Petintrideseta
delavnica o telekomunikacijah

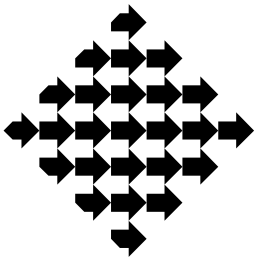
UPORABNA VREDNOST INTERNETA VSEGA

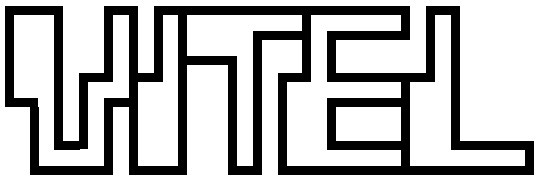
USE VALUE OF INTERNET OF EVERYTHING

20. in 21. maja 2019 Brdo pri Kranju

Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije

SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE
ELEKTROTEHNIŠKA ZVEZA SLOVENIJE





Petintrideseta delavnica o telekomunikacijah

35th Workshop on telecommunications

UPORABNA VREDNOST INTERNETA VSEGA

USE VALUE OF INTERNET OF EVERYTHING

ZBORNIK REFERATOV

PROCEEDINGS

20. in 21. maj 2019 Brdo pri Kranju, Slovenija

Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije
Stegne 7
1521 Ljubljana, Slovenija
www.drustvo-sikom.si

35. delavnica o telekomunikacijah VITEL

ZBORNIK REFERATOV

35 Workshop on Telecommunications VITEL

PROCEEDINGS

Vsi referati v tem zborniku so recenzirani.

All papers in this proceedings have been peer reviewed.

Organizirata / *Organised by*: Slovensko društvo za elektronske komunikacije

Elektrotehniška zveza Slovenije

Pokrovitelj / *Sponsored by:* IEEE Communications Society

Uredila / *Editors*: Tomi Mlinar, Nikolaj Simič

Priprava za tisk / *Prepress:* Tomi Mlinar, Nikolaj Simič

Naslovnica / *Cover design:* Nikolaj Simič, Filip Samo Balan, Aleksander Vreže

Izdajatelj / *Publisher:* Slovensko društvo za elektronske komunikacije

Tisk / *Printing house:* Tiskarna DTP, d. o. o., 2019

Število izvodov / *Copies:* 100

ISSN 1581–6737

Programski in organizacijski odbor delavnice

Programme and Organizing Committee

Programski odbor delavnice

Programme Committee

Ana Robnik, predsednica
Ivica Kranjčevič
Tomi Mlinar
Nikolaj Simič

Organizacijski odbor delavnice

Organizing Committee

Nikolaj Simič, predsednik
Ivica Kranjčevič
Tomi Mlinar

Zgodovina delavnic o telekomunikacijah VITEL

History of Workshops on Telecommunications VITEL

1993: 1. *ISDN omrežja in storitve v Sloveniji*, Brdo pri Kranju
1994: 2. *Mobilne in brezvrvične telekomunikacije*, Brdo pri Kranju
1995: 3. *Podatkovna omrežja in storitve v Sloveniji*, Brdo pri Kranju
1995: 4. *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*, Brdo pri Kranju
1997: 5. *Varnost in zaščita v telekomunikacijskih omrežjih*, Brdo pri Kranju
1997: 6. *Zbliževanje fiksnih in mobilnih omrežij ter storitev*, Brdo pri Kranju
1998: 7. *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*, Brdo pri Kranju
1999: 8. *Omrežja IP, internet, intranet, ekstranet*, Brdo pri Kranju
1999: 9. *Upravljanje omrežij in storitev*, Brdo pri Kranju
2000: 10. *Mobilnost v telekomunikacijah*, Brdo pri Kranju
2001: 11. *Dostop do telekomunikacijskih storitev*, Brdo pri Kranju
2002: 12. *Poslovne telekomunikacije*, Ljubljana
2002: 13. *Kakovost storitev*, Brdo pri Kranju
2003: 14. *Varnost v telekomunikacijskih sistemih*, Brdo pri Kranju
2003: 15. *Mobilni internet*, Brdo pri Kranju
2004: 16. *Pametne stavbe*, Brdo pri Kranju
2005: 17. *Telefonija IP (VoIP)*, Brdo pri Kranju
2005: 18. *Storitev trojček = Triple play*, Ljubljana
2007: 19. *Brezžični širokopasovni dostop*, Brdo pri Kranju
2007: 20. *Optična dostopovna omrežja*, Brdo pri Kranju
2008: 21. *Povsem IP–omrežja*, Brdo pri Kranju
2009: 22. *Širokopasovna mobilna omrežja*, Brdo pri Kranju
2009: 23. *Konvergenčne storitve v mobilnih in fiksnih omrežjih*, Brdo pri Kranju
2010: 24. *Prehod na IPv6*, Brdo pri Kranju
2011: 25. *Internet stvari*, Brdo pri Kranju
2011: 26. *Komunikacije in računalništvo v oblaku*, Brdo pri Kranju
2012: 27. *Telekomunikacije in zasebnost*, Brdo pri Kranju
2012: 28. *Pametna mesta*, Brdo pri Kranju
2013: 29. *Infrastruktura za izpolnitev digitalne agende in kaj po tem – primer Slovenije;* Brdo pri Kranju
2014: 30. *Omrežja prihodnosti,* Brdo pri Kranju
2015: 31. *Kritična infrastruktura in IKT,* Brdo pri Kranju
2016: 32. *Pametna omrežja informacijske družbe*, Brdo pri Kranju
2017: 33. *Omrežja 5G za digitalno preobrazbo*, Brdo pri Kranju
2018: 34. *Zaupanja vreden internet*, Brdo pri Kranju

Zgodovina mednarodnih simpozijev VITEL

History of International Telecommunication Symposium VITEL

1992: *VITEL*, Ljubljana
1994: *Subscriber Access*, Ljubljana
1996: *Broadband Communications Prospects and Applications*, Ljubljana
1998: *Mobility and Convergence Communication Technologies*, Ljubljana
2000: *Technologies and Communication Services for the Online Society*, Ljubljana
2002: *NGN and Beyond*, Portorož
2004: *Next Generation User*, Maribor
2006: *Content and Networking*, Ljubljana
2008: *DVB–T and MPEG4*, Bled
2010: *Digital Television Switchover Process*, Brdo pri Kranju

Uvodnik

Foreword

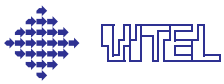
Temeljno gonilo digitalne preobrazbe gospodarskih sektorjev, javnega sektorja in družbe kot celote je inovativna uporaba naprednih tehnologij ter pridobivanje informacij in znanj iz podatkov, ki nam jih ponujajo te tehnologije. Tehnologija Internet vsega (IoX – Internet of Everything - the intelligent connection of people, process, data and things) nadgrajuje koncept povezanih stvari z inteligentno povezljivostjo ljudi, procesov in podatkov, njegova razširitev uporabe pa omogoča naprednejše spremembe operativnih in poslovnih procesov, ki so tesno spojene s spremenjenimi in naprednimi poslovnimi modeli in inovativnimi aplikacijami. Take napredne integracije ponujajo številne nove priložnosti vsem deležnikom v podaljšanih in prenovljenih verigah vrednosti. Internet vsega, torej tudi stvari, dobi pravo moč in uporabno vrednost šele v povezavi z ostalimi naprednimi tehnologijami dostopa in povezljivosti, predvsem z omrežji 5G, z uporabo analitičnih metod in napovedi, umetne inteligence in strojnega učenja preko pridobljenih zlitih podatkov, z zagotavljanjem varne komunikacije in avtentikacijskih mehanizmov med napravami, s kiber-fizikalnimi sistemi ter tehnologijami v oblaku in kognitivnimi računalniki.

V zbranih člankih tega zbornika so predstavljene rešitve in primeri uporabe s področja oskrbovalnih verig, železniškega prometa in logistike, zdravstva, energetike, javne varnosti, pametnih mest in skupnosti, pametnih domov. Uporabljene IoT platforme imajo zelo raznoliko tehnološko in funkcionalno naravnanost ter stopnjo zanesljivosti, kar je v veliki meri odvisno od njihove rabe, bodisi v segmentu potrošnikov in družbenih dejavnosti bodisi na strogo industrijskih področjih. Ekosistem deležnikov ter nove storitve in aplikacije, ki se gradijo na teh platformah, se razlikujejo glede na rabo, nemalokrat pa se obe rabi tudi povežeta in prepleteta v kompleksno verigo vrednosti - tak primer je oskrbovalna veriga. Ne glede na namembnost in rabo pa v prispevkih ugotavljamo, da morajo rešitve vključevati celovito podporo identifikaciji objektov različnega tipa po vsej verigi, učinkoviti in varni povezljivosti naprav in stvari v velike mreže, varni in zaupanja vredni izmenjavi občutljivih podatkov ter njihovi večstopenjski obdelavi in večnamenski uporabi v novih storitvah in produktih. Ob predstavljeni uporabni vrednosti in prednostim uvajanja interneta vsega, v prispevkih podamo kritično oceno in pomisleke zaradi včasih prevelikih in neosnovanih pričakovanj, tako industrije kot tudi potrošnikov.

Vse zapisano v tem zborniku nas potrjuje v prepričanju, da prinaša povezovanje tehnologij interneta vsega in umetne inteligence z ostalimi tehnologijami v inovacijske platforme in partnerske ekosisteme širšo uporabno vrednost industriji, državi in družbi. Najpomembnejše je dejstvo, da je ta tehnološki, poslovni in družbeni val tu in zdaj, da je torej neizbežen. Ob razumni in etični rabi je to nova gospodarska, razvojna in družbena priložnost, ki je izjemnega pomena za Slovenijo kot del enotnega evropskega digitalnega trga in njeno vpetost v svetovni digitalni prostor.

mag. Ana Robnik,
vodja programskega odbora

Brdo pri Kranju, 20. maja 2019



Kazalo prispevkov

Table of contents

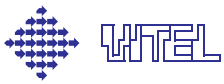
20. 5. 2019

21. 5. 2019

PRISPEVKI

ARTICLES

20. 5. 2019



The next IoT: Internet of Transformation

Nenad Gligoric, Srdjan Krco, DunavNET, Serbia

Milos Loncar, Microsoft, Serbia

Abstract — The proliferation of new technologies is impacting all domains of the traditional business. One of the key digital transformation technologies is IoT, provisioner of the next wave with tendency to disrupt the way we work, buy, travel, live, eat... Accordingly, new types of sensors are becoming reality, printable and able to collect, sense, and read environmental parameters of relevance to the product and its use. New global specifications enabling creation of unique identifiers to each individual product item (package on item-level) in a standardized manner, the embedding of such IDs into product packaging together with sensors and their integration with powerful data analytics tools, represent the basis for creation of the new generation of supply chains, transparent and trusted, providing additional value to all stakeholders, from manufacturers to consumers and society in general. In this paper, we describe the opportunity of the digital transformation leveraging IoT in different domains, with the focus on the supply chain, including the experience from several pilots done across Europe and the potential ways forward.

Keywords — IoT, digital, transformation, GS1, retail, FCMG, supply, chain

I. INTRODUCTION

Disruption of traditional business is everywhere around us and its penetrating horizontal market as never before, making the digitally transformed companies ahead of its traditional twins. The report [1] that surveyed 200 individuals at North American industrial companies, who make decisions about IoT purchases, showed that digital transformation leaders are more than willing to accept the Internet of Things (IoT) for their corporate business processes. If we go back in time, say in 2005, who would say that in 10 years the world's largest taxi company (Uber) will own no vehicles and that the largest accommodation provider (Airbnb) will own no real estate? The next digital transformation wave should come with IoT, which is still not meeting its expectations in compare to predictions. What is still missing is data sharing across value chains that could open a wide set of opportunities. One of the sectors that offers a lot of innovation potential based on IoT is the consumer sector, the consumption products that we use every day (milk, eggs, meat, water, etc). Essential for each object to be able to communicate or be communicated with, is to have unique identifier, an address such as IP, URL, or its unique ID that will enable distinction of one type of object from its million duplicates. The basic level of identification of an item is to be able to look up its specific properties, usually in terms of description and branding information. There are already some widely-adopted identification standards such as those under the GS1 organization [2] that provide a mechanism to create globally recognized identifiers for products. However, currently these identifiers are mostly used to recognize products at the Stock Keeping Unit (SKU) level, which leaves two key aspects to transform a product into a digital asset unsolved: on the one hand, how to identify the specific item itself, not only the product, and on the other hand, objects connected to Internet will have a unique lifecycle and can be shared among different stakeholders and different systems. Further to this, item-level identification can serve as a disruptive innovation, but it needs to be tackled carefully.

In this paper we will explain digital transformation cross value chain by involving the ecosystem using co-creation methodology as a wheel and new ratified standard for unique identification of devices as a driver.

In section II, the importance of a strong ecosystem for successful and sustainable market presence in the IoT world is explained. It analyses emerging value and business models together with the ecosystem structure and the roles of different stakeholders as well as importance of the "open source". Section III presents method of identification of objects on item-level and explains its use leveraging supply chain domain related use cases developed using the proposed approach, supporting the ecosystem as well as ways of creating and expanding such ecosystem based on the experience of H2020 TagItSmart [3] project ran over three years with more than 30 partners. Section IV concludes the paper.

II. DIGITIZATION OF VALUE CHAINS AND ECOSYSTEM

In the (very) near future, Internet of Things (IoT) will be everywhere. IoT technology is re-enforcing the businesses to transform into a software company, regardless of the industry vertical that an organization originates from. Digitization will impact and drive changes in society and life; it will become its integral part, even in more conservative industries that still believe that the wave of changes will not affect them. What these incumbent industries are forgetting is that no matter how their industry might be protected from technology disruptions, their customers are not. Buyers and users will drive the change because they will expect the same experience they are having in other areas of life that run on IoT [4].

The IoT has the potential to significantly change business as we know it, while its added value goes beyond operational cost savings from smart devices that report position of vehicles, temperature in a room, or failures before they occur. This singular value of IoT, based on insights gained through the collected and analysed disparate data, is not the full picture of innovation. IoT can completely reshape the business landscape with its natural drive to create digital business ecosystems, where: value is co-created, everyone is a partner and a competitor at the same time and every

organization offers software solutions based on open source technology approach.

A well-developed ecosystem with a diverse set of partners bringing in a set of complementary skills, services and geographical coverage is essential for successful delivery of IoT solutions but this requires expertise in a diverse set of domains, not only to understand the business requirements, but also to be able to process captured data and generate reports in the most meaningful manner for the business needs. This is not easy for a single company, not even a large one. Further to this, development, provision and maintenance of IoT solutions is complex and requires knowledge of several technical areas. First, edge devices (sensors, actuators, gateways) must be selected based on the use case requirements and environment conditions (availability of network connectivity, planned maintenance etc.). The number of communication networks which can be used is growing every day (WiFi, GPRS, 3G, Bluetooth, LoRa, NB-IoT, LTE-CAT1, Weightless, etc.) thus requiring a very good knowledge of the intrinsic details of each communication interface/protocol and how that impacts performance of the planned IoT solution. Security is one of the major concerns across all industries, requiring a detailed knowledge of the potential threats and how to minimize associated risks. Similarly, growing concerns over data privacy and upcoming introduction of GDPR [5] require extensive experience of this domain, including options for integrating adequate tools in commercial IoT solutions. Finally, the deployment of IoT solutions requires physical presence at the client site, thus presenting demand for geographical coverage. While it might look as an everyday business for IT system integrator, in many cases it is not. Often, installation of sensors requires substantial domain knowledge and has to be done carefully to ensure that captured information/measurements are of adequate quality for the solution.

Let's look at it in an example of a smart home. If an organization wants to sell smart homes, it needs to partner up with several different companies because machines and objects in the house come from various manufacturers. All of them need to talk to each other: the lights need to talk to the fridge, which needs to talk to the furniture, and so on, and they all "report" to the central control system. Also, when certain parts of that system require upgrades or add-ins, a new manufacturer with the right skills, that is already in the business of producing such products, may join this ecosystem. With the velocity of changes in today's world, nobody has the time to develop an innovative product or service from the ground up and spend six months or a full year for development. The solution is to partner up with someone who already does it successfully and leverage each other's competencies into a novelty in the market. That is the biggest power of a digital ecosystem: creating added value through partnerships.

The benefits of a well-developed IoT ecosystem are numerous. First and foremost, it allows easy access to domain specialists' know-how and expertise at reasonable costs, an essential factor in the success of IoT projects. Then, it accelerates the time to market thanks to the reuse of multiple components and more distributed workload. The result of it is improved return on investment (ROI) for each stakeholder and enhanced customer experience as visible results are achievable in a very short timeframe. Last, but not the least, IoT solution built inside a well-developed ecosystem provide assurance to customers that their investment will have continued support and innovation across the entire value chain. This is particularly important having in mind that many, if not all IoT solutions, are being deployed with long-term exploitation plans.

A. Ecosystem roles

Many manufacturers have already taken the first steps towards the digital transformation of their facilities by creating "smart factories", where the quick wins are seen mostly through the increase of productivity. By developing complex ecosystems of self-regulating machines and sites, the output is customized, resources optimally allocated, and they managed to create a seamless interface between the physical and virtual segments of construction, assembly, and production. In this ecosystem we usually have manufacturers as factory owners, producers of different machines as their suppliers, logistic companies connected to their production process, their customers that want to get insights in production process real time, raw materials suppliers, IoT platform providers, solution providers (Independent Software Vendors) & system integrators.

Main challenge is to connect machines produced more than 20 years ago that never meant to be connected, as well as to stay opened for new players that will become part of their value chain and ecosystem. Because of all mentioned it is mandatory to have structured data governance and openness to all members in ecosystem. All big cloud providers (Microsoft, AWS, Google) as well as solution providers for manufacturing industry (Siemens, ABB, General Electric) realised that IoT is ecosystem play and they alone are not capable to satisfy needs of new digital world. One good example of how companies are changing their strategy we see with Microsoft that now provides many pre-configured solutions as open source solutions as well as community efforts like open source OPC foundation [6] aiming to overcome the challenge of multiple protocols used in manufacturing.

According to Krco et all [4], the overall ecosystem stakeholders can be categorized into one of the three roles:

- Horizontal: providing scalable, interoperable and cost-effective technologies, reusable and future-proof functionality, not specific to any particular business domain or user scenario. Examples are cloud infrastructure, security solutions, device management, networking etc.
- Vertical: addressing market-specific challenges and use cases, providing functionalities specific to a specific business domain and enabling full integration of IoT products into existing systems and lines of business. These stakeholders have to understand business operational and technical environments and their unique requirements, to have relationships with the business lines, operational technology or building technology teams.
- Geographic: responsible for local solution deployment, compliance with user's work processes and national legislation, first line customer support.

The important aspect of working in an ecosystem and delivering a solution in collaboration with multiple partners is teamwork. In other words, it is important to have well defined roles and the business value flow among the partners,

not only to set the expectation, but also to enable efficient execution in a competitive environment.

One example that directly indicated importance of ecosystem was example from the Rolls Royce, which in past 20 years delivered more than 3,000 engines for commercial aircrafts. At certain moment, data coming from many different types of aircraft equipment was increasing too rapidly, which hindered company's ability to analyse and gain quality insights. They deployed a new IoT solution and Microsoft Azure platform to transform their customer experience, but something else happened as well. By examining these growing data analysis challenges, Rolls-Royce came up with a new plan to address the changing market with a more compelling set of services by providing meaningful insights across more of the airlines' operations. One of them is fuel efficiency. By analysing new data against existing forecasts, reference tables, and historical trends, Rolls-Royce is now able to help airlines understand exactly which factors—including flight plans, equipment maintenance, weather, and discretionary fuel—have the most impact on fuel performance. This example directly shows how the IoT can be used to transform business to a new level offering innovative services leveraged on value generated from different actors' data of the same ecosystem.

B. Open platforms

Platforms have upgraded and changed over time. Kelly explains it well in "The Inevitable", stating how one of the first platforms was Microsoft's OS operating system, where anyone with the ambition could build and sell a program that ran on an OS that Microsoft owned. Apple's iTunes was a second generation of platforms, which also became a marketplace for mobile apps. Apple owns the platform, sets rules and protocols, tracks financial transactions and so on. The marketplace itself (iTunes) is, therefore, one of Apple's products. The tech giant kept improving the iPhone device, while different contributors of its platform kept innovating the software that runs on those devices. Third generation of the platforms is also a combination of a market and a company, but with more complex market attributes. Unlike the traditional two-sided market, this platform ecosystem became a multi-sided market. Initially, Facebook created a set of rules and protocols that formed a marketplace where independent sellers produced their profiles, which were matched up in a marketplace with their friends. But then it went further: the attention of the students was sold to advertisers, game companies sold to students, third-party apps sold to other third-party apps, and so on. This ecosystem with multiple matches is based on inter-dependent products, and it will expand as long as Facebook is managing the rules and grows as a company. In the more B2B segment examples of successful platforms are popular cloud platforms from leading providers such as Microsoft Azure, Amazon Web Services and Google Cloud. While platforms collect partners that are focused around one service or product (such as Apple's iOS), ecosystems are much broader than that.

Just like the entire suite of technologies around, IoT is a true ecosystem where many different, interconnected and codependent parts (devices, IoT software, data platform, analytic tool, virtual desktop etc.) are orchestrated to generate useful information – in a similar way, IoT replicates that same environment for businesses that use it.

Over time, they co-evolve their capabilities and roles, and tend to align themselves with the directions set by one or more central companies. Those companies holding leadership roles may change over time, but the function of ecosystem leader is valued by the community because it enables members to move toward shared visions to align their investments, and to find mutually supportive roles.

Ecosystem in Industrial IoT is made of different actors, even competitors but they all share standardized digital platforms to achieve mutual benefit. For a digital ecosystem to succeed, it needs a platform with an open technology approach. This is the key because platforms and ecosystems cannot thrive on closed systems and protected data – instead of data ownership, they nurture data access.

III. DIGITAL TRANSFORMATION USING ITEM-LEVEL IDENTIFIERS

In the vision of Web of Things [7], physical objects have an active, individual presence on the Web to be able to integrate themselves with existing Web applications. One critical question is how to identify the physical objects. There is solution Active Digital Identities (ADIs) [8], which implements the vision of the Web of Things and makes it straightforward for any physical object to instantiate an identity for itself, providing a persistent and unique presence on the Web available to any application authorized to access it. Identity, and uniqueness of identity, is vital for each physical object to be discoverable on the Web. For unconnected objects to actually bind the digital identity of an object with the physical item, the URL of the object's ADI can be encrypted in a physical tag to uniquely identify that object – for example, a unique QR code or NFC tag acting as a pointer to the ADI on the Web. All disruptive businesses have one thing in common: they adopt new business models and technologies much faster than the others. Another crucial fact is that they share information across the value chain partners and co-create that value in partnerships. This trend is freeing up trapped business value, enhancing innovation, and driving the evolution of product offerings into service offerings. In the next two sections unique identification of objects using existing standards is explained together with co-creation methodology.

A. GS1 uniform resource identifiers

Current GS1 standards do not allow consumer interactions as barcodes and 2D barcodes (QR codes) used today on packages are embedding static information. The main goal would be to connect products to the Web at massive scale using GS1 identifiers, but at the same time to reduce the need for multiple codes on packs, while ensuring a glide path with industry toward a future where a single 2D barcode could serve the needs of all parties.

QR code supports URL which is a good start for enabling interaction with the consumer in both directions, having in mind that consumer phones now have native scanning capabilities. The missing part was a standardized way of communication (i.e. URL domain, value and parameters) over barcode that will enable all stakeholders to communicate, e.g. producer to create initial datasheet and product information, transport providers to provide transport related data, retailers to dynamically manage the product; consumers to interact with retailer, buy product, recycle it,

etc. Since the standard [9] was recently released (with significant contribution from TagItSmart partners), the adoption should take time to allow employment of the digital link in the larger extent.

In Figure 1, proposed standardized URI implementation for the GS1 is provided showing different parts of URL composed of: protocol, brand domain/ service provider, GTIN[1] [10], item level serial number and the optional parameter that can be passed over to application.

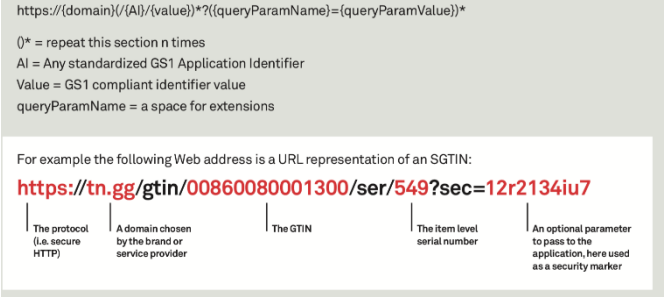


Figure 1: GS1 Uniform Resource Identifier

Main benefit of this standard is the ability to build the information knowledge base about the product cross value chain, where different actors can contribute and use data about the product using a single reference.

B. Co-creation methodology

The need for non-technical research in the area of machine to machine communication and Internet of Things, as the developments got closer to market, was acknowledged in the 1996 EU Call for Proposals of the i³: Intelligent Information Interfaces, an Esprit Long-Term Research initiative. Its aim of i³ ("eye-cubed") was to develop new human centred interfaces for interacting with information, aimed at the future broad population. This approach was later adopted and the participation of the user during development process was not ended at the idea's compilation or brainstorming.

IoT technologies offer limitless opportunities that are to be applied in society innovation beyond industry and business, although this task is not always self-evident. Each innovation is risky in terms of its success and there are attempts trying to indirectly tackle uncertainties that may arise around innovation itself. One strategy is Responsible research and innovation (RRI), which as a main driver fosters involvement of stakeholders, end-users and society from the beginning to the end in the innovation process [11]. According to Stahl et al [12], core features of the RRI in ICT are product, process, purpose and people; where the focus is on the purpose of the development needs as well as on the people involved in the innovation, i.e. co-creation of the product.

The process of developing new IoT services for end user requires parallel collaboration during the complete proceeding in order to finally achieve the expected results and acceptance of the final service. The user should participate in the discussion when searching for requirements that the final service should provide, and after the correspondent work of developers building the service, the user should appear again to be taught about how to use the technology and to test and evaluate the final results.

From this, important aspects can be extracted, which can be considered as the base of the creation of IoT services: co-creation of the use cases with final consumers, the search for requirements, the technical development, the user training in the new technology and the final evaluation. All of them will be of great importance in order to finally achieve the objectives with the developed services.

Figure 2: Co-creation of digital service

To allow unique identification we have used SmartTags with embedded QR code and partially printed with functional ink (printed sensors), enabling collection, sensing, and reading of parameters from environment as well as tracking a products' lifecycle. Before using QR codes as a method for encoding information for the SmartTag, we have evaluated different concepts with the end-users. This was done as a part of TagItSmart project using an online Open Web Laboratory, Owela (http://owela.fi), supporting active user involvement in the innovation process from the early ideas to piloting and actual use and to gather knowledge and feedback from the users about SmartTags. The concepts were presented to the consumers as stories to make it easier for them to understand the idea of novel solutions and easily implement the possibilities the solution offers for their daily life.

The concept themes were about:

1. Digital product (virtual entity product given after barcode scan) and recycling,
2. Fast moving consumer goods and dynamic pricing, and
3. Authenticity of the products.

After reading the stories, participants discussed about their interest towards the different concepts. Totally, 45 consumers participated the discussion and gave 341 comments to the discussion during two weeks in January 2017. In total, conclusion in general was, that SmartTags based on QR codes are user friendly and users are familiar with this technology so utilization of SmartTags instead of static QR codes will not change user behaviour.

The involvement of different actors in the value chain is done during co-creation workshops where methodology was based on creating the framing conditions for dialogue, organizing interaction and collecting conclusion and procedural lessons [13]. The goal behind is to put stakeholder's focus on understanding the other stakeholders that will make transformation and joint action possible. This requires engagement with interested participants committed

[1] GTIN describes a family of GS1 (EAN.UCC) global data structures that employ 14 digits and can be encoded into various types of data carriers.

to the dialogue with alignment between theme, information, and participants of the workshop. The workshop interaction should find a balanced way to include self-interests. The interest and perspectives of participants should be included, while also making room for learning new perspectives.

Disagreement is essential for learning, and there should also be room to give participants ownership of the process to feel that their work shapes the process. Good questions can help to open up discussion and reflection and to check whether relevant perspectives are taken into account in the argumentation. Collecting the conclusions and procedural lessons should include agreements and disagreements documented and evaluation from perspective of different actors.

C. *Use Cases*

In this section, use cases based on unique level identifiers and proposed methodology are presented. Unique item-level identifiers are being used with tags labelled on packages and devices (SmartTags) to evaluate the efficiency in real word use cases.

i. Brand protection

In this use case each bottle is digitized by assigning of a unique smart tag. The authenticity is based on the capabilities of functional inks. For this pilot solution, the emphasis was on photochromic (light sensitive) inks (Figure 3). QR codes printed with photochromic inks have two states, normal and active. Active state of the QR code is achieved by illuminating the QR code in normal state with LED light (i.e. mobile phone flash light). That is how additional information can be carried within the same QR code based tag. After the source of the illumination is gone, QR code will revert to normal state in short time (reversible ink).

Figure 3: Stakeholders of the brand protection

Photochromic ink with non-reversible active state was considered for marking the bottle of wine as consumed to prevent refilling the authentic bottle. However, this functionality is replaced by collecting the information on the product status (“in store”, “on the table”, ”consumed”) from the user via mobile application.

Figure 4: Wine bottles tagged

In Figure 5 the stakeholders are presented on the diagram that depicts main components of the pilot and provides high-level connection between them. The ability to uniquely identify each bottle “glues” all of the stakeholders together, including consumers. The stakeholder applications include:

– Mobile application for customer, distributor and retailers that provides main experience for the end users, wine consumers, transport providers and it is used to perform wine bottle authentication. This application is also used to obtain feedback from the users on the status of the bottle (unsold, sold, opened, transported) and to obtain customer satisfaction (product rating).
– Web application at the wine maker’s site utilized to support tagging of bottled products. A nice to have feature would be to interface this component with the existing wine maker’s information system in order to extract information on the current product batch as well as to support automated integration with transport bill creation for boxes/pallets.

Mobile application for distributors provides optional functionality to scan/control the content of the shipment received a distributor’s site (optional). Mobile application for retailer provides an optional function to provide sales confirmation at the TagItWine platform. Each sold bottle would be marked as sold. Optionally, this feature can be achieved with an integration/interface between retailer’s information system and TagItWine platform (optional).

