Chapter 22

INTERNET OF INTELLIGENT DEVICES APPLICATION IN INSURANCE

Internet of Things (IoT), Blockchain technology, software robots and various aspects of artificial intelligence, as trends within the Fourth Industrial Revolution[1], have great potential for applications in insurance field.

The Internet of intelligent devices consists of a large number of sensory devices, which are connected to the Internet and independently collects, share and use data without human assistance, by executing software commands set by humans.

IoT devices enable essential digitalization, that is, connect the digital and physical worlds by letting parameters from the real world to enter digitized into the virtual world of the Internet. An inverse transformation is also possible when needed, so the processed data requires real-world intervention via actuators. On the other hand, the potential danger is the fact that this innovation is encroaching on privacy and can have a major impact on a person's private life.

Televisions, refrigerators, lamps, thermostats, radiators, speakers, trash cans, switches, etc. whose sensors detect motion, smoke, temperature, sound, lighting and the like can be connected to the Internet. Gartner estimates[2] that by 2020, the number of intelligent devices connected to the Internet will exceed 20 billion.

The subject of this paper is the analysis of possibilities for improving the business of the insurance industry using the technology of the Internet of intelligent devices, as well as the challenges that arise. The paper aims to point out the potential benefits of the involvement of Serbian insurance companies in one of the trends brought about by the Fourth Industrial Revolution.

[1] Pavlović. B. (2019). Robot Application in Insurance. In: Contemporary Trends in Insurance at the Beginning of the Fourth Industrial Revolution. Kočović, J., Tomašević, M. et all (eds.). Belgrade: Faculty of Economics Publishing Center, p. 143-160.

[2] Vega, M. (2019). Connect All the Things – Internet of Things Statistics 2020. http://review42.com

The name[3] Internet of Things was introduced by a British scientist who led the RFID sensor research at the Massachusetts Institute of Technology (MIT) in Cambridge, Kevin Ashton in 1999 to describe a system that connects the Internet to the physical world through ubiquitous sensors.

Definition

The Internet of intelligent devices is defined[4] as a global network infrastructure that enables the connection of physical and virtual devices with interoperable communication protocols and intelligent interfaces.

The Internet of intelligent devices is based on many different technologies, which are necessary to create an environment for its functioning. These are: semiconductors, chips, processors, memories, etc., of which the necessary hardware is made; software modules for connecting devices, e.g. API connectors; IoT platforms - specialized operating systems and the like; the wireless or cable network to which the devices are connected.

IoT system components

The IoT system consists of three basic components: smart devices, the network infrastructure to which they are connected and systems that receive, store and process data generated and sent by smart devices.

A smart device

An intelligent device is a simple computer that has power, memory, a processor, an input/output interface for sensors, and a communication interface that can communicate with other devices in the environment and perform pre-programmed operations. Smart devices include: environmental sensors, which can be classified by the type of physical phenomenon they measure: thermal, mechanical, chemical, optical, radiation sensors, acoustic and other sensors; actuators or control motors that, based on changes in the environment detected by the sensors, perform activities in the physical world; microcontrollers with interfaces for connecting to other devices: sensors, actuators and communication devices for wireless data transmission; microcomputers that have a microprocessor, memory, and input-output devices.

[3] Eshton, K. (2009). *That 'Internet of Things' Thing*. http://www.rfidjournal.com

[4] Radenković, B., Despotović-Zrakić, M. et al. (2017). *Internet inteligentnih uređaja*. Fakultet organizacionih nauka, Beograd

Two following open-source operating systems for smart devices are most commonly used. Contiki is the first operating system to enable IP communication, implemented in programming language C. FreeRTOS is an operating system that allows the application to run in real-time, just when an event on the system is about to occur and enable TCP / IP communication.

IoT devices are connecting, exchange data and analyze them without human involvement in these processes. Human intervention is only required when installing and programming the device.

Internet intelligent devices can be home appliances, printers, cars, industrial machines, devices in power systems, devices in health systems and others. Although similar in nature, computers, smartphones and routers are not considered to be IoT devices but part of the traditional Internet. The OECD, on the other hand, thinks such a division is incorrect[5] because the devices mentioned are the brains and hearts of any smart device system involved.

