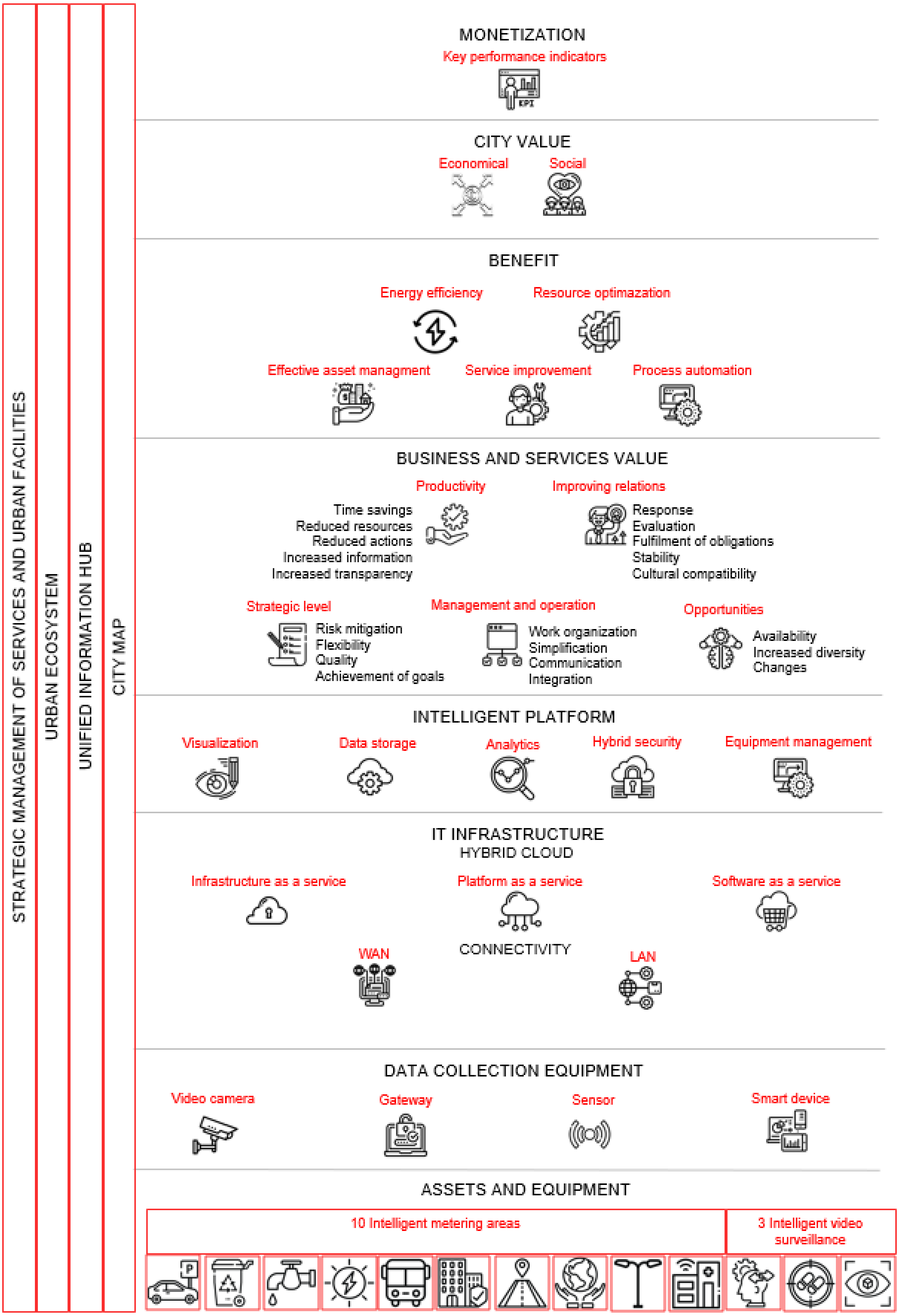


Figure 1. Components of Internet of Things

MONETIZATION

Key performance indicators

The development of the Internet of Things shall be based on change, so the implementation of each Internet of Things case in any of the areas of application of the Internet of Things shall be measured. The measurement indicator, which expresses the benefit pursued, shall be based on the key performance indicators of the City of Vilnius or its subordinate enterprises / institutions – KPIs, the improvement of which is pursued, or the expression of monetization, where a non-monetary, profitless or unprofitable activity is turned into a monetary, cost-reducing, profitable value-creating activity, which can be calculated financially. Often, KPIs are associated with monetization and can be measured financially.

CITY VALUE

Economical Social

Evaluation of the value added of a higher level being created for the city. The value created for the city (enterprise) shall be specified from the perspective of the evaluation of economic efficiency or social responsibility. Based on examples of good practice, both indicators are usually evaluated. The evaluation of one indicator may depend on the evaluation result of another indicator. The most commonly created social value has a direct or indirect economic impact on the city. Indirect economic value is calculated by estimating the assumptions that could be affected by the planned social change, if it is achieved.

BENEFIT

The benefit is defined using 5 (five) criteria used to evaluate it:

Energy efficiency

Implementation of a solution, which allows reducing the use of energy or sources necessary for energy generation.

Resource optimization

Implementation of a solution, which allows reducing human, technical and financial resources in presence of the same or growing needs of the organization, but achieving the goals set.

Process automation

Implementation of a solution, which allows automating complex business processes through the use of technological equipment, data or artificial intelligence, consistently moving from one task to another with a minimal human intervention or without it.

Effective asset management

Implementation of a solution, which allows to facilitate inventory of assets (monitor the movement of assets) and change preventive maintenance and repair of assets as needed, or planned maintenance by monitoring the condition of assets being operated (machinery, equipment, parts, materials), deviations from norms, extending their lifetime, avoiding accidents and breakdowns leading to adverse consequences on the organization.

Service improvement

Implementation of a solution, which allows improving the service-level agreement and providing the respective service faster and more efficiently. This definition also applies when the aim is to improve the quality of service provision or to reduce the likelihood of errors.
Note: One case of the Internet of Things technology may cover all 5 (five) benefit criteria.

BUSINESS AND SERVICES VALUE

The Internet of Things technology essentially offers more opportunities and measures to manage activities and to provide services more efficiently. The value created for activities and services shall be evaluated in this level of components of Internet of Things taking the following criteria into account:

Efficiency:

a. Time savings;
b. Reduced resources;
c. Reduced actions;
d. Increased information (knowledge);
e. Increased transparency.

Improving relations:

a. Response;
b. Evaluation;
c. Fulfilment of obligations;
d. Stability;
e. Cultural compatibility.

Strategic level:

a. Risk mitigation;
b. Flexibility;
c. Quality;
d. Achievement of goals.

Management and operation:

a. Work organization;
b. Simplification;
c. Communication;
d. Integration.

Opportunities:

a. Availability;
b. Increased diversity;
c. Changes.

INTELLIGENT PLATFORM

The Intelligent Platform is 1 of the 5 areas in the Intelligent Operation category. All data received from asset and equipment shall be processed in this operation centre through integrations with other software tools and systems. The main functions are to receive, manage and transfer data in accordance with the established requirements for case reporting, registration, dispatch and handling. Aside from the ability to structure data and understand what is what, the platform shall also be able to manage many large-scale data flows from different sources. In order to accurately assess the impact of the IoT technology case implementation on the operation centre and the need and scope of development of its functionality, general requirements for the following components shall be assessed:

Visualization

Requirements that determine the method and the format for displaying information to the user shall be set. 4 main criteria define these functionality requirements: **2D image** (control boards, information panels, charts, map and layers), **3D image** (displaying information in projected 3D space, zooming in, zooming out, rotating at 360 degrees, 3D map and its layers, and so on), **video and real-time video streaming** (video streaming from stationary, mobile and other video transmission and storage devices, digital photos, etc.), **reports and event lists** (text messages).

Data storage

Requirements for data collection, storage and management shall be assessed. There is a purpose for data processing (collection, use, storage, etc.), which is known and defined in advance and which shall be realistic and necessary. Data may be sent continuously or depending on changes in status, so data volume, speed, flow, and intensity shall be defined. Terminals shall ensure that the data are transmitted using standard protocols that the platform can read. Only as much data as is necessary to achieve the set objectives (BDAR) shall be collected and stored, therefore the equipment installed shall cover as many different groups of IoT use cases as possible. The listed general criteria shall be necessary for proper development of the operation centre functionality and selection of facilities.

Analytics

Analytics solutions are not directly implemented as a direct service of the intelligent operation centre, but the requirements for the use of analytics tools and data exchange between systems shall be evaluated to ensure the desired results. The functionality of analytics, which is used for in-depth learning, forecasting and decision making, shall be evaluated based on the business case (benefit) and defined by 3 criteria:

- Anomaly detection – deviations from norms.
- Deep learning – sets of rules.
- Regression analysis – factors and causes that affect the condition.

Hybrid security

The IoT technology and advanced solutions being implemented as well as data shall be protected and defended from violations, their illegal use or modification, exploitation, and the making of wrong decisions. This requirement shall apply not only to cyber security, but shall also take into account such factors as sabotage seeking to intentionally damage equipment, falsification of data at edge equipment (smart metering, video surveillance equipment) and cases of unreliable and insecure providers. Also it should ensure public safety and protect against wrong decisions made by human factor, algorithms and artificial intelligence.

Equipment management

Asset and equipment may be monitored and / or managed. Requirements which monitoring is subject to are defined in two scenarios:

- real-time data shall be received constantly or at certain set time intervals;
- real-time data shall be received on demand, i.e. upon a change of the condition of assset or equipment or when receiving all the data accumulated in terminal equipment at a particular time.

Asset and equipment management is understood as the automatic sending of a command to edge device or a group of such devices dedicated for changing the status of those devices, and shall be realized without human intervention. Decisions on team execution shall be made in systems that are integrated into the IoT platform, but in some cases, human factor can be necessary to validate the command being executed for the safety requirements.

