IoT AND THE POLISH ECONOMY

REPORT OF THE WORKING GROUP FOR THE INTERNET OF THINGS
AT THE MINISTRY OF DIGITAL AFFAIRS

Ministry of Digital Affairs

Table of contents

First edition
Released for print: April 2019.
Print run: 200 copies.
An electronic version of this document is available at www.gov.pl/cyfryzacja

The report has been prepared thanks to the work of the Working Group for the Internet of Things comprising experts working *pro publico bono* at the behest of the Minister of Digital Affairs since 24 August 2018.

The work of the group was led by Leszek Maśniak and Dr Maciej Kawecki – Ministry of Digital Affairs.

Editorial Team

Ministry of Digital Affairs:
Leszek Maśniak
Katarzyna Marcisz
Jakub Płodzich
Ewa Świętochowska
Anna Tomala
Jan Zaboklicki

Polish Chamber of Information Technology and Telecommunications (PIIT):
Borys Stokalski, leader of the IoT stream in the "From Paper to Digital Poland" task force at the KRMC **(**Council **of** Ministers Committee for Digital Affairs)
Michał Gałagus

Industry group leaders:
Krystian Bień, Polpharma sp. z o.o.
Aleksander P. Czarnowski, AVET Information and Network Security Sp. z o.o.
Tomasz Dylik, Exatel
Paweł Gora, University of Warsaw, Faculty of Mathematics, Informatics and Mechanics
Damian Hajduk, strategic advisory and management in transport and logistics
Michalski Mateusz, mTechnology / Hackerspace Wrocław Association
Piotr Mieczkowski, Digital Poland Foundation
Kamil Nawrocki, BConnect
Marcin Płóciennik, Poznań Supercomputing and Networking Center (PSNC IBC PAS)
Jaroslaw Smulski, IDC Poland & Baltic States
Krzysztof Wadas, Cyfrowy Polsat Group
Remigiusz Wiśniewski, Detecon International
Marcin Wolski, Billon Group Ltd.
Marek Zamłyński (until 2018)

Coordinating authority
Ministry of Digital Affairs

Public institutions supporting the Group's activities:
Ministry of Infrastructure, Ministry of Investment and Development
Ministry of Entrepreneurship and Technology,
Head Office of Geodesy and Cartography
Institute of Communications – National Research Institute
EMAG Institute of Innovative Technologies
Civil Aviation Authority

Key Business Partner:
PIIT
Polish Chamber of Information Technology and Telecommunications

Substantive Partner:
digitalpoland
Digital Poland Foundation

Layout and graphic design: NAŁ Albert Łukasiak
Printing: Drukarnia Offsetowa Express Druk
Financed from the budget of the Ministry of Digital Affairs

Ladies and Gentlemen,

I cannot start this brief introduction in any other way than with a few words of gratitude. The presented report is the result of good cooperation between more than a hundred representatives of business, academia and public administration. I would like to express my sincere gratitude not only as the head of the institution that had the honour and pleasure of hosting the group, but also as a representative of the government to which this collective voice is addressed.

Information and communication technology is the most promising direction for the development of this country, including its public administration. As a very dynamic field, it constantly surprises us with its impact on social and economic life. Even the greatest of minds did not manage to predict what the surrounding world would look like these days, and we need to be frank with ourselves – we cannot reliably predict what technology will bring us in future. Therefore, government action on new technologies requires a more agile approach compared to other areas characterised by a slower pace of change. This means, among other things, a broader introduction of so-called smart law – laws that define objectives and rules of conduct that can be applied despite the ongoing changes in the environment, instead of arbitrarily indicating specific technologies and actions. This was the underlying principle for our data protection laws, our constitution for business, and our national cybersecurity framework.

The second agility factor, which I believe to be crucial as the Minister of Digital Affairs, is a continuous and active collaboration with business and academia, because they are the ones who see both the new opportunities, as well as emerging risks and dangers connected with ICT. As a government, we have a number of positive examples of successful collaboration in this field, and we can see how important the general public's voice is in shaping the laws and activities of government institutions. The Ministry of Digital Affairs actively runs a number of working groups at various levels, dominated by representatives of business, legal and academic circles. These include a working group on artificial intelligence, protection of personal data, and blockchain technology.

The Working Group for the Internet of Things managed to work out a joint position within just six months, in spite of the great diversity of participating companies and institutions, and we are pleased to present it on the following pages of our report. Once again, you have proved that even direct competitors have a common interest in the development of the country and in stimulating innovation in the economy, and most importantly, that the government's priorities for action can remain in harmony with the expectations of citizens and enterprises.

Your voices and opinions are valued, noticed and appreciated by more entities than just the Ministry of Digital Affairs. Other ministries have also declared their willingness to collaborate in order to take better advantage of your suggestions and proposals.

Moreover, we would like to ask you for more. We continue to encourage active participation in the ongoing and future initiatives launched by central and local governments, as well as working groups, consultations and partnerships, and we invite you to take advantage of our support programmes. Poland remains an important centre of ICT competencies – this is not merely a prediction, but a fact – and it would be advisable to exploit this potential.

Marek Zagórski, Minister of Digital Affairs

WARSAW, 23 APRIL 2019

01

ABOUT THE REPORT

The Working Group for the Internet of Things was established in response to the changing technological environment and the growing role of new technologies in stimulating economic growth. The main objective of the Group is to develop recommendations for actions which the Polish government should undertake in order to ensure proper conditions for the development and promotion of IoT technologies based on Polish know-how, which can be used to improve the quality of life in Poland and to give the Polish economy a competitive edge over international markets, with particular emphasis on supporting the promotion of innovative Polish companies worldwide. The work of the Group focuses on the following areas:

- analysis of the needs of the Polish economy pertaining to the implementation of IoT technologies and identifying specific solutions which should be enacted at the level of individual ministries and the government;
- support for working out solutions aimed at stimulating the growth of companies, as well as the development of IoT-oriented products and services by the Ministry;
- identifying legal barriers limiting IoT development;
- defining areas in need of standards and regulations in order to harmonise these parts of the market.

The Group encompassed experts representing companies investing in IoT-related products and services in Poland, as well as economic sectors whose development depends on these solutions. The constantly growing Group also encompassed representatives of industry associations, academic circles, unions and employer groups, as well as social organisations.

In preparing this report, the Working Group for the Internet of Things worked to describe the current institutional and legal status, as well as the business environment of the IoT industry, working out recommendations, the implementation of which will contribute to significant benefits for the Polish economy resulting from the introduction of IoT technologies. The report also identifies sectors where the use of IoT technology can result in tangible benefits for citizens, companies, local government units and the state as a whole, significantly contributing to improving the quality of life in Poland.

The work was carried out within the framework of 10 subgroups:

General
Leaders: Marek Zamłyński (until December 2018),
Piotr Mieczkowski, Digital Poland Foundation
Jaroslaw Smulski, IDC Poland & the Baltic States

Security and Certification
Leader: Aleksander P. Czarnowski, AVET Information and Network Security Sp. z o.o.

Finance and Insurance
Leader: Marcin Wolski, Billon Group Ltd.

Smart Cities and Buildings
Leader: Remigiusz Wiśniewski, Country Manager, Detecon International GmbH

Healthcare
Leader: Krystian Bień, Polpharma sp. z o.o.

Smart Metering
Leader: Krzysztof Wadas, Cyfrowy Polsat Group

Industry
Leader: Kamil Nawrocki, BConnect

Agriculture and Environmental Protection
Leader: Marcin Płóciennik, Poznań Supercomputing and Networking Centre (PSNC IBC PAS)

Telecommunications
Leaders: Tomasz Dylik, Exatel, and
Michalski Mateusz, mTechnology and Hackerspace Association Wrocław

Transport, Logistics and Autonomous Vehicles Leaders: Paweł Gora, University of Warsaw, Faculty of Mathematics, Informatics and Mechanics,
and Damian Hajduk, strategic advisory and management in transport and logistics

02

EXECUTIVE SUMMARY

Internet of Things in the context of national technological strategies

The report outlines the potential of IoT technology from the standpoint of development priorities of the Polish economy. It presents the identified barriers and obstacles, along with suggestions on how to remove them in order to unleash potential. The document also reviews current global trends, focusing on drawing conclusions from the observed phenomena and recommendations for Poland concerning key aspects connected with the development of IoT systems – legal regulations, education and ethics.

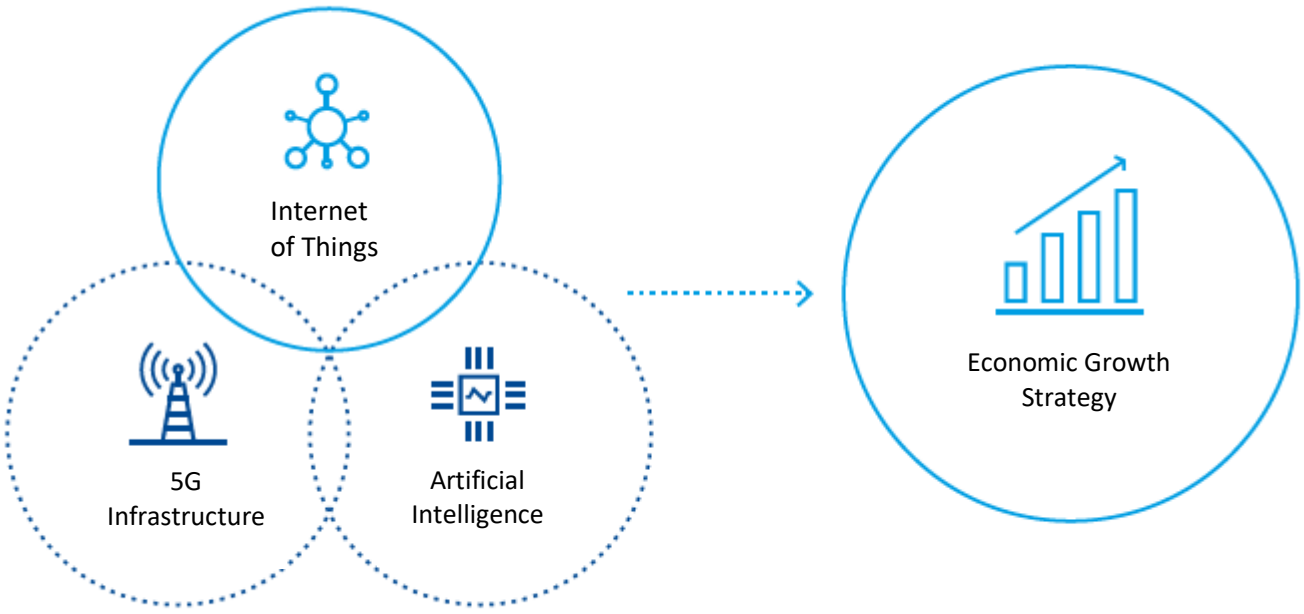
It should be pointed out that the development of the Internet of Things concerns a wave of innovative solutions taking advantage of a network of smart objects – devices equipped with the ability to process data and work together – aiming for more than just meeting the current and emerging needs. As in the case of the first Internet revolution, we are seeing the emergence of new areas of use, unexpected consumer behaviours and new business models.

This is certainly an area that offers enormous opportunities, while also exhibiting a number of serious risks characteristic and inherent for mass waves of innovation. While trying to highlight the directions which seem to be particularly promising these days, we are forced to extrapolate from the things we already know and to speculate about what may come.

This is why this report should be regularly updated in order to maintain its value as a guide, as well as a set guidelines for formulating technological strategies that will enable taking advantage of the development of the Internet of Things. This process should be coordinated in a manner that takes into account two directions closely related to the Internet of Things – national plans for the development of Artificial Intelligence (AI), as well as the 5G infrastructure development programme. These topics are closely interlinked with each other and require harmonisation in a number of fields, including in the context of plans for economic growth, since they constitute a key supporting factor.

Looking at various initiatives emerging in Poland and around the world, we can quote William Gibson – the future is already here – it's just not evenly distributed.

The context of the concept of the development of the Internet of Things



The potential of the ICT and electronics industries

The development of IoT-related products and services primarily requires innovative concepts of value and business models. The industry perspective presented in this report is dedicated mainly to those topics. Their creations and implementations is a matter of adequate potential of the ICT and electronics industries. This is why the diagnosis of the potential of Polish companies which comprise the broadly understood digital products and services sector makes up a significant part of this document. The available data and experience of industry experts point to the fact that we are in a good starting position, both from the standpoint of technological competencies, as well as the number and dynamics of companies capable of developing IoT solutions. Whether this potential can be exploited in an effective and efficient way will be determined by the pace of transition of our ICT and electronics industries from the current model, which entails providing integration services and sub-contracting the development of components, to building product companies, offering their creations to end customers in the global market. Supporting this transition by means of technological diplomacy and funding programmes for the implementation of innovative solutions for end customers seem to be the most important actions that the state can undertake in order to support the growth of the IoT market.

Industry outlook and common conclusions

The detailed characteristics of the industries that were considered particularly promising in the context of IoT development in Poland constitute a particularly important part of this report. It should be pointed out that within the majority of them, Polish enterprises and engineers develop specific solutions and products that fit in with global IoT trends.

In the context of each of them, the Working Group has identified specific legal and institutional obstacles to the widespread use of IoT solutions in Poland. The authors also outline solutions which may be conducive to removing these barriers. The final conclusions encompass general horizontal recommendations, the implementation of which will help unleash the full potential of the IoT-based economy.

In the course of the Group's work a number of issues and problems common to all industries have been identified. These include:

- Lack of specialised education – as of now, only individual universities offer IoT-related majors, which may translate into an inability to meet the ever-increasing demand for qualified staff in this area;
- Lack of orders and commissions (RFP) concerning IoT solutions from large state-owned companies – leading to problems with scaling solutions in the domestic market for Polish IoT system developers;
- Lack of registers of prototypes, and actually implemented innovative solutions – asymmetry of information, which limits knowledge exchange between market participants;
- Imprecise legal framework concerning IoT – IoT-related issues are scattered across many acts and laws, with no regard for their consistency;
- Current applications (mainly in logistics and asset protection industries) being limited to M2M (Machine-to-Machine) solutions, which may limit the development of Polish IoT solutions for the consumer market;
- The existing legislation concerning collecting, storing, using and sharing data[1] limit the development of IoT solutions in Poland. One of the most important legal challenges pertaining to data involves issues concerning intellectual property. Given that IoT infrastructure is based on the cloud computing model and Big Data, similar challenges will emerge in an exponential manner.[2]

In addition to industry recommendations, the Working Group for the Internet of Things proposes the following actions, the implementation of which will bring about dynamic development of IoT in Poland:

- Improving coordination concerning the activities of government agencies in the context of IoT and other modern technologies;
- Developing and launching a funding programme for pilot and reference implementations of innovative IoT solutions with high internationalisation potential (developed both by IoT startups, as well as mature companies) in order to lower the risks of innovation;
- Regulating the possibility of exchanging or commercialising IoT-based data and information in a scope that does not infringe upon fundamental laws concerning protection of personal data, as well as sectoral and professional secrets;
- Promoting good practices and pioneering solutions, for example in the form of contests organised by the government to distinguish exemplary IoT companies;
- Creating supporting programmes for public entities at the central level (financing, support in selecting and implementing technologies);
- Increasing the transparency of the activities of supervisory authorities, including – when a given matter falls within the scope of competence of several such bodies – issuing common and unambiguous explanations resulting from social consultations and agreements between individual bodies;
- Introducing tax exemptions for using IoT solutions.

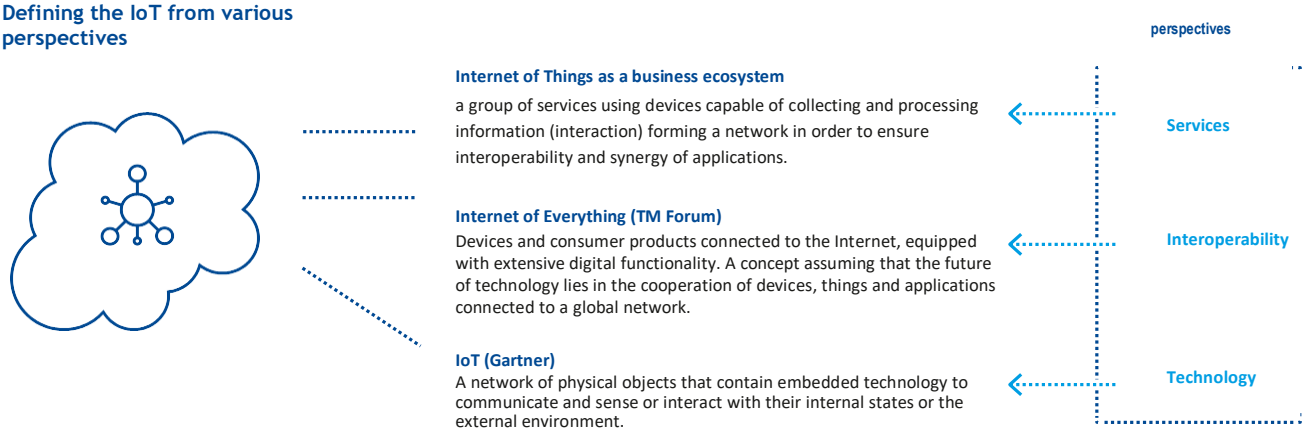
1 McKinsey Global Institute, The Internet of Things: Mapping the value beyond the hype, https://www.mckinsey.com/business-functions/digital- mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

2 Kerr, 2014

03

DEFINING THE INTERNET OF THINGS (IoT)

Defining the IoT from various perspectives



Technological definition

IoT is a wired or wireless network used to connect devices which work autonomously (without any human interaction) to collect, share and process data, or to interact with their surroundings on the basis of said data.

It is a concept concerning building highly distributed telecommunication networks and information systems, which can be used for developing smart measuring and control devices, as well as analytical and control systems, which can be implemented in every area of life, economy or science.

Architectural definition

IoT is a concept of information architecture which enables cooperation (interoperability) between various information and communication systems supporting a wide variety of field applications, based on the following layers:

- Hardware – devices (or objects that include said devices), in particular sensors and actuators, but also controllers, smartphones, tablets, laptops and computers, which are capable of communicating and processing data without, or with limited, human interaction;
- Communication – a telecommunications infrastructure and network (wired or wireless), based on any data transmission standards with any scope and range (in this case – the internet).
- Software – IT systems used by IoT devices and software enabling data exchange and processing, as well as managing the system and its security;
- Integration – groups of defined IT services which ensure software interoperability at all levels of the architecture.

Business definition

The IoT is an ecosystem of business services using devices capable of collecting and processing information (interaction), forming a network in order to ensure the interoperability and synergy of applications. Combining Internet of Things products and services enables better understanding of the end consumers, environment, products and processes, as well as identification of relevant events and reacting in order to immediately optimise or ensure more precise customisation.

04

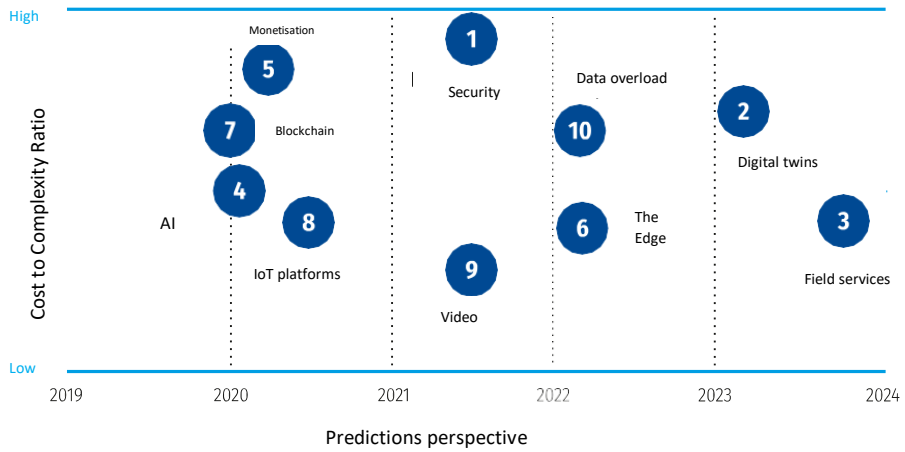
IoT DEVELOPMENT PROSPECTS AROUND THE WORLD

The upcoming two years are crucial when it comes to preparations for the changes ushered in by the popularisation of IoT solutions. The IoT is going to be a starting point for a lot of significant changes in the majority of organisations, causing an increase in demand for new, scarce competencies (among others, experts in analysing large data sets – **Data Scientists**) and creating new sources of demand for electronic industry products and services, as well as industrial automation solutions. This is also the final moment to strengthen education in this area in order to better prepare staff for the upcoming challenges.

According to data, the adoption of the IoT in the world is going to erupt in 2020. This means that Poland and its enterprises have the last chance to join the race for the highest stakes. It may be worthwhile to take a closer look at the following IoT phenomena, which will certainly interest global players in the IoT market in the coming months:

- focus on ROI-effective IoT adoption scenarios, as well as a dynamic growth of the number of such scenarios;
- more than 90% of IoT solution implementations will be based on artificial intelligence mechanisms, and the role of cooperation between the engineers implementing these solutions and data scientists will significantly increase;
- the market will experience a significant shortage of workers with the skills required in these respective areas;
- it is estimated that by 2020, more than 70% of all companies will invest in technical infrastructure and build an IoT platform for their organisations by developing software whose aim will be to connect individual elements of the Internet of Things system;
- increased interest in the opportunities of deploying IoT solutions will generate demand for dedicated electronic and electromechanical component design and production services (sensors, actuators, consoles, autonomous mobile and desktop devices, etc.), and the number of such devices will exceed the number of desktop and portable computers currently in use.

Worldwide forecasts for the Internet of Things market



Source: IDC Futurescape: (Internet of Things, IoT), 2019

Prediction 1*: Over 50% of G2000 companies will have modernised and IoT enabled their industrial control systems by 2021 without addressing cybersecurity or public safety concerns, prompting regulators to legislate..

Prediction 2: By 2024, 50% of manufacturers will network related product and asset digital twins into digital twin ecosystems for a systems-level view of their business and 5% reduction in cost of quality.

Prediction 3: Despite supply chain complexity hindering innovation, 50% of manufacturers will have implemented predictive field services across connected assets to improve delivery speed and customer value by 2024.

Prediction 4: By 2020, the success rate of AI implementations in IoT will have reached 90%, with the major factor behind this success being collaboration between data scientist and engineering teams.

Prediction 5: By 2020, over 30% of IoT initiatives worldwide will fail to demonstrate a clear ROI, with organizations lacking the necessary KPIs to monitor progress from the early stages of such projects.

Prediction 6: With 40% of initial IoT data analysis occurring at the edge by 2022, organizations will invest more in gateways to aggregate and analyze edge data, especially in the context of IT, OT, and CT systems.

Prediction 7: In 2019, blockchain's limitations in processing vast numbers of IoT transactions in real time will limit IoT integration into blockchain and thus IoT-related spend to 5% of overall blockchain spend.

Prediction 8: By 2020, 70% of organizations will leverage commercial IoT platforms to develop and deploy IoT applications, and more than 50% will have multivendor IoT platform environments.

Prediction 9: By 2021, 45% of video surveillance content will be used to provide context to data from IoT endpoints in public safety scenarios and in transportation hub and campus monitoring, among others.

Prediction 10: By 2022, problems aggregating and rationalizing sensor data into actionable insight will have forced 20% of large manufacturers to insist on OEM data being reconciled in IoT data exchanges.

*Courtesy of:
IDC FutureScape: Worldwide IoT 2019 Predictions

Adoption of Digital Transformation in Poland

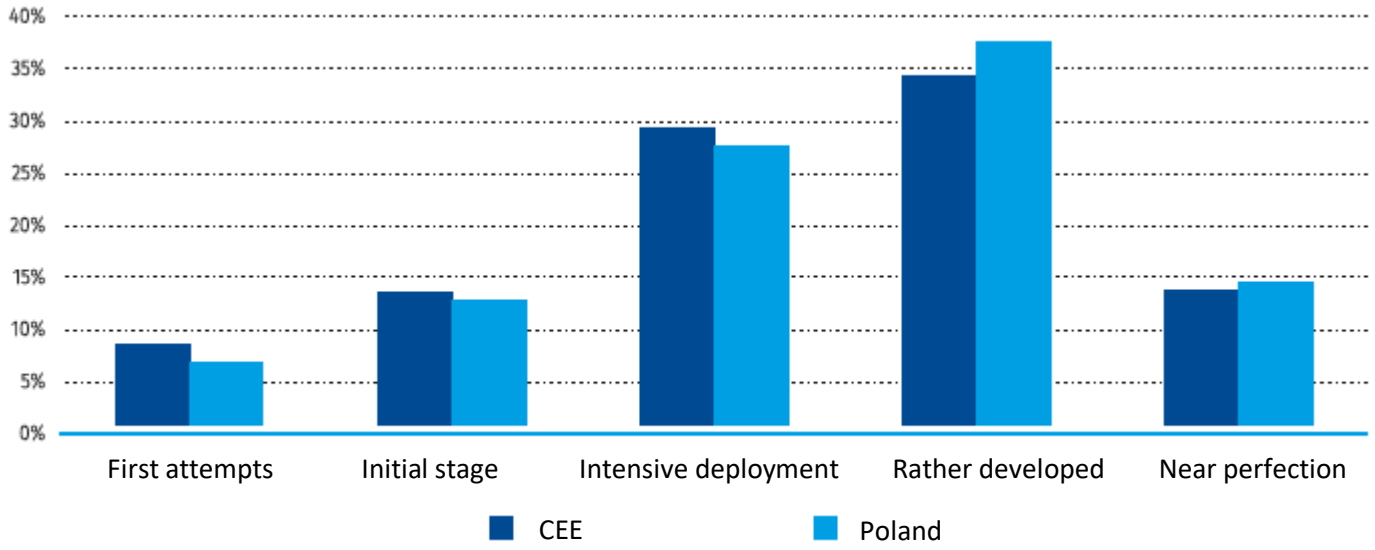
The openness of Polish organisations to digital transformation is conducive to ensuring the expected high level of IoT adoption in our market.

The study of the level of digital transformation adoption in Poland indicates that Polish organisations have confidence in these phenomena. In spite of the fact that the high level of their adoption in a *rather developed* phase may be potentially attributed to the respondents' willingness to be included in a technologically advanced group, this result can also be interpreted as a manifestation of Polish companies' aspirations and their interest in innovative digital solutions.

IoT constitutes one of the elements of the digital transformation process, and – what is more – it also serves as a basis for data processing and monetisation technology, machine learning, deep learning, as well as AI. In other words, there is a significant correlation between the willingness to adopt digital transformation processes and openness towards adopting IoT solutions.

In the coming years, the market for IoT technologies and solutions is expected to grow at a high rate (approx. 13% year on year). This means that the Polish economy has great chances of absorbing this technology – removing the pertinent obstacles may only increase this potential. Removing the existing barriers concerning regulatory issues and the development of new communication technologies (including **5G**) will result in the dynamic development of IoT in Poland.

Declared level of adoption of Digital Transformation solutions in Poland compared to Central and Eastern Europe



Source: IDC CEE Digital Transformation Survey, 2017; n=311

05

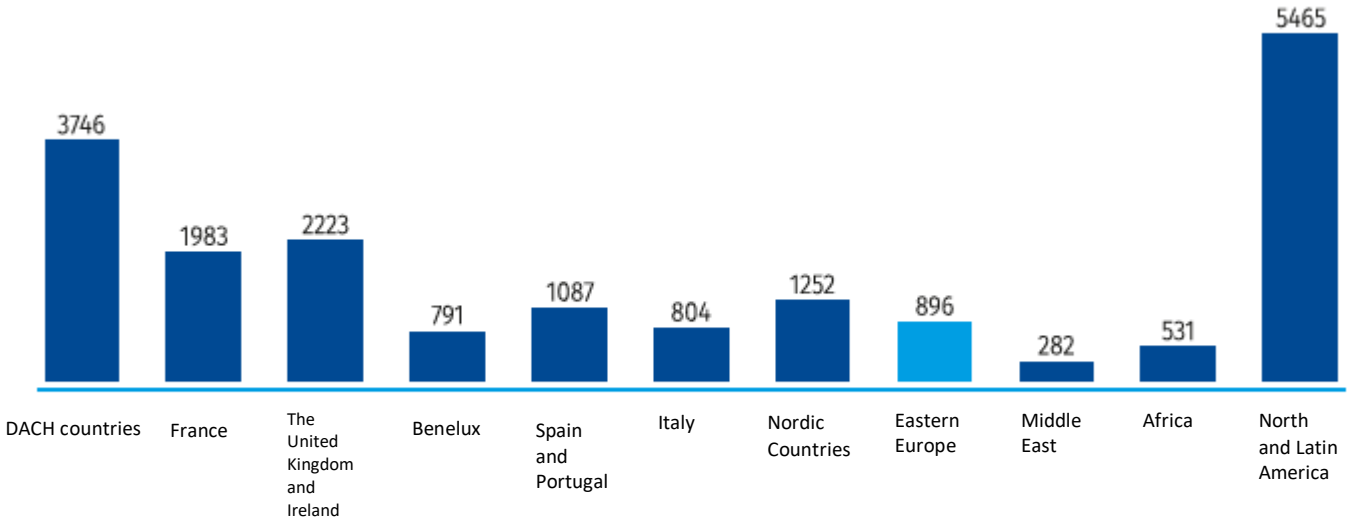
CONDITIONS FOR THE DEVELOPMENT OF THE IoT IN POLAND – DIAGNOSIS

The market for companies offering IoT solutions based on available statistics

There are numerous companies in Poland offering diverse IoT solutions tailored to the needs of various sectors of the economy; however, their overall number is still small, and the supply is not commensurate with the demand for Internet of Things solutions. Creating conditions that enable further growth of companies which strive to meet the needs of end consumers is crucial for the development of the IoT and economic growth in Poland. According to CompuBase[1] data, in terms of the number of companies offering IoT solutions, our region is trailing behind both Western European and North American countries, yet remains close to regions at a similar development level. More importantly, there are nearly 900 companies offering IoT solutions in Eastern Europe, the majority of which operate in Poland. Given that fact, there are enough of them to meet the growing demand for IoT solutions.

In terms of the segment in which the companies offering IoT solutions operate, the sector is dominated by companies espousing the **B2B** model, offering software for other companies, which make up 26% of all companies offering IoT solutions. Second to them are software development service providers, which make up 20% of all companies operating in this market. These two segments are the most relevant for IoT-related activities, which is why government action should focus on supporting companies that develop their own solutions or work on existing ones, thus growing the entire market.

The number of companies offering IoT solutions in particular markets



Source: CompuBase

1 http://en.compubase.net/Companies-working-with-IoT-related-skill-sets_a315.html

Companies offering IoT solutions by segment (based on global data)

Company type	Percentage
Manufacturer	7%
Software publisher	4%
Publisher of software for a specific activity	3%
Publisher of software for a specific process of companies	7%
Software solutions or services integrator (developed by third parties)	2%
IT services, software development	20%
Telecom services (e.g. Telecom operator, ISP…)	5%
Telecom & network infrastructure integrator	6%
IT infrastructure integrator	4%
Consulting	1%
Reselling to individuals	6%
Reselling to enterprises (hardware, software & services & assemblers)	26%
Wholesaler (resale of IT and Telecom products to resellers)	6%
Web agency	0%
Other IT and Telecom related activities	1%

Source: CompuBase

Market potential and main barriers from the perspective of the IoT solution category (qualitative analysis) To date, no universal model of the functioning of companies offering IoT solutions has been developed. Many companies run the entire processes – from the development of the product, through marketing, sales, and implementation, to maintenance and management – on their own. Some companies decide to focus on a part of a given project where they feel most competent, leaving the rest of the process to distributors. What is more, it is becoming increasingly easy to distinguish market segments corresponding to different levels of the definition of the Internet of Things:

1. Manufacturers of simple interactive devices controlled via the internet, dedicated for specific categories of applications (technology level):
   - beacons;
   - sensors;
   - webcams;
   - remote-controlled light sources, locks, etc.

   Examples of Polish manufacturers: AIUT, Estimote, Comarch, Action

2. Manufacturers of complex devices offering complex functionalities, generating data and/or controlled via the internet (technology level):
   - autonomous transport devices;
   - industrial robots;
   - mobile devices (smartphones, smartwatches, etc.);
   - smart and digital measuring devices.

   Examples of Polish manufacturers: CEIT/Asseco, AIUT, Atende, VersaBox, Flytronics/WB Electronics

3. Developers and operators of digital platforms and business services using Layer 1 and 2 devices (architectural and business level):
   - energy consumption optimisation;
   - smart transport;
   - urban transport systems;
   - smart parking systems;
   - **omnichannel** solutions.

   Examples: Virtual Power Plant, VersaBox, NextBike Poland, PROPARK, iTaxi

4. IoT solution integrators (business level):
   - traditional **integrators**;
   - companies implementing comprehensive smart building investments;
   - companies implementing complex measurement systems;
   - companies implementing comprehensive robotics solutions for production and logistics.

   Examples: Asseco Data Systems, Atende, AKE Robotics, AIUT

IoT market potential from a technological perspective

Electronic devices (listed under items 1 and 2 of the list) constitute the basis for every implementation, since they are what enables the "things" to process and transmit information. These devices can be complex systems, as well as fully-fledged computers found in robots and vehicles. They can also be simple, mass-produced sensors. In any case, the producers must ensure that they have appropriate computing power and communication interfaces for a given application, as well as an efficient power supply.

Technological capabilities for manufacturing basic electronic components and batteries are concentrated among a rather small group of international enterprises (such as Intel and Samsung). In addition, apart from technology, another crucial aspect is access to raw materials and their distribution. The manufacturing of electronic devices is a complex and technologically advanced process which requires state-of-the-art technologies. The simplest, passive components – capacitors, resistors and so on – are relatively cheap and easy to manufacture. Active components, including integrated circuits such as processors, are components whose production requires nanotechnology. The first 800 nm processors were manufactured in 1989, and currently we are on our way to developing 5 nm transistor technology, which is expected to hit the market in 2020.

For several years now, one of the elements most conducive to the development of the IoT has been the popularisation of so-called SOCs (System-on-a-Chip devices), which encompass the processor, random access memory, radios, analogue systems and flash memory in a single integrated circuit. This enables the production of a nearly feature-complete device characterised by tiny size and high functionality, with the only drawback being its poorer thermal performance.

There is considerable potential for manufacturers of devices built from numerous widely available and proven components. The production of application-specific IoT devices is fully possible in any plant with electronics assembly lines. So far, there has been a tendency to outsource manufacturing, mainly to Asian countries; however, this trend is gradually getting reversed due to the growing awareness of technology among companies and their desire to have their own production capacity. This is a very positive sign for local economies.

The electronics manufacturing market in Poland is considered mature and offers considerable potential, including in terms of purchasing power, which is very important to ensure timely deliveries in the case of large production volumes.

> The manufacturing process also hinges on the traceability of a single device from the moment of the introduction of components from specific suppliers to the production line, through assembly, quality checks, packaging, shipment and installation at the customer's site.

The quality of the devices and their durability is ensured not only by properly using components, as well as proper assembly and testing, but also by taking care of an appropriate production environment (ESD protection at every stage of production, as well as protection against pollution and contamination).

The key aspects concerning IoT devices are:

1. Using optimal components from the standpoint of:
   - power consumption;
   - size;
   - computing power;
   - reliability;
   - longevity;
   - resistance to extreme environmental conditions;
2. Ensuring certification.
3. Preparing appropriate design and making PCBs, which are used for installing electronic components.
4. Designing and building a case.
5. Power supply (long-life batteries, renewable energy).

IoT devices need to be characterised by a compromise between high computing power and low power consumption, since in many cases they need to rely on battery power. It is possible to use renewable energy sources such as photovoltaic cells, as well as conventional ones such as lithium-ion batteries. The life span of the batteries is also crucial, since it enables operation for years to come. Also particularly important is a feature in the device's firmware that informs the user that the battery needs to be replaced.

The market for IoT devices forces manufacturers to adapt them to different, often varying needs. As a result, they need to manufacture numerous versions of the same devices, using different power supplies or communication interfaces, including different antennas. Manufacturers' flexibility should manifest itself in quick prototyping and short time to market – the time between preparing the prototype and mass production of the device in question. This is also connected with the possibility of quickly and reliably installing software, as well as device certification. The increasing use of 3D printing for prototyping enclosures is becoming increasingly crucial in this respect.

SiDLY bracelets for seniors, which monitor their activity and vital signs.

Versabox autonomous mobile robot, part of the AUTONOMY@WORK internal logistics automation platform.

Companies which have the ability to manufacture their own devices and develop their own software become industry leaders, since they keep control over every aspect of the operation of their products – both the hardware and the entire ecosystem.

Given the above-mentioned conditions, the electronics industry in Poland is characterised by a large share of foreign capital, represented by worldwide companies, such as JabilCircuit, Royal Philips Electronic, LG, Samsung, and Motorola.

The consequence of this state of affairs is the fact that a large group of Polish enterprises serve the role of suppliers for global companies. Paradoxically, Polish companies are simultaneously their clients and customers when it comes to basic components. This translates into lower profitability of manufacturing in Polish plants, which is reflected by the fact that Poland's negative foreign trade balance when it comes to high-technology products amounted to 6.8 billion EUR in 2015, according to Eurostat's data, including 3.1 billion EUR spent on trade with other EU Member States.[2]

The requirements for modern electronics and electrotechnology continue to grow, in particular in terms of capabilities. This can be compared to a race in which all participants continue to increase the pace, breaking the limits and constantly setting new records. This concerns in particular the miniaturisation of components and finished products, while improving their performance and feature sets at the same time.
However, this sometimes leads to manufacturers not being able to meet the stringent requirements concerning their entire product ranges.

The market is driving the growing demands, which makes manufacturers have to look for new ways to meet them. One such models envisions taking advantage of outsourcing for individual components and entire electronic devices. Specialised companies which provide contract assembly services, such as Electronic Manufacturing Services - EMS, are usually well-equipped and have industry-specific know-how, which enables them to take advantage of the full scope of opportunities offered by specialisation and constantly adapt to changing market conditions. This also allows them to run technologically complex operations, including automated optical inspection, which enables them to check the quality of assembly of components on both sides of the PCB.

By using EMS services, companies selling electronic and electrical products under their own custom brand can focus on developing their core business. Another key benefit also entails the lower capital expenditure required to start production, as well as higher flexibility when it comes to adapting the product range to the needs of the market. The advantages of using outsourcing companies are particularly evident in the case of short and medium production runs.