Figure 5: Stakeholders of the brand protection

The web application was used to request and create QR codes for production batch, to create digitized version of bottled products and link them with smart tags and labelled bottles.

ii. Recycling

The objective of the recycling use case is to propose a Circular Economy of slow-moving circular goods (SMCG), leveraging existing eReuse.org community to allow their platforms’ users to test and evaluate the feasibility (technical and commercial) and to use SmartTags to control devices and components to exchange certified data about the status, value and traceability of digital devices.

Potentially, customers segments are all stakeholders that participate in the circular economy of electronics. The stakeholders are grouped into three groups: 1) suppliers of used devices interested in monitoring the devices’ lifecycle, 2) refurbishers are businesses that refurbish devices using a set of tools that allow them to reliably erase their data, performing tests and benchmarks, algorithmic estimation of price for a B2B marketplace, and reinstalling the OS, and 3) retailers that purchase refurbished devices from refurbishers

and distribute them to second-hand consumers via ecommerce and physical storefronts, offer warranty, post-sales support, maintenance and ensure takeback or final recycling.

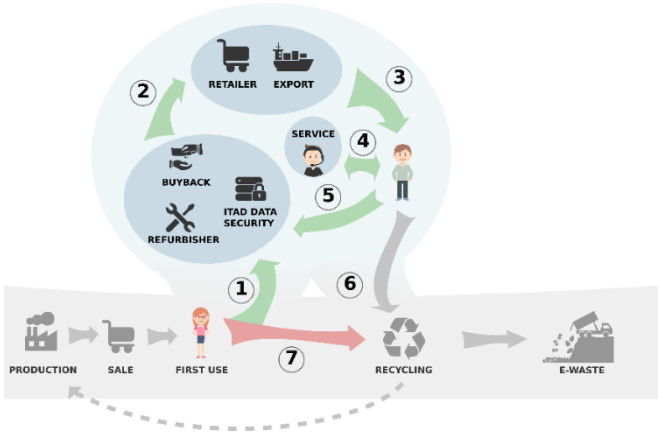


Figure 6: Stakeholders of the circular economy

The above drawing shows interactions between circular economy stakeholders. Some of them are customer segments and others are 3rd channels. For a better understanding the users who participate in this recycle pilot are marked in bold. "First use" users, as depicted in the drawing (also referred to as suppliers in the beginning of this section), are public administrations, companies or individuals willing to donate their used devices, and IT asset management businesses (ITAM) that manage their customers' device fleets.

At suppliers' facilities, usually there is a selection process through which devices with sufficient use value are assigned to refurbishers and those with insufficient use value to recyclers. If data of devices has not been erased, data erasure must be carried out by ITAMs at suppliers' facilities, or by refurbishers at their own facilities. Devices are received and refurbished (1) by refurbishers and acquired (2) by retailers, who can be for-profit or non-profit in the case of Digital Divide Initiatives. Retailers distribute (3) devices to users locally or export them to other countries. Some users may need maintenance which is done by service (4) businesses. When a user wants to get rid of his device, his retailer makes sure that it enters (5) a reuse circuit again if the device still has sufficiently high use value. Otherwise it is sent (**6**) to an authorized **recycler**.

In order to get rid of their devices, suppliers access one of two types of reuse programs: i) Non-profit reuse programs, which are usually run by digital divide initiatives and zero waste Initiatives, which operate individually or are grouped in collaborative/commons platforms, or ii) Commercial reuse programs that normally pay a fee for devices they receive. At this point supplier and reuse circuit (Digital Initiative or directly a refurbisher) sign an agreement to transfer the devices, in exchange for economic reward or for social impact. In this exchange, reuse programs take the role of buyback, as they acquire used devices from their user. The offer of a non-profit program is social impact that the donation will have, and the offer of the commercial reuse program, is to pay for the devices. In the first case traceability is more important because suppliers (e.g. a public administration) want to be able to trace devices to validate the claim on social impact. In the second case traceability is not so important; the supplier's motivation here is to have an economic reward.

In eReuse pilot project users of the eReuse community tested the integration with the TIS platform and the use of smart tags to control devices and components. 8 customer segments were chosen with different business needs: **1) Buyback**: use a scoring and pricing systems to automate the price calculation for the purchase or exchange/trad-in of used computers, **2) Retailer**: A B2B service to purchase refurbished computers and to assess the state of functioning and features of computers in order to offer warranty or its extension, **3) Service**: a desktop application that allows to check the incidences of an individual computer registered in the system, including hardware details about each component and provide after sale channel support, **4) Exporters**: secure tags that report and certify the state of, either good operation or its classification as ewaste, of the computers being exported, **5) Refurbishers**: can share their certified stocks with retailers, **6) ITAD/ITAM**: ITADs are IT asset disposal companies and with ITAMs they are interested in data security and compliance solutions and stock sharing, **7) Recyclers**: being able to offer their collection services and reporting systems to the competent authorities and, finally **8) Digital divide initiatives**: public or NGOs, similar to retailers, but must guarantee a fair price to receivers, with a minimal charge for circularity services to support economically disadvantaged recipients while ensuring traceability until final recycling.

The following Figure 7 presents the main interactions between actors in the ecosystem. The refurbishers, who receive the devices that must be repaired or upgraded for their second hand sale, use the system to certify their correct operating status, and this information is shared by the next actors in the reverse supply chain. Finally, the recycler, through the application, notifies the recycling point. The use of SmartTags and automatic tools for hardware scanning and diagnostic allows to make the system safe and transparent to Zero Waste, Digital Divide and governmental authorities.

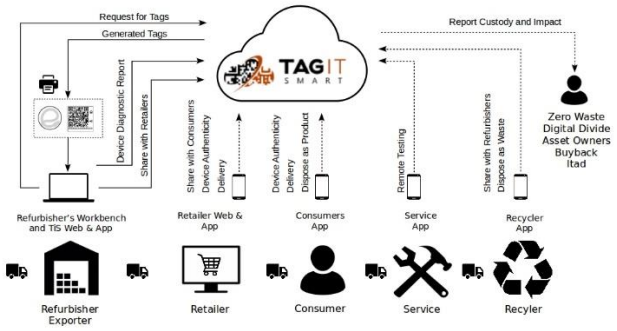


Figure 7: Stakeholders of the circular economy and communication flow

iii. eHealth

In this use case, SmartTags are used in health pilot executed in the City Clinic, a private hospital in Athens. Aiming at promoting high-end health services towards the general population of adults and seniors, it combines medical expertise with the state of the art medical technology. The institution focuses on personalized care, taking into consideration individual needs and desires of patients. City Clinic provided an ideal environment for the pilot, offering

four floors of mostly spacious two-bed rooms to a total of sixty beds, clinics, and diagnostic laboratories and a fully equipped surgical floor. More specifically, the pilot took place in the Orthopaedics department involving 2 doctors and 2 nurses for duration of 10 months. Although the pilot was validated in a real environment, no real patients or prescriptions were involved. Instead, "virtual patients" were used in potentially free beds of the Clinic. These "virtual patients" were assigned "virtual prescriptions" and health records through the platform. In this way, the pilot conditions simulated as close as possible the real case with real patients, prescriptions and health records.

Figure 8: SmartTag used in cold chain in health monitoring

The purpose of the pilot was to monitor storing condition of medication and using SmartTag to digitalize different processes such as drugs' stocktaking, in-hospital medication, smart medical exams, pre-surgery check and patients' monitoring by using data from different channels.

This use case managed to achieve their set goals of changing the way how the work at hospitals is done. The developed components introduced a new assisted way of working that adds a layer of verification that leads to an automation of above mentioned processes. The goals were clearly defined and achieved. The testing methodology and questionnaires are thorough throughout the project.

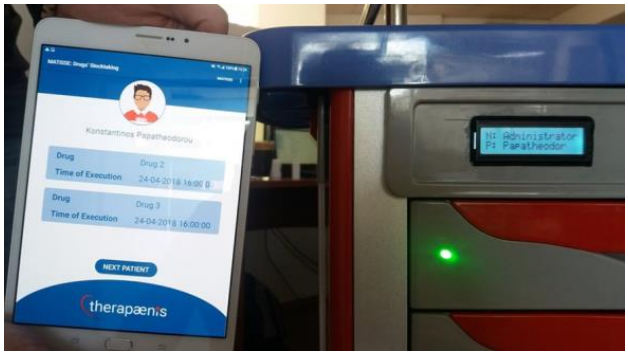


Figure 9: Mobile application and Smart cart interaction

IV. CONCLUSION

In this paper we have presented current trends and methodology for digital transformation using IoT. In each business there is data hidden from different actors in the ecosystem that could generate value and potentially create a new digital footprint and eventually digital twins. These twins exist as sets of properties in an analytic layer that is in many commercial hands at the moment but not really under multi stakeholder control. The first step is to grasp the practice and theory of assigning, withdrawing, validating and defining the very nature of entitlements. This demands a new toolset on the notion of identity itself. Uncoupling identity in thinking of "entitlements' opens up a new field of value and services. In the case of self-driving cars this way of thinking could argue for liability not with real person-identities but with 'entitlements'; any combination of a particular driver (with particular points on a passport and certain characteristics) and a particular car. This reasoning can be extended to basically any service in the network. A new category of tools and services for empowering independent customers is starting to emerge that triggers economic signalling between demand and supply in far more direct and efficient way. It will also support genuine two-way relationships and minimize the need for surveillance and "big data" based guesswork by companies.

ACKNOWLEDGMENTS

This research was funded by European Commission under framework of Horizon 2020 TagItSmart project (Grant Agreement No. 688061).

REFERENCES

[1] IFS World, IFS unveils IOT solution TO help customers drive digital transformation, Accessed 15.03.2019, available online: https://www.ifsworld.com/us/news-and-events/newsroom/2016/10/25/ifs-unveils-iot-solution-to-help-customers-drive-digital-transformation/
[2] Gs1.eu. GS1 in Europe. 2018. Available online: http://www.gs1.eu/ (accessed on 14 December 2018).
[3] H2020 TagItSmart EU research project, www.tagitsmart.eu
[4] Srdjan Krco, Rob van Kranenburg, Miloš Lončar, Xenia Ziouvelou, University of Southampton, Frank Mcgroarty Digitization of Value Chains and Ecosystems: Driving Transformation and Innovation book: Digital Business Models ISBN 978-3-319-96902-2 (eBook)
[5] General Data Protection Regulation: https://www.eugdpr.org/)
[6] OPC Foundation, https://opcfoundation.org/
[7] Dominique Guinard, A Web of Things Application Architecture, December 1, 2011.
[8] Andy Perrin, Active digital identities, Accessed 15.03.2019. Available online: https://evrythng.com/videos/active-digital-identities/
[9] Digital Link GS1 Standard. Available online: https://www.gs1.org/standards/gs1-digital-link (accessed on 14 December 2018).
[10] GTIN, Available online: https://www.gtin.info/
[11] Von Schomberg, Rene (2013). "A vision of responsible innovation". In: R. Owen, M. Heintz and J Bessant (eds.) Responsible Innovation. London: John Wiley, forthcoming
[12] Bernd Stahl, Marina Jirotka, Grace Eden, Responsible Research and Innovationin Information and CommunicationTechnology: Identifying andEngaging with the EthicalImplications of ICTs, DOI: 10.1002/9781118551424.ch11
[13] Morten V. Nielsen Nina Bryndum Bjørn Bedsted, Organising stakeholder workshops in research and innovation – between theory and practice, Journal of Public Deliberation, Volume 13, Issue 2

ABOUT THE AUTHORS

Dr. **Nenad Gligoric** is project manager and research group lead at DunavNET, DNET Labs R&D department. He holds PhD from the Faculty of Organizational Sciences, University of Belgrade. Since 2016, Nenad is engaged as associate professor at Faculty of Information Technology, Alfa University Belgrade.

Dr. **Srdjan Krco** is a co-founder and CEO of DunavNET, a company designing turnkey IoT solutions. He has over 20 years of experience, working with large multinational companies and international collaborative research and innovation projects. Srdjan is one of the founding members of the International IoT Forum and is actively participating in IERC, IoT-EPI and AIOTI activities.

Milos Loncar is Business Development & IoT professional in Microsoft with regional experience and deep understanding of business models and IoT partner ecosystem. Global Black Belt IoT team member. Graduated in Belgrade, Serbia on Electrical Engineering university with MBA on Sheffield, UK.

Pogled podjetij na internet vsega – miti in resnice

Andrej Planina, Špica International, Ljubljana

Povzetek — Internet stvari nezadržno prodira v vse pore delovanja podjetij in v naša osebna življenja. Pri tem se podjetja in posamezniki stalno soočajo s prednostmi in pomisleki, ob tem pa je veliko neosnovanih in pretiranih pričakovanj. Dotaknili se bomo nekaj najbolj pogostih pomislekov, ki ovirajo hitrejšo uvedbo interneta stvari v poslovanje podjetij, in načinov za njihovo premagovanje. Senzorji na vseh stvareh, senzorji iz okolice, vse povezano, vpogled nadzornih IT sistemov v dejansko fizično stanje procesov, med sabo povezane naprave, deljenje podatkov. Ali je vse to res možno doseči, kaj podjetja navajajo kot ovire in kako jih premagujejo? Dani dokument ponuja vpogled v dejansko stanje v podjetjih in v dejanske projekte na področju interneta vsega, predvsem na področju industrije in oskrbovalnih verig.

Ključne besede – Internet stvari, senzorji, algoritmi, umetna inteligenca

Abstract - The Internet of things permeates virtually all aspects of our lives and is inextricably linked with business operations. In doing so, companies and individuals are constantly faced with the advantages and concerns, while there are many unfounded and exaggerated expectations. We will touch some of the most common concerns that hinder the speedy introduction of the Internet of Things into the business of companies and ways to overcome them. Sensors on all things, sensors from the surroundings, everything connected, and insight of control IT systems into the actual physical state of processes, interconnected devices, and data sharing. Is it all really possible to achieve what companies cite as obstacles and how to overcome them? The given document provides an insight into the actual situation in companies and in real projects in the Internet of everything, especially in the field of industry and supply chains.

Keywords – Internet of things, sensors, algorithms, artificial intelligence

I. UVOD

Koncepti digitalizacije in četrte industrijske revolucije v zadnjih letih zavzemajo naslovnice tako strokovnih kot tudi poljudnih medijev. Vsi govorijo o digitalizaciji in o njenem vplivu na poslovni svet in se sprašujejo, kako bodo spremembe vplivale na naša življenja. Beseda digitalizacija je postala vsakodnevni del besednjaka podjetij, na to temo je bilo objavljenih veliko člankov in marketinških sporočil. Kaj pa se je v resnici spremenilo? Kaj so podjetja pridobila in kje se zatika?

Glavni elementi interneta stvari, ki je temelj digitalizacije in 4. industrijske revolucije, so senzorji, omrežja, podatkovna skladišča, algoritmi in roboti. Vsa ta tehnologija je pripravljena in na voljo za uporabo. Vendar se koncepti in internet stvari v poslovnem svetu še niso razširili toliko, da bi lahko bistveno spremenili poslovanje podjetij. Kaj je narejenega, kje se zatika in kaj moramo kot inženirji še narediti? Poglejmo glavne sklope, z močnim poudarkom na industrijskih podjetjih.

II. SENZORJI, ALGORITMI IN UMETNA INTELIGENCA

A. Senzorji

Najprej poglejmo področje zbiranja podatkov iz fizičnega sveta in njihovo hranjenje v virtualnem svetu.

Podjetja imajo v svojem poslovanju že vpeljane različne tipe senzorjev. V primeru oskrbovalne verige se preko črtne kode ali RFID že avtomatično zaznavajo premiki blaga in palet, podjetja sledijo svojim vozilom, beležijo temperature v dostavnih vozilih, skladiščih in poslovnih prostorih, prisotnost ljudi in zasedenost cest. Podatke iz senzorjev hranijo v svojih podatkovnih skladiščih. Vendar podjetja le redko delijo podatke, ki jih imajo v svojih skladiščih. Le v primeru podatkov o javni infrastrukturi so podatki na razpolago javnosti (primer DARS, ARSO). Pojavlja se vprašanje poslovne vrednosti vseh zbranih podatkov in podjetja ne vedo dobro, kaj naj naredijo z vsemi zbranimi in razpoložljivimi podatki. Pogosto niti ne vedo, kakšno bogastvo podatkov imajo shranjeno v svojih podatkovnih skladiščih in kaj vse jim je na voljo. Po drugi strani pa se podjetja bojijo deliti te podatke, saj se zavedajo njihove vrednosti.

Mit št. 1: Podjetja so med sabo povezana v „internet podjetij“.

Slišimo izjave, da naj bi bila podjetja med sabo intenzivno in avtomatsko povezana v t.i. *internet podjetij*. V resnici podjetja med sabo niso povezana na avtomatski način, da bi se podatki izmenjevali samodejno ali da bi podjetja medsebojno gledala v podatke svojih partnerjev. Resnica je taka, da si podjetja podatke izmenjujejo polavtomatsko in kampanjsko, šele ko je poslovni dogodek že nastal ali šele takrat, ko prejmejo zahtevek za neke podatke in še to le v primeru, da je to nujno potrebno – bodisi zaradi predpisov bodisi zaradi pogodb s partnerji.

Zakaj je tako? Kot že rečeno, se podjetja zavedajo vrednosti podatkov, zato svojih podatkov niso pripravljena deliti. Hkrati ne zaupajo popolnoma v podatke, ki jih dobijo od drugod. Tretji problem pa je bolj tehničen in sicer v tem, da standardi za izmenjevanje podatkov še niso uveljavljeni in se morajo podjetja vsakič sproti dogovoriti, kako si bodo izmenjala podatke. Izmenjevalni formati za osnovne poslovne dogodke, kot so računi, naročila ali dobavnice, so sicer dogovorjeni in uveljavljeni. Formati za izmenjevanje podatkov o na primer proizvodnih kapacitetah ali o stanju zalog pa še niso uveljavljeni.

Kot primer dobre prakse lahko pomislimo na pošiljanje računov v Sloveniji. Računi so se digitalizirali šele takrat, ko je leta 2015 elektronske račune začela zahtevala državna uprava. Podobno napovedujem tudi za izmenjevanje drugih dokumentov. Šele ko se bo pojavil nekdo zunanji, ki bo zahteval elektronsko izmenjavo poslovnih podatkov in za to predpisal določen format, bodo podjetja začela izmenjevati druge podatke, najprej bodo na vrsti naročila, nato dobavnice.

Nasvet: pri izbiri in razvoju IT rešitev za izmenjavo podatkov uporabljajte standarde. Le tako bo povezovanje in izmenjevanje podatkov uspešno.

Naslednji problem v poslovnem svetu je zaupanje v prejete podatke. Kako prejemnik ve, da so prejeti podatki pravilni in zaupanja vredni? Pojav tehnologije bločnih verig sicer rešuje problem verodostojnosti podatkov, vendar je ta tehnologija pogosto neprimerna za izmenjevanje velike količine malih podatkov. Cena transakcije je prevelika, transakcije so prepočasne, podatka se ne da izbrisati. Zato bločne verige niso primerne za na primer izmenjevanje in hranjenje podatkov o temperaturi tekom življenjske dobe svežega mleka od proizvajalca do trgovca. Pojavila so se že podjetja, ki s svojimi storitvami rešujejo te težave in nastopajo kot neodvisni posrednik med podjetji, ki skrbi za verodostojnost.

Nasvet: Ideje s področja veriženja blokov se lahko aplicira tudi na druge načine. Na voljo so že neodvisne platforme tretjih oseb, ki so primerne za zaupanja vredno izmenjavo poslovnih podatkov.

B. Algoritmi

Poslovno odločanje je izredno zahtevna in odgovorna naloga v vseh podjetjih. Z dobrimi algoritmi bi sicer lahko nadomestili človeško razmišljanje, vendar je težko predvideti vsa pravila, ki jih uporabljajo ljudje pri svojem delu, razen pri najbolj monotonih delih. Še posebej težko je ta pravila opisati dovolj natančno, da bi jih lahko inženir nato sprogramiral. Zaradi pomanjkljivosti in togosti klasičnih fiksnih algoritmov vsi računajo na razvoj umetne inteligence, ki bi samo ugotovila, kako je najbolje ravnati v določenih situacijah in kakšen je optimalni algoritem.

Umetna inteligenca, ki bi sama ugotovila kako je najbolj ravnati v določenih situacijah, sicer obeta veliko. Vendar mora imeti umetna inteligenca na voljo veliko podatkov, iz katerih se lahko nauči in pa nekoga, ki se bo odločil, kaj je dobra in kaj slaba odločitev. Tu pa spet trčimo na problem razpoložljivosti podatkov, ki smo ga obravnavali v prejšnjem poglavju. V poslovnem svetu, še posebej v industriji, ki nastopa povezano v velike in kompleksne oskrbovalne verige, so podatki razpršeni med več podjetji in nepovezani. Od kod naj se torej umetna inteligenca nauči in kaj naj uporablja za svoje odločitve?

Mit št. 2: Človek rešuje probleme bolje kot stroj na podlagi umetne inteligence.

Od ljudi v podjetjih pogosto slišimo, da noben stroj ne more rešiti problema tako dobro, kot ga lahko on s svojimi izkušnjami in občutki. To drži le v primeru, če so obseg in okoliščine problema omejene. Človek lahko v svoji glavi dobro obvladuje le probleme z omejenim številom spremenljivk. Pri večjem številu vnaprej znanih spremenljivk pa človeško odločanje močno zaostaja za računalniškimi algoritmi. Kot primer pokažimo kompleksnost planiranja dostavnih poti za tovorna vozila:

Število vozil	*Število postankov na eno vozilo*	*Število možnih poti med točkami za postanke*
1	1	1
1	5	120
1	10	3.628.800
5	10	37.267.043.023.296.000

Nasvet: Pri razvoju rešitev morajo inženirji poskušati razumeti managerje, ki morajo pojasniti svoj način odločanja.

III. ROBOTI IN AVTONOMNI STROJI

Če smo se v prejšnjem poglavju ukvarjali z upravljavskimi funkcijami v podjetjih, poglejmo še izvrševalske funkcije. Govorimo o delavcih v proizvodnji, logistiki, trgovini. Njihov unikatni doprinos k poslovanju podjetij so njihove oči, možgani in roke. Posledice pojava interneta stvari se bodo močno dotaknile tudi njih, celo prej kot upravljavska delovna mesta. Izvršujejo namreč rutinska in ponavljajoča se opravila, ki ne zahtevajo pretiranega analitičnega delovanja, in jih je lažje avtomatizirati.

Fizično delo v ponavljajoči se proizvodnji so marsikje že nadomestili s stroji, ki postajajo vedno bolj celoviti in jim v najbolj napredni obliki rečemo tudi roboti. Vendar stroji za svoje delovanje potrebujejo popolnoma predvidljivo okolje. Predmet, ki ga morajo obdelati, mora biti vedno na istem mestu in v isti obliki. Če je okolica nepredvidljiva, je človek nepogrešljiv. V takih nepredvidljivih okoljih se uveljavlja t.i. obogatena resničnost (ang. augmented reality), kjer delavcu tehnologija pomaga k pravilnemu in učinkovitemu delovanju. Delavcu večinoma pomagamo z nosljivo tehnologijo. Kamera, ki jo delavec nosi na sebi, računalniku pomaga zaznati okolico delavca, preko ekrana, slušalk ali pametnih očal pa delavec od računalnika prejme navodila za delo. Gre za trenutno izredno učinkovito kombinacijo človekovih kognitivnih in ročnih spretnosti z računalnikovo analitično in procesno zmogljivostjo, ki se bo vedno bolj pogosto pojavljala. Včasih ji rečejo tudi kolaboracija med roboti in človekom oz. kolaborativni robot.

Prikaz dveh primerov kolaborativnih delovnih mest in obogatene resničnosti je na naslednjih povezavah:

- Gorenje: https://youtu.be/DeOuIwMX2Ws ,
- Plodine: https://youtu.be/bJGkSlclHhw?t=17 .

Kakšne pa so posledice take digitalizacije izvrševalskih delovnih mest? Kaj si o tem mislijo podjetja in kaj delavci? V časopisih beremo naslove, kot so na primer: *Prihajajo roboti in vzeli vam bodo delovna mesta!*. Kaj žene podjetja, da v svoje procese uvajajo avtomatizacijo in robotizacijo?

Prvi razlog za avtomatizacijo je v želji po povečevanju lastne produktivnosti – narediti čim več s čim manj vložka in čim hitreje. V to podjetja žene potreba po konkurenčnosti in zahteva lastnikov po povratku njihovega kapitalskega vložka.

Drugi vzgib podjetij pa je v pomanjkanju primernih delavcev. Podjetja po celi Evropi zadnja leta vedno težje dobijo delavce, ki bi bili pripravljeni opravljati manj zahtevna in manj plačana delovna mesta. Težko je dobiti delavce v proizvodnji, skladiščnike, voznike tovornih vozil. Zato so podjetja primorana iskati tehnološke rešitve in vedno bolj zahtevajo robotizacijo.

Vmesna rešitev med ročnim delom in robotiziranim delom so že omenjene hibridne rešitve (nosljivi senzorji, glasovna komunikacija, pametna očala…).

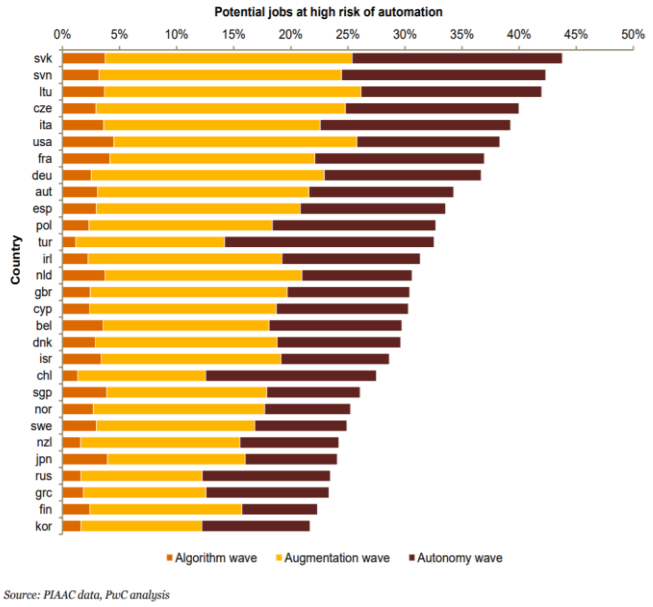
Mit št. 3: Zaposleni se upirajo digitalizaciji.

Zaposleni se sicer res upirajo digitalizaciji, saj to predstavlja spremembo in sprememb se večina ljudi boji. Digitalizaciji se upirajo tudi iz osebnega strahu, da bodo izgubili lastno delovno mesto. Razumljivo! Hkrati pa je res tudi to, da so podjetja prisiljena iskati avtomatizacijo in

robotizacijo, ker za nekatera delovna mesta ne najdejo več dovolj zaposlenih. Bazen delovne sile je namreč omejen.

Kaj je torej vzrok in kaj posledica? Pomanjkanje zaposlenih ali roboti?

Na tem mestu lahko omenimo tudi rezultate raziskave *Will robots really steal our jobs?*, ki so jo v letu 2018 naredili v podjetju Pricewaterhouse Coopers (PwC). V študiji so napovedali, da bo okoli leta 2035 po svetu izginilo okrog 30 % sedanjih delovnih mest v trgovini, 40 % v industriji in 50 % v logistiki. V Sloveniji naj bi zaradi avtomatizacije izginilo okoli 45 % delovnih mest – skoraj največji odstotek v celotni skupini od 29 obravnavanih držav!



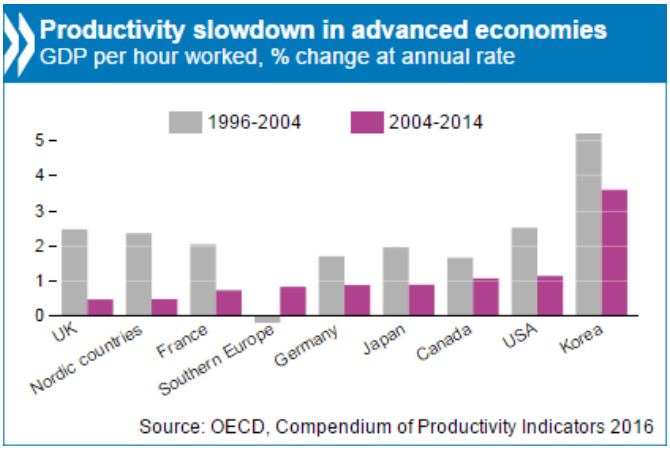
Vir: [1] PWC, Will robots really steal our jobs, 2018

Nasvet: ne pozabite na delavce, ki morajo uporabljati IT rešitve ali delati skupaj z roboti. Delavce te novosti lahko globoko motijo.

Mit št. 4: zaradi avtomatizacije narašča produktivnost.

Če slišimo izjavo, da zaradi avtomatizacije delovnih procesov narašča produktivnost, bomo brez veliko razmišljanja prikimali. Zato so bili rezultati raziskave organizacije OECD iz leta 2016 izredno presenetljivi. V večini držav OECD se je rast produktivnosti namreč upočasnila. Do leta 1980 je produktivnost rasla z okrog 4 % letno, v letih okoli 2010 pa je rast produktivnosti padla na 1 % letno. Kaj je razlog za to? OECD je postavil tezo, da se digitalne tehnologije v resnici v gospodarstvo širijo počasneje, kot si mislimo, hkrati pa so bili največji učinki digitalizacije že doseženi.

Nasvet: iščite poslovne rezultate uvedbe tehnoloških rešitev, ne zasledujte samo uvedbe tehnologije kot take.



Vir: [2] The global productivity slowdown, technology divergence and public policy: a firm level perspective, Dan Andrews, Chiara Criscuolo, Peter Gal, 2016.

IV. POSLOVNI IZZIVI PODJETIJ

Ko razmišljamo o uporabi interneta vsega v podjetjih, ne smemo pozabiti ključnih gonil za kakršne koli spremembe v poslovanju industrijskih podjetij - povečevanje produktivnosti in posledično večjih dobičkov in povratka investicije. Podjetje se ne bo odločilo za investicijo, kot je uvedba digitalizacije, če v njej ne bo videlo poslovnih koristi. Samo inženirski pristop k tehnoloških inovacijam za podjetja ni dovolj. Potrebujejo jasno vidne koristi zase. Če pa pogledamo na to, kako na poslovne odločitve gledajo posamezni odločevalci v podjetjih, ne smemo pozabiti na njihove človeške lastnosti:

1. težko razumevanje potencialov tehnološkega napredka, kratkoročnih in dolgoročnih,
2. strah pred spremembami, odpiranjem in povezovanjem.