Network infrastructure

The network infrastructure consists of routers, switches, cables, etc. Typically, IoT devices are connected to the Internet wirelessly. Wireless sensor networks use small multifunctional platforms that connect wirelessly and deliver collected data from sensors to remote systems that process data.

Intercommunication of intelligent devices enables reading of measurements of various physical parameters, remote control of vehicles, monitoring of patients' health status, remote security monitoring, automation of various industrial processes, etc.

The following protocols are commonly used to communicate IoT devices:

- Ethernet (IEEE 802.3 standard) is the most widely used wired technology for LAN and WAN networks, characterized with possession of an interface card with a 48-bit MAC address, which is a unique device identifier, by each device;
- Wi-Fi (IEEE 802.11 standard) is a technology for local wireless networks;
- WiMAX (IEEE 802.16 standard) was named from Worldwide Interoperability for Microwave Access, it is a broadband wireless technology that can be used over longer distances, with faster throughput and more users than Wi-Fi technology;
- Bluetooth (IEEE 802.15.1 standard) is an example of ad hoc wireless networking of a large number of devices by radio waves;

[5] OECD (2015). *OECD Digital Economy Outlook 2015*. OECD Publishing

- ZigBee (IEEE 802.15.4 standard) provides access to LR-WPAN (Low Rate Wireless Personal Area Networks), a short-range wireless network with low data rates.

Data processing and storage systems

The optimal solution for developing and deploying applications using IoT data is cloud computing.

Cloud computing enables users, on request, to access via the Internet, all the necessary computer resources: servers, data storages, applications, services, etc. It is based on virtualization technology, which involves hosting services and user data on shared resources and provider infrastructure.

By increasing the use of the Internet, intelligent devices are significantly increasing the amount of data transmitted over the Internet and stored in data storages worldwide. Such data cannot be processed using traditional database management tools. That's why new ways of storing and analyzing large amounts of real-time data have been developed, based on Big Data technologies.

The term Big Data is an information resource of high volume, high speed and great variety of data, which requires new and innovative methods of processing and optimizing information and improving insight into data content and decision making.

1. LITERATURE REVIEW AND HISTORICAL DEVELOPMENT

A large number of authors around the world have been dealing with the Internet of intelligent devices over the last forty years, while the use of this technology in the insurance industry has begun to intensify relatively recently, some ten years ago. The authors in Serbia have also shown interest in this topic.

The basic concept of connected smart devices was developed at Carnegie Mellon University on a modified Coca-Cola beverage vending machine in 1982, which could have informed the plant how many cans it had for sale and whether the cans in the refilled device were sufficiently chilled.

In 1991, Mark Weiser[6] described the vision of the modern Internet of intelligent devices in his work "Computer of the 21st Century"; while in 1994 Reza Raji[7] published the concept of IoT in the IEEE magazine.

The first attempts to realize the Internet of intelligent devices were Microsoft at Work (MaW)[8] and Novell Embedded System Technology (NEST)[9]. MaW provided protocols for connecting photocopiers and fax machines to computers and Lexmark supplied the first such device, WinWriter 600, in 1994. Due to the few devices that supported such a protocol, the project was abandoned in 1995. Novell wanted to connect devices such as TV set-top boxes, candy vending machines and the like to the network. Lexmark and several other printer manufacturers joined the project in 1994. For the same reasons as Microsoft, Novell quit the NEST project in 1997.

The name Internet of Things[10] was introduced by a British scientist at the Massachusetts Institute of Technology (MIT) in Cambridge, Kevin Ashton, in 1999 as the title of a presentation for Procter & Gamble on advancing their supply chain.

Cisco introduced the interesting definition of the Internet of intelligent devices, as the moment when more devices than humans will be connected to the Internet, which happened in 2008. In the same year, a group of companies, including Cisco and Sun, promoted IPSO (IP for Smart Objects) Alliance to promote the use of IP protocols for smart device networking.

Telecommunication Standardization Division of the United Nations ITU (The International Telecommunication Union) formed the Global Standards Initiative on the Internet of Things (IoT-GSI) working group, which in 2012 defined[11] IoT as a global information society infrastructure that enables advanced (physical and virtual) networking of things, building on existing and interoperable information and communication technologies in development.