According to the results of studies presented in the 2017 Electronics Market Guide, the needs of enterprises who decide to go with outsourcing services far exceed only the assembly process. The surveyed companies often point out purchasing components, testing and starting up the finished products, making PCBs and templates, as well as design services and technical support.[3]

2 A. Ostrowski: *Przemysł elektroniczny i elektrotechniczny w Polsce – raport*, 17.10.2017, published at: www.magazynprzemyslowy.pl/zarzadzanie-i-rynek/Przemysl-elektroniczny-i-elektrotechniczny-w-Polsce-raport,9970,1

EMS companies need to anticipate market changes by introducing new services to their respective offers, which requires them to respond to the unspecified needs of their clients. This is related to the need to anticipate potential risks which the manufacturers of electronic and electrical devices can face due to cost and technological limitations.

In Poland, the group of enterprises and companies offering EMS services features more than 100 entities of different sizes, offering various services and scales of operations.[4] Many electronics or electrical engineering manufacturers still manufacture their products in-house, using their own resources and production lines. They attach greater importance to maintaining control over the entire production process, protection of intellectual property, as well as the continuous development of the company's manufacturing potential. However, the ever-growing market pressure and the significant economic potential of the use of EMS services will be conducive to the future development of this segment.

Currently, Polish EMS companies focus on providing services to international clients, mainly from Western Europe and Nordic states. Their advantage stems from lower costs, qualified manufacturing staff, high level of technological development and geographical proximity; however, they face pressure resulting from the situation in the labour market, which will lead them to have to continuously improve the quality of their services.

The Internet of Things opens up new opportunities for Polish manufacturers, creating completely new classes of applications which enable innovative use of basic components and processing them into products for end customers. Given the expected high supply volume, the need for long-term operation of the devices, and the need to provide maintenance services along with spare parts, the IoT market will be particularly attractive to manufacturers of electronic devices.

In other words, building an appropriate supply chain of components for the manufacturing of devices becomes a critical issue. These days, the vast majority of IoT elements are produced as separate, independent devices fulfilling a specific function, working in certain specific environmental conditions, including availability of power and communication services, temperature and relative humidity. It is expected that in the near future we are going to see higher integration of the IoT with other commonly used devices, for example, both street and household lamps, road signs, cars, clothes and a number of other kinds of devices. This will result in the use of new materials, and cooperation between manufacturers.

For years, electronics production has been dominated by Asian countries, China chief among them. Large manufacturing plants in Asia can absorb nearly any number of electronic components, which disrupts global markets. From the point of view of the market structure, the difficulties with purchasing the components needed for the manufacturing of the end device are a significant concern. The cost of buying off-the-shelf elements is too high in view of the need to retain competitive advantage, and there are only a few brokers on the market where manufacturers can order basic components. This also affects lead times, in particular in the case of the most popular components such as SOCs and capacitors.

The manufacturing of electronic devices will be associated with continuous improvement of quality, increasingly short delivery times for new devices. and price competition, which will drive small players out of the market. Start-ups with good device designs will be forced to collaborate with larger players with real production capacities. This will require safeguarding their interests through appropriate patent proceedings. The customers for various applications, in particular the most popular ones, will expect to be able to lease the devices, along with full service and maintenance support.

Another key aspect concerning the IoT will be the use of state-of-the-art electronic equipment solutions. In the market, we can increasingly see the emerging need to use so-called high-tech electronics, including for example flexible PCBs, which enable the installation of sensors in clothing and other materials without the risk of them breaking.

Manufacturing new devices is also closely linked to the availability of more efficient power supply technologies. Work is underway on hydrogen microcells, graphene batteries and perovskites, which are an alternative to silicon solar cells.

Given the difficulties in supplying adequate batteries for the growing IoT market and other fields, Poland should invest in the raw material base and focus on cell manufacturing. As of now, there are already companies in Poland with the ability to purchase mining plots all over the world.

Apart from the market limitations mentioned above, the Working Group has also identified other significant barriers to the development of the electronics industry from the point of view of IoT solutions:

3 www.elektronikab2b.pl/download/Informator_Rynkowy_Elektroniki_2017.pdf
4 Ibid.

- Lack of specification of IoT solutions for public authorities, hindering the execution of contracts by the public sector. The problems with developing the so-called ToR (Terms of Reference) result from the lack of reference projects which would constitute an adequate **technological benchmark**.

- The need to provide restrictive warranty conditions in public procurement offers, which makes the manufacturer of the solution (including the supplier or integrator) virtually fully responsible for device failures. Therefore, only large companies that are able to bear the high costs of possible repairs and maintenance can apply for tenders. In the case of the IoT, the distances between the individual devices comprising the system can also become a significant problem, translating directly into high transport costs.

- High costs associated with the use of modern methods of building device cases. The so-called productization of devices is closely related to manufacturing device cases and housings. The needs of preparing prototypes are perfectly served by 3D printing, whereas serial production requires injection moulding, the cost of which is high, often exceeding the financial possibilities of smaller players in the market.

- Procedures and costs for testing devices for EMC (Electromagnetic Compatibility) and their certification.

- Growing pressure on Polish companies offering IoT solutions, pertaining to continuous improvement of quality, timely deliveries and ensuring interoperability, so that they are competitive against solutions available in international markets.

IoT market potential from an architectural and business perspective

For companies operating in categories 1 and 2 of the above market map, the main obstacle is the ability to develop "ecosystems of applications." The products offered by companies are merely one of the business components of IoT solutions – alone, they usually do not offer the value that the end customer could pay for.

Even consumer devices, including **smart home solutions**, gain value only when they are integrated into an ecosystem that meets the specific needs of the inhabitants of a home, without burdening them with the need to constantly interact with technology. On the other hand, the dynamics of the technology markets leads to the fact that investors these days are primarily attracted by products which give an opportunity for international implementation. The competence to create complex solutions, service ecosystems corresponding to points 3 and 4 of the market map above is mostly possessed by large IT companies, which have the ability to combine a product model with an integrator model, as well as telecom operators.

After several decades of dynamic **development of the IT market** based on local demand, which was satisfied by the integration of solutions offered by global technology companies, the Polish ICT market is undergoing intensive transformation, implementing product strategies and orienting itself towards international expansion. In this process, the key obstacle is the lack of natural dissemination channels in the form of an ecosystem of Polish companies with an international presence, seeking opportunities to modernise their offerings and expand the market based on innovation. Domestic demand is not strong enough for the transformation of the ICT sector to proceed at a rapid pace, and there is an apparent lack of experience in the internationalisation of Polish digital products and services.

From this point of view, the key issue is the support of public institutions for the internationalisation of the existing and growing market of Polish IoT products by means of:

- effective technological diplomacy, carried out in cooperation with the business community;

- support in activities related to the certification of IoT products in international markets;

- participation in the creation of cooperation networks with global entities investing in development centres working on their own IoT products and services in Poland;

- establishing a fund to secure the financial liquidity of companies manufacturing or implementing innovative electronic devices which constitute a staple of IoT systems. This fund would support smaller companies that have to deal with the relatively high risk of implementing IoT solutions (such as unpredicted costs of maintenance and modification of prototype devices);

- promoting cooperation between large companies and start-ups, which enables young and developing companies to carry out larger projects. The key to the growth of companies in the industry is the development of line production devices, which in turn requires obtaining large orders and significant investment in production capabilities;

- working out framework specifications for IoT solutions for potential implementations of IoT systems for the public sector, which will accelerate the procurement process for such systems and reduce their costs.

Demand barriers to the development of IoT companies in Poland

One crucial barrier that prevents many companies from implementing business solutions using IoT is the fear of innovation risks. Some market participants prefer to observe new trends rather than transform their business processes to take advantage of the IoT.

In the context of the IoT, the size of the company becomes particularly relevant. According to CompuBase data, 21% of companies from **the EMEA region** active in the IoT market employ more than 500 people. Additionally, the smaller the company, the less often it operates in this area.[5] Thus, it becomes important to support both large companies offering such solutions, as well as smaller players that have potential for growth and may become important providers of IoT solutions in the near future.

Costs may constitute a significant barrier that makes it difficult for smaller integrators to offer their own IoT solutions. In particular, this concerns purchasing the devices that make up the infrastructure of an IoT solution, which may amount to a considerable expense for both the integrator and the end customer, all while the services which enable establishing such infrastructures, such as low-energy **mesh networks** for smart agriculture, are still hardly accessible today. This can be an insurmountable barrier for smaller companies, which often cannot afford to invest a large part of their capital in the equipment needed to manufacture IoT systems. This leads to holding up the implementation of larger projects.

The so-called productisation of devices is closely related to manufacturing device cases and housings. Prototyping is perfectly served by 3D printing, whereas serial production requires injection moulding, the cost of which is high, often exceeding the financial possibilities of smaller players in the market.

Another key barrier concerns lack of competencies pertaining to IoT-related issues, such as legal aspects, including privacy. There are still too few experts in the market who can provide professional services in this area. In many cases, these companies are forced to operate under conditions of high business risk, or resort to slowly developing the competencies within the company. Many of them therefore abandon innovative projects, focusing on their core business.

From this point of view, it is crucial to build and deploy a funding mechanism for the deployment of innovative solutions in which financing innovation is ensured by supporting medium-sized and developing companies which are interested in pilot projects, and – in the case of their success – large-scale deployment of innovative solutions. This funding mechanism should encompass competence building on the part of the innovation-implementing organisation as a prerequisite for obtaining the financing.

Behavioural barriers can also play an important role in the development of systems based on the concept of the Internet of Things. They are linked to aspects such as consumer attitudes towards acceptance of specific IoT solutions or lack thereof, stemming from, for example, trust. It is also worth pointing out one more area which may be of key importance for the development of the Internet of Things, namely structural changes.

Regulatory environment

The regulatory environment in Poland is not only not conducive to the development of IoT systems. In reality, it constitutes a significant obstacle which stifles its growth. The Polish legal system lacks separate and detailed regulations for IoT technologies. Scattered over many legal acts (such as **GDPR**, telecommunication law and sectoral secrets, **NIS**), IoT regulations often give administrative or supervisory authorities the power to impose severe financial penalties.

Given the broad definition of personal data, a lot of the data collected by the devices within the IoT ecosystem may be subject to the restrictive rules of the GDPR. The lack of regulation for enterprises on access to or exchange of non-personal data is also a problem, since it limits the possibilities of using this type of data in IoT systems. The recently adopted Regulation of the European Parliament and of the Council (EU) on a framework for the free flow of non-personal data in the EU does not address the challenges of using anonymous data in IoT solutions. For a detailed description of regulatory barriers see chapter 17, page 102.

Education

In its current shape, the education system does not ensure a sufficient inflow of qualified staff specialised in IoT solutions. Only a couple of universities have decided to offer IoT courses, usually as post-graduate studies. At this scale, there is no chance of meeting the expected market demand.

Those interested in studying IoT solutions can take advantage of the following courses identified by the Working Group:

- WSB University – **Computer Networks and the Internet of Things** (post-graduate studies)
- University of Economics in cooperation with the Adam Mickiewicz University in Poznań – **Internet of Things Applications** (MA studies)
- University of Social Sciences – **Internet of Things** (post-graduate studies)

5 www.crn.pl/artykuly/raporty-i-analizy/internet-of-things-nisza-z-potencjalem?page=1

- WSG in Bydgoszcz – **Industrial Internet of Things**
  (MA studies)
- Poznań University of Technology – **Internet of Things**
  (major in the Computer Science course)
- AGH University of Science and Technology in Krakow – **IoT research group**
- Wrocław University of Technology – **Internet Engineering**
  (major in the Computer Science course)

Some support in this area can be provided in general IT and computer science courses (software development and hardware), as well as mathematics (analytical models, data collection and processing, artificial intelligence). However, in view of the dynamic development of the IoT-based economy in Poland, we are going to face a real issue – grave shortages of staff specialised in this field.

Ethics

In the absence of regulations governing the ethical use of IoT technologies and systems, their dynamic development raises a number of questions which we are unable to answer today. One of these dilemmas is the division of responsibilities for the results and outcomes of the operation of autonomous devices, for example the failure of an autonomous drone delivering a shipment, as a result of which its contents were destroyed and third parties were injured, between the owner of the device, the courier company, the developer of the control system, and the operator and creator of the air traffic coordination system. Another concerns the ownership of the data recorded by smart building equipment – do they belong to the tenant, the landlord, or the individuals concerned? For what purposes can the data be used by individual stakeholders? What level of reliability of a telemedicine device – for example an insulin dispenser – is required for its mass use in therapeutic settings?

Ethical issues need to be discussed prior to legal action. In addition, ethics touch upon the area of security, pointing out the potential risks associated with the use of IoT systems. In particular, the outcome of this debate will affect the following areas:

- minimising the data used by IoT devices;
- implementing voice commands (or other specific gestures used for activating the devices);
- the possibility of the user deleting data freely;
- data encryption;
- managing user identity.

06

STRATEGIC CONTEXT

Poland and Europe have long recognised the opportunities for economic growth based on IoT technologies.

The European Commission cooperates with industry, organisations and academia, implementing the *Digital Single Market Strategy* adopted in 2015. The strategy is implemented taking into account the assumptions adopted in the working document *Advancing the Internet of Things in Europe*, which constitutes a part of *Digitising European Industry*, and the *Liability for emerging digital technologies* vision.

Within the framework of the **Digital Single Market** the creation of Digital Innovation Hubs (**DIHs**) was identified as a priority task, enabling access to new technologies for small and medium-sized enterprises. These are listed in the European DIH catalogue, run by the European Commission and containing as many as 244 DIHs from all over Europe, including six Polish ones. Each of them takes into account the issues of the Internet of Things within the framework of their activities.

The European Union also supports the development of Internet technology by allocating R&D funding under the Horizon 2020 programme. Nearly €500 million earmarked for the programme in 2014 is slated to be fully distributed by 2021. The programme encompasses platforms for the cooperation of IoT devices and systems, such as Inter-IoT, VICINITY and BIG IoT.

The Commission's activity is also particularly apparent when it comes to promoting IoT development internationally. In January 2016 the *EU-China Joint White Paper on the Internet of Things*, a joint document describing several years of cooperation and initiating further steps in the field of research and innovation, with particular emphasis on policy making, technical requirements, international standards and information exchange within the framework of the common market, was signed in cooperation with the Ministry of Industry and Information Technology of the People's Republic of China.

In line with global trends, **Poland** is undertaking a number of initiatives aimed at developing the economy in the direction set by world leaders. This approach was articulated in a resolution of the Council of Ministers adopting the 2020 Responsible Development Strategy (with an outlook until 2030), which promotes a pro-innovation approach that will allow for added value. The Internet of Things is explicitly mentioned in it as an example of a digital technological revolution.

The Strategy points out a number of **National Smart Specialisations** (hereinafter: **NSS**), which are areas of focus, in which the competitiveness of the Polish economy should be built and elevated. The registry of such specialisations is managed and updated by the Ministry of Entrepreneurship and Technology, and the last update took place on 1 January 2019. Companies and solutions that fit in with smart specialisations can count on preferential access to **R&D&I support funds** for research, development and innovation. IoT technologies can be found in several smart specialisations, including:

- **NSS 1.** Healthy society – in terms of **telemedicine** and health monitoring using devices, sensors and accessories;
- **NSS 2.** Innovative technologies, processes and products in the agri-food, forestry and timber sectors – for remote sensing, **Life Cycle Assessments**, as well as the implementation of modern monitoring and early warning systems;
- **NSS 4.** High-performance, low-carbon and integrated energy generation, storage, transmission and distribution systems, used for the development of smart grids;
- **NSS 9.** Sensors (including biosensors) and smart sensor networks, encompassing the construction and development of sensor networks based in particular on **M2M communication**;
- **NSS 11.** Printed, organic and flexible electronics for smart object printing.

The First Speed Programmes provided for in the Strategy include the elimination of obstacles to development, including legislative, organisational and institutional ones, including those identified within the scope of this report by the Working Group for the Internet of Things.

The national strategy in the area of support for IoT-based innovation also takes into account regulations concerning the processing of personal and non-personal data, and the potential for using machine data generated largely by the users themselves. In the age of new technologies, the value of data cannot be overestimated, but its wide availability must be accompanied by high security standards. Only by ensuring that these two elements go hand in hand will it be possible to enable the full development of the economic potential without harming individuals' right to privacy and the intellectual value of businesses.

The government is well-aware of the fact that the real growth potential of the state depends on a holistic approach to the development of new technologies, which may complement, improve and work together with other state-of-the-art technologies, such as **artificial intelligence**, **blockchain** solutions based on **cloud computing**, as well as 5G networking.

The foundations for the dynamic development of the Internet Things are laid by numerous programmes, such as the 5G Strategy for Poland proposed by the Ministry of Digital Affairs or the activity of the Working Group for the Artificial Intelligence. These technologies can function independently, but it is only when they are interconnected into larger systems and economic organisms that they demonstrate their potential to contribute both to the comfort of the citizens and the value of the business sector.

No less important is establishment of legal forms of running businesses conducive to innovation. To this end, some projects have been undertaken to create a new type of company – Simple Joint Stock Company, which is a private company, with reduced capital requirements, characterised by simplified incorporation and liquidation procedures. This is a solution dedicated **to startups**, in particular those operating in the innovative technologies sector. By detaching the value of the shares from the company's share capital, the shareholders enriching the entity with intellectual resources will be able to counterbalance the shareholders contributing capital in the form of a cash contribution or in-kind contribution with their votes.

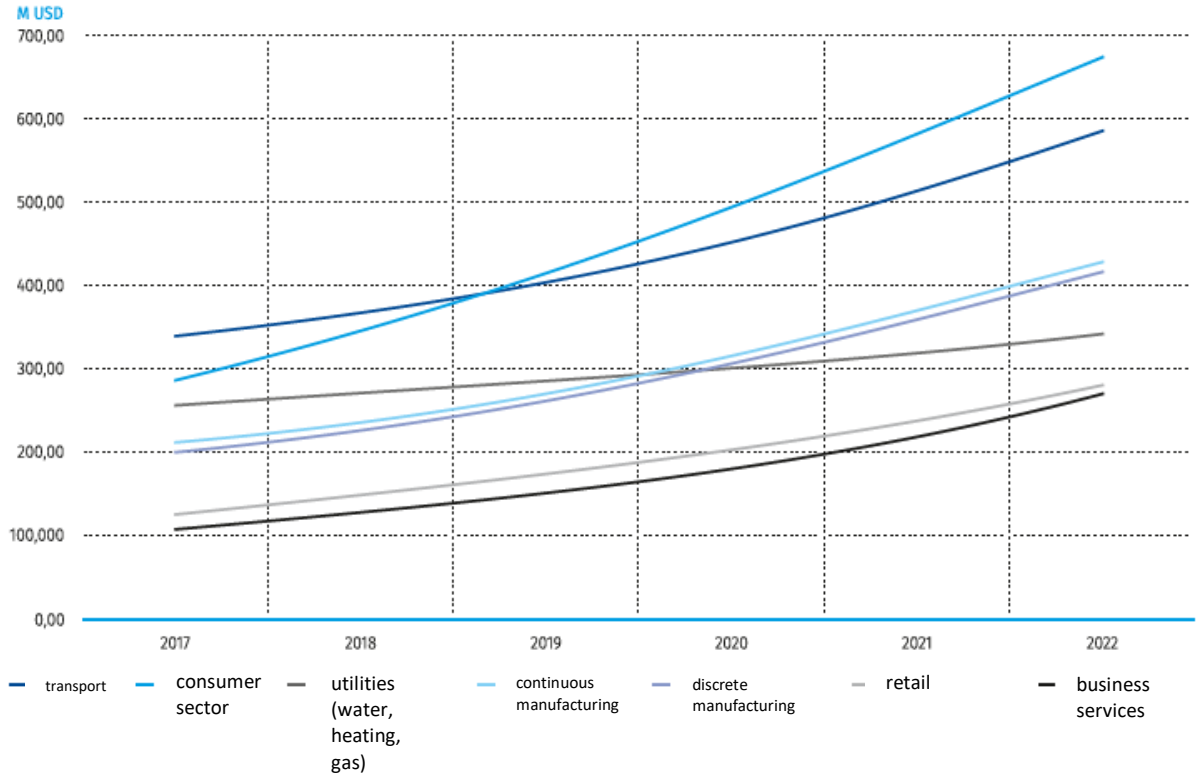
07

SECTORS WITH PARTICULAR POTENTIAL FOR IoT-BASED DEVELOPMENT IN POLAND

IoT technology is horizontal in nature. This means that it can be used in many different sectors and across various business solutions. In addition, within each industry IoT systems can be found at different stages of the supply chain, creating an ecosystem of solutions that permeates the various market segments. However, some industries will be much more dependent on IoT systems, and they should be the main focus of activities supporting the development of the IoT market.

According to global market data, the leaders in growth and spending volumes in the IoT area are: the consumer market, logistics and transport sectors, as well as industry. Of all the industries that invest the most in IoT solutions, only the commercial sector has not yet taken up the challenge of the broad adoption of IoT systems, despite being ranked 6th in terms of IoT-related spending. This phenomenon is probably related to the lack of sufficiently convincing scenarios for monetising these investments.

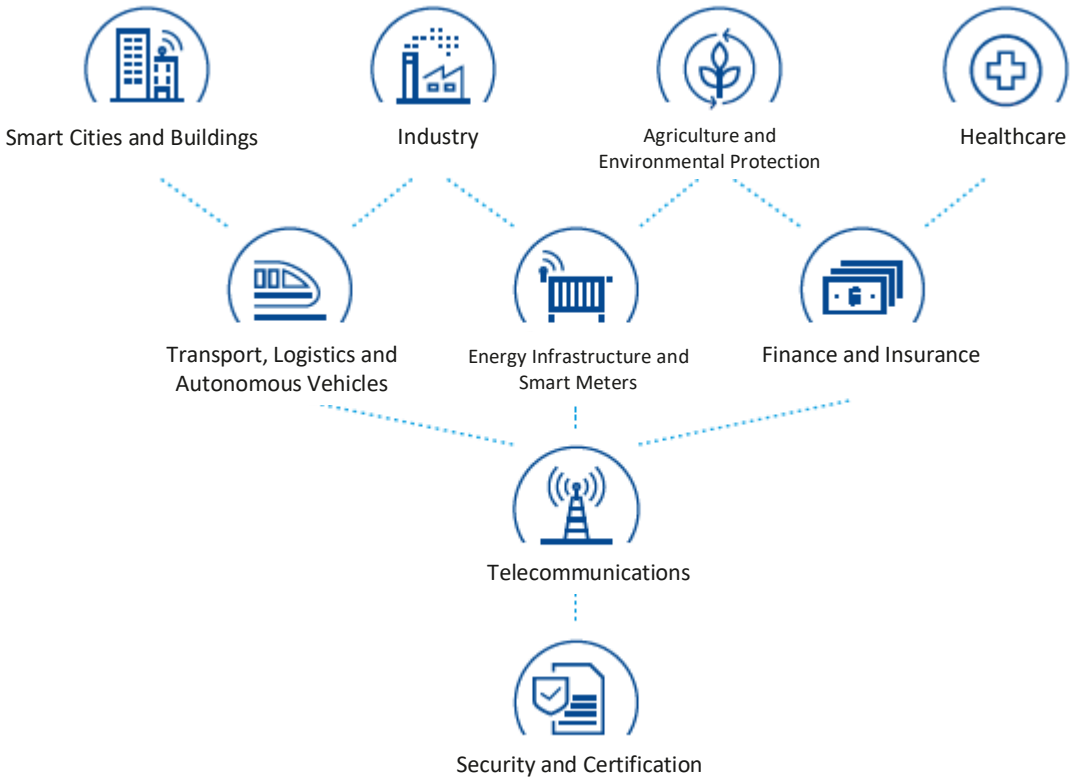
IoT spending by industry



Source: IDC Worldwide Semi-annual, Internet of Things spending by industry, June 2018

Sector	2017	2018	2019	2020	2021	2022
consumer sector	287.82	345.15	412.49	492.50	581.47	677.56
transport	338.89	367.43	404.24	450.29	511.36	585.19
continuous manufacturing	208.53	234.85	270.34	313.94	366.55	428.96
utilities	258.37	269.87	284.29	301.29	320.80	343.64
discrete manufacturing	196.39	224.62	260.48	307.40	356.96	421.32
retail	126.51	146.98	173.14	201.85	237.06	278.99
business services	106.59	124.35	149.93	178.61	214.96	269.67
national/local authorities	72.77	81.56	91.63	104.31	119.92	140.02
public services	56.20	64.91	77.35	95.89	118.25	149.62
wholesale sales	56.10	64.31	77.31	92.78	108.58	127.19
federal/central authorities	58.02	66.05	76.87	89.34	101.70	118.30
healthcare	62.24	66.79	73.24	80.48	90.66	104.90
education	29.81	34.97	43.76	54.12	65.10	77.55
construction	31.78	35.80	41.02	48.50	56.55	65.93
telecommunications	28.07	31.89	36.94	43.24	49.95	57.90
media	26.38	29.93	34.81	42.07	49.54	58.62
mining	17.04	19.69	22.80	26.58	31.09	36.36
Insurance	8.65	10.60	13.33	17.43	22.13	28.44
securities and investment services	6.56	7.21	8.19	9.24	10.72	12.33
banking	3.44	4.16	5.04	5.93	7.05	8.14
Total	**1980.14**	**2231.10**	**2557.18**	**2955.78**	**3420.39**	**3991.66**

Based on the trends described above, and taking the structure of the Polish economy into account, the Working Group has selected nine key industries in terms of the volume of benefits resulting from the opportunities for employing IoT in Poland. These are:



08

SECURITY AND CERTIFICATION

An IoT with no regard towards cybersecurity poses a greater threat to the state than abandoning the use of an IoT altogether.

AUTHORS:
ALEKSANDER P. CZARNOWSKI, AVET INFORMATION AND NETWORK SECURITY – SUBGROUP LEADER
ANDRZEJ KARPIŃSKI, ORANGE POLSKA KONRAD KOWALCZUK, MGK.NET.PL
ANDRZEJ PIOTROWSKI, UTC FIRE & SECURITY POLSKA RAFAŁ RADAWIEC, WROCŁAW UNIVERSITY OF TECHNOLOGY
MARIOLA WIĘCKOWSKA, LEXDIGITAL

General characteristics

Due to the widespread use of the IoT and the mass processing of data of economic and national defence importance, the IoT simply cannot exist without cybersecurity. The lack of adequate legal and certification regulations will lead to Poland losing an important part of its competitive edge in various contexts – economic, protection of citizens, and innovation.

Innovation and dynamic technological development, globalisation and the ever-shorter time-to-market mean that manufacturers, importers and retailers of IoT products face a number of challenges. These include both strict market requirements concerning the reliability and performance of the products, as well as changing regulations, which contribute to the increasing feeling of pressure.

In order to change consumer behaviour, one must pay particular attention to existing regulations and the requirements rooted in them, as well as presenting the relationship between product certification and its safety criteria. This way, anywhere in the world, the buyer of the solution is aware that their rights are protected and that all the regulations are followed. Certification is the most reliable way to asure a buyer that the purchased products and services conform to the relevant standards.

Security is a critical element of product quality. The level of safety is difficult to assess in a simple way, which is why it is necessary to develop standards and best practices in this area. The above elements need to be compatible with already existing international and European standards, and at the same time they need to ensure the protection of Polish interests. On the other hand, over-regulation can stifle innovation and dangerously increase the barrier to entry for new solutions, which might result in negative economic effects on domestic enterprises in the long term. Security should be seen as a fundamental building block of the IoT world. Without meeting the security requirements, and without the use of standards and best practices, the IoT world itself poses more of a threat than abandoning IoT technologies ever would. Security is therefore a prerequisite for the development of IoT solutions. However, without adequate IoT product certification, a proper level of security simply cannot be ensured.

Security in IoT systems can be further divided into several subcategories, including:

- **product safety**, taking into account aspects such as hygiene, toxicity, functionality, ergonomics, etc., standards which guarantee safe use of the product;
- **product cybersecurity**, which means proper product manufacturing, and equipping it with tools and mechanisms that enable counteracting ICT threats;
- **data security**, which concerns the security of data processed by the product or the ecosystem, both personal and technical (including **telemetry** and non-personal data);
- **physical safety**, which concerns the impact of the IoT technology and its application on the physical world – direct impact and influence of the IoT world on the daily life of citizens, for example door lock functions, autonomous vehicle turning, flow control in waterworks, as well as correct functioning of a telemedicine device such as a pacemaker;
- **legal and regulatory security**, which refers to the compliance of IoT devices with legal standards concerning the admissibility of their processing certain information;
- **national and military security**, which concerns potential opportunities to use the IoT infrastructure for, among other things, spying by collecting information, unauthorised use of metadata, causing intentional breakdowns of important critical infrastructure elements or a large-scale failure, the possibility of using IoT tools as a direct tool for attack or to cause a disaster (for example a drone or **an autonomous vehicle**).

Certification for IoT solutions should concern:

- Confirmation that the appliance complies with national and international standards within a scope typical of any given class/category of equipment – this entails certification by the Institute of Mother and Child for children's products, certification concerning energy standards, acceptable noise level, pollutants, type of material used, operating temperature range, etc.
- Identification of the quality class of the equipment, which is established by determining the accuracy of measurement or precision of operation, the conditions under which the parameters will be maintained and the time for which it can be assumed that the measured parameters will be maintained. This is important, since the expected precision directly depends on the specific application, and users must have access to precise information concerning the class of the devices they are working with. These classes should be standardised – it would be advisable to establish a set catalogue of IoT device parameters with accuracy classes, as in the case of electronic components (for example 10 Ohm with an accuracy of 10%, guaranteed for 10 years, provided that it is used at X-Y temperature range).
- Certification of the communication elements for compliance with generally accepted IoT communication standards – degree of fulfilment of protocol definitions, **application programming interfaces** *(API)*, etc.

- Cybersecurity certification – at the moment, there is no single internationally adopted standard for IoT. ENISA reports and the Common Criteria are the two documents which are the closest to such a standard in terms of their content. Work on a certification laboratory based on Common Criteria in Poland is currently underway.

It seems necessary to establish a national certification body or to entrust tasks pertaining to certification to an existing institution/laboratory. At the same time, the accreditation and certification mechanisms need to be compatible with the mechanism established by the GDPR. The Working Group sees considerable business potential in the existence of an efficient national certification body supporting the domestic market of IoT manufacturers and Poland's participation in establishing international standards, as well as offering the opportunities to carry out commercial testing by a national certification body, instead of certifying equipment outside the country.

Benefits of certification for industry:

- certification is a marketing and sales tool that opens up local and international markets. Additionally, a certification scheme that complies with international standards ensures that local certification will be accepted globally;
- certification is an essential tool in decision making and risk management. Organisations can save time and money by choosing certification schemes to ensure that their product can be recognised in order to comply with international standards;
- certification ensures precise measurements and tests carried out in accordance with best practices, reduces the number of defective products, reduces production and inspection costs, and enables the implementation of innovative solutions (in this respect, certification can make the time-to-market of innovative solutions longer);
- certification reduces risk in business relationships;
- certification allows for curbing low quality products which are designed to resemble products made by top manufacturers, and reduces the number of counterfeits.

Benefits of certification for consumers:

- certification enables reliable and precise results of analyses and studies concerning areas related to safety, health and the environment (such as medical analyses, mechanical research, chemical research);
- certification bodies provide reliable information which can facilitate decision making, in particular in areas such as cybersecurity and environmental protection (**RoHS**, CE certificate);
- certification contributes to the elimination of barriers to trade through mutual recognition of conformity assessment procedures (free international trade is a stimulus for economic growth).

Benefits of certification for Poland:

- certification provides an opportunity to support the national market;
- certification opens up opportunities for advancement to the position of a global player in a given market;
- certification guarantees the safety of products and ecosystems from the point of view of individual and mass events.

Growth prospects for the industry

The amount of autonomous traffic generated by the IoT on the internet is expected to exceed the amount of traffic directly generated by users in the coming years. In some categories this phenomenon has already occurred – one example is e-mail, where nearly 90% of messages sent via the internet are generated automatically. Such rapid growth of the amount of traffic and the number of devices connected to the internet will translate directly into new kinds of security risks, occurring on an unprecedented scale. Even these days, the largest networks (**botnets** – networks consisting of multiple malware-infested computers) which are used for successful attacks on other systems, and sometimes entire countries, are based on IoT devices.

The Internet of Things is a trend that manufacturers cannot ignore. The IoT is expected to connect up to 28 billion devices by 2020. More and more often, new devices are connected to the internet, and as such they are turning into elements of IoT systems – from smart TVs, **digital assistants**, smart toys, **fitness trackers**, smart home appliances, up to comprehensive smart home solutions. This of course offers many benefits – more convenience, more safety and lower energy consumption. Consumers are willing to pay for the convenience of connected devices that can improve their way of working and quality of life.

In the case of IoT devices intended for use near the human body, such as wearables, **SAR tests** and tests for compliance with **IEEE/FCC requirements** are also required. In spite of the fact that interoperability is mostly invisible to the end user, it is important that manufacturers make sure that their IoT device can communicate seamlessly with other devices. Each manufacturer should ask themselves whether their IoT product or service complies with the stringent requirements of data protection and data security legislation, and take into account consumers' privacy expectations.

The Polish Centre for Accreditation is a national accreditation body authorised to accredit certification bodies (assessing conformity) based on international and Polish standards. Poland has 50 accredited research units.

Below, you can find an example of a list of attributes that can be used to create a regulation for consistent certification for different IoT devices.

Example IoT classification

1 IOT AS A SYSTEM OF DEVICES
- 1.1 Auto-configuration
- 1.2 Management of components and functions Operations
- 1.3 Distributed System
- 1.4 Network Connection between devices
- 1.5 Equipment and access management
- 1.6 Synchronisation of activities
- 1.7 Quality (protocols/standards)
- 1.8 *Licences/Subscriptions/Operating model

2 IOT AS A SERVICE SYSTEM
- 2.1 Service description according to documentation (Content-Awareness)
- 2.2 Service operation according to the scheme (Context-Awareness)
- 2.3 Accessibility (as an ISO 27001 attribute)

3 IOT AS A COMPONENT
- 3.1 Compliance with conventions
- 3.2 Traceability
- 3.3 Modularity
- 3.4 Network access
- 3.5 Accessibility
- 3.6 Unique number/name

4 COMPATIBILITY
- 4.1 Technical support
- 4.2 Backwards compatibility

5 USEFULNESS
- 5.1 Ease of use (compliant with standards)
- 5.2 System

6 SPECIALISED
- 6.1 Accuracy (for measuring equipment)
- 6.2 Durability (concerning operational limits)
- 6.3 Lifespan (for battery-powered devices/ sensors)

7 SECURITY
- 7.1 Accessibility
- 7.2 Confidentiality
- 7.3 Integrity
- 7.4 Security (penetration/fuzz testing)

8 INFORMATION SECURITY MANAGEMENT
- 8.1 GDPR
- 8.2 PSD2 / NIS
- 8.3 National legislation
- 8.4 Other legislation

9 OTHER ATRIBUTES
- 9.1 Credibility
- 9.2 Writability and readability in other systems and diversity of data use (legal aspects)
- 9.3 Compliance with EU legislation

Source: The Singapore Economic Development Board, IoT Proposal Draft, 2017

Prospects for the use of IoT solutions

Ensuring safety by applying appropriate norms, standards and certification is certainly possible, but requires raising awareness among the general public and promoting knowledge about the use of IoT solutions. The spheres of social and economic life that offer the greatest potential for value creation through the use of the concept of the Internet of Things include:[1]

- people,
- living spaces,
- retail,
- offices,
- factories,
- work/construction sites (such as oil extraction sites),
- vehicles;
- cities;
- external areas – areas between urbanised environments.

At the same time, the potential economic impact of the Internet of Things will vary greatly, depending on the sphere of influence in question. According to McKinsey's projections, by 2025 the largest impact of the IoT will be apparent in the factory sphere ($1.2-3.7 trillion), while the office sphere will see the smallest impact ($70-150 billion).[2] In this context, it should also be noted that only around 10% of the financial value derived by organisations from the Internet of Things will come from "things" themselves – the remainder will be based on the way the devices are connected to the Internet and their purposes.[3] Therefore, the way the countries and organisations are going to establish their IoT ecosystems is a particularly crucial aspect.

Barriers

In the course of its work, the Working Group has identified the following barriers for the industry:

An apparent lack of a national IoT certification scheme with an accreditation scheme for national certification bodies compatible with the Common Criteria and mechanism of accredited codes of conduct described in section 5 (Codes of conduct and certification) of the GDPR, in particular Articles 40, 41, 42 and 43.

Lack of regard for the IoT phenomenon in legislation concerning safety and security, in particular in the Telecommunications Law and the National Cybersecurity System Act; lack of definition of the IoT as a market by the Office for Electronic Communication;

- Lack of clear legislative solutions to regulate and address various issues concerning the IoT and cybersecurity;
- Issues with ensuring interoperability, openness and accessibility.

As early and relatively simple implementations in the IoT area show, the scale of potential problems related to these issues can be significant.[4]

When it comes to interoperability issues, according to the McKinsey consulting firm, this is a critical aspect for the future and development of IoT systems. This aspect requires the development of open standards in all areas and at all levels to enable smooth and seamless interoperability and communication between devices delivered by different suppliers and building IoT ecosystems based on such devices.

According to McKinsey's assessments, at least 40% of the potential benefits of the Internet of Things will not be realised without interoperability.[5] At the same time, a number of non-technical challenges can be easily pointed out. Since in the case of IoT systems the majority of the value is derived from the collected, transmitted, processed and analysed data,[6] data-related issues are one of the key aspects that can become barriers to the development of this concept, as well as foster its development.

At the same time, barriers and challenges which can turn into stimuli can be found at various levels, including:

- global – global price trends for IoT infrastructure components, global standards;
- regional – EU standards and regulations on various aspects of the Internet of Things;
- national – regulations and standards in individual countries' markets;
- sectoral – sector-specific regulations and standards.

1 McKinsey Global Institute, The Internet of Things: Mapping the value beyond the hype, https://www.mckinsey.com/business-functions/digital- mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
2 Ibid.
3 Bauer et al. 2015, McKinsey 2014
4 cf. Blaich 2016
5 McKinsey 2015
6 Heppelmann, Porter 2014, p. 64-88.