Delo, 2. 6. 2016: *Več kot polovica organizacij se sooča z izzivi oblikovanja pravilne strategije, kako novo tehnologijo in inovacije uporabiti za nove poslovne modele in storitve in kako tehnologija pomaga pri rasti, produktivnosti, zdravju človeka, mobilnosti ter pametni uporabi naravnih virov.*

Mit št. 5: Podjetja se o spremembah odločajo na podlagi analiz.

Analize so pogosto res podlaga za poslovne odločitve. V resnici pa se na koncu o neki poslovni potezi odloči človek z vsemi svojimi frustracijami in pomanjkljivostmi. Pogosto so poslovne odločitve instinktivne ali zasnovane na črednem in ohranitvenem nagonu in ne na analitičnem pristopu.

Nasvet: razmišljajte celovito, upoštevajte vse od osebnosti ljudi do poslovnih koristi nove tehnologije.

V. ZAKLJUČEK

Internet stvari, internet podjetij in digitalizacija so gibanja, ki se jim podjetja ne smejo izogniti, če želijo biti uspešna. Pogosto pa uporaba novih pristopov zahteva tudi spremembo miselnosti v podjetjih. Zahtevana je večja stopnja odprtosti, deljenje podatkov, več sodelovanja. Podjetja morajo premagati strah pred temi spremembami in se povezati v čvrste in hkrati fleksibilne oskrbovalne verige, ki

pa postajajo vedno bolj kompleksne. Obvladovanje modernih digitaliziranih oskrbovalnih verig bodo prevzela specializirana podjetja, ki bodo prevzela odgovornost za povezovanje in učinkovitost cele verige. To bo tudi manjšim podjetjem močno olajšalo vstop v velike svetovne oskrbovalne verige. Prihodnost je v odprtih digitalnih povezovalnih platformah.

LITERATURA

[1] PWC, Will robots really steal our jobs, 2018 https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/impact_of_automation_on_jobs.pdf

[2] The global productivity slowdown, technology divergence and public policy: a firm level perspective, Dan Andrews, Chiara Criscuolo, Peter Gal, 2016 https://www.oecd.org/global-forum-productivity/events/GP_Slowdown_Technology_Divergence_and_Public_Policy_Final_after_conference_26_July.pdf

O AVTORJU

Andrej Planina je zaposlen kot direktor divizije na Špici in se ukvarja z rešitvami za oskrbovalno verigo, od proizvodih podjetij, preko distribucije do trgovcev. Dolgoletne izkušnje pri uvajanju IT rešitev v poslovanje podjetij mu omogočajo širok pogled tako na tehnologijo kot na spremembe v poslovanje podjetij.

Predlog poenotenega zbiranja in ponovne uporabe podatkov s pomočjo integracijske platforme IoT

Egon Milanič in Jurij Dolžan, Direktorat za informacijsko družbo, Ministrstvo za javno upravo RS

Povzetek — V tem članku je predstavljen predlog standardiziranega zbiranja in (ponovne) uporabe podatkov iz različnih sistemov, platform in omrežij. Predlog temelji na uporabi standardiziranih gradnikov, ki jih zagotavlja Evropska komisija in je potencialno uporaben tudi kot prototip za izmenjavo podatkov znotraj državne/javne uprave ter med različnimi administracijami znotraj EU.

Ključne besede — digitalizacija, pametna mesta in skupnosti, internet stvari, IoT, zbiranje podatkov, izdelovalci podatkov, potrošniki podatkov, masovni podatki, odprti podatki, digitalno preoblikovanje

Abstract — In this article a proposal for standardised data gathering and (re)use is presented. Data from different systems, platforms and networks can be collected and made available for (re)use by implementing standardised building block(s) provided by European Commission. Similar prototype may be used for data exchange inside public administration and between Member States.

Keywords — digitalisation, smart cities, IoT, big data, open data, data producers, data consumers, digital transformation

I. UVOD

Internet stvari (ang. Internet of Things; IoT) je že nekaj časa »naslednja velika stvar«. Napovedi vodilnih analitskih hiš navajajo več milijard stvari, ki bodo povezane krojile naše vsakdanjike in omogočile na stotine milijonov evrov zaslužkov in prihrankov. Evropska komisija je prepoznala možnosti, ki jih ponuja IoT, prav tako Slovenija, kot izhaja iz strategije Digitalna Slovenija 2020 in Strategije pametne specializacije. Ministrstvo za javno upravo (MJU) temu področju namenja veliko pozornosti. Na infrastrukturnem področju načrtuje vzpostavitev razvojno-inovacijskega oblaka (RIO), v katerega bo vključena tudi platforma IoT (Milanič, 2017).

Digitalizacija mest in skupnosti pelje po poti zahtevnega preoblikovanja, ki vključuje družbene, gospodarske, urbane, mobilnostne, izobraževalne, tehnološke in kulturne spremembe. Mesta s tem postajajo izhodiščna digitalna platforma za digitalno preoblikovanje celotne družbe, kar navaja tudi strategija Digitalna Slovenija 2020, v kateri je razvoj pametnih mest in skupnosti ena izmed dveh vsebinskih prioritet (Turk, 2017).

Cilj uporabe tehnologije interneta stvari v mestih in skupnostih je razviti povezan inteligentni sistem, ki bo prispeval h gospodarskim dejavnostim, izboljšal zadovoljstvo občanov z javnimi storitvami, prispeval k javni varnosti, trajnostnemu upravljanju z okoljem, učinkovitejšemu upravljanju mest in k spopadanju z drugimi izzivi, s katerimi se soočajo mesta in skupnosti (Turk, 2017).

MJU bo omogočilo zbiranje in ponovno uporabo podatkov iz IoT platform, na katerih bodo rešitve za pametna mesta in skupnosti (oz. občine), financirane iz javnega razpisa.

Temelj razvoja, raziskav in inovacij znotraj RIO bodo, v velikem delu, zbrani in drugače dosegljivi (masovni) podatki. Zato je potrebno zagotoviti zbiranje podatkov v čim večjem obsegu iz čim več virov. Zbrani podatki pa bodo uporabni le, če bodo enostavno dosegljivi in bo poznan njihov pomen ne glede na to iz katerega vira izhajajo.

Z realizacijo tukaj predstavljenega predloga lahko MJU omogoči poenoteno zbiranje in ponovno uporabo podatkov iz različnih IoT virov. Predlog hkrati razširja zbiranje in uporabo podatkov tudi na druge »izdelovalce« in »potrošnike« podatkov. Utemeljitev predloga je podana v nadaljevanju.

Predlog temelji na standardiziranem načinu zbiranja in (ponovne) uporabe podatkov. Vse potrebne naloge »izdelovalci« in »potrošniki« podatkov opravijo preko standardiziranih odprtih programskih vmesnikov (API), prav tako pa je standardiziran tudi podatkovni model za opis podatkov, ki se zbirajo oz. izmenjujejo. Uporabljeni standardi za izmenjavo podatkov in podatkovni modeli so nastali znotraj EU. Predlog vsebuje tudi ustrezne informacijsko-varnostne rešitve za zagotovitev varnosti in zasebnosti podatkov.

Realizacija temelji na uporabi »Context Brokerja[1]«, enega od obstoječih CEF[2] digitalnih gradnikov[3], ki jih zagotavlja Evropska komisija in so namenjeni enostavnejši vzpostavitvi Enotnega digitalnega trga v EU. »Context Broker« omogoča organizacijam, da enostavno delijo podatke. Temelji na EU standardih, podobno pa velja tudi za podatkovne modele, ki jih uporablja. Uporaba (odprtokodnega) digitalnega gradnika je brezplačna, zagotovljeno je tudi dolgoročno vzdrževanje ter podpora pri uvajanju s strani Evropske komisije oz. CEF. Predlagana rešitev je širše uporabna in je lahko temelj za različne izmenjave podatkov med administracijami znotraj SI in znotraj EU.

V nadaljevanju je predlog podrobneje opisan, prav tako pa so razdelani tudi predvideni nadaljnji koraki potrebni za realizacijo.

II. TEHNIČNA ZASNOVA

A. *Predlog*

Predlog je povzet po modelu OASC (Open Agile Smart Cities) iniciative in sicer z implementacijo OASC Minimal Interoperability Mechanisms (MIMs), ki zajema vzpostavitev:

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Context+Broker
[2] CEF Connecting Europe Facility oz. IPE Instrument za povezovanje Evrope, https://ec.europa.eu/inea/en/connecting-europe-facility
[3] Connecting Europe Facility (CEF) Digital Building Block

1. Context Information Management-a na temelju standardiziranih API vmesnikov;
2. Skupni podatkovni model (Common data models), harmoniziran s strani OASC oz. Sinchronicity;
3. Podatkovne tržnice (Ecosystem Transaction Management (marketplaces)).

Ad 1) Za osnovni element nove realizacije platforme IoT je predlagan Context Broker, ki je vmesnik med »izdelovalci« podatkov in »potrošniki« le teh in je zasnovan tako da prekine povezanost oz. odvisnosti med njimi (decoupling). Context Broker temelji oz. je realizacija standardiziranih vmesnikov API za, poenostavljeno, objavo (»izdelovalec«) in rabo (»potrošnik«) podatkov, ki se pretakajo preko Context brokerja. Context Broker zagotavlja tudi opis in s tem pomen podatkov.

Ad 2) Skupni podatkovni model je ključen za zagotavljanje interoperabilnosti rešitev oz. za ponovno uporabo zbranih podatkov. Zelo poenostavljeno je predpis, ki določa, na kakšen način bodo zbrani podatki opisani.

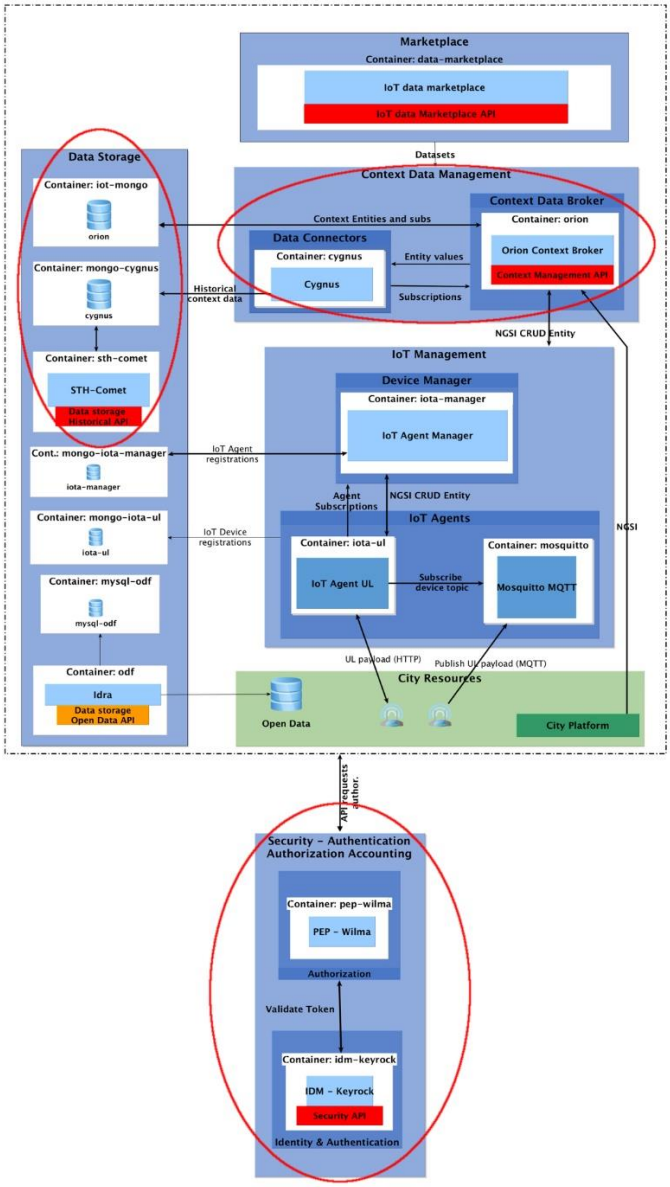
Ad 3) Javna tržnica (IoT) podatkov, ki daje na razpolago zbrane podatke iz različnih virov, predstavljene na poenoten način, je opcijska in se lahko izvede v naslednji (drugi) fazi. Glede na dosedanje vedenje je vzpostavitev precej kompleksna, nekatere od komponent pa so šele v fazi razvoja. Tržnica podatkov omogoča različne načine uporabe podatkov kot so sklepanje pogodb, zagotavljanje SLA, plačila za uporabo podatkov ipd.

Tehnična izvedba je v osnovi povzeta po projektu SynchroniCity (synchronicity-iot.eu), ki je realizacija zgoraj navedenega MIM koncepta in temelji na FIWARE komponentah med katerimi je najpomembnejši »digital building block« FIWARE/CEF Context Broker. Tudi (opcijska) tržnica podatkov temelji na FIWARE/ SynchroniCity[4].

B. Ključne komponente

Ključna komponenta (building block) je FIWARE/CEF Context Broker na temelju standarda OMA NGSI za poenoten dostop do podatkov (API-ji). Standardizacija oz. harmonizacija podatkovnih modelov poteka v okviru projekta SynchroniCity v sodelovanju z asociacijo Open Agile Smart Cities (OASC Shared Data Models for Smart City domain). Predstavljeni koncept je skladen z MIM (Minimal Interoperability Mechanisms) OASC. Za delovanje je potrebno še nekaj podpornih komponent, ki jih ravno tako lahko zagotovi CEF oz. FIWARE. Opisani koncept je že vzpostavljen v Synchronicity »large scale« IoT projektu, ki ga financira Evropska komisija.

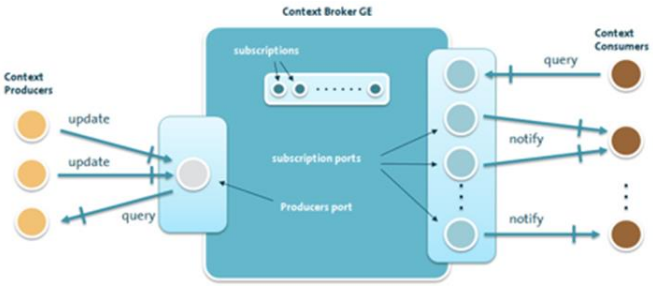
Implementacija SynchroniCity referenčne arhitekture je povzeta na spodnji sliki[5]. Predlog (v prvi fazi) predvideva realizacijo z rdečo obkroženih komponent (na sliki predstavljene kot Docker vsebniki[6]). Rdeče pobarvani pravokotniki predstavljajo (na ven) izpostavljene stične točke platforme/predloga, ki so realizirane kot standardizirani odprti API-ji.



Slika 1: SynchroniCity referenčna arhitektura

Poleg Context Brokerja s pripadajočim Data Connector-jem, so na sliki še podporne komponente namenjene zapisu historičnih podatkov (Data Storage na sliki levo) ter varnostne komponente (na sliki spodaj).

V nadaljevanju je podrobneje prikazana ključna komponenta - Context Broker[7].



Slika 2: Context Broker

[4] Iniciativa Digital Catapult UK vzpostavlja storitev podatkovne tržnice na osnovi teh komponent.

[5] https://synchronicity-iot.eu/wp-content/uploads/2018/09/SynchroniCity_D2.10.pdf (str. 63).

[6] ang. container

[7] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773700

FIWARE/CEF Context Broker deluje kot posrednik med izdelovalci (producers) in potrošniki (consumers) podatkov/informacij. Potrošniki po podatkih povprašujejo ali/in se na podatke naročajo in jih prejemajo na podlagi naročnin. Med izdelovalci in potrošniki ni neposredne povezave. Ključno je, da so podatki opremljeni s pomenom in da so, s stališča naročnikov, poenoteni. Naročnik se torej lahko naroči na posamezen tip podatkov ne glede na vir podatkov.

C. *Informacijska varnost*

Varnost podatkov in platforme je zagotovljena z uporabo ustreznih komponent za identifikacijo, avtentikacijo in avtorizacijo. Upravljanje komponent poteka preko ustreznih API vmesnikov. S tem je omogočena tudi integracija z drugimi/obstoječimi sistemi.

D. *(Odprti) podatki*

Prikazani predlog rešitve omogoča ustrezno zaščito varovanja podatkov v smislu varstva osebnih in drugih občutljivih podatkov.

Podatki, zbrani in ponovno uporabljeni na osnovi tukaj predlagane rešitve, bodo sicer v večji meri odprti podatki. Tehnična rešitev pa omogoča tudi ostale načine uporabe podatkov ob zagotovitvi zgoraj navedene zaščite.

Prikaz presega namen tega članka. Principi in implementacija so podrobno opisani v dokumentu »D2.4. Basic data market place enablers[8]« projekta SinhroniCity.

III. UTEMELJITEV PREDLOGA

Odprti in standardizirani načini dostopa do podatkov ter podatkovni modeli so ključni za uspešno ponovno uporabo podatkov, ki se nahajajo v posameznih (silosnih) rešitvah oz. platformah. CEF z digitalnim gradnikom (FIWARE) Context Broker naslavlja ključno potrebo tržišča: standardizirano upravljanje konteksta podatkov. Odprti API vmesniki so definirani in objavljeni (trenutno FIWARE-NGSI v2, nova verzija brokerja bo skladna s pravkar objavljenim standardom ETSI[9]). Standardizacija oz. harmonizacija podatkovnih modelov poteka v okviru projekta SynchroniCity v sodelovanju z OASC (OASC Shared Data Models for Smart City domain[10]). Možno je tudi dodajanje novih podatkovnih modelov – na predpisan način.

Z uporabo FIWARE/CEF Context Broker-ja je zagotovljena:

- Implementacija standardov, ki so v domeni EU (FIWARE/Synchronicity Data models).
- Podpora pri načrtovanju in implementaciji FIWARE komponent (building blocks) s strani EK CEF Connecting Europe Facility kot gradnikov enotnega digitalnega trga.
- Dolgoročna podpora in razvoj zagotovljena s financiranjem EK za naslednjo finančno perspektivo.
- Podpora uporabi s strani OASC (koncept MIM).

A. *FIWARE*

i. *Kaj je FIWARE?*

FIWARE je odprta pobuda Evropske komisije v sklopu javno-zasebnega partnerstva za internet prihodnosti, katerega cilj so večja učinkovitost poslovnih procesov in pametnejša infrastruktura, ki podpira inovativne aplikacije v različnih sektorjih. Podjetjem in vladam poskuša pomagati z razvojem internetnih rešitev, ki bodo zmožne obdelovati eksponentno povečane spletne podatke, s katerimi se srečujemo v današnjem svetu in jim obstoječe tehnologije niso več kos. Projekt FIWARE tako ustvarja trajnostni, globalen in odprt ekosistem inovacij z namenom, da podjetnikom olajša uresničitev idej in priložnosti novega vala digitalizacije. Projekt temelji na petih stebrih, in sicer: tehnološki platformi FIWARE, prosto dostopnem testnem okolju FIWARE Lab, zbirki orodij za upravljanje FIWARE Ops, programu pospeševalcev FIWARE Accelerate in programu za promocijo pobude izven Evrope FIWARE Mundus (Kos, 2015).

ii. *Platforma FIWARE*

Tehnološka platforma FIWARE, ki predstavlja jedro projekta, je razširitev odprte in hitro razvijajoče se oblačne platforme OpenStack. Poleg osnovnih možnosti gostovanja v oblaku ponuja dodano vrednost v obliki množice storitveno usmerjenih osnovnih gradnikov (Generic Enabler – GE), ki zagotavljajo odprte aplikacijske programske vmesnike (API) za enostavnejši razvoj inovativnih aplikacij. Tako prinaša komponente, ki med drugim omogočajo povezavo z internetom stvari (IoT), podporo pametnim in kontekstno odvisnim aplikacijam s pomočjo procesiranja velike količine podatkov v realnem času, kot tudi analizo velikih podatkov (Big Data) in vključitev naprednih spletnih vmesnikov. Specifikacije vseh komponent oziroma osnovnih gradnikov so javno dostopne, kar omogoča različne implementacije posameznih ponudnikov, hkrati so podprte z odprtokodnimi referenčnimi implementacijami, ki so na voljo v katalogu FIWARE in omogočajo takojšno uporabo, s tem pa hitrejši prodor na trg (Kos, 2015).

B. *CEF – Connecting Europe Facility*

CEF oz. Instrument za povezovanje Evrope (IPE) omogoča pripravo in izvajanje projektov skupnega interesa v okviru politike vseevropskih omrežij za energetski, prometni in telekomunikacijski sektor ter kohezijske politike. Instrument za povezovanje Evrope bo financiral velike infrastrukturne projekte za izboljšanje evropskih prometnih, energetskih in digitalnih omrežij. S tem instrumentom se bo zagotovilo financiranje projektov, namenjenim vzpostavitvi manjkajočih povezav v evropskih energetskih, prometnih in digitalnih omrežjih, kar bo pripomoglo k dopolnitvi enotnega trga EU. Projekti bodo okrepili tudi okoljske ukrepe v gospodarstvu s spodbujanjem uporabe čistejših prevoznih sredstev, hitrih širokopasovnih povezav in energije iz obnovljivih virov. Instrument za povezovanje Evrope je naslednik vseevropskih mrež na področju energije in transporta (TEN-E in TEN-T) (SBRA, 2014).

Med specifičnimi cilji CEF najdemo tudi projekte za dograditev temeljne infrastrukture za širokopasovna omrežja, infrastrukture za čezmejne projekte e-vlade in e-zdravja, za elektronski dostop do javnih informacij in večjezičnih storitev, za čezmejni dostop do sistemov elektronskih

[8] https://synchronicity-iot.eu/wp-content/uploads/2018/09/SynchroniCity_D2.4.pdf

[9] ETSI GS CIM 009 V1.1.1 (2019-01); ETSI is one of only three bodies officially recognized by the EU as a European Standards Organization (ESO); https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.01.01_60/gs_CIM009v010101p.pdf

[10] https://gitlab.com/synchronicity-iot/synchronicity-data-models

identifikacij za državljane in podjetja, za elektronska javna naročila, infrastrukture in za sklepanje poslov po elektronski poti v drugih državah članicah.

CEF kot enega od vzvodov za doseganje naštetega, v okviru CEF Digital[11] financira digitalne gradnike. Trenutno so na voljo naslednji: Context Broker, eArchiving, eDelivery, eID, eInvoicing, eSignature in eTranslation. Ti gradniki omogočajo osnovne funkcionalnosti, ki se lahko uporabijo za pospeševanje vzpostavljanja digitalnih javnih storitev.

V CEF so, poleg gradnikov, za katerih vzdrževanje skrbi Evropska komisija, zagotovljena še nepovratna sredstva za podporo državam članicam pri implementaciji projektov, ki uporabljajo zgoraj omenjene gradnike.

IV. POVEZAVA Z JAVNIM RAZPISOM ZA VZPODBUJANJE IOT REŠITEV V OBČINAH

Lokalnim skupnostim se sofinancira uvajanje IoT senzorskih omrežij, s katerimi bodo mesta in skupnosti reševala svoje najbolj pereče probleme. Podpre se projekte, ki rešujejo realne potrebe iz lokalnega okolja. Spodbuja se povezovanje lokalnih skupnosti oz. projekte, ki bodo vključevali čim večje število lokalnih skupnosti, po možnosti organiziranih na ravni združenj občin (Turk, 2017).

Ponudnike IoT rešitev (na lastnih ali tujih platformah) za občine (oz. »izdelovalce« podatkov) se zaveže k izmenjavi podatkov na osnovi standardiziranih API-jev za izmenjavo podatkov in predpisanih podatkovnih modelov za opis posredovanih podatkov. V praksi bi to pomenilo, da bi se ponudniki IoT rešitev z API klici povezali na Context Broker kot »producer-ji« oz. »izdelovalci« ali kot potrošniki podatkov drugih »izdelovalcev«.

Pri pripravi razpisa bomo izhajali iz slovenskih strateških dokumentov, iz dobrih praks tujine in iz dokumenta, ki ga je pripravila Evropska komisija »Blueprint for cities and regions as launchpads for digital transformation[12]«.

V. ZAKLJUČEK

Prvotni načrti Ministrstva za javno upravo, Direktorata za informacijsko družbo so bili, da za potrebe pametnih mest in skupnosti v okviru Razvojno-inovativnega oblaka vzpostavi platformo interneta stvari, ki bi omogočala priklop senzorjev, podpirala najrazličnejše načine komunikacije, omogočala zbiranje podatkov ter izdelavo aplikacij, ki bi služile pametnim mestom in skupnostim. Načrti so nastali v začetku finančne perspektive 2014 - 2020. Nagel razvoj trga in s tem pojav komercialnih IoT platform je privedel do odločitve, da Ministrstvo za javno upravo zagotovi zgolj dostop in ponovno uporabo podatkov. V tem članku predstavljena realizacija zgoraj navedenih zahtev z uporabo Context Brokerja in ostalih potrebnih komponent, predstavlja evropsko zgodbo, ki je že uveljavljena in primerno standardizirana. Ministrstvo za javno upravo z realizacijo predloga ne bi poseglo na trg, hkrati pa bi podprlo rešitve, ki lahko naredijo naše življenjsko okolje boljše, pametnejše in učinkovitejše. Hkrati bi slovensko gospodarstvo imelo možnost postaviti odlične primere dobrih praks, kot odskočno desko za nastope na tujih trgih.

[11] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/The+Vision
[12] https://ec.europa.eu/growth/content/blueprint-cities-and-regions-launch-pads-digital-transformation-0_en

ZAHVALE

Avtorja se zahvaljujeva Ministrstvu za javno upravo, Direktoratu za informacijsko družbo za podporo pri udeležbi na 35. delavnici o telekomunikacijah VITEL 2019: Uporabna vrednost Interneta vsega.

VIRI

[1] Kos, J. (2015). *Postavitev in upravljanje računalniškega oblaka na platformi FIWARE : diplomsko delo.* Ljubljana: Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.

[2] Milanič, E. (2017). Internet stvari in nizkoenergijska prostrana omrežja v okviru razvojno-inovacijskega oblaka – priložnost za pametnejša mesta in skupnosti. *Informatika v javni upravi - Zbornik.* Brdo pri Kranju: Slovensko društvo Informatika.

[3] SBRA. (2014). *Instrument za povezovanje Evrope.* Pridobljeno iz Slovensko gospodarsko in raziskovalno združenje (SBRA): https://www.sbra.be/sites/default/files/instrument_za_povezovanje_evrope.pdf

[4] Turk, M. (2017). IoT za pametna mesta. *33. delavnica o telekomunikacijah VITEL.* Brdo pri Kranju: Slovensko društvo za elektronske komunikacije SIKOM.

Egon Milanič je univ. dipl. inž. računalništva in informatike ter magister znanosti s področja kakovosti in varnosti informacijskih sistemov. Poklicno pot je začel kot razvojnik strojne in programske opreme za mikrokrmilnike. Na carini je delal v podpori uporabnikom ter nato vodil Skupino za Informacijsko varnost in Oddelek za tehnološko podporo. Profesionalno kariero je nadgradil na mednarodnem projektu Evropske komisije – kot ključni izvedenec je skrbel za IT in zagotavljanje kakovosti. Od leta 2017 je zaposlen na Ministrstvu za javno upravo v Direktoratu za informacijsko družbo.

Jurij Dolžan je magister znanosti s področja elektrotehnike. Poklicno pot je začel kot razvojnik programske opreme za števce električne energije. Na Ministrstvu za visoko šolstvo, znanost in tehnologijo je prevzel delo na strukturnih skladih s pripravo ukrepov za spodbujanje raziskovalno razvojnih projektov informacijske družbe. Trenutno je zaposlen na Ministrstvu za javno upravo v Direktoratu za informacijsko družbo, kjer skrbi za pripravo politik, digitalizacijo slovenskega jezika, trgovinske sporazume in pripravo ukrepov kohezijske politike.

Slovenska iniciativa 5G – spekter za vertikale in IoT

Janja Varšek, Meta Pavšek Taškov, Agencija za komunikacijska omrežja in storitve RS, Ljubljana

Povzetek — Agencija za komunikacijska omrežja in storitve AKOS želi v okviru svojih pristojnosti prispevati k cilju čim hitrejšega uvajanje novih tehnologij skladno z usmeritvami na EU in nacionalnemu nivoju in prispevati k temu, da bi bila Slovenija med prvimi državami v Evropi, ki bodo uvedle tehnologijo 5G. Tako že nudi podporo projektom 5G v smislu sodelovanja v projektih, sproščanja novih frekvenc za testiranja tehnologij 4G/5G, skladno z ZEKom-1 ter povezovanja s tujimi regulatorji za podporo meddržavnim projektom. Članice Evropske Unije so že začele izvajati priporočila prvega in drugega mnenja *Odbora za politiko upravljanja radiofrekvenčnega spektra RSPG* o 5G. Tretje mnenje prinaša strategijo radiofrekvenčnega spektra za vertikale in predlaga priporočila za posamezne vrste vertikal. Agencija je pripravila triletno *Strategijo upravljanja z radiofrekvenčnim spektrom*, ki je v postopku sprejemanja. Članek opisuje: (a) spekter za IoT, (b) vrste vertikal opisane v tretjem mnenju RSPG, (c) možne rešitve za vertikale preko 4G/5G omrežij, (d) predlog spektra za omrežja 4G/5G preko mobilnih operaterjev in namenskega spektra za vertikale v osnutku *Strategije upravljanja z radiofrekvenčnim spektrom*.

Ključne besede — 5G, 3. mnenje RSPG, poslovno kritične vertikale, vertikala sistema za javno varnost ter zaščito in reševanje, predlog spektra za 4G/5G za javne mobilne storitve, predlog možnega namenskega spektra za vertikale, M2M, IoT, LP-WAN, WAS/RLAN, ITS

Abstract — Within its framework and competencies Agency for Communications Networks and Services (Agency) wishes to contribute to the goal, to introduce new technologies as soon as possible in accordance with the EU regulation and national level strategic guidance and possibly become one of the first countries in Europe to introduce 5G technology. Within its competencies Agency has already started to support the 5G projects in terms of the releasing new frequencies for 4G/5G testing in accordance with ZEKom-1, and by cooperation with other European regulators in order to support the announced 5G projects. EU Member States have started to implement some recommendations from the first and second Radio Spectrum Policy Group (RSPG) Opinions on 5G at national level. In addition, in this third opinion the RSPG provides spectrum strategic views on verticals and proposes some high level recommendations. The Agency has prepared a three-year *Radio Frequency Spectrum Management Strategy* that is currently in approval process. This paper present also: (a) Spectrum for IoT (b) Types of verticals in accordance with 3rd opinion of RSPG, (c) Possible 4G/5G solutions for verticals, (d) Proposal for 4G/5G spectrum over mobile operators and possible dedicated spectrum for mission and business critical verticals in draft Spectrum Strategy.