IT INFRASTRUCTURE

Hybrid cloud. The implementation of the IoT technology and advanced solutions subjects data management and processing to certain requirements. Data volumes, velocity, sensitivity, confidentiality, security requirements, support and maintenance costs are the key parameters that define the requirements for data upload and storage.

Infrastructure as a Service

Leased or On Premises Infrastructure as a Service (IaaS) are a cloud service model, which requires hardware resources, which are subject to the following requirements, only:

- Infrastructure shall be flexible and easy to develop, taking into account the growth of data volumes and the need for resources.
- The solutions used shall ensure high availability and performance.
- High level of authentication shall be ensured.
- Connection encryption using the latest and most secure protocols shall be ensured.
- Cyber security shall be ensured.

Platform as a Service

A public cloud service level or Platform as a Service (PaaS) is a model of cloud services where the user is provided with a complete computing platform that covers the necessary operating system, programming languages, and etc. Public cloud services shall be subject to the following requirements:

- Infrastructure shall be flexible and easy to develop taking into account the growth of data volumes and the need for resources.
- The solutions used shall ensure high availability and performance.
- High level of authentication shall be ensured.
- Connection encryption using the latest and most secure protocols shall be ensured.
- Cyber security shall be ensured.

Software as a Service

A public cloud service level or Software as a Service (SaaS) is a model where a cloud service provider assumes responsibility for a hardware and software environment, such as an operating system and an application software. This model is adapted for a limited commerce cloud that is subject to the following requirements:

- Infrastructure shall be flexible and easy to develop, taking into account the growth of data volumes and the need for resources.
- The solutions used shall ensure high availability and performance.
- High level of authentication shall be ensured.
- Connection encryption using the latest and most secure protocols shall be ensured.
- Cyber security shall be ensured.

Connectivity. Solely the connection standards specified in this policy shall be used to implement IoT technologies and advanced solutions. Requirements which the technologies and standards that are used to organize global and local connection in the areas of Intelligent Metering (IM) and Intelligent Video Surveillance (IVS) of the Internet of Things are listed below. If the field is marked with an "X", it means that the technologies listed in the line are appropriate for the scope of the Internet of Things indicated in the column. The communication technology and standards in Table No. 2 and Table No. 3 have been listed in the order of priority from top to bottom, therefore a lower priority technology for data transmission or other data transmission technology not listed in Table No. 2 and Table No. 3 shall only be chosen in cases when the advantages outweigh any disadvantages of a higher priority data transmission technology.

Figure 2 presents the essential scheme of application of the connection technology to be followed.

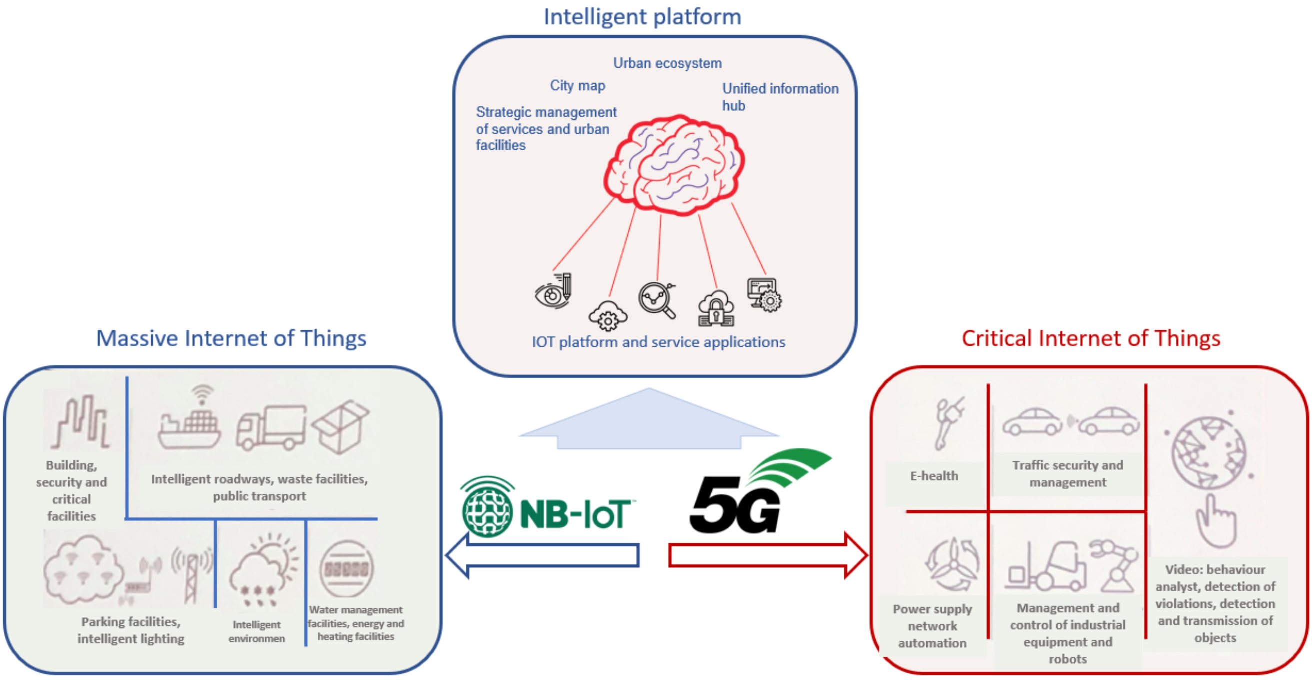

Intelligent platform
Urban ecosystem
City map
Unified information hub
Strategic management of services and urban facilities
IOT platform and service applications
Massive Internet of Things
Building, security and critical facilities
Intelligent roadways, waste facilities, public transport
Parking facilities, intelligent lighting
Intelligent environmen
Water management facilities, energy and heating facilities
NB-IoT
5G
Critical Internet of Things
E-health
Traffic security and management
Power supply network automation
Management and control of industrial equipment and robots
Video: behaviour analyst, detection of violations, detection and transmission of objects

Figure 2. Principle of application of communication technology

WAN

Wide Area Network (WAN) shall be arranged using the data transmission technologies and standards specified in Table 2 below or using alternative technologies in all cases when new or upgraded smart devices, sensors, video cameras are installed, except when the technologies specified in the said table or alternative technologies have not been developed in the city. Each communication technology listed or not listed in the table bellow shall meet guidelines for ensuring communication services requirements stated in Policy Annex No. 2. Advanced level - global communication data transmission shall be used to transmit data directly to the platform from smart devices, video cameras or metering devices of an advanced generation.

Priority	**Technology and standards**	**IM**	**IVS**
First	LTE/5G (3GPP)	X	X
	LTE/NB-IoT (3GPP)	X	-

Table No. 2

LAN

Local Area Network *(LAN)* may be organized in application of the data transmission technologies and standards specified in Table No. 3 below and used only when the technologies listed in Table No. 2 are not developed in the city, or to ensure the Master-Slave solution, i.e. for connecting sensors into a net, but with the master device communicating with the platform directly via the technologies listed in Table No. 2. In exceptional cases, in presence of specific requirements which the equipment is subject to due to safety requirements or environmental disturbances, optical or copper cables may be used to connect sensors to the hub.

Priority	**Technology and standards**	**IM**	**IVS**
First	LoRa	X	-
Second	IEEE 802	X	X
Third	Bluetooth Low Energy (BLE)	X	-
Fourth	Optical cable	X	X
Fifth	Copper cable	X	X

Table No. 3

DATA COLLECTION EQUIPMENT

Special equipment shall be used for asset conditions monitoring and management. Asset and equipment may have integrated or additionally mounted (for monitoring certain parameters) sensors, concentrators, smart devices or video cameras.

Sensor

Asset and equipment shall be monitored using sensors and detectors, which have parameters and characteristics specific of a certain area of application of Internet of Things. Newer generation sensors have an integrated Global Connectivity module and connect directly to the IoT platform.

Gateway

Concentrators, which may function as a sensor aggregation hub or be used to process the data collected from sensors in order to reduce the amount of data sent with lower-level rules and analytical solutions, may be used to aggregate the network of sensors or detectors.

Smart device

High-end sensors and mobile devices with integrated software rules, analytical solutions and Global Connectivity modules, which send data that may be both a primary (GPS tracking equipment, metering devices) and a secondary (smart phones, smart watches, etc.) function.

Video camera

Requirements for the installation and functionality of video cameras may vary. The specific requirements for the need for a camera to have an integrated analytical software solution - artificial intelligence - and other parameters are defined for each case of use of Internet of Things differently according to the need, which is determined by the stakeholder controlling the implementation of the Internet of Things Policy. According to their nature and the functionality provided by analytics, cameras shall be suitable for the purpose of the intelligent video surveillance of Internet of Things and the cases of its use. The camera manufacturer shall comply with the recommendations of interdepartmental institutions of the Republic of Lithuania.

ASSET AND EQUIPMENT. 3 CATEGORIES OF INTERNET OF THINGS

This policy defines 3 (three) IoT categories which includes the IoT application areas: *10 Intelligent Metering Areas, 3 Smart Video Surveillance Areas, 5 Intelligent Command Areas*, each of them defines use cases or groups of use cases.

Intelligent Metering

Intelligent Video Surveillance

Intelligent Command

Each of the three mentioned categories covers areas of application of Internet of Things falling within it, which meet the basic needs of the society and the city and are an essential indicator for stakeholders, entities of all types of economy and business, which must comply with the *Internet of Things Development Policy of Vilnius City.*

5 Intelligent Command Areas

Intelligent platform. Case reporting, registration, dispatch, handling.

City map. Status tracking: City operating status displayed on a single map.

Unified information hub. Analytics and decision-making: one-click decision-making support and management.

Urban ecosystem. Innovative services: one-step self-evolution and innovation platform.

Strategic management of services and urban infrastructure. Management: integrated city operations and linage. Intelligent command platform.