[6] Weiser, M. (1991). The Computer for the 21st Century. *Scientific American 265* (3), p. 94-104.

[7] Raji, R. (1994). Smart Networks for Control. *IEEE Spectrum 31* (6), p. 49-55.

[8] Baran, N. (1995). Whatever Happened To... Microsoft At Work? *Byte Magazine Vol. 20* (7), p. 30.

[9] Salamone, S. (1995). Novell Builds a NEST. *Byte Magazine Vol. 20* (8) p. 151-152.

[10] Eshton, K. (2009). *That 'Internet of Things' Thing*. http://www.rfidjournal.com

[11] Global Standards Initiative on Internet of Things (2012). *Recommendation ITU-T Y.2060*

In recent years, Serbian authors have published papers on the application of IoT in the infrastructure of educational institutions[12], educational games[13], cultural heritage monitoring[14], retail promotion[15], measurement of health parameters in wearing devices[16], rail traffic[17], etc.

2. THE CONCEPT OF IoT

The basic concept of the Internet of intelligent devices is explained in Figure 1. A key feature of IoT devices is to add value to classic products by connecting them to the Internet or adding a digital service to a physical product that enhances its core function. In this way, a new product is obtained, through the synergy of the physical product and digital services, which together have a greater value than the sum of their values. Apple's watch, iWatch, is still a watch, but it also has a microphone, speaker, GSM card or Bluetooth connection to a mobile phone, so it can serve as a phone call. The iWatch also has additional property, it is fashion detail. The Intellion box, in addition to its basic storage function, has sensors that detect its occupancy and when emptied to a certain level, the box contacts the seller to send a refill.

[12] Simić, K., Despotović-Zrakić, M. et al. (2015). Model infrastrukture obrazovne institucije zasnovan na Internetu inteligentnih uređaja. *Infoteh Jahorina Vol 14*. p. 681-685.

[13] Petrović, L., Jezdović, I. et al. (2017). Razvoj edukativne igre zasnovane na Internetu inteligentnih uređaja. *Infoteh Jahorina Vol. 16*, p. 506-509.

[14] Matejić, T., Marković, N. et al. (2017). Monitoring dobara materijalne kulturne baštine primenom interneta inteligentnih uređaja. *Časopis Info M 64,* p. 11-17.

[15] Tomanović, I. (2017). Primena internet inteligentnih uređaja u unapređenju maloprodaje. *Časopis Info M 64*, p. 18-25.

[16] Rodić Trmčić, B., Labus, A. & Bodanović Z. (2016). Model mobilnog zdravstva zasnovan na tehnologijama wearable computinga. *Časopis Info M 57,* p. 48-54.

[17] Mladenović, S., Uzelac, A. et al. (2016). IoT u železničkom saobraćaju – realnost i izazovi. In: *Zbornik radova sa XXXIV Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju PosTel 2016*.

Figure 1. The logic of IoT products and services

Thing + hardware & software =		Function of thing	+	Extra digital service
		Timing		Phoning
		Keeping things in a box		Refilling
		Riding a bicycle		Bicycle Rental and Fleet Management
		Refrigeration		Establishing energy efficiency, remote control and cost savings
		Driving a car		Insurance, usage billing, theft prevention, driving style recognition
		Lighting		Security monitoring, heating control and remote control
		Anything		Installation and maintenance instructions, maintenance schedule and history, usage billing, recharge services, warranty checks, insurance, etc.

Source: Fleisch, E., Weinberger, M. & Wortmann, F. (2014). *Business Models and the Internet of Things*. Zurich: Bosch IoT Lab White Paper, p. 8.

Characteristics of IoT

IoT devices dynamically adapt to the environment and independently respond to changes from the environment. They are configured with minimal user participation. IoT devices communicate with each other through standardized interoperable communication protocols and have a unique identifier, such as an IP address or Uniform Resource Identifier (URI), through which users can access a device via the Internet, remotely control, configure and monitor a device. They are connected to a computer network that allows them to communicate with each other and be visible to other devices and applications.