Proposals for government action

Security is a key element of the IoT ecosystem, which is why the right tools for ensuring, evaluating and certifying security are essential. The tools must be based on appropriate legislation, as well as conform to standards and best practices. Interoperability is a key requirement not only for managing cybersecurity, but also for other business applications. Therefore, we recommend taking the following actions:

- Establishing a common glossary of IoT terms which will be used throughout the legislation, as well as in standards, best practices and educational materials. This will reduce the existing uncertainty about the specific language used in the documents and speed up the standardisation of IoT systems.
- Developing standards regarding cybersecurity, interoperability and standardisation, as well as corresponding certification methods. The standards must be adapted to market needs. Different certification thresholds should be introduced, depending on the life expectancy and applications of IoT solutions.
- The need to prepare the legal system for the emergence of the IoT ecosystem, taking into account such aspects as: The National Cybersecurity System, GDPR, Telecommunications Law, PSD2 and ePrivacy.
- It is necessary to introduce clear regulations concerning the right to use the collected data and their storage.
- A certain consideration should be given to aspects pertaining to the processing of non-personal data and related metadata (telemetry and related trends, insight into the events described by telemetry data), as well as the possibility of linking them with personal data.
- Considering security in a holistic manner in the course of the activities – it is not enough to secure endpoints or to provide global surveillance tools alone. IoT ecosystems should be built in line with the security-by-design principle – security should be an integral part of the design, in accordance with Article 25 of GDPR, as well as security-in-depth, which means that security should be adequate to the role of the device, and each threat should have more than one safeguard against it. Another important aspect concerns raising awareness among users themselves.
- Making manufacturers and integrators of equipment and IoT systems responsible for ensuring security and defining liability in case of product recall, bankruptcy, or closure of the manufacturer.
- Establishment of national certification bodies. The three types of certification recognised by law are associated with high costs and long waiting times. This is a challenge and a barrier stifling startup development, hence it is necessary to change the approach set out in the European Common Criteria to a more flexible one that would not lead to the risk of losing a certificate if the solution is improved.

09

FINANCE AND INSURANCE

For the financial and insurance sectors, ensuring permanent access to IoT data streams is one of the key challenges. Our response to this challenge will determine failure or success in business.

AUTHORS:
MARCIN WOLSKI, BILLON GROUP STARTUP – SUBGROUP LEADER
PIOTR JAN BROZOWSKI, NATIONAL CHAMBER OF TAX ADVISERS
TOMASZ KLUWAK, NATIONAL CHAMBER OF TAX ADVISERS
PRZEMYSŁAW KRZYWANIA, BKF MYJNIE BEZDOTYKOWE
MARIUSZ KUNA, POLISH CHAMBER OF INSURANCE
MICHAŁ KWIECIŃSKI, PLATFORMA DETALISTÓW
MACIEJ LECIJEWSKI, REGENT INSURANCE BROKERS (POLAND)

General characteristics of the sector

The financial and insurance sector is represented by entities providing payment services, insurance companies, payment institutions and companies providing banking services.

The financial sector recognised the potential of the IoT relatively recently with the emergence of commercial solutions based on collecting information from data sensors.

The processes in the financial and insurance sector are based on data and their relations. The analysis of data sets allows forecasting risks and helps with estimating financial implications.

While considering the topic of the IoT in the context of finance and insurance, it is important to remember that collecting and transmitting data will practically always be linked with service payments. This means that the element of payments, micro-payments and taxation of such activities should be included in the national IoT strategy.

It will become an integral part of IoT services and should therefore be regarded as a mandatory element in the design of all kinds of products and services.

The regulatory area is an indispensable aspect which conditions the state of the industry. However, it has undergone significant changes in recent years. One of the most important legal acts for companies from the financial and insurance sector operating in the European Union is the **PSD2 Directive**, which opens up new opportunities for IoT devices.

Growth prospects for the industry

The IoT is seen as an opportunity for the insurance industry and the customers of insurance companies.

Insurers forecast that new data types and their high availability may significantly change the landscape of insurance services and products from the perspective of both the insurers themselves and their customers. The IoT opens a new way of looking at these data.

In the insurance sector, the IoT will primarily concern property insurance.

The sensors will allow companies to control the condition and changes taking place in the insured items, as a result of which:

- the catalogue of insurable items will be extended. This will make it possible to insure items and their elements which cannot be covered by insurance due to the lack of mechanisms enabling verification of information about their condition and risks. The idea of measuring various elements of everyday objects creates an opportunity to offer insurance for new products, such as bicycles and electric vehicle insurance;
- the information concerning the insured items will be more organised, as the data will come directly from the insured item, not as a result of processing and classification by another party;
- the precision of estimating the probability of events and the risks they generate will increase, based on a constantly growing number of measurements;
- it will be possible to offer new products and services, developed on the basis of data obtained from new sources. IoT data will allow for the introduction of proactive actions after the event has occurred. The Working Group assumes that thanks to sensor data, insurance companies will be able to react in real time to events recorded by the sensors, for example by sending roadside assistance in the event of a vehicle malfunction or a plumber in the event of an increase in floor humidity in rooms;
- settlement of damages will become easier and simpler, as the policyholder will not have to report anything. By analysing the data, the insurance company will be able to deduce, based on the changes in data received, that the insured event – car crash, flooding, fire, etc. has actually occurred;
- IoT data will help counteract insurance fraud, thanks to comparing actual data with data received from the policyholder.

CASHLESS MOBILE PARKING WITH A LICENCE PLATE RECOGNITION SYSTEM

HTTPS://WWW.MONTERAIL.COM/BLOG/PARKING-SYSTEM-SOFTWARE-ADMYT

AUSTRIA / POLAND

PROBLEM

Parking a car in privately owned car parks, such as in shopping malls, requires paying a fee at automated ticket booths based on data recorded on a ticket printed out earlier. This causes a number of gripes and inconveniences, including cases where the driver loses their ticket, waiting in lines at ticket booths, or having to pay in cash.

SOLUTION

The admyt mobile application gives users the ability to park without the aforementioned hassles. A convenient registration process allows drivers to link their account to the car's licence plate number, while cameras placed at the entrance to the car park scan the oncoming vehicle and open the gates, thus starting the parking time countdown. The application keeps the user informed about the billed amount. When leaving the car park, the fee is charged directly to the account, while the parking summary together with the bill appears in the application. Currently, the solution has been implemented in 14 shopping malls in South Africa. Planned deployments include the Pasaż Grunwaldzki shopping mall in Wrocław (launch date: 03/04.2019).

BENEFITS

User-oriented registration process, reliable and secure payment system.

Scope of possible use of IoT solutions

The coming years will bring considerably more changes in the way people conduct transactions than the last few decades. IoT technology will require far-reaching changes in the attitudes of customers and partners towards information sharing. The customer experience changes will result mainly from payment security measures (**biometrics and tokenisation**). Installing sensors in various products and everyday use objects will directly and indirectly affect the provision of insurance, payment and financial services.

IoT technology will be an opportunity for the financial, insurance and payment industry to introduce completely new products and services based on data received from sensors and their subsequent analysis. Modern payment solutions will allow the introduction of new fares and new methods of managing public transit vehicle fleets, while reducing the costs of infrastructure used for managing ticket sales.

More than 20 billion **connected devices** by 2020 will lead to an enormous increase in the number of places where secure trading can take place. Payments are becoming increasingly invisible, taking place in the background, making it easier for consumers to use online and F2F services (such as Netflix and Uber). The tokenisation of devices will allow for an increase in the range of payment tools and a potential increase in transactionality.

TELEMATICS IN MOTOR INSURANCE

HTTPS://PAYHOWYUDRIVE.PL/
POLAND

PROBLEM

Currently, the valuation of civil liability or accidental damage insurance is based on static elements (such as age, car make and model), and it does not depend on the driver's behaviour on the road. The algorithm does not take into account people who drive safely but belong to a group deemed to be more of a risk, for example young drivers. In addition, reckless drivers may be included in a lower risk group, and as a result the contribution amount is determined in an inadequate and unfair manner.

SOLUTION

YU! is an offer developed by Yanosik and ERGO Hestia based on a solution that makes the insurance price dependent on the driver's driving style. YU! It's the first universal Pay-How-You-Drive offer. YU! offers Yanosik users an insurance price based on a risk assessment which is conducted on the basis of a safety analysis concerning the driver's driving style. The solution takes into consideration things like dynamic driving, behaviour in dangerous places, and compliance with traffic laws. Drivers can build their driving record by driving with the Yanosik application. Thanks to the app, their smartphone turns into a device that records their driving parameters.

BENEFITS

The purpose of YU!'s insurance offer is to recognise drivers who drive safely. Thanks to the Yanosik mobile application, they can get the cheapest liability, accident, and assistance insurance offers. Safe drivers will be able to take advantage of customised offers.

The Government of the Republic of Poland and its subordinate public institutions (including the National Treasury Administration, the Ministry of Finance, the Ministry of Entrepreneurship and Technology, and the Central Office of Measures) are planning to replace nearly 2 million cash registers which could potentially become IoT-class devices. Taking advantage of the IoT can foster the implementation of the so-called online fiscalisation concept.

The financial and insurance sectors plan to use the IoT to:

- automate and improve their existing processes and services;
- build and offer their customers completely new product and service categories;
- minimise and optimise risks stemming from their ongoing processes (for example by monitoring the status and parameters of the insured items, as well as identifying and responding to the risks in order to limit the consequences of their occurrence);
- increase integration of services and settlements in B2B and B2C relations;
- automate loss adjustment processes and claims payments in the insurance sector;
- increase the integration of services and settlements in B2B and B2C relations;

- integrate IoT-based services (sensor status changes) with microtransactions and tax services.

Barriers

In the course of the work, the sub-group identified the following barriers for the industry:

- Lack of sufficient competencies and capacity to exploit the potential of IoT technologies in the sector.
- Reluctance and concerns of customers and business partners to share data on how they use everyday-use items and products, where the insurance industry sees great potential.
- Lack of clear, precise regulations on the classification, protection, transferring and processing of individual IoT data streams.
- Legal restrictions on the classification, exchange, storage and processing of IoT sensor data. As a sector regulated by a number of restrictive rules, the financial sector will have difficulty in making efficient use of this technology. Amendments to the laws on professional secrecy and GDPR seem necessary.

Proposals for government action

Technological changes must go hand in hand with changes in law and supervisory regulations in order to exploit the potential of the IoT, particularly in sectors as highly regulated and supervised as the financial sector and insurance. Therefore, we recommend taking the following actions:

- Support of local governments in the development and standardisation of new payment methods for public transit services through the installation of Bluetooth beacon sensors in public transit vehicles and at bus stops;
- Establishing a cohesive legislative framework – the innovativeness of the implemented solutions should go hand in hand with the openness of public entities to accept changes (changing legislation, open tender procedures, taking innovation into account in the tender criteria).
- Working out clear rules to enable unambiguous classification, protection, processing and transfer of IoT data.

  Amending the provisions of the Act on Insurance and GDPR to enable IoT data processing. In particular, it is required to develop solutions that enable excluding IoT data from the category of sectoral secrets, and change the way they are treated in the context of GDPR.
- Regulating motor insurance based on driver behaviour (individual rates based on driving style assessment).

  Redefining online data exchange protocols for connected cash registers and changing receipt data standards to reduce the cost of devices and accelerate the implementation of online fiscalisation, as well as new payment methods, while reducing the investment outlays of the Polish Government (from 320 million PLN) and enterprises (from 3 billion PLN) over the next 10 years. We postulate removing the fiscal memory of the device and moving it to the application layer (for example to the cloud, with optional blockchain-based cryptographic protection) to speed up and reduce the cost of online fiscalisation and to support the adoption of new payment methods, as well as electronic receipts.

10

SMART CITIES AND BUILDINGS

Thanks to the Internet of Things and the development of ICT technologies, our cities have an opportunity to become more citizen-friendly, be better organised and make better use of available resources. In the long run, the implementation of the Smart Cities concept may be an important driving force for the Polish economy, bringing tangible benefits to residents, public administration units and private companies.

AUTHORS:
REMIGIUSZ WIŚNIEWSKI, DETECON INTERNATIONAL GMBH – SUBGROUP LEADER
MICHAŁ BAŁOS, EMITEL S. A.
KRYSTIAN BERGMANN, FIBAR GROUP S. A.
DAMIAN KLIMAS, UNIVERSITY OF WROCŁAW
FRANCISZEK MAROSZEK, NOKIA SOLUTIONS AND NETWORKS SP. Z O. O. AND THE HACKERSPACE ASSOCIATION WROCŁAW
MIROSŁAW POLSKI, HEWLETT PACKARD ENTERPRISE POLSKA SP. Z O. O.
MATEUSZ STEFAŃSKI, MICROSOFT
ARNOLD WIERZEJSKI, NOKIA

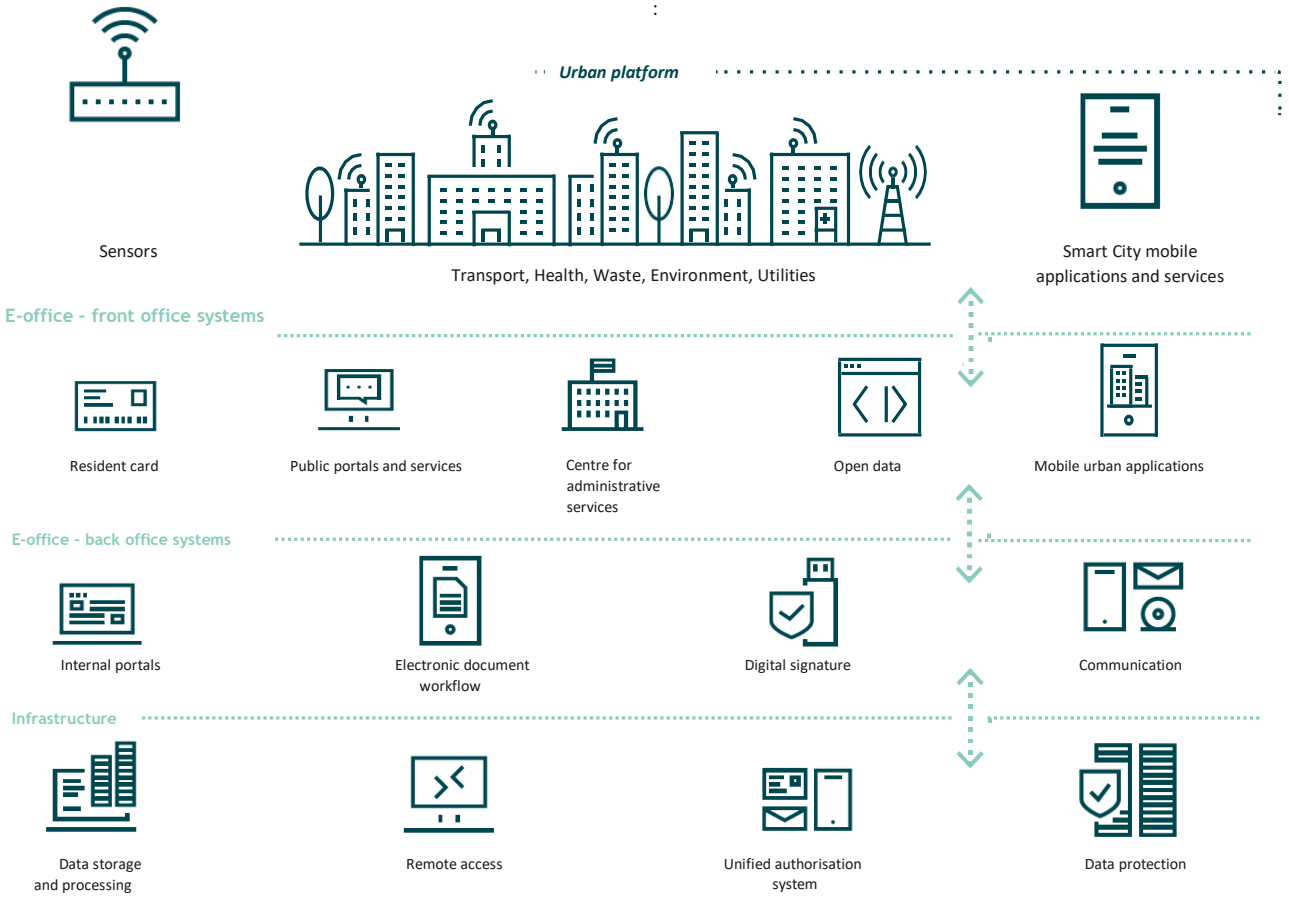
General characteristics of the sector

A Smart City can be defined as a space that "uses information and communication technologies to increase the interactivity and efficiency of urban infrastructure and its components, as well as to raise the awareness of its residents." A city can be considered as "smart" when it invests in human and social capital and communication infrastructure in order to actively promote sustainable economic development and a high quality of life, including wise use of natural resources through civic participation,[1] which should translate, into (among other things):

- universal access to information about the city as well as its development plans, etc.;
- cost efficient, effective and eco-friendly transport services;
- optimal use of urban infrastructure and the resources used by the residents (electricity, gas, heat);
- cares for the environment, in particular ensuring low pollution;
- safety of the residents;
- improving the quality, efficiency and availability of healthcare services;
- efficient handling of official matters in municipal offices and institutions;
- efficient operation of municipal services;
- high city attractiveness to investors;
- broad range of available leisure activities (cultural and sports events, etc.);
- active participation of residents in improving the city through cooperation with the administration;
- ensuring equal opportunities and conditions for different social groups;

The key element of the Smart Cities concept is the digitisation of urban space, to build cities that are more citizen-friendly, eco-friendly and more economical. From a technological point of view, the key element enabling the implementation of this concept is Internet of Things, or – in other words, according to the definition outlined in Chapter 3 – a concept based on communication between devices (M2M - machine to machine) assuming the possibility of communication, collection, processing and exchange of data by these devices via a local or Internet network. In a nutshell, this means installing sensors in the urban space, public venues as well as households and buildings in order to enable real-time event monitoring and data exchange between machines and people. Increasing the level of access to the information about, for example, traffic, occupied parking spaces or the required light intensity will help with significant optimisation of the use of available resources and remove many bottlenecks in urban infrastructure. The outline of the idea is shown in the figure below:

:



1 Azkuna I. (red.), Smart Cities Study: International study on the situation of ICT, Innovation and Knowledge in Cities. Bilbao, 2012

Considering the above, the implementation of the Smart City concept actually covers most areas of urban life, in particular:

- Transport & Mobility (urban traffic optimisation solutions also known as Intelligent Transport, car/bike sharing, intelligent car parks and public transit stops);
- Waste management (real time waste monitoring, untreated waste tracking);
- Environment (real time air pollution monitoring, monitoring of rivers and water reservoirs);
- Road and urban infrastructure lighting (smart lighting –monitoring and control of streetlamps and their surroundings);
- Houses and buildings infrastructure (smart buildings and home automation);
- Security and safety (surveillance and monitoring of public areas and venues, crime identification, emergency response systems, crowd control and event management);
- Utilities (consumption monitoring, anomaly detection, etc.);
- Healthcare (medical devices for measuring physiological parameters, remote patient monitoring, remote therapy).

Most of the above areas are the responsibility of municipalities, hence local government bodies will be naturally the main sponsors of such projects and deployments. After all, it is the local governments, next to IoT solution providers, are the most motivated to build smart cities:

- cheaper provision of the municipality's services;
- protection of the natural environmental (for example air quality improvement);
- improving the quality of life of residents;
- increasing availability of services and information for residents;
- employment growth;
- political capital gains.

Thus, any efforts to identify barriers and prepare recommendations for the Smart Cities and Buildings sector should encompass significantly local government bodies.

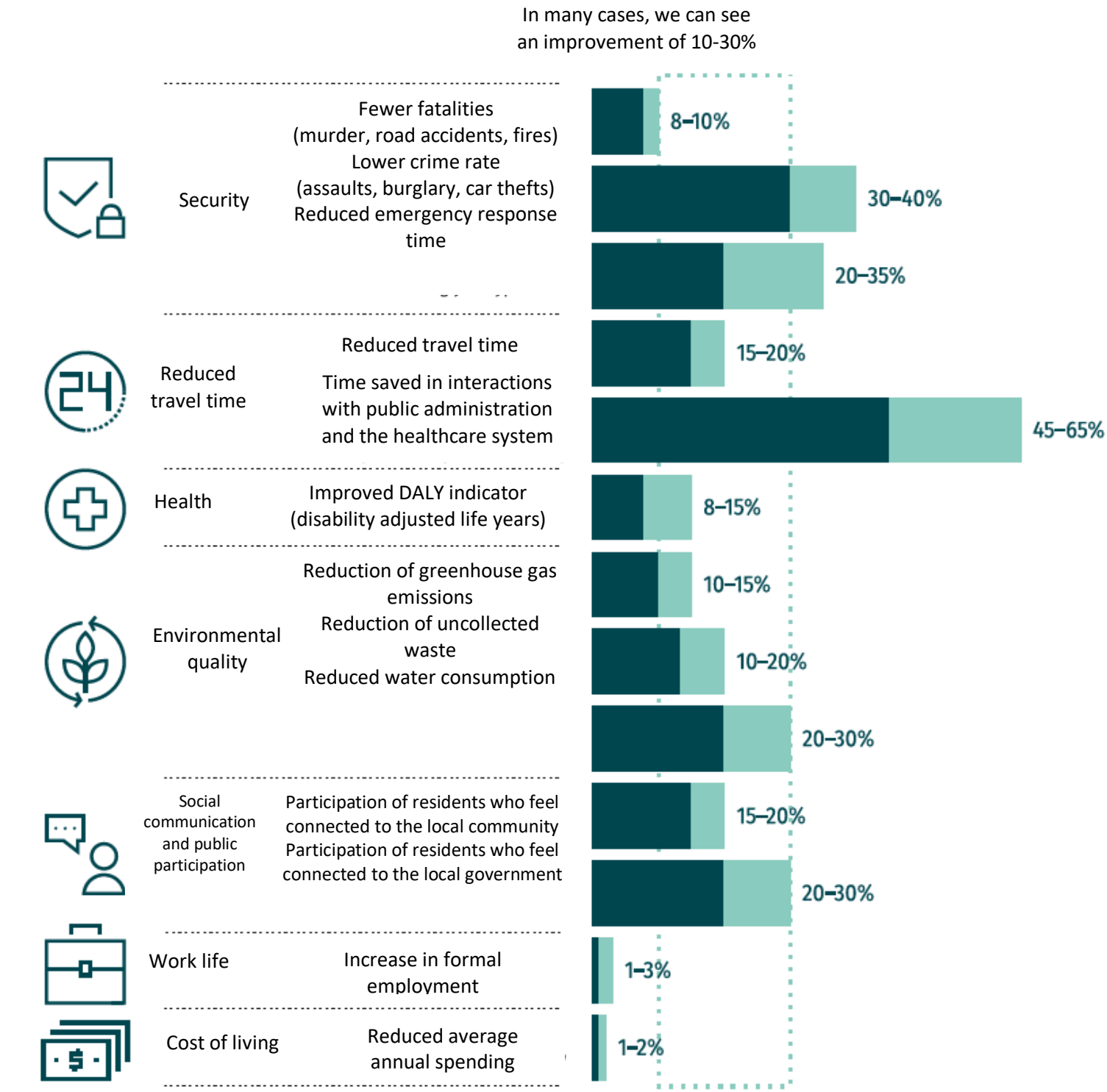
The examples of application areas presented above show the Smart Cities and Buildings sector from the demand point of view , where local governments, public utility companies and residents are direct beneficiaries of the deployments. However, bearing in mind the objectives of this report, it is also necessary to take into account the supply perspective – the market of providers and suppliers of solutions in the entire value chain related to the Smart City, which includes:

- sensors, cameras and other devices that collect and send data,
- devices providing communication via different protocols, using both licensed and unlicensed bands (GPRS, 3G, 4G, LoRaWAN, LoRa, Sigfox, 868 MHz, 900 MHz, NB IoT, LTE Cat0, LTE Cat1, LTE Cat M ZigBee, 802.15.4, Wi-Fi, RFID, NFC, Bluetooth 4.0, Z-Wave and HomeKit);
- mediation platforms, integration frameworks;
- data management systems and fleet management systems;
- cloud computing resources;
- reporting and analysis systems, AI;
- security systems;
- application layer providing services for end users.

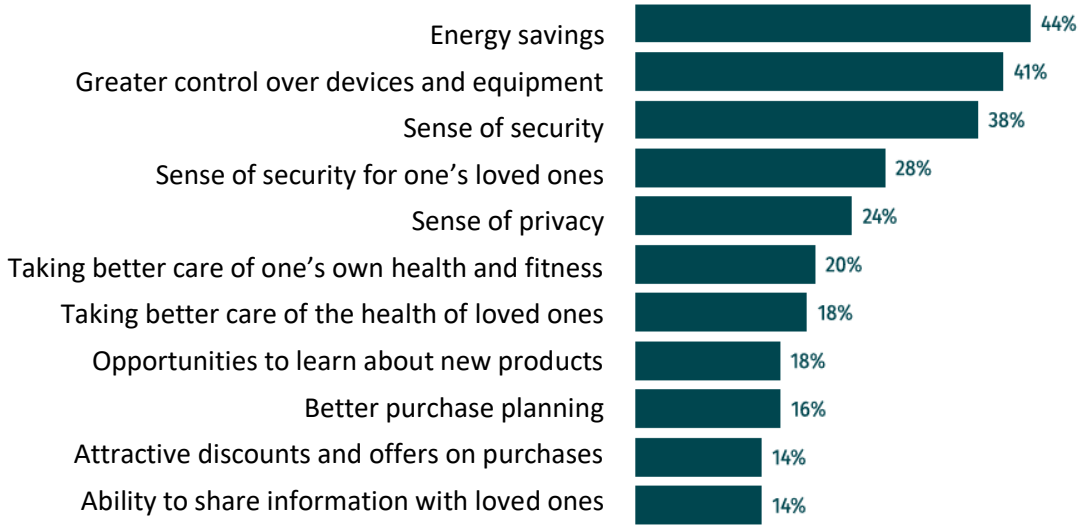
Significant development potential can be expected in each of the above segments,; however, it will not be the same in every area, due to factors such as the varying number of stakeholders and players in their respective markets and different entry barriers. Nevertheless the development prospects for domestic suppliers seem to be very high, given the growth potential of the local, European and global markets. This would, however, require multifaceted actions stimulating both demand – significantly increasing the level of Smart City investments in Poland, as well as activities supporting companies operating in this market.

Growth prospects for the industry

The market for Smart City solutions is growing rapidly, addressing many of the challenges related to rapid urbanisation it should be borne in mind that these processes will deepen. Forecasts indicate that by 2050 more than 80% of the population of developed countries and more than 60% of the population of developing countries will live in cities. Thus, it can be expected that today's issues pertaining to environmental pollution, availability of infrastructure, public and private transport, waste, as well as growing energy demand will keep intensifying. As a result, city authorities will be forced to undertake urgent remedial action. The implementation of the Smart Cities and Smart Home concept can alleviate at least some of the problems. The expected benefits are shown in the graph on page 35.



According to a study conducted by IAB Polska in 2015, the benefits of the IoT according to Polish Internet users are as follows:

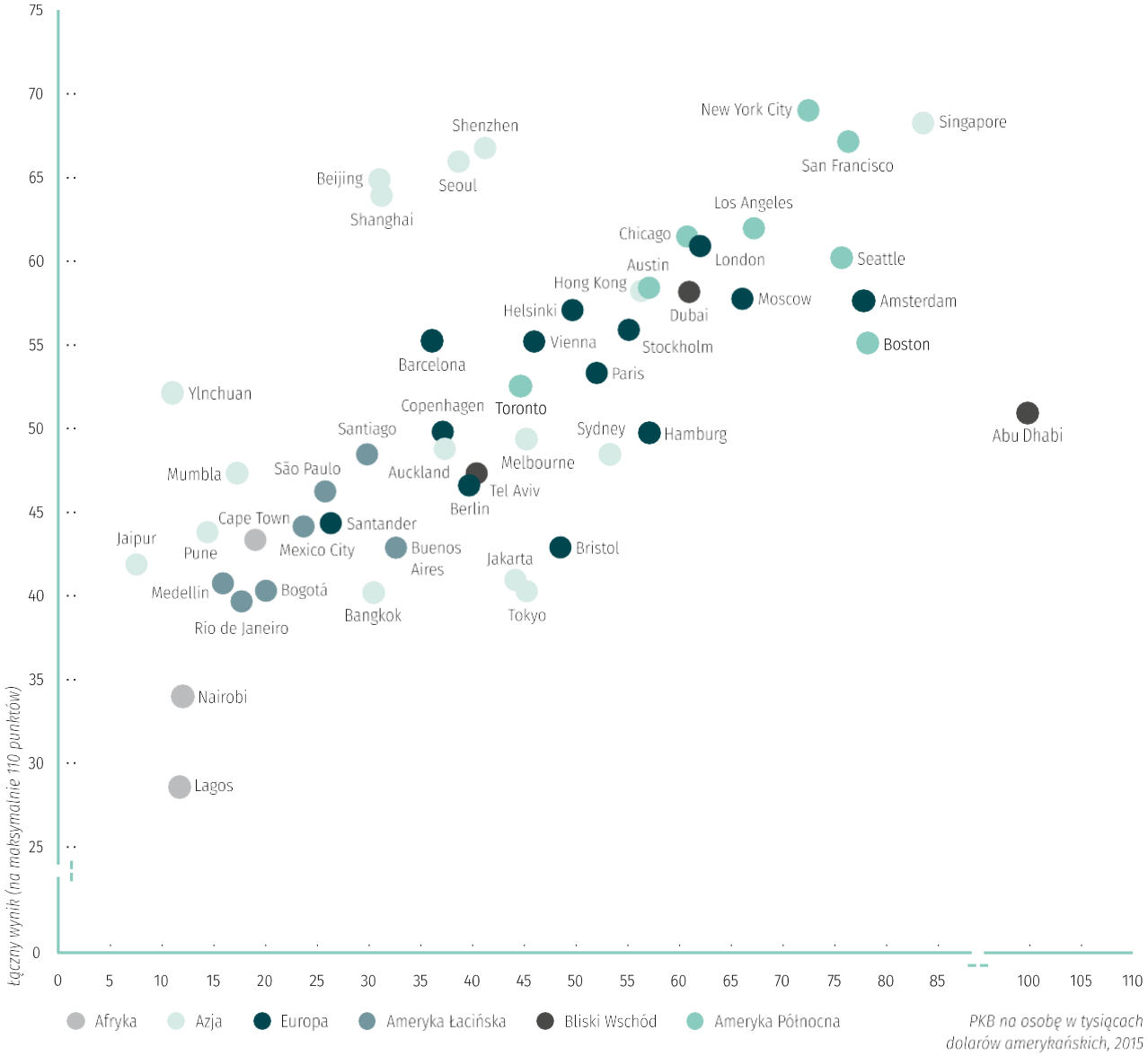


Source: IAB Polska, *Internet of Things*: May 2015, Internet users aged 15+, n=1221, via: webankieta.pl

The challenges of urbanization are of course not the only element impacting the development of Smart Cities – other important factors also include:

- economic growth;
- sustainable development policy;
- the need to take decisive action to protect the environment globally;
- public safety;
- growing number of cars – an estimated 1 billion cars by 2020;
- availability of telecommunications infrastructure;
- development and improved availability of technologies (artificial intelligence, Internet of Things, 5G, blockchain);
- access to Big Data and increasing possibilities to analyse the data and make decisions based on this data , (data from systems, applications, IoT sensors);
- digitisation in various fields and sectors of the economy;
- social expectations and new generations requirements.

This is why many countries and cities are making efforts to realise the Smart City concept in a widespread manner. The chart below presents cities implementing Smart City concepts around the world.



Source: McKinsey Global Institute Cityscope Database

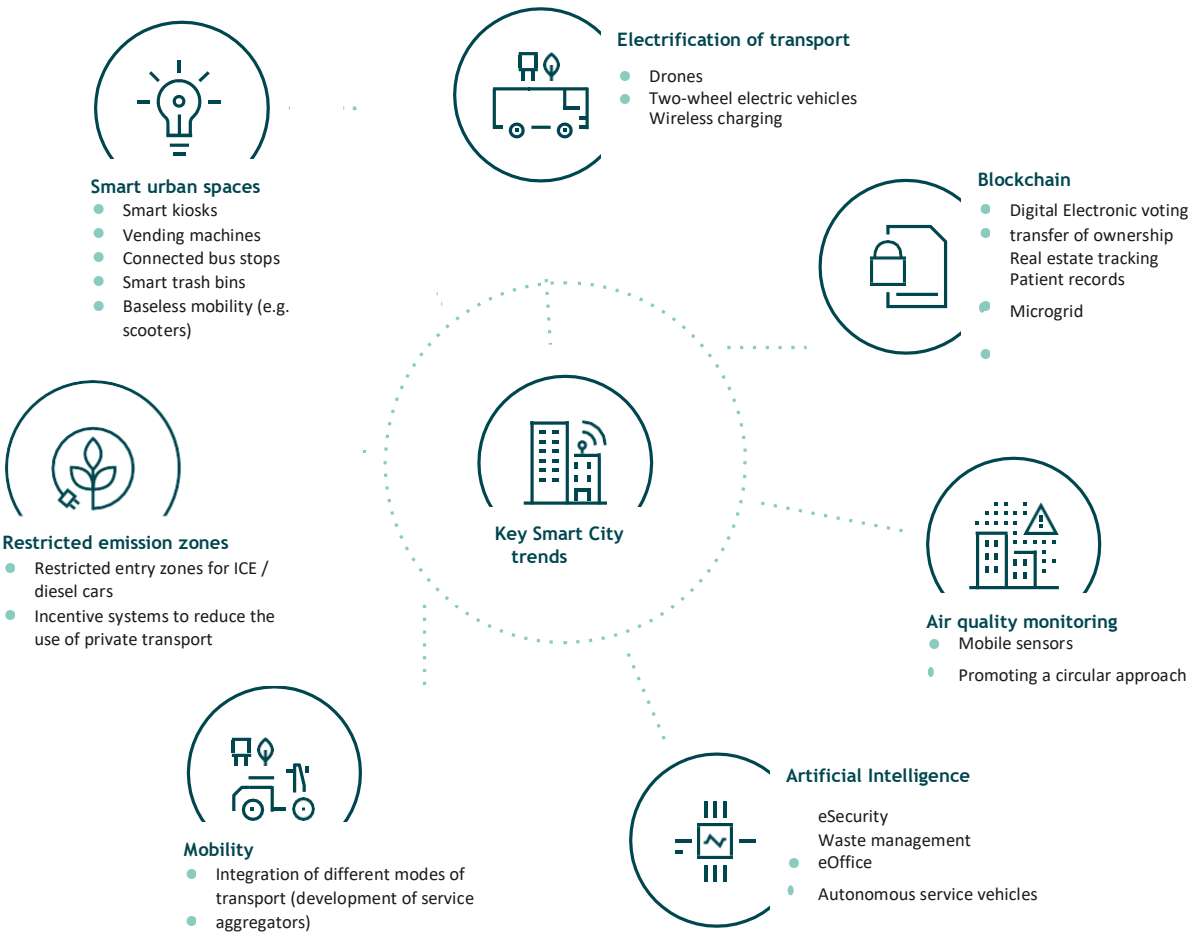
This translates into growth forecasts for the entire industry. The Machina Research institute and McKinsey estimate the global IoT market size for Smart City applications at 10 trillion EUR by the end of 2025.[1] Frost & Sullivan is slightly more cautious in its estimates, indicating a potential of $2 trillion in the similar time frame; however, in both cases the market potential is very high. The outlook is similar when it comes to individual market segments – for example, according to industry analyses, smart buildings have the highest potential in the consumer branch of the Internet of Things. The smart home industry is growing at 38% in Europe and could be worth up to $20 billion by 2020. It is also estimated that the number of households with automation solutions in the European Union will increase from 13 million in 2018 to 27 million in 2020. The highest demand can be observed when it comes to energy-saving devices and equipment ensuring the people safety.

The growth potential of the IoT industry in Poland is yet to be analysed but the strive and the tech savvy of the nation resonates very well with global predictions. However, it can be expected that both the growth rate and potential in the long run will correspond to global trends. Taking advantage of the trends constitute an important boost for the Polish economy, especially considering how these solutions are currently implemented (very selectively and in silos, mainly focusing on smart lighting and smart transport systems) and given that the quality of life in Polish cities is relatively low compared to the leaders of worldwide rankings.

In the nearest future, the most promising segments in the Polish market are:

- segments of interest for the European Union concerning Smart Cities (EU budget, EU requirements);
- infrastructure and environment: environmental protection, water and energy, transport;
- basic public services: public safety, health, education;
- planning and management: smart buildings, open government, management and planning intelligence;
- easier access to data and offices;
- improving safety and convenience;
- improving the environmental quality;

Long-term planning should also take into account global trends indicating the growing adoption of electromobility solutions, the use of autonomous vehicles, as well as the use of blockchain in various areas shown in the chart below.



Activities catalysing the realisation of the Smart Cities and Buildings concept on a large scale, both from the supply and demand perspectives, can result in many social and financial benefits for cities, residents, public companies, as well as private enterprises that develop and create new solutions. This can stimulate social and economic growth, contributing to the increase of increasing the competitiveness of the Polish economy. On the other hand, in view of current trends and the high dynamics of changes in the global economy, one can claim that disregarding the existing opportunity offered by the technological revolution associated with the IoT, Industry 4.0, artificial intelligence and 5G may cause a significant decrease in productivity and competitiveness of the Polish economy in the long run, in particular in comparison to other developed countries.

Scope of possible use of IoT solutions

IoT devices constitute one of the technological foundations of Smart Cities – they are what makes it possible to remotely supervise and control urban infrastructure.

The scope of possible use cases of IoT technology is very vast, as the implementation of the Smart Cities concept hinges on the integration of many areas and the exploitation of the potential offered by data collected in different contexts. Integration of IoT and IT/ICT systems and infrastructure allows the creation of intelligent systems, among which the most popular are the following :

- utility management (municipal lighting, water/electricity supply, waste disposal);
- public space monitoring;
- environmental pollution monitoring;
- transport systems (Intelligent Transport Systems, smart car parks);
- vehicle sharing;
- protecting the health of residents.

Scope of IoT use within the framework of the implementation of the Smart Cities and Buildings concept

Solution	Description	Benefits
Smart transport	A broad range of solutions increasing both the level and the exchange of information between the participants of the municipal transport network, aimed at providing a safer and more efficient transport infrastructure. These solutions are capable of identifying and responding to changing road conditions, setting the optimal routes for drivers and optimising fuel consumption. In particular, these include Intelligent Transport Systems (ITS), which collect data from available sources - sensors, cameras, devices installed in public transport vehicles, meteorological stations, speed cameras, etc. Continuous communication between individual devices in combination with advanced data analysis systems is intended to allow transport companies to predict failures or faults, thus avoiding costly repairs and downtime in the future.	• Increasing transport infrastructure capacity. • Improving safety. Reduced travel time, reduced consumption of fuel and energy. • Improved efficiency of public transport (lower fleet costs). • Effective crisis management.
Bike/car sharing	Vehicle sharing systems using mobile applications enable renting bicycles / cars / scooters / electric scooters in the city. These solutions respond to a variety of issues, including poor access to poorly connected areas or the “last mile” problem – getting from the bus stop to a destination that is located far away from it. The availability of car-sharing systems can also lead to lower need for car ownership among residents.	• Fewer cars entering cities / better use of space in city centres. • Greater flexibility of public transport. • Increased use of vehicles.