Keywords — 5G, 3rd opinion of RSPG, business critical verticals, mission critical verticals, proposal of 4G/5G spectrum for public mobile services, proposal of possible dedicated spectrum for verticals, M2M, IoT, LP-WAN, WAS/RLAN, ITS

I. UVOD

Agencija za komunikacijska omrežja in storitve (AKOS) na podlagi javnega pooblastila, skladno z Zakonom o elektronskih komunikacijah, upravlja z radijskim spektrom in številskim prostorom v Republiki Sloveniji. Poleg učinkovite izrabe radiofrekvenčnega spektra in zagotavljanja učinkovite konkurence na trgih brezžičnih storitev elektronskih komunikacij so njene prednostne naloge predvsem uporaba radiofrekvenčnega spektra za dosego največjega možnega družbeno ekonomskega napredka, zagotovitev stabilnega okolja za uporabnike radijskega spektra, spodbujanje naložb za razvoj in čim hitrejšega uvajanja novih tehnologij, skladno z usmeritvami na EU in nacionalnemu nivoju.

Agencija želi v okviru svojih pristojnosti prispevati k cilju čim hitrejšega uvajanje novih tehnologij, skladno z usmeritvami na EU in nacionalnemu nivoju in prispevati k temu, da bi bila Slovenija med prvimi državami v Evropi, ki bodo uvedle tehnologijo 5G. Tako v okviru svojih pristojnosti že nudi podporo projektom 5G v smislu sodelovanja v projektih, sproščanja novih frekvenc za testiranja tehnologij 4G/5G, skladno z ZEKom-1 ter povezovanja s tujimi regulatorji za podporo meddržavnim projektom.

II. SPEKTER ZA IOT

Odbor za politiko radijskega spektra (RSPG) je v svojem mnenju o spektru in drugih vidikih interneta stvari (IoT, Internet of Things) in komunikacij stroj-stroj (M2M) [1] zapisal:

1. Aplikacije IoT so zelo raznovrstne in imajo zelo različne zahteve glede hitrosti prenosa podatkov, zakasnitev, zanesljivosti in izhodne moči.

Massive communications	Critical communications
Use cases	
Collection/gathering of information Smart building Logistics, tracking and fleet management Smart meter Smart agriculture Capillary networks	Command/control/monitoring Remote health care Traffic safety and control Industrial application and control Remote manufacturing, training, surgery Industrial IoT, critical infrastructures (factory automation, motion control, remote control, smart grid, tactile internet, process automation)
Operational requirements	
Low device cost, simple cheap devices, low energy consumption Small data volumes, intermittent uses Can tolerate signal latency, no delay sensitive Massive number of devices Extended coverage (urban and rural environment), coverage inside of buildings	Ultra-reliability High availability Potentially uninterrupted communications Real-time communications, very low signal latency Guaranteed in-time delivery Often local coverage

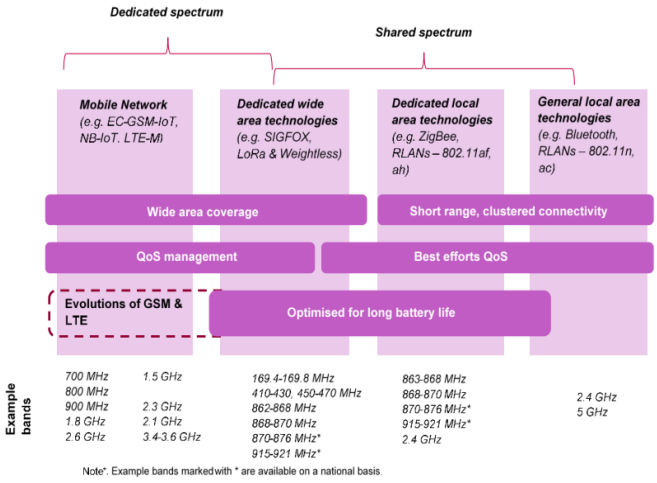
Slika II-1: Različne zahteve aplikacij IoT

2. Zaradi potreb vertikal se obeta eksponentna rast uporabe teh naprav, zlasti v spektru pod 1 GHz,.

Telemetry	Fleet management	Service and maintenance	Security and surveillance
• Utility meters • Parking meters • Industrial meters • Elevators • Vending machines	• Cargo tracking • Stock management • Temperature control • Route planning • Order tracking • Vehicle diagnostics	• Industrial machines • Vending machines	• Public surveillance • Asset monitoring • Congestion and movement monitoring • Urban management
Telematics and transport	**Home applications**	**E-health applications**	**Sales and payment**
• ITS • Navigation • Traffic / weather info • Road safety • Vehicle diagnostics • Location services	• Heating control • Electrical appliances • Alarms and security • Surveillance cameras • Garage and garden	• Patient monitoring • Remote diagnostics • Activity monitoring • Lifestyle suggestions • Personal security	• Point-of-sale terminals • Vending machines • Gaming and entertainment

Slika II-2: Primeri vertikal, ki uporabljajo IoT

3. Ni potrebe po določitvi dodatnega namenskega spektra za IoT, obstoječi spekter (Slika II-3) zadostuje.



Slika II-3: Spekter za IoT

4. Glede na velike potrebe industrije za dostop do spektra v frekvenčnem pasu 800-900 MHz, predlaga RSPG harmonizacijo z upoštevanjem potreb za železniške aplikacije.
5. Za IoT je pomembna ekonomija obsega, zato predlagajo harmonizacijo pasov za naprave kratkega dosega (SRD, Short Range Devices) in naprave za širokopasovni prenos podatkov (LP WAN, Low Power Wireless Area Network), vključno s pasovi za WiFi in harmonizacijo pasov za javne mobilne storitve za uporabo storitev IoT.
6. V točkah 6 – 12 priporoča RSPG uporabo storitev LP WAN in ostalih IoT v licenčnih pasovih za PMR (Private Mobile Radio) za nove aplikacije, možno uporabo satelitskih IoT, tudi M2M (Machine-to-Machine) preko sistemov P-P (Point-to-Point) in P-MP (Point-to-Multipoint) v pasovih za fiksne in mobilne zveze, IoT znotraj javnih ali zasebnih celičnih omrežij, tehnološko nevtralno uporabo, različne možnosti licenciranja (od uporabe brez odločbe o dodelitvi radijskih dovoljenj do javnega razpisa z javno dražbo), odvisno od načina uporabe in frekvenčnega pasu. Pomembno je osvestiti uporabnike, katere možnosti imajo.

III. NOVI REGULATIVNI OKVIR ZA NE-CELIČNI IOT

Glede IoT v pasovih 800 in 900 MHz, v šesti posodobitvi izvedbenega sklepa o napravah kratkega dosega[1], je EC vključila pas 863–868 MHz za naprave za širokopasovni prenos podatkov (LP WAN). Poleg tega je EC sprejela izvedbeni sklep (EU) 2018/1538[2] z dne 11. oktobra 2018 o harmonizaciji radijskega spektra za uporabo naprav kratkega dosega v frekvenčnih pasovih 874–876 MHz in 915–921 MHz, ki omogoča uporabo naprav kratkega dosega v tem pasu (priloga omenja tudi LP WAN). Skladno s tretjim členom se države članice vzdržijo uvajanja novih uporab v podpasovih 874,4–876 MHz in 919,4–921 MHz, dokler se v skladu z Odločbo 676/2002/ES zanju ne sprejmejo harmonizirani pogoji zaradi sistemov mobilnih železniških komunikacij. Ker lahko skladno z drugim členom države članice sprejmejo ustrezne ukrepe v potrebnem obsegu za zaščito obstoječe uporabe v frekvenčnih pasovih 874–876 MHz in 915–921 MHz in kadar ni mogoče najti nobenih alternativnih zaščitnih rešitev, je v frekvenčnem pasu 915–918 MHz uporaba IoT omejena, zaradi zaščite državne uporabe.

Po predlogu *Splošnega akta o spremembah in dopolnitvi splošnega akta o načrtu uporabe radijskih frekvenc* (NURF-4a)[3], ki je v postopku sprejema, se bo tako lahko brez odločbe o dodelitvi radijskih frekvenc uporabljalo: naprave za širokopasovni prenos podatkov LP WAN (npr. LoRa) v pasovih 863–868 MHz in 917,4–919,4 MHz, nespecifične naprave kratkega dosega v pasovih 874–874,4 MHz in 917,3–918,9 MHz ter RFID na frekvencah 916,3 MHz, 917,5 MHz in 918,7 MHz, skladno s parametri v prilogi A2 novega NURF. Priloga A2 določa storitve, za katere velja splošna avtorizacija. IoT so del te priloge.

Za ne-celični in celični IoT v pasovih PMR, licenciran z odločbo o dodelitvi radijskih frekvenc, je ECC marca 2019 sprejel odločbo ECC (19)02 o kopenskih mobilnih sistemih v pasovih 68-87,5 MHz, 146-174 MHz, 406,1-410 MHz, 410-430 MHz, 440-450 MHz, in 450-470 MHz, ki zajema tudi sisteme LTE, LP-WAN (LoRa) v frekvenčnih pasovih 400 MHz.

Na področju spektra za sisteme WAS/RLAN (WiFi in ne-licencirani spekter za 4G/5G) je bil sprejet osnutek poročila ECC 302[4] o kompatibilnosti *brezžičnih dostopovnih sistemov z vključenimi RLAN* (Wireless Access Systems including Radio Local Area Networks) z ostalimi storitvami v pasu 5925-6425 MHz. Kompatibilnost je zagotovljena pod pogoji v poročilu, pas bo lahko na voljo za navedene storitve.

CEPT-ovo poročilo 70, izdelano na podlagi trajnega mandata EC, za 7. posodobitev izvedbenega sklepa o napravah kratkega dosega (SRD, Short Range Devices), predlaga uporabo sistemov 5G in WiGig v pasu 57-66 GHz, z možnostjo razširitve uporabe do 71 GHz, če bo sprejet nov Aneks 3 priporočila 70-03, ki je v javni obravnavi. 7. posodobitev izvedbenega sklepa EC o spremembi sklepa EC (Decision 2006/771/EC) o napravah kratkega dosega bo preko kategorij 75a, 75b in 75c predvidoma omogočila uporabo podatkovnih širokopasovnih komunikacij (npr. 5G in WiGig) v pasu 57-71 GHz.

IV. 5G IN NOVI REGULATIVNI OKVIR ZA VERTIKALE IN LICENČNI SPEKTER ZA IOT

5G je peta generacija mobilne telefonije in predstavlja tehnološki preboj. Ker je omrežna arhitektura razdeljena na več različnih vertikal, ki so lahko različno konfigurirane glede na vrsto uporabe (npr. različna pasovna širina, različne

[1] IZVEDBENI SKLEP KOMISIJE (EU) 2017/1483 z dne 8. avgusta 2017 o spremembi Odločbe 2006/771/ES o harmonizaciji radijskega spektra za uporabo naprav kratkega dosega in o razveljavitvi Odločbe 2006/804/ES, https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32017D1483&from=EN

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.257.01.0057.01.ENG&toc=OJ%3AL%3A2018%3A257%3ATOC

[3] https://www.akos-rs.si/poziv-k-predlozitvi-mnenj-k-predlogu-splosnega-akta-o-spremembah-in-dopolnitvi-splosnega-akta-o-nacrtu-uporabe-radijskih-frekvenc-(nurf-4a)

[4] https://cept.org/files/9522/Draft%20ECC%20Report%20302rev..docx

prenosne hitrosti, različna kvaliteta storitev, različne zakasnitve, ipd.), omogoča tehnologija 5G hkratno delovanje različnih storitev, kot so storitve v realnem času, množični prenos podatkov, ultra hiter širokopasovni internet in prenos avdiovizualnih vsebin, podporne storitve in kritične storitve, primerne za varnost in zaščito. 5G gre pretežno v smeri izboljšane podpore komunikaciji stroj-stroj (M2M), poznani tudi pod imenom Internet stvari.

Vse omenjeno naj bi močno pospešilo razvoj »pametnih« tehnologij, aplikacij in storitev. Razvoj gre v smeri čim cenejših napravic z vgrajenimi karticami SIM in majhno porabo baterije. Takšne napravice bodo gonilo avtomatizacije industrije 4.0, avtomatiziranega prometa, pametnih mest, pametnih vasi, pametnega doma, pametnih zgradb in podobno. Tehnologija 5G naj bi omogočila velik napredek pri implementaciji avtonomnih vozil in transporta naslednjih generacij. V zdravstvu bo razvoj omogočil operacije na daljavo, v šolstvu učenje z uporabo navidezne ali obogatene resničnosti. Tudi obstoječi uporabniki spektra – t.i. vertikale, bodo prešle na tehnologijo 5G, tako kritične storitve za javno varnost, zaščito in reševanje, kot tudi poslovno kritične storitve: energetika, vodovod, kanalizacija, plin, letališča, pristanišča, postaje, banke in podobno.

Osnova za nastanek *Akcijskega načrta za 5G v Evropi* je zapisana v dokumentu COM (2016)588. [1] Skladno z Akcijskim načrtom za 5G mora vsaka članica Evropske unije (EU) do konca leta 2020 s tehnologijo 5G opremiti vsaj eno večje mesto, do leta 2025 pa morajo imeti vsa večja mesta in transportne poti nemoteno pokrivanje z omrežjem 5G. Članice EU so že začele uresničevati priporočila prvega[5] in drugega mnenja[6] *Odbora za politiko radijskega spektra* (RSPG) o prioritetnih pasovih za omrežja 5G in ustrezno spremenile svoje alokacijske tabele, nekatere pa so tudi že izvedle javne razpise z javnimi dražbami.

Tretje mnenje RSPG [2] pa poleg priporočil o de-fragmentaciji pasov v frekvenčnem območju 3400–3800 MHz, govori tudi o pomenu vertikal in njihovega prehoda na tehnologijo 5G. 5G bo ob obstoječih tehnologijah igral pomembno vlogo pri zagotavljanju komunikacijskih storitev za specifične potrebe vertikal. Komunikacije za vertikale bodo lahko ponujali mobilni operaterji preko svojih omrežij, ostali ponudniki (nišni operaterji, MVNOji) ali pa vertikale same preko svojih omrežij v harmoniziranih pasovih EU za mobilne tehnologije ali pa v namenskem spektru. Kot namenski spekter za kritične vertikale predlaga RSPG spekter izven harmoniziranih pasov EU za elektronske komunikacijske storitve in sicer ekskluzivno ali pa v souporabi z ostalimi storitvami. Kot namenski spekter za vertikale se lahko uporabi spekter, kjer je oprema dostopna drugje po svetu (nižja cena zaradi ekonomije obsega), vendar je to opremo potrebno uporabljati v skladu s harmoniziranimi tehničnimi pogoji, ki veljajo znotraj EU. Govori tudi o namenskem harmoniziranem spektru za pan-evropske vertikale, npr. v transportu, kjer svetuje tehnološko nevtralno uporabo. Upravičenost za tak spekter se oceni od primera do primera. Mnenje omenja torej štiri vrste vertikal:

- 1) preko mobilnih operaterjev,
- 2A) preko namenskih omrežij – regionalno,
- 2B) preko namenskih omrežij lokalno in
- 3) pan-evropske vertikale.

A. *Vertikale oziroma IoT preko mobilnih omrežij*

Glede vertikal preko mobilnih operaterjev tretje mnenje ugotavlja, da bo povpraševanje po njih v veliki meri odvisno od mobilnih operaterjev samih (obstoječih ali novih vstopnikov, vključno z MVNO-ji). Torej, če bodo znali preko omrežnih rezin 5G, poleg ponudbe za obstoječe zasebne in poslovne uporabnike, ponuditi poslovno zanimive rešitve za vertikale z zahtevano kvaliteto storitve (KPIs). To je scenarij, ki ga priporoča RSPG, saj lahko tehnologija 5G z rezinami zadovolji potrebe današnjih uporabnikov omrežij PPDR, FRMC in aplikacij IoT. Za ta namen je predviden harmoniziran spekter. Poleg prioritetnih pasov 700 MHz, 3.4-3.8 GHz in 26 GHz, bosta v prvi fazi na voljo tudi pasova 800 MHz in 1.5 GHz, ki bosta ključna za 5G in vertikale preko mobilnih omrežij. V drugi fazi bo na voljo spekter 900/1800 MHz, 2,1 GHz in 2,6 GHz. Predmet poslovne odločitve operaterjev in omejitve v ODRF v nekaterih članicah je tudi uporaba 5G v ostalih pasovih za javne mobilne storitve, kjer je na voljo ustrezna oprema.

CEPT je že sprejel Poročilo ECC 266[7] o primernosti regulative ECC za uporabo širokopasovnih in ozkopasovnih storitev M2M v pasovih 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2,1 GHz in 2,6 GHz. Evropska komisija naj bi letos sprejela tehnično regulativo za uvedbo tehnologije 5G v več frekvenčnih pasovih (700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 3400-3800 MHz in 26 GHz). V ostalih frekvenčnih pasovih (npr. 2300 MHz) se bo tehnologija 5G lahko uporabljala pod pogoji v veljavni regulativi ECC. Agencija se že pripravlja na javne razpise za podelitev frekvenc za mobilna omrežja 5G, ki čakajo na sprejem *Strategije upravljanja z radiofrekvenčnim spektrom*.

Tretje mnenje RSPG podaja razloge, kdaj mobilni operaterji za vertikale ne morejo zagotoviti ustreznih pogojev za vertikale in zanje predlaga namenski spekter:

- če gre za poslovno specifične aplikacije, ki zahtevajo nenehen razvoj, ki jim operater ne more slediti;
- če aplikacija zahteva pokrivanje v zahtevnih območjih;
- nekatere vertikale zahtevajo preveč specifične in predrage KPI-je za svoje storitve;
- operater nima poslovnega modela za pokrivanje s storitvami 5G;
- nekatere vertikale želijo obdržati popoln nadzor nad svojim omrežjem zaradi varnosti, …

B. *Vertikale oziroma IoT preko namenskih omrežij*

Tretje mnenje RSPG o tehnologiji 5G opisuje značilnosti vertikal preko namenskih omrežij za regionalno pokrivanje, ki potrebujejo namenski spekter za širše področje:

- imajo lastno omrežje ali imajo navidezno omrežje preko operaterja (ki nudi posebne zahteve – kvaliteto storitev);
- lahko izrazijo skupne zahteve (ultra zanesljivost, množični IoT,..);

[5] http://rspg-spectrum.eu/wp-content/uploads/2013/05/RPSG16-032-Opinion_5G.pdf

[6] https://circabc.europa.eu/sd/a/fe1a3338-b751-43e3-9ed8-a5632f051d1f/RSPG18-005final-2nd_opinion_on_5G.pdf

[7] https://www.ecodocdb.dk/download/61d8e0fa-8bcf/ECCRep266.pdf

- gre za poslovno kritične vertikale (energetika, vodovod, plin, kanalizacija, transport, …);
- države jim namenijo del harmoniziranega spektra (npr. Francija 2,6 GHz TDD, Nizozemska, Nemčija del pasu v 3,5 GHz TDD,…)
- individualna avtorizacija s tehničnimi pogoji za 5G;
- način podeljevanja je z javnim razpisom. V primeru, da je dovolj spektra, lahko tudi brez javnega razpisa, na zahtevo.

EC je v izvedbenem sklepu komisije (EU) 2016/687 z dne 28. aprila 2016 o harmonizaciji frekvenčnega pasu 694–790 MHz za prizemne sisteme, ki lahko v Uniji zagotavljajo brezžične širokopasovne elektronske komunikacijske storitve in za prožno nacionalno uporabo v Uniji[8] dala pravno podlago za možno uporabo namenskega spektra 2 x 3 MHz v frekvenčnem pasu 700 MHz za radijske komunikacije stroj–stroj (M2M). Poleg tega je dala pravno podlago tudi za uporabo namenskega spektra 2 x 5 MHz v frekvenčnem pasu 700 MHz za sistem javne varnosti ter zaščite in reševanja (PPDR), kar pomeni radijske aplikacije, ki jih nacionalni organi ali zadevni operaterji uporabljajo za javno varnost in varovanje ter obrambne namene, da se odzovejo na zadevne nacionalne potrebe v zvezi z javno varnostjo in varovanjem tudi v izrednih razmerah.

CEPT je za primer uporabe frekvenčnih pasov 2 x 3 MHz v spektru za M2M izdelal smernice v ECC-jevem poročilu 242[9] in harmoniziral možno uporabo sistemov PPDR v pasovih 400 MHz in 700 MHz v ECC-jevi odločbi(16)02[10].

Razpis z javno dražbo za podelitev radijskih frekvenc za namenska omrežja za zagotavljanje storitev M2M za kritično infrastrukturo v radiofrekvenčnem pasu 700 MHz (733–736 MHz / 788–791 MHz) je že pripravljen in čaka na sprejem *Strategije upravljanja z radiofrekvenčnim spektrom*[11]. Radijske komunikacije stroj–stroj (M2M) za namen tega razpisa pomenijo radijske povezave za posredovanje informacij med fizičnimi ali virtualnimi enotami, ki tvorijo kompleksen ekosistem, vključno z internetom stvari. Take radijske povezave se ustvarijo z elektronskimi komunikacijskimi storitvami na podlagi mobilne tehnologije z uporabo licenciranega spektra. Namensko omrežje za namen tega javnega razpisa pomeni zaprto omrežje, ki ponuja elektronske komunikacijske storitve oziroma M2M in ne deli virov ali ponuja storitev končnim uporabnikom. Zgradi ga lahko operater zasebnega ali javnega omrežja.

Za ostale vertikale osnutek *Strategije upravljanja z radiofrekvenčnim spektrom* predvideva del spektra v frekvenčnih pasovih 2,3 GHz in 3,5 GHz.

Tretje mnenje RSPG - za lokalna namenska omrežja (npr. industrijske komplekse, tovarne (roboti, vozila), posebne lokalne storitve tudi na več lokacijah (npr. avtobusne postaje), množične komunikacije v omejenem območju (npr. letališča, pristanišča) - predvideva uporabo spektra v frekvenčnem pasu npr. 26 GHz. Za uporabo v notranjosti zgradb lahko članice namenijo neharmoniziran spekter v EU, za katerega obstaja oprema drugje po svetu, a le v primeru, da ne moti harmoniziranih storitev v teh pasovih.

Agencija spremlja testiranja v ostalih članicah.

C. *Pan-evropske vertikale s harmoniziranim namenskim spektrom*

Za pan-Evropske vertikale, ki za namenska omrežja potrebujejo harmonizirani namenski spekter na nivoju EU, tretje mnenje RSPG predlaga namenski spekter za cestne inteligentne transportne sisteme (ITS) ter za mestni železniški promet (metroje in primestne vlake) v frekvenčnem pasu 5,9 GHz. Lahko gre za ne-licenciran ali licenciran spekter, odvisno od okoliščin in tehničnih pogojev. Predlaga tudi dodatni spekter za železniške aplikacije FRMCS. CEPT na podlagi mandata Evropske komisije proučuje pasove 874,4-880 MHz / 919,4-925 MHz in 1900-1920 MHz. Dodatno proučuje tudi možnost uporabe dela spektra v pasu 2290-2400 MHz.

Za cestni ITS obstajata dve tehnologiji (G5 in LTE/5G). Na podlagi mandata Evropske komisije je ECC sprejela Poročilo CEPT 71[12]. Poročilo predlaga tehnološko nevtralnost glede cestnega ITS. Za delitev spektra med cestnim in železniškim ITS, poročilo predlaga uporabo frekvenčnega pasu 5895-5915 MHz prioritetno za cestni ITS, uporabo pasu 5915–5935 MHz pa prioritetno za mestno železnico. V pasu 5915-5925 MHz je dovoljen cestni ITS le za povezave vozila proti infrastrukturi (V2I, Vehicle-to-Infrastructure). Za povezavo vozilo–vozilo pa samo, če se zagotovi, da ne bo motena cestna železnica. Evropska komisija bo izvedbeni sklep o ITS izdala predvidoma marca 2020, ko bo ETSI končal delo glede združljivosti/sobivanja tehnologij za cestni ITS.

V. SKLEP

Spekter za internet stvari (IoT) delimo na spekter za ne-celične sisteme IoT ter celične sisteme.

Na področju ne-celičnih sistemov IoT predlog *Splošnega akta o spremembah in dopolnitvi splošnega akta o načrtu uporabe radijskih frekvenc* (NURF-4a)[13] v prilogi A2 prinaša pogoje uporabe za IoT brez odločbe o dodelitvi radijskih frekvenc in sicer za naprave za širokopasovni prenos podatkov LP-WAN (npr. sistem LoRa) v pasovih 863–868 MHz in 917,4–919,4 MHz, nespecifične naprave kratkega dosega v pasovih 874–874,4 MHz in 917,3–918,9 MHz ter RFID na frekvencah 916,3 MHz, 917,5 MHz in 918,7 MHz.

Za ne-celični in celični IoT v pasovih PMR, licenciran z odločbo o dodelitvi radijskih frekvenc, odločba ECC (19)02 določa pogoje za uporabo sistemov LP-WAN (LoRa) v frekvenčnih pasovih 400 MHz.

Na področju spektra za *brezžične dostopovne sisteme vključno z RLAN* (WAS/RLAN), ki se uporablja brez odločbe o dodelitvi radijskih frekvenc, osnutek Poročila ECC 302 prinaša tehnične pogoje za koeksistenco teh sistemov z ostalimi storitvami v pasu 5925-6425 MHz, sedma posodobitev izvedbenega sklepa EC o napravah kratkega dosega (SRD) pa bo predvidoma omogočila uporabo podatkovnih širokopasovnih komunikacij (npr. 5G in WiGig) v pasu 57-71 GHz brez odločb o dodelitvi radijskih frekvenc.

[8] https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32016D0687&from=EN
[9] https://www.ecodocdb.dk/download/2a5c1708-a1a2/ECCREP242.DOCX
[10] https://www.ecodocdb.dk/download/1cadc836-23e4/ECCDEC1602.docx
[11] https://www.akos-rs.si/radijski-spekter-novice-2018-strategija-upravljanja-z-radiofrekvencnim-spektrom
[12] https://www.ecodocdb.dk/download/19a361a9-d547/CEPTRep071.pdf
[13] https://www.akos-rs.si/poziv-k-predlozitvi-mnenj-k-predlogu-splosnega-akta-o-spremembah-in-dopolnitvi-splosnega-akta-o-nacrtu-uporabe-radijskih-frekvenc-(nurf-4a)

Za celični IoT je CEPT že sprejel Poročilo ECC 266 o primernosti regulative ECC za uporabo širokopasovnih in ozkopasovnih storitev M2M v pasovih 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2,1 GHz in 2,6 GHz.

Evropska komisija naj bi letos sprejela tehnično regulativo za uvedbo tehnologije 5G v več frekvenčnih pasovih (700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 3400-3800 MHz in 26 GHz). V ostalih frekvenčnih pasovih (npr. 2300 MHz) se bo tehnologija 5G lahko uporabljala pod pogoji, zapisanimi v veljavni regulativi ECC. Agencija se že pripravlja na javne razpise za podelitev frekvenc za mobilna omrežja 5G, ki čakajo na sprejem *Strategije upravljanja z radiofrekvenčnim spektrom*.

Tretje mnenje RSPG o uporabi tehnologije 5G opisuje značilnosti vertikal preko namenskih omrežij za regionalno pokrivanje, ki potrebujejo namenski spekter za širše področje. Te vertikale imajo lastno omrežje ali imajo navidezno omrežje preko operaterja (ki nudi posebne zahteve – kvaliteto storitev). Agencija na pobudo deležnikov proučuje možnost implementacije te rešitve preko omrežij 4G, ter kasnejše rešitve za 5G.

EC je v izvedbenem sklepu komisije (EU) 2016/687 o pasu 694–790 MHz dala pravno podlago za možno uporabo namenskega spektra 2 x 3 MHz v frekvenčnem pasu 700 MHz za komunikacije stroj-stroj (M2M) in 2 x 5 MHz v frekvenčnem pasu 700 MHz za storitve PPDR. CEPT je za primer uporabe 2 x 3 MHz spektra za M2M izdelal smernice v ECC-jevem poročilu 242. Javni razpis z javno dražbo za podelitev radijskih frekvenc za namenska omrežja za zagotavljanje komunikacij M2M za kritično infrastrukturo v radiofrekvenčnem pasu 700 MHz (733–736 MHz / 788–791 MHz) je že pripravljen in čaka na sprejem *Strategije upravljanja z radiofrekvenčnim spektrom*.

Za ostale vertikale osnutek *Strategije upravljanja z radiofrekvenčnim spektrom* predvideva del spektra v pasovih 2,3 GHz in 3,5 GHz.

Pan-evropske vertikale – do predvidoma marca 2020, ko bo ETSI končal delo, bo Evropska komisija glede združljivosti/sobivanja tehnologij za cestni ITS sprejela izvedbeni sklep o uporabi ITS v frekvenčnem pasu 5,9 GHz. Za železniške aplikacije pa CEPT na podlagi mandata Evropske komisije študira pasove 874,4-880 MHz / 919,4-925 MHz in 1900-1920 MHz ter proučuje tudi možnost uporabe dela spektra v pasu 2290-2400 MHz.

LITERATURA

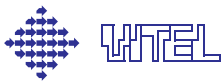
[1] RSPG: „RSPG Opinion on the Spectrum Aspects of the Internet-of-things (IoT) including M2M,“ 07 02 2017. [Elektronski]. Available: https://circabc.europa.eu/sd/a/a0faa1a5-ca41-42c3-83d5-561b197419b0/RSPG17-006-Final_IoT_Opinion.pdf.

[2] Comission, European: „COM(2016) 588 final: 5G for Europe: An Action Plan {SWD(2016) 306 final},“ EC, Bruselj, https://ec.europa.eu/digital-single-market/en/towards-5g, 2016.

[3] RSPG: „RSPG Opinion on 5G implementation challenges (RSPG 3rd opinion on 5G),“ 30 01 2019. [Elektronski]. Available: http://rspg-spectrum.eu/wp-content/uploads/2013/05/RSPG19-007final-3rd_opinion_on_5G.pdf.