Application of IoT

Deployment of intelligent devices can be encountered in many different areas:

- Automation of apartments, offices, houses and office buildings by: smart devices for controlling electricity, lights and heating; remote media management; increasing energy efficiency; maintenance automation; remote reading and measurement; sensors for chemical, biological, radiological and nuclear damage to home security;
- City automation using; telemetry (smart parking, remote sensing and various vending machines); intelligent transport systems; smart city traffic management; connecting citizens with public infrastructure; power grid management;
- Automation of industrial plants and factories;
- Fleet management implies that IoT devices enhance the following services: autonomous vehicles; driver and passenger safety; emergency services; operating and supervising rental vehicles; integration of entertainment and travel information services; GPS services; monitoring of delivery of goods; remote diagnostics of malfunctions, i.e. correctness of vehicles;
- Monitoring of vital parameters of patients and athletes using wearing IoT devices;
- Assistance to patients in daily life and medical services;
- Security surveillance;
- Monitoring of weather, air pollution, noise, fires and floods;
- Automation of irrigation systems and control of greenhouses in agriculture;
- Payment via Point of Sale terminal;
- Military applications in advanced weapons and systems and
- Insurance, which will be discussed more in this paper.

Various devices have nowadays received Internet connectivity and a certain level of intelligent behavior. According to Gartner's research[18], more than half of all intelligent devices are home consumer products, but the best-selling IoT devices in the world are security cameras and smart electrical meters.

Challenges in implementing IoT

Many companies refrain from implementing new technologies because they are not sure that the expected benefits of implementation are large enough to pay off all the challenges. The implementation of the Internet for intelligent devices raises some concerns about Internet security. With the device connecting to the Internet, there is a serious threat of hacking and misuse of sensor data. In case of a successful compromise of the data from the sensor, an additional risk lies in the automatic response of the system to the wrong input data, which certainly cannot be adequate. Therefore, since the beginning of the implementation of IoT technology, special attention has been paid to cybersecurity. Given that the entire IoT platform is connected to the Internet and open to attack, it can never be completely certain that hackers will fail in their intentions. However, by implementing the following measures, the risk of hacking attacks can be reduced to a reasonable extent: deployment of a demilitarized zone into the system, systematic identity management on the local network, VPN connections with IoT devices, monitoring of intrusions into the system, adequate management of network equipment, updating operating system versions and software, implementation of all available patches, regular cyber risk assessment with the help of an IT auditor, performing penetration tests, detecting system vulnerabilities and preparing a plan of action in case of hacker attacks detection.

The return on investment in IoT is not fully known, which further complicates the company's management's decision to implement. In addition to security risks, managing organizational change that requires "the silo" to break down in organizations increases the uncertainty of implementation success. The introduction of IoT integrates and changes all processes and sectors within a company, which some sectors are often not prepared for. It also requires new knowledge and technological skills, adopting new business models, as well as changing the way employees work and think, to which a certain number of employees cannot adapt.

Integration with systems with outdated technology can be a challenge for implementing IoT in individual companies. Does it make sense to replace a 25-year-old machine in a factory that still does its job perfectly, just to make the

[18] Antić, D. (2019). *Šta je Internet of Things (Internet inteligentnih uređaja)?* http://samoobrazovanje.rs

new machine compatible with IoT technology? Will the benefits of introducing IoT be large enough to pay off a new machine? If new technologies are ignored, how long will the company survive in the market?

Finally, the legal risk of introducing IoT platforms cannot be ignored. The issue of data ownership is still open, while data privacy can be relatively easily compromised.

When deciding on the implementation of IoT technology, it is important to take a good look at all of these challenges. If a decision is made, a prerequisite for successful implementation is to prepare a strategy to avoid all potential problems.

3. APPLICATION OF IoT IN INSURANCE

There is great potential in insurance companies which decide to apply IoT. They will be able to develop higher-quality tariffs, more accurate risk measurement, more adequate premiums for policyholders, automatic receiving of claims data, more accurate claims assessment, prevention, etc.

Tariffs

The abundance of data from an IoT device can help insurance companies to more accurately measure risks, introduce more parameters into tariffs, and thus more adequately charge risk to policyholders, and even introduce an individual tariff for each policyholder in the future. Currently, insurance companies are most concerned with the use of telematics vehicle insurance data to determine the specific risk of each driver.