10 Intelligent Metering Areas

Intelligent Environment

Water Facilities

Parking Facilities

Energy & Heating Facilities

Building, Security & Critical Facilities

Intelligent Lightning

Intelligent Roadway

Waste Facilities

eHealth

Public Transport Ecosystem

3 Intelligent Video Surveillance Areas

Behaviour Analysis

Violation Detection

Object Detection

Quality data becomes a key prerequisite for increasing the efficiency of any activity and ensuring the validity of decisions. All decisions made in the city shall be based on data that allows identifying priority areas, monitoring return rendered by cases, incidents, actions taken and decisions made, simulating future scenarios and accurately distributing the limited available resources.

Considering of the above, Internet of Things shall be developed and expanded following a systemic approach and uniform standards. In order to provide wider, easily expandable opportunities for adapting technologies and to avoid the occurrence of patented or limited solutions, two key principles shall be followed:

- application of widely used standards;
- definition of the architecture of Internet of Things.

APPLICATION OF STANDARDS

The latest generation widespread, globally and European Union-recognized standards set and validated by relevant organizations shall be used for the implementation and development of the IoT technology and advanced digital solutions. Closed systems or case-by-case technologies based on specific standards with limited market availability or scope, and standardized technologies the design life cycle of which ends and will not be future developed shall be unacceptable. Standards that specifically apply to technological components, categories, areas or individual use cases of Internet of Things and advanced digital solutions shall be specified in separate methodological requirements and rules of the *Internet of Things Development Policy of Vilnius City*.

ARCHITECTURE OF INTERNET OF THINGS

The basis of the architecture is easy communication and interoperability between assets (things, equipment, objects), facilities, intelligent Internet of Things operation centre and other software platforms. Sensors, intelligent devices and systems shall be connected to the network and to each other in order to utilize the most of Internet of Things opportunities, therefore the Policy specifies the requirements for the architecture of Internet of Things.

The goals of the equipment to be installed generally include the optimization and automation of processes, and the reduction of human participation in the processes. Development of the solutions must provide interfaces (for both people and equipment):

- Integration of equipment lifecycle event management functions with third party proprietary systems, e.g. with equipment installers, with technical support: such events (e.g. decommissioning or commissioning of a device when its parameters, including connection quality, meet the requirements of the solution) must be automatically recorded in asset management or business management systems).
- Integration of equipment electronic identity life cycle processes with equipment manufacturers and asset management or business management systems (e.g. commissioning of new equipment (commissioning) and disconnection of old equipment (decommissioning or transfer for warranty repair) must be performed via an automatic interface with all systems, including third parties who performing installation, support or dismantle equipment.

Selecting or switching equipment provider, e.g. once the list of devices whose connection parameters of poor quality in the network of a particular communication provider has been detected, it must change to another communication provider network automatically, via an automatic interface without human intervention or additional manual switching / configuration actions.

The architecture of the Internet of Things technology is based on a unified software platform designed to fully ensure easy interaction of devices, hardware and external systems in the Internet of Things ecosystem. The architecture covers a set of core services, specifies the structure of equipment interfaces, and the key development principles for implementing IoT ecosystem management.

Figure 3 presents the conceptual scheme of the target IoT architecture.

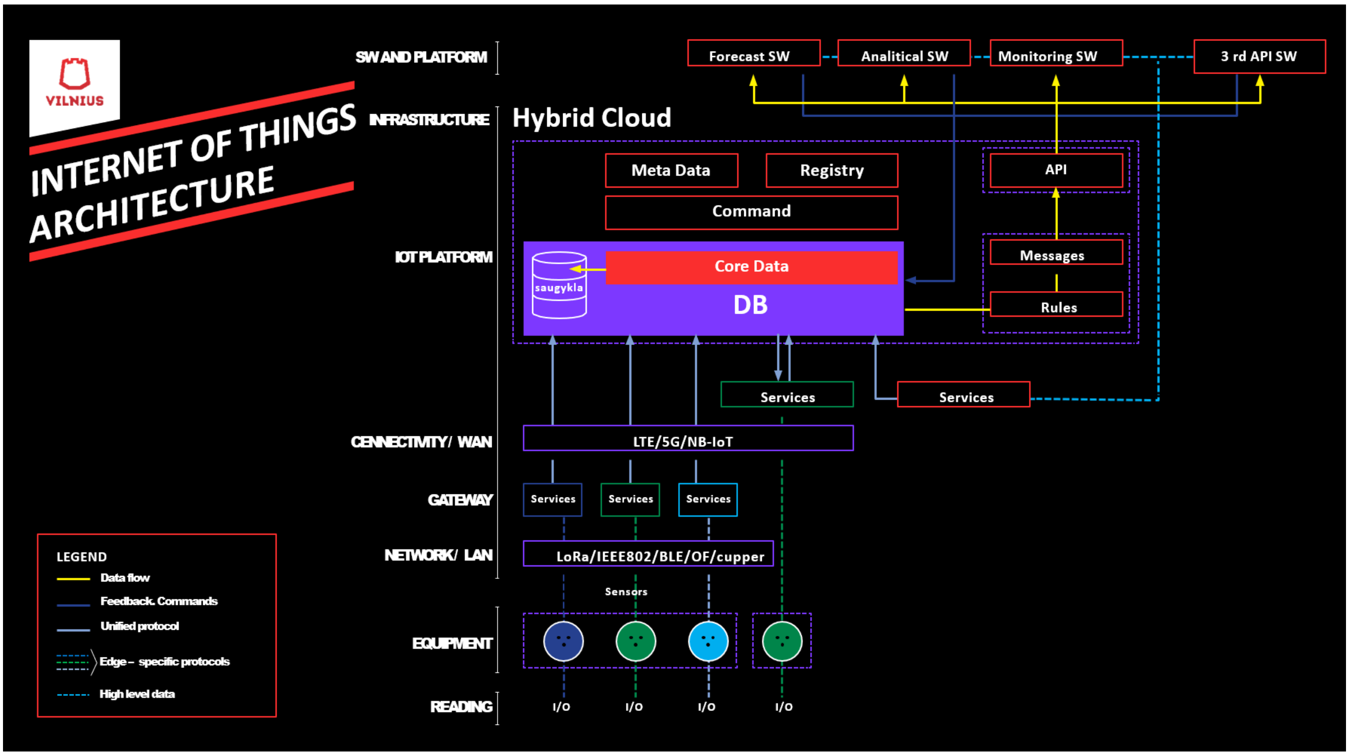


Figure 3. Architecture of Internet of Things

SW AND PLATFORMS
The highest level of the Internet of Things architecture, which specifies connections and data exchange interfaces between business management software tools or platforms and the Internet of Things platform.

INFRASTRUCTURE
Infrastructure cover a hybrid cloud that processes and collects data, runs the Internet of Things operation centre and computing with all the necessary plug-ins.

IOT PLATFORM
The IOT platform shall allow integrating real - time event data in other analytical, image processing and recognition systems. It shall also process, analyse and respond in real-time event data according to planned scenarios by sending notifications and instructions to responsible parties. The platform shall be able to work with a large number of real-time data sources, which shall also apply to receiving and sending information.
The platform shall also have the functionality to share data via the WebSocket protocol; spatial filtering by geometric and attribute properties of events, a possibility to use Geo-fencing functionality for monitoring important places; connecting additional data sources to event data; archiving event data.
The platform shall support the main exchange protocols: WebSocket; REST; HTTPS polling; RSS.
There shall be a possibility to share the following data formats via the core protocols: JSON, GeoJSON, XML, CSV and other text formats.

CONNECTIVITY
Two-level standardized data transmission technologies that help organize local and global connection between equipment and the Internet of Things platform. Local connection can be used to transmit data in a protocol encrypted by the manufacturer to a concentrator or a sensor for interconnection. Global connection is used to transfer data using standard data protocols read by the Internet of Things operation centre. The data transmission technologies and standards specified in this Policy shall be followed at each connection level. Data transmission shall be subject to security requirements and thus data shall be encrypted in advanced encryption standards.

CONCENTRATOR
A concentrator in the Internet of Things technology is a software or a physical device with software services, which acts as an intermediate data processing equipment between the Internet of Things operation centre and sensors. These devices convert the unreadable sensor data protocol (format) on the IoT operation centre into an operation centre-readable protocol used to efficiently utilize the existing equipment resources by moving away from unnecessary data transmission, processing and storage. Depending on a specific case, it shall be able to collect and transmit raw data, transmit it in a certain order or conditions, receive commands from the Internet of Things platform, and manage sensors and edge equipment.

EQUIPMENT
Sensors, smart devices, video cameras, metering and all associated equipment for collecting data from assets and equipment shall be assigned to this level of the Internet of Things architecture. These devices shall be strong and resistant to mechanical impact, and shall meet environmental and climate requirements. The equipment shall send data in real time in accordance with the specified conditions and / or at time intervals, and / or continuously, according to requirements of each specific case.

READING
The lowest level of the architectural hierarchy, which defines the parameters of information and data needed to receive information about the characteristics of assets and equipment or other conditions falling into the 3 Internet of Things categories.

5. APPLICATION OF THE POLICY

Natural and legal entities (hereinafter – the Entities) operating in the public and private sector in the territory of the City of Vilnius, including the City of Vilnius and its subordinate companies and institutions, shall be subject to this Policy.

The City of Vilnius and its subordinate enterprises and institutions are responsible for the drafting of this policy, methodology and rules, controlling and ensuring their proper and correct implementation in all 3 (three) categories of IoT technology defining the areas of intelligent command, intelligent metering and intelligent video surveillance.

The Internet of Things Development Policy shall be included in all normative legal and technical documents at the disposal of the City of Vilnius and its subordinate enterprises and institutions, which are related to the acquisition of goods – services or works.

Before design (pre-design) solutions, documents approval or before issuing construction, development, modernization, connection and service provision or other permits or conditions, Vilnius City municipality divisions and municipality-owned enterprises and institutions, which are subject to the definition of a responsible stakeholder, shall indicate which Internet of Things use case groups shall be implemented in accordance with this Policy. Section 7 hereof lists stakeholders, their roles and responsibilities.