Janja Varšek je diplomirala leta 1989 na Fakulteti za elektrotehniko Univerze v Ljubljani in magistrirala leta 2016 na Fakulteti za organizacijske vede Univerze v Mariboru. Od leta 1992 je zaposlena na AKOS (Agenciji za komunikacijska omrežja in storitve RS), ki se je takrat imenovala Uprava RS za telekomunikacije), in sicer na področju telekomunikacijske opreme, elektromagnetne kompatibilnosti in regulacije trgov. Delala je tudi kot nadzornik trgov in inšpektor za telekomunikacije. Leta 2014 je vodila večfrekvenčno javno dražbo in po uspešni izvedbi postala vodja Sektorja za upravljanje z radiofrekvenčnim spektrom. Je članica RSPG in ECC..

Meta Pavšek Taškov je diplomirala leta 1990 in magistrirala leta 1993 na Fakulteti za elektrotehniko. Od leta 1989 je bila zaposlena v Iskri Hipot – Šentjernej, v mešanem razvojno raziskovalnem oddelku Inštituta Jožef Stefan in Iskre Hipot na Inštitutu Jožef Stefan v Ljubljani. Od leta 1995 je zaposlena na AKOS (Agenciji za komunikacijska omrežja in storitve RS), ki se je takrat imenovala Uprava RS za telekomunikacije, in sicer na področju za radiokomunikacije oz. upravljanje radiofrekvenčnega spektra. Leta 2012 in 2013 je bila vodja LTE projekta, 2014 pa namestnica predsednice razpisne komisije za javni razpis z javno dražbo za mobilne tehnologije v pasovih 800/900/1800/2100/2600 MHz. Novembra 2015 se je udeležila svetovne radijske konference WRC-15 kot namestnica vodje delegacije. Od 2016 je vodja oddelka za mobilne zveze na AKOS. Vodi priprave na 700 MHz dražbo in ostale dražbe ter podpira projekte v okviru Slovenske 5G pobude. Vodi dve mednarodni skupini: CEPT/ECC/SE21 od leta 2013 in HCM – TWG od 2010. Je aktivna članica RSCom, ECC PT1, WGSE in HCM.



Internet vsega – zlato industrijskih vertikal

Gorazd Kovačič, Ana Robnik, Rene Benassi, Peter Metljak, Grega Prešeren, Iskratel, d.o.o, Kranj

Povzetek — Digitalnega preoblikovanja je bil najprej deležen sektor IKT, ki pa je za tem s svojimi naprednimi tehnologijami, med njimi tudi internetom vsega, pomembno prispeval k digitalnemu preoblikovanju raznovrstnih industrijskih področjih kot so energetika, javna varnost in transport. V tem članku želimo izpostaviti širši namen in globlji pomen inteligentnega zbiranja in obdelave raznovrstnih podatkov, ki jih generirajo ali za sebe hranijo posamezni deležniki, za nadaljnje razumevanje celotne vrednostne verige in iskanje dodane vrednosti skozi zanimive primere uporabe. Nekateri najbolj reprezentativni primeri uporabe so tudi detajlneje opisani.

Ključne besede — IoT/IoE, vrednostna veriga, podatkovna analitika, velepodatki, pametna omrežja in transport, digitalno preoblikovanje.

Abstract — The ICT sector has been at the forefront of digital transformation and through this, with its advanced technologies, including the Internet of Everything, has made a significant contribution to the digital transformation of diversified industrial domains such as energy, public security and transportation. In this article, we want to highlight the broader purpose and the deeper significance of intelligent collection and processing of diverse data generated or stored by individual stakeholders, for further understanding of the entire value chain and the search for added value for different interesting use cases. Some of the most representative use cases are also described in more details.

Keywords — IoT/IoE, value chain, data analytics, big data, smart grids and transport, digital transformation.

I. DIGITALNO PREOBLIKOVANJE V INDUSTRIJI

Vsem je znano, da so informacijsko-komunikacijske tehnologije v prejšnjem stoletju oblikovale informacijsko družbo in v tem stoletju s tehnološko revolucijo posegle v industrijske sektorje in narekujejo digitalno preoblikovanje podjetij, državnih ustanov ter imajo vpliv na vsa področja človeškega življenja.

Digitalnega preoblikovanja je bil najprej deležen sam sektor IKT, kjer je ta tema aktualna že več kot dve desetletji. V zadnji dekadi je v ospredje stopil koncept Industrija 4.0, ki v svojem jedru tudi in predvsem temelji na digitalizaciji. Pri konceptu Industrija 4.0 je pametna tehnologija ali zbirka medsebojno prepletenih tehnologij postavljena v ospredje proizvodnje in/ali verig poslovnih in operativnih procesov. Rezultat tega so učinkoviti procesi, avtomatizacija in novonastali proizvodi po meri posameznika. Vse te dimenzije omogočajo zmanjševanje operativnih stroškov, nadomeščanje rutinskih ali izjemno natančnih del s stroji, podpirajo široko paleto možnosti izvedb po meri in nudijo pomoč pri sprejemanju izjemno zahtevnih odločitev.

Pa vendar se prava dodana vrednost in pomen teh dimenzij pokaže, ko ponovno vključimo človeško kreativnost in inovativnost v proces sodelovanja in sožitja med ljudmi ter pametnimi sistemi in napravami. Tako preidemo v koncept Družba 5.0, ki bo nasledil informacijsko družbo in vključil napredne koncepte Industrije 4.0. Slednje pomeni v praksi kakovostni preskok, ne le v uporabi tehnologij, ampak tudi v načinu razmišljanja in v kulturi organizacij, ki vse te koncepte uporabljajo.

Ne moremo tudi mimo dejstva, da so v Evropski uniji v zadnjih petih letih na pomenu pridobili gospodarski interesi in vzpostavitev enotnega digitalnega trga.

II. TEMELJNI GRADNIKI PLATFORME INTERNETA VSEGA

Temeljni tehnološki gradniki Industrije 4.0 so: centralna in razpršena oblačna infrastruktura in programje (ang. Cloud infrastructure, Fog computing), internet stvari in internet vsega (ang. Internet of Things – IoT, Internet of Everything – IoE) ter velepodatki (ang. Big Data), podatkovna analitika s strojnim učenjem (ang. machine learning), pametna omrežja in omrežja 5G (ang. Smart Networks, 5G Networks). Po senzorskih in kapilarnih omrežjih raznolikih rešitev na področjih industrijskih vertikal in javnega sektorja se pretakajo zlata zrna, ki se zbirajo v digitalnih platformah na robu ali na centralnem mestu. Ta zlata zrna so podatki, ki so zgodovinsko gledano pridobivali na vrednosti in pomenu. V prejšnjem stoletju so bili zbrani podatki obravnavani le kot stranski proizvod, kmalu nato pa so ob drugačni obravnavi ti podatki omogočili optimizacije procesov in nastanek novih inovativnih proizvodov. Dandanašnji pa so ti podatki že sami po sebi proizvod, torej so postali naravno bogastvo, ki se trži.

Kje se torej skriva prava vrednost v tako kompleksnem digitalnem okolju? Ali se skriva vrednost v samih podatkih in iz teh podatkov pridobljenih znanjih in vedenjih, ali je vrednost v poslovnih modelih in inovacijskih ekosistemih, ali pa je prava vrednost v simbiotičnem odnosu med človekom ter pametnimi sistemi in napravami? Prava vrednost je po našem mnenju v uravnoteženosti vseh treh dimenzij.

Družba Iskratel se z zanimivim področjem industrijske in družbene digitalizacije ukvarja že zadnjih nekaj let, prvih primerov industrijske digitalizacije pa se je dotaknila na področju energetike. Infrastruktura električnega omrežja, kot je zasnovana danes, glede na trende velike rasti porabe električne energije v prihodnje [1] ne bo prenesla že danes velikih obremenitev, kar bo zagotovo vodilo k številnim izzivom (kakovost prenosa energije, odpovedi omrežja,..). Pametna energetska omrežja (angl. *smart grids*) predstavljajo korak v smeri reševanja nekaterih izzivov za varno, robustno, učinkovito, fleksibilno ter trajnostno dobavo električne energije. Slednje je mogoče doseči edino z integracijo raznovrstnih informacijskih in operativnih sistemov (IT/OT), senzorike (za izboljšanje nadzora), inteligentnih algoritmov za obdelavo zbranih podatkov, vse skupaj v kombinaciji s sodobno komunikacijsko infrastrukturo, ki zanesljivo in varno poveže različne deležnike.

IoT kot koncept predstavlja zelo pomemben tehnološki fenomen, to je zaznavanje vrednostnih verig, npr.: v

energetskem omrežju pametni števec predstavlja člen ali enoto vrednostne verige. V svetu IoT takšna enota vrednostne verige postane oddaljeno naslovljiva. Energetsko omrežje predstavlja enega večjih in bolj kompleksnih strojev, ki ga je človeštvo zgradilo. Zaradi zgoraj omenjenih razlogov se infrastruktura energetskih omrežij danes širom po svetu nadgrajuje s številnimi senzorskimi napravami na različnih nivojih električnega omrežja (transformatorji, preklopniki, podpostaje) ter drugimi sodobnimi sistemi, kar omogoča naprednejše naslavljanje omrežja v celoti.

Ustvarjamo torej celovito platformo in aplikacije s pomočjo naprednih tehnologij, ki bodo uresničile vizijo – digitalno povsod, za vse in v vsakem trenutku. V nadaljevanju navajamo nekatere od aplikativnih primerov uporabe, ki pojasnjujejo dodano vrednost, ki jo te rešitve ponujajo našim kupcem. V ospredju so primeri uporabe na področju elektroenergetskih sistemov, ki pa se uporabljajo tudi na področju železniškega in ostalega prometa. Opišemo tudi varnostne vidike in naš pogled v prihodnost.

III. APLIKATIVNI PRIMERI UPORABE

A. *Integracija v energetiki za prehod v pametna omrežja*

Pomemben omogočevalec interneta stvari je prav integracija raznovrstnih sistemov, ki vsak za sebe zbira dragocene podatke. V sklopu projekta NEDO, ki je dvostranski projekt sodelovanja med slovenskim operaterjem transportnega omrežja ELES s partnerji in japonsko agencijo NEDO, smo za potrebe integracije predhodno nepovezanih sistemov vzpostavili sistem integracije, temelječ na standardih družine CIM (IEC61970, IEC61968 in IEC62325).

Ključni dejavnik za digitalizacijo poslovanja storitvenih podjetij je vpeljava najsodobnejših IT/OT/senzornih sistemov in rešitev, ki pa za svoje delovanje potrebujejo učinkovito izmenjavo že predhodno filtriranih, normaliziranih, oveljavljenih in razporejenih podatkov, ki so servirani vsakemu akterju v skoraj realnem času in z visoko kakovostjo. Starejšim sistemom v distribucijah, ki skrbijo za delovanje, nadzor, meritve, planiranje, vzdrževanje in upravljanje s sredstvi, pa primanjkuje sposobnost komunikacijskih vmesnikov za izmenjavo podatkov.

Zato smo z razvojem integracijske platforme združili tri sisteme:

- geografski informacijski sistem (GIS),
- sistem merilnih podatkov (MDMS),
- distribucijski sistem upravljanja (DMS).

Za potrebe izmenjave podatkov smo identificirali štiri primere uporabe:

- izmenjava modela distribucijskega omrežja (SN, NN) iz GIS in DMS,
- izmenjava statusov stikal iz DMS v GIS,
- izmenjava merilnih podatkov iz MDMS v DMS,
- izmenjava merilnih podatkov med DNO–TSO.

Preko izkušenj, pridobljenih na projektu, smo prišli do sledečih bistvenih rezultatov in zaključkov:

- s čiščenjem, filtriranjem, oveljavljenjem podatkov smo dvignili njihovo kakovost na bistveno višjo raven,
- zmanjšali smo kompleksnost integracijske matrike,
- z vpeljavo skupnega krovnega semantičnega modela smo umestili podatke iz različnih sistemov na skupni imenovalec,
- sisteme smo pripravili za prihodnje posodobitve ali vpeljave novih sistemov,
- naročniku smo omogočili samostojno nadgradnjo sistema zaradi uporabe odprtokodnih komponent.

B. *Z dobrimi napovedmi do optimiziranega upravljanja železniške infrastrukture*

Učinkovita raba energije in napovedi uporabe niso ključnega pomena le v samih elektroenergetskih sistemih in v energetiki nasploh, pač pa so pomembni tudi za porabnike energije v drugih sektorjih.

V nadaljevanju opisani rezultati so plod raziskovalnega dela na evropskem projektu IN2DREAMS [2], ki je projekt širšega programa javno-zasebnega raziskovalno-razvojnega partnerstva Shift2Rail med Evropsko komisijo na eni strani ter industrijo železniškega prometa in raziskovalnimi organizacijami na tem področju na drugi strani.

Za upravljavce železniške infrastrukture ali operaterje železniškega prometa je izjemnega pomena, da imajo na voljo spremljanje rabe energije in stroškov, povezanih z njo, ter sprotni vpogled v obnašanje sistema glede porabe energije in ustrezne prilagoditve. Najpomembnejše pri tem pa je, da imajo učinkovite sisteme za napovedi porabe energije na podlagi pridobljenih informacij in ob uporabi učinkovitih algoritmov za napovedovanje porabe v različnih časovnih obzorjih. Tako trenutne prilagoditve dopolnjujejo s kratkoročnimi ali dolgoročnimi napovedmi, kar je vse bolj pogost primer.

V nadaljevanju bomo predstavili primer uporabe, ki je usmerjen na področje železniškega prometa, tramvajev in drugih podobnih vozil, ki bodisi prevažajo ljudi ali tovor. Pametno merjenje električne energije se izvaja na statičnih elektronapajalnih postajah (polnilnih postajah) ob progah in/ali gibajočih se objektih (neposredno na vlakih, tramvajih, …). Izvajanje korakov “izmeriti” in “analizirati” je z uporabo pametnega merjenja porabe relativno enostavno opravilo in sicer se izvaja v širšem konceptu metode DMAIC, ki vključuje za sistem upravljanja energije naslednji nabor korakov: opredeliti, izmeriti, analizirati, izboljšati in obvladati (ang. Define, Measure, Analyse, Improve, Control). Metoda DMAIC podpira in je povsem v skladu s standardom ISO 50001.

Dani primer uporabe temelji na več nivojskem modeliranju podatkov, ki vključuje tudi izgradnjo celotne infrastrukture za zajem podatkov in analitično obdelavo. Za potrebe modeliranja podatkov in oblikovanja analitične infrastrukture se zbirajo podatki s pomočjo pametnega merjenja iz dveh različnih kategorij virov, iz polnilnih postaj komercialno delujoče železniške proge v običajnih prometnih razmerah in z merilne enote na samih vlakih. V ta namen sta bila izdelana dva napovedna modela porabe energije, in sicer za polnilne postaje in za vlake. Napoved energetske obremenitve vlaka vključuje načrtovanje in razvoj modela za kratkoročno napoved porabe energije vlaka, in sicer za časovni horizont od nekaj sekund do nekaj minut. Pri modeliranju moramo upoštevati povpraševanja po energiji premikajočega se predmeta, vključno z značilnostmi, kot je geolokacija.

Pri napovedih za polnilne postaje ob progi, ki so statične, pa je na voljo napovedovanje povpraševanja po energiji za časovno obdobje od 1 ure do 1 dneva. Primer uporabe zahteva modeliranje energijskega vozlišča (postaje za polnjenje) kot stacionarnega vozlišča v času in ne kot premikajoči se objekt. Podatki iz števcev so dopolnjeni z zunanjimi viri, ki neposredno prispevajo k napovedi porabe. Ti dodatni viri so lahko podatki o vremenu (pretekli, trenutni, napovedani), koledarski podatki (npr. prazniki), topološki podatki ter tudi drugi podatki, ki pomembno vplivajo na kakovost napovedi.

Kaj je dodana vrednost napovedi za porabnika? Porabnik električne energije lahko ukrepa v dveh smereh:

– varčuje z energijo, pri čemer ima natančno vedenje o virih s prekomerno porabo,
– zmanjša stroške električne energije s preklapljanjem porabe na cenejša obdobja, če in ko je to mogoče.

Opisani primer uporabe s svojimi napovedmi je odlično izhodišče in podpora za vrsto aplikacij kot so:

– upravljanje energetskega portfelja,
– učinkovito upravljanje s sredstvi, pri čemer je tudi energija sredstvo,
– optimizacija porabe energije in upravljanje s porabo (DSM),
– odkrivanje odpovedi v sistemu in drugo.

Dane aplikacije vsekakor dajejo širšo uporabno vrednost modela napovedovanja obremenitev omrežja postaj in porabe na samih vlakih, tudi v širšem topološkem smislu za večje področje ali podobne kategorije vlakov in polnilnih postaj.

C. *Veliki industrijski porabniki iščejo zmanjšanje stroškov lastnega obratovanja*

Veliki industrijski uporabniki so soočeni z izzivom napovedovanja optimalne porabe električne energije. Na podlagi približne ocene porabe energije za naslednji dan se izvaja nakup energije po najnižji nabavni ceni v trenutku porabe. Ob napačni presoji porabe energije so uporabniki soočeni z dodatnimi stroški bodisi z nakupom dražje energije v trenutku porabe oz. s kaznimi regulatorja zaradi možne preobremenitve omrežja.

Učinkovito zmanjšanje pogreška z dnevnimi odkupi energije je mogoče doseči z vpeljavo analitičnega modela za napovedovanje porabe. Iskratelov analitičen modul za napovedovanje porabe je zasnovan na obdelavi podatkov senzorjev v realnem in v preteklem času. Podatki senzorjev so dopolnjeni z zunanjimi viri, ki neposredno prispevajo k napovedi porabe. Ti dodatni viri so lahko podatki o vremenu (pretekli, trenutni, napovedani), koledarski podatki (npr. prazniki), topološki podatki ter lahko tudi drugi podatki, ki pomembno vplivajo na kakovost napovedi (npr. informacija o prireditvi na prostem). Z uporabo vseh omenjenih vhodnih podatkov modul napoveduje porabo in proizvodnjo v nizko napetostnem omrežju, porabo večjih potrošnikov el. energije ali pa napove proizvodnjo deležnikov, priključenih v srednji napetosti. Poleg tega so možne tudi napovedi o pretokih moči na višjih ravneh arhitekture drevesne mreže z uporabo izračunov pretoka obremenitve kot dodatnega vhodnega vira.

Vpeljava analitičnega modula sloni na funkcijskem inženiringu (ang. feature engineering), kjer zasnova temelji na primeru uporabe uporabnika, kar je tipično poraba energije. Končni izdelek je zaključena rešitev, prilagojena za stranko, ki temelji na:

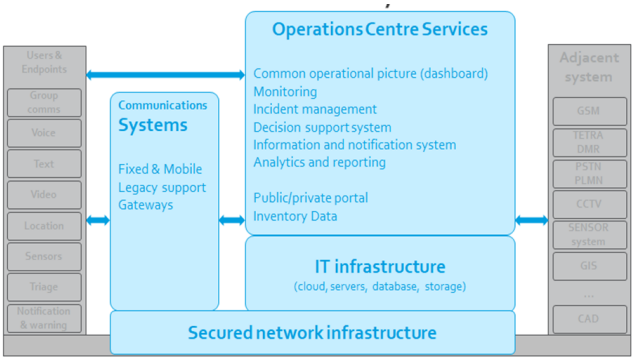
– Podrobnem razumevanju poslovanja. Temeljno je razumevanje in priprava podatkov, kjer poleg razpoložljivih neobdelanih podatkov model vključuje časovne značilnosti in statične podatke z zaznavanjem delovnih dni zaradi dnevnega in tedenskega obdobja.
– Modeliranje in vrednotenje, ki zagotovi najprimernejšo kombinacijo za algoritem modeliranja.
– Uporaba na primerni platformi za pridobitev hitrosti in stabilnosti.

Slika 1: Fuzija raznovrstnih podatkov za potrebe izdelave modela.

D. *Zlivanje in obdelava podatkov za potrebe rešitev javne varnosti*

S koncepti IoT se družba Iskratel srečuje tudi na področju javne varnosti (ang. public safety). Tipično rešitev sistema obravnave klicev v sili na številko 112 v okviru prevzemnih klicnih centrov (PSAP – ang. Public Safety Answering Point), katerega danes ponuja v kar 23 regijah njenega največjega tržišča, razširja na področje ponujanja sistema operativnega centra. Tovrstni sistem tipično povezuje sisteme 112, konvencionalne sisteme javnega obveščanja (npr. sirene) ter vrsto, v večini primerov že prisotnih, samostojnih IT/OT sistemov. Taki sistemi so lahko npr.: sistem detekcije požara, video nadzorni sistemi (CCTV – ang. Closed-circuit television), geoinformacijski sistem (GIS – ang. Geographic Information System) za potrebe topološke umestitve opazovanega področja, sistem nadzora vozil/registrskih tablic, sistemi za podporo pri odločanju (DSS – ang. Decision Support System) ob dogodkih, sistemi nadzora sevanja (npr. ACKPO), detektorji nivoja vode (npr. Seba/Keller), nadzor senzorskih podatkov v stavbnih enotah (npr. Жилье), sistem z vremenskimi napovedmi ipd. Nekateri od teh sistemov (npr. DSS) že vsebujejo tudi lastno prediktivno analitiko in omogočajo na podlagi pridobljenih senzorskih podatkov (npr. nivo vode) zelo dobro napovedati verjetno stanje (npr. obseg področja poplav), kar lahko potem operativni center uporabi v okviru lastne poslovno-procesne logike.

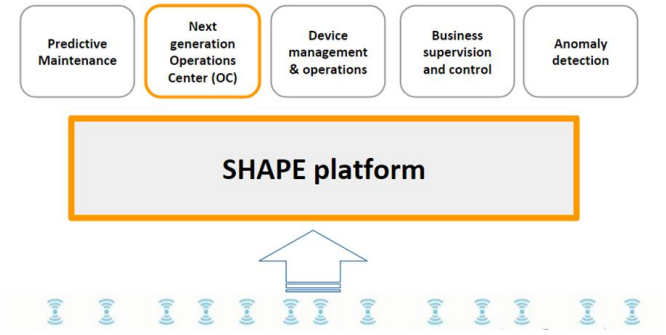
Glavna naloga operativnega centra je tako operaterju ponuditi enovit pogled na stanje opazovanega okolja kot tudi skupno operativno sliko, na osnovi podatkov ter stanj vseh sistemov, priključenih v obravnavo, v določenem delu omogočiti čim bolj avtomatiziran način ukrepanja na dogodke (npr. generiranje poročil ter njihovo posredovanje ključnim akterjem v obravnavo), hkrati pa preko javnih ter zasebnih komunikacijskih medijev (npr. spletnih portalov) omogočiti čim boljše obveščanje, tako širše javnosti kot tudi urgentnih služb (npr. gasilci) v primeru izrednih dogodkov.



Slika 2: Operativni center za celovit in avtomatiziran način obravnave dogodkov na osnovi podatkov z raznovrstnih priključnih naprav.

IV. NA ČEM GRADIMO PRIMERE UPORABE

Inteligentna aplikacijska platforma (SHAPE), na kateri temeljijo omenjeni primeri uporabe, je plod Iskratelovega lastnega razvoja in je zasnovana v večini na odprtokodnih gradnikih. Platforma igra pomembno vlogo v integracijskem delu povezovanja ter agregacije raznovrstnih podatkov iz IT/OT sistemov in senzorike na standardiziran način, na protokolnem delu pri izmenjavi sporočil preko spletnih storitev in sporočilnih posrednikov (npr. SOAP/REST/MQTT), v primerih uporabe s področja energetike dodamo tudi izmenjavo sporočil preko podatkovnega modela CIM. Platforma omogoča hrambo raznovrstnih tipov podatkov (SQL, noSQL, Triplestore), je osnova za varno povezovanje med sistemi ter omogoča dostop in delo uporabnikov z aplikacijami platformami (npr. preko uporabe mTLS, SDP). Vključuje nabor vseh ustreznih programskih komponent za potrebe podatkovne analitike/strojnega učenja, hkrati pa predstavlja tudi enoten način za dostop in delo s podatki na nivoju aplikacij preko aplikacijskega prehoda (API GW) in odprtih podatkovnih vmesnikov (API) – cilj je omogočiti delo s podatki poljubnemu aplikacijskemu ekosistemu na platformi. Platforma želi ponuditi uporabniku, preko vgrajenega IoT ogrodja (ang. IoT Framework), tudi možnost enostavnega dodajanja/upravljanja ter nadzora poljubnega števila senzorskih naprav.



Slika 3: Shematična umestitev platforme SHAPE kot osnove za gradnjo aplikativnega ekosistema.

V. VARNOSTNI VIDIKI

Internet vsega v industriji skoraj vedno povezuje do pred kratkim nepovezani omrežji, to sta poslovno omrežje (omrežje informacijskih tehnologij) in operativno omrežje (omrežje operativnih tehnologij). Danes se informacijske tehnologije (strežniki na x86 arhitekturi, operacijski sistemi Linux in Windows, ter protokolni sklad TCP/IP) že uporabljajo za upravljanje operativnih procesov. Mnogo operativnih aplikacijskih protokolov je s standardom prilagojenih za delovanje na protokolnem skladu TCP/IP. Le to omogoča relativno enostavno povezavo med poslovnim in operativnim omrežjem, kar pa nadalje omogoča izdelavo novodobnih aplikacij, ki jih opisujemo v predhodnih poglavjih. Poleg opisanih koristi pa povezovanje poslovnega in operativnega omrežja neizbežno vnaša v celoten sistem nova varnostna tveganja, ki jih moramo znati upravljati, da še naprej zagotavljamo nemoteno delovanje operativnih procesov. Toleranca do morebitnih izpadov v operativnem omrežju je veliko nižja kot v poslovnem omrežju. V teoriji varnosti to opisujemo z varnostnimi zahtevami (ang. Security requirements), ki so v operativnem omrežju bolj stroge kot v poslovnem omrežju.

Ko povežemo dve omrežji z različnima nivojema varnostnih zahtev, moramo upoštevati vse do zdaj uveljavljene dobre prakse, poleg seveda uveljavljenih standardov, tako za informacijske kot za operativne tehnologije (npr. IEC 62443). Najboljša analogija med dvema omrežjema z različnimi varnostnimi zahtevami je prehod iz Interneta v poslovno omrežje. Nekateri ključni ukrepi, ki jih tipično izvedemo za poslovne storitve, ki jih naredimo dostopne iz Interneta:

- vzpostavitev varne DMZ cone, kjer so locirani strežniki in storitve;
- varovanje z dodatnimi varnostnimi napravami, kot je požarna pregrada (ang. Firewall), aplikacijska požarna pregrada (ang. WAF), sistem za zaznavo in zaščito pred vdori (ang. IDP, IPS), ipd.;
- nameščanje kritičnih varnostnih popravkov;
- upravljanje aplikacijske varnosti (spletne aplikacije, spletne storitve, ipd.);
- enake ali bolj zaostrene ukrepe moramo sprejeti na prehodu med poslovnim in operativnim omrežjem. Rešitve *Interneta vsega* v industriji poleg tega zahtevajo še dodatne varnostne ukrepe, ki niso značilni za večino drugih digitaliziranih sistemov, npr.:
  - fizična varnost stvari (ang. things) in kraja,
  - varnost stvari pred vdorom v programsko opremo preko fizičnega dostopa do stvari,
  - nezmožnost nameščanja varnostnih popravkov na stvari,
  - nezmožnost upravljanja nastavitev stvari.

Nazadnje lahko ugotovimo da je Internet vsega skupek mnogih tehnologij; vgrajeni sistemi (ang. embedded systems), različna komunikacijska omrežja, oblačne arhitekture (ang. cloud), različne aplikacijske rešitve, ipd. Načelu, da so bolj kompleksni sistemi v splošnem manj varni, se ne moremo izogniti. Zato je za ustrezno ščitenje *Interneta vsega* potrebnega veliko znanja in truda. To pa je v nasprotju z načeli tehnologij v vzponu, kjer se na trgu najprej pojavijo "nedodelani" izdelki, saj je čas vstopa na trg (ang. time to market) zelo pomemben.

VI. POGLED V PRIHODNOST

V prihodnosti vidimo veliko izzivov na področju digitalnega preoblikovanja industrij, države in družbe, predvsem skozi raznovrstne primere uporabe na industrijskem področju. Želja je, da v okviru inteligentne aplikacijske platforme ponudimo celovit spekter inteligentnega aplikacijskega ekosistema, ki bi kupcu prinašal kar največ gospodarskih koristi (ang. *economic benefits*). Slednje vidimo na primer v aplikacijah tipa PdM (ang. Predictive maintenance), kjer na primer na področju transporta že vidimo prve primere uporabe, nameravamo pa jih predstaviti v bližnji prihodnosti. Eden izmed zelo svetlih dolgoročnih ciljev je tudi, da področje rešitev javne varnosti ter energetike tehnološko nadgradimo v smeri, da bo kot združena predstavljala osnovo za prihajajoče projekte pametnih mest (ang. Smart cities). Slednja predstavljajo korak naprej pri naprednem, inteligentnem upravljanju ter sprotni izmenjavi informacij med vsemi deležniki urbanega okolja, a je tukaj potrebno vpeljati še nekaj standardov (podatkovni modeli za izmenjavo podatkov) ter urediti tudi pravno-formalne vidike izmenjave podatkov med trenutno nepovezanimi pravnimi subjekti.

ZAHVALE

Projekt IN2DREAMS (INtelligent solutions 2ward the Development of Railway Energy and Asset Management Systems in Europe) je prejel sredstva iz programa Evropske Unije za raziskave in inovacije Obzorje 2020 na podlagi pogodbe številka 777596.

Na tem mestu bi se želeli zahvaliti tudi vsem avtorjem tega članka.

LITERATURA

[1] International Energy Agency , https://www.iea.org/weo2018/
[2] PROJEKT IN2DREAMS, http://www.in2dreams.eu/
[3] Iskratel interna dokumentacija.
[4] Projekt NEDO, https://www.eles.si/projekt-nedo

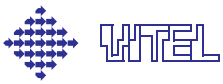
Rene Benassi je diplomiral iz elektrotehnike na Univerzi v Ljubljani. Dosedanje delovne izkušnje ima večinoma s sistemi SCADA in integracijo podatkov po meri v elektro-distribucijah. Trenutno se ukvarja s "prevajanjem" raznih sistemov (za varno mesto, energetiko, transport...) na skupni "jezik". Oboževalec odprtokodnih sistemov z več kot devetimi leti vpogleda v delovanje storitvenih podjetij, tem sedaj poskuša olajšati življenje.