Prevention

Once the inappropriate behavior of the contractor is identified, the insurer will be able to respond on time and propose, and even in certain cases, take corrective action. Also, pre-programmed corrective actions for certain types of insurance, such as property and liability insurance, will be able to automatically correct human errors and thus significantly reduce the frequency of damages.

Damage settlement

When an insured event occurs, the sensors will send enough data to quickly assess the damage. It will be easier to decide on the justification of the claim because it will be known for every insured person and the insured thing if they are behaving per the contractual conditions, e.g. whether the insured vessel sailed an approved route, whether the insured supplies were kept at the appropriate temperature and the like.

Other

In addition to standard processes in the insurance industry, IoT can be applied to improve the customer experience with insurance companies, that is, to increase the loyalty of policyholders. IoT can help create added value for both the policyholder and the insurer and thus strengthen their relationship. Insurance companies can obtain a large amount of personal information of the insured persons, which can be used to better understand their health, living conditions, living environment, movements, etc. to offer them a better and more personalized service.

The implementation of modern technologies in insurance, as a side effect, which is not insignificant, changes the impression of millennials that the insurance industry is boring and the products incomprehensible. On the contrary, they are keen to work at insurance companies and take an interest in insurance products, which give them additional benefits, such as tips on driving style or health.

Challenges of using IoT in insurance

Like any other technology, IoT also has specific[19] challenges.

A drastic change in the existing business model

The obvious benefits of implementing IoT for insurers are better risk management and claims reduction. These benefits lead to a significant reduction in insurance premiums, which can be a big problem for the traditional insurance business model. As the claims becomes less and less frequent, the fear of risk naturally diminishes and the demand for insurance decreases.

Traditional insurance companies face an additional problem, as in the field of IoT insurance they compete with new companies focused only on that segment, which is why they can operate cheaper and more efficiently. Automobile manufacturers and major IT companies like Google and Amazon are also planning to join IoT insurance. They has an initial advantage because have already developed some IoT technology for vehicles.

[19] Black, N. (2020.) *5 Challenges for IoT in the insurance industry*. www.sas.com

Finally, insurance that relies on the Internet of intelligent devices brings big discounts to policyholders who are at lower risk and big malus to others. Therefore, it may be possible for most good clients to switch to new technology companies that use IoT in risk measurement, while bad ones remain with traditional insurers, making their existing insurance price unsustainable.

In the end, as IoT devices in autonomous vehicles take over safety concerns, so the MTPL insurance will become less important, and the focus will shift to liability insurance for vehicle manufacturers and road management companies.

Data management

The insurance business is based on the use of past data, especially in actuarial and business decision making. Smart devices generate a huge amount of data, which cannot be processed in the traditional way, which poses a particular challenge for insurers who have failed to process even existing data appropriately.

Data ownership

The open question, to which data about the insured persons or their property, collected by the IoT devices provided by the insurers to the clients and processed by the insurers belong, depending on the position taken by the regulators, may lead to certain problems in the future.

Data security

The Internet of intelligent devices is inherently interesting and accessible to hackers. In addition to the relatively high vulnerability of data capture devices (cameras, sensors, etc.), transporting large amounts of data through the Internet provides an additional opportunity for hackers to intercept, exploit, or modify data sent by IoT devices to insurers.

Examples of implementing existing IoT devices into insurance

Often, information from existing non-insurance IoT device sensors can be used to reduce risk exposure for policyholders and insurers to avoid damages, which will be explained in the few examples[20].

[20] Cannan, M., Lucker, J. & Spector, B. (2016). *Opting in: Using IoT connectivity to drive differentiation – the Internet of things in Insurance*. Westlake: Deloitte University Press.

One of them is embedded sensors in commercial infrastructure which can serve to detect the occurrence of smoke, water or polluted air, thereby reducing the risk of potential insured hazards being realized. Sensors worn in clothing or footwear monitor health parameters may also serve to alert the insured person to move in the danger zone and to provide information that prevents insurance fraud. Sensors in the home or office can detect the appearance of moisture in the wall, which precedes the bursting of the water pipe, and promptly warn the insured to repair the pipe and prevent the occurrence of major damage due to water leakage from the installation. Diabetic socks with sensors that alert to poor blood circulation in the feet, high pressure, etc. which can also be used preventively for other policyholders to warn of possible upcoming cardio-vascular problems and to avoid higher health insurance costs.