Solution	Description	Benefits
Smart Parking — parking space occupancy detectors	The aim of Smart Parking solutions is to optimise the use of parking spaces. Given that several dozen percent of traffic in city centres is generated by drivers looking for parking spaces, making it easier to find a free space significantly reduces car traffic in the area. Sensors installed in the vicinity of the parking spaces provide information about the location of the available spaces, the number of vehicles passing by, or even their speed and size. Information on free spaces is then provided to drivers.	• Optimal use of parking spaces, higher income from parking fees. • Free parking spaces becoming easier to find.
Air Quality Monitoring — air pollution sensors	Installing sensors to measure air quality at sensitive points of urban space helps to diagnose air composition in terms of harmful gases (sulphur/nitrogen/carbon oxides) and particulate matter (PM10 and PM2.5). This type of information facilitates the identification of pollution sources and enables early warning about exceeding pollution limits, which has a significant impact on the health of city residents.	• Better air quality control; • Easier identification of pollution sources; • Informing residents more quickly about exceeding pollution limits;
Smart Lighting	Smart city lighting, using sensors for pedestrian and car traffic in the immediate vicinity, has two functions – it illuminates intersections to improve safety and saves energy by reducing brightness when there is no traffic in the area.	• Lower energy consumption, lower costs of city lighting; • Increased road safety;
Smart Home	A Smart Home comprises a system of sensors and devices with a single, integrated management system, which enables remote access to data. Thanks to the data coming from the sensors, the system can automatically react to changes through interaction with the user or its own programmed set of instructions. The basic functions of building automation can be divided into the following areas (in terms of control, monitoring, optimisation and reporting): • Controlling lighting and other electrical devices; • Controlling roller shutters, gates, access control systems; • Air conditioning (temperature control, air quality, ventilation); • Health, life and property protection (detectors, transducers, video surveillance, alarm systems); • Integration with consumer electronics and household appliances; • Monitoring and optimisation of energy production and consumption; • The application areas for smart homes and buildings concern both public buildings, commercial buildings and housing.	• Lower use of utilities (power, gas, water); • Improving residents' safety; • Improving the living comfort of residents.

Solution	Descriptio	Benefits
Smart Security	A group of solutions addressing various aspects of protection of the life, health and property of residents. These include, but are not limited to: • Smart public space surveillance – camera systems and environmental monitoring (motion sensors, fire and flooding sensors, detectors of dangerous compounds in the air, etc.); • Shot detection – solutions including both sensors / cameras as well as systems for detecting events potentially related to crime or accidents. • Smart emergency response systems. Crowd control / assembly management - crowd analytics – systems for monitoring the movement of residents based on telecommunications data. • Smart crisis management centres which aggregate sensor data and video analytics.	• Improving residents' physical safety. • Lower crime and accident rate, as well as reduction of possible consequences. • Better use of infrastructure and resources of uniformed services.
Smart Metering	A range of solutions for automating utility meter readouts: • Leak detection. • Consumption monitoring. • Quality monitoring. • Smart irrigation measurement of ponds and rivers. • Gas metering. The area of smart metering is described in more detail in Chapter 12.	• Reduction of utilities consumption. • Lower failure and defect rate.
Smart Healthcare	A wide range of solutions taking advantage of the IoT in combination with advanced data analysis and artificial intelligence solutions can be used for remote diagnostics and therapy. The healthcare field is further described in Chapter 11.	• Lower treatment costs. • Higher quality of medical services.

The list presented above is obviously not exhaustive, as the number of applications is virtually unlimited. Today's technological capabilities allow us to place and install sensors in the majority of objects in modern cities in order to collect and process huge volumes of data, drawing conclusions, forecasting and predicting events. The Smart Cities solution implementations provide significant social and financial benefits resulting from using this technology. The new systems enable, among other things:

- 20% reduction of travel time by public transit;
- 65% reduction in time spent in offices;
- 35% reduction in emergency response times;
- 40% reduction in the crime rate;
- 3% reduction in the cost of living;
- 3% increase in the employment rate;
- 15% reduction of harmful emissions and water consumption.

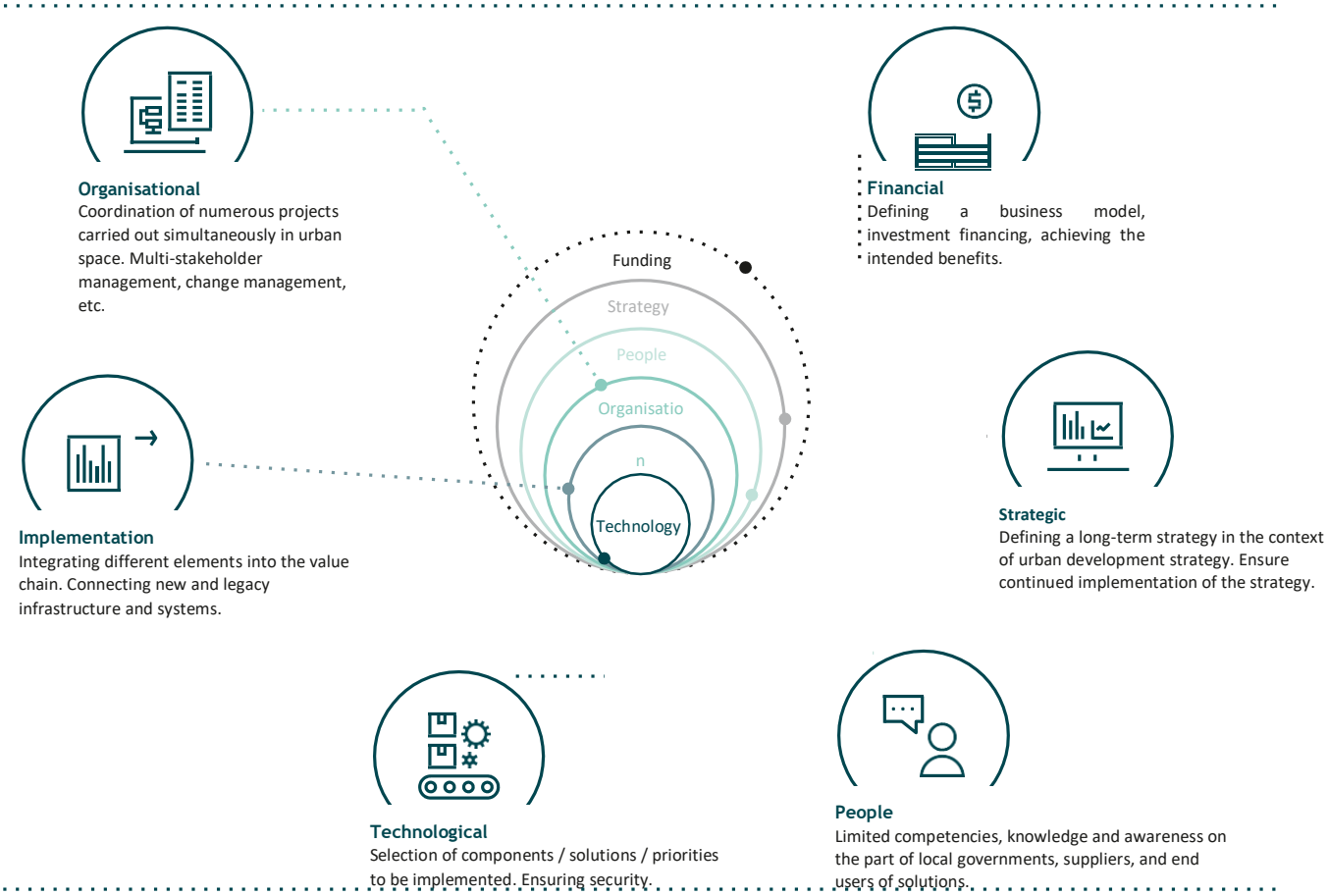
The greatest benefits can be achieved by integrating individual areas; hence a holistic view of the whole concept is required. It is also worth taking a closer look at the approach and examples of implementation of solutions in entire urban agglomerations.

Barriers

The development of information and communication technologies undoubtedly contributes to the popularisation of the Smart City concept in cities, but its implementation often takes place in an uncontrolled, insular and uncoordinated manner, carried out by various entities operating in the local area. This results in the duplication of solutions and the use of various non-interoperable standards, resulting in cost inefficiencies. Even in a common area – such as a local administrative unit – various entities and players (state administration bodies, public and private entities) acting within their authority and in line with their business objectives can and most often do implement their projects in an uncoordinated manner, which makes it impossible to build an integrated public Smart City infrastructure.

This duplication of infrastructure and systems prevents the use of EU funds and limits the development of Smart Cities. This concerns Poland in particular, since the level of adoption of IoT solutions in cities remains abysmal.

This is a result of numerous challenges pertaining to the implementation of Smart City solutions, presented in the chart below.



Another key issue at the current stage of implementation of IoT solutions is the limited interest of potential customers. There is a marked lack of awareness on the part of residents, as well as local authorities. Industry growth is driven by suppliers, not by the actual needs of users. In many cases, the potential advantages lose on importance when confronted with reality. The organisational, economic and formal constraints mean that potential end users do not see the need to implement these solutions, and therefore the assessment of actual needs is very important.

The IoT cannot be seen only through the prism of novelty and as a source of potential additional revenue. Instead it should respond to the needs of the residents and serve to improve life in the city, especially when it comes to the field of Smart Cities solutions.

Various barriers can be seen in different areas and at different stages of adoption of IoT solutions in cities. The main barriers identified during the work of the Working Group are presented below. This is where the authors need to point out that Smart Cities are ecosystems of systems, and hence it was impossible to refer to the individual application groups within the framework of the Working Group. Thus, the following part of this chapter presents barriers concerning only a number of selected segments.

URBAN AGGLOMERATIONS – A HOLISTIC APPROACH TO CITY ORGANISATION

AMSTERDAM

Smart Parking – a way to view information about free parking spaces via information boards and mobile applications. Benefits: reduction of CO^2 emissions, reduction of traffic jams, lower operating costs for parking (payment via application). Other applications facilitating using public transit (Citimapper) or allowing the city to verify rights to parking in specific zones (licence plate photos).

Electric cars – the city has a fleet of 300 cars. Opening and closing the vehicle is done via the mobile application, just like starting the car. Benefits – reduced CO^2 emissions, increased mobility and time saving – the car is available within just 30 minutes at the desired location. A similar service was also implemented for electric scooters.

Energy distribution – Climate Street project – an initiative of 40 enterprises supporting sustainable development. After a two-year pilot stage encompassing 20 of the 40 projects, they have achieved energy savings of 8%, which translates into a reduction of emissions by an equivalent of 194 tonnes of CO^2.
The projects concerned, among others, the replacement of street lamps with LED-based ones, the use of smart meters for controlling air conditioning, and the use of electric waste collection vehicles.

BARCELONA

Smart Parking – sensors in a number of places, for example in the vicinity of Sagrada Familia. Benefits: 33% increase in revenue from parking fees.

Smart Stops – touchscreen information boards with timetable information and additional data about tourist attractions. Wi-Fi networking, since each stop is connected to the Internet via a fibre-optic cable, along with phone chargers.

Street Lighting – In cooperation with Philips, 1100 streetlamps were replaced with multifunctional units. In addition to variable lighting, the lamps are equipped with Wi-Fi hotspots, pollution sensors and surveillance cameras.

Waste management – sensors that signal full bins, a pneumatic collection system using a suction mechanism and a central hub, as well as a network of underground pipes.

Others – smart meters, bicycle rental, smart park and garden irrigation system, sensor network: pollution, noise, flow of residents, traffic.

More: http://www.22barcelona.com/ https://arkinetblog.wordpress.com/2010/03/22/barcelona-will-vote-for-diagonal-redesign/

BERLIN

Autonomous minibuses – unmanned minibuses carrying about 12 people, driving on strictly defined routes. One vehicle underwent pilot testing in 2016-2017. Hundreds of such vehicles are expected to operate in the city in a few years.

Others - smart meters, electric car chargers, air pollution sensors to identify the causes, trash bin filling sensors with communication using an app, CUBE Berlin construction - smart office building.

More: https://www.statistik-berlin-brandenburg.de/home.asp, http://www.5g-berlin.org/

SINGAPORE

Smart transport – the use of autonomous vehicles on less congested streets, traffic signal control system powered by data from sensors installed under junctions. Benefits: adapting green lights to the needs of traffic users, reducing CO^2 emissions due to better flow of traffic.

Waste management – pneumatic system for sucking waste through a pipe system. Waste bins equipped with sensors which enable optimisation of the waste collection schedule. Benefits: time and cost optimisation: the pneumatic system takes care of the task in a few minutes compared to a full day's worth of work of a traditional truck; increased recycling.

AUCKLAND

In the adopted strategy the city aims to improve digital communication in the city, open up access to urban data, support innovations proposed by the residents, promote digital education, improve public transit, as well as optimise energy consumption and waste management.

The city council has opened up to the implementation of projects proposed by commercial entities, instead of designing and developing its own solutions; however, it does not limit itself to a single supplier.

The council defined a test area for the implementation of new Smart City projects. The projects adopted to date include the revitalisation of port areas and the construction of an innovation centre in Wynyard.

More: http://www.aucklandcouncil.govt.nz/EN/planspoliciesprojects/reports/ Documents/aucklandprofileinitialresults2013census201405.pdf

BRISTOL

Open platform – the key project – Bristol is Open – aims at opening access to public data obtained from process management systems in the city.

*More: https://www.bristol.gov.uk/documents/20182/33191/ Bristol+Econominc+Briefing+Sept+2016/e171a9ee – 8da6-427e-825d-3a06b7f488*61)

VIENNA

Smart parking – the solution includes a mobile application for residents integrated with the parking fee collection system

Smart transport – a mobile application allowing users to buy public transit tickets.

Air quality monitoring – real-time air quality monitoring system.

IoT platform – a platform aggregating data from smart solutions and sensors, managing devices and providing access to external applications.

The city's strategy is to combine data from IoT solutions into a single, comprehensive aggregation layer for use by any certified application. Its authorities put great emphasis on innovation in transport and ecology.

Strategic

- Lack of long-term strategies due to the focus on typical scopes of functioning of the city, without exploring new challenges and analysing available solutions, especially in smaller urban centres.
- Lack of a cohesive strategy, vision and concept for the development of Smart Cities at regional and national levels – lack of system solutions which would facilitate the implementation of the concept by local government bodies.
- Lack of continuity in decision-making among elected officials in their subsequent terms, which translates into issues concerning both strategy and operations.
- Lack of provisions concerning the development of Smart Cities in strategic documents pertaining to urban development.

Financial

- Lack of funds for the implementation of investments in the area of Smart Cities, in particular given the more urgent local government spending in the short term. This is compounded by difficulties in estimating return on investment in the short term. On the other hand, there are no budgets for solutions which can bring benefits going beyond a given local government unit.
- Limited funding opportunities for projects from various sources, using various funding models.
- Complicated procedures for obtaining EU funds.
- Lack of allocated budgets for fast-track pilot implementations.
- Lack of priorities for the implementation of Smart Cities and Smart Home/Buildings projects.

Political

- Lack of decision-making continuity holds back key analyses, defining long-term requirements, applying solutions and investing in innovative technologies.
- Economic pressure creates the challenge to provide more services and solutions at a lower cost, which requires modern approaches, new technologies and business models.

Technological

- The high complexity of technological solutions (large selection, lack of stability, lack of standards) is a significant barrier at the stage of solution selection, realisation, tender process, and later implementation and integration of solutions, which results in rather slow adoption of technologies and IoT projects.
- The lack of standards (concerning sensors, communication, platforms) and the multitude of solutions cause interoperability issues.
- Existing systems and infrastructure – problems with integration.

Organisational and procedural

- Internal procedures which do not facilitate the realisation of projects that often affect many departments.

  Lack of coordination of projects being carried out which are often siloed and implemented independently of each other.

  Lack of a horizontal and holistic approach to the harmonisation of processes related to the operation and implementation of vertical Smart City applications.
- Individual elements of urban infrastructure fall under the scope of responsibility of different organisational units, which significantly hinders coordination .
- In many cases there is a marked lack of clear ownership of the Smart City area – some cities appoint coordinators or plenipotentiaries who deal with the subject in question, but they often also have limited powers in this regard.

People

- Lack of knowledge and awareness of the directions of urban evolution, as well as of the implementation and integration of innovative technologies. This applies both to public administration representatives, who are responsible for growth and development, as well as to end users – the residents.
- Digital exclusion – inability to use modern technologies among selected social groups.
- Security (for more information on security, see Chapter 8).

Legal

Lack of a predefined framework for innovative business models in which investments are covered, both from the budgets of central and local government programmes, as well as private sector companies. Local governments are reluctant to get involved in non-standard business models for fear of lack of regulation. Barriers to purchasing in an as-a-service model or other models (PPP).

- Lack of recommendations for the framework of the technological dialogue process.

- Restrictions concerning the involvement of private investors in public projects when launching innovative business models as a source of income for the city.

The following barriers were also identified at the level of individual areas:

Waste management

- Waste management companies are very conservative in implementing innovative systems due to a lack of awareness of possible savings. The short lead time following the tender (1-3 years) stops investments in systems in cases where return on investment appears in the long run.

- Durability of sensors, resistance to vandalism, cost effectiveness of the sensors themselves and their replacement cost (given the short lifespan of waste bins), breaking monopolies in waste disposal, incorrect readings due to the variety of the types of waste.

Smart lighting

- Urban lighting infrastructure belongs to a variety of entities, which makes it impossible to implement integrated systems that would be optimised in terms of cost and technology. Lack of regulation and predefinition of the scope of Smart Lighting implementations which can open up access to a broad range of applications using the same infrastructure.

Smart Urban Data Platforms

- Lack of technological recommendations concerning the standardisation of platforms using public data results in pilots and the implementation of (closed) siloed solutions, which are hard to develop and grow further.

Smart buildings and homes

- Lack of tax incentives that would motivate investing in smart building management in order to optimise energy consumption.

  Lack of awareness – the potential users are hardly aware of the existence of solutions that can realistically increase their safety.

Smart parking

- The risk of damage to sensors in winter due to snow removal and vandalism; appropriate information for drivers about the system and its operation.

Environmental pollution

- Authorities are reluctant to show the state of air pollution openly and transparently, hence the reluctance towards financing Vending Telemetry.
- Scale of investment, additional costs resulting from the increase of signal power (underground sensors, as well as sensors installed deep below ground level, so called minus n), sensor technologies vs existing types of meters.

Proposals for government action

Many Smart Cities applications can bring tangible benefits, but only a fully holistic and integrated approach will provide considerable benefits in the long term. This will enable connecting transport, transactional, energy management and infrastructure systems to ensure the highest value of integrated applications.

However, this requires the Polish authorities to take a number of measures to stimulate the implementation of the Smart City concept in cities, in particular:

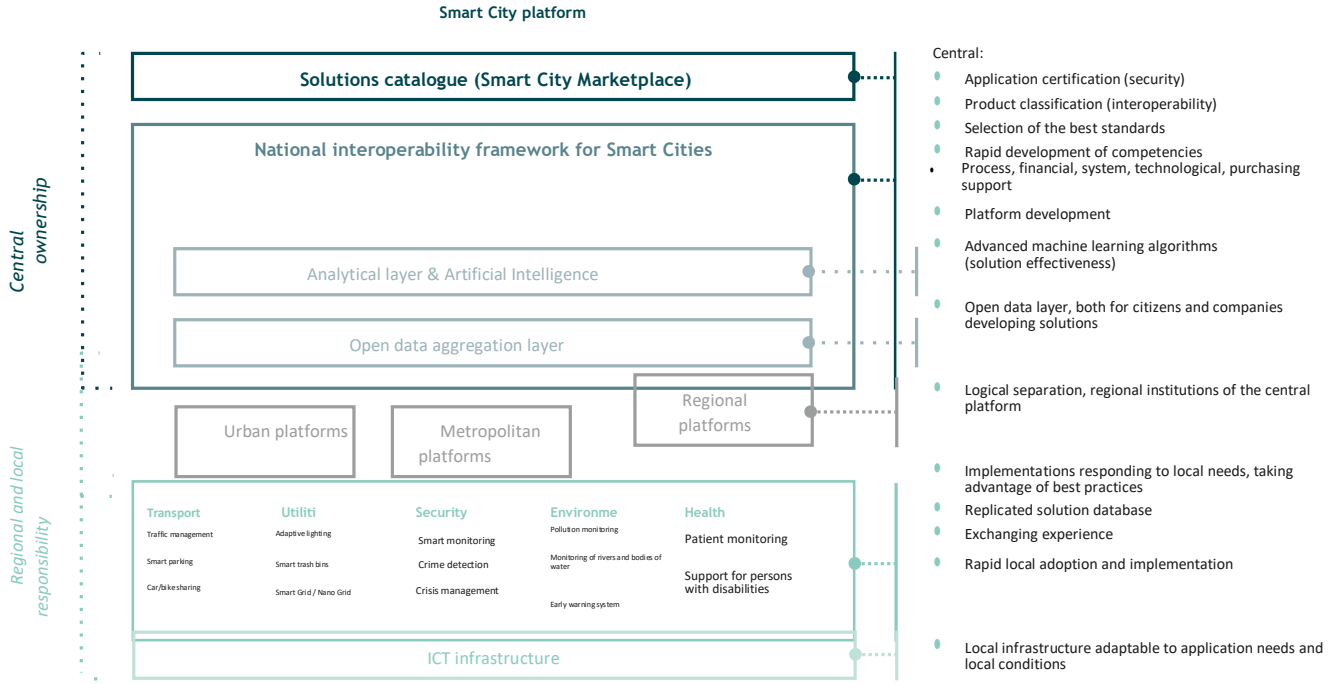
A central strategy to foster implementation and address the challenges faced by regional and local governments, integrated with the state digitisation strategy. Such a strategy should encompass mechanisms for financing deployments and addressing the issue of the interoperability of Smart City platforms in terms of data sharing, interoperability of communication systems, interoperability of solutions for public safety, healthcare, etc. These mechanisms should be based on the nationwide Smart City Operational Framework, supported by approval/certification mechanisms for services and solutions.

- Systematised processes and procedures for the implementation of Smart City projects in local governments, as well as supporting central technological competencies. In particular, this would require working together with business organisations to develop models and best practices in order to support the ordering of technologically complex solutions such as Smart City service platforms.

- Creating an open forum for exchanging experience and information.

  Getting rid of many barriers and obstacles related to lack of knowledge and awareness of technologies as the directions of development of cities, lack of models based on Public-Private Partnerships, and the limitations in the use of different financing and funding models.

Given the identified barriers and obstacles, the facilitation of technology adoption could be achieved by centralising some of the services (for example at regional, provincial or national levels) by building one or more Integrated Urban Platforms and creating a central “Catalogue of Solutions” – a marketplace of sorts, offering ready-made components for individual areas. It is important to ensure that smaller towns and municipalities have access to the same technologies. An outline of the concept is presented on page 46.



The centralisation of selected functions also requires removing a number of obstacles and barriers. Recommendations are presented below:

Strategic and Financial

- Developing programmes to support local governments at the central level – support for technology selection and implementation, co-financing initiatives carried out by local governments.
- Involvement of State financial companies (PKO, PZU, BGK) in financing and granting guarantees using a spectrum of financial instruments (such as leasing).
- Implementation of programmes aimed at supporting the development of Smart Buildings – education, tax breaks.
- Analysis and technological recommendations for building application deployment strategies and data platforms.
- Enabling earmarking budgets for the implementation of the fast track pilot schemes from local government funds.

Inclusion of Smart City projects in other activities and strategic documents – programmes, schemes including aspects such as spatial planning, long-term development plans, waste management plans, energy policy, water and sewage system development policy, environmental policy, programmes related to health protection and to strategic plans for the construction of municipal housing estates.

Technological

- Development of native cloud architecture aimed at virtualising resources and enabling the rapid development and deployment of new services and applications.
- Support for the development of telecommunications infrastructure, both in terms of the Internet of Things and 5G technologies, which will open up completely new perspectives.

  Taking advantage of existing regional infrastructures – the utilisation rates of these resources remain very low, which is why it can be assumed that some computing resources could be used to achieve the objectives related to the development of infrastructure for Smart Cities.

Organisational and People

- Building a network of collaborating City Labs where different solutions would be tested hand in hand with their suppliers.
- Training and education programme concerning Smart City technologies for local governments.
- Inspiring and supporting local government initiatives aimed at building a central repository of knowledge and best practices.

  Creating project implementation models for municipal structures (encompassing integration and cooperation between departments).

- Development of benchmarks for estimating project viability in a given city, municipality, etc.

  Following up on the work initiated by the Working Group for the Internet of Things – extended and more detailed analysis of barriers and obstacles in cooperation with key stakeholders and the development of a detailed action plan.

- Ensuring the cohesion of work carried out by individual ministries and government units.

- Improving cooperation between central government and local governments.

General legal

The need to increase the flexibility of Public Procurement Law – introducing service models, such as Smart Lighting as a Service and enabling various forms of public-private partnerships. The need to predefine the framework of the technical dialogue process.

- Analysis and predefinition of new business models together with recommendations for local governments.

- Defining a framework for establishing local government special purpose vehicles in the field of innovation and supervision of innovative infrastructure.

Specific legal

- Waste management – Legislation proposal: The Group suggests adding the following language as Section 5 to Article 33 of the Waste Act: "The minister responsible for the environment, in consultation with the ministers responsible for construction, spatial planning, development and housing, economy, communications, informatisation, transport, and internal affairs, shall determine by regulation the implementation and maintenance of smart waste management systems in municipalities, and will in particular define the objectives, requirements, installation, ways of working, financing, maintenance of the systems, rules for determining fees for residents by means of a system and rules for processing personal data in connection with the use of smart waste management software, guided by the need to ensure that the technology works properly and efficiently in order to properly manage waste and to protect the rights and freedoms of citizens."

- Smart lighting – Legislation proposal: Changing the language of Item 4 in Article 18, Section 1 of the Energy Law Act of 10 April 1997, which should read as follows: "planning and organising measures aimed at ensuring energy efficiency and promoting energy saving solutions in municipalities, in particular by implementing and maintaining integrated smart lighting systems;"

- Environmental pollution – Legislation proposal: Changing the language of Item 2 in Article 90, Section 5 of the Environmental Protection Law Act of 27 April 2001, which should read as follows: "the use of smart devices for assessing air composition, as well as aggregating and sharing information pertaining to such assessments."

- Smart buildings and homes – Tax break, similar to the existing thermal upgrade break.

Other recommendations

- Involvement in cooperation with PKP in various aspects:

  - Developing a Smart City strategy in cooperation with PKP – inclusion of railway infrastructure in the concept of smart transport.

  - Cooperation regarding the development of Smart Cities from scratch (*Greenfield* approach), where the construction of housing estates is planned under the Mieszkanie Plus (Apartment Plus) programme in the lots belonging to PKP. This will enable the gathering of invaluable experience and the testing of variants in actual projects.

- Support for Smart Buildings

  - A support programme or the introduction of a law forcing the installation of smoke and carbon monoxide detectors.

  - Further investment in clean air programmes. Replacing boilers with gas-powered ones, which will reduce the use of solid fuel boilers. Verification of the possibility of subsidising air purifiers in public utility buildings (schools, kindergartens, crèches, retirement homes).

  - Programmes to increase education and raise awareness of burglary and neighbourhood self-help programmes.

  - Programmes to increase education concerning energy-saving.

  - Support for preferential taxation conditions for energy-efficient buildings.

Recommended pilot projects:

- Development of the Smart City Platform architecture encompassing central and regional functions. Development of a pilot Urban/Regional Platform.

- Development of a pilot Smart City implementation for selected housing estates built under the Mieszkanie Plus programme.

- Development of a central repository of knowledge and best practices.

11

HEALTHCARE

A wise man ought to realise that health is his most valuable possession and learn how to treat his illnesses by his own judgement.

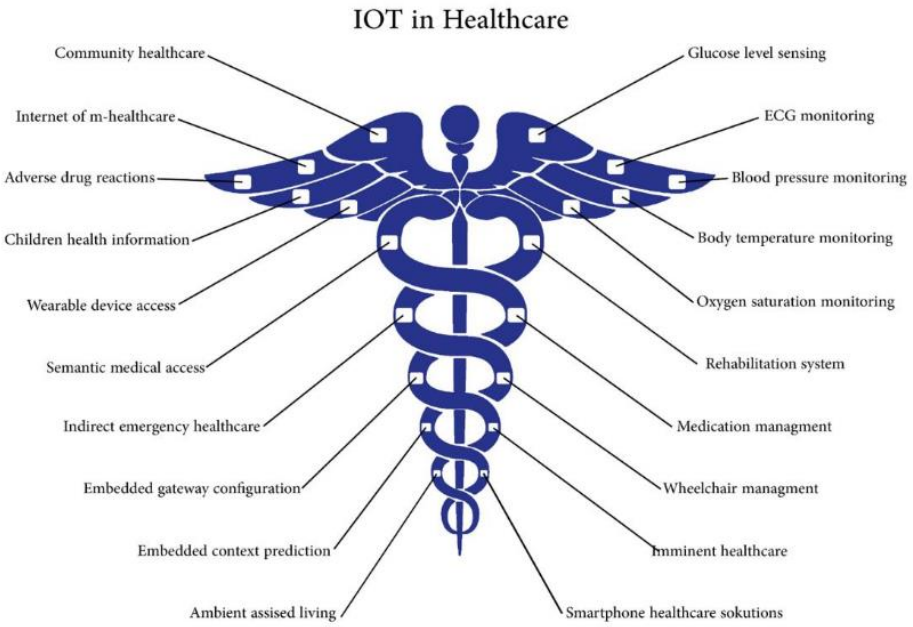
— *Hippocrates*

AUTHORS:
KRYSTIAN BIEŃ, POLPHARMA S P. Z O. O. — SUBGROUP LEADER
MICHAŁ JACKOWSKI, DSK KANCELARIA & LEX DIGITAL
MICHAŁ KOMAR, KANCELARIA PRAWNA D. DOBKOWSKI SP. K. ASSOCIATED WITH KPMG IN POLAND
MICHAŁ KURASIŃSKI, POLPHARMA SP. Z O. O.
BARTOSZ NIEWIADOMSKI, AVIVA GROUP
PIOTR TALAREK, TBT I WSPÓLNICY
PIOTR ZWOLIŃSKI, ŁAZARSKI UNIVERSITY

General characteristics of the sector

Healthcare is currently an area with very high added value potential for the Polish economy. The Ministry of Health and the National Health Fund are two institutions that play a key role in this field, which is why it is crucial that the authorities in charge of these institutions are aware of the value of the IoT throughout the Business to Business to Consumer chain.

Selected services and applications of the Internet of Medical Things



Source : https://arxiv.org/ftp/arxiv/papers/1902/1902.00675.pdf ("Characterizing IOMT/Personal Area Networks Landscape"; Effat University; Adil Rajput, Tayeb Brahimi)

Growth prospects for the industry

According to a report by Allied Market Research,[1] the value of the global market for Internet of Things solutions in healthcare will reach $136.8 billion by 2021. Even today the world is using 3.7 million medical devices.

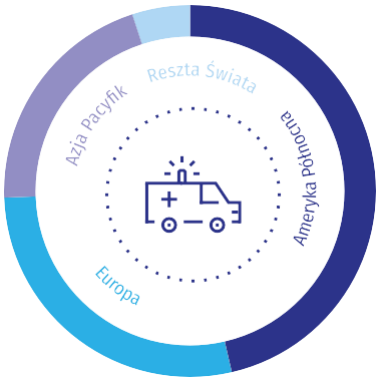
The growth potential of the healthcare sector in terms of the IoT is illustrated by the following data:

- 60% of healthcare providers around the world already use IoT solutions at their facilities;
- By 2019, 87% of healthcare providers will have introduced IoT solutions in services offered in this area;
- The IDC report predicts that 40% of healthcare providers will use IoT biosensors by 2019;
- 80% of healthcare providers reported an increase in innovation thanks to the implementation of IoT solutions;
- According to the report on the state of the Internet of Things[2] released by Aruba Network, 73% of healthcare providers managed to reduce costs by deploying IoT solutions;
- It is estimated that the smart tablet market will grow to $6.93 billion by 2020;

1 https://www.alliedmarketresearch.com/iot-healthcare-market
2 Aruba Network

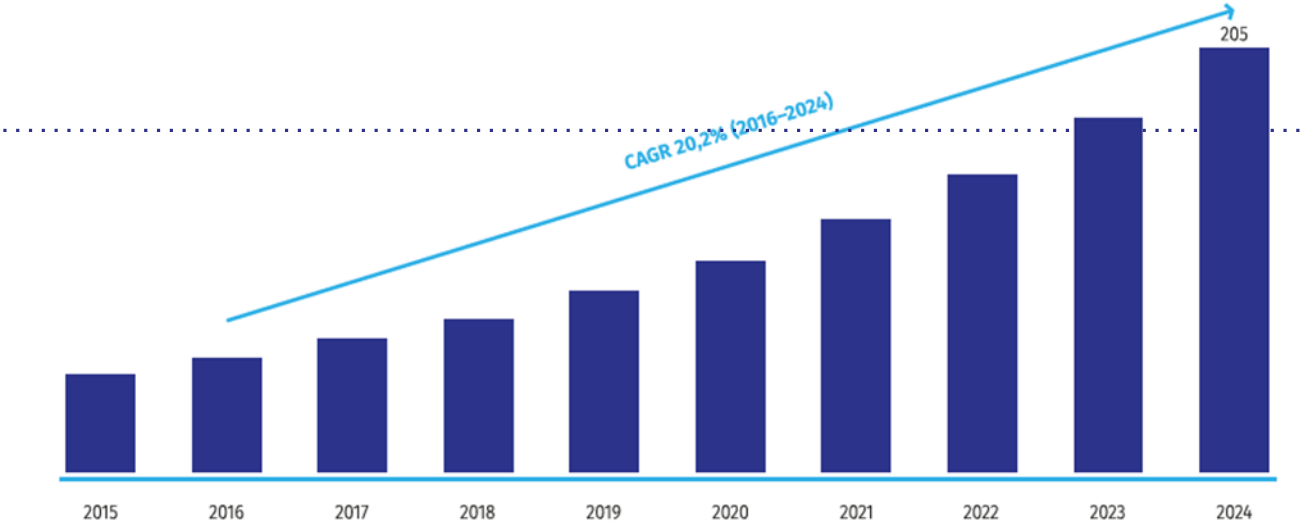
- The most popular IoT solutions in healthcare organisations are used for monitoring and keeping patients in good condition – 73%, as well as for remote surveillance – 50%;
- The IDC report predicts that by 2020, Internet of Things spending will have reached a total of $1.29 billion;
- Global IoT-related spending will amount to $1.4 billion by 2021.

Healthcare market across continents



Source: Variant Market Research

Global IoT market - current state and projections until 2024. (in billions of dollars)



Source: Variant Market Research

Scope of possible use of IoT solutions

Properly implemented diagnostics services and remote therapy solutions based on the IoT reduce treatment costs and improve the quality of medical services.

One of the main aspects is the fact that deploying IoT solutions as part of an integrated emergency medical system will significantly improve survival rates and will reduce the cost of treatment in the cases of injuries, accidents or sudden health deterioration. What is more, properly implemented diagnostics and remote therapy services using IoT solutions can reduce treatment costs and improve the quality of medical services, as shown by the following data:

- Remote doctor's appointments thanks to a cloud-based care system using all IoT tools (personal computers, smart devices, biosensors and access structure) is a new standard, which should replace existing solutions. That is what 70% of the population want today.[3]
- Properly functioning cybernetic systems (cloud-based medical servers based on modern ontology databases) will enable the improvement of the quality of medical services, their unification, and taking advantage of economies of scale.
- Telemedical communication and IoT systems using AI robots will improve patient flow and significantly shorten or eliminate waiting lines to see the doctor, enabling better use of regional medical access points.

3 PwC Report – 12.2016 https://www.pwc.pl/pl/pdf/pacjent-w-swiecie-cyfrowym-raport-pwc.pdf

- In view of direct and indirect costs linked to civilisational diseases (including cardiovascular diseases and cancers), the burden of which is estimated to reach 100 billion PLN by 2030, the use of IoT solutions in diagnostics, therapy and prevention may bring significant savings at every stage.[4]

- The use of IoT solutions by patients enables ongoing supervision of their medication adherence, including in particular ongoing reminders about the need to take the next dose of the medication, easily accessible instructions concerning their medication, combining different kinds of medication therapies carried out at the same time, and noticing interactions between medicines.

The data collected through IoT solutions are used by manufacturers of medicines and medical devices to supervise the use of products after they end up on the market:

- Monitoring the medication adherence of patients via IoT solutions (*wearables*) enables ongoing monitoring of the effects of drugs and identifying possible side effects.

- The deployment of IoT solutions in medical devices enables ongoing monitoring of possible defects, errors in use, as well as incidents that take place while using the devices.

- Data collected through IoT solutions used in medical devices enable manufacturers to take the necessary precautions and corrective actions, even if there is no reaction from the users of the products.

- Data collected through IoT solutions used in medical devices complement the data collected as part of device supervision after its sale. As such, they are used in particular to update the risk-to-benefit analysis of a given device, as well as to improve risk management.

IoT solutions can also improve the well-being of the ageing population, as well as the quality of life for patients:

- Data collected using IoT devices (such as wearables certified for medical uses) can contribute to early qualification for dementia screening (AOTiM does not recommend testing due to the low sensitivity of the existing tests; IoT devices can carry out non-invasive, continuous monitoring of the elderly person's condition and behaviour).

- Shortened time of various medical procedures.

- Cybernetic systems and numerous automatic machines can perform procedures previously carried out by the doctor, as well as those that the patient had to remember and do themselves.

Barriers

Proper deployment of IoT systems and devices in healthcare requires a number of legislative changes, particularly in the area of consumer protection against discrimination, the definition of service provider liability, and the possibility of using non-personal data collected in the public domain. It is also necessary to allow for public funding of IoT-based treatment services.

The use of the IoT in healthcare system (IoMT) is currently at a very early stage of development. It is stifled by rather low awareness of the benefits of the IoT among regulators, patients, doctors and healthcare professionals.

In the course of the work, the sub-group identified the following barriers for the industry:

- Lack of a single standard defining communication between both IoT devices and IoT devices interfacing with external services in healthcare.