Each Entity whose activities in the service, urban development, infrastructure development or maintenance sector, and the related property acquired or created fall into at least one group of cases of use of IoT category areas or if the said activities may have an impact (interfaces) on at least one IoT use case group specified in Annex No. 1 to the Policy, shall implement requirements of this Policy.

6. BENEFIT FOR THE CITY AND EVALUATION

INCREASING SECURITY OF THE CITY

Security of the city is the key for both residents and guests of the city. Innovations in video surveillance technologies such as facial and behavioural recognition, detection of flames, smoke or fire, violations, objects and other incidents, increasing advantage in ensuring security in the city. The development of IoT technology and advanced solutions in the city will facilitate inter-institutional cooperation and a rapid response. The development of these initiatives will also have a preventive effect and prevent malicious planned criminal actions.

ECONOMIC GROWTH

The development of the IoT technology and advanced solutions in the city is a great opportunity not only to save the city budget, but also to generate higher revenues. The introduction of innovations in the city attracts and encourages the creation of business and reduces unemployment. Meanwhile, appreciating a safer environment, a significant reduction of operating costs and better profit margins, businesses and enterprises also seek to take advantage of the growth opportunities offered by the Internet of Things technology and the development of advanced solutions in the city.

IMPROVING THE QUALITY OF SERVICES

The implementation of the Policy will allow obtaining and analysing more high-quality data and creating conditions not only to monitor the condition of the city and the services provided, but also to manage them in real time. Information of the past does not allow to flexibly adapt to constant change and to quickly make the right decisions, as the changing environment, needs and hobbies of the community change depending on many conditions. Therefore, the environment and conditions need to be monitored, and the pursuit to manage the city effectively means to have a better understanding of the pulse of life of the city, to plan and to monitor the implementation of changes, and their delivery of the expected results. The growth and dynamic change of the city requires the provision of services to be purposefully aligned with urban policy, development and daily life. Consistent implementation of the Policy will allow to quickly respond to the needs of residents and guests of the city, to monitor the level of quality of the services provided, to create new and improve the existing services, while they do not yet experience problems due to a shortage of services, which means focusing on a service that creates value rather than a function. The data provide an opportunity to speed up the improvement of services, to respond to each situation accurately and in a calculated manner.

EFFICIENCY OF USE OF RESOURCES

Digital transformation and the Internet of Things technology allow organizations managing large assets to significantly automate processes using data on the condition of the environment, assets and equipment. An advanced asset management strategy allows moving forward in today's competitive marketplace by maximizing asset availability, reliability and performance and minimizing operating costs of each asset. The Internet of

Things technology provides more opportunities in maintenance strategies and decision-making, avoiding higher costs for asset repairs or financial losses, if an upcoming event and its causes are known in advance. Machine to Machine (M2M) facilitate the exchange of information between machines and can perform operations without human intervention. Automation makes processes more efficient by reducing the number of errors and improving asset efficiency. The development of intelligent solutions and real-time data allow for a more efficient use of energy, human and financial resources in all senses, provide much greater information management capabilities and automate decision-making or enable them to be made much faster.

COMMUNITY WELL-BEING

Creating a city friendlier environment includes modernizing urban facilities, improving environmental conditions, quality of service provision, planning and change monitoring that imply a state of physical, mental and social well-being of residents. The emotional side of residents creates value for economic growth of the city, so the development of digital innovations and the present, modern philosophy focused on bold decisions and experimentation shall encourage residents to participate more actively in city life and create better conditions for their well-being. The implementation of the policy is based on the benefits of smart solutions and harmonious communication to residents. The development of the Internet of Things technology will increase the opportunities of residents to understand the general condition of the city, allow for more objective choices, shorten the path to the service, and plan activities.

EVALUATION PARAMETERS

The implementation of the Policy contributes to the creation of economic and social value as well as a friendlier environment of the city. The development of the Internet of Things technology and smart solutions covers and applies to projects, services and initiatives that fall within horizontal and vertical areas of a smooth city:

1. Services.
2. Planning.
3. Management excellence.
4. Environment and city development.
5. Social security.
6. Mobility.
7. Culture.
8. Security and protection.
9. Health and wellness.
10. Education.

The evaluation shall be based on key urban indicators and their monitoring in light of quality, maintenance, mobility, data, processes, energy consumption, material consumption and cost-effectiveness.

7. STAKEHOLDERS, THEIR ROLE AND RESPONSIBILITIES

The City of Vilnius and its subordinate enterprise and institutions implement and control the Internet of Things Development Policy of Vilnius City. Every developer of facilities or services - in the areas of communication, transport, buildings, construction, roads and streets, environment, water management, energy, waste, security, engineering networks, lighting, health, public services, entertainment, catering, supply chain and other areas operating in the territory of the City of Vilnius, shall ensure the implementation of this Policy.

There are 4 (four) types of stakeholders who are participants in the Internet of Things technology development process, including natural and legal persons, drafters of technical conditions, designers, suppliers, contractors, private and public sector entities:

1. Responsible (R), who must implement policy requirements; both internal and external stakeholders.
2. Accountable (A), who are responsible for developing methodological guidelines, requirements and rules and for ensuring that policy requirements are implemented correctly, achieving the planned results. Divisions of the City of Vilnius and municipality-owned enterprises and institutions are the key controlling entities.
3. Consulting (C), who are responsible for including the Policy in all relevant legal documents governing design, performance of activities, issuing of conditions and permits, provision of services, planning,

management and administration in the areas of environment and urban development, social security, mobility, culture, security and protection, health and wellness, and education; they are also entitled to offer supplements and changes to the Policy.

4. Informing (I), who can make and have an impact, pose risk or restrictions to the implementation of the Policy, initiating supplements to and adjustments of the Policy.

The owner or owners of the Internet of Things use case are responsible for identifying all stakeholders in the early stage of the *Process Participants* illustrated in Figure 3 *Integrated Policy Implementation Process.* Owners of the Internet of Things use case may themselves be attributed to one or more groups of stakeholders. Owners of IoT use cases are listed in Annex No. 1 to the Policy.

POLICY IMPLEMENTATION

The Policy shall be implemented following the integrated process (the Process), which helps stakeholders to evaluate technical, qualitative and usefulness aspects of each IoT use case, to define the applicable requirements for IoT technology constituent parts and components, and to monitor the results. Figure 4 illustrates the integrated Policy Implementation Process.

The process defines the **management of sustainable development of the Internet of Things technology**, including the **management of requirements and stakeholders**.

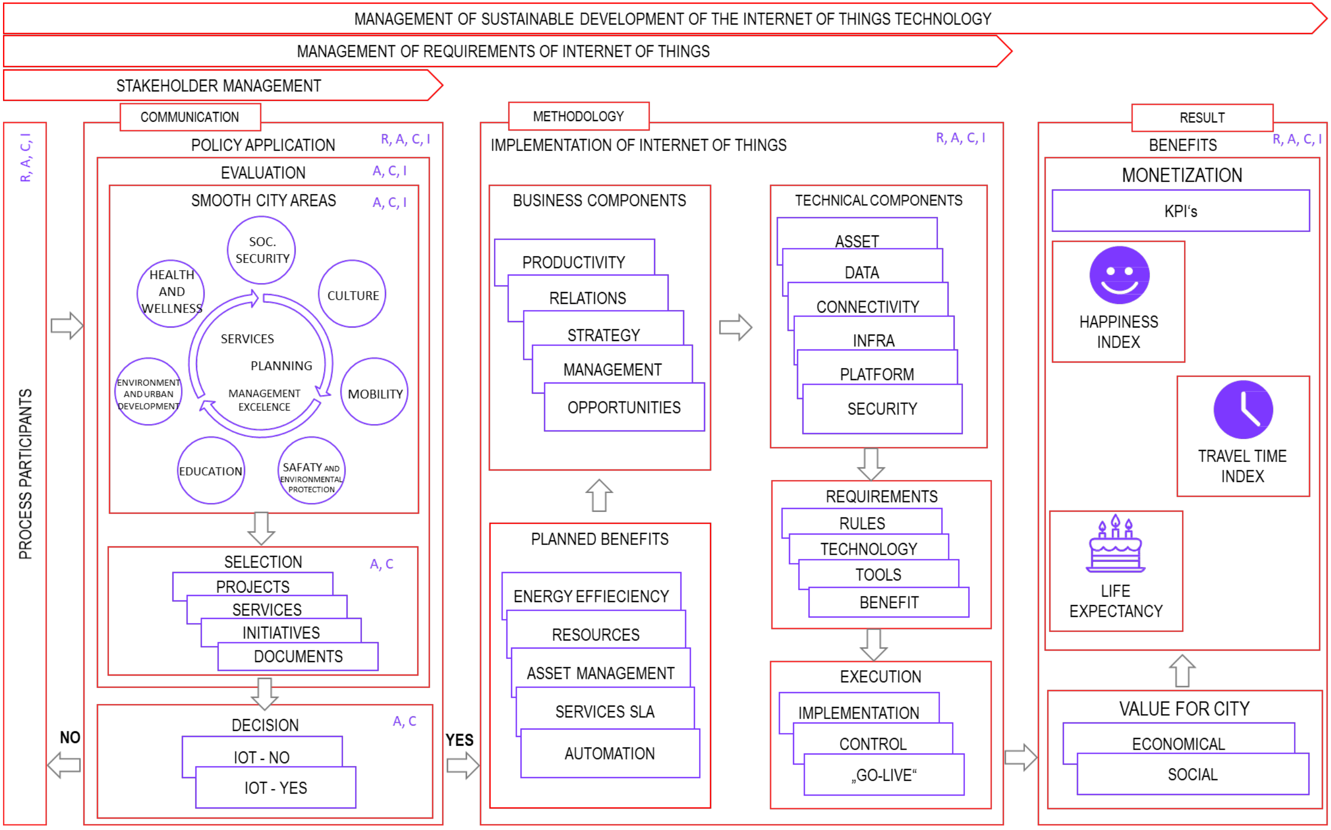


Figure 4. Integrated policy implementation process

Process participants. All the stakeholders defined in Section 7 (A, K, C, I) are involved in the Process according to their type and ensure the performance of tasks delegated to them.