Examples of IoT Implementation in Insurance

Certain IoT solutions have already been implemented in practice and are being used by insurers around the world, and there is one example in the insurance market in Serbia. The following will address several specific examples of the application of this technology in the insurance industry.

Telematics in vehicle insurance

One of the first applications of IoT in insurance is telematics. More than ten years ago, the use of sensors in vehicles began, which provided insurers with information about the driving style of the insured to determine the individual risk profile. Initially, sensors were installed by insurers in vehicles, whereas nowadays, sensors are installed by vehicle manufacturers, and drivers and insurance companies use their data through mobile applications. In determining the driving risk of an individual driver, telematics IoT devices collect the following information[21]: mileage, driving frequency, driving duration, time of day driving (in peak hours, at night, etc.), frequency of sudden braking, velocity, a way to accelerate, use of the device while driving (radio, telephone, etc.), data on the roads used (highway, rural road, etc.), driver’s behavior in danger zones, and driver's moods while driving (anger, calmness, etc.).

The set of parameters based on which the price of the policy was previously determined (vehicle type, the engine power of the vehicle, age and sex of the driver, previous damages, etc.) has now been expanded by a large number of data. Insurers analyze the correlations of the collected data with claims and use

[21] Cannan, M., Lucker, J. & Spector, B. (2016). *Opting in: Using IoT connectivity to drive differentiation – the Internet of things in Insurance*. Westlake: Deloitte University Press.

them to stimulate an improvement in the driving style of the insured with a lower policy cost.

Many worldwide insurance companies have implemented telematics; while in Serbia Triglav Insurance first started offering discounts on Casco insurance to policyholders who agree to use the app “Drive” on a mobile phone to track their driving style.

IoT platform for preventative action

The Danish insurance company Topdanmark, has developed an IoT platform for processing data coming from sensors installed with policyholders. Based on the data processed, the platform generates reports and alerts, thus preventing the occurrence of insured events. The robust IoT platform is cyber-protected and meets GDPR requirements. It is based on edge computing technologies, Amazon Kinesis Analytics and Amazon S3 for cloud computing, developed within Amazon Web Services. It integrates various sensors, which can measure temperature, humidity and the like. The IoT platform was developed in Java and Python programming languages.

The platform is currently being used in the following property insurance cases: to monitor whether the insured's refrigerators have an optimum temperature to prevent damage to inventory. If the temperature rises above the critical value, a SMS message is sent to the policyholder to take action; integration with LeakBot devices to detect household water spills; Integration with the *landmark.dk* portal to measure fertilizer levels in farm-type tanker fertilizers and alert farmers to possible anomalies.

Wearable IoT device in life insurance

The American life insurance company, John Hancock, has incorporated a smartwatch into the life insurance product, Vitality. The product is designed to reward policyholders who have a healthy life, which is determined by smartwatch data. After testing the product, they concluded[22] that Vitality insured persons have 30% fewer hospital costs than the general population, walk almost double the average American, and have significantly more physical activity such as swimming and cycling, live longer and access the application 576 times on average yearly. It means they interact with the insurance company almost 2 times a day, unlike the average insurer who communicates with the insurer up to 2 times a year.

[22] Octo Group S.p.A. (2019). *The Power of Insurance IoT for Risk Management*. http://www.octotelematics.com

Scoring the insured's behavior

A major Swiss IT company with annual revenue of more than € 100 million, which has a subsidiary in Serbia also, MSG Global Solution, has developed a software solution for analyzing the behavior of insured msg.IoTA (MSG Internet of Things Analyzer). Previously, risks were modelled based on historical data, while this software tool, thanks to the processing of a large amount of data obtained from various sensors, allows real-time risk analysis. The msg.IoTA software enables insurance companies to implement their policy model for the behavior of the policyholder and to better understand the policyholder's lifestyle. Thus, insurers can understand the insured's needs and offer him the right product. Swiss insurance company Die Mobiliar first implemented the software solution msg.IoTA in 2018.