- "Smart" medical implants and security of communication interfaces (wireless communication in particular).

- Ethical aspects related to the data provided by IoT technologies.

- Trust in technology (generational differences).

- Lack of public funding for health services provided using telemedical equipment – As of now, only cardiological and geriatric remote consultations are covered.[5]

- Personal data protection and cross-border data flows:

  - one of the most fundamental issues related to the legal aspects of the IoMT is the issue of personal data protection, including data about patients' health;
  - given that this issue is the subject of the work of the Working Party for the Protection of Personal Data, established by the Ministry of Digital Affairs, our team deliberately decided not to carry out any in-depth analyses concerning this subject, opting only to point out key problems related to this area.

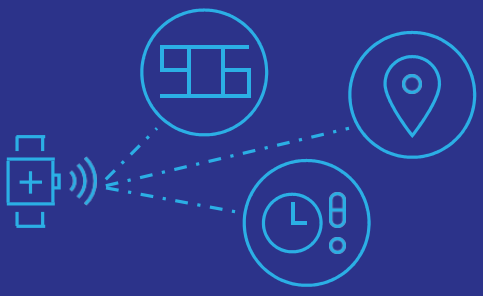
4 http://www.zdrowepokolenia.org/uploads/news/Raport_kpmg.pdf?PHPSESSID=35qu106b0vup9p9i0m980sfkt5
5 http://www.nfz.gov.pl/aktualnosci/aktualnosci-centrali/telekonsultacja-kardiologiczna-i-geriatryczna-finansowana-przez-nfz,6758.html

- The apparent key problems pertaining to data processing are:
  - problems related to personal data processed by IoT systems are regulated by the GDPR – this is a very general regulation which needs to be implemented in a form that would be adapted to IoT solutions;
  - the Act implementing the GDPR does not contain any provisions which would specify the rules of personal data processing in the IoT area, such as the rules of joint controlling of data by equipment suppliers and data recipients;
  - there are no instruments regulating specific rules of action in the area of the IoT – it is recommended to adopt industry codes and introduce certification mechanisms as soon as possible;
  - there are no mechanisms that enable transferring personal data to third countries in line with Articles 44 to 47 of the GDPR – they should be adopted as soon as possible.
- Discrimination linked to the use of data collected using IoT solutions.
  - Data collected by means of medical sensors and other IoT systems, which can be used to precisely determine patients' health condition, can also be used for purposes which are nefarious for the data subject, including discriminatory and exclusionary practices. Even today there are insurance policies available in the United States which offer premium terms in exchange for access to health tracking devices. Some of the issues identified in connection with this area include:
    - offering cheaper services in exchange for providing medical data and biometrics under conditions which make these services the only ones affordable for less affluent groups, thus making this "choice" the only option;
    - punishing people whose habits are perceived by IoT systems as negative, in spite of the fact that these people have no other options due to their family or financial situation (insomnia of a single parent, poor diet of a less affluent person);
    - price discrimination using medical data enhanced by metadata (date, time stamps and geolocation markers);
    - lack of sensor objectivity – it always analyses only a certain scope of data, which may differ from the mean, but in a given specific case and circumstances may not be harmful to the data subject;
    - IoT sensors can collect personal data without the knowledge and consent of the data subjects, as well as generate large streams of continuous data without human intervention, connecting to other devices outside the data subject's control;
    - the opacity of the employed algorithms may result in the unfair categorisation of users.
- The Working Group recognises that existing regulations and laws do not prevent such discrimination:
  - For example, the law implementing the GDPR provides for a wide range of automated processing options, including the profiling of data, including medical data, as well as making decisions solely on the basis of such processes.
  - Apart from sector-specific regulations, there are no laws that can counteract the discrimination described above:
    - Act of 3 December 2010 on the implementation of certain laws of the European Union concerning equal rights defines the areas and means of counteracting infringements on the principle of equal treatment based on sex, race, ethnic origin, nationality, religion, faith, beliefs, disability, age or sexual orientation; thus, as far as it concerns the IoMT, the Act only refers to disability;
    - sectoral regulations are also incomplete – for example the aforementioned insurance sector may not discriminate only on the basis of gender, pregnancy and motherhood, which can be seen in the existing jurisprudence.[6]
  - in cooperation with the Financial Ombudsman, the problem of discrimination and price discrimination should be analysed in order to develop methods of counteracting this phenomenon.

6 http://www.ptpa.org.pl/site/assets/files/1029/wybrane_orzecznictwo_rownosc_kqed_info.pdf

TELEMEDICINE WRISTBANDS IN MEDICAL AND CARE SERVICES

HTTP://SIDLY.EU/PL
POLAND



PROBLEM

An ageing society and a growing number of people who are not fully fit – physically and mentally. A low sense of safety among nursing home residents. Limited trust in local governments and foundations. Time consuming activities related to filling in medical records. A high number of unnecessary visits to doctor's offices, emergency services or ambulance calls. Limited funds and insufficient staffing levels. The need to optimise processes in the care and medical system.

SOLUTION

SiDLY telemedicine wristbands, which enable the automation of medical measurements, detecting falls with the option of notifying the caregiver, include an SOS button, help prevent residents of nursing homes from straying away unconsciously, remind them about taking medication, and allow staff to locate the wristband user.

BENEFITS

Doctors: reduction of time to fill in medical records and documentation by 60%; direct contact with the patient +29%; possibility to see additional patients.

Hospitals: reduction in hospitalisation rates by 35%; 53% fewer ER interventions, number of hospital bed-days down 59%.

Local governments: improved implementation of senior care strategy, improved quality of social services in local government, increased attractiveness and innovation of social policy, increased attractiveness of nursing homes as places of residence for persons requiring assistance, persons with disabilities, seniors and those requiring constant monitoring. SiDLY telemedicine wristbands enable seniors, as well as people living alone who require assistance in their daily lives, to remain in their environment without having to move to a care facility.

Care centres: improved quality of provided services, increased sense of safety of the residents, optimised work of carers, increased competitiveness.

REANIMATOR

APPLICATION FACILITATING HELPING A PERSON IN CARDIAC ARREST
POLAND

PROBLEM

In Poland there are 40 000 cases of cardiac arrest every year. Among people who suffer from cardiac arrest, only 7% survive in Poland, while in the Nordic countries this rate is as high as 40% (according to European Resuscitation Council data). Poles lack common knowledge about providing first aid in such cases.

SOLUTION

The application encompasses two main modules: an Automatic External Defibrillator (AED) location module, indicating where the nearest AED is located and leading the application user to the location using the shortest possible route, as well as a "Virtual Assistant" which guides the user through the whole process of helping an unconscious person. The application can complement the survival chain, which consists of the diagnosis of a cardiac arrest, calling professional help, early defibrillation, as well as emergency medical services carried out by professionals.

BENEFITS

Increase in the survival rate of people suffering from cardiac arrest, and reduction of the financial and social costs of the death of a person of working age. These are estimated by the Social Insurance Institution at about 400 000 PLN. A 1% improvement in survival rate means 400 fewer deaths, which translates into savings of 160 000 000 PLN in the long run. The use of applications (smartphones) and the LTE network coverage in Poland is an indispensable element for improving the operation of the National Emergency Medical Services System.

- there is also a lack of comprehensive regulations concerning discriminatory refusal to provide service – this issue has only been regulated by Article 138 of the Code of Offences and raises doubts (cf. the decision of the Supreme Court of 14 June 2018, II KK 333/17 and the statements by the Ombudsman and Minister of Justice.)[7]

- Use of IoT devices and systems for the purposes of ensuring user rights, law enforcement and public safety;
  - Telemedicine services:
    - remote diagnostics and therapy services, resulting in lower costs and broader availability of medical services,
    - legalised thanks to 2015 and 2018 changes, but still hardly used,
    - it is still unclear whether and when certain services can be provided electronically and when they require an in-person appointment (in 2018, the government amended Article 42 of the Act on the professions of a doctor and a dentist, specifying that the service may be provided remotely after analysis of the patient's medical records, while Article 8 of the Act on Patient Rights and the Patient's Rights Ombudsman requires due diligence in accordance with the professional requirements set out by separate regulations,
    - there are no regulations that would allow for the reimbursement of telemedicine services by the National Health Fund.
  - There are no legal regulations that would enable structural use of IoT systems and devices for:
    - Screening campaigns;

7 https://www.rpo.gov.pl/pl/content/rzecznik-praw-obywatelskich-wyjasnia-jakie-przepisy-obliguja-do-interwencji-w-sprawie-dyskryminacji

- Epidemiological research;
- Using Big Data in medical activities;
- All the actions that are taken in this area are private initiatives. The data collected by these entities are not in the public domain even after their anonymisation, and cannot be used for prevention purposes and preventing epidemics.

- There are no regulations which would stimulate positive health behaviours and which could be monitored by means of IoT systems and sensors (an example of such a regulation is sec. 10408, or the so-called Affordable Care Act (Obamacare)[8]

- Liability of users of IoT services and systems:
  - Polish law does not include any regulation pertaining to the manufacturer's or service provider's liability for their IoT products – this issue is regulated by a number of provisions of the Civil Code, GDPR, the Act on the Provision of Electronic Services.
  - Among the most important problems that should be highlighted in this area are:
    - fuzzy liability when services are linked and data are shared with multiple third parties – it is unclear who is responsible for the breach;
    - lack of clear regulation pertaining to refusal to provide the service;
    - lack of clear regulations concerning the continuation of the service – support duration, scope of licences of subsequent software versions;
    - lack of regulations concerning the scope of security required in IoT devices – it is the user who is the controller of data processed using the devices and responsible for their proper protection;
    - insufficient regulations concerning product information, data processed through the product, and the effects of their use;
    - lack of requirements pertaining to warranties, liability, encryption, etc., especially in regulations between businesses, where it is almost possible to fully exclude the liability of the service provider and, on the other hand, the users may tamper with the product themselves – add data, modify the device, or connect it to other ecosystems,
    - lack of regulations enforcing transparency of data processing algorithms to ensure their accuracy and accountability.
  - There is a general awareness of the fact that EU authorities are working on a new regulation on cybersecurity.[9]

- Use of IoT equipment in the course of court proceedings:
  - There are no provisions governing the use of data contained in IoT devices for the purposes of court and administrative proceedings – they are subject to general rules concerning evidence.
  - Apparent issues and problems:
    - lack of availability of the data, especially when the service provider is processing data outside the country – the parties to the court proceedings taking place in Poland, even the court, will have significant problems with obtaining access to this data, especially when they are encrypted;
    - lack of clear procedures to verify the veracity and accuracy of the data – lack of access to algorithms, lack of experts with appropriate knowledge, no possibility to question the manufacturer as an expert;
    - preference for other sources of evidence (personal testimony, expert opinions);
    - technical limitations of Polish courts – there is no possibility to include data in the court files (especially when they cannot be recorded on a disc or saved on a USB stick), no possibility of displaying the data once disconnected from the IoMT (*Internet of Medical Things*).

8 http://housedocs.house.gov/energycommerce/ppacacon.pdf
9 https://www.consilium.europa.eu/pl/policies/cyber-security/

Proposals for government action

We recommend the following legal actions:

- Supplementing the provisions of the Act on the healthcare information system with provisions on telemedicine and the IoMT, corresponding to the current level of development of this technology.
- Amending legislation, especially in the field of consumer protection against discrimination, liability of service providers, as well as introducing changes allowing for the public funding of medical services taking advantage of the IoT and the use of non-personal data collected in the public domain as part of these services.
- Allowing data from medical devices (thermometers, blood pressure monitors, spirometers) to be added to electronic patient records.
- Adopting comprehensive regulations counteracting the discriminatory use of data, including medical data obtained via IoT systems.
- Introducing regulations enabling the provision of telemedicine services via IoT devices using Big Data and without the intervention of a doctor, especially when it is unnecessary (screening campaigns for healthy people, data collection for epidemiological reasons).
- Introducing regulations allowing the use of anonymous data collected by private entities by the public health service.
- Active involvement of authorities in the work on EU regulations.
- Undertaking work on a legal act, consistent with the EU regulations, governing the liability of IoMT manufacturers and service providers (it can be modelled on the draft US Internet of Things (IoT) Cybersecurity Improvement Act of 2017).[10]

We recommend the following non-legal actions:

- Projects aimed at educating school students, concerning leading healthy lives – providing information to their parents / grandparents ("tell your parents" campaigns) concerning devices / applications that can be used in disease diagnosis / health monitoring.
- We recommend preparing plans geared towards educating the general public on the use of devices / systems supporting EMS processes.
- We also recommend preparing plans concerning the education of medical professionals, pharmacists and patients, devoted to the use of IoT devices and the opportunities opened up by their use.
- Incentives and training for doctors regarding using data made available to them by patients, including data from health monitoring devices / applications.
- Health insurance premiums discounts / discounted prices of reimbursed medicines for people who constantly monitor their health and transmit health data to electronic medical records.
- Enabling public funding of telemedicine services.
- Introducing clear procedures that would clarify the issue of the admissibility of telemedicine services.
- Launching pilot projects by the Ministry of Health, taking advantage of the possibilities offered by IoT technology. The solutions that offer the greatest benefits in terms of: savings, use of existing infrastructure, effectiveness of prevention and treatment, or the greatest potential for use in other services provided by the state, should be implemented on a larger scale in the first place.
- Establishment of a special purpose public fund (e.g. within the National Health Fund) supporting (subsidising) the implementation of Polish innovations – IoT solutions for the medical sector developed in Poland.
- Introducing new regulations concerning the certification of devices, applications and systems supporting first aid, qualified first aid and EMS activities.
- Selected Health Policy Programmes of the Ministry of Health (for example preventive ones) should be complemented by opportunities for promoting and using IoT solutions, for example:
  - the Cardiovascular Disease Prevention and Treatment Programme (POLKARD for 2017-2020);
  - the Comprehensive Care Programme for People with Heart Failure (KONS), in order to enable non-invasive monitoring of the health and/or activity of persons in risk

10 https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?q=%7B%22search%22%3A%5B%22S.1691%22%5D%7D&r=1

groups (which would allow a lowered number of hospital stays and visits to outpatient facilities). This should particularly concern the elderly, often deprived of ongoing care, as well as geriatric patients (over 70 years of age), where the aim of the healthcare system is to ensure the longest possible welfare at home;

- The implementation of the IoT in senior care, financed by local governments, will improve operations in the sector and increase its efficiency while maintaining operating expenditures;
- Services provided by suppliers should be compliant with the HL7 protocol;
- Transmission of telemetric data used for the purpose of EMS operations should be excluded from the need to obtain consent for the processing of specific personal data;
- It would also be worthwhile to introduce rules enabling the prioritisation of communication channels for devices, applications and systems operating in emergency rescue mode.
- It would be worthwhile to include the ability to send a video stream from the incident site to the control room / rescue team in the Command Support System of State Medical Rescue Services;
- Another recommendation is to create a national register of AEDs (formal requirement). Such information could be fed to the GUGiK dataset. This repository could be used as a source of data for current and future IT solutions;
- It is recommended to set up a national register of persons who are trained qualified first aid providers, which can be useful in crisis situations;
- It is recommended to introduce and apply a standard for the extensive reporting of adverse reactions by medical professionals and patients;
- The primary and secondary prevention systems concerning many diseases could be extended to reduce the risk of illness resulting in reduced quality of life, absenteeism and disabilities;
- Diagnostics based on (or supported by) IoT solutions can support the updating and development of Health Needs Maps by the Ministry of Health;
- It is recommended to allow the data collected by IoT solutions to be used for reporting adverse reactions and for epidemiological purposes;
- It is worth considering the selection of parameters of customised medicine for individual patients, which will allow health service providers to optimally determine health profiles and ensure better and longer life. They would be determined and then monitored by biosensors;
- The use of IoT solutions, financed at national (prevention programmes) and local (senior care) levels will increase the safety, well-being and independence of older people, especially those:
  - without constant care at home;
  - whose condition does not require hospitalisation, under 70 years of age;
  - who are not struggling with comorbid diseases (weakness syndrome, depression, Parkinson's disease, dementia, falls).

12

SMART METERING

The best way to predict the future is to create it.

— Abraham Lincoln

AUTHORS:
KRZYSZTOF WADASM CYFROWY POLSAT GROUP – SUBGROUP LEADER
JERZY GREBLICKI, AIUT SP. Z O.O.
RADOSŁAW KOTEWICZ, COMARCH S.A.
RAFAŁ KOWALSKI, DEIHL METERING SP. Z O.O.

General characteristics of the sector

The industry is increasingly aware of the benefits of linking IoT solutions with AI, BI and Big Data. More and more companies are building their own competencies in these areas, and the first pilot implementations are already taking place, making real use of IoT technologies (IoT devices, IoT applications and data transfer using new technologies). There is also a growing awareness among end customers of the possibility of using the data to optimise their household expenses, thanks to electricity, water or gas consumption patterns. Data collected from IoT meters in the industry sectors will be made available online on customers' smartphones.

Polish companies operating in the sector analyse the available data transmission technologies – NB-IoT, CAT-1M, LoRaWAN, Sigfox – in trial implementations and explore them in terms of their usefulness for future implementations. International data show that global IoT implementations in the energy sector and broadly defined utilities grew by 36% in 2019.[1] In Poland, we can safely say that the years 2019-2021 will be marked by significant growth when it comes to the IoT, as we are going to see the first major implementations.

Challenges for the industry include: securing against over-regulation, which stifles Polish innovation in this area, outdated power grid and misunderstanding the benefits of using new technologies in local government (it is necessary to develop and publish the "Polish Lexicon of Internet of Things Concepts"), dependence of decisions concerning investing in products and services on the availability of communication infrastructure (no state-driven efforts to build operator services / develop infrastructure through real interest in IoT projects in state-owned companies).

Growth prospects for the industry

At the moment, the Working Group sees a very good opportunity to increase the contribution of the IoT and AI sectors in Poland's GDP. This requires support for the development of unknown Polish global champions. References, even from small projects in Poland, can be a springboard for expansion abroad. It should be pointed out that the main goal here is not to dominate the local market – instead, we should strive to go global (EU, US, Asian and Middle East markets), which will bring about an increase in the competitiveness of Polish companies, which in the long run translates into the growth of the country's GDP. Poland already has local companies which are successfully expanding their IoT businesses.

Poland also has a chance to be a kind of a European IoT Hub, which can provide IoT devices, applications for IoT services, as well as the certification of Polish and international IoT devices for the EU market (faster and more effective certification of products in Poland which will be sold in the EU). This certification of IoT equipment for the energy and smart metering sectors will result in new revenue sources. In addition, we should assume openness to new technologies and standards, as well as ensure the transparency of solutions and openness of adopted technical solutions, including their protocols. Openness towards new technologies, supported by experience and knowledge management, will enable the creation of a "Book of Good Practices for the IoT", which will translate into faster public deployments, as well as implementations in the industry and the consumer market. This will result in the reduction of technical risks, presenting an effective methodology for running IoT projects, proposing a quality plan with a division of responsibilities between supplier and buyer, along with proposals for minimum (unmeasured) safety requirements.

1 Vodafone IoT Barometer 2019

Scope of possible use of IoT solutions

Actual projects and statistics from abroad show that the implementation of smart meters is done mainly to measure consumption (67% of implementations abroad) and to monitor companies' infrastructure – 75% of implementations use these solutions to monitor security.

In Poland, utilities also see the benefits of the IoT – examples include waterworks companies, which want to use IoT solutions to quickly detect leaks (large water flows from defective pipes). Implementation of IoT solutions results in tangible benefits for companies (process optimisation, faster data transmission and analysis, network security monitoring), as well as for end customers (better knowledge of water, energy or gas consumption). It should be noted that the implementation of remote meter reading significantly extends the possibility of implementing metering solutions in facilities where the existing technology is not economically viable. One of the most prominent examples is the metering of gas meters for individual customers using the W1-W3 rates, enabling remote reading of home gas meter indications, operation of pre-paid gas meters, and operation of debt collection gas meters. Furthermore, it is possible to measure the pressure in the distribution network and monitor subnetwork terminals (for most remote recipients) in order to assess the quality of the service (availability of gas at an adequate pressure). Such solutions can contribute to the improvement of safety, thanks to identifying faults by means of monitoring the cases where working pressure alert thresholds in transport networks (medium and high pressure) are exceeded, as well as thanks to metering home gas / carbon monoxide sensors at the end user's location. The development of IoT technology may also facilitate the implementation of intrinsically safe solutions (for use in explosive atmospheres) – in particular given the low energy consumption of IoT solutions, and thus more efficient use of battery power sources than ever before.

In addition, infrastructure based on dedicated telecommunication solutions for metering (SigFox, LoRa) can be used more widely as a mass communication platform for IoT devices, as well as an alternative to currently available solutions (GSM, LTE).

NRW – Non-Revenue Water

Non-revenue water means the difference between the volume of water produced and pumped into the network and the volume that is not delivered to the customer during the distribution process, and therefore not invoiced in any way. This may be due to many factors such as leaks or illegal water use, but also due to maintenance work carried out by companies on networks.

SMART METERING IN WATERWORKS – SOLUTION IMPLEMENTED BY MPWIK IN PIEKARY ŚLĄSKIE

POLAND

PROBLEM

The Municipal Water Supply and Sewerage Company (MPWiK) in Piekary Śląskie wanted to monitor their water meters on an ongoing basis and reduce data transfer costs within the city.

SOLUTION

A project based on LoRa transmission technology developed by a Polish company AIUT, based in Gliwice. The solution for MPWiK, which has been operational since July 2018 and which is constantly being developed, is a system which enables remote reading of water meters in the city. The system consists of LoRa Kerlink network antennas, which make up a separate network in the city. They enable the reading of more than 6500 water meters within the city.

BENEFITS

Reducing the cost of data transfer in the city and minimising losses. Using hourly readings or daily device checks allows for quick detection of leaks at customers' locations and identifying cases of illegal tampering. With a LoRa network covering the city, the company can easily expand the metering zones and monitor pressure in the water supply system. The antennas, which are installed throughout the city, can also easily connect with other types of devices, for example for measuring heat meters or controlling the number of free parking spaces.

On the basis of the Water Law Act of 20 July 2017, the State Water Management Company Polish Waters was established as the central institution managing national water management, while the National Water Management Board and regional water management boards became organisational units of the Polish Waters company.

As a result, the interest of water management companies in solutions to minimise their costs of producing non-revenue water has increased rapidly. In order to enable the reduction of such costs, it is necessary to monitor and balance water consumption in District Metered Areas. Additionally, a knowledge of network topology and pressure is also required.

IoT communication technologies can contribute to the acceleration of the implementation of the NRW strategy by Polish waterworks companies and have a significant impact on increasing their efficiency (for example by ensuring more frequent collection and transfer of measurement data for further processing without the need for additional investments, as well as maintaining their own communication infrastructure).

SMART METERING – A SOLUTION USING THE NB-IoT NETWORK

UNITED ARAB EMIRATES

PROBLEM

Access to drinking water is a common problem in the United Arab Emirates, which requires rational infrastructure management. The local water and energy company in Dubai has asignificant number of water meters distributed throughout the country, 2-8 meters below ground level. Traditional water, electricity, gas or heat meters require manual reading of data, which generates high maintenance costs and results in gaps in current flow information and alarms.

SOLUTION

Remote meter reading. In early 2019, in partnership with the local mobile network operator, the company installed 500 M-Bus - NB-IoT modules supplied by COMARCH. By using the NB-IoT communication standard, the device provides increased (compared to other GSM technologies) network coverage and low power consumption, allowing up to 12 years of battery life. Thanks to its IP68 housing, the device is resistant to flooding during heavy rains in the desert.

BENEFITS

Reduced costs generated by manual meter reading by employees. Real-time monitoring of the condition of the water supply network allows for early prevention of water supply failures. The solution does not generate additional costs because it does not require the replacement of existing infrastructure – Comarch M-Bus – NB-IoT modules provide long-range wireless communication.

Over-regulation is the greatest threat to the energy and utilities sectors. Regulations should ensure openness, eliminate restrictions, and at the same time prevent the establishment of monopolies, restrictions on the creation of new communication standards, as well as blocking the introduction of new technologies. Today, we are witnessing a true technological revolution in the IoT industry – the fewer legal or procedural restrictions there are, the faster new technologies based on immature solutions can be commercialised. We should base our approach on American corporate freedom.

The subgroup believes that all attempts at centralising data access processes need to be approached with due care and caution. Time-consuming procedures for accessing information can significantly stifle innovation in the industry and the motivation to quickly respond to changes.

Another barrier is the availability of B2B and public domain communication services. Popularisation of NB-IoT or LTE CAT-M networks depends on the strategic and investment decisions of existing telecommunications operators. Currently, commercial rates for these services are unavailable, which fundamentally limits the possibility of building economic models for offering services, leading to stifled investments in the development of hardware applications. It seems that one of the reasons for this state of affairs is the lack of agreement between the operators concerning creating a plan for the implementation of particular technologies in Poland, and the dependence of such a strategic decision on the strategy for the entire capital group of a given operator. Often such decisions are made abroad.

Other IoT technologies, such as LoRa or SIGFOX, require private investment in infrastructure development, and only a portfolio of long-term and volume contracts can prompt such a decision. Thus, state-owned companies should become one of the key market players stimulating this development, in particular those operating across the country, whose role would be to implement IoT investment projects.

Such projects should support the possibility to diversify suppliers so as not to lead to monopolisation of suppliers of innovative solutions, which – instead of stimulating innovation and development – locks the market up for many years. This is particularly important in sectors where public enterprises hold a dominant market share.

Proposals for government action

Openness of standards is the key to the development of the IoT in Poland, which can be interpreted as full transparency of data exchange methodologies across all layers, which is guaranteed by law. In this model, any implementation of IoT solutions would require the provision of both the solution itself, along with comprehensive and non-confidential documentation for the contracting authority, with ensured availability to other entities. Such an approach will provide virtually unlimited opportunities for integration for both small local and nationwide projects, and will foster innovation based on combining heterogeneous solutions. This openness will also translate into increased security, owing to open access to protocols, where security is based on widely used cryptographic methods rather than the secrecy of the protocol itself.

Recommendations for best practices in IoT projects will eliminate procedural errors in the supervision of innovative projects. The current tendering procedures focus on technical details instead of assessing the performance and quality of the presented solutions. The SLA model, where the supplier guarantees quality under pain of contractual penalties, provides the buyer with investment security. This gives the supplier greater freedom in the choice of technical means to achieve the assumed objectives.

In order to ensure the quality and support of projects implemented by local governments, a list of best practices should be developed, along with a standardised glossary of terms concerning the IoT area. Polish companies, representatives of academia and lawyers, together with the support of the Ministry of Digital Affairs, should prepare and publish the “Polish Lexicon of IoT Concepts”, which will be used in tenders and purchases based on Public Procurement Law, as well as commercial ones. It will constitute a real transfer of knowledge and information to local governments.

In the case of IoT devices, regulations should be replaced with well-defined procedures for the assessment of quality measurement and approvals. It is possible to introduce voluntary quality certificates issued by commercial entities based on general conditions, common to all players – this could be done by telecommunication operators, which would potentially increase the credibility of the solutions in question.

13

INDUSTRY

In the coming years, industry will become one of the sectors that will take the greatest advantage of IoT technologies. The growth of the Polish economy depends on innovation and the ability to implement new solutions. Emerging barriers or lack of effective support may stifle its dynamic growth.

AUTHORS:
KAMIL NAWROCKI, BCONNECT – SUBGROUP LEADER
SZYMON BONIECKI, MONTERAIL
DARIUSZ GOŁĘBIEWSKI, PZU LAB S.A.
DARIUSZ NACHYŁA, EVERY EUROPEAN DIGITAL
TOMASZ SERAFIN, AIUT SP. ZO.O.
BOGDAN ŚLĘK, SIGNIFY POLAND SP. Z O.O.
JAROSŁAW WIDÓREK, COMARCH S.A.
TOMASZ ZALEWSKI, BIRD & BIRD KANCELARIA PRAWNA

General characteristics of the sector

As a sector, industry has a long history of taking advantage of technology to optimise manufacturing and logistics processes. The operational specificity of these processes – with their large volumes, high downtime and breakdown costs, as well as high initial cost and long depreciation periods for machinery – makes this sector highly focused on issues concerning optimisation of performance and reducing operational risk. At the same time, nowadays, this sector faces new challenges:

- shortening product life cycles;
- fluctuations in demand, which require more flexible cycles in production processes and logistics;
- the trend of transforming products into intelligent services, making elements of the IoT concept appear in the product architecture and leaving their impact on the nature of manufacturing processes.

The emergence of new product categories allows for building a production capacity that can fully exploit the emergent potential of new technologies (for example Tesla's Gigafactory concept). As a result, the world's manufacturing and logistics companies are facing the need to undertake transformative actions, the framework for which is defined by the Industry 4.0 concept.

Poland has a number of medium and large companies, in particular in the power and fuel industries, heavy industry, as well as the electrotechnical, automotive, furniture and other industries. They demonstrate varying readiness to invest in new technologies, automation, and production process control. Barriers to modernisation in the spirit of the Industry 4.0 concept include, on the one hand, a lack of knowledge, a lack of benchmarks, and uncertainty about the economics of investments related to the digital transformation of industry. On the other hand, there is increasing pressure to take these measures. Polish companies that partner with global automotive companies see the need to adapt to a new class of processes and operational requirements concerning response times, flexibility and quality. Companies that successfully export their products also often face the need to adapt them to the realities of digital business and lifestyle. The most difficult circumstances concern local medium-sized companies. The inability to take advantage of economies of scale makes modernisation investments ineffective and increases the uncertainty of decision making. However, these companies also experience pressure (in the form of difficulty with attracting staff) and see opportunities (EU funding) that can lead to growing interest in the capabilities of the Internet of Things, especially in the context of production automation and intra-logistics.

On the other side of the market, technology companies in the field of the Industrial IoT (IIoT) and innovative technologies are developing dynamically and are ready to adjust, develop and deploy their best products in all industries, wherever they are required or useful. It is worth noting that there are Polish companies, such as Design House, which provide design and manufacturing services for dedicated electronics, as well as emerging companies creating intelligent systems for intra-logistics based on their custom autonomous self-guided vehicles and robots.

There are also many research centres and universities in Poland which carry out research in the area of the Industrial IoT, AI, Virtual Reality (VR) and Augmented Reality (AR), machine learning, Big Data, as well as User Experience, which can actively support the development of the IIoT.

Growth prospects for the industry

Modern industry is the growth engine of the economy from both global and local standpoints. Countries that cannot expand in this area are doomed to be marginalised in the global market. Most companies in the industry are open to launching new industrial plants with hardly any regard for national borders. This creates a number of opportunities for capital and technology migration between markets. The key opportunity to attract investments and develop existing ones is to have stable legal regulations, as well as human resources, preferably with industry-specific competencies. The cost of operations in a given country is still an important factor – Poland is still attractive in this respect, but there are many indications that the level of costs in EU countries will gradually level off, which is a threat to the continued high demand for investment and development in our country. The operational activity of companies is strongly dependent on the logistical capacity and availability of suitable roads, railways, ports, as well as cargo and passenger airports – this translates into the need to involve state authorities in proper planning of infrastructure development, taking into consideration the needs of industry, which often requires specific solutions (high capacity, tonnage, etc.). Infrastructure investments should also take into account ensuring stable energy supply (in particular the availability of adequate connection power and grid reliability) and the existence of adequate ICT networks (high bandwidth and reliability of radio and fibre-optic cable connections). Industry is facing increasing barriers concerning environmental regulation. One of the most significant challenges faced by the sector is the need to conform with the increasing number of environmental regulations, which often do not take into account the interests of industry.

FUELPRIME SYSTEM – THE IOT IN THE FILLING STATION NETWORK

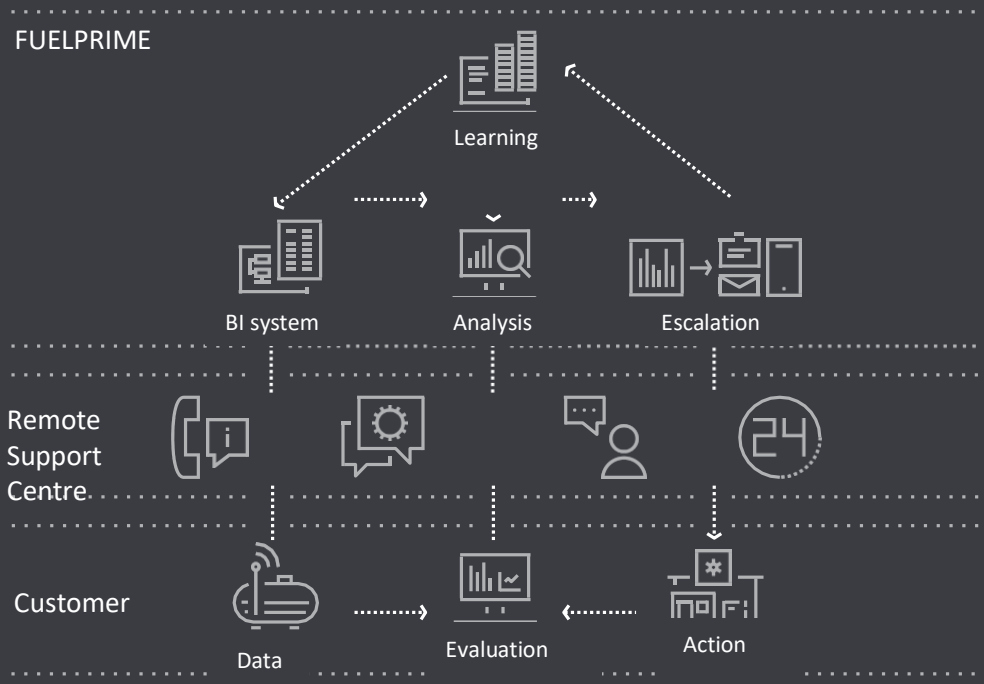
EUROPE / POLAND

PROBLEM

Large losses resulting from sub-optimal organisation of the fuel distribution process from the refinery to the end customer.

SOLUTION

The FuelPrime system implemented by Shell stations in Poland. The system enables the control of liquid fuels at each stage of distribution, comparing the differences that appear in the transfer process, and monitors the process of customers purchasing fuel from dispensers at filling stations.



Each fuel terminal, tanker and filling station is equipped with dedicated sensors and data concentrators. A central management system and helpdesk have also been developed. AIUT provides a comprehensive service – from the manufacturing of devices, through installation, to 24/7 system operation. High efficiency has been achieved thanks to accurate sensors designed with fuel measurements in mind, as well as a method based on the analysis of large data sets – Business Intelligence (BI). The FuelPrime server enables both the analysis of current data and access to historical data, and sends e-mail or SMS notifications about critical situations, which include attempts to tamper with equipment, or an unpredicted fuel outflow. FuelPrime sensors are vandal-resistant and certified for use in hazardous areas.

BENEFITS

- Full control over the fuel level – the system allows users to predict the need to order fuel deliveries;
- Reduction of operational risk – practical elimination of liquid fuel losses (the solution implemented by Shell resulted in the reduction of losses to the level of only 5 litres/24h across Poland).
- Delivery management (confirmation, monitoring) – elimination of unnecessary deliveries.

In general, industry is one of the most technologically advanced sectors in the world, which has been undergoing automation and robotization processes for least 60 years now. However, these days it is far less susceptible to innovation than, for example, the IT industry, which is now the main focus of innovation giants. This leads to difficulties in the implementation of innovative solutions, especially when new methods or equipment are related to safety in the manufacturing halls or enable external access to production data (for example as a result of opening industrial ICT networks up for the IIoT). Therefore, promotion activities showcasing the benefits of implementing innovative solutions are crucial in this regard. This should be an area of particular focus for the government in cooperation with companies (conferences, joint work on standards, academic publications, articles in industry magazines). The term *Industrial Internet of Things* has only existed in the English Wikipedia since May 2017, and has only had 5000 hits since its creation, which clearly shows the need to promote the term within the industry.

Polish companies are becoming more and more global. Apart from maintaining their own plants in the country, they make efforts to open their branches not only in countries with developing economies, but also in countries such as the USA and Germany. This promotes technology exchange and knowledge transfer to these organisations – and this also includes the IIoT.

Scope of possible use of IoT solutions

The Industrial IoT should be divided into two types from the very outset:

- Offline IIoT – solutions that support the collection of sufficiently large amounts of data and allow for their subsequent processing in order to optimise processes. As such, they do not affect the ongoing operation of industrial plants until the effects of data analysis allow for changes;
- Online IIoT – tools and systems that work operationally and influence the operations of an industrial plant on an ongoing basis.

In many cases, the implementation of the IIoT system allows users to run online and offline tools at the same time, and in many cases these functionalities tend to be intertwined. However, it should be noted that access to offline data may be difficult in many situations due to the risk connected with collecting industrial data, as well as the need to invest in computing power and appropriate software for big data analysis.

The basic task of IIoT systems is to optimise industrial processes, starting with efficiency of operations, up to consumption of raw materials and resources. In reality, this all boils down to the reduction of risks and operating costs.

The first important element is the logistics chain. Collecting information about the exact time of delivery of goods required for production and potential delays allows the companies to react almost immediately and deal with problems, for example by changing over the production lines. Such possibilities are provided by vehicle location systems linked to a central production management system, thanks to which truck drivers can report failures and delays directly from their vehicle in real time.

If the industrial plant in question already has had the required components delivered, they must be properly stored and distributed inside. This purpose may be served by systems gathering information about shelving unit space, as well as by running autonomous pallet trucks to pick up the material from the warehouse and deliver it to the right line just in time, taking into account the optimal path through the production hall. Historical information concerning shelving unit occupancy enables the companies to carry out offline analyses and decide on the need to expand or reduce storage space, depending on the activity at the time.

Every package, every autonomous or manned vehicle and all employees should be located on site. This is what IIoT location systems are used for, as they allow companies to keep track of every moving object in the factory. Thanks to such systems, traffic operators have an overview of the situation in the plant, which allows them to properly respond to crises. The analysis of offline data from the location system enables optimisation of employment, modifying transport routes in production halls and much more.

In order to further improve the functioning of plants, it is necessary to keep environmental parameters – such as temperature, humidity, dust level, etc. – at an appropriate level. This enables proper management of employee breaks and machine maintenance, as well as carrying out predictive maintenance. if the supervisor sees, for example, an increase in humidity in a given area of the hall, they can send a serviceman who will turn the machine off, change its operational parameters or detect the failure of another machine, which may affect its operation, for example a water supply failure.

Controlling all environmental parameters is also linked to the concept of smart buildings – energy management in industrial plants is key to reducing their operational costs, and the most typical example of IIoT applications in this field is smart lighting based on twilight and movement sensors.