Application and evaluation of the Policy. An evaluation shall be conducted and a decision shall be made on which areas of a smooth city the implementation of the Policy affects, identifying all stakeholders, which fall within the respective areas and their roles. The areas of a smooth city are connected in several ways with the groups of IoT use cases specified in Annex No. 1 to the Policy. Once these links, preliminary benefits and the planned valueto be created have been determined, a selection procedure shall be held when Controlling and Consulting stakeholders shall determine the application of the Policy to a project, to a service, to an initiative or to a documents.

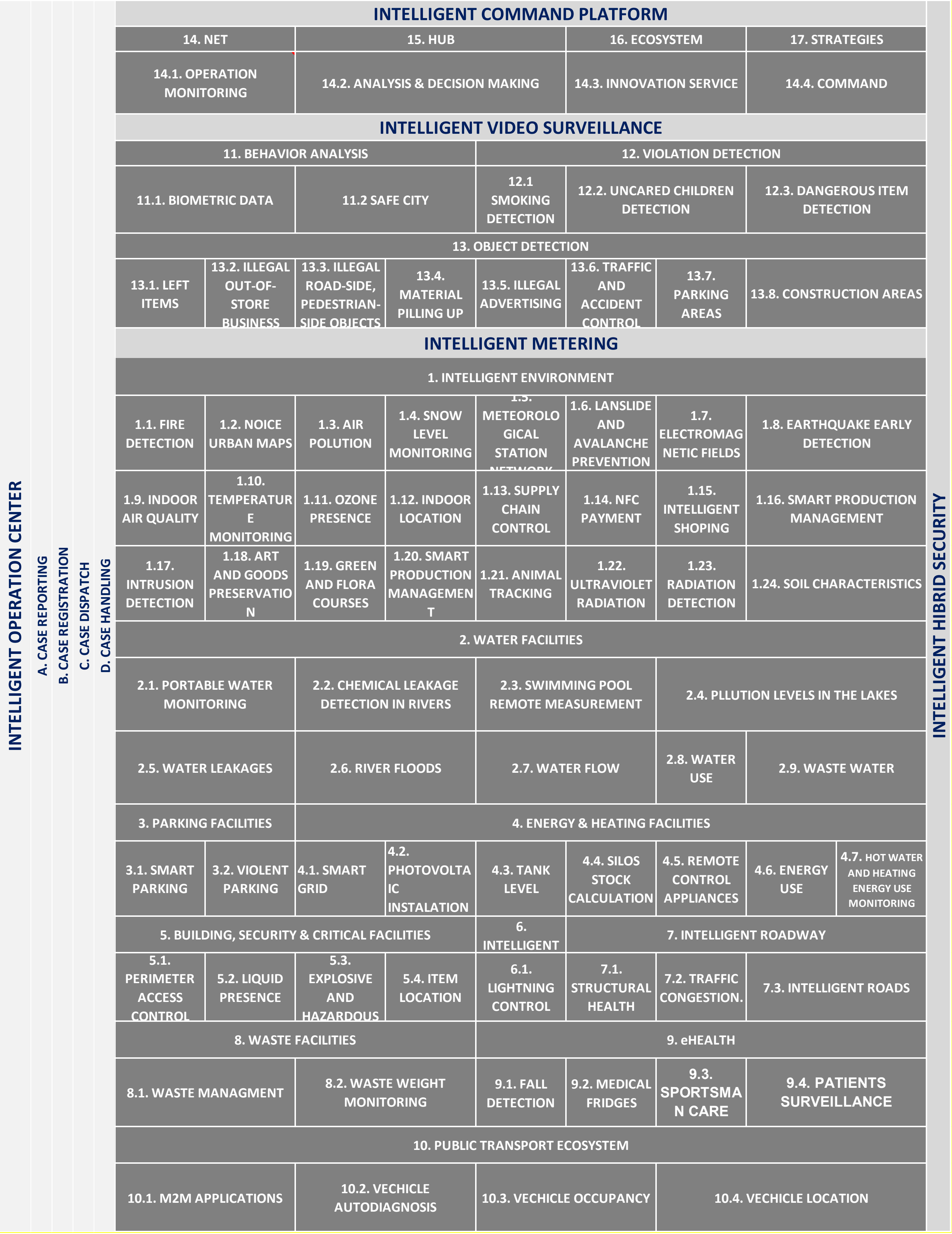
Implementation of the Internet of Things technology. The Internet of Things technology shall be implemented in accordance with this Policy and methodological guidelines, which may be different for each group of IoT use cases specified in the Annex No. 1 to the Policy. The methodological guidelines for the IoT use case group shall cover all levels of constituent parts and components of the IoT technology. Therefore, the value added for activities and services, the benefit, the value created for the city and the monetization indicators shall be assessed before starting the implementation, also setting requirements for technical components: the intelligent platform, the IT infrastructure, the data collection equipment and the data parameters necessary to obtain the characteristics of assets and equipment or other conditions.

Benefit. The benefit is the planned outcome of the entire process, which is pursued and which measures how the development of the Internet of Things technology affects the city, a municipal structural division or an enterprise, a services, or other significant indicators. The target change of the indicators to be improved shall be evaluated before the start of the implementation, then monitoring its achievement and drawing conclusions on the improvement of the implemented solutions in the future developing additional or similar solutions.

8. MONITORING POLICY IMPLEMENTATION

The implementation of the Policy shall be monitored on the Heat Map. This map is used to monitor the maturity of application of Internet of Things falling within separate categories of Internet of Things and their use case groups.

The structural scheme of the Heat Map is presented in Figure 5.



INTELLIGENT OPERATION CENTER

A. CASE REPORTING

B. CASE REGISTRATION

C. CASE DISPATCH

D. CASE HANDLING

INTELLIGENT COMMAND PLATFORM

- 14. NET
- 15. HUB
- 16. ECOSYSTEM
- 17. STRATEGIES
- 14.1. OPERATION MONITORING
- 14.2. ANALYSIS & DECISION MAKING
- 14.3. INNOVATION SERVICE
- 14.4. COMMAND

INTELLIGENT VIDEO SURVEILLANCE

- 11. BEHAVIOR ANALYSIS
- 12. VIOLATION DETECTION
- 11.1. BIOMETRIC DATA
- 11.2 SAFE CITY
- 12.1 SMOKING DETECTION
- 12.2. UNCARED CHILDREN DETECTION
- 12.3. DANGEROUS ITEM DETECTION
- 13. OBJECT DETECTION
- 13.1. LEFT ITEMS
- 13.2. ILLEGAL OUT-OF-STORE BUSINESS
- 13.3. ILLEGAL ROAD-SIDE, PEDESTRIAN-SIDE OBJECTS
- 13.4. MATERIAL PILLING UP
- 13.5. ILLEGAL ADVERTISING
- 13.6. TRAFFIC AND ACCIDENT CONTROL
- 13.7. PARKING AREAS
- 13.8. CONSTRUCTION AREAS

INTELLIGENT METERING

- 1. INTELLIGENT ENVIRONMENT
- 1.1. FIRE DETECTION
- 1.2. NOICE URBAN MAPS
- 1.3. AIR POLUTION
- 1.4. SNOW LEVEL MONITORING
- 1.5. METEOROLOGICAL STATION NETWORK
- 1.6. LANSLIDE AND AVALANCHE PREVENTION
- 1.7. ELECTROMAGNETIC FIELDS
- 1.8. EARTHQUAKE EARLY DETECTION
- 1.9. INDOOR AIR QUALITY
- 1.10. TEMPERATURE MONITORING
- 1.11. OZONE PRESENCE
- 1.12. INDOOR LOCATION
- 1.13. SUPPLY CHAIN CONTROL
- 1.14. NFC PAYMENT
- 1.15. INTELLIGENT SHOPING
- 1.16. SMART PRODUCTION MANAGEMENT
- 1.17. INTRUSION DETECTION
- 1.18. ART AND GOODS PRESERVATION
- 1.19. GREEN AND FLORA COURSES
- 1.20. SMART PRODUCTION MANAGEMENT
- 1.21. ANIMAL TRACKING
- 1.22. ULTRAVIOLET RADIATION
- 1.23. RADIATION DETECTION
- 1.24. SOIL CHARACTERISTICS
- 2. WATER FACILITIES
- 2.1. PORTABLE WATER MONITORING
- 2.2. CHEMICAL LEAKAGE DETECTION IN RIVERS
- 2.3. SWIMMING POOL REMOTE MEASUREMENT
- 2.4. PLLUTION LEVELS IN THE LAKES
- 2.5. WATER LEAKAGES
- 2.6. RIVER FLOODS
- 2.7. WATER FLOW
- 2.8. WATER USE
- 2.9. WASTE WATER
- 3. PARKING FACILITIES
- 4. ENERGY & HEATING FACILITIES
- 3.1. SMART PARKING
- 3.2. VIOLENT PARKING
- 4.1. SMART GRID
- 4.2. PHOTOVOLTAIC INSTALATION
- 4.3. TANK LEVEL
- 4.4. SILOS STOCK CALCULATION
- 4.5. REMOTE CONTROL APPLIANCES
- 4.6. ENERGY USE
- 4.7. HOT WATER AND HEATING ENERGY USE MONITORING
- 5. BUILDING, SECURITY & CRITICAL FACILITIES
- 6. INTELLIGENT
- 7. INTELLIGENT ROADWAY
- 5.1. PERIMETER ACCESS CONTROL
- 5.2. LIQUID PRESENCE
- 5.3. EXPLOSIVE AND HAZARDOUS
- 5.4. ITEM LOCATION
- 6.1. LIGHTNING CONTROL
- 7.1. STRUCTURAL HEALTH
- 7.2. TRAFFIC CONGESTION.
- 7.3. INTELLIGENT ROADS
- 8. WASTE FACILITIES
- 9. eHEALTH
- 8.1. WASTE MANAGMENT
- 8.2. WASTE WEIGHT MONITORING
- 9.1. FALL DETECTION
- 9.2. MEDICAL FRIDGES
- 9.3. SPORTSMAN CARE
- 9.4. PATIENTS SURVEILLANCE
- 10. PUBLIC TRANSPORT ECOSYSTEM
- 10.1. M2M APPLICATIONS
- 10.2. VECHICLE AUTODIAGNOSIS
- 10.3. VECHICLE OCCUPANCY
- 10.4. VECHICLE LOCATION

INTELLIGENT HIBRID SECURITY

Figure 5. Structural scheme of the Heat Map.