Ana Robnik je svetovalka za telekomunikacije, koordinira delo v standardizacijskih organizacijah in vodi »Raziskovalno skupino ISKRATEL« na ARRS. Svojo poklicno pot je po univerzitetnem študiju uporabne matematike na Fakulteti za matematiko, fiziko in mehaniko Univerze v Ljubljani in opravljenem magisteriju iz računalništva na Fakulteti za računalništvo Univerze v Ljubljani nadaljevala v razvojno raziskovalni enoti Iskra Kibernetika, nato pa v IT-oddelku Iskratela. Ima več kot 20 let izkušenj na področju telekomunikacij in vodenja. Vodila je razvoj sistemov za upravljanje in spremljanje omrežnih elementov portfelja Iskratel v sodelovanju z mednarodnimi in domačimi podjetji ter zunanjimi raziskovalnimi skupinami. Koordinira in sodeluje v različnih nacionalnih, evropskih in mednarodnih sofinanciranih projektih. Koordinira vertikalo Varnost v Strateškem razvojno-inovacijskem partnerstvu Pametna mesta in skupnosti v Sloveniji in projekt 5G Varnost.

Gorazd Kovačič je diplomiral in magistriral iz elektrotehnike na Univerzi v Ljubljani v letih 2008 in 2012. Deset let je zaposlen v podjetju Iskratel. Sprva je bil vpet v delo raziskav in razvoja in si je nabiral izkušnje kot sistemski inženir na področju razvoja raznovrstne sistemske programske opreme za potrebe Iskratelovega produktnega portfelja SI 3000. Kasneje je sodeloval pri razvoju Iskratelove oblačne platforme (CSP), predvsem s poznavanjem porazdeljenih podatkovnih sistemov oblačne infrastrukture, zadnje tri leta pa je aktivno vpet v številne aktivnosti Iskratelovega novejšega področja, med drugim tudi vodenje Iskratelovih sektorjev energetike in javne varnosti. Trenutno se ukvarja z vodenjem razvoja rešitve v okviru Iskratelove nove industrijske vertikale, to je inteligentne aplikacijske platforme (SHAPE), v katere zasnovo je bil kot arhitekt rešitve predhodno močno vpet. Povezan je tudi z aktivnostmi pri razvoju rešitve operativnega centra za varna mesta (Safe City Operational Center), ki je umeščena nad platformo SHAPE. Obe predstavljata danes pomemben del Iskratelovega novejšega produktnega portfelja SI 5000.

Peter Metljak je integracijski inženir in koordinator razvojnih rešitev za implementacijo produkta CIM repozitorij v DSO EL LJ. Specializiral se je za uvedbo napredne rešitve shranjevanja modela elektroenergetskega omrežja, ki sledi principom semantičnega spleta. Diplomiral je na Fakulteti za elektrotehniko Univerze v Ljubljani na temo Migracija mobilnih jedrnih elementov v oblak. Ima več kot 20 let izkušenj na področju sistemske administracije in integracije ter vodenja. Vodil je integracijo implementacije obsežne naročniške baze in sistema za upravljanje naročniških profilov v sodelovanju z domačimi in mednarodnimi podjetji. Že vrsto let se ukvarja z integracijo sistemov na različnih IT in TK področjih, prav tako pa je udeležen v razvojno-inovacijskem projektu integracije pametnih mest.

Grega Prešeren se od vsega začetka profesionalne kariere primarno ukvarja z revizijami varnosti informacijskih in industrijskih sistemov, varnostnimi pregledi in vdornimi (penetracijskimi) testi, ter svetovanjem pri obvladovanju tehnoloških ranljivosti. V podjetju Astec je od leta 2010 vodil in izvedel več kot 50 varnostnih pregledov omrežij, IT storitev, spletnih, mobilnih in drugih aplikacij, industrijskih sistemov ipd. Od leta 2015 je bil član varnostne ekipe v podjetju S&T Svetovanje, kjer je opravljal vlogo svetovalca za kibernetsko varnost, od leta 2017 naprej pa je odgovoren za kibernetsko varnost rešitev in produktov v podjetju Iskratel. Je nosilec več strokovnih certifikatov s področja informacijske, industrijske in aplikacijske varnosti (GXPN, GMON, GWAPT, GICSP) in informacijskih omrežij (CCNP, CCNA Security, CCAI). Izvaja tudi izobraževanja s področja aplikacijske varnosti in večkrat letno predava na konferencah s področja kibernetske varnosti.



Varnostna arhitektura 5G za internet stvari

Janez Sterle, Luka Koršič, Internet institut, d.o.o., Ljubljana
Urban Sedlar, Mojca Volk, Univerza v Ljubljani, Fakulteta za elektrotehniko, Ljubljana

Povzetek — V prispevku je podan konceptualen pregled arhitekture in zmogljivosti sistemov 5G s poudarkom na varnostnih rešitvah, ki jih uvaja nova generacija mobilnih tehnologij. Podani so kriptografski mehanizmi ter novosti na področju varnostnih storitev, ki poleg integritete uporabniške ravnine in zaupnosti identitete omogočajo uvedbo novih pristopov pri zagotavljanju medsebojne avtentikacije in zasebnosti uporabnikov mobilnega sistema, kar bo še posebej pomembno pri uvedbi bodočih rešitev za masiven IoT. Podani so varnostni elementi in mehanizmi ter pripadajoče varnostne procedure, ki so podprte tako na radijskem kot hrbteničnem delu sistema 5G. Na osnovi tehnologije 5G bo omogočena podpora delovanju različnim industrijskim vertikalam, od kritičnih komunikacij, pametnih energetskih sistemov, do avtonomne vožnje vozil, ki bo prvič v zgodovini lahko potekala na enotni tehnološki rešitvi 5G.

Ključne besede — 5G, varnost, zaupnost, integriteta, enkripcija, zgoščevalne funkcije, SA, NSA, 5G NR, 4G, LTE, EPC, 3GPP

Abstract — The article provides a conceptual overview of the 5G architecture and capabilities with the emphasis on the new security solutions introduced by the next generation of mobile technologies. Cryptographic mechanisms and innovations in the field of security services are provided, which, in addition to the integrity of the user plane and user identity confidentiality, enables the introduction of new approaches in ensuring mutual authentication and privacy of the users of the mobile system, which will be even more important with the introduction of the massive IoT and machine type communications. Based on the 5G technology, support will be provided for the operation of various industrial verticals, from critical communications, smart energy systems to autonomous driving, which for the first time in history can take place on a single 5G technology platform.

Keywords — 5G, security, confidentiality, integrity, encryption, hash functions, SA, NSA, 5G NR, 4G, LTE, EPC, 3GPP

I. UVOD

Sistem pete generacije (5G) predstavlja najnovejšo različico mobilnih tehnologij, ki bodo v prihodnosti nadomestile obstoječe mobilne sisteme ter omogočile podporo delovanju različnim industrijskim vertikalam, tj. kritičnim komunikacijam, pametnim energetskim sistemom, pametnim mestom, avtonomni vožnji, itd.

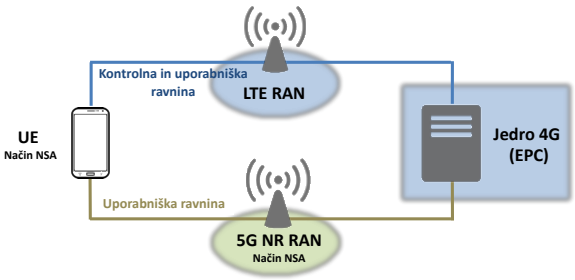
Komunikacija med napravami ter širši koncept interneta stvari v vertikalnih industrijah predstavlja enega izmed ključnih izzivov, ki jih rešuje naslednja generacije mobilnih sistemov z uvedbo mehanizmov za množično komunikacijo med stroji (angl. mMTC – massive Machine Type Communications) in rešitvami za zelo zanesljive komunikacije z nizkimi zakasnitvami (angl. URLLC – Ultra-Reliable Low-Latency Communication).

Ustrezna varnostna arhitektura, ki bo zajela vse ključne vidike delovanja industrijskih vertikal, bo tako igrala ključno vlogo pri uspešni implementaciji novih mobilnih tehnologij v produkcijska okolja. V prispevku predstavljamo varnostno arhitekturo 5G, kriptografske mehanizme ter novosti na področju varnostnih storitev, ki poleg integritete in zaupnosti uvajajo nove pristope pri zagotavljanju medsebojne avtentikacije in zasebnosti uporabnikov sistema.

A. *Arhitektura sistema 5G*

Prva različica specifikacij 5G (Release 15), sprejeta decembra 2017, je zaradi hitrejše uvedbe tehnologije ter možnosti pouporabe elementov in posledično zaščite investicij v obstoječa omrežja četrte generacije (4G) definirala dva osnova pristopa k uvedbi mobilnega sistema naslednje generacije[1]:

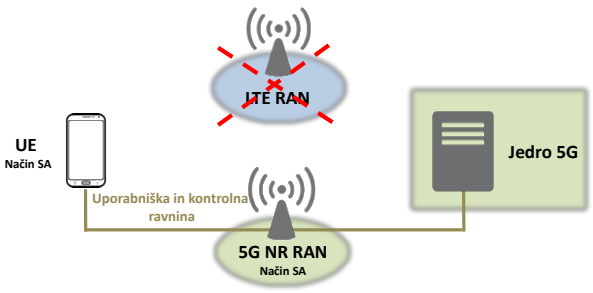
– Postopen način uvedbe baznih postaje 5G (angl. 5G NR – 5G New Radio)[2] prek pouporabe baznih postaje LTE (eNb) ter jedrnih elementov sistema 4G - način, poimenovan NSA (angl. Non-Standalone mode). Bazna postaja LTE in jedro EPC tako zagotavljata vse kontrolne in sistemske funkcije, potrebne za delovanje mobilnega omrežja, medtem ko bazna postaja 5G NR zagotavlja le prenos uporabniškega prometa (Slika 1) in tako razširja obstoječ mehanizem dvojne radijske povezljivosti iz 4G (angl. DC – Dual Connectivity) z novim radijskim vmesnikom 5G NR.
– Samostojen način implementacije sistema 5G (angl. SA – Standalone mode), kjer so bazne postaje 5G (gNb) polno funkcionalne in neposredno povezane v mobilno jedro 5G (Slika 2). Kontrolne in sistemske funkcije se tako izvajajo izključno na tehnologijah 5G.



Slika 1. Delovanje sistema 5G – način NSA

Ker način NSA temelji na pouporabi radijskih in jedrnih sistemskih funkcij 4G, v praksi ne uvaja novosti na varnostnem področju. V nadaljevanju prispevka se bomo zato osredotočili le na delovanje sistema 5G v načinu SA.

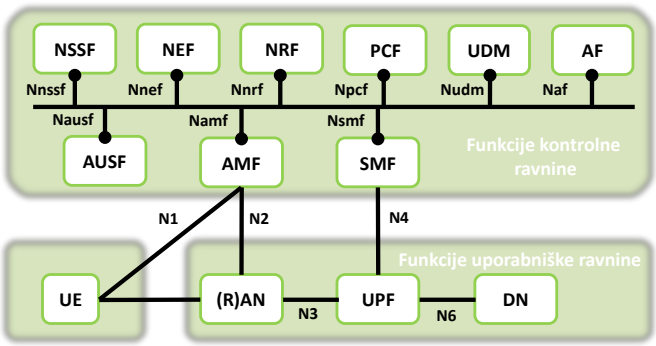
[1] Standard 5G izdaja 15 (december 2017) določa več podopcij postopnega prehoda iz omrežja 4G v omrežje 5G prek tako imenovanih opcij. Specificirane so opcija 3, 4, 5 in 7.
[2] Bazna postaja 5G (angl. 5G NR – 5G New Radio) brez implementirane kontrolne ravnine 5G.



Slika 2. Delovanje sistema 5G – način SA

Tehnologija 5G uvaja popolnoma nov koncept izvedbe, implementacije in operativnega delovanja mobilnih omrežij naslednje generacije (Slika 3). Temelji na "storitveno usmerjeni arhitekturi sistema", ki sledi konceptu strogega ločevanja uporabniških in kontrolnih funkcij.

Elementi krmilne ravnine 5G so opredeljeni kot omrežne funkcije z enim vmesnikom, ki so med seboj povezani na principu "enotnega vodila". Koncept enotnega vodila omogoča neposredno komunikacijo med elementi kontrolne ravnine ter poenostavlja način implementacije sistema na osnovi koncepta navideznih omrežnih funkcij (angl. VNF – Virtual Network Functions).



Slika 3. Storitveno usmerjena arhitektura 5G

Ključni elementi sistema 5G so predstavljeni v tabeli 1. Osnovni koncept delovanja sistema 5G ter posamezni elementi in funkcije so bolj podrobno opisane v dokumentu [1].

Tabela 1. Elementi in funkcije omrežja 5G

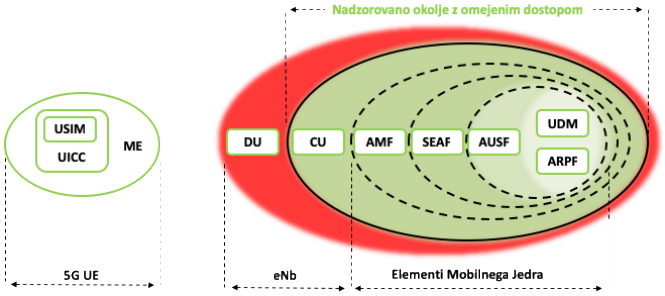
Omrežni elementi sistema 5G	Angleško ime
NSSF: Funkcija za izbiro omrežne rezine	Network Slice Selection Function
NEF: Funkcija za izpostavljanje podprtih fukcionalnosti elementov 5G	Network Exposure Function
NRF: Repozitorij elementov omrežja	NF Repository Function
PCF: Funkcija za kontrolo politik	Policy Control Function
UDM: Centralna baza naročnikov omrežja	Unified Data Management
AF: Aplikacijska funkcija	Application Function
AUSF: Funkcija avtentikacijkega strežnika	Authentication Server Function
AMF: Funkcija upravljanja dostopa in mobilnosti	Access and Mobility Management Function
SMF: Funkcija upravljanja sej	Session Management Function
RAN: Radijsko dostopovno omrežje	(Radio) Access Network
gNb: Bazna postaja 5G	next Generation Node B
UPF: Funkcija uporabniške ravnine	User Plane Function

B. *Varnostni koncepti 5G*

Skladno z novo arhitekturo mobilnega sistema 5G so ustrezno prilagojeni tudi vgrajeni varnostni koncepti, ki jih lahko ločimo na funkcije:

– uporabniškega agenta (angl. UE – User Agent), ki je v domeni uporabnika, ter
– segment radijskega in jedrnega omrežja 5G, za katerega skrbi mobilni operater.

Terminal UE je sestavljen iz dveh varnostnih komponent: varnostnega modula UICC (angl. Universal Integrated Circuit Card), na katerem je varno shranjen USIM (angl. Universal Subscriber Identity Modul), ter mobilne opreme (angl. ME – Mobile Equipment). Skupaj tako tvorita napravo UE (Slika 4).



Slika 4. Varnostni model sistema 5G – domače omrežje

Na strani radijskega in jedrnega omrežja je zaradi podpore različnim implementacijskim opcijam varnostna arhitektura bolj kompleksna in je definirana na konceptu ugnezdenih varnostnih con, katerih elementi so lahko izpostavljeni različnim stopnjam ogroženosti (Slika 4).

Radijsko omrežje sestavljata dva logična modula, distribuirana (angl. DU – Distributed Units) in centralna enota (angl. CU – Central Units), ki skupaj tvorita bazno postajo 5G, imenovano gNb. Enota CU izvaja signalizacijske funkcije ter zagotavlja varnostne storitve (enkripcija in integriteta) signalizaciji in uporabniškemu prometu, zato je praviloma implementirana v nadzorovanem okolju, kjer je dostop do naprav omejen tudi fizično. Naloga enote DU je pa transparentno posredovanje signalizacije in uporabniškega prometa prek radijskega vmesnika 5G do terminala UE, zato so slednje lahko nameščene tudi v oddaljenih in varnostno bolj izpostavljenih okoljih.

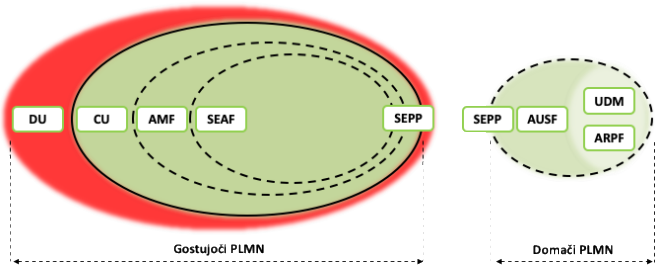
Število varnostnih elementov mobilnega jedra je zaradi zahtevane modularnosti ter razširljivosti jedrnega dela sistema 5G večje. Izvajanje varnostnih procedur je tako porazdeljeno med več komponent sistema:

– Centralizirano funkcijo avtentikacijskega centra (angl. ARPF – Authentication credential Repository and Processing Function), na kateri so permanentno shranjeni dolgoročni varnostni ključi naročnikov (angl. LSK – Long term Secret Key), ki so potrebni za izvajanje primarne avtentikacijske procedure.
– Funkcijo strežnika AUSF, v katero se po uspešni avtentikaciji in prijavi v omrežje shrani korenski varnostni ključ uporabnika[3].

[3] AUSF uporabniku omogoča sočasno prijavo na več različnih dostopovnih sistemov 5G, npr. na radijsko omrežje 5G in omrežje Wi-Fi.

– Funkcijo za upravljanje dostopa in mobilnosti AMF, ki zagotavlja terminacijo varnostnih relacij ter funkcijo varnostnega sidra (angl. SEAF – SEcurity Anchor Function[4]), kjer se hrani varnostni vektor uporabnika UE, ki je dodeljen radijskem omrežju 5G, na katerem se uporabnik trenutno nahaja.

Predstavljena varnostna arhitektura je zastavljena na način, da omogoča ločitev nalog, ki zagotavljajo izvajanje mobilnosti uporabnika (npr. AMF) in funkcij, ki nudijo varnostne storitve sistemu 5G (npr. SEAF).



Slika 5: Varnostni model sistema 5G – gostovanje

V primeru mobilnega gostovanja, kjer je uporabnik prek gostujočega omrežja povezan v domače jedrno in storitveno omrežje 5G, je varnostna arhitektura razširjena z varnostnim proksi prehodom (angl. SEPP – Security Protection Proxy), ki skrbi za kontrolirano in varno izmenjavo signalizacije med gostujočim in domačim mobilnim omrežjem (angl. PLMN – Public Land Mobile Network) in predstavlja novost, ki jo vpeljuje 5G. Prehod SEPP je bil vpeljan predvsem zaradi varnostnih izzivov in incidentov, ki so se pojavili na obstoječih GRX in IPX sistemih, v primeru napadov na signalizacijo SS7 in protokol DIAMETER.

II. VARNOSTNE PROCEDURE 5G

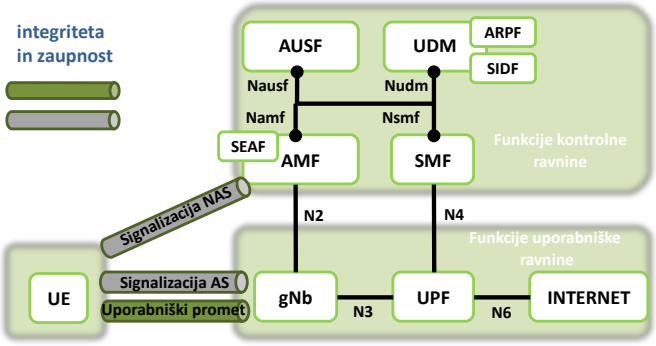
Navkljub temu, da varnostna arhitektura sistema 5G vpeljuje vrsto novosti v primerjavi z obstoječimi mobilnimi tehnologijami, so določene ključne metode in postopki povzeti iz obstoječega standarda 4G. Izhodišča pri zasnovi so bila podpreti vse temeljne varnostne storitve in mehanizme, ki omogočajo:

– zaupnost identitete uporabnika in terminala UE,
– vzajemno avtentikacijo med terminalom UE in sistemom 5G,
– razširjeno avtentikacijo med napravo UE in storitvenimi podsistemi,
– integriteto in zaupnost kontrolne ravnine,
– integriteto in zaupnost uporabniške ravnine.

Zaradi lažje združljivosti z obstoječimi mobilnimi omrežji ter vertikalnimi industrijami sta bili tako vpeljani komplementarni avtentikacijski metodi 5G-AKA ter EAP-AKA, ki bosta omogočili postopen prehod na novo generacijo mobilnih tehnologij ter, v prihodnosti, vpeljavo dodatnih avtentikacijskih metod, kot je npr. EAP-TLS. Prav tako je primarni avtentikacijski proces razširjen s sekundarno avtentikacijo v storitvene podsisteme, ki temelji na procedurah EAP.

[4] V trenutni izdaji specifikacij 3GPP je predvideno, da element AMF zagotavlja tudi naloge funkcije SEAF.

V skladu z idejo neodvisne razširljivosti komponent mobilnega sistema 5G so varnostne relacije med terminalom UE in sistemom 5G razdeljene na dostopovne in jedrne. Dostopovne relacije (angl. AS – Access Stratum) omogočajo varno komunikacijo v radijskem delu omrežja med terminalom UE in bazno postajo gNb, jedrne relacije (angl. NAS – Non-Access Stratum) pa zagotavljajo varno povezovanje terminala UE na ključno kontrolno entiteto sistema 5G, tj. element AMF.



Slika 6. Varnostna arhitektura sistema 5G

Osnovo za ločitev varnostnih relacij predstavlja koncept hierarhije varnostnih ključev, ki omogoča uporabo ločenih delovnih ključev za zaščito signalizacije in uporabniške ravnine, tako na radijskem kot jedrnem delu sistema 5G.

Sistem 5G omogoča uporabo treh različnih enkripcijskih in integritetnih metod. Trenutno so v specifikacijah 3GPP predvideni algoritmi AES, SNOW in ZUC.

A. *Zaupnost identitete uporabnika*

V sistem 5G je bila vpeljana sicer nova globalna identiteta uporabnika, imenovana identifikator naročnika (angl. SUPI – Subscription Identifier), ki pa je v praksi lahko zapisan v formatu obstoječega globalno unikatnega identifikatorja mobilnega naročnika (angl. IMSI – International Mobile Subscriber Identity) oz. identifikatorja EAP. Identifikator SUPI je varno shranjen na modulu USIM ter v sistemu UDM, kot del naročniškega profila. Identifikator SUPI unikatno določa naročnika in se uporabljata v procesu prijave v omrežje in pri drugih sistemskih procedurah.

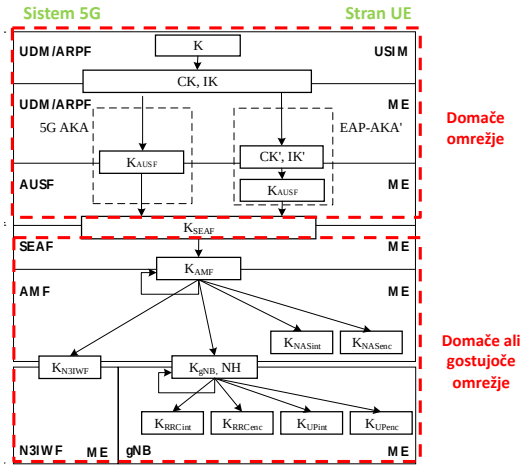
Ena izmed ključnih novosti, ki jo vpeljuje sistem 5G, je zaupnost identitete SUPI, ki se prenaša prek nezaščitenega radijskega kanala, tudi v primeru, ko uporabnik še nima vzpostavljenih varnostnih relacij z domačim omrežjem 5G. Zaupnost se zagotavlja na osnovi asimetrične enkripcije (angl. ECIES – Elliptic Curve Integrated Encryption Scheme) identitete SUPI, ki se izvede na modulu USIM[5] z javnim ključem mobilnega operaterja[6]. Preko nezaščitenega radijskega kanala se tako prenaša le v kriptirani obliki, kot skrita identiteta naročnika (angl. SUCI – Subscription Concealed Identifier), ki se nato na strani sistema 5G, natančneje v elementu SIDF (angl. Subscription Identifier De-concealing Function), dekriptira z zasebnim ključem operaterja. Slednji metoda onemogoča sledenje uporabnika s pomočjo prestrezanja komunikacije na nezaščitenem radijskem kanalu.

[5] Opcijsko se lahko izvede tudi na ME delu enote UE.
[6] Izjemo lahko predstavlja klic v sili (npr.112), kjer se SUPI prenese v nekriptirani obliki.

B. *Proces avtentikacije in hierarhija ključev*

Primarna avtentikacija naročnika poteka na osnovi mehanizma 5G AKA ali EAP-AKA in temelji na principu deljene skrivnosti ključa LSK, ki je shranjena tako na modulu USIM kot v avtentikacijskem centru ARPF. Deljena skrivnost LSK predstavlja primarni varnostni vektor v procesu medsebojne avtentikacije in poteka med terminalom UE in elementom AMF/SEAF, ki izvaja vmesno posredovalno funkcijo za pošiljanje avtentikacijske zahteve prek elementa AUSF do entitete UDM/ARPF.

V primeru uspešne medsebojne avtentikacije se na strani terminala UE in sistema 5G izračunata integritetni ključ (angl. IK – Integrity Key) in enkripcijski ključ (angl. CK – Cypher Key), ki omogočata preko procesa distribucije varnostnih ključev 5G (Slika 7) generiranje končnih delovnih enkripcijskih in integritetnih ključev[7]. Slednji se uporabljajo za zaščito kontrolne in uporabniške ravnine med UE in bazno postajo gNb.



Slika 7. Hierarhija varnostnih ključev v sistemu 5G

Skladno z novo arhitekturo 5G je bil vpeljan tudi nov koncept hierarhije varnostnih ključev. Metoda omogoča razširljiv in varen način generiranja ter distribucije varnostnih vektorjev med elementi sistema 5G, od centralne avtentikacijske funkcije UDM/ARPF do entitet AUSF, SEAF in AMF, in na koncu do posamezne bazne postaje gNb, na kateri je trenutno aktiven UE.

Po končanem postopku generiranja in distribucije varnostnih ključev imajo entitete UE, gNb ter AMF pripadajoče pare varnostnih vektorjev, ki jih uporabljajo za zagotavljanje zaupnosti in integritete v procesu medsebojne komunikacije.

Predstavljen koncept varnosti omogoča preprosto generiranje novih unikatnih varnostnih vektorjev KgNb, ko terminal UE prehaja med posameznimi baznimi postajami gNb, kar še dodatno povečuje stopnjo varnosti sistema 5G. Vdor oz. razkritje varnostnih vektorjev na posamezni bazni postaji gNb tako ne pomeni vdora v celotno domeno 5G.

[7] Integritetni ključ za zaščito signalizacije NAS (K_{NASint}) in AS (K_{ASint}) ter uporabniške ravnine (K_{UPint}), ter enkripcijski ključi za zaščito signalizacije NAS (K_{NASenc}) in AS (K_{ASenc}) ter uporabniške ravnine (K_{UPenc}).

C. *Varnost kontrolne in uporabniške ravnine*

Varnostne storitve sistema 5G lahko delimo na funkcije, ki omogočajo zaščito kontrolne ravnine, ter funkcije za zaščito uporabniške ravnine.

Na nivoju kontrolne ravnine je omogočena zaupnost in integriteta signalizacijskih sporočil, ki se prenašajo med:

– terminalom UE in bazno postajo gNb; slednje predstavljajo varnostne relacije AS (angl. AS – Access Stratum);
– terminalom UE in entiteto AMF; slednje zagotavljajo varnostne relacije NAS (angl. NAS – Non Access Stratum).

Na nivoju podatkovne ravnine je prav tako omogočena storitev zaupnost in integritete uporabniških podatkov, ki se prenašajo med UE in gNb. Integriteta uporabniškega prometa je tako ena izmed varnostnih novosti, ki jih vpeljuje sistem 5G.

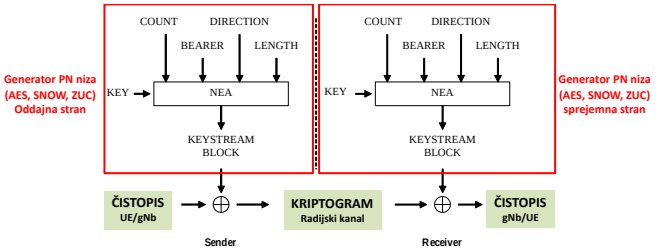
Varnostni algoritmi, ki se uporabljajo za zaščito komunikacije med terminalom UE in elementi sistema 5G, so lahko različni in so odvisni od sistemskih nastavitev posameznega mobilnega operaterja PLMN. Njihova uporaba v praksi bo odvisna od več dejavnikov, varnostne politike operaterja, regulatornih zahtev ter zakonodaje.

Predstavljena varnostna arhitektura 5G tako omogoča popolno ločitev varnostnih relacij med UE, bazno postajo gNb in entiteto AMF. Bazna postaja gNb mora hraniti varnostne kontekste za posamezen terminal UE samo takrat, ko je terminal aktiven, tj. »connected«. Ko preide terminal UE v neaktivno stanje »idle«, pa bazna postaja lahko sprosti vse varnostne relacije, vključno z varnostnimi ključi, ki so povezani s terminalom UE, ter tako razbremeni svoje sistemske vire.

Ko terminal UE ponovno preide v aktivno stanje, se znova vzpostavijo varnostne relacije AS med terminalom UE in bazno postajo na osnovi ključa KgNb, ki ga bazni postaji posreduje entiteta AMF in ga hkrati pozna tudi terminal UE. Navkljub temu, da je sistem distribuiran in optimiziran za razbremenitev sistemskih virov, ki niso nujno potrebni, stopnja varnosti ter odzivnost sistema posledično nista zmanjšana.

D. *Proces zaupnosti*

Zaupnost komunikacije prek radia 5G NR se izvaja na osnovi enkripcije podatkov in signalizacije, ki v 5G poteka v načinu »stream cipher«. Oddajna in sprejemna stran poganjata enega izmed enkripcijskih algoritmov (AES/SNOW/ZUC), na osnovi katerega generirata psevdonaključni niz (PN). Rezultat matematične operacije XOR nad čistopisom in psevdo-naključnim nizom predstavlja kriptogram, ki omogoča zaščito komunikacije pri prenosu signalizacije in uporabniških podatkov prek radijskega prenosnega kanala 5G.