IoT investments insurance

Finally, one opposite example[23] of Internet of smart devices and insurance relationship will be mentioned. Hartford Steam Boiler (HSB), part of one of the world's largest reinsurance companies, Munich Re, together with the US company specializing in IoT solutions, Relayr, among the first in the world in 2016, offered the opportunity for technology companies to insure their investments in IoT.

4. ACTUARIES IN IoT ENVIRONMENT

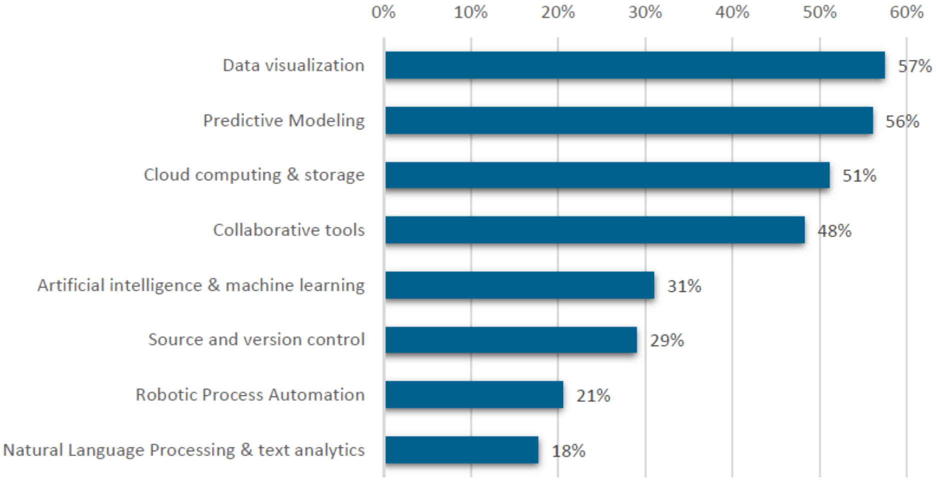
Thanks to the billions of smart devices already installed, which send information every day on what they "see", much more information about the world around us will be available. The big challenge for insurance companies is to leverage that information to the best of their ability, in which actuaries will play a key role.

The data that actuaries analyze will come soon from non-traditional sources, from the Internet of intelligent devices. Not only demographic and financial data will be used, but also climate data, vehicle telematics, wearing sensor medical data, camera data, publicly available IoT data, artificial intelligence data, etc. Sensors send structured but also unstructured data (video, images, text and sound) that are harder to analyze. Actuaries will, therefore, need to learn new skills, predictive analytics, data visualization (e.g. using Tableau software),

[23] Bond, J. (2016). *IoT Infrastructure Investments to be Covered by First-of-a-Kind Industrial Insurance*. http://www.munichre.com

statistical processing and analysis of large amounts of data (e.g. R programming language) and machine learning.

Figure 2. Trends in the use of actuarial technology in 2019



Source: Sondergeld, E. & Purushotham, M. (2019). *Top Actuarial Technologies of 2019*. Schaumburg, IL: Society of Actuaries.

In a survey by the American Society of Actuaries in March 2019, actuaries answered questions about their expectations of advanced technologies to use over the next year. The result is shown in Figure 2.

Thanks to these advanced techniques of analyzing the large amount of new data sent by IoT devices, actuaries will be able to improve tariffs, individual risk-taking and claims management.

Today's actuaries are experts in analyzing the financial effects of uncertain events. Actuaries of the future will be forced to become experts[24] in case studies as well, as the demand for their services will be expanded beyond the insurance and financial sectors. For example, manufacturers of connected smart devices such as telematics cars will need expertise in: monitoring the parameters of autonomous vehicle management to prevent accidents, reducing the amount of damage when an accident occurs, determining the likelihood of failures, planning the dynamics of preventive vehicle maintenance, assessing cost/benefit ratio of risk mitigation and transfer management, etc.

[24] Mango, D. (2015). The Internet-of-Things and Actuarial Engineering. *Actuarial Review Vol. 42*(6).