3 (three) colours define the maturity of case groups: red, orange and green.

🟥 Red colour indicates that the maturity of the Internet of Things is attributed to the Human to Machine (H2M) communication model, which means that less than 30% of assets and equipment in the use case group marked in this colour can independently send data on their status to data processing platforms, or the process of data collection or processing inevitably needs a person or devices controlled by a person, the data of which shall be entered manually.

🟧 Orange colour indicates that the maturity of the Internet of Things is attributed to the Machine to Machine (M2M) communication model, which means that 30% to 85% of property and things in the use case group marked in this colour can independently send data on their status to data processing platforms and that data are processed automatically or semi-automatically. This model is best illustrated by the example of the SCADA system.

🟩 Green indicates that the maturity of the Internet of Things is attributed to the Internet of Things (IoT) communication model, which means that 85% of property and things in the use case group marked in this colour can independently send data on their status to data processing platforms, and data are processed automatically and used comprehensively (or have the potential and possibility to be used) for decision-making or equipment management where the participation of the human factor is minimal, i.e. where a person only performs the role of a supervisor, who monitors the operation of the system, but results and decisions are made without his intervention.

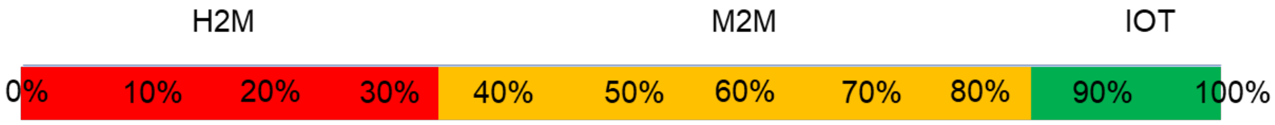


Figure 6. Maturity evaluation scale of objects and assets.

An example of the colour-marking of the map is presented in an extract from the Heat Map below. A certain group of IoT use cases may consist of different types of assets and equipment that need to be evaluated to determine the method of communication.

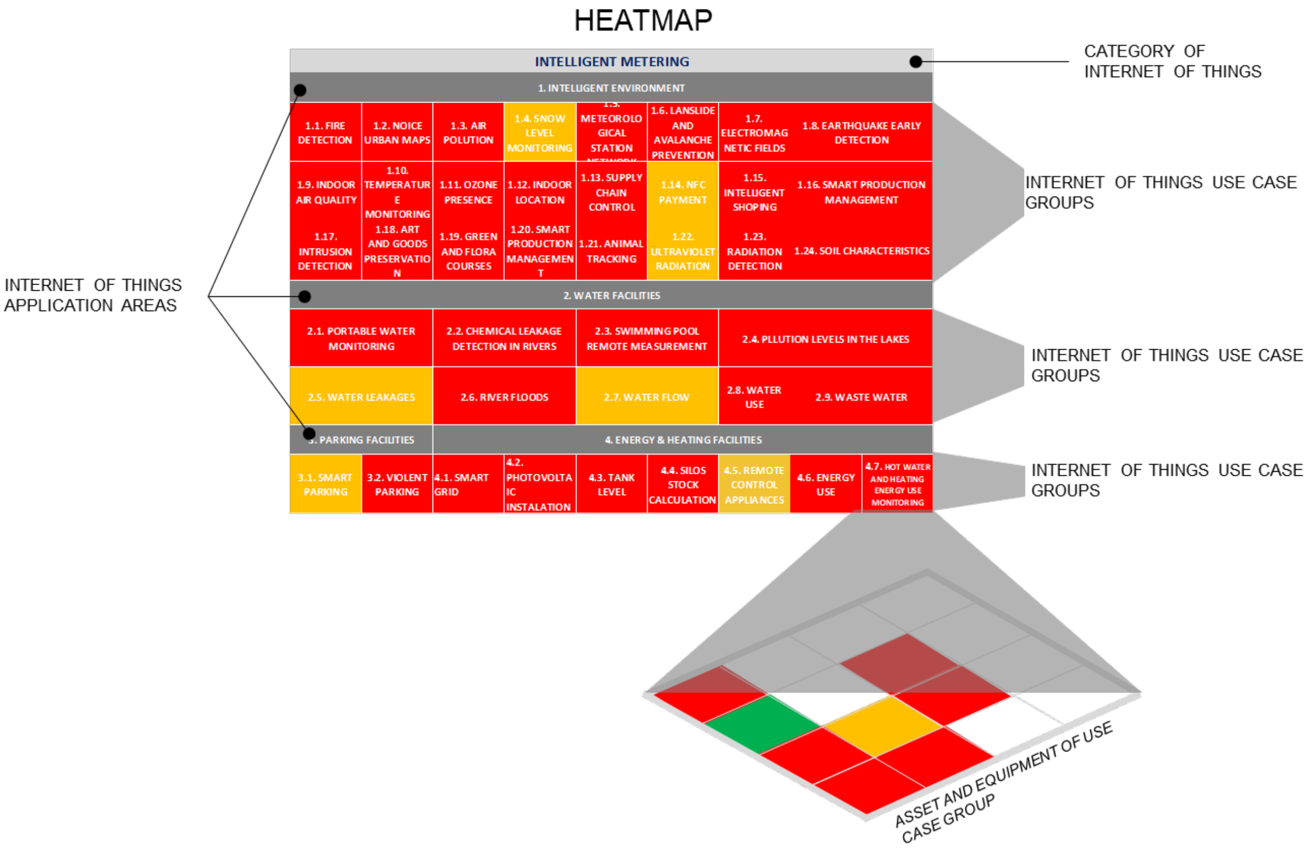

HEATMAP
INTELLIGENT METERING
CATEGORY OF INTERNET OF THINGS
1. INTELLIGENT ENVIRONMENT
1.1. FIRE DETECTION
1.2. NOICE URBAN MAPS
1.3. AIR POLUTION
1.4. SNOW LEVEL MONITORING
1.5. METEOROLOGICAL STATION NETWORK
1.6. LANSLIDE AND AVALANCHE PREVENTION
1.7. ELECTROMAGNETIC FIELDS
1.8. EARTHQUAKE EARLY DETECTION
1.9. INDOOR AIR QUALITY
1.10. TEMPERATURE MONITORING
1.11. OZONE PRESENCE
1.12. INDOOR LOCATION
1.13. SUPPLY CHAIN CONTROL
1.14. NFC PAYMENT
1.15. INTELLIGENT SHOPING
1.16. SMART PRODUCTION MANAGEMENT
1.17. INTRUSION DETECTION
1.18. ART AND GOODS PRESERVATION
1.19. GREEN AND FLORA COURSES
1.20. SMART PRODUCTION MANAGEMENT
1.21. ANIMAL TRACKING
1.22. ULTRAVIOLET RADIATION
1.23. RADIATION DETECTION
1.24. SOIL CHARACTERISTICS
INTERNET OF THINGS USE CASE GROUPS
INTERNET OF THINGS APPLICATION AREAS
2. WATER FACILITIES
2.1. PORTABLE WATER MONITORING
2.2. CHEMICAL LEAKAGE DETECTION IN RIVERS
2.3. SWIMMING POOL REMOTE MEASUREMENT
2.4. PLLUTION LEVELS IN THE LAKES
2.5. WATER LEAKAGES
2.6. RIVER FLOODS
2.7. WATER FLOW
2.8. WATER USE
2.9. WASTE WATER
INTERNET OF THINGS USE CASE GROUPS
3. PARKING FACILITIES
4. ENERGY & HEATING FACILITIES
3.1. SMART PARKING
3.2. VIOLENT PARKING
4.1. SMART GRID
4.2. PHOTOVOLTAIC INSTALATION
4.3. TANK LEVEL
4.4. SILOS STOCK CALCULATION
4.5. REMOTE CONTROL APPLIANCES
4.6. ENERGY USE
4.7. HOT WATER AND HEATING ENERGY USE MONITORING
INTERNET OF THINGS USE CASE GROUPS
ASSET AND EQUIPMENT OF USE CASE GROUP

Figure 7. Example of colour-marking of the Heat Map.

A Controlling (Accountable) stakeholder shall assess the maturity of each IoT use case group and its change. Stakeholders, their roles and responsibilities are defined in Section 7 of this document.

9. COMPATIBILITY

The Internet of Things policy is drafted taking into account the Strategic Plan of Vilnius for 2020-2030, the Vilnius City Strategic Direction Vilnius2IN, the Vilnius City Master Plan and the Smart Cities Initiative of the European Commission European Innovation Partnership for Smart Cities and Communities (EIP-SCC), which brings together cities, industries, small businesses, banks, research and others. The EIP-SCC aims to improve urban life through more sustainable integrated solutions and to solve specific urban challenges in different policies, such as energy, mobility, transport and the development of information and communication technologies. The EIP-SCC is based on the involvement of the society, industry and other stakeholders in the development of innovative solutions and participation in management of the city.