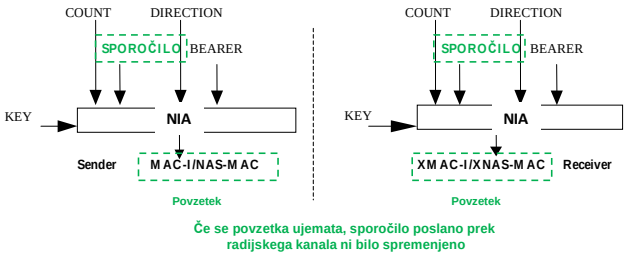


Slika 8. Proces enkripcije na radijskem vmesniku 5G NR

Ker so nizi PN, ki jih generirajo algoritmi AES, SNOW in ZUC, končne dolžine, je potrebna redna menjava vektorjev, iz katerih se izračunavajo. Vektorji se zato na novo generirajo vsaj ob prijavi terminala UE v sistem 5G ter v primeru procesa izročanja, ko terminal UE menja bazno postajo gNb.

E. Proces integritete

Proces izvajanja integritete signalizacijskih sporočil in uporabniškega prometa je zasnovan na klasičnih zgoščevalnih funkcijah, ki vključujejo metodo, temelječo na konceptu uporabe deljene skrivnosti (angl. HMAC – Hash Message Authentication Codes). Integritetni postopki temeljijo na 128-bitnih algoritmih AES, SNOW ter ZUC.



Slika 9. Uporaba zgoščevalnih funkcij v procesu zagotavljanja integritete signalizacije in uporabniških podatkov na radijskem vmesniku 5G NR

Pred prenosom preko radijskega kanala 5G se izvede proces izračuna integritete, ki posredovanim signalizacijskim sporočilom oz. uporabniškim podatkom doda 32-bitni povzetek vsebine, na osnovi katere lahko sprejemna stran preveri integriteto sprejetega sporočila. Če se povzetek, ki je pripet prenešenemu sporočilu (angl. MAC-I/NAS-MAC), ujema s povzetkom, ki ga izračuna sprejemna stran (angl. XMAC-I/XNAS-MAX), sporočilo med prenosom preko radijskega kanala 5G ni bilo spremenjeno. Sprejemno in oddajno stran, ki izvaja integriteto sporočil v sistemu 5G, lahko predstavljata terminal UE in bazna postaja gNb ali pa terminal UE in entiteta AMF.

ZAKLJUČEK

Tehnologija 5G predstavlja neizogiben evolucijski korak k modernizaciji komercialnih mobilnih sistemov, ki vpeljuje vrsto tehnoloških novosti tako na sistemskem kot varnostnem področju. Komunikacija med napravami ter širši koncept interneta stvari v vertikalnih industrijah predstavlja enega izmed ključnih izzivov, ki jih rešuje naslednja generacija mobilnih sistemov. S tehnologijo 5G bo omogočena podpora delovanju različnim industrijskim vertikalam, od kritičnih komunikacij, pametnih energetskih sistemov, do avtonomne vožnje, ki bo prvič v zgodovini lahko potekala na enotni tehnološki rešitvi 5G. Enega izmed ključnih vidikov pri uspešni implementaciji sistema v industrijske vertikale in širše bo nedvomno predstavljala ustrezna varnostna arhitektura, ki bo morala podati odgovore na vsa ključna tehnološka in regulatorna vprašanja.

V prispevku je podan konceptualen pregled arhitekture in zmogljivosti sistemov 5G s poudarkom na varnostnih rešitvah, ki jih uvaja nova generacija mobilnih tehnologij. Podani so kriptografski mehanizmi ter novosti na področju varnostnih storitev, ki poleg integritete in zaupnosti omogočajo uvedbo novih pristopov pri zagotavljanju medsebojne avtentikacije in zasebnosti uporabnikov mobilnega sistema, kar bo še posebej pomembno pri uvedbi bodočih rešitev za masoven IoT. Prav tako so obravnavani varnostni elementi in mehanizmi ter pripadajoče varnostne procedure, ki so podprte tako na radijskem kot hrbteničnem delu sistema 5G.

Navkljub predstavljenim novostim in očitnim prednostim nove tehnologije (t.j. zaupnost identitete uporabnikov, razširjene avtentikacijske metode, integriteta uporabniške ravnine, mehanizem SEPP itd.), ki še dodatno izboljšujejo že sedaj visoko stopnjo varnosti obstoječih mobilnih sistemov, področje odpira številne znanstvene, razvojne in implementacijske izzive ter zastavlja vrsto strateških vprašanj, predvsem z vidika preizkušenosti tehnologije ter regulacije, ki s stališča vertikalnih industrij in vzpostavitve novih poslovnih modelov še ni dorečena. Ti vidiki danes predstavljajo ključna področja nadaljnjih raziskav, ki bodo omogočila, da se tehnološki preboj na področju tehnologij 5G uresniči hitreje, kot lahko sicer pričakujemo.

ZAHVALE

Znanstveno-raziskovalno delo je bilo delno podprto s strani projekta MATILDA, ki ga sofinancira Obzorje 2020 raziskovalni in inovacijski program Evropske Unije št. 761898, projekta 5GINFIRE, ki ga financira Obzorje 2020 raziskovalni in inovacijski program Evropske Unije št. 732497, in projekta 5G Varnost, ki ga financirata Ministrstvo za izobraževanje, znanost in šport ter Evropski sklad za regionalni razvoj.

LITERATURA

[1] System architecture for the 5G System (5GS); 3GPP TS 23.501, april 2019;
[2] Security architecture and procedures for 5G System; 3GPP TS 23.501, marec 2019;
[3] Technical Specification Group Services and System Aspects; 3GPP TS 23.401, december 2018;
[4] System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401, december 2018;
[5] Janez Sterle, 5G is ready for deployment. For real? https://www.linkedin.com/pulse/5g-ready-deployment-real-janez-sterle/;
[6] Janez Sterle, EVOLUCIJA JEDRNIH PAKETNIH SISTEMOV, magistrsko delo, september 2012;
[7] PPDR ONE, 5GINFIRE, H2020 projekt, https://5ginfire.eu/ppdr-one-facility/

Janez Sterle (janez.sterle@iinstitute.eu) je magistriral leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Trenutno je zaposlen v podjetju INTERNET INSTITUT d.o.o. Njegova raziskovalna področja obsegajo omrežne sisteme, rešitve in storitvene koncepte naslednje generacije 5G s poudarkom na varnostnih arhitekturah ter rešitvah QoS in QoE ter njihovo apliciranje na vertikalne industrije.

Luka Koršič (luka.koršič@iinstitute.eu) je magistriral leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Trenutno je zaposlen v podjetju INTERNET INSTITUT d.o.o. Njegova raziskovalna področja obsegajo omrežne sisteme nove generacije ter rešitve za testiranje in verifikacijo omrežnih rešitev.

Mojca Volk (mojca.volk@fe.uni-lj.si) je doktorirala leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Zaposlena je v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Področja njenega dela obsegajo sisteme in storitve za kritične komunikacije ter zaščito in reševanje, rešitve in aplikacije za e-zdravje, ter napredne komunikacijske sisteme in storitve (IoT, FMC, LTE, EPC, 4G in 5G, QoS, QoE).

Urban Sedlar (urban.sedlar@fe.uni-lj.si) je doktoriral leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Zaposlen je v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko, kjer se ukvarja z raziskavami in razvojem na področju internetnih sistemov in storitev, računalništva v oblaku in sistemi za obdelavo velike količine podatkov.

Ohranjanje zasebnosti v Internetu stvari s pomočjo funkcijskega šifriranja

Miha Stopar, XLAB, Ljubljana

Povzetek — Članek opisuje, kako je mogoče s funkcijskim šifriranjem izvajati podatkovne analize, hkrati pa ohranjati zasebnost. Funkcijsko šifriranje se od običajnega šifriranje razlikuje v tem, da omogoča različnim vpletenim dešifriranje različnega dela podatkov. V Internetu stvari to pomeni, da lahko naprave oziroma senzorji šifrirajo podatke, različne enote, ki analizirajo te podatke, pa dobijo posebne funkcijske ključe, s katerimi dešifrirajo zgolj določene lastnosti oziroma funkcije teh podatkov.

Ključne besede — Internet stvari, zasebnost, funkcijsko šifriranje, podatkovna analiza

I. UVOD

Zasebnost je mogoče zagotavljati s šifriranjem podatkov. Vendar pa – ali lahko kljub šifriranju ohranimo vso funkcionalnost programa? Ali lahko v Internetu stvari izvajamo analize, čeprav so podatki, ki jih pošiljajo naprave, šifrirani?

Analiziranje šifriranih podatkov se sliši kot paradoks – običajno šifriranje podatke namreč spremeni v (psevdo) naključen niz znakov. Vsakršen najmanjši vzorec, ki se pojavi v šifriranih podatkih, pomeni varnostno luknjo.

Vendar pa obstajajo kriptografske tehnike, katerih namen je ravno omogočanje vsaj delnega računanja nad šifriranimi podatki. Pri uporabi teh tehnik, ena od njih je funkcijsko šifriranje, se je potrebno zavedati, da je zaradi omogočitve računanja razkrit del podatkov (oziroma nekatere lastnosti podatkov). Več računanja kot omogočimo, več lastnosti o podatkih je razkritih. Ko uporabljamo tovrstne tehnike, je potrebna predhodna analiza, koliko uhajanja informacij je še sprejemljivega za naš primer.

Poleg funkcijskega šifriranja računanje nad podatki omogočajo še naslednje tehnike:

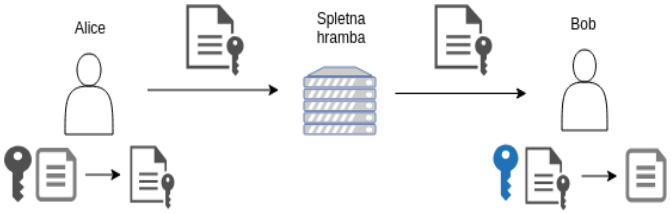
– homomorfno šifriranje,
– dokazi z ničelno informacijo (zero-knowledge proofs),
– sheme za delitev skrivnosti.

Homomorfno šifriranje ponuja izjemne možnosti računanja nad šifriranimi podatki, vendar je računsko izrazito potratno in počasno. V nasprotju s homomorfnimi shemami, funkcijsko šifriranje ponuja sheme, ki so funkcionalno omejene, vendar dovolj hitre za uporabo v konkretnih sistemih. Dokazi z ničelno informacijo omogočajo preverjanje določenih lastnosti šifriranih podatkov, manj so primerni za računanje nad šifriranimi podatki. Sheme za delitev skrivnosti omogočajo razmeroma učinkovito računanje nad podatki, vendar ne premorejo raznolikosti funkcijskega šifriranja, ki denimo omogoča tudi računanje nad šifriranimi podatki, zajetimi iz neodvisnih virov.

Članek se zaradi možnosti praktične uporabe in hitrosti shem osredotoča na funkcijsko šifriranje. V nadaljevanju bomo pokazali, v čem je razlika med običajnim in funkcijskim šifriranjem, kakšne so prednosti funkcijskega šifriranja, predstavili bomo odprtokodne knjižnice za funkcijsko šifriranje ter prikazali primer uporabe v Internetu stvari.

II. OBIČAJNO ŠIFRIRANJE

Poglejmo najprej primer običajnega asimetričnega šifriranja.

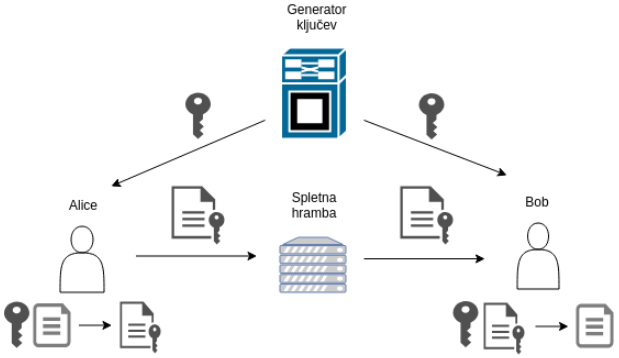


Slika 1: Asimetrično šifriranje in spletna hramba

Denimo, da želi Alice zašifrirati svojo datoteko in jo shraniti pri ponudniku spletne hrambe v oblaku. Pozneje želi Alice svojo datoteko deliti z Bobom, ki je prav tako uporabnik istega ponudnika spletne hrambe. Alice zašifrira datoteko z javnim ključem Boba in jo odloži v spletni hrambi (v izogib več šifriranim kopijam ene datoteke je navadno datoteka šifrirana samo enkrat s ključem, ki pripada samo tej datoteki in je skriven, pri deljenju datotek pa se ta ključ zašifrira z javnim ključem). Bob iz spletne hrambe naloži datoteko in jo dešifrira s svojim skrivnim ključem.

Ali lahko ponudnik spletne hrambe izve karkoli o vsebini datoteke? Čisto ničesar, brez Bobovega skrivnega ključa je zašifrirana datoteka samo niz naključnih znakov.

Poglejmo si primer spletne hrambe, kjer so datoteke šifrirane s simetričnim šifriranjem. V tem primeru je potrebna organizacija oziroma ponudnik storitve generiranja ključev. Generator ključev je enota, ki ji zaupata tako Alice kot Bob. Od nje prejmeta simetrični ključ (isti), s katerim Alice zašifrira datoteko, Bob pa dešifrira.



Slika 2: Simetrično šifriranje in spletna hramba

Ponudnik spletne hrambe tudi v tem primeru datoteko vidi zgolj kot niz naključnih znakov. Potrebno je omeniti, da se tak sistem zanaša na to, da je generator ključev zaupanja vreden. Če generator preda ključe ponudniku spletne hrambe, ima ta dostop do vsebine datotek.

III. FUNKCIJSKO ŠIFRIRANJE

Funkcijsko šifriranje [1][2] je posplošitev šifriranja z javnim ključem. Omogoča nam delegiranje računanja določenih funkcij nad šifriranimi podatki s pomočjo posebnih, funkcijskih ključev. V nasprotju z običajnim šifriranjem z javnim ključem nam omogoča več nadzora nad tem, kaj se lahko dešifrira.

Pri običajnem asimetričnem šifriranju ima uporabnik Bob javni in skriti del ključa. Javni ključ objavi, skriti del skrbno zavaruje in ga ne sme nikdar razkriti. Ko želi Alice zašifrirati datoteko, ki jo bo lahko prebral samo Bob, se izvedejo naslednji koraki:

- Alice zašifrira datoteko *x* z Bobovim javnim ključem: *c = enc(x, Bob_javni_ključ)*
- Bob dešifrira datoteko s svojim skritim ključem: *x = dec(c, Bob_skriti_ključ)*

Pri funkcijskem šifriranju Alice zašifrira datoteko, vendar želi, da Bob dešifrira zgolj del oziroma neko funkcijo te datoteke.

Funkcijsko šifriranje določajo štirje algoritmi, običajno pa je vpleten tudi generator ključev, ki mu zaupata tako Alice kot Bob. Vzemimo poljubno funkcijo *f* (primer funkcije je podan v nadaljevanju članka):

- Generator generira glavni javni in skriti ključ
- Alice zašifrira datoteko *x* z glavnim ključem (v nekaterih shemah je dovolj glavni javni ključ, pri drugih je potreben tudi glavni skriti ključ): *c = enc(x, glavni_ključ)*
- Generator generira ključ *sk_f*, ki omogoča dešifriranje *f(x)*, ter ga izroči Bobu
- Bob dešifrira datoteko *x* oziroma zgolj *f(x): f(x) = dec(c, sk_f)*

IV. ODPRTOKODNE KNJIŽNICE ZA FUNKCIJSKO ŠIFRIRANJE

Podjetje XLAB je v okviru projekta FENTEC [3] razvilo več knjižnic za funkcijsko šifriranje. Gre za prve celovite knjižnice za funkcijsko šifriranje, ki omogočajo izbiro in uporabo različnih shem preko uporabniku prijaznega vmesnika za programiranje (API-ja).

Glavni del sestavljata knjižnici za funkcijsko šifriranje:

- GoFE [4]: knjižnica za funkcijsko šifriranje v jeziku Go
- CiFEr [5]: knjižnica za funkcijsko šifriranje v jeziku C

Obe knjižnici ponujata isti nabor shem in preko podobnega vmesnika:

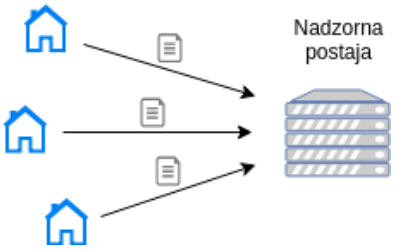
- Simple Functional Encryption Schemes for Inner Products [6]
- Fully Secure Functional Encryption for Inner Products, from Standard Assumptions [7]
- Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings [8]
- Decentralized Multi-Client Functional Encryption for Inner Product [9]
- Reading in the Dark: Classifying Encrypted Digits with Functional Encryption [10]
- Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data [11]
- FAME: Fast Attribute-based Message Encryption [12]

Poleg GoFE-ja in CiFEr-ja je podjetje XLAB pripravilo tudi knjižnico, ki predstavlja, kako je mogoče s funkcijskim šifriranjem in knjižnico TensorFlow [15] izvajati strojno učenje nad šifriranimi podatki, ter knjižnico za Barreto-Naehrig bilinearna parjenja [16], ki omogoča nekatere funkcije (zgoščevalne funkcije v grupi G1 in G2 ter pretvorba teksta v grupo GT in nazaj), ki so potrebne za funkcijsko šifriranje, vendar jih v veliki večini knjižnice za parjenja ne omogočajo.

Več o knjižnicah ter njihovi uporabi je mogoče najti na Githubovih straneh projekta.

V. PREDNOSTI FUNKCIJSKEGA ŠIFRIRANJA

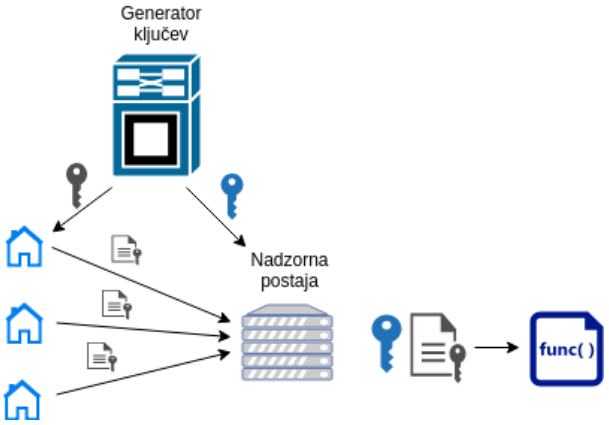
Analiza podatkov prinaša mnoge koristi. V pametnih domovih lahko denimo z analizo temperature, vlage, prisotnosti v prostorih, primerjavo s temperaturo ozračja privarčujemo pri ogrevanju. Podatki se običajno pretakajo v nadzorno postajo, kjer potekajo analize.



Slika 3: Nešifrirani podatki pametnih domov

Ker bi šifriranje podatkov pomenilo, da nadzorna postaja ne more izvajati analiz, kajti podatke vidi kot zgolj niz naključnih znakov, se podatki iz domov proti nadzorni postaji običajno pretakajo nešifrirani. S popolnim razkritjem podatkov pa nadzorni postaji morebiti razkrijemo več, kot bi želeli. Denimo: kdaj smo doma, v katerih prostorih se zadržujemo, kdaj kuhamo (povečana vlažnost).

Ali obstaja srednja pot – ponudniku ne razkrijemo vseh podrobnosti, hkrati pa mu še vedno omogočamo izvajanje analiz? To je mogoče doseči s shemami, ki omogočajo računanje nad šifriranimi podatki. Kot že omenjeno, topogledno najbolj praktične so sheme za funkcijsko šifriranje.



Slika 4: Šifrirani podatki pametnih domov

Tako kot zgornji primer s simetričnim šifriranjem, večina shem za funkcijsko šifriranje potrebuje generator ključev. Generator s šifrirnimi ključi oskrbi pametne domove, ti podatke zašifrirajo ter jih pošljejo nadzorni postaji.

Generator ključev bi v tem primeru lahko bil upravljan s strani pametnih domov, vendar bi vsakdo z dostopom do generatorja lahko dostopal do ključev ter imel tako možnost dešifriranja podatkov vseh domov (še vedno pa bi potreboval dostop do podatkov). Najbolje je torej, da je generator ključev povsem samostojna, zaupanja vredna enota (denimo plačljiva storitev). Lastniki pametnih domov določijo, za katere funkcije lahko generator generira ključe ter jih izdaja nadzorni postaji.

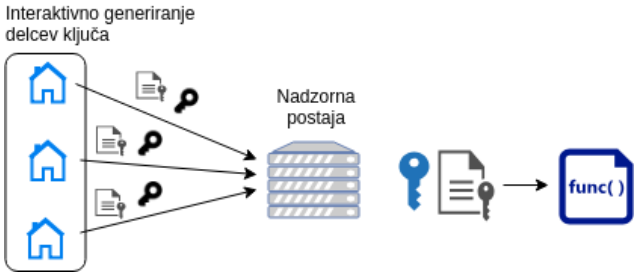
Postaja od generatorja prejme poseben funkcijski ključ – enega za vsako funkcijo, ki jo postaja želi izračunati. Nadzorna postaja lahko tedaj uporabi funkcijski ključ in izračuna vrednost funkcije. Primer funkcije bi lahko denimo bil:

*f(vlažnost, temperatura, zaprta_luč) = vlažnost * 0.3 + temperatura * 0.2 + zaprta_luč * 10*

Postaja bi s funkcijskim ključem za to funkcijo izračunala vrednost, hkrati pa ne bi poznala podatkov o vlažnosti, temperaturi in luči. V primeru, ko bi vrednost presegla neko mejo, bi postaja lahko avtomatsko sprožila akcijo, denimo odpiranje okna:

f(vlažnost, temperatura, zaprta_luč) > 200 => odpri okno

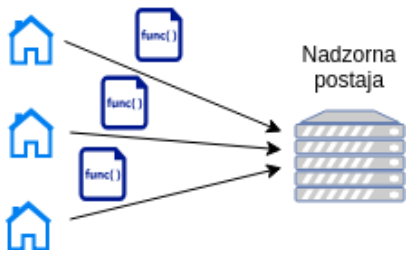
Shema [9], ki je vključena v knjižnici GoFE in CiFEr, omogoča decentralizirano generiranje ključa, kjer generator ključev ni potreben. Pametni domovi se med seboj povežejo in generirajo vsak svoj del ključa, ki ga pošljejo nadzorni postaji. Podatke lahko dešifrira samo tisti, ki pozna vse dele ključa.



Slika 5: Decentralizirano generiranje ključev

VI. KDAJ JE FUNKCIJSKO ŠIFRIRANJE EDINA MOŽNOST

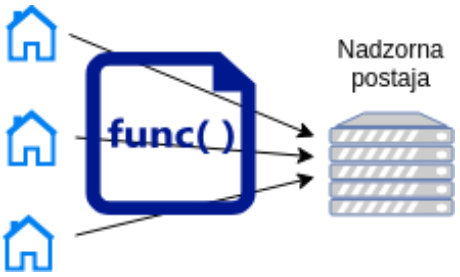
Pa je funkcijsko šifriranje res potrebno za zgoraj omenjeni primer pametnih domov? V primerih, ko se računa funkcija za vsak dom posebej, ni.



Slika 6: Lokalno računanje funkcij podatkov

Vrednost funkcij namreč v tem primeru lahko izračuna vsak dom posebej ter pošlje vrednost nadzorni postaji. Tako ima nadzorna postaja dostop do natanko istih podatkov kot v zgornjem primeru s funkcijskim šifriranjem, hkrati pa ni potreben generator ključev in potrebne je manj računske moči (na strani nadzorne postaje). Vendar pa – če bi nadzorna postaja pozneje želela poznati vrednost kake druge funkcije nad istimi podatki, bi morali domovi znova lokalno izračunati vrednosti ter jih poslati postaji. Z uporabo funkcijskega šifriranja to ni potrebno, zgolj generator mora pripraviti nov ključ, ki ga postaja uporabi za izračun nove funkcije.

Hkrati pa rešitev z lokalnim računanjem vrednosti funkcij ni mogoča v primerih, ko se računa funkcija, ki kot vhodne parametre prejme podatke več domov. V takih primerih bi morali namreč domovi drug drugemu razkriti podatke, česar lastniki najverjetneje ne želijo.



Slika 7: Računanje funkcij nad podatki več domov hkrati

Funkcije nad podatki več domov omogočajo denimo računanje, ob katerih urah je poraba elektrike preko vseh domov največja ali najmanjša. Shemi, ki to omogočata in sta del knjižnic GoFE in CiFEr, sta [8] in [9].

Računanje nad podatki, ki prihajajo od različnih enot, je morebiti še veliko bolj uporabno v primerih velikih mrež naprav, denimo za merjenje kakovosti vode ali zraka.

VII. FUNKCIJSKO ŠIFRIRANJE IN STROJNO UČENJE

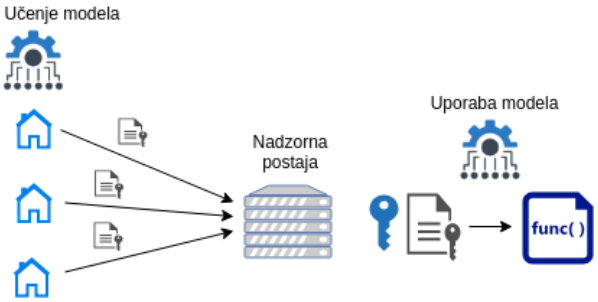
Internet stvari pomeni povezovanje naprav in izmenjavo podatkov. Uporaba umetne inteligence nad podatki, ki prihajajo iz najrazličnejših naprav, odpira skoraj neomejene možnosti. Denimo v zdravstvu umetna inteligenca na mnogih področjih (analiza rentgenskih posnetkov) v nekaterih pogledih prekaša človekovo presojo. Uporaba samonadzornih naprav, denimo za merjenje glukoze v krvi pri sladkorni bolezni, lahko omogoča tudi povezavo z zdravnikom ter analizo in primerjavo podatkov z drugimi pacienti. S pomočjo umetne inteligence oziroma strojnega učenja se lahko podatki natančno razvrščajo in pacient prejme zanesljiva nadaljnja navodila. Vendar pa se v takih primerih odpirajo številna vprašanja s področja varnosti in zasebnosti. Kako omogočiti dostop do podatkov samo avtoriziranim osebam? Kako preprečiti zlorabo podatkov? Kako omejiti dostop do podatkov?

V prejšnjih poglavjih smo pokazali, da funkcijsko šifriranje lahko reši nekatere teh težav. Podatki so šifrirani, torej brez ključa neuporabni. Ključe lahko dodelimo samo avtoriziranim osebam. Ključi omogočajo samo delen uvid v podatke. Pa funkcijsko šifriranje omogoča tudi strojno učenje nad šifriranimi podatki?

Shema [10] omogoča uporabo dvoslojne nevronske mreže nad šifriranimi podatki, kar omogoča učinkovite algoritme strojnega učenja. Na Githubovem računu projekta FENTEC

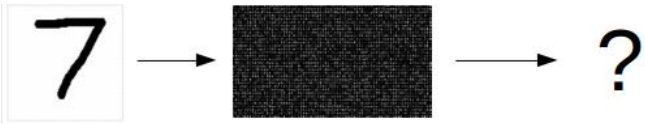
[13] je podan primer algoritma za razvrščanje šifriranih slik. Gre za nabor slik ročno napisanih števk MNIST [14].

Učenje modela poteka na nešifriranih slikah, nato je izdan funkcijski ključ, ki dešifrira zgolj to, katera števka je na šifrirani sliki.



Slika 8: Strojno učenje nad šifriranimi podatki

Imetnik funkcijskega ključa ne more do nobenih drugih podatkov o sliki – denimo do lastnosti pisave, kot sta velikost ali nagib števke.



Slika 9: Razpoznavanje števk v šifriranih slikah

Uporaba tovrstnih shem omogoča varno analizo podatkov, saj so ti šifrirani in zgolj delno dostopni samo tistemu, ki ima funkcijski ključ.

VIII. ZAKLJUČEK

Članek predstavlja funkcijsko šifriranje ter prve celovite in odprtokodne knjižnice za tovrstne kriptografske sheme. Knjižnice je v okviru projekta FENTEC razvilo podjetje XLAB. Predstavljene so nekatere možnosti uporabe funkcijskega šifriranja v Internetu stvari ter sheme, ki to omogočajo in so del odprtokodnih knjižnic iz projekta FENTEC. Funkcijsko šifriranje lahko ponudi rešitve za vedno bolj pereča varnostna in zasebnostna vprašanja, ki se porajajo v Internetu stvari ob povezovanju naprav v velike mreže, ki si med seboj izmenjujejo občutljive podatke.

LITERATURA

[1] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, TCC 2011: 8th Theory of Cryptography Conference, volume 6597 of Lecture Notes in Computer Science, pages 253–273, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany.

[2] Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010.

[3] http://fentec.eu/

[4] https://github.com/fentec-project/gofe

[5] https://github.com/fentec-project/CiFEr

[6] Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional en- cryption schemes for inner products. In Jonathan Katz, editor, Public-Key Cryptography - PKC 2015, volume 9020 of Lecture Notes in Computer Science, pages 733–751. Springer, 2015.

[7] Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Matthew Robshaw and Jonathan Katz, editors, Advances in Cryptology - CRYPTO 2016, volume 9816 of Lecture Notes in Computer Science, pages 333–362. Springer, 2016.

[8] Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu. Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings. In Hovav Shacham and Alexandra Boldyreva, editors, Advances in Cryptology - CRYPTO 2018, volume 10991 of Lecture Notes in Computer Science, pages 597–627. Springer, 2018.

[9] Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. Decentralized multi-client functional encryption for inner product. Cryptology ePrint Archive, Report 2017/989, 2017. http://eprint.iacr.org/2017/989.

[10] Sans, Edouard Dufour, Romain Gay, and David Pointcheval. "Reading in the Dark: Classifying Encrypted Digits with Functional Encryption." IACR Cryptology ePrint Archive 2018 (2018): 206.

[11] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine- grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. Acm, 2006.