By collecting data from any online IIoT system, a number of offline analyses can be carried out, which can lead to further savings and optimisation, for example analysing employee movements around the hall enables planning things like removing some of the lighting or reusing less frequented paths as storage space (taking into account health and safety rules, which can also be considered by mathematical models).

Modern manufacturing companies that want to implement Industry 4.0 concepts use IIoT solutions mainly to obtain an accurate analysis of data from devices that communicate with each other in real time (Online IIoT). Company resources, manufactured goods, data, market and customers represent an ecosystem that requires efficient means to access and exchange information.

In the case presented below, the aim is to create an IIoT ecosystem for solutions which are characterised by broad scalability, both in terms of hardware, as well as software.

The IIoT platform may be the main component of this ecosystem. By connecting the IIoT platform with network components such as IoT hubs, signalling devices and RFID tags (transmitters), it is possible to ensure real-time communication and data collection from machines and sensors. This ensures the control and continuity of access to data throughout the entire production chain, from communication between devices, through the assembly line, to the management processes and distribution of products to the customer.

Source: Comarch SA

Among the most spectacular IIoT applications for the future are VR and AR. VR enables the virtual training of staff on the basis of visualisations of machines or even entire plants with virtual assistants. AR is a tool which can serve, for example, service technicians who can walk around the factory wearing glasses with a built-in display, and when they approach a given machine they can receive full diagnostic information and a virtual repair manual should the need arise.

The IIoT sector opens up new opportunities for industry – the manufacturing process of IIoT devices is often based on innovative solutions, thanks to which the experience gained during the process can serve as a model for industrial plants operating in other sectors.

Barriers

The barriers should be subdivided into two categories:

- internal – related to procedures in production plants;
- external – related to the development and growth of the IIoT market.

Internal barriers are related to the high level of regulation in every industrial plant. Given the circumstances of the Polish market, most industrial plants are owned by companies with foreign capital, which results in the fact that their corporate and global procedures are very often imported from abroad. Hence, it would be necessary to demonstrate high efficiency in the implementation of innovations which can provide opportunities for expansion into global markets, as local plants can transfer technology to facilities in other countries.

PRODUCTION PROCESS OPTIMISATION THANKS THE TO IoT

SWITZERLAND

PROBLEM

The Swiss company ABNOX manufactured short product series using manual assembly processes, which generated very high losses and high production costs. Insufficient control of the production process and printing paper manuals for employees caused considerable management problems and prevented a proper quality control process. The client did not consider buying new equipment, which is why it was necessary to carry out retrofitting and use the existing infrastructure which was already in place.

SOLUTION

At ABNOX, Comarch experts have implemented Industry 4.0 IoT solutions, integrating the production process with the Comarch ERP system, while equipping the production line (and its individual components) with detectors recording the status, sequence and time of each stage. Additionally, special screens were added which are used to inform employees about the order of performed tasks and detailed assembly instructions, which led to abandoning paper production documentation. Additionally, an Integrated Manufacturing Execution System (MES) was implemented at the client's site which enables real-time data collection and analysis, ensuring full control over the manufacturing process.

BENEFITS

Thanks to the Comarch IoT solutions installed at the plant, the client managed to automate part of the production line operations (including a laser marking machine), and shortened production time, which enabled them to increase the number of produced variants of their devices to more than 100, drastically reducing the number of employee mistakes and the learning curve for new staff. The new implementation reduced production work by 50%, and the solution implemented by Comarch allowed the company to effectively control all stages of the production process, eliminating the cost of purchasing new equipment and modernising the older system at a lower cost. Currently, the production data collected by the system are used for business analysis and for further process optimisation.

External barriers are a development issue related to the possibility of finding a suitable IIoT system contractor. Many companies have IIoT software, but they find it difficult to provide an adequate volume of physical devices, and adapt them to often difficult industrial conditions. Given the circumstances in Poland, supporting local manufacturers who are able to provide supplies to the Polish market would be important in order to give them a chance for global expansion – for example in the market of specialised sensors or location systems for industrial plants.

The development of the IIoT will also require stimulation of the public sector. Companies in this sector should open up to IIoT implementations, for example as a result of deregulating the procurement of innovative systems.

This concerns in particular a number of sectors subject to public procurement law such as mining, airports and sea ports, power generation, as well as rail transport. Due to their innovativeness, the implementation of IIoT solutions requires the inclusion of elements promoting innovation in the public procurement process. Unfortunately, current practice in Poland does not promote this kind of conduct. In Poland, it has long been said that public procurement should promote innovation. In April 2008, the Council of Ministers adopted the document "New approach to public procurement. Public procurement and SME – innovation and sustainability." There have also been a number of studies, reports and surveys indicating the need for a pro-innovative approach to public procurement.

However, these measures have not led to a significant change in this respect. Certainly, one of the reasons was that support for innovation was a rather low priority in terms of issues with Polish public procurement. In recent years the Polish public procurement system has been struggling with other fundamental issues, such as changing the approach to criteria for evaluating tenders and moving away from using price as the only deciding factor. Other issues included the formal nature of the process and the restrictive approach of the inspectors to any non-standard solutions used by the contracting authorities. There are, of course, examples of innovative Polish public procurement, but they are exceptions to the rule.

Proposals for government action

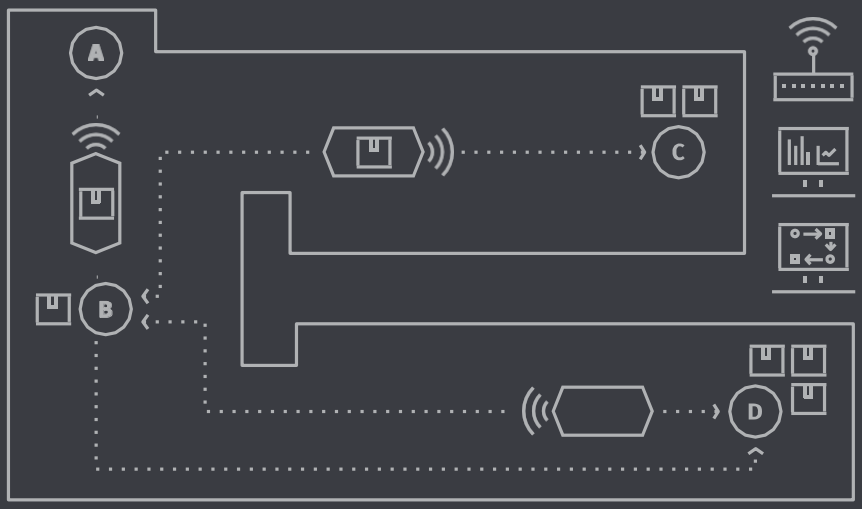
The Working Group recommends the following actions:

- Developing the National IoT Development Strategy for Industry.
- Increasing the effectiveness of using EU funds for R&D projects.
- Increasing the involvement of the public sector in high-risk investments in the area of new technologies, for example by facilitating running pilot projects with new solutions.
- Continuously supporting the growth of small and medium-sized technology companies, including start-ups, for example through dedicated Polish Development Fund programmes.
- Actually supporting SMEs to enable a real knowledge transfer from academia to business through technology companies, as well as to facilitate the exchange of information and demand to develop strategic projects in the IIoT area.
- Developing mechanisms, clear and unambiguous standards, as well as verified and accepted templates for public procurement documents, enabling purchasing innovative technologies.
- Actively promoting innovative procurement and shaping guidelines for the inspection of innovative procurements, so that formalistic control mechanisms do not cause reluctance of the ordering parties to purchase innovative IIoT solutions.
- Equipping contracting authorities with tools in the form of descriptions of best practices for innovative public procurement and pre-commercial procurement. Pre-commercial procurement is an R&D contract co-financed by contractors that has the prospect of being commercialised and then covered by public procurement. Thanks to pre-commercial procurement, the public sector could significantly support Polish industry developing IIoT solutions and give it the opportunity to develop innovative products that could then be offered on both the domestic and global markets.
- The cooperation of all stakeholders (industry, technology companies, research centres, universities) within the framework of the Industry Platform of the Future Foundation in the context of the Strategy for Responsible Development. The first and most urgent objective of the recently established Industry Platform Foundation should be the promotion of Industry 4.0 by raising awareness of the need for digital transformation, as well as transferring experience and knowledge to potential partners. In order to ensure the full effectiveness of the Foundation's activities, it is necessary to actively involve the largest possible number of representatives, in particular business ones, in the Foundation's initiatives, especially given the fact that to date interest has been lukewarm at best, as evidenced by low participation in the public consultation of the draft law on the Platform (out of 85 invited entities, only 8 took part). The German "Industry 4.0 Platform" may serve as an example in this area, as it brings together the activities of different industrial circles, organises different forms of application of technological solutions in industry thanks to deployment scenarios, establishes a common reference framework, and prepares studies and surveys concerning topics related to the development of Industry 4.0. The platform encourages cooperation by sharing information about the opportunities for joining various working groups and sub-groups, as well as about opportunities to share implementation experiences with other enterprises by sending information for publication on the implementation map.[1]

1 https://www.plattform-i40.de/I40/Navigation/Karte/SiteGlobals/Forms/Formulare/karte-anwendungsbeispiele-formular.html

ROBOTISATION OF INTRALOGISTICS AUTONOMY@WORK

POLAND



PROBLEM

Intralogistics processes (ensuring the flow of materials and components between production stations, warehouses and logistics buffers) are an important element of manufacturing processes. Despite the fact that robotisation of manufacturing activities has a long tradition in industry, intralogistics processes are still carried out by simple automation – conveyor belts, forklifts and transport equipment, which requires manual operation. The existing solutions cannot keep up with the needs of Industry 4.0, which requires increased flexibility of production lines due to the variability of cycles, product ranges or configurations. Accidents at work involving workers, which generates additional costs associated with production stoppages, investigations and compensation processes, are yet another problem.

SOLUTION

Intralogistics systems based on autonomous mobile robots (AGV / SGV), devices capable of independent navigation in the dynamic environment of a modern factory, adapted to typical transport tasks and integrated with production management systems. Such a solution is offered, among other companies, by the Polish company VersaBox. The VersaBox intralogistics platform uses mobile robots designed and manufactured by the company, and certified to conform with the applicable safety standards. Pilot implementations verifying their suitability for real production system conditions took place in manufacturing plants supplying components for the automotive industry and are now being implemented in further factories. The TRUE AUTONOMY® navigation system developed by VersaBox experts is also used to “autonomise” specialised equipment provided by third parties.

https://versabox.eu/smart-intra-logistics/

BENEFITS

Reduction of the number of accidents, improved production line operation and, consequently, lower production costs.

14

AGRICULTURE AND ENVIRONMENTAL PROTECTION

The use of the Internet of Things in agriculture and environmental protection can help with solving important civilisational problems, such as production optimisation and improvement of food quality, monitoring of changes and phenomena in the natural environment (such as smog, droughts, water pollution), as well as ensuring support in taking appropriate measures.

AUTHORS:
MARCIN PŁÓCIENNIK, INSTITUTE OF BIOORGANIC CHEMISTRY OF THE POLISH ACADEMY OF SCIENCES, POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER (PSNC) – SUBGROUP LEADER
JERZY BIAŁOUSZ, INVENTIA SP. Z O.O.
RAFAŁ MAŃKOWSKI, POLISH CHAMBER OF INSURANCE
MICHAŁ MISIEK, AIRLY SP. Z O.O.
TOMASZ RAJTAR, IBC PAS, PSNC

General characteristics of the sector

Agriculture increases the efficiency of its production by using modern ICT technologies to collect, process and analyse data, as well as by automating processes in order to optimise farm operations.

According to data provided by Statistics Poland, there are about 1.4 million farms in Poland, mainly small and medium-sized ones. Only 20% of the total agricultural area is made up of farms with a total area of more than 20 hectares. The total area of agricultural land is about 18810.1 thousand hectares, while forests and woodlands cover about 9513.2 thousand hectares.

The challenges faced by the agriculture sector in Poland include reduction of production costs and demand for manual work, optimisation of water, fertiliser and pesticide use, increasing the security of food production and supply, the application of agricultural practices consistent with environmental protection principles (biodiversity, water, soil), and monitoring the production cycle.

The biggest pressure concerning modernising food production in Poland is exerted these days by large distributors (such as large chain stores), which on the one hand impose strict monitoring of the quality of products as a result of EU regulations in this regard, and on the other, they force producers to be efficient due to their strong bargaining power. This makes agriculture an industry that is beginning to attract innovators who are undertaking successful experiments with IoT solutions supporting economically efficient and high-quality production. The progressing consolidation of producers seems to be one of the important conditions for the "industrialisation" of these experiments, whether through cooperative or capital mechanisms.

Environmental protection is a sector that focuses on reducing and repairing damage to the surrounding environment and natural resources. Environmental protection faces a number of challenges, including climate warming, air pollution, waste management, contamination of the environment with toxic substances, accumulation of environmentally hazardous waste, fires, protection of biodiversity and forests, as well as protection of inland and sea waters.

One of the biggest threats – global warming – is largely driven by so-called greenhouse gases, such as carbon dioxide, methane and water vapour. It is important to monitor their concentration and emission sources, as it allows us to estimate their impact and take appropriate measures aimed at reducing emissions.

The ubiquitous nature of vehicles powered by internal combustion engines, so-called low emissions, industrial emissions and forest fires in turn have a direct impact on air quality. Air pollution is one of the major problems that European countries are trying to tackle these days. In 2016, air pollution was estimated to have killed 4.2 million people worldwide. Unfortunately, we are the leader in terms of air pollution, as 36 of the 50 most polluted European cities are located in Poland. The annual European standards for PM2.5 and PM10 are exceeded several times over. The main reason for this is low emissions – heating homes using inefficient coal furnaces and low-quality fuel generating large amounts of particulate matter. Another issue is the high concentration of Benzo[a]pyrene, the measured concentrations of which during winter months in Poland exceeded the generally accepted limit of 1 ng/m3 more than ten times over.

The most important challenges concerning environmental protection in Poland include improving air quality, finding out the main sources of particulate matter pollution, as well as toxic gases and volatile organic compounds (VOCs, such as benzo[a]pyrene), neutralising the risk of droughts and water pollution, reducing soil erosion and water eutrophication, improving the efficiency of plant irrigation, and mitigating risks concerning animals and plants (agrophages, reduction of species populations and biodiversity).

Growth prospects for the industry

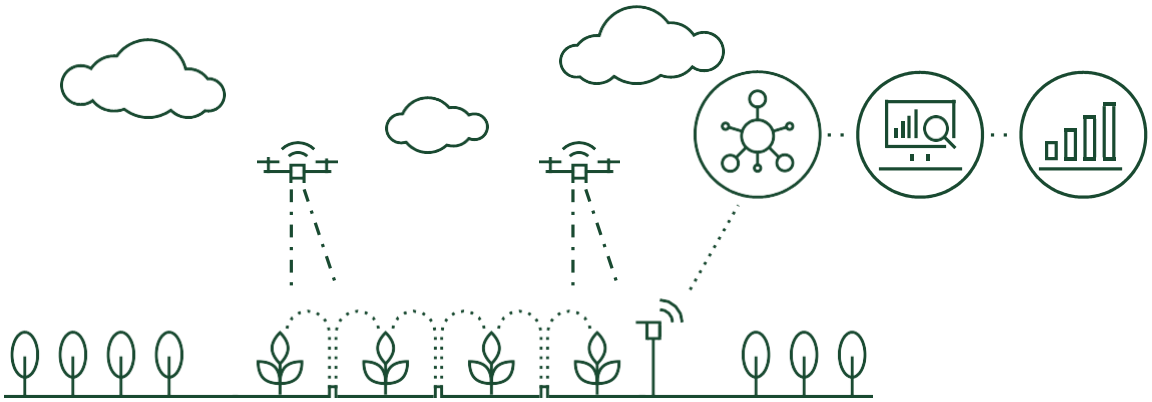
Agriculture in Poland and in the world is facing major civilisational challenges related to the projected growth of the population to 9 billion people by 2050 and the resulting increase in the demand for food, which makes it necessary to optimise food production by increasing productivity by about 70 percent. Given these circumstances, the Internet of Things is one of the key technologies that has great potential to support the management and optimisation of agricultural processes.

Other related civilisational challenges concern environmental protection (smog, droughts, water pollution, soil erosion, increasing salinity, negative changes in the natural environment in terms of fauna and flora). The Internet of Things is a key technology for monitoring these phenomena and supporting rapid action.

Agriculture

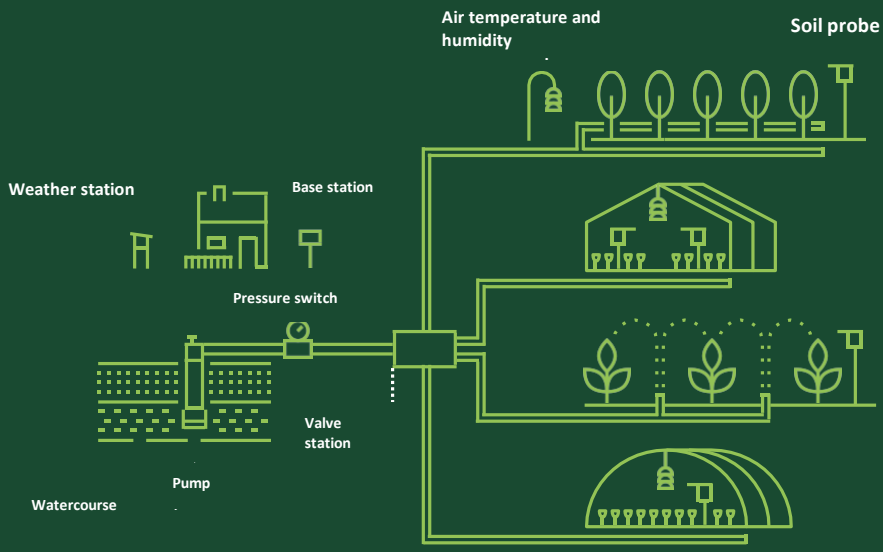
The potential for action in agriculture covers many aspects, including:

- increasing plant productivity through the use of precision agri-technology and plant protection, intensifying activities aimed at breeding more productive varieties, developing functional food production, taking into account resistance of plants to biotic (biological, such as crop diseases and pests) and abiotic (physical, such as extreme temperatures, limited or excessive water availability, soil erosion, strong winds) stresses in growing programmes;
- increased profitability of agriculture due to increased demand for good quality and healthy products, reduced environmental impact through the implementation and development of integrated production and the development of organic farming;
- further development of technologies for the storage and processing of agricultural produce, reduction of manual work by improving harvesting techniques;
- introduction of robotics for the harvesting and care of vegetables and fruit grown under cover (tomato, cucumber, pepper, aubergine, strawberries, etc.), introduction of autonomous machines for field work and plant protection;
- increasing safety at work;
- development of Decision Support Systems which will assist in making key decisions during plant protection and harvesting.



eSAD PROJECT

HTTPS://WWW.INVENTIA.PL/NEWSY/AGREUS-ROLNICTWO-4-0-CZYLI-IIOT-W-PRAKTYCE-ROLNEJ/
POLAND



PROBLEM

Currently, only a dozen or so percent of the surveyed farms use any method to assess the water needs of their plantations. The lack of systems allowing for the optimisation of crop irrigation has a direct impact on the competitiveness of Polish farms in comparison with agricultural production enterprises from technologically developed countries.

SOLUTION

In Poland, the eSad project – "Development of an innovative system of distributed measurement of soil and climate parameters as a tool for the optimisation of irrigation, plant protection and agrotechnical works" is being carried out as part of the Regional Operational Programme of Mazowieckie Province. The participants of the project are working on developing the Agreus system.

BENEFITS

The Agreus system, implemented by the Polish company Inventia, allows for far-reaching savings in water consumption in plant cultivation using a network of measurement sensors (used for climate and soil moisture monitoring) and an automatic valve station.

COMPREHENSIVE AIR MONITORING SYSTEM

HTTPS://AIRLY.EU/PL/COMPANY/
POLAND

PROBLEM

According to annual reports of the European Environment Agency (EEA), Poles suffer from breathing poor quality air, which causes over 48,000 people to die prematurely each year. The first step in improving the situation is to raise awareness among the general public, as well as to enable them to identify the sources of the issue and the most sensitive areas. However, this is stifled by high costs of installing and operating air pollution monitoring equipment.

SOLUTION

Airly – a comprehensive air quality monitoring system, supplementing the State Environmental Monitoring stations. The devices have a built-in laser which measures the airborne fractions of particulate matter – PM1, PM2.5, PM10, as well as toxic gases: nitrogen dioxide, ozone, sulphur dioxide and carbon monoxide. The system enables spatial and dynamic analysis of the quality of air in cities, built-up areas and rural areas.

BENEFITS

Reducing the size of smog sensors has led to reduced production and maintenance costs compared to reference stations. The devices are characterised by high measurement accuracy, which has been repeatedly tested in comparative studies carried out by academia. Due to the significantly lower costs, they make it possible to estimate the condition of air quality in places that have not been covered by state measurement systems. The Airly system comprises many elements which allow for informing residents about air quality through its Web platform (https://airly.eu/map), mobile applications (iOS, Android), as well as accessing data via API or LED information boards. Additionally, Airly provides a 24-hour air quality forecast using artificial intelligence (AI).

In Poland, the main activities are carried out under European Structural Funds, including the RDP. The IoT sector has the potential to become involved in the majority of priority actions identified by the EU for rural development, including:

- improving the profitability and competitiveness of all types of agriculture, as well as promoting innovative technologies for farms and sustainable forest management;
- improving the organisation of the food chain, animal welfare and risk management in agriculture;
- restoring, protecting and enhancing ecosystems dependent on agriculture;
- promoting resource efficiency and supporting the transition to a low-carbon and climate-resilient economy in agriculture, the food sector and forestry.

Environmental protection

The potential for action is linked to the numerous environmental risks and challenges mentioned in the previous section. IoT technologies offer the possibility of significant improvement in the field of environmental monitoring by increasing the number of measuring stations - both in the form of reference stations and by creating a supplementary monitoring network offering higher density. Monitoring enables the creation of pollution maps, as well as maps showing the occurrence of negative phenomena, analysing their impact on the environment (using Big Data and AI), managing the problems and effects of adverse conditions, as well as taking preventive actions. Well-organised monitoring provides quantified knowledge of specific environmental and process parameters, enabling quick and effective decision-making to improve the situation in a given field. Additionally, the lower energy consumption of IoT solutions enables more effective use of battery power sources than ever before.

In addition, infrastructure based on dedicated telecommunication solutions for metering (SigFox, LoRa) can be used more widely as a mass communication platform for IoT devices, as well as an alternative to currently available technologies (GSM, LTE).

Scope of possible use of IoT solutions

Agriculture

- Managing the use of fertilisers and plant protection products.
- Managing water consumption in agricultural production / high-precision irrigation.
- Fertilisation optimisation / high-precision fertilisation.
- Monitoring of pests and weeds threatening crops, monitoring environmental conditions by using sensors in cultivation and breeding, as well as in plant protection, animal husbandry, supervising growth phases.
- Precise feeding.
- Stock tracking.
- Waste management and recycling in agricultural production.
- Apiary management and monitoring.
- Climate control in horticultural production under cover, management of technological parameters in cold stores, storage rooms and dryers.

Food safety

- Monitoring of food supply chains (farmer, food processor, logistics and storage, retailer, consumer - combining relevant data generated at each stage).

Environmental protection

- Air quality monitoring, including particulate matter, toxic gases (such as NO2, O3, CO) and volatile organic compounds (VOCs), carbon dioxide and its potential emission sources.
- Monitoring of ionizing radiation intensity.
- Continuous monitoring of potential sources of air pollution, such as factories and production plants.
- Water quality and quantity monitoring, monitoring of algal blooms.
- Soil quality and garden substrate quality monitoring.
- Environmental noise monitoring, noise monitoring in urban areas.

- Biodiversity and habitat status monitoring.
- Waste management monitoring.

Barriers

In the course of the work the sub-group identified the following barriers:

- Lack of coverage of LPWAN open wireless networks.
- Lack of education concerning the opportunities and solutions offered by the IoT in agriculture which would result in actual tangible benefits.
- Lack of demonstration farms which would serve as examples for IoT solutions.

Proposals for government action

The Working Group suggests taking the following measures aimed at developing the IoT in the sector:

- Supporting activities aimed at covering the whole area of the country with wireless network coverage using technologies suitable for battery-powered IoT devices (for example LoRaWAN, Weightless, Sigfox, NB-IoT). For agricultural and environmental applications (sparsely populated areas with few base stations) infrastructure is needed to connect a sufficient number of devices, including sensors running for months or years on battery power. This infrastructure should be available not only in a B2B model for large companies. The SME sector should also be supported. Providing a sufficient amount of constantly updated data is required for making appropriate business decisions concerning analysis or optimisation.
- Establishing publicly available resources of climatic and hydrological data at the level of the state administration with high grid density, providing actual data from weather stations and measurement points, and not just simulations and forecasts.
- Ensuring access to data from multiple sources, opening and making data from the national systems (including historical data) available free of charge. High accuracy and timeliness of data are paramount in this respect. In the case of creating new databases, mechanisms should be implemented for providing information concerning the reliability/accuracy ratio of a given data source (taking into account aspects such as ageing of sensors). We suggest providing funding in parallel to public entities for the provision and maintenance of such databases, as well as for the development of institutional competencies in this area. The IT part of the infrastructure also constitutes its important element, related to the storage and processing of data. The methodology of data collection, the interoperability of data, and the possibility of aggregating data from different sources for analytical purposes, as well as using existing open standards in this respect are paramount. Data from national databases (operated by public bodies) should be available to users free of charge.
- Financial support for reference installations – demonstration farms (for example farms belonging to agricultural advisory centres in direct contact with clients – farmers), support for IoT pilot schemes. We suggest creating a legal framework for public-private partnerships that allows for easy testing and demonstrating business ideas.
- Creating institutional forms of financial support for IoT projects of particular social importance (where profit is not a priority) – for example, smog monitoring infrastructure (dense network of air quality sensors in cities, sensors on chimneys, at production plants, communication routes), application of the IoT in drought measurements, apiary management, breeding, support for rational use of plant protection products and fertilisers in agricultural production.
- Developing subsidised forms of education on the digital economy, including the IoT. Further training in IoT technology for institutions such as agricultural advisory centres, scientific institutes related to agriculture, and universities of natural sciences (for knowledge promoters).

CROP IRRIGATION SYSTEM

POLAND

PROBLEM

High costs of field irrigation during dry periods.

SOLUTION

The integrated iHorti crop irrigation system for medium and large horticultural farms. The system works by:

1. Determining the optimal irrigation level for a given part of the field on a given day by means of a network of sensors monitoring environmental conditions such as soil moisture, evapotranspiration of crops and soil, solar irradiance, wind, natural precipitation, air temperature, shape of the field surface, green mass gain.

2. Irrigation based on rain barrels with rotating sprinklers or sprinkler consoles. Rain barrels equipped with digital controllers allow for the precise control of the water dose, full remote programming of irrigation works, geolocation of the irrigation unit in order to precisely administer the water dose in a particular area of the field, collection of data on irrigation and water consumption, as well as other system parameters.

The combination of these two components with the central application ensures that the horticultural enterprise can centrally plan, supervise and optimise its irrigation in daily, weekly, seasonal and multiannual periods.

BENEFITS

Reduced water consumption per hectare of field and per kilogram of yield. Environmental protection by protecting water resources. Optimisation of food (vegetable) production cost.

15

TELECOMMUNICATIONS

After nearly two hundred years of the development of telecommunications, which has changed the world and brought people from around the globe closer together, the sector faces yet another challenge.

Connecting billions of IoT devices can accelerate economic growth and help solve some of the problems of our civilisation.

AUTHORS:
MATUSZ MICHALSKI, MTECHNOLOGY / HACKERSPACE WROCŁAW ASSOCIATION – SUBGROUP LEADER
TOMASZ DYLIK, EXATEL
JANUSZ GÓRSKI, T-MOBILE POLSKA S.A.
MAGDALENA KOGUD-CZARKOWSKA, IAB POLSKA ASSOCIATION OF EMPLOYERS OF THE INTERNET INDUSTRY

General characteristics of the sector

The telecommunications sector plays a key role in the implementation and development of the Internet of Things. Based on the services provided by the telecommunications industry, it is possible to quickly implement IoT concepts on a large scale, just like before, when Internet access was becoming widespread.

From the beginning of telecommunications, technical solutions were mainly focused on meeting the needs of people as end users of services. As of now, the telecommunications market is approaching mass deployment of autonomous systems based on devices that will communicate with each other with negligible human intervention or without it at all. These devices, connected in a network, form the Internet of Things, and as such, they introduce a new type of connection/traffic in telecommunications networks. The traffic flow has different characteristics and different requirements compared to the standard, user-generated one. Currently, IoT systems usually take advantage of technological solutions that were originally designed for use by humans. Device developers use standards such as GPRS, UMTS, Wi-Fi, LTE, Ethernet and others to provide wireless or wired connectivity to their devices. However, the telecommunications industry has prepared new communication standards to meet the needs stemming from mass IoT implementation.

Wireless telecommunications for IoT

Wireless telecommunications standards for the IoT play a key role as "last mile" technologies, making it easier to integrate IoT devices into networks and make them available almost anywhere. International organisations have developed wireless communication standards for both licensed and unlicensed bands. These are standards for so-called LPWANs (*Low Power Wide Area Networks*).

The main assumptions underlying the development of standards dedicated to the IoT are:

- Energy-saving – ensuring long battery life (even over 10 years);
- increased coverage – enabling the installation of equipment in places where it is currently not possible (basements, elevator shafts, forests, etc.);
- low cost of communication modules;
- low cost of infrastructure implementation;
- high network capacity supporting a *massive IoT*.

Standards in the licensed band

1. GSM, UMTS, LTE, NR

GSM/GPRS (*Global System for Mobile Communications*, UMTS (*Universal Mobile Telecommunications System*) and LTE (*Long Term Evolution*) are common digital standards used in cellular networks. Each of them enables the transmission of voice, text messages, multimedia messages and mobile data. Despite the fact that current IoT solutions use these standards, they cannot really be considered optimal for such uses, in particular in the case of simple devices, such as water meters. None of these standards meets all the above-mentioned assumptions, which should be met by a cellular network standard created with the IoT in mind. As a result, implementing IoT solutions on a mass scale simply loses its economic viability. The NR *(New Radio*) standard, which will constitute the backbone of 5G networks, is also focused on very fast data transfer, based on the assumption that IoT connections should be ensured using other technologies. Supporting the IoT is only planned at further stages of development of the NR standard, in a similar manner as in the case of the IoT, by introducing technologies such as Cat-M, NB-IoT, V2X, ProSe, etc. The only exceptions are devices such as autonomous vehicles and other applications that require very low latency and high connection quality. These devices will have to use the latest and most efficient solutions offered by LTE, 5G or other standards.

2. NB-IoT

NB-IoT (*Narrow Band – Internet of Things*) is a mobile standard for the IoT, using a 200 kHz band. NB-IoT makes up a part of the LTE mobile network standard; however, from a technical point of view, this is a new radio access technology. There is no compatibility between NB-IoT devices and regular LTE networks. The NB-IoT cellular network can be run on the basis of the existing LTE network, which can be adapted to the new standards thanks to a software update, which significantly impacts both the cost and time of implementation. From the point of view of radio, NB-IoT can be implemented in 3 different ways, all of which can be used simultaneously within a single radio network. NB-IoT cells can be set up in the *in-band mode*. The NB-IoT cell can also be set up next to an LTE cell in the so-called *guard-band mode*. This is a very effective solution because it does not affect the bandwidth of the main cell, despite using the same hardware. The last way to set up an NB-IoT cell is in standalone mode. which enables the reuse of frequency channels used by the GSM/GPRS standard. For an end device, the operating mode of the network is of no relevance whatsoever.

NB-IoT was designed for simple devices that do not require high data rates and also connect to the network relatively rarely. It is a good solution for applications currently using GSM/GPRS networks. An ideal example of devices suitable for use with NB-IoT technology are metering, agriculture, and logistics devices, as well as weather sensors, alarms, etc. NB-IoT ensures high energy efficiency provided that the amount of data sent is relatively small (for example short consumption reports, alerts, sensor readings) and reported rarely (several times a day or less frequently). In such cases, a 5Wh battery can provide power for 30 years or more. When sending larger amounts of data or sending them frequently, Cat-M may be a more efficient standard. The NB-IoT standard also assumes that more than 50,000 IoT devices can operate within a single cell, given the assumed traffic model.

Another key feature of the NB-IoT standard is its increased coverage. NB-IoT offers more than 20 dB gain in coverage when compared to GSM/GPRS. This makes it possible to install devices in places where existing cellular networks no longer have coverage, such as elevator shafts, cellars, manholes, forests, etc. Unfortunately, this adversely affects battery life, the data rate achieved, and latency. In extreme cases, the latency may be as long as several minutes, which means that sending a larger amount of data may prove to be practically impossible.

After the development period, the cost of the NB-IoT radio modules should drop below $5 per piece. Currently, they often command prices in excess of $10. This may be a key factor delaying the implementation of the standard on a mass scale, as GSM/GPRS modules have long since reached a price well below $5.

3. EC-GSM-IoT

EC-GSM-IoT (*Extended Coverage GSM IoT*) is a standard that introduces changes in the functioning of GSM networks, adapting them to the requirements of IoT. This solution uses the resources of a conventional GSM/GPRS network, adding NB-IoT-like functionalities, such as increased coverage, as well as energy efficiency. In addition, it introduces a variety of security solutions, the lack of which has plagued the 2G system. The battery life is expected to be similar to NB-IoT.

What is more, this solution only requires updating the GSM network software by the network operator. EC-GSM-IoT services enable sending data and text messages, while voice calls can be made after switching to conventional GSM mode and cannot be made with increased coverage. Like NB-IoT in-band mode, EC-GSM-IoT negatively affects GSM cell capacity for conventional services.

The radio resources are divided in time between EC-GSM-IoT and other GSM devices. Despite this, it is assumed that more than 50,000 IoT devices will be able to function within a single cell, as in the case of NB-IoT.

It is expected that the cost of the radio module will be lower than the cost of the NB-IoT unit due to the fact that they are based on existing GSM modules. Hence, the standard seems to be a perfect candidate for quick implementation; however, it can hardly be considered popular. In reality, telecommunication operators from Europe and countries where LTE network coverage is similar to that of GSM tend to rely primarily on solutions based on the LTE standard. Perhaps this standard will later be developed in countries which have better GSM coverage compared to other technologies.

4. Cat-M

Cat-M (*Category-M*), often also referred to as eMTC (*Enhanced Machine-Type Communication*) or LTE-M, is a standard which, like NB-IoT, is based on LTE networks, but is not considered as a separate radio access technique. Cat-M – as the name may suggest – is considered to be a special category of the LTE terminal device with a simplified design and limited capacity compared to other categories found in the LTE standard. The key difference is the supported bandwidth – 1.4 MHz or 5 MHz, compared to standard devices, which use the 20 MHz band. Cat-M can be positioned between NB-IoT and LTE. This means that the achieved data transmission rates are much higher than in the case of NB-IoT, but also much lower than with classic LTE. In addition, compared to NB-IoT, this standard enables making voice calls in VoLTE technology, offering slightly extended coverage compared to the LTE standard. Cat-M is a standard designed mainly for low-cost mobile devices with low data transfer requirements (below 1 Mb/s). Examples of devices using Cat-M are very cheap LTE phones (offering voice calls and text messages), health and elderly monitoring devices, payment terminals and other IoT devices requiring frequent connections, while remaining in motion.

Using Cat-M technology in the operator's network requires only updating base station software and some backbone network devices. This technology supports all the energy efficiency solutions known from NB-IoT, as well as the increased coverage, which was originally intended to be about 12 dB higher compared to GSM networks. However, many studies indicate that Cat-M is able to get close to 20 dB gain, just like NB-IoT. Battery life for simple applications exceeds 10 years, provided good radio conditions are ensured.

LORAWAN-BASED WASTE COLLECTION OPTIMISATION

SPAIN

PROBLEM

Regular waste collection along a regular route is hardly optimal and generates unnecessary costs, as well as exhaust fumes.

SOLUTION

In the province of Salamanca in Spain, a system has been implemented to optimise the waste collection process based on the LoRaWAN* standard. Sensors were installed in waste bins which reported the fullness levels of the bin to the central system. On the basis of this data, the system prepared optimal routes for waste collectors.

BENEFITS

Significantly reduced cost of waste collection and air pollution thanks to exhaust emissions reduction. Before the system was implemented, waste collection vehicles covered a daily distance of about 3050 kilometres. After the system was launched, the total distance was shortened on average by about 1076 kilometres.

* *"Smart Waste Collection System with Low Consumption LoRaWAN Nodes and Route Optimization" https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5982603/*

Standards in the unlicensed band

1. **LoRaWAN**

LoRaWAN is a standard created by the *LoRa Alliance* consortium, operating in ISM bands below 1 GHz. In Europe, the system operates using 433 or 868 MHz bands. Just like NB-IoT, LoRaWAN is an LPWAN networking standard, which is aimed at the transmission of small amounts of data from terminal devices. This standard offers lower bit rates compared to NB-IoT, fewer connections and lower guarantees, due to the requirements for ISM bands. The vast majority of LoRaWAN applications are the same as NB-IoT, which is why this standard can be considered to be direct competition to NB-IoT for applications that do not require a high resource guarantee.

The LoRaWAN specification is focused on simple radio solutions which enable significant reduction of production costs of the radio modules. Longer development compared to its cellular counterparts results in much lower costs for radio modules at the moment.

The standard, depending on the implementation, ensures 10-20 dB higher gain than GSM networks, which makes it similar to NB-IoT and CaT-M.

LoRaWAN networks can be established by non-profit organisations and private users on the basis of publicly available devices, just like in the case of the Wi-Fi standard. This standard also interests telecommunication operators who would like to offer it as a commercial service.

2. **SigFox**

SigFox is a partially closed LPWAN networking standard. On 13 January 2019, the radio part of the standard was opened, allowing for the development of custom implementations of terminal equipment. The standard owner builds their own access networks independently or in partnership with local operators. SigFox networks are not yet available in Poland, although according to media reports the company is interested in entering the Polish market in the near future.

NB-IoT-BASED HEAT METER READING

POLAND

PROBLEM

High costs of reading heat meters in four municipalities: Biały Dunajec, Poronin, Szaflary and Zakopane.