10. FINAL PROVISIONS

The goals and objectives laid down in the Internet of Things Development Policy of Vilnius City will be implemented taking into account provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

The development of IoT technology and advanced solutions requires special attention to be paid to the supply of equipment to be improved. The constituent parts and components as well as architecture of Internet of Things discussed in this policy is not an innovation, but an extension of solutions for their implementation and the need for simpler integration and smoother interoperability shall allow applying the latest standards, for example, in cloud computing and data transmission; in the context of IoT platform and applications, the development of Internet of Things in Vilnius shall be based on the latest generation technology and implemented in accordance with the latest standards. The role of the latest standards in the development of IoT technology shall be treated as the key requirement for their success.

Proper implementation of the Internet of Things Development Policy and the achievement of the set goals and tasks will allow to create a strategic model of intelligent city management focused on service efficiency, to pursue higher key indicators of the city and to accurately implement change, to create more attractive conditions for investment, to promote citizenship and development of innovations creating direct practical benefit in the city.

The Policy shall not apply to its full extent to pilot projects and proof of concept trials aimed at justifying a technical solution, the value being created for activities and services, benefits, the value being created for the city or for setting monetization indicators.

PREPARED BY:

Simas Sodys – Vilnius City Administration, Dalius Kazlauskas - Vilnius City Administration, Linas Bartusevičius - Vilnius City Administration, Benita Petrošiūtė - Vilnius City Administration, Marius Brigmanas - Vilnius City Administration, Aistė Paludnevičiūtė - Vilnius City Administration, Renata Michalkevičienė - Vilnius City Administration, Andžej Dinkis - Vilnius City Administration, Sandra Norbutaitė - Vilnius City Administration, Giedrė Čeponytė - Vilnius City Administration, Jonas Bartlingas - Vilnius City Administration, Gintaras Leperskas - Vilnius City Administration, Gintautas Runovičius - Vilnius City Administration, Rasa Strupienė - UAB Vilniaus Viešasis Transportas, Aurelijus Deksnys - SĮ Vilniaus Planas, Povilas Rinkūnas - SĮ Vilniaus Planas, Guoda Ropaitė-Beigė - BĮ Vilniaus miesto savivaldybės visuomenės sveikatos biuras, Daina Juršytė - BĮ Vilniaus miesto savivaldybės visuomenės sveikatos biuras, Pavel Atraškevič - UAB Vilniaus Apšvietimas, Robertas Kontrimavičius – UAB Vilniaus Vystymo Kompanija, Domas Stanelis - AB Vilniaus Šilumos Tinklai, Rimvydas Sinius - UAB Vilniaus Šilumos Tinklai, Egidijus Steponavičius - UAB Grinda, Laimonas Murinas - SĮ Vilniaus atliekų sistemos administratorius, Vilius Kasperavičius - SĮ Susisiekimo Paslaugos, Karolis Žemaitis - VŠĮ Go Vilnius.

CHECKED BY:

Povilas Poderskis - Vilnius City Administration, Dr. Eglė Radvilė - Vilnius City Administration.

ANNEXES

ANNEX NO. 1 TABLE OF APPLICATION OF INTERNET OF THINGS TECHNOLOGY.

ANNEX NO. 2 GUIDELINES FOR ENSURING COMMUNICATION SERVICES.

APPROVED

INTELLIGENT VILNIUS CITY BRAIN |BIG DATA|

INTELLIGENT METERING |IOT|

Use cases

1 Intelligent Environment

1.1	**Fire Detection** Monitoring of combustion gases and preemptive fire conditions to define alert zones.
1.2	**Noise Urban Maps** Sound monitoring in bar areas and centric zones in real time.
1.3	**Air Pollution** Control of CO2 emissions of factories, pollution emitted by cars and toxic gases, solid elements, tree pollen, other elements in the air generated by many factors.
1.4	**Snow Level Monitoring** Snow level measurement in real time and corps avalanche prevention.
1.5	**Meteorological Station Network** Study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes.
1.6	**Landslide and Avalanche Prevention** Monitoring of soil moisture, vibrations and earth density to detect dangerous patterns in land conditions.
1.7	**Electromagnetic Field Levels** Measurement of the energy radiated by cell stations and WiFi routers.

1.8	**Earthquake Early Detection** Distributed control in specific places of tremors.
1.9	**Indoor Air Quality** Monitoring of chemical elements, toxic gases and oxygen levels inside buildings to ensure workers and goods safety.
1.10	**Temperature Monitoring** Control of temperature inside industrial and medical fridges with sensitive merchandise.
1.11	**Ozone Presence** Monitoring of ozone levels during the process in agriculture and food industry.
1.12	**Indoor Location** Asset indoor location by using active and passive tags (RFID/NFC).
1.13	**Supply Chain Control** Monitoring of storage conditions along the supply chain and product tracking for traceability purposes.
1.14	**NFC Payment** Payment processing based in location or activity duration for public transport fare collection

1.15	**Intelligent Shopping** Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.
1.16	**Smart Product Management** Control of rotation of products in shelves and warehouses to automate restocking processes.
1.17	**Intrusion Detection** Detection of windows and doors openings and violations to prevent intruders.
1.18	**Art and Goods Preservation** Monitoring of conditions inside museums and art warehouses.
1.19	**Green & Flora Courses** Selective irrigation in dry zones to control the water resources required in the green, monitor tree branches, leaves and etc.
1.20	**Smartphone Detection** Detect iPhone and Android devices and in general any device which works with WiFi or Bluetooth interfaces.
1.21	**Animal Tracking** Location and identification of dogs, cats, rats and other animals population in city areas and animals grazing in open pastures.
1.22	**Ultraviolet Radiation** Measurement of UV sun rays to warn people not to be exposed in certain hours.

1.23	**Radiation Levels** Distributed measurement of radiation levels (in nuclear power stations) surroundings to generate leakage alerts.
1.24	**Soil characteristics** Monitoring of beach, sport and games areas, sand boxes, soil characteristics in leaving areas, microbiological and chemical pollution detection
2	**Water facilities**
2.1	**Potable water monitoring** Monitor the quality of tap water in the city.
2.2	**Chemical and radiation leakage detection in rivers** Detect leakages and wastes of factories in rivers.
2.3	**Swimming pool remote measurement** Control remotely the swimming pool conditions.
2.4	**Pollution levels in the lakes** Control Realtime leakages, microbiological and wastes level in the lakes.

2.5	**Water Leakages** Detection of liquid presence outside tanks and pressure variations along pipes.
2.6	**River Floods** Monitoring of water level variations in rivers, dams and reservoirs.
2.7	**Water Flow** Measurement of water pressure in water transportation systems, water tank levels.
2.8	**Water Use** Water supply consumption monitoring to obtain advice on how to save cost and resources.
2.9	**Water Waste** Monitoring of water waste facilities in local and centralized areas
3	**Parking facilities**
3.1	**Smart Parking** Monitoring of parking spaces availability in the city.
3.2	**Violent Parking** Detection of violent parking in forbidden places in the city.

4	**Energy & Heating facilities**
4.1	**Smart Grid** Energy consumption monitoring and management.
4.2	**Photovoltaic Installations** Monitoring and optimization of performance in solar energy plants.
4.3	**Tank level** Biofuel, oil and gas levels in storage tanks and cisterns.
4.4	**Silos Stock Calculation** Measurement of emptiness level and weight of the goods.
4.5	**Remote Control Appliances** Switching on and off remotely appliances to avoid accidents and save energy.
4.6	**Energy Use** Energy supply consumption monitoring to obtain advice on how to save cost and resources.
4.7	**Hot Water and Heating Energy Use** Hot water and heating energy supply consumption monitoring

5	**Building, Security & Critical facilities**
5.1	**Perimeter Access Control** Access control to restricted areas and detection of people in non-authorized areas.
5.2	**Liquid Presence** Liquid detection in data centers, warehouses and sensitive building grounds to prevent break downs and corrosion.
5.3	**Explosive and Hazardous Gases** Detection of gas levels and leakages in industrial environments, education institution, living buildings, surroundings of chemical factories.
5.4	**Item Location** Search of individual items in buildings, big surfaces like warehouses or harbors.
6	**Intelligent Lighting**
6.1	**Lighting Control** Intelligent and weather adaptive lighting in street lights.
7	**Intelligent Roadway**
7.1	**Structural health** Monitoring of vibrations and material conditions of viaduct, bridges and historical monuments.

7.2	**Traffic Congestion** Monitoring of vehicles and pedestrian levels to optimize driving, public transport and walking routes.
7.3	**Intelligent Roads** Intelligent Highways and sidewalks with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.
8	**Waste facilities**
8.1	**Waste management** Detection of rubbish levels in containers to optimize the trash collection routes.
8.2	**Waste Weight Monitor** Detection of rubbish levels in containers to optimize the trash collection routes.
9	**eHealth**
9.1	**Fall Detection** Assistance for elderly or disabled people living independent.
9.2	**Fridges** Control of conditions inside freezers storing products, medicines, organic elements and etc.

9.3	**Sportsmen Care** Vital signs monitoring in high performance centers and fields.
9.4	**Patients Surveillance** Monitoring of conditions of patients inside hospitals and in old people's home.
10	**Public transport ecosystem**
10.1	**M2M Applications** Machine auto-diagnosis and assets control.
10.2	**Vehicle Auto-diagnosis** Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.
10.3	**Vehicle occupancy** Monitoring vehicle occupancy
10.4	**Vehicle location** Tracking vehicle location in the city.
	INTELLIGENT VIDEO SURVEILLANCE |VIDEO|
	Use cases
11	**Behavior analysis**
11.1	**Biometric data** Measure and calculate human body characteristics to identify physiological and psychological behavior.