Insurer projects requiring big data analysis typically involve a multidisciplinary team[25] consisting of actuaries, statisticians, IT experts and data processing experts, i.e. Data Scientist. Actuaries in such teams are, as a rule, experts in the fields of insurance and risk management. With some effort and proper training, actuaries of the future will be imposed as the undisputed leaders of the teams mentioned.

LITERATURA

Antić, D. (2019). *Šta je Internet of Things (Internet inteligentnih uređaja)?* http://samoobrazovanje.rs

Baran, N. (1995). Whatever Happened To... Microsoft At Work? *Byte Magazine Vol 20* (7), p. 30.

Big Data Task Force. (2018). *Big Data and the Role of Actuary*. Washington: American Academy of Actuaries.

Black, N. (2020.) *5 Challenges for IoT in the insurance industry*. www.sas.com

Bond, J. (2016). *IoT Infrastructure Investments to be Covered by First-of-a-Kind Industrial Insurance*. http://www.munichre.com

Cannan, M., Lucker, J. & Spector, B. (2016). *Opting in: Using IoT connectivity to drive differentiation – the Internet of things in Insurance*. Westlake: Deloitte University Press.

Eshton, K. (2009). *That 'Internet of Things' Thing*. http://www.rfidjournal.com

Fleisch, E., Weinberger, M. & Wortmann, F. (2014). *Business Models and the Internet of Things*. Zurich: Bosch IoT Lab White Paper, p. 8.

Global Standards Initiative on Internet of Things (2012). *Recommendation ITU-T Y.2060.*

Mango, D. (2015). The Internet-of-Things and Actuarial Engineering. *Actuarial Review Vol. 42*(6).

Matejić, T., Marković, N. et al. (2017). Monitoring dobara materijalne kulturne baštine primenom interneta inteligentnih uređaja. *Časopis Info M 64*, p. 11-17.

Mladenović, S., Uzelac, A. et al. (2016). IoT u železničkom saobraćaju – realnost i izazovi. In: *Zbornik radova sa XXXIV Simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju PosTel 2016.*

[25] Big Data Task Force. (2018). *Big Data and the Role of Actuary*. Washington: American Academy of Actuaries.

Octo Group S.p.A. (2019). *The Power of Insurance IoT for Risk Management*. http://www.octotelematics.com

OECD (2015). *OECD Digital Economy Outlook 2015*. OECD Publishing.

Pavlović. B. (2019). Robot Application in Insurance. In: *Contemporary Trends in Insurance at the Beginning of the Fourth Industrial Revolution*. Kočović, J., Tomašević, M. et all (eds.). Belgrade: Faculty of Economics Publishing Center, p. 143-160.

Petrović, L., Jezdović, I. et al. (2017). Razvoj edukativne igre zasnovane na Internetu inteligentnih uređaja. *Infoteh Jahorina Vol. 16*, p. 506-509.

Radenković, B., Despotović-Zrakić, M. et al. (2017). *Internet inteligentnih uređaja*. Beograd: Fakultet organizacionih nauka.

Raji, R. (1994). Smart Networks for Control. *IEEE Spectrum 31* (6), p. 49-55.

Rodić Trmčić, B., Labus, A. & Bodanović Z. (2016). Model mobilnog zdravstva zasnovan na tehnologijama wearable computinga. *Časopis Info M 57*, p. 48-54.

Salamone, S. (1995). Novell Builds a NEST. *Byte Magazine Vol. 20* (8) p. 151-152.

Simić, K., Despotović-Zrakić, M. et al. (2015). Model infrastrukture obrazovne institucije zasnovan na Internetu inteligentnih uređaja. *Infoteh Jahorina Vol 14.* p. 681-685.

Sondergeld, E. & Purushotham, M. (2019). *Top Actuarial Technologies of 2019*. Schaumburg, IL: Society of Actuaries.

Tomanović, I. (2017). Primena internet inteligentnih uređaja u unapređenju maloprodaje. *Časopis Info M 64*, p. 18-25.

Vega, M. (2019). *Connect All the Things – Internet of Things Statistics 2020*. http://review42.com

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American 265* (3), p. 94-104.