SOLUTION

T-Mobile Polska in cooperation with ABARO has implemented a comprehensive system for automatic heat meter reading based on NB-IoT technology for Przedsiębiorstwo Energetyki Cieplnej Geotermia Podhalańska S.A., the largest company in Poland producing heat from geothermal sources. Thanks to this solution, Geotermia is the first district heating provider in Poland with remote reading entirely based on NB IoT networking technology.
As part of the contract, T-Mobile and ABARO provided more than 1500 telemetry devices and full telemetry infrastructure (NB-IoT data transmission handling, servers, software, technical support and maintenance services).

BENEFITS

Thanks to frequent and automated collection of the most important data from the whole district heating network, the project has enabled optimisation of energy consumption and increased customer service comfort.

This standard operates on the 868 MHz ISM band. SigFox is based on very short messages. The useful portion of data that can be sent within one message comprises only 12 octets. Of all the wireless standards described in this chapter, it is the standard with the most limited data transmission capabilities. SigFox is suitable for use only with very simple devices such as sensors or geolocation tags.

3. **Other**

The most popular LPWAN networking standards were all described above. Of course, there are other communication standards in the world, but they are not popular enough for their presentation to be warranted in this report.

All short-range standards such as Bluetooth, ZigBee and others are treated by the telecommunications industry as standards dedicated to specific systems, mainly with local coverage. Since they do not fit the purpose of becoming publicly available services, they were also not covered by the Working Group.

Wired telecommunications and infrastructure

Just like short-range wireless connectivity, all wired standards for the IoT are considered as tailor-made solutions with local coverage.

The only exception would be the technology which enables data transmission over electrical networks, but over the course of the project the Working Group has not identified any specific needs or applications for this technology.

Launching wireless LPWAN and 5G networks may require developing the telecommunications infrastructure, including backbone networking infrastructure, as well as the construction of new access points and base transceiver stations. The latter may be particularly required by 5G networking technology, even in places that do not seem obvious at the moment. From the point of view of the industry, it is important that Polish legal regulations do not stifle the rapid expansion of the telecommunications infrastructure, which could result in a delay in the widespread implementation of 5G in Poland.

Growth prospects for the industry

In its November 2018 report on mobile telecommunications entitled *Ericsson Mobility Report*, the company estimated that by 2024 the number of IoT devices in the world will grow at a rate of 17% per year (cumulative annual growth rate), reaching 22.3 billion devices from the initial 8.6 billion in 2018:

Number of IoT devices in billions

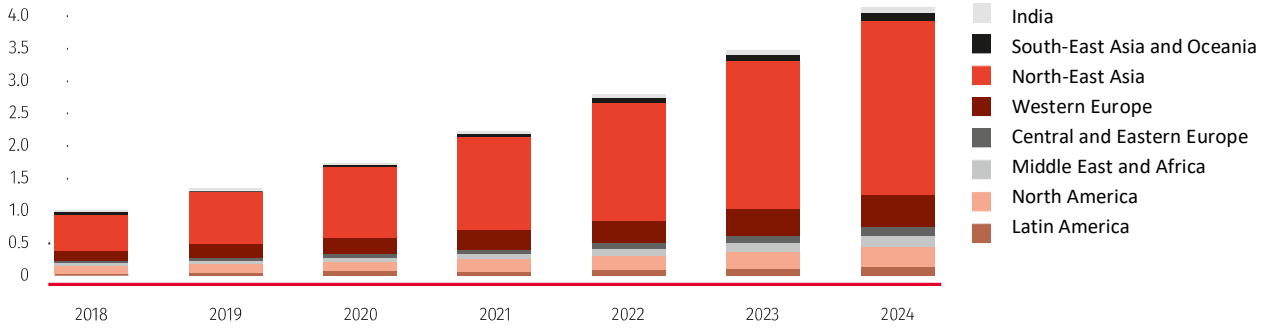
IoT	2018	2024	CAGR
Long-range IoT (LPWAN)	1.1	4.5	27%
Cellular IoT	1.0	4.1	27%
Short-range IoT	7.5	17.8	15%
Total	**8.6**	**22.3**	**17%**

Source: Ericsson Mobility Report, November 2018

The report predicts the highest growth rate for long-range connections (LPWAN), which are to be driven by the implementation of cellular IoT. Short-term and wired IoT communication will grow at a rate of 15% per year.

The chart below shows the forecast number of connected devices using cellular IoT standards in a given year, broken down by world regions. As can be seen, the report does not forecast a significant change in the proportions of the market breakdown in terms of the number of connected devices, suggesting similar market growth across the globe.

Number of connected cellular IoT devices by region [in billions]

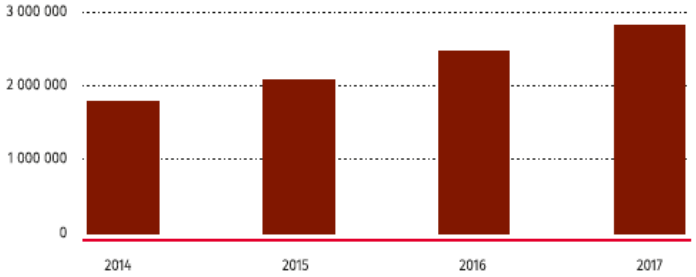


Source: Ericsson Mobility Report, November 2018

The chart below shows the number of SIM cards officially recognised by operators as M2M in 2014-2017. The relevant data were obtained from reports submitted to the President of the Office for Electronic Communication by telecommunications operators.

In 2017, the number of SIM cards classified as M2M communication cards amounted to approximately 2.8 million.

The number of M2M SIM cards in Poland



Source: Working Group, based on data provided by the Office of Electronic Communication

If we assume the growth rate estimated by Ericsson and the number of cards officially recognised as M2M in Poland, we should reach about 12 million active M2M SIM cards in 2024. The data provided by UKE show that the mobile communications market in Poland has been saturated – without including M2M cards, it has about 50 million subscriptions. That means that if the current trend is to remain at the current level, by 2024 the number of M2M cards in the Polish market could constitute about 20% in relation to all SIM cards. The number of "hidden" M2M cards, which are counted among regular subscribers in the data, remains unknown. However, based only on the official number of M2M cards, it can be concluded that the third decade of the 21st century will be the age of the development of the IoT for the telecommunications industry, in addition to 5G networking.

As of now, in Poland, mobile technologies for the IoT have been implemented partly by T-Mobile Polska, which has provided NB-IoT coverage in a certain part of its network, as well as by Orange Polska, which is testing Cat-M technology in several locations. In some cities, private companies and organisations have provided LoRaWAN access points. This may be an opportunity to actually implement universal access to mobile IoT services in Poland in the coming years.

Scope of possible use of IoT solutions

The telecommunications sector can be considered to be a sector dealing solely with data transmission services. Hence, it is up to end users from other industrial sectors to exploit the potential of telecommunication services. On the other hand, the current market situation often makes IoT users interested in comprehensive solutions for their industries, and telecom operators can serve as aggregators of third-party products, and as such they can offer ready-made solutions for other industries.

Barriers

In the course of its work the Working Group has identified the following barriers for the telecommunications sector:

1. Limited availability of IoT-compliant telecommunications infrastructure on a mass scale.

2. EMF standards which are much stricter than the EU average, and hamper the development of 5G and IoT technologies based on mobile networks.

3. Limited financial resources for carrying out the necessary large-scale infrastructure investments.

4. Legal regulations incompatible with IoT/M2M device communication.

5. Regulatory constraints concerning Big Data analysis.

Proposals for government action

The basic legal act regulating the telecommunication sector is the Telecommunication Law. Together with the growing importance of ICT services for various sectors of the country's economy, we have been observing a constant expansion of the scope of standards, regulations and laws affecting telecommunications companies. This applies not only to data processing, but also to the security of provided services, as well as conditions regulating the provision of Internet access service.

One of the most characteristic phenomena is the ever-growing complexity of laws and their contradictory nature, which stifles the development of new and innovative IoT services, in particular in situations where communication services are seen as a component of the IoT device itself.

In addition, the legislation mostly concerns the provision of telecommunications services dedicated to interpersonal communication. For this reason, a number of legal provisions regulate in detail the relationship with an individual that are irrelevant for communication between IoT devices.

Hence, it is necessary to adapt the legal provisions to the specific conditions of IoT communication. The current process of implementing the provisions of the *European Code of rights of users of electronic communications services* in Polish law can be a good time to introduce changes in this respect.

The second key piece of legislation relevant to IoT communication is the draft ePrivacy Regulation, which directly addresses issues related to the processing of data produced in the telecommunications network by IoT devices.

Therefore, the Working Group recommends taking the following actions:

1. Adapting Polish laws and standards concerning electromagnetic fields (EMF) to other standards relevant for other EU Member States. This will enable the expansion and modernisation of the radio telecommunications network, which is the foundation for the provision of complex IoT services. In addition, future diverse expectations concerning the conditions for the provision of IoT services by operators will direct investments for the implementation of 5G networking.

2. Bearing in mind the complexity of the regulatory environment, which mostly concerns interpersonal communication, the Group recommends creating a definition of the legal concept of an IoT device/user, which will then enable adjusting (by reducing) the scope of regulatory obligations concerning IoT communication. This applies in particular to legal provisions concerning interpersonal relations, such as detailed billing, phone number portability, contract duration, making emergency numbers calls, addressing devices without using telephone numbers, etc.

CELLULAR IoT AND NIDD IMPLEMENTATION

JAPAN

PROBLEM

Risk of attacks on IoT systems accessible via IP protocol.

SOLUTION

The Japanese mobile operator SoftBank conducted successful NIDD* (Non-IP Data Delivery) connection tests in autumn of 2018. NIDD connections enable exchanging data without allocating an IP address for the device. In the future this will also extend to phone numbers. The connections were made in a commercially operating network using the NB-IoT standard.

BENEFITS

Reducing the risk of hostile attacks on IoT devices in IP networks and establishing a secure connection from the device to the data processing infrastructure. By removing the overhead generated by IP protocol, simple NB-IoT devices will have longer battery life. The example of a Japanese operator presents a model process of preparing telecommunications infrastructure for the implementation of *massive IoT*.

* *"SoftBank Launches World's First Experimental Services in Commercial Environment Using NIDD Technology for NB-IoT" https://www.softbank.jp/en/corp/group/sbm/news/press/2018/20180928_01/*

3. Starting a dialogue with telecommunications operators on the introduction of eSIM card portability as an alternative to number portability for IoT applications. This need is motivated by the physical impossibility of replacing eSIM cards in thousands of devices with a life span of more than 10 years.

4. Reducing restrictive requirements concerning the use of Big Data produced by IoT devices in telecommunication networks. In particular, it should be clearly indicated that after anonymisation/pseudonymisation the data may be used for other purposes.

5. Ensuring open data flows at least within the European Economic Area.

6. Removing administrative barriers that stifle the development of telecommunications infrastructure – one such example is the amendment of the Act of 7 May 2010 on supporting the development of telecommunications services and networks, and its extension to include the construction of telecommunications antennas and masts, which will be required by 5G networking technologies.

7. Enabling universal access to data owned by the state and collected by ICT systems funded by public money, such as smart urban transport systems, city car park monitoring systems, etc.

16

TRANSPORT, LOGISTICS AND AUTONOMOUS VEHICLES

In view of the current challenges facing the transport industry
and the increasing number of trips and deliveries,
the implementation of IoT technology is paramount.

AUTHORS:
SUBGROUP LEADERS: PAWEŁ GORA, UNIVERSITY OF WARSAW
DAMIAN HAJDUK, STRATEGIC ADVISORY AND MANAGEMENT IN TRANSPORT AND LOGISTICS

AND:
ŁUKASZ GAWLICZEK, AVE CARGO SP. Z O.O.
AGAZA HORZELA, GS1 POLSKA
ANNA KONERT, ŁAZARSKI UNIVERSITY
TOMASZ KOSIŁO, WARSAW UNIVERSITY OF TECHNOLOGY
KONRAD KOSTRZEWA, VETURAI AUTOMOTICE SP. Z O.O.
MAGDALENA KRYTYNIECKA-KONOPCZAK, PLL LOT S.A.
KAROLINA KRZYKOWSKA, WARSAW UNIVERSITY OF TECHNOLOGY
BARTOSZ MAZUR, GOP GEAR, "NAPRAW SOBIE MIASTO" FOUNDATION
RADOSŁAW MOSKWA, CM LOGISTIC
PIOTR PRZECHERSKI, OLCZAK KLIMETK, VAN DER KROFT, WĘGIEŁEK KANCELARIA RADCÓW PRAWNYCH SPÓŁKA PARTNERSKA
GRZEGORZ WILCZEWSKI, DAWIS IT SP. Z O.O.
EWA WOLNIEWICZ-WARSKA, KAPSCH TELEMATIC SERVICES SP. Z O.O.

SUBSTANTIVE CONSULTING:
MAŁGORZATA DAROWSKA, MINISTRY OF INFRASTRUCTURE
MICHAŁ KLUSEK, HEAD OFFICE OF GEODESY AND CARTOGRAPHY
ZBIGNIEW MALINOWSKI, SPATIAL INFORMATION INFRASTRUCTURE COUNCIL, GEO-SYSTEM SP. Z O.O.

"*We dream of a transport system in which all users have their own light and ecological means of personal transport, powered by renewable energy sources, adapted to human volume with some space to spare, allowing the transporting of small hand luggage. Let us call it a capsule. The capsule moves slowly along the first and the last mile, fully autonomously. The capsule can be disassembled and assembled in a matter of seconds from/to a portable form, the size of a small handbag. We can also call this capsule a car. Individual capsules can be further combined into capsule assemblies that move slightly faster in any available configuration with an upper limit on the first level integration points. Let us call them buses and stops. In the case of longer journeys, the capsule assemblies are arranged into an even faster long-distance assembly at the second level integration points. We will call them stations and trains. Journeys over even longer distances can then be handled by special, very fast vehicles, filled with capsules at the third level integration hubs. Let us call them ships and ports. (...)*" (from the work of the TLVA subgroup)

General characteristics of the sector

Transport is understood as the organised movement of people (passenger transport) or goods (freight/cargo transport) from one location to another. The smooth functioning of transport is essential to ensure the efficient growth of the entire economy; however, transport also faces certain risks stemming from incidents (collisions, accidents) and the negative impact on the environment. It is estimated that people commuting to and from work using individual means of transport in the 7 largest cities in Poland lose about 3.6 billion PLN annually due to the inefficiency of the transport system. In Warsaw, for example, the average travel time is 38% longer than it could be if there were no obstacles or obstructions on the roads. On the other hand, during the morning and afternoon traffic rush, travel time is extended by 66 and 73%, respectively. The World Health Organisation (WHO) estimates that approximately 1.25 million people die each year in road accidents. In view of the current challenges facing the transport industry, the increasing number of trips and amount of goods generated by economic growth, investments, increased consumption of goods and services, efforts to implement IoT technology are paramount. The biggest challenge for the transport industry in the context of the IoT is the organisation of open, standardized interfaces allowing for broad integration, as well as preparing the infrastructure to transmit, store and process the large amount of data generated by the IoT.

As of now, transport can take place in five environments: on the ground (land transport), underground, on water or (less frequently) below water (water transport), in the air (air transport) and in space.

The IoT can be used in any of those environments, but given the number of vehicles, the prevalence of their use and the possible benefits of the IoT, land and air transport are currently key areas for its implementation. Each of these environments enables the use of different means of transport – in the case of land transport, it can be trains, trams, cars, trucks, buses, scooters, bicycles, as well as foot traffic. This chapter focuses on those modes of transport and various aspects of transport where the IoT has the potential to bring step change and the largest benefits in the coming years.

Growth prospects for the industry

Transport and logistics in the world have experienced quantitative growth in recent years, taking advantage of favourable conditions, which include:

1. Good economic situation in the second half of this decade.

2. Successive increase in the volume of world trade (despite opposing protectionist trends).

3. "Physical" convergence of Eurasian markets through measures aimed at improving the functioning of transport between the Far East (China) <-> Europe (EU):

    - growing prospects for trans-Eurasian land routes are clearly visible after years (centuries) of the dominance of sea routes;

    - the *One Belt, One Road* initiative is used as a tool for continental partnership and cooperation, as well as Chinese expansion.

The European Union's single market and, more broadly, the European Economic Area, have powered mobility, trade, the flow of services, as well as supply and value chains in Europe. Economic exchange, despite the echoes of the crisis in Southern Europe, political and economic tensions (including the unclear prospects of Brexit), as well as external and internal threats to the countries of the single market, is still on the rise.

In the context of transport, logistics, as well as their automation processes, the Polish economy remains in a state of economic dualism. The world, especially Europe, with an increasing focus on a territorial and multimodal approach, keeps linking various branches and modes of transport to offer territorially and functionally integrated services. Meanwhile, in Poland, a single-mode approach (branch planning, microscopic approach) is still upheld to a large extent. The national road transport fleet is conquering Europe, while the dynamics and internal offer of multimodal transport, especially Polish railways, is clearly lower – this is particularly apparent considering Poland's location, although in recent years we have also seen quantitative and qualitative growth in this area.

Economic growth does not only concern consumption, but also investments that enable us to take advantage of our geographical location on the routes, which has been a problem for many years and is only now becoming our new opportunity. Large infrastructural and civilisational programmes, such as the expansion of sea ports (Central Port) or the mega-programme concerning the construction of the Solidarity Transport Hub are accompanied by hesitant, inconsistent actions aimed at breaking and dismantling the largely inadequate 19th century layout of communication networks. From time to time, one can observe the emergence of various concepts that are inconsistent with the logic of the economy and the settlement network, which preserve (and even enhance) the dysfunctional nature of the country's transport network, which is particularly apparent in western Poland.

The lack of consistency in the decision-making process is particularly evident in the context of the turmoil surrounding the programme for the construction of the planned high-speed rail network. The Working Group also considers the realism of the government's plans to modernise the country and its economy towards the concept of Industry 4.0 unclear, especially in the field of transport and logistics. In addition to these deficits and unnecessary constraints in organisation and planning, there is a lack of an integrated approach to human resources training. Modern industry, including transport, logistics and their automation from simple everyday use (transport) devices to the level of space expansion, requires systemic competencies and trained staff.

The changes which are currently taking place concerning various modes of transport focus on extending the mobility of people while increasing the safety, efficiency and sustainability of transport itself. Particular attention is currently paid to the development of digital technologies (automation of transport) which will be based on a data layer, encompassing static data (digital maps, traffic regulations) as well as dynamic data (real time conditions and traffic information). Digital technologies contribute to reducing the impact of human error, which is the main cause of incidents concerning transport. They can also contribute to the creation of a multimodal transport system combining all modes of transport into one integrated service, which will enable efficient *door-to-door* transport of people and cargo. The European strategy for low-emission mobility, which was approved in July 2016[1], focuses on the development of services integrating connected, cooperative and automated vehicles which have the potential to reduce energy consumption and emissions.

In the near future, such services will be closely linked, for example vehicles will be able to communicate with each other (V2V – vehicle-to-vehicle communication), with road infrastructure (V2I – vehicle-to-infrastructure communication), with pedestrians (V2P – vehicle-to-pedestrian communication) and with ICT networks (V2N – vehicle-to-network communication). This will be a coordinated action to enable road users and traffic managers to exchange information and make their actions interoperable. Cooperative vehicles will be able to establish the *Internet of Vehicles* and warn each other about potentially dangerous situations (such as sudden braking, accident, blocked road), as well as synchronise their plans, routes and manoeuvres to ensure efficient and safe driving. It will also be possible for vehicles to communicate with transport infrastructure, for example in order to send other vehicles the optimal route or speed, or to enable better traffic management (detecting traffic jams, accidents or bad conditions, adapting traffic light settings). Vast amounts of data collected from moving vehicles will serve as a source of valuable knowledge for Artificial Intelligence algorithms enabling better planning and optimal management of transport networks in real time. Connecting vehicles to an ICT network will in turn make it easier for passengers to work, rest or enjoy their journey, which will also be an important boon for the economy.

Tests concerning C-ITS (Cooperative Intelligent Transportation Systems, encompassing cooperative components of a transport network that can exchange data) technology have been successfully conducted by many companies and countries for many years now. The Netherlands, Austria and Germany became the first European countries with V2I communication in the C-ITS Corridor. The technology of vehicles equipped with V2X *(vehicle-to-everything*) communication capabilities has already been developed by such companies as Toyota, Volkswagen, Volvo and Mercedes. V2X technology will be particularly useful in the era of software-controlled autonomous vehicles, as it will be able to provide additional opportunities for safer and more efficient driving. Autonomous vehicles have been in the works for many years, developed by most companies from the automotive industry, as well as IT companies. One of the leaders is Waymo, which at the end of 2018 launched the first commercially available, partially autonomous taxi service. In 2019 in Sweden, the T-Pod autonomous electric vehicle was approved for driving on public roads, and in the beginning it will drive between warehouses and terminals. Work is also underway on the automation of other modes of transport, including rail transport.

1 A European Strategy for Low-Emission Mobility, COM(2016) 501 final.

The European strategy on Cooperative Intelligent Transport Systems (COM (2016) 766) lists the services that will require the so-called rapid uptake (the so-called Day 1 list) and services implemented in the second phase, where specifications and standards may not be completed (Day 1.5 service list).

Solution	Description	Benefits
Day 1 C-ITS services list	1.1. Hazardous location notifications:	Slow or stationary vehicle(s) & traffic ahead warning;
		Road works warning;
		Weather conditions;
		Emergency brake light;
		Emergency vehicle approaching;
		Other hazards;
	1.2. Signage applications:	In-vehicle signage;
		In-vehicle speed limits;
		Signal violation / intersection safety;
		Traffic signal priority request by designated vehicles;
		GLOSA (Green Light Optimal Speed Advisory);
		Probe vehicle data;
		Shockwave damping;
Day 1.5 C-ITS services list		Information on fuelling & charging stations for alternative fuel vehicles;
		Vulnerable road user protection;
		On street parking management & information;
		Off street parking information;
		Park & ride information;
		Connected & cooperative navigation into and out of the city (first and last mile, parking, route advice, coordinated traffic lights);
		Traffic information & smart routing.

eCALL RAPID ACCIDENT NOTIFICATION SYSTEM

HTTPS://WWW.IRISHTIMES.COM/NEWS/IRELAND/IRISH-NEWS/NEW-CARS-TO-AUTOMATICALLY-INFORM- AUTHORITIES-OF-CRASHES-1.3447079

EUROPE

PROBLEM

Automatic accident detection and informing relevant emergency services.

SOLUTION

From 1.04.2018, all new passenger and commercial vehicles up to 3.5 tonnes approved for use on public roads are fitted with eCall devices.

BENEFITS

The system can help to reduce the number of casualties as a result of road accidents. From October 2017 (when the Emergency Notification Centre was adapted to the requirements of the eCall system) to the end of 2017, 43 eCall notifications were directed to the 112 emergency number in Poland.

In addition to the automation of transport and C-ITS, it is worth pointing out trends such as mobility-as-a-service (instead of owning means of transport, users rent available means of transport as needed), shared mobility (users share their own or rented means of transport with other users), and the integration of multimodal transport (planning the development and use of transport in an approach that integrates all available modes of transport).

The development of Polish rail infrastructure and rolling stock, and their communication and data exchange (including the use of IoT devices) are becoming paramount in the 21st century. The challenges stemming from building an integrated domestic transport system, while ensuring its intermodal and international interoperability, as well as including future quasi-rail solutions such as magnetic, vacuum or already implemented dual- and multi-system solutions (universalisation and interoperability of transport) require specific actions, carried out by an identified and efficient (not functionally dispersed) research, implementation and decision-making centre. The main effects should encompass:

1. Increased speeds of railway transport, including in the context of the construction of high-speed railways, in particular those linked to the Solidarity Transport Hub.
2. Rationalising the labour intensity and maintenance costs of increasingly complex infrastructure.
3. Digitalisation and automation of processes in rail transport, both internal and at the interface with its economic environment, in order to effectively integrate rail into transport chains (multimodalisation of supply and travel chains), along with ensuring broadly understood cybersecurity.
4. Ensuring, through the participation of railway entities in research and development processes, that new solutions will meet the expectations of their future users (UX – user experience).
5. Creating conditions fostering the development of Polish innovative solutions, intelligent specialisation aimed at developing the concept of Industry 4.0 and value-added export.

In the rail transport sector, the conditions for the development of the IoT are particularly peculiar, which mainly stems from the different philosophy of transport organisation. The vehicle is “driven” along the rail, and the only differences concern the degree of freedom to determine the speed and fluidity of the vehicle on a predefined route. To put it in a more metaphorical way, road transport is characterised by

a “green light by default” approach, where traffic is allowed by default, and in the case of railways, the approach is the opposite – “red light by default”, where traffic is only allowed following official approval. The requirements are also far more stringent, which in return ensures greater safety (in line with the *fail-safe* principle).

Rail transport abounds in numerous safety devices, and their high numbers (especially when considered in the context of the European single market) is a challenge in itself. The same functionalities are implemented in various ways on different national rail networks, and the implementation of interoperability is hampered by the inherent differences, hence the priority to achieve full interoperability on the main rail routes in order not to impose excessive costs on the adaptation of the overall infrastructure.

People remain the primary link used to transfer information in rail transport, which is why the main objective of developing IoT solutions is automation. The most prominent example of direct communication between individual elements of the railway system are automatic crossing signalling devices. As a result of an impulse generated by the vehicle reaching a certain point on the railway line, the crossing gets automatically closed – direct communication between the vehicle-track system and the automatic crossing signalling devices eliminates the job of a crossing supervisor. At the same time, for greater safety, the correct closure of barriers (proper road/rail crossing protection) is signalled by an appropriate message, which enables the train to go through, displayed on the railway semaphore. In this case, however, the signal is not received by the vehicle, but by a human being (the driver), and it is their duty to react appropriately (by stopping the train) in the absence of an appropriate signal.

The proper functioning of rail transport is supervised by a number of sensors responsible for transmitting information about the status of a given device. These are train detection devices which form the automatic crossing signalling systems, switch point control devices, track occupation control devices, automatic train braking systems, which initiate train stopping in the absence of an activity signal from the driver. Progress in the field of railway automation is best illustrated by rolling stock emergency detection devices, which identify faults in passing trains, indicating a specific element even in a 40-car train passing at a speed of several dozen kilometres per hour. The development of rail transport sensors combined with the development of direct communication between the individual devices can significantly increase the level of safety, reliability and transport capacity of railways.

The situation is similar for unmanned aerial vehicles, where the sensors enable the collection and analysis of data, and in the future transport services, air quality measurements and support for ICT networks will allow them to be used in various sectors of the economy.

The current increase in the number of UAVs is a result of the good economic situation, the increasing availability of technologies, liberal regulations, and the decreasing costs of such devices. In Poland, the number of drone operators holding a certificate of competence in January 2019 exceeded 10 000. However, the future of UAVs mostly concerns automatic and autonomous vehicles.

The GSA (European Global Navigation Satellite Systems Agency) at the European Space Week conference in Marseilles in December 2018 pointed out UAVs as a new user of EGNOS and Galileo, as evidenced by numerous projects funded by EU programmes (including Horizon 2020). Several projects aroused particular interest, including REAL (RPAS EGNOS Assisted Landings), as part of which scientists develop navigation sensors based on EGNOS (European Geostationary Navigation Overlay Service) using, among other things, the integrity of the satellite signal, as well as GAUSS (Group of Astrodynamics for the Use of Space Systems), which aims at using the Automatic Dependent Surveillance-Broadcast system for positioning aircraft.

One of the most important elements of legal regulations concerning the use of UAVs is the protection of privacy and personal data. It should be kept in mind that personal data will also be processed during the use of UAVs. The issue of who should be assigned the role of data controller, as well as the way of fulfilling their obligations under the provisions on personal data protection laws, needs to be carefully analysed. In any case, particular emphasis should be placed on ensuring the privacy of data subjects, not only in the design phase, but also protection of data by default in the use of UAVs.

In February 2019, the Ministry of Infrastructure joined forces with the Polish Economic Institute to publish a White Paper on Unmanned Aerial Vehicles. The paper summarises the conceptual and implementation stage of a programme, the aim of which was to develop and implement the MoI regulation facilitating BVLOS (Beyond Visual Line of Sight) flights and allowing fully autonomous flights, as well as to launch the CEDD (Central European Drone Demonstrator) programme in the area of the Metropolitan Association of Upper Silesia and Dąbrowa Basin. The CEDD programme is a pilot activity, preparing the infrastructure for automatic and autonomous flights, along with the assumptions for the further regulatory phase for UAVs.

Work is ongoing on legal frameworks for the use of UAVs at both international and European levels, but these do not cover private law issues. As long as there are no such regulations, national regulations are paramount. Poland was one of the first countries to create regulations for VLOS (Visual Line of Sight) operations – they entered into force in 2013 and were amended in 2016. In February 2019, a regulation was adopted which enables BVLOS operations. Work to bring national regulations in line with the EU regulation is currently ongoing under the scientific project "Unmanned aerial vehicles. A new era in aviation law", financed by the National Science Centre (No. 2017/27/B/HS5/00008).

The project is carried out at the Faculty of Law and Administration of Łazarski University in Warsaw (project website: https://prawodrony.pl).

A major breakthrough in the logistics in the 20th century came with the standardisation of the way cargo is transported thanks to palletisation and (especially) containerisation. A similar breakthrough in the 21st century can (and should) be achieved through digitisation and a gradual integrating multimodalisation of transport. In order for this to be possible, greater coordination of measures in these areas will be required. Technological solutions, such as the dissemination and standardisation of data exchange systems, which will be strongly supported by the Internet (including the Internet of Things), and digitisation of transport and logistics processes, have and will have a significant role in the development of integrated multimodal supply chains, along with crucial organisational and mental changes.

Transport documentation – waybills – are one of the key elements of the supply chain. Its storage and correctness have a direct impact on numerous aspects, including the possibility to use a preferential VAT rate. The process of digitising transport documents will certainly improve and enable greater automation of transport and logistics processes.

The digitisation of transport documents is being carried out mainly thanks to two international projects: e-AWB (air waybill) for air transport, and e-CMR (CMR = French: *Convention relative au contrat de transport international de marchandises par route*) for road transport.

IATA (the International Air Transport Association) has recently announced that as of 1 January 2019, e-AWB will become the default form of an air cargo transport contract. At the time, the percentage of electronic waybills worldwide exceeded 60%; in Europe the number exceeded 50%. In Poland this indicator went up to 26.5%, exhibiting dynamic growth from 9.5% a year earlier.

However, some cargo carriers in Poland still do not allow for e-AWB data transmission. Fortunately, this situation should be ameliorated this year. The restrictions also apply to various destinations around the world, due to local conditions in the destination countries.

A complete departure from paper waybills is not yet possible in Poland. Even if e-AWB is used, from a practical point of view a paper printout of this document is usually necessary for the needs of cargo operators at airports (usually state-owned companies) as well as customs and treasury administration.

Container terminals at the sea port in Gdynia can be considered as a model example, where the integration of systems, including digital data transmission between the forwarder, shipowner, container terminal operator and customs and fiscal service, reduces the need to use paper waybills to an absolute minimum (usually only at the exporter's express request). Polish airports still have a lot of catching up to do.

The e-CMR electronic waybill for road transport is still undergoing development and testing. The first test transport using e-CMR took place only two years ago, on a route from Spain to France. The practical application of e-CMR will bring many benefits to all stakeholders. Shippers and recipients will have greater possibilities than before for remote shipment tracking, greater integration of systems for ordering shipments, confirmation of deliveries (for example for intra-Community acquisition of goods), not to mention the circulation of accounting documents and more efficient cashflow. The public authorities will have better possibilities concerning inspecting and controlling transports in real time, which should have a positive impact on crime-proofing the tax systems. The integration of e-CMR with the e-Call system used in vehicles will translate into better safety on the road – (for example, in a situation where a vehicle carrying dangerous goods is involved in an accident, the e-Call system automatically notifies the relevant emergency services about the incident, while e-CMR data will allow real time identification of the scale of the potential hazard). In the case of carriers and freight forwarders, e-CMR will enable, among other things, more efficient administration of documents and accounting processes. Currently, in the case of road transport in Europe, the payment deadline for a transport service performed is usually calculated from the date of receipt of the paper version(!) of the original CMR transport document to the paying company's office. Replacing a paper waybill with an electronic document should make cashflows much smoother, shortening the timeline by anywhere from two to six weeks, which will significantly reduce costs and free up capital currently tied up in the settlement processes.

A key element of e-CMR is the Additional Protocol to the CMR Convention, which was ratified in 2008. To date, it has been signed by: Bulgaria, Czechia, Denmark, Estonia, Finland, France, Spain, the Netherlands, Iran, Lithuania, Luxembourg, Latvia, Moldova, Russia, Slovakia, Slovenia, Switzerland and Turkey. Poland is a party to the CMR Convention, but we have not yet signed the additional protocol concerning e-CMR. Work is underway in this area.

SAFETY PILOT – ACCIDENT WARNING SYSTEM TESTS

HTTP://SAFETYPILOT.UMTRI.UMICH.EDU
ANN ARBOR, MICHIGAN, USA

PROBLEM

A large number of road accidents and traffic jams caused by accidents.

SOLUTION

In 2012, Dziennik Internautów (Internet Journal) described tests of the Safety Pilot solution, which combined the V2I and V2V concepts.
As part of the tests conducted in Ann Arbor, MI, 3 000 cars were fitted with devices that recorded data about the speed and position of the vehicles, and sent them to other cars on the road. This allowed the driver to be warned about a possible accident.

BENEFITS

According to the National Road Safety Agency (NHTSA), it has been proven that the already developed technologies really work and are generally accepted by drivers.

According to estimates, the share of Polish carriers in the whole European market exceeded 30%, putting us in the leading position. That is why we should be all the more interested in implementing e CMR. Meanwhile, the digitisation of transport documents in road transport in Poland mainly comprises the digitisation of paper versions after the service has been provided(!). This solution is obviously sub-optimal, especially given the benefits that the use of e-CMR throughout the supply chain can generate.

In the absence of top-down regulation, bottom-up initiatives such as the GS1 global standards for identification and communication are being developed as a key factor in making the IoT concept work. GS1 is a global system of standards and business solutions created since 1973 on the initiative and under the leadership of a group of companies. The GS1 standards comprise agreed principles and guidelines that are applied uniformly by operators in many industries to improve supply chain operations.

The GS1 global standards allow the use of unique keys to identify goods, services, resources, locations, etc. worldwide. These keys can be presented in data media such as barcodes or EPC/RFID (Electronic Product Code / Radio- Frequency Identification) tags for automatic readouts.

They can also be used in electronic communication, improving the speed and accuracy of the transmitted basic data, transaction data, as well as data on current events in the supply chain. Large data sets can be collected, stored, analysed, directed, retrieved, and shared, which offers possibilities reaching far beyond the capabilities of traditional relational database systems. These days, data quality is more important than ever, and the GS1 standards are the foundation for reliable, accessible, searchable and linkable data, from basic data to extended attributes related to the identification of individual objects in the supply chain.

Information sharing as a pillar of GS1 concerns four areas:

- GS1 EDI (electronic business documents);
- GDSN (basic product data);
- EPCIS (information on events concerning the movement of goods in the supply chain);
- description of product information on the Internet.

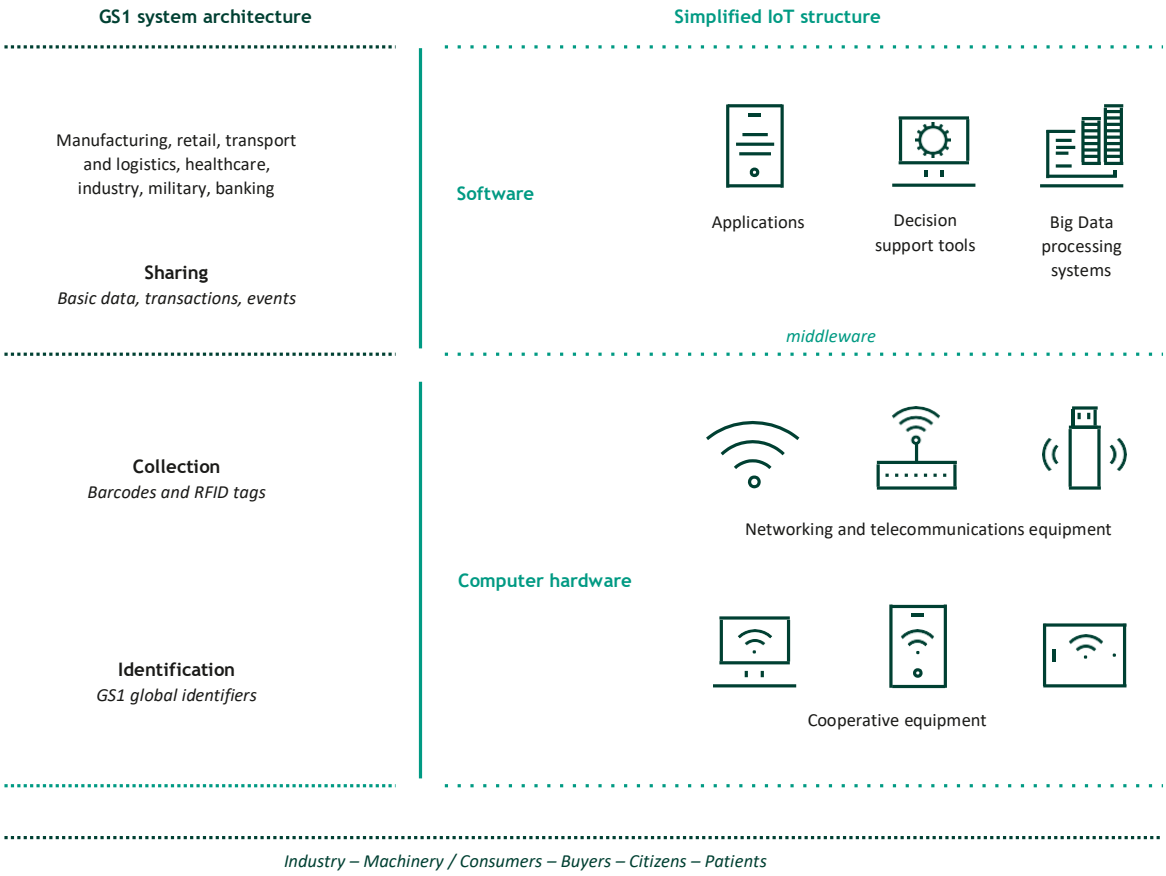
Building open registers, platforms or standard communication links in order to enable the exchange of collected data is an essential part of the GS1 organisation's activities. This aspect is also extremely important in the IoT concept for the application layer, the basic functions of which – besides ensuring data security – are data storage and analysis.