11.2	**Safe city** Recognise of criminal and aggression indications.
12	**Violation detection**
12.1	**Smoking detection** Smoking detection in smoking forbidden areas, children gardens and school premises.
12.2	**Uncared children detection** Children without adult supervision detection near water, dangerous areas, vehicles and etc.
12.3	**Dangerous item detection** Violent items, knife, gun detection in public areas.
13	**Object detection**
13.1	**Left items** Uncared items detection in public areas.
13.2	**Illegal out-of-store business** Illegal stalls, outdoor bars, trading in market premises detection.
13.3	**Illegal road-side, pedestrian-side objects** Bikes, electric scooters left messy, unidentified dangerously left items on road-side, pedestrian-side, bicycle-side

13.4	**Material piling up** Trash, waste, construction waste detection outside buildings, near garbage containers, trash cans and on streets.
13.5	**Illegal advertising** Illegal and inappropriate content advertising detection on buildings, streets, parking areas.
13.6	**Traffic and accident control** Control traffic accidents, speed limits and average, detect unauthorized vehicle movement on pedestrian-side and entries in to yellow dashed areas, unauthorized pedestrian street crossings.
13.7	**Parking areas** Control parking areas occupancy, detect parking violence in parking restricted areas.
13.8	**Construction areas** Conrol of contractors course work performance, building areas, teritorries, detect restricted actions.
	INTELLIGENT OPERATION CENTER |AI| **Use cases**
X	**Intelligent Command Platform**
X.1	**Case reporting** Automatically identify case behavior, events, violations and generate alarms.

X.2	**Case registration** Automatically generate a case registration work order (location, time and incident type) based on the event information.
X.3	**Case dispatch** Automatic case distribution to multi-level comprehensive support and dispatch converged voice and video consultation.
X.4	**Case handling** Support converged command and handling of urban management cases, enchanting urban management efficiency.
14	**Net**
14.1	**Operation Monitoring** City operating status displayed on one map.
15	**Hub**
15.1	**Analysis & Decision-making** One-click decision-making support & management.
16	**Ecosystem**
16.1	**Innovation Service** One-step self-evolution & innovation platform

17. Strategies

17.1 Command

Integrated city operation & linkage

1. Scope

The guidelines for ensuring communication services laid down in the Annex define the conditions for requirements to be detailed for each case of IoT or smart solution being implemented and its specifics.

2. Requirements for protection from interference

If a communication service uses a certain part of a radio spectrum which can be used without a separate permit in accordance with the conditions set in advance (often such use is referred to as unlicensed use), the communication service provider shall ensure all the necessary measures to protect communication service from any external interferences, third-party attacks disrupting network operations, and shall immediately take action to eliminate them, thus ensuring the quality and integrity of the service. The communication service provider shall indicate the equipment, technical means and methods used to detect external interferences.

The communication service provider shall provide a detailed action plan to protect communication quality and the service from external unforeseen factors, to eliminate interferences, incidents and to maintain the communication service parameters for equipment operating in the same frequency band so that other systems operating on the same frequency do not interfere with each other (do not cause any interferences).

3. Requirements for communication technology coverage

The communication technology used for the implementation of the Internet of Things and advanced solutions shall fully cover at least 99.5% of the territory of the city of Vilnius. This condition shall also apply outside the territory of the city of Vilnius, when solutions installed by a group of Vilnius city municipality enterprises fall within other territories bordering the Vilnius city municipality.

Coverage shall be published in publicly available sources of information, providing a clear calculation methodology and criteria used as a basis for calculating coverage, assessing, *inter alia*, the maximum growth of devices connected in the network, devices and communication technologies operating on the same frequency and other conditions under which the existing network would retain the same coverage characteristics.

4. Communication security

The service provider shall ensure that the communication network is secure. Any solutions based on data transmission over public networks (Internet) are not acceptable and shall be implemented by separating the data transmission network at the physical (dedicated optical network) and / or logical (VPN / APN) levels.

The service shall meet data security requirements, i.e. security shall be ensured to prevent the possibility of altering, scanning, copying or otherwise affecting the data transmitted in the network, or transferring them to third parties.

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

5. Standards

The communications operator shall meet conditions of the “Application of Standards” Policy.

6. Requirements for the provision and maintenance of the communication service

The communication service provider shall ensure monitoring of service provision and troubleshooting 24 /7:

a. It shall have a network equipment monitoring and maintenance center for monitoring network operation parameters, diagnosing problems and restoring communication.

b. Troubleshooting shall be done without intervention of the recipient of the communication service. If the infrastructure is critical, the communication service provider shall ensure the functionality of automatic switching to another operating network without any additional configuration actions. If a device serves non-critical infrastructure, KPIs indicated according to sample requirements in clause 10 (optional or additionally required) and conditions laid down in clause c shall be met, or automatic connection to the network of another communication service provider shall be triggered for devices the connection of which does not meet quality KPIs.

c. It shall have a technical support center registering reports on communication service failures, inquiries and applications by phone, e-mail or using Help-desk software tools, also consulting on issues relating to the provision of the communication service.

d. An emergency engineering service shall be ensured for urgent restoration of network operation and troubleshooting of failures and disruptions in locally remote network equipment locations.

Classification of communication service failures and troubleshooting times (SLA):

a. Service availability is a period of time calculated per month; requirements which the communication service availability is subject to shall be specified in light of a specific case and its specifics. This parameter is expressed as a percentage: (A-B) / A x 100%, where A is a period of one month (in hours), B – period when service is unavailable (in hours). Technical maintenance time shall not be included in the period of non-provision of the communication service when calculating the availability of the communication service.

b. Technical maintenance is the period of time when works planned in advance are conducted in the data transmission network, which may result in disruptions in the provision of communication services. The communication service provider shall notify the service recipient of the planned technical maintenance works, which may result in communication service disruptions, 48 (forty-eight) hours in advance, also indicating the estimated duration of the works. The technical maintenance time may not take longer than 2 (two) hours per month at each place of installation of the communication service.

c. Service failure is a disruption in the provision of the communication service when the provision of the communication service is interrupted or its technical parameters become worse than provided for in the requirements which the communication service is subject to.

d. Failure report. Having noticed any communication service failure, the service recipient shall report them to the technical support centre of the communication service provider, which is open 24/7.

e. Response time is a period of time from the moment when the service recipient reported a communication service failure till the moment when the service recipient was first notified of the type of the failure and of the estimated time of restoration of the communication service. The communication service provider undertakes to respond to a failure report within 1 (one) hour at the most.

f. Troubleshooting time is a period of time from the moment when the service recipient reported a communication service failure to the communication service provider until the restoration of the provision of the communication service. In presence of conditions under which conducting works related to communication service troubleshooting shall be prohibited in accordance with the procedure established by legal acts of the Republic of Lithuania, communication service failures shall not be fixed and the duration of fixing of communication service failures shall not be calculated. The communication service provider shall fix failures of its network equipment within the time period specified in the table at the most:

Failure priority	Troubleshooting time	Note
1	4 - 8 working hours	To be indicated according to the need of a specific case
2	6 - 8 working hours	To be indicated according to the need of a specific case
3	72 working hours - 1 week	To be indicated according to the need of a specific case

Failure priorities and explanation

Failure priority	Description
1	Service downtime, a significant number of errors (>0,5%) in the data transmission channel, resulting in complete failure of data transmission
2	Partial service downtime, non-compliance of certain parameters with the parameters provided for in the agreement; more errors (<0,5%) in the data transmission channel, but data can be transmitted
3	Decline in values of some communication parameters, few errors (<0.1%) in the data transmission channel

7. Requirements for switching the communication operator

For critical infrastructure (if the device is used in solutions the downtime of which may lead to a disruption of important functions and services provided by the company), the communication solution shall be able to support at least two different communication providers selected from the device in real time (if infrastructure of one/ main communication provider is (becomes) unavailable, the device itself shall switch to infrastructure of another communication provider).

or

the communication technology shall allow switching communication operator (communication service provider) remotely. This requirement shall be mandatory in order to maintain service integrity for 10 years or more without being tied to the communication service provider. The applicable solution shall allow switching the communication operator remotely, without changing the device or taking over the communication infrastructure.

8. Requirements for data reading and their collection from devices

Communication technology shall ensure two-way sending / receiving of data to / from devices. Device connection shall always be available for data reading at any time and shall not be subject to any restrictions. Device requirements shall provide for device’s response time.

Communication technology shall be based on principles that shall not allow all devices to send data on specific functions or failures of such devices simultaneously. The communication service provider shall monitor and manage (at the logical level of network parameter change) radio frequency interferences and protect the network against congestion. Despite the growing number of devices, the quality of service and the speed of the communication service shall not become worse. There shall also be a possibility for certain specific devices to get a priority to send data faster.

9. Requirements for backup power supply

Base stations shall have uninterruptible power supplies (UPS) ensuring an average of 3 hours of power supply in case of the outage of the main power supply.

10. Requirements for physical protection

Accesses to base stations shall be protected from unauthorized access, unauthorized connections and other activities that may endanger the operation of the equipment and data security without the permission of the operator.

11. Requirements for key communication quality indicators

Requirements shall be set according to the conditions of a specific solution (time intervals when data must be handed over / collected, the amount of data to be handed over / collected, etc.). KPIs may be supplemented with additional values that are needed to implement a specific solution under development and to monitor network parameters.

All the collected data*		
Time after registering information (indicating Mb) (indicating the number of devices, in thousand)	**1 hour**	**8 hours**
Data received and processed, %	E.g. >= 99%	E.g. >= 99.9%

**Excluding disabled and deactivated devices*
Table Data Collection KPIs

Urgent (real time) incidents			
Time after an incident	**30 s**	**60 s**	**120 s**
Signals received and processed, %	E.g. >=90%	E.g. >=95%	E.g. >=99,9%

Urgent incident KPIs

Transfer of information (indicating Mb) to remote devices			
Time from the initiation of the sending	**After 1 hour**	**After 3 hours**	**After 6 hours**
Devices received and processed %	E.g. >=90%	E.g. >=95%	E.g. >=99,9%

KPIs of information transfer to remote devices

Information reading on request	
Time from the initiation of a request	E.g. <= 30 s

reading on request KPIs

Equipment visibility (availability)*	
Information on devices visible at any given time %	E.g. >= 98%

Equipment availability KPIs