Information sharing as a pillar of GS1 concerns four areas: electronic business documents (GS1 EDI), basic product data (GDSN), information on events concerning the movement of goods in the supply chain (EPCIS), and the description of product information on the Internet. Building open registers, platforms or standard communication links in order to enable the exchange of collected data is an essential part of the GS1 organisation's activities. This aspect is also extremely important in the IoT concept for the application layer, the basic functions of which – besides ensuring data security – are data storage and analysis. Other key elements of the IoT include interconnected devices, which can encompass both barcode readers, RFID tags and sensors.

They work as interfaces between uniquely identified objects and the underlying layers of the IoT architecture, which transmit, store and analyse data.

The IoT concept also promises far-reaching benefits from the perspective of the Transportation, Freight Forwarding and Logistics sector, in particular for logistics operators, their business clients, as well as end customers. These benefits cover the entire logistics value chain, from procurement, production, warehousing operations, transport and distribution to the end customer. Thanks to monitoring the status of resources, shipments, logistics units or people in real time, the IoT provides full transparency throughout the entire supply chain. The Internet of Things can optimise the way people, systems and resources work together while coordinating their activities. Standardisation in this area is aimed at increasing the efficiency of business processes and providing savings through automation based on globally unique object identification and standardisation of communication in global supply chains.

GS1 standards in the IoT concept



Source: GS1 Poland.

Space transport is characterised by far different conditions of use, requiring specialised launch infrastructure to ensure its very existence. Breaking through the barrier of Earth's gravity and taking a spacecraft into space requires very high speeds (first and second cosmic velocities), which in turn requires equipping the spacecraft with a powerful and energy-consuming drive. This kind of transport also requires extremely precise monitoring and measuring devices, including IoT solutions, as well as a significant degree of automation. This is due to the cost of the rather expensive human factor (including the crew), the use of which involves significant inconveniences and risks, and thus costs (lack of gravity and access to natural resources, ionising radiation). Unmanned vehicles (including satellites) with varying – usually high – degrees of automation constitute a significant share of the spacecraft fleet.

The mission of the Crew Dragon capsule is an unmanned test of the system, which in the near future will be used for taking astronauts to the International Space Station (ISS) and bringing them back to Earth. Since the end of the space shuttle era the American crew programme and ISS crew exchange flights have been dependent on the Russian Soyuz system. NASA wants to end this dependence with commercial contracts for lifting crews, won by SpaceX and Boeing.

SpaceX Crew Dragon took off on 2 March at 8:49 a.m. Polish time, strapped to a Falcon 9 rocket, to start its first demonstration flight to the International Space Station. On 3 March, the Crew Dragon capsule performed a successful approach and docked with the International Space Station. The spacecraft was automatically attached to the IDA port at the Harmony module, and astronauts at the station boarded the capsule. Before docking, the spacecraft carried out several demonstration manoeuvres near the station, showing the readiness of its systems for future operations with people on board. During the flight, the booster – the lower part of the rocket – was discarded and it landed autonomously on a barge. It is worth noting that a Polish developer, Tomasz Czajka, a graduate of the Faculty of Mathematics, Informatics and Mechanics at the University of Warsaw, worked for several years on navigation and guidance algorithms. This was the first flight of an American crew capsule since the end of the space shuttle programme in 2011.

Space flights do not only include flights to the International Space Station – they can also be commercial passenger flights. Air tourism exists and is constantly growing with each passing year. It is estimated that by 2030, five million space passengers per year is a realistic goal.

The vision is to create a sophisticated space tourism infrastructure with a total of over a hundred orbital hotels and sports centres, as well as a daily lunar flight schedule and polar hotels. There are currently two ways that enable experiencing suborbital flights. The first one is modelled on the SpaceShipOne spacecraft. It uses an airplane which takes the actual spacecraft to an altitude of several kilometres, where it disconnects and launches its own rocket drive, climbing higher on its own. The return can take place in one of two ways. The spacecraft either returns to the point of departure, or to another place on Earth (this is called "space transport"). The second option, modelled on Delta Clipper Experimental, uses a rocket with a capsule on top. Then the capsule separates from the rocket at a certain altitude. Both parts return to the ground independently of each other.

In connection with space tourism, there will be a need to regulate liability for damage caused to such tourists. The conventions which are currently in force were adopted several decades ago, and not only did they not provide for such possibilities, but they also ceded all responsibility to states, which does not seem appropriate for commercial flights.

It is worth noting that Poland has the Lunares Research Base (the only one of its kind in Europe), which runs research on the psychology of human factors during manned space flights and tests of modern technologies, not only from the space sector, with the help of IoT sensors. The facility is completely isolated from the outdoor environment, and includes 250 square metres of space walking area. The infrastructure of the Base enables the constant monitoring of the vital parameters and behaviour of residents. It also ensures full immersion during simulated crew missions. The Lunares Base (also known as the Habitat) is a unique facility, bringing tangible benefits to both scientific centres, as well as the business world. The Habitat was used, among other things, for research conducted by scientists from the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw. In the study, human astronauts were cut off from the outside world, natural light and external sounds. Communication with mission control was delayed, and the astronauts themselves followed the adapted Martian time. The purpose of such simulations is to identify potential problems that may occur during actual space missions. Until now, however, the behaviour of the crew has not been measured with sociometric tools that enable high accuracy. An additional distinguishing factor of the presented mission was the simulation of accidents – the impact of disability and death on the success of the mission.

Scope of possible use of IoT solutions

In addition to the Day 1 and Day 1.5 services listed in Table 1, other applications of the IoT in transport are also possible:

- optimisation of electricity consumption in autonomous vehicles – development of the KERS (Kinetic Energy Recovery System) system based on location sensors and selection of the route with the lowest resistance;
- traffic prediction: driving times and traffic density;
- traffic management systems – collection of data on the positions, speeds and routes of other vehicles for better traffic management, by means of controlling traffic lights, proposing safe and fast routes for different modes of transport, for example drones or rail transport;
- accident or collision identification and automatically informing emergency services (eCall);
- collecting data on water levels and ice (water transport);
- vessel monitoring, vessel position mapping;
- locating vehicles, improving the capacity of the network by reducing the distance between vehicles (if necessary and possible), controlling their speed;
- supervision of the operation and maintenance of infrastructure equipment;
- optimisation of the use of individual elements of transport infrastructure, route optimisation, optimisation of the operations of the entire system;
- optimisation of the operation of public transit vehicles;
- prioritising public transit;
- detection of traffic law offences (verification of speed, unauthorised entry into a clean transport zone);
- monitoring of shipments in logistics, for example conditions of transport of special or sensitive loads (such as medicines, food, hazardous materials, oversized loads).

Barriers

In the course of its work the Working Group has identified the following barriers for the industry:

1. High complexity of transport and logistics processes.
2. Micro-scale transport planning and management (independent for different modes of transport, different spatial units and different transport managers), lack of macroscopic, holistic planning.
3. Closing transport and logistics subsystems within their own frameworks, without making data available to the outside world. Unclear prospects for the implementation of Directive 2010/40/EU of 7 July 2010 on a framework for the deployment of Intelligent Transport Systems in the Member States, including Poland.
4. Insufficient exchange of information between infrastructure managers, operators and users (licensing, closed systems, custom interfaces); this includes lack of interoperability between TMS, WMS and GPS systems, lack of exchange of information on accidents and traffic disruptions between infrastructure managers.
5. Lack of standardisation of processes and tools or their low level of dissemination, which causes companies to develop their own solutions and processes, which are not interoperable. One of many examples of this issue is the archaic data transmission process in the case of transport orders, where it is estimated that 90% of orders are sent by e-mail as a PDF file, while 10% are sent as text files. Lack of standardisation makes it non-viable to develop affordable process management programmes that disseminate modern communication and data exchange standards in line with the expectations of transport and logistics companies, especially small and medium-sized enterprises.
6. Lack of legal obligation to have geolocation equipment – in reality, this equipment is the norm for heavy vehicles, but in the case of light transport vehicles of up to 3.5 tonnes the ratio of installed geolocation equipment in cars is much lower.
7. Lack of uniform standards concerning geolocation equipment.
8. Insufficient regulation for V2V and V2I communication, as well as autonomous vehicles, despite the advanced progress of these solutions.

SCOOP@F PROJECT – STUDY OF THE INTEROPERABILITY OF MULTIPLE C-ITS SERVICES

HTTP://WWW.SCOOP.DEVELOPPEMENT-DURABLE.GOUV.FR/EN/
FRANCE

PROBLEM

Lack of verified interoperability between different C-ITS services, especially on a large scale.

SOLUTION

The aim of the project was to support the implementation of basic C-ITS services at the national level by testing the interoperability of numerous services on a large scale. This was supposed to enable verification under real-life conditions in order to test the implementation and test the interoperability of different technical solutions and services. SCOOP@F was a pre-implementation project for various C-ITS technologies in France, carried out after the successful completion of the SCORE@F field test project in July 2013. The project involved industry stakeholders and road administration, and its key partners were Renault and PSA, who were looking for a business model for all stakeholders.

BENEFITS

Large-scale cooperation of many C-ITS services has been tested in real life conditions, which will be crucial for the future implementation of such services.

9. Insufficient number of C-ITS infrastructure installations, and restrictions on reliable and efficient data transmission both towards the infrastructure (V2I) and between vehicles (V2V).

10. The use of frequencies dedicated to ITS technology by entities which obtained licences to use this band before the Ordinance of the President of the Office of Electronic Communications (Ordinance No. 56 of the President of the Office of Electronic Communications of 15 October 2009, amending the Ordinance on a frequency plan for the 5875-5925 MHz band) went into force, as well as those who are using this band illegally.

11. Insufficient possibilities for the creation of clean transport zones despite the pressing issue of air pollution in Polish cities.

12. Lack of legal possibilities for urban road managers to use automated systems to detect certain traffic law violations.

13. Currently, the SIM card used for eCall data transmission is kept on stand-by – it only activates after an accident, so the system cannot be used, for example, to find a stolen car or to monitor vehicle location for traffic forecasting or traffic management systems (autonomous vehicles may be increasingly rented for a short period of time rather than being owned, leading to lower concerns about the potential identification of users, so that information about vehicle positions can be collected on an ongoing basis). eCall is a closed, custom manufacturer subsystem which – due to its status as a critical subsystem – does not allow access to its resources (network interface) for other augmented/value-added/enhanced services.

14. Regulating the use of UAVs for video recording, seen as the greatest threat to citizens' privacy, remains a challenge.

15. Barriers to implementing automation solutions in small and medium-sized enterprises. In transport companies the generational difference is a common reason for not automating processes using IoT solutions. A significant number of business owners are reluctant to implement new IT solutions because they do not fully understand and see the need for change, or the resulting benefits. Another common issue is that they are used to old solutions and fear new systems.

Proposals for government action

The Working Group recommends the following actions:

1. Establishing a legal framework for macroscopic transport management, especially in metropolitan areas and urban agglomerations, in order to eliminate the growing problems of microscopic management; Implementing the Sustainable Transport Strategy 2030, metropolitan (agglomeration) act, acts on local government, act on public roads, act on railway transport, act on public transport into Polish legal reality, implementing (pilot) integrated multimodal, directional (defining the directions of development of transport networks and systems) and detailed (with planning value) studies, in metropolitan areas and agglomerations, with particular emphasis on multimodal nodes of the TEN-T network. Within the framework of integrated multimodal studies at a detailed (planning) level, it would be possible to identify clean transport zones and autonomous transport development zones.

2. Getting acquainted with the work of Professor Tadeusz Zipser's group at the Wrocław University of Technology, developing transport simulation software. The group is also planning to share the Orion software – a simulation and decision model, which is designed to model planning decisions taking into account the compromise between the course of spontaneous phenomena in space and the rules to be implemented according to the adopted planning doctrine.

3. Standardisation of data exchange and sharing between:
    - various infrastructure managers,
    - infrastructure managers and operators/carriers;
    - infrastructure managers and end users;
    - various vehicles (V2V communication), vehicles and
    - infrastructure (V2I);
    - geolocation systems (such as GPS), fleet management systems (TMS) and warehouse logistics systems (WMS).

4. Data protection regulations: vehicles (such as cars or drones) scan the environment and collect a lot of data, which can be further exchanged between vehicles and the infrastructure. These data should be secured. The growing availability of non-personal data should coincide with strengthening the protection of personal data.

5. Creating more precise regulations for autonomous vehicles (the Electromobility Act is not sufficient in this regard):
    - Definition of an autonomous vehicle.
    - Conditions for the approval of autonomous vehicles for testing (and then for use on public roads), including:
        - research insurance / insurance for vehicles in traffic;
        - defining liability for accidents and procedures to be followed after an accident;
        - protection of vulnerable users of the shared space;
    - Installation of sensors / V2X communication devices in vehicles.

6. Enabling local governments to create and manage access to real clean transport zones. It is necessary to introduce changes in the regulations in order to be able to use IT systems for clean transport zones in health resorts, tourist resorts and cities with fewer than 100 000 residents.

7. Enabling automatic recording of violations (such as unauthorised entry into clean transport zones). Currently, cities which can create clean transport zones do not have sufficient enforcement capacity to do so if they establish a clean transport zone.

8. Introducing an obligation to use geolocation equipment in the transport of goods.

9. Preparing technical infrastructure for the transmission, storage and processing of large amounts of data from vehicles equipped with V2I communication devices. In particular: building an infrastructure of C-ITS equipment enabling the collection of data from all kinds of vehicles, preparing databases and installing sensors and data transmission systems to collect information on vehicle locations and speeds, as well as additional transport infrastructure services, such as free parking spaces.

10. Eliminating devices which may cause interference in the frequency spectrum dedicated to intelligent transport systems. Priorities include bands dedicated to safety-related use cases (Commission Decision 2008/671/EC of 5 August 2008).

11. Establishment of the Railway Scientific and Technological Park, supporting the development of innovative solutions, as well as cooperation and coordination of activities (including in the area of R&D) between manufacturers of products, service providers and railway stakeholders.

12. Introducing a requirement for the automatic transmission of data relevant for transport and logistics processes (for example change of cargo or vehicle status) collected offline when it connects to the Internet.

13. Establishing a research and implementation centre and a decision-making centre (not functionally dispersed) in the area of transport.

14. Developing (within the Ministry of Infrastructure, in collaboration with the Ministry of Digital Affairs, as well as the Ministry of Entrepreneurship and Technology) a White Paper on Transport Automation. The White Paper should: describe projects and national programmes pertaining to transport automation, collect experiences concerning pilot projects by types and modes of transport, assess the impact of actions implemented to date. The White Paper should highlight the infrastructure layer and the vehicles. The V2V and V2I communication technologies should also be taken into account. It should also assess the production potential in Poland and the possibility of establishing value chains in the field of automation. The White Paper should offer a vision, general and detailed objectives, and recommendations for organisational activities, regulation and financing of the activities. It should also launch consultations in order to develop assumptions for a future transport automation strategy.

15. Creating and promoting educational programmes in the field of innovative technologies that solve the challenges posed by the 21st century, including the Internet of Things and Industry 4.0, including autonomous vehicle technicians (autonomous vehicle fleet managers, etc.), space transport technicians, space vehicle fleet managers, space tourism managers, space medicine technicians.

16. Establishing a competence centre responsible for the development, testing and commissioning of autonomous technologies. The creation of such a centre should take place in two stages.

    - Integration of the activities of relevant centres working on the development and testing of autonomous vehicles, taking into account all aspects necessary for the approval and commissioning of autonomous vehicles for operational use. The integration of the centres should be accompanied by the integration of the proving grounds and test areas, as well as the development of a standard for the acceptance of land for autonomous vehicle (technology) tests. Guidelines concerning the tests should be developed in order to establish tests necessary to obtain certain authorisations (such as leaving the proving grounds and moving to the testing area, or moving from the testing area to an urban area). A plan for the development of autonomous technologies should be developed with dedicated financial instruments, for example within the National Centre for Research and Development.

    - Introducing pilot lanes/calm traffic zones for autonomous vehicles during larger accompanying investments, such as the overhaul of the bypass in Warsaw.

    - Establishing a single decision-making or coordination centre for the above-mentioned activities, regulated by law, with appropriate funding.

17

FOLLOW-UP DIRECTIONS

The Working Group sees a clear need to continue the work and to jointly focus on two areas – inviting the relevant ministries to analyse in detail the proposed legal changes, and preparing practical R&D projects. The working proposals of the group are presented below.

Suggested legal changes

One of the most important barriers to the development of the IoT, which has been identified by practically all industry subgroups, is the fact that the legal system is not adapted to the challenges posed by modern technologies. In the course of the work, several dozen suggestions were drafted, which can be further divided into the following areas of law:

Telecommunications law:

- adapting the law to the characteristics of M2M communication;
- increasing limits for electromagnetic fields;
- Introducing definitions of M2M communication, an M2M terminal device;
- enabling a flexible approach to the addressing of M2M devices;
- adjusting the duration of contracts between the consumer and the supplier to the lifetime of the product;
- introducing the possibility of using biometric data for the registration and authorisation of users using telecommunication services;
- abolishing the obligation to include numbers of M2M devices in the directory enquiries service and subscriber directories;
- enabling wireless operator switching using the eSIM standard for M2M communication;
- removing the possibility of making emergency calls in M2M communication, except for IoT devices which are used for emergency and rescue purposes;
- excluding M2M communication from the obligation to provide detailed call lists on a regular basis;
- abolition of the obligation to assign numbers to M2M devices in the National Numbering Plan, introduction of lower fees for numbering M2M devices, if it is required;
- extending the powers of the President of the Office for Electronic Communication to enable taking action if there is a threat to the interoperability of communication interfaces used to transmit data from M2M terminal devices;

- extending the powers of the President of the Office for Electronic Communication with regard to the possibility of blocking / restricting sales of M2M terminal devices that pose a risk to the network due to non-compliance with telecommunications standards;

- providing the ability to process metadata from M2M/IoT communications for analytical purposes without requiring user consent, while maintaining the conditions to protect users' privacy.

Public procurement law:

- introducing provisions that will force the promotion of solutions based on advanced technologies, such as those identified in national smart specialisations;

- introducing a predefined technical dialogue process and innovation partnership supported by *soft law* instruments (such as guidelines and standards) to facilitate the application of this mode of innovation partnership in practice;

- extending the catalogue of situations in which special purpose vehicles may be used;

- promoting open tender formulas, taking into account the innovation factor in the tender criteria.

Entrepreneurship law:

- providing capabilities for the relevant body to formulate recommendations encompassing a set of contractual clauses for innovative projects using IoT technology by industry, in consultation with the NGO sector;

Personal data law:

- regulating the collection and use of machine data;

- regulating the interoperability standards for IoT equipment, for example by means of a Regulation to the Directive on the free flow of non-personal data;

- working out recommendations or other soft law instruments concerning processing data in the cloud by the Ministry of Digital Affairs in cooperation with the President of the Office for the Protection of Personal Data;

- developing soft law guidelines on the use of IoT data in the insurance sector;

- introducing language to the Act on Insurance and Reinsurance Activity granting the minister in charge of informatisation, in consultation with the minister in charge of financial institutions, the power to issue a regulation regulating the use of non-personal data by the insurance sector;

- developing regulations which will regulate the issues of the classification of individual IoT data streams, the ways they are protected, as well as the rules of data transmission and processing; as an alternative, the Ministry of Digital Affairs may also issue guidelines concerning this area;

- excluding IoT data from sector-specific secrets and developing a new way of treating such data in the context of GDPR;

- regulating motor insurance based on driver behaviour (individual rates based on driving style assessment) in the on assessment of driving style) in the Act on Compulsory Insurance, Insurance Guarantee Fund and Polish Motor Insurers' Bureau, or the Act on Insurance and Reinsurance Activity;

- adopting comprehensive regulations counteracting the discriminatory use of data, including medical data obtained via IoT systems.

- introducing regulations enabling the provision of telemedicine services via IoT devices using Big Data and without the intervention of a doctor, especially when it is unnecessary (screening campaigns for healthy people, data collection for epidemiological reasons), and financing such services from public funds;

- introducing regulations allowing the use of anonymous data collected by private entities by the public health service.

Tax law:

- regarding on-line cash registers, a change in language concerning VAT regulations from "device permanently contained in the cash register" to "device permanently contained in the cash register or application-service available on the Internet" is required, along with adding definitions of a cryptographic module, protected memory, optionally: fiscal memory in the executive regulations to the Act;

- removing the fiscal memory from the device to the application layer in order to reduce the cost of devices and accelerate the implementation of online fiscalisation, as well as new payment methods, while reducing the investment outlays of the Polish Government (from 320 million PLN) and enterprises (from 3 billion PLN) over the next 10 years;

- removing the fiscal memory of the device and moving it to the application layer (for example to the cloud, with optional blockchain-based cryptographic protection) to speed up and reduce the cost of online fiscalisation and to support the adoption of new payment methods, as well as electronic receipts.

Security:

- extending the circle of entities subject to the Act on the National Cybersecurity System to include selected industry representatives, who should meet higher cybersecurity requirements due to the data processed and the scale of such processing;

- analysis and technological recommendations for building application deployment strategies and data platforms;

- implementing additional regulations complementing the areas where the Regulation of the European Parliament and of the Council (EU) on a framework for the free flow of non-personal data in the EU does not address the challenges of using anonymous data in IoT solutions;

- developing security standards for the IoT in the Act on the National Cybersecurity System;

- issuing the "Recommendation of the Minister of Digital Affairs concerning the conditions of processing data of public entities in a public cloud," taking into account the issues and specificity of the IoT solutions, or developing another document on this subject;

- regulating the use of non-personal data by the insurance sector;

- active involvement of authorities in the work on EU regulations concerning cybersecurity reform, in particular undertaking work on a legal act, consistent with the EU regulations, governing the liability of medical IoT device manufacturers and service providers https://www.consilium.europa.eu/pl/policies/cyber-security/.

Civil law/obligations:

- extending the catalogue of forms of contract conclusion, in particular to include a form in which an enterprise could authorise a system to automatically place orders using M2M communication, without involving the natural persons authorised to conclude contracts on behalf of the enterprise in the process.

Administrative law:

- introducing changes in acts on local government and in the Act on Informatisation of the Activity of Entities Performing Public Tasks to ensure better coordination of the activities of public administration units in the area of IoT technology and popularisation of the vision of Smart Cities;

- developing a government strategy for IoT development in Poland;

- introducing amendments to acts on local government concerning the creation and supervision of special purpose vehicles, so as to maximise the sharing of IoT infrastructure between individual entities;

- establishing and implementing projects taking advantage of IoT solutions within the framework of government administration and local government, for example adopting an action strategy in this respect by the Council of Ministers, providing for the achievement of specific objectives within the framework of the implementation of financial solutions based on the IoT;

- developing soft law documents by the government administration (for example guidelines, standards or opinions on the IoT); preparing documentation templates for specific projects.

Transport and land use planning law:

- establishing a legal framework for macroscopic transport management, especially in metropolitan areas and urban agglomerations, in order to eliminate the growing problems of microscopic management; carrying out pilot integrated multimodal studies in the proposed functional areas (according to the list prepared by the TLAV subgroup) of cities and agglomerations;

- removing double mandatory civil liability insurance requirements, and basing civil liability insurance resulting from the use of autonomous vehicles solely on mandatory insurance for motor vehicle owners;

- removing the possibility for the owner of a property adjacent to the road on which the autonomous vehicles are to be tested to object to the testing of autonomous vehicles on public roads, and replacing it with a regulation in which the decision to allow the testing of autonomous vehicles on public roads will be made by the road manager at the provincial (local government roads), municipal (city with district rights), and national (GDDKiA) levels, respectively, after consultation with the provincial police chief or the provincial road transport inspector; it is reasonable to analyse the possibility of the analogous application of regulations on (road) traffic of oversize vehicles;

- introducing the possibility of testing autonomous vehicles without the physical presence of the driver in the car, for example remote-controlled vehicles;

- introducing an amendment to the Act on Traffic Law enabling the use of automated traffic supervision tools (including rule violation detection) by the infrastructure manager (city) for the area covered by the established clean transport zone;

- enabling the creation of clean transport zones in all cities, not only those with more than 100, 000 residents, in particular in cities characterised by high tourism and health resort values,

as well as abolishing time limits for charging fees; optionally: establishing clean transport zones as part of integrated multimodal studies in agglomerations.

The Working Group declares its readiness to continue working on necessary legal changes, including the development of assumptions for amendments to the laws.

R&D projects

The following list contains suggestions for projects submitted by members and supporters of the Working Group, which should be considered as a starting point for further debate. The selected projects will be the focus of the Group's work starting in June 2019. We invite every stakeholder interested in this area to work with the Group.

At the level common to all sectors, the Working Group identified the following necessary areas of focus:

- developing recommendations for universities offering new majors focusing on IoT technology, regarding educating experts with skills relevant to market needs (my personal proposal – to be approved/modified);
- establishing an IoT project incubator at the Ministry of Digital Affairs;
- establishing the National/Integrated Innovation Support System, which would support innovators on the journey "from idea to industry";
- establishing an innovation financing mechanism to co-finance pilot implementations and PoC projects for end users, covering innovative products of both start-ups and mature companies;
- providing adequate infrastructure for IoT data transmission, as well as for data storage and processing.

The ideas of industry project groups are also worth considering.

Security and Certification

- building a common glossary of IoT terms

which will be used throughout the legislation, as well as in standards, best practices and educational materials;

- developing standards regarding security, interoperability and standardisation, as well as corresponding certification methods;

Transport, Logistics and Autonomous Vehicles

Planning multimodal / integrated transport:

- integrated territorial transport network planning;
- planning optimal, multimodal travel and delivery routes (taking autonomous vehicles into account) using IoT devices;
- using the IoT to reduce transport pollution, for example by planning and establishing clean transport zones;
- linking transport with other Smart City elements in agglomerations;
- carrying out simulation analyses of autonomous vehicle traffic and autonomous transport systems, taking into account multi-criteria sub-optimisation, as well as structural and parametric sensitivity, with particular emphasis on the specificity of Polish cities.

Finance and Insurance

- conducting technical dialogue and carrying out a pilot implementation of a new architecture for exchanging information with the Internet and recording cryptographically protected receipt data outside the protected physical memory of cash registers;
- developing new payment methods for public transit services through the installation and standardisation of Bluetooth beacon sensors in public transit vehicles and at bus stops;
- promoting solutions for the insurance sector based on the use of real-time telematics for vehicle data, including location, information on whether the vehicle is in use or stationary, as well as drivers' driving style safety.

Smart Cities and Buildings

Establishing a national Smart City interoperability framework.

Healthcare

developing a national system for providing cybernetic, cloud-based care for a large population of patients (to be built on the basis of a demo version created as part of Demonstrator 1.1.2 of the National Centre for Research and Development).

Agriculture and Environmental Protection

- building a network of agro-meteorological stations across the country; expansion of the existing ODR network, installed in certain areas of the country, which enables the collection of data on risks, aggregated in an agricultural data cloud and made available via an API;
- monitoring the condition of bees in Poland – creating a competitive national monitoring solution to enable beekeepers to ensure bee health by controlling the living conditions of bees in hives, including temperature, humidity and disease detection, as well as developing an apiary management and decision support system, along with bee maps of the country;
- monitoring air quality based on low-cost air quality sensors calibrated using reference stations; the expansion of the network supplementing the State Environmental Monitoring system will enable collecting of a lot of data that were previously impossible to obtain solely using the State Environmental Monitoring system.

Industry

- implementing a research (TRL I-VI) and development project (TRL VII-IX) — Development of an open data exchange platform available to market participants and technology companies;
- implementing projects for the construction of a test road between Poland and Lithuania using IoT technologies for testing autonomous vehicles; implementing an innovative services model, including insurance services in the new reality of autonomous cars;
- carrying out a dedicated Scale Up programme for the development of IoT technologies in Poland.

Working Group for the IoT – Members, observers and supporters

The following list includes all the people who actively participated in Working Group meetings or took part in the editorial work remotely (making comments directly to the MoDA Editorial Team or to respective subgroup leaders).

Security and Certification

Leader – Czarnowski Aleksander, AVET Information and Network Security
Jakubiak Adam, Polkomtel
Karpiński Andrzej, Orange Polska
Kowalczuk Konrad, MGK.net.pl
Krauze Michał, T-Mobile Polska S.A.
Kubiak Wojciech, GASPOL S.A.
Kuczorski Arkadiusz, Oracle
Łazarz Łukasz, CAN-PACK S.A.
Oko Jacek, Wrocław University of Technology
Piotrowski Andrzej, UTC Fire & Security Polska
Radawiec Rafał, Wrocław University of Technology
Steczowicz Bartłomiej, Teraz Energia
Więckowska Mariola, LexDigital
Zarembiński Jakub, Sygnet

Finance and Insurance

Leader – Wolski Marcin, Billon Group startup
Brozowski Piotr Jan, National Chamber of Tax Advisers
Kluwak Tomasz, National Chamber of Tax Advisers
Krzywania Przemysław, BKF Myjnie Bezdotykowe
Kuna Mariusz, Polish Chamber of Insurance
Kwieciński Michał, Platforma Detalistów
Leciejewski Maciej, Regent Insurance Brokers (Poland)
Panufnik Tomasz, Dell EMC|Public
Zacharjasz Igor, Visa Innovation Incubator

Smart Cities and Buildings

Leader – Wiśniewski Remigiusz, Detecon International GmbH
Bakalarz Rafał, Netia
Bałos Michał, EmiTel S.A.
Bergmann Krystian, Fibar Group S.A.
Chomiczewski Witold, Chamber of Electronic Economy
Choroś Patryk, SAS Institute
Czuszek Krzysztof, Stowarzyszenie e-Południe – EPIX
Gamza Zbigniew, Municipal Data Processing Centre – Wodzisław Śląski
Jarosiewicz Mateusz, Smart Cities Poland
Kamysz-Turbak Marta, Tarnobrzeg Municipal Office
Klimas Damian, University of Wrocław
Kołoszczyk-Jakubowski Tomasz
Kraska Marcin, Institute of Logistics and Warehousing
Maroszek Franciszek, Nokia Solutions and Networks / Hackerspace Wrocław Association
Leśniak Klaudia, Indoorway
Orchowski Kacper, Deloitte Consulting
Pietrzak Roman, ITI EMAG
Polski Mirosław, Hewlett-Packard Enterprise Poland
Serafin Marcin, Kancelaria Maruta Wachta
Stefański Mateusz, Microsoft
Urbaniak Maciej, Ministry of Investment and Development
Wierzejski Arnold, Nokia

Healthcare

Leader – Bień Krystian, Polpharma sp. z o.o.,
Kozminski University
Jackowski Michał, DSK Kancelaria & LexDigital
Kołc Bogusław, PZU Zdrowie S.A.
Komar Michał, kancelaria prawna D. Dobkowski
Kurasiński Michał, Polpharma sp. z o.o.
Niewiadomski Bartosz, Aviva Group
Talarek Piotr, TBT i Wspólnicy
Wiktor Dawid, cryptocurrency investor
Zwoliński Piotr, Łazarski University

General

Leaders: Zamłyński Marek, IDC (until December 2018);
Mieczkowski Piotr, Digital Poland Foundation
Smulski Jarosław, IDC
Besiekierska Agnieszka, Kancelaria Noerr Biedrecki
Dyśko Mateusz, Peter Nielsen & Partners Law Office Sp.k.
Federowicz Rafał, federowicz.eu
Gałęzowska Karolina, PwC Legal
Grabia Michał, Institute of Logistics and Warehousing
Hryszko Arnika, Stowarzyszenie Jakości Systemów Informatycznych
Hryszko Jarosław, Stowarzyszenie Jakości Systemów Informatycznych
Gałagus Michał, Polish Chamber of Information Technology and Telecommunications
Kocięcki Maciej, Orange Polska
Konarski Xawery, Kancelaria Traple Konarski Podrecki i Wspólnicy
Mednis Arwid, PwC Legal / University of Warsaw
Matysiak Michał, Kancelaria Traple Konarski Podrecki i Wspólnicy
Mińkowski Marcin, Oracle
Sikorski Marcin, Stowarzyszenie Jakości Systemów Informatycznych
Stokalski Borys, Polish Chamber of Information Technology and Telecommunications

Smart Metering

Leader – Wadas Krzysztof, Cyfrowy Polsat Group
Chorążyczewski Artur, Revive Machines
Falandysz Jaromir, ENERGA, Association of Energy Trading
Gabryś Marek, AIUT
Galant Marek, Revive Machines
Galas Paweł, Orange ENERGA, Association of Energy Trading
Golik Piotr, T-Matic Systems S.A
Gręblicki Jerzy, AIUT
Grochla Krzysztof, Institute of Theoretical and Applied Informatics, Polish Academy of Sciences
Jankowski Andrzej, Aquard
Kotewicz Radosław, Comarch S.A.
Kowalski Rafał, Diehl Metering
Pietrzyk Slawomir, IS-Wireless
Ratyński Mikołaj, T-Mobile Polska
Smoliński Rafał, Yoberi
Ślęczek Wojciech, Polkomtel
Wądołowski Piotr, T-Matic Systems S.A.
Zawadzka Anna, kancelaria prawna Lewandowska

Industry

Leader – Nawrocki Kamil, Bconnect
Boniecki Szymon, Monterail
Gliszczyńska Beata, PZU Lab S.A.
Gołębiewski Dariusz, PZU Lab S.A.
Iwaniuk Maciej, Ernst & Young
Kuczyński Marek, PZU Lab S.A.
Łobaziewicz Monika, University of Warsaw
Nachyła Dariusz, Every European Digital
Serafin Tomasz, AIUT
Ślęk Bogdan, Signify Poland
Widórek Jarosław, Comarch S.A.
Zalewski Tomasz, kancelaria Bird & Bird

Agriculture and Environmental Protection

Lider – Płóciennik Marcin, Poznań Supercomputing and Networking Center (PSNC IBC PAS)
Białousz Jerzy, Inventia
Mańkowski Rafał, Polish Chamber of Insurance
Misiek Michał, Airly
Kolasiński Michał, Agrospot
Kowalski Piotr, Orange Polska
Pietroń Jakub, JMLabs
Poniewierski Aleksander, Ernst & Young
Prądzyński Michał, Agrotechnology
Rajtar Tomasz, Poznań Supercomputing and Networking Center (PSNC IBC PAS)

Telecommunications

Leader – Michalski Mateusz, mTechnology / Hackerspace Wrocław Association
Barcikowski Michał, T-Mobile Polska
Dylik Tomasz, Exatel
Dziomdziora Wojciech, Kancelaria prawna
Domański Zakrzewski Palinka
Gęsiak Przemysław, Polkomtel
Gorzkowska Katarzyna, AP Law
Górski Janusz, T-Mobile Polska S.A.
Grabowski Sebastian, Orange Poland
Kogut-Czarkowska Magdalena, IAB Polska Association of Employers of the Internet Industry
Kozłowski Krzysztof, Orange labs
Modelski Józef, Warsaw University of Technology
Mroczkowski Jarosław, EmiTel S.A.
Piechocki Artur, Internet Domain Arbitration Court at the Polish Chamber of Information Technology and Telecommunications
Staszak Maciej, EmiTel
Sugak Marcin, Ericsson

Transport, Logistics and Autonomous Vehicles

Leaders – Gora Paweł, University of Warsaw
Hajduk Damian, strategic advisory and management in transport and logistics
Chłopik Monika, Polish Chamber of Insurance
Choromański Włodzimierz, Warsaw University of Technology
Darowska Małgorzata, Ministry of Infrastructure
Domański Marcin, Napraw Sobie Miasto Foundation
Dzięcielski Michał, Adam Mickiewicz University in Poznań
Gawliczek Łukasz, Ave Cargo
Grabarek Iwona, Warsaw University of Technology
Grabowski Waldemar, University of Zielona Góra / SNaFi Association of Physics Teachers
Horzela Agata, GS1 Polska
Jacyna Marianna, Warsaw University of Technology
Klusek Michał, Head Office of Geodesy and Cartography
Konert Anna, Łazarski University
Kosiło Tomasz, Warsaw University of Technology
Kostrzewa Konrad, Veturai Automotive Sp. z o. o.
Kruszewski Mikołaj, Motor Transport Institute
Krystyniecka-Konopczak Magdalena, LOT Polish Airlines
Krzykowska Karolina, Warsaw University of Technology
Malinowski Zbigniew, Geo-System
Matysiak Arkadiusz, Motor Transport Institute
Mazur Bartosz, Napraw Sobie Miasto Foundation
Moskwa Radosław, CM Logistic
Orzechowska Renata, Polish Chamber of Insurance
Przecherski Piotr, Olczak – Klimek, Van der Kroft, Węgiełek Kancelaria Radców Prawnych
Siergiejczyk Mirosław, Warsaw University of Technology
Stańczyk-Miścicka Paulina, Civil Aviation Authority
Szafrański Zbigniew, Doradztwo Kolejowe
Szarata Andrzej, Krakow University of Technology
Szustek Jarosław, Tramwaje Warszawskie
Wilczewski Grzegorz, DAWIS IT Sp. z o.o.
Wolniewicz-Warska Ewa, Kapsch Telematic Services

In addition, the Working Group was joined during individual meetings by special guests:

24.08.2018 – Inauguration of the Working Group's project – Minister Karol Okoński, Secretary of State, Ministry of Digital Affairs, and Minister Marcin Ociepa, Undersecretary of State, Ministry of Entrepreneurship and Technology.
16.10.2018 – Tomasz Jamróz, Counsellor, Department of Economic Cooperation, Ministry of Foreign Affairs (Polish Technology Hub – opportunities for Polish IoT technologies on the international forum).
06.11.2018 - Waldemar Izdebski, Chief National Surveyor (Spatial data visualisation possibilities and the potential of GUGIK systems for Polish business in terms of IoT).
04.12.2018 – representatives of sister working groups at the Ministry of Digital Affairs: The Working Group for Data Openness – (New ISP Reuse Directive and High Value Data Catalogue proposal) and the Working Group for AI – Michał Pukalak, coordinated by the Department of International Policy.
22.01.2019 – Luiza Modzelewska, Deputy Director of the Department of Economic Regulation Improvement, Ministry of Entrepreneurship and Technology (presented the concept of the Simple Joint Stock Company (PSA), and Dr. Elżbieta Andrukiewicz, Institute of Communications (IoT device certification – reference standards and first initiatives).
05.03.2019 – Małgorzata Darowska, Plenipotentiary of the Minister of Infrastructure for Unmanned Aircraft and the Central European Drone Demonstrator Programme, Ministry of Infrastructure (BSP White Paper), and Jarosław Rupiewicz, Department of Unmanned Aircraft, Civil Aviation Authority (Unmanned Flight Regulations).

WE ARE WORKING ON THE

POLISH INTERACTIVE INNOVATION MAP

Check out what your neighbours are doing.

Add your project!

Visit the website at:

www.gov.pl/web/cyfryzacja/mapa-innowacji