[12] Shashank Agrawal and Melissa Chase. FAME: fast attribute-based message encryption. IACR Cryptology ePrint Archive, 2017:807, 2017.

[13] https://github.com/fentec-project/fe-ml-example

[14] https://en.wikipedia.org/wiki/MNIST_database

[15] https://www.tensorflow.org/

[16] https://github.com/fentec-project/bn256

Miha Stopar je razvijalec kriptografskih knjižnic v podjetju XLAB.

Uporaba tehnologij IoT v elektroenergetiki

Andrej Souvent, Elektroinštitut Milan Vidmar, Ljubljana
Uroš Salobir, ELES, d.o.o., Ljubljana

Povzetek — V članku sta predstavljena dva primera uporabe IoT tehnologij v elektroenergetiki – uporaba IoT protokola MQTT pri integraciji kompleksnega demonstracijskega okolja v okviru projekta FutureFlow in zasnova koncepta za izmenjavo podatkov z razpršenimi viri električne energije, kar zahtevajo nova Navodila za priključevanje in obratovanje proizvodnih naprav, priključenih v distribucijsko elektroenergetsko omrežje.

Ključne besede — FutureFlow, IoT, MQTT, integracija, izmenjava podatkov, elektroenergetski sistem

Abstract — The paper present two examples of the use of IoT technologies in electric power system, where the integration of the complex demonstration environment within the FutureFlow project and where the concept of the data exchange with distributed generation of electricity, as required by the new Rules for connection and operation of distributed generation connected to the distribution grid, are based on the IoT MQTT protocol and related technology.

Keywords — FutureFlow, IoT, MQTT, integration, data exchange, electric power system

I. UVOD

Projekt FutureFlow [1], ki se financira iz programa Obzorje 2020, se ukvarja z razvojem naprednih e-rešitev za izravnavo in upravljanje pretokov v evropskem elektroenergetskem omrežju s poudarkom na čezmejni izrabi sekundarne regulacije in vključevanjem agregiranih razpršenih virov in odjema v to storitev. V okviru projekta so bile razvite in implementirane: (1) regionalna IT platforma, ki omogoča čezmejno izrabo sekundarne regulacije, (2) kompleksno demonstracijsko okolje, ter (3) platforma za agregiranje razpršenih proizvodnih virov ter odjema za nudenje storitev izravnave elektroenergetskega sistema (Slika 1).

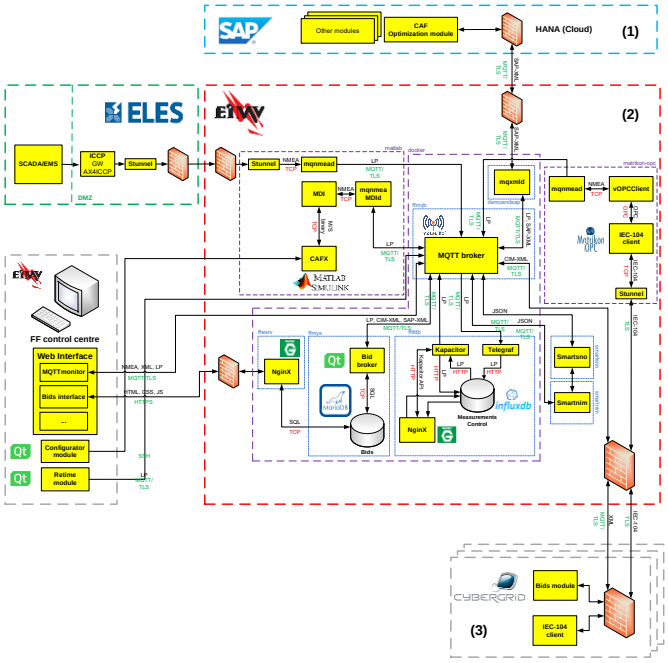
Tako za integracijo demonstracijskega okolja s platformami, kot za notranjo integracijo med številnimi moduli, je bil uporabljen IoT MQTT protokol, ki nudi učinkovit in zanesljiv transport podatkov, hkrati pa je agnostičen glede na vsebino, kar s pridom izkoristimo za prenos tovora sporočil skladno z izbrano semantiko.

Pozitivne izkušnje z MQTT iz projekta FutureFlow so bile temelj za zasnovo sistema za izmenjavo podatkov z razpršenimi viri.

II. DEMONSTRACIJSKO OKOLJE FUTUREFLOW

A. *Funkcija demonstracijskega okolja*

Demonstracijsko okolje je namenjeno izvedbi pilotnih testov, s katerimi se preverjajo rešitve razvite v okviru projekta FutureFlow. Okolje je razvil, implementiral in tekom testov upravljal EIMV. V realnem času omogoča simulacijo štirih sodelujočih prenosnih operaterjev (Eles – Slovenija, APG – Avstrija, MAVIR – Madžarska in TRANSELECTRICA – Romunija) oziroma njihovih sekundarnih regulatorjev ter odzivov enot v njihovih kontrolnih conah (državah), ter ustrezno krmili agregirane razpršene vire in odjem, ki preko agregacijskih platform v štirih državah sodelujejo v sistemski storitvi sekundarne regulacije oziroma skladno z novim poimenovanjem storitvi »avtomatske rezerve za povrnitev frekvence« (ang. *Automatic Frequency Restoration Reserve)*. Pri tem je treba poudariti, da gre za krmiljenje realnih virov in sicer v obsegu 40 MW [2]. Simulacija prenosnih operaterjev – sicer z njihovimi realnimi historičnimi podatki – je bila nujna, saj bi sicer morali posegati v enega izmed najbolj kritičnih procesov uravnavanja frekvence v elektroenergetskem sistemu, kar pa bi predstavljalo preveliko tveganje.



Slika 1 Integracija komponent FutureFlow demonstracijskega okolja

Ključne komponente demonstracijskega okolja so:

- Matlab/Simulink, ki je integriran z viri podatkov in deluje v realnem času. Ključna naloga je simuliranje sekundarnih regulatorjev in odzivov enot sodelujočih prenosnih operaterjev, zmore pa tudi izvajati optimizacijo izbora enot, kadar se ta funkcija ne opravlja v oblačni regionalni platformi;
- InfluxDB podatkovna baza, ki poleg tega, da shranjuje vse rezultate, vsebuje še realne historične podatke prenosnih operaterjev, ki se v proces plasirajo tako, kot da bi se vse dogajalo v realnem času;
- Grafana, ki omogoča vizualizacijo signalov oziroma vseh procesnih veličin;

– Mosquitto MQTT posrednik in pripadajoče aplikacije za integracijo.

B. Integracija

Slika 1 prikazuje komponente demonstracijskega okolja, ki so integrirane predvsem prek izmenjave sporočil z MQTT protokolom. Osnovna komponenta, ki se uporablja za prenos podatkov preko protokola MQTT, je posrednik (ang. *broker*) Mosquitto. MQTT odjemalci se naročijo na teme (ang. *topics*) na posredniku MQTT in prejemajo sporočila, ki jih objavijo drugi odjemalci na teh temah. Vse komponente programske opreme uporabljajo večnitnost (angl. *multithreading*), kar zagotavlja, da so povezave z drugimi programskimi komponentami neodvisne in da lahko pošiljajo in sprejemajo podatke bodisi sinhrono ali asinhrono.

MQTT se je uporabil tudi za izmenjavo podatkov z zunanjimi partnerji, konkretno z regionalno (*cloud*) platformo, ki jo je razvil SAP in agregacijsko platformo za razpršene vire, ki jo je razvilo podjetje CyberGrid.

MQTT je IoT protokol, ki je definiran s standardom ISO/IEC 20922:2016. Omogoča prenos sporočil po principu objavi/naroči (*publish/subscribe*). Odjemalci se povežejo z MQTT posrednikom, slednji se lahko povežejo tudi z drugimi posredniki. V posredniku so definirane teme (topics), ki služijo ločevanju podatkovnih tokov.

MQTT je glede na vsebino agnostičen protokol, zato lahko sporočila definiramo tako, kot nam ustreza. Se je pa smiselno čim bolj držati standardov in zato smo vsebino sporočil v primeru izmenjave z zunanjimi partnerji definirali skladno s CIM semantiko [3], kot jo določajo družine standardov IEC 61968, 61970 in 62325. Podatki se skladno s semantičnim modelom in pripadajočimi profili oziroma shemami prenašajo v XML obliki. Poleg CIM-XML smo v določenih primerih znotraj platforme uporabili še JSON in InfluxDB Line protokol.

C. Kibernetska varnost

Za varovanje povezav je uporabljen kriptografski protokol TLS (*Transport Layer Security*). Tako strežnik kot odjemalci imajo PKI certifikate overitelja digitalnih potrdil, poleg tega se uporablja tudi avtentikacija / avtorizacija z uporabniškim imenom in geslom.

Ker so gesla navadno del konfiguracije MQTT odjemalca, jih generiramo z zadostno dolžino in entropijo. Vsak odjemalec mora imeti lastno uporabniško ime in vsak uporabnik ima lahko največ eno MQTT sejo. MQTT *ClientID* mora biti prepisan z uporabniškim imenom odjemalca, tako da enemu odjemalcu ni mogoče vplivati na sejo drugih odjemalcev (z različnimi uporabniškimi imeni). Dostop do vsebin MQTT je filtriran, tako da se lahko vsak odjemalec naroči in objavi le pod dovoljenimi temami.

V okviru projekta je podjetje Trusted labs izvedlo obširno penetracijsko testiranje demonstracijskega okolja, ki pa ni zaznalo nobenih varnostnih tveganj [4].

III. KONCEPT IZMENJAVE PODATKOV Z RAZPRŠENIMI VIRI

Na osnovi zelo pozitivnih izkušenj z MQTT protokolom iz projekta FutureFlow, tako iz vidika izvedbe, kot tudi uporabe, zanesljivosti delovanja in zadostne stopnje kibernetske varnosti, smo koncept izmenjave podatkov z razpršenimi viri energije zasnovali prav na tem protokolu. Poleg tega je MQTT še enostaven in zelo učinkovit protokol, ki ga je enostavno izvesti ter deluje tudi na skromni strojni opremi, kar je tudi pogoj za cenovno ugodne rešitve.

Nova *Navodila za priključevanje in obratovanje proizvodnih naprav priključenih v distribucijsko elektroenergetsko omrežje* [5] prinašajo tudi IKT zahteve, po katerih bo glede na razred vsake nove priključene naprave zahtevan daljinski izklop (razred A), ali daljinsko vodenje in izmenjava obratovalnih podatkov (razredi B, C, D) z operaterjem omrežja. Če vzamemo v obzir, da se razred A začne že z viri moči 0,8 kW, razred B z 10 kW, itn., vidimo, da je treba računati v prihodnje na veliko količino naprav pri končnih uporabnikih, ki bodo zahtevale ustrezno povezljivost. Pri vpeljavi IKT rešitev za povezovanje velikega števila razpršenih virov s centralno lokacijo operaterja omrežja je potrebno predvideti možnost izrabe čim širšega spektra IKT medijev in omrežij (mobilnih, fiksnih, javnih, privatnih) pri tem pa zagotoviti ustrezno raven informacijske varnosti, parametrov komunikacijskih storitev, kot tudi cenovno čim ugodnejše rešitve, saj delež stroškov IKT opreme ne sme predstavljati znatnega deleža pri sami investiciji v proizvodno napravo [6].

Predlagana rešitev temelji na MQTT/TLS s pripadajočo IT infrastrukturo.

A. Zahteve glede komunikacij z razpršenimi viri

Razpršeni vir (RV) mora omogočati izmenjavo informacij (obratovalne meritve, komande,…) v realnem času s sistemom zadevnega sistemskega operaterja distribucijskega omrežja – DO in/ali sistemskega operaterja prenosnega omrežja – SO. Glede na tip[1] vira se zahteva [5]:

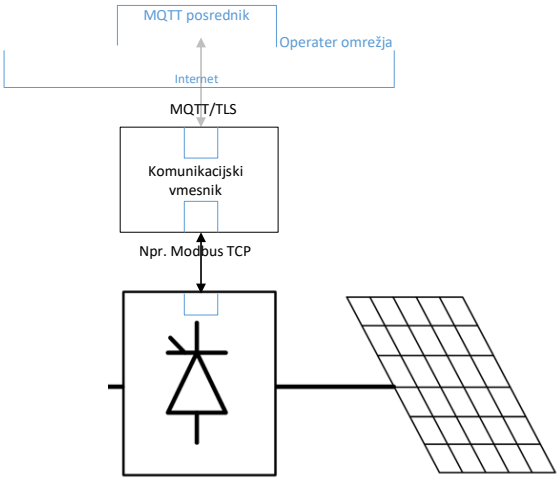
– tip A (daljinski izklop/vklop) mora imeti na voljo digitalni vhod, ki omogoča prenehanje zagotavljanja delovne moči na izhodu v času 5 sekund od sklenitve releja, ki je na ta vhod priključen. Rele za izklop zagotovi zadevni operater omrežja, predvidoma v okviru elektronskega števca ali druge daljinsko krmiljene naprave.
– tip B (obratovalne meritve in komande): osveževanje vsaj na 1 minuto pri RV tip B, dovoljena zakasnitev največ 10 sekund, zanesljivost 99 %. Hitrost prenosa informacij: do 64 kb/s. Natančnost ure realnega časa, na podlagi katere se določijo časovne značke meritev, naj bo znotraj 10 ms.
– tip C (obratovalne meritve in komande): osveževanje vsaj na 2 sekundi, dovoljena zakasnitev največ 100 ms, zanesljivost med 99,9 in 99,99 %. Hitrost prenosa informacij: do 64 kb/s. Natančnost ure realnega časa, na podlagi katere se določijo časovne značke meritev, naj bo znotraj 10 ms.
– tip D (obratovalne meritve, PMU[2] meritve in komande): osveževanje na 20 ms, dovoljena zakasnitev največ 100 ms, zanesljivost med 99,99 in 99,999 %. Hitrost prenosa informacij: do 1 Mb/s. Natančnost ure realnega časa, na podlagi katere se določijo časovne značke obratovalnih podatkov, naj bo znotraj 10 ms, razen za WAMS PMU podatke, kjer se zahteva časovna sinhronizacija < 10 ns.

[1] V razred A razvrščamo vire oziroma energetske module (EM) moči od 0,8 kW do 10 kW, v razred B EM moči od vključno 10kW do 5 MW, v C in D pa EM moči nad 5 MW.

[2] Phasor measurement unit (PMU) oz. meritve za Wide Area Measurement Systems (WAMS)

B. *Komunikacije z RV*

Razpršeni viri imajo različne elektronske naprave (inverterje, krmilnike,...), s katerimi je treba komunicirati. Ker ni splošno uveljavljenega standarda za komunikacijo s temi napravami, je treba predvideti komunikacijski vmesnik, ki poskrbi za komunikacijo z DO in SO na eni strani ter napravami na drugi. Če je na primer možna Modbus komunikacija z inverterjem, se komunikacijski vmesnik in povezave izvedejo tako, kot prikazuje Slika 2. Če inverter nima možnosti komunikacije, lahko meritve in komande izvedemo s pomočjo zunanje naprave oz. merilnika/krmilnika, ki ga integriramo s komunikacijskim vmesnikom.



Slika 2: Primer integracije RV v sistem za daljinski nadzor in vodenje

V [5] so predvidene naslednje komunikacijske rešitve za različne tipe RV:

Tip B: Za izmenjavo podatkov se uporabi MQTT/TLS protokol z vključeno TLS podporo ter skladno z XML shemami in načinom izmenjave podatkov, definiranim s strani DO. Komunikacija poteka preko Interneta, primerne dostopovne tehnologije so naslednje:

– FTTH,
– DSL,
– LTE,
– 3G,
– NB-IoT,
– Internet preko satelita.

Tip C: Za izmenjavo podatkov se uporabi MQTT/TLS protokol z vključeno TLS podporo ter skladno z XML shemami in načinom izmenjave podatkov, definiranim s strani DO (določi se na podlagi dogovora obratovanje-telekomunikacije). Opcijsko se lahko v dogovoru z DO oziroma SO uporabi tudi komunikacijski protokol IEC 60870-5-104, IEC 60870-6 ali ali ustrezni protokoli iz družine standardov IEC 61850, ki temeljijo na IEC 61850-90-5. Komunikacija poteka preko Interneta ali preko zasebnega/avtonomnega omrežja DO oziroma SO, primerne dostopovne tehnologije so naslednje:

– FTTH,
– DSL,
– LTE,
– 3G,
– Internet preko satelita,
– LTE-M,
– zasebno LTE omrežje,
– avtonomno omrežje DO oziroma SO.

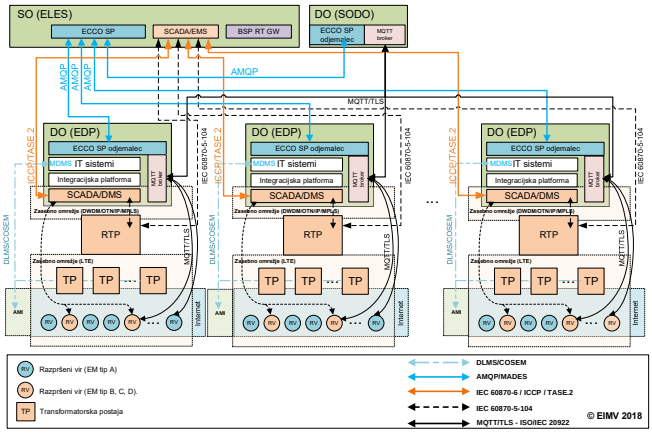
Tip D: V primeru uporabe WAMS PMU merilnika za modul D se le ta poveže s PDC koncentratorjem SO z uporabo protokola IEEE C37.118.2 ali IEC 61850-90-5. Za obratovalne podatke se uporabi MQTT/TLS protokol z vključeno TLS podporo ter skladno z XML shemami in načinom izmenjave podatkov, definiranim s strani DO (določi se na podlagi dogovora obratovanje-telekomunikacije). Opcijsko se lahko v dogovoru z DO oziroma SO uporabi tudi komunikacijski protokol IEC 60870-5-104, IEC 60870-6 ali ustrezni protokoli iz družine standardov IEC 61850, ki temeljijo na IEC 61850-90-5. Primerne tehnologije so naslednje:

– zasebno LTE omrežje,
– avtonomno omrežje DO oziroma SO.

Kot smo že omenili, je MQTT glede na vsebino agnostičen protokol. V primeru uporabe MQTT za komunikacijo z RV uporabimo CIM semantiko [3], kot jo določajo družine standardov IEC 61968, 61970 in 62325. Podatki se skladno s semantičnim modelom in pripadajočimi profili oziroma shemami prenašajo v XML obliki. XML sheme določi DO.

Uporaba standardiziranega semantičnega modela je ključnega pomena, saj se na ta način izognemo zamudnemu procesu ročne preslikave (mapiranju) podatkov v aplikacijah, kot je to na primer v primeru IEC 60870-5-104 in drugih protokolov [6].

IV. KONCEPT IZMENJAVE PODATKOV



Slika 3: Koncept izmenjave podatkov med RV in DO oz. SO

Slika 3 prikazuje potek izmenjave podatkov med operaterji omrežij (DO in SO) ter razpršenimi viri (RV). MQTT/TLS komunikacije potekajo od RV do MQTT posrednika pri DO. MQTT posrednik DO ima povezavo s SO, tako da je skladno s pravicami omogočen tudi neposreden pretok informacij med RV in SO za tiste RV, za katere je to potrebno. Poudariti je še treba, da se podatki med DO in SO prenašajo preko AMQP protokola, zato se pri DO uporabi ustrezen MQTT/AMQP prehod, oziroma se MQTT posrednik integrira z odjemalcem ECCO SP platforme (*ENTSO-E Communication & Connectivity Service Platform*), ki je predvidena za izmenjavo podatkov med SO in DO ter drugimi akterji. Prav tako se povežejo med sabo

MQTT posredniki DO, na primer posrednika elektrodistribucijskega podjetja s SODO.

Povezave se ščitijo s TLS protokolom, pri čemer je treba uporabiti zadnje stanje tehnike, torej najmanj TLS različico 1.2. Komunikacijski vmesnik mora imeti PKI certifikat overitelja digitalnih potrdil (CA – *Certificate Authority*), ter podpirati avtentikacijo / avtorizacijo z uporabniškim imenom in geslom, ki ga dodeli DO. Smiselno bi tudi bilo, da SODO deluje kot CA, tako da se že ob izdaji soglasja za priključitev pridobijo vsi potrebni podatki za komunikacijo.

V. ZAKLJUČEK

Masovna integracija razpršenih virov v elektroenergetsko omrežje vse bolj kaže na to, da je treba naprave teh virov smatrati kot IoT naprave in posledično tudi uporabiti IoT tehnologije za izmenjavo podatkov z njimi. Zelo pomembno je tudi dejstvo, da cena virov na kW inštalirane moči pada in da stroški komunikacije ne smejo predstavljati znatnega deleža pri investiciji. To je še en argument zakaj iti v smeri IoT. Ključnega pomena je tudi, da uporabimo sporočilne sisteme, ki omogočajo prenos informacij, ki je skladen s standardiziranim semantičnim modelom, kar zelo poenostavi konfiguriranje in vzdrževanje IT sistemov, saj lahko aplikacije same razumejo pomen informacij in zamudno ročno preslikovanje podatkovnih točk ni več potrebno. V okviru projekta FutureFlow preizkušen MQTT protokol, s TLS zaščito in vsebino sporočil skladno s CIM semantičnim modelom, se kaže kot dobra, zanesljiva, varna in cenovno ugodna rešitev, na kateri zasnujemo izmenjavo podatkov z razpršenimi viri.

ZAHVALA

Projekt FutureFlow se 100% financira iz sredstev programa za raziskave in inovacije Horizon 2020 v okviru EU v skladu s sporazumom o dodelitvi sredstev št. 691777.

LITERATURA

[1] „Project FutureFlow“. [Na spletu]. Dostopno na: http://www.futureflow.eu/. [Pridobljeno: 19-mar-2019].
[2] Rok Lacko, „WP5 - pilot tests“, predstavljeno na FutureFlow 2nd periodic technical review, Ljubljana, apr-2019.
[3] „IntelliGrid Common Information Model Primer: Third Edition“, EPRI, Palo Alto, CA, 3002006001, 2015.
[4] „EIMV Pentesting report (FutureFlow project)“. Trusted labs, 22-avg-2018.
[5] „Navodila za priključevanje in obratovanje proizvodnih naprav priključenih v distribucijsko elektroenergetsko omrežje, (Priloga študije EIMV št. 2346) - osnutek“. SODO, d.o.o., apr-2019.
[6] Andrej Souvent, Peter Ceferin, Brane Zupan, in Uroš Hrovat, „Vpeljava IoT tehnologij v luči priključevanja razpršenih virov ter souporaba pridobljenih podatkov za zagotavljanje kvalitetnih IKT storitev“, *14 Konf. Slov. Elektroenergetikov*, maj 2019.

Andrej Souvent je diplomiral in magistriral na Fakulteti za elektrotehniko Univerze v Ljubljani. Zaposlen je na Elektroinštitutu Milan Vidmar, kjer vodi Oddelek za vodenje in delovanje elektroenergetskih sistemov. Je član organizacij IEC, IEEE, CIGRÉ, SIST in Inženirske zbornice Slovenije. Ima 20+ let izkušen na področju informacijskih tehnologij, sistemov vodenja in procesne informatike, predvsem za podjetja splošne in elektro-energetike. Področje njegovega dela so sistemi nadzora in vodenja elektroenergetskih sistemov, koncepti, tehnologije in rešitve pametnih elektroenergetskih omrežij, procesna informatika in integracija sistemov.

Uroš Salobir je je diplomiral in magistriral na Fakulteti za elektrotehniko Univerze v Ljubljani. Na Elesu je zasedal več pomembnih položajev kot denimo Pomočnik direktorja za upravljanje s sredstvi, Koordinator za razvoj elektroenergetskega sistema, Direktor področja za obratovanje, maja 2017 pa je postal Direktor področja za strateške inovacije. Strokovno se je izpopolnjeval na področju procesov obratovanja in sistemov vodenja, razvoja trga električne energije, projektov na področju sistemskih storitev, upravljanja sredstev ob upoštevanju tveganj ter nadzora nad izvajanjem investicijskih projektov. Zelo tesno je vpet v mednarodno poslovanje družbe, kjer je sooblikoval strategije in vodil skupino za izravnalni trg v JV Evropi ter skupino za planiranje obratovanja v CV Evropi. Odkar je kot direktor Področja za strateške inovacije v družbi prevzel odgovornost za inovacije, je pomagal oblikovati in koordinirati nekatere velike inovacijske projekte, kot so SINCRO.GRID, slovensko japonsko partnerstvo NEDO, FutureFlow, Defender, OSMOSE in druge.

Internet vsega v železniškem okolju

Jože Urbanc, DRI upravljanje investicij, d. o. o., Ljubljana

Povzetek - Tako kot na področju industrije, se je tudi na področju železnic sprejela strategija Železnice 4.0 (Ž.4.0), ki ga nekatere železnice poimenujejo tudi »Pametne železnice 4.0«. V železniškem okolju, katerega značilnost je relativna togost pri uvajanju tehnoloških novosti, je takšna odločitev vsekakor spodbudna in korak v pravi smeri. Ključno pri uvajanju novih tehnologij v železniškem okolju, tako tudi Ž.4.0, pa je razumevanje soodvisnosti z varnostjo železniškega prometa in soodvisnosti med infrastrukturo in izvajalci storitev na njej.

Ključne besede – železniška infrastruktura, digitalizacija, prevoznik

Abstract - Like in the industrial environment, the Railway Strategy 4.0 (R 4.0) has been adopted in the railway sector, and is also referred to as "Smart Railways 4.0". In the railway environment, which has traditionally been characterized by relative hesitation in introducing technological innovations, such a decision is certainly encouraging and shows a step forward in the right direction. The key in introducing new technologies and R 4.0 in the railway environment is the understanding of its interdependence with the safety of railway transport and interdependence between infrastructure and its service providers.

Key Words – Railway Infrastructure, Digitalisation, Rail Carrier

I. UVOD

Železnice kot transportni sistem in tudi kot industrijska panoga, so v dosedanji zgodovini odigrale pomembno vlogo. Bile so nosilec in generator razvoja. Kot velik sistem so se v nekem trenutku ujele v past, ki bi jo lahko poimenovali *zamrznitev v času*. Tehnološko so zaostale. Pri tem ne gre kriviti samo železnic, oziroma je potrebno pogledati širši kontekst in ugotoviti, da je tehnološki razvoj dobil tak tempo, da ga je bilo železnicam praktično nemogoče slediti. Toda v sedanjem trenutku se dogaja tudi na železnicah velik korak naprej in, ne glede na vse moremo in moramo ugotoviti, da se je železniški sektor odločno in nepovratno podal na pot digitalizacije, ki se opredeljuje kot železnice 4.0 (R 4.0). To velja za Evropo in enako za ostali svet. Na tem področju je veliko iniciativ, delovnih skupin in različnih dokumentov [1].

A. *Vstop v digitalni čas železnic*

Kot v vseh dosedanjih tehnoloških preskokih, se tudi tokrat železnice segmentirajo na tiste, ki so vodilne pri raziskovanju možnosti in uvajanju tehnologije digitalizacije in tiste, ki bodo z manjšim ali večjim časovnim zamikom sledile. Ob tem pa so ugotovitve o ključnih prednostih za železniški sektor, ki jih lahko prinese digitalizacija, praktično enake v Avstraliji, Južni Koreji, Indiji, Ameriki in Evropi. Strnemo jih lahko v naslednje tri sklope:

1. Železniška infrastruktura:
   a. povečanje kapacitet za zadovoljitev sedanjih in prihodnjih potreb,
   b. povečanje zanesljivosti storitev.
2. Prevozne storitve:
   a. izboljšanje informiranosti uporabnikov (potnikov in izvajalcev prevoznih storitev),
   b. zmanjšanje porabe energentov,
   c. skrajšanje prevoznih časov (v potniškem in tovornem prometu).
3. Upravljanje z infrastrukturo:
   a. nižji investicijski (Capex) in operativni (Opex) stroški,
   b. povečanje učinkovitosti pri upravljanju prometa in vzdrževanju infrastrukture.

Poleg teh dejavnikov, oziroma kot četrti in hkrati najpomembnejši dejavnik, ki povezuje vse tri navedene sklope, pa moramo dodati povečanje varnosti (safety) prometa.

Na tem mestu se lahko vprašamo še, kakšen bi bil pogled na digitalne železnice s strani uporabnikov železniških storitev. Ob dejstvu, da v digitalnem okolju poznamo dve stanji – 0 in 1, bi ga morda lahko opisali nekako tako:

- stanje »1« pomeni, da je potnik ali tovor prispel od točke A do točke B v točno tistem časovnem oknu, kot je bil z voznim redom predviden; da je potnik pri tem lahko čas potovanja preživel udobno in z dostopom do službenih ali zabavnih vsebin; da je tovor prispel nepoškodovan in je njegov lastnik ves čas vedel, kje se trenutno nahaja in v kakšnem stanju je.
- Stanje »0« pomeni, da je prišlo do motnje pri izvedbi prevozne storitve in le-ta ne bo med točkama A in B opravljena v predvidenem času. Ob tema bo potnik pravočasno in popolno informiran o nastali situaciji in o alternativnih možnostih; lastnik tovora bo prav tako pravočasno in popolno informiran o nastali spremembi in pričakovani zamudi dostave tovora.

B. *Železniško okolje kot osnovno izhodišče*

Na železnicah je veliko soodvisnosti med infrastrukturo (proga, signalno-varnostna in telekomunikacijska oprema, električni sistem vleke) in voznim parkom (lokomotive, vagoni, potniške garniture). Uvedba rešitev na infrastrukturi največkrat zahteva tudi spremembe, ali pa vsaj prilagoditve, tudi na voznem parku. V cilju odpiranja trga, povečanja konkurenčnosti med prevozniki in želenim, pa tudi pričakovanim znižanjem stroškov, je bil železniški sektor v EU dereguliran v smislu dosledne ločitve med lastnikom infrastrukture in izvajalci prevoznih storitev, tako v tovornem kot tudi v potniškem prometa. Medtem, ko je infrastruktura na tak ali drugačen način ostala v državni lasti, so prevozniki v večini primerov zasebne družbe. V praksi se je razvilo sicer veliko modelov, s katerimi so države poskušale obiti te

predpise in državne prevoznike ohraniti pod proračunskim dežnikom, vendar to ne spreminja ključnega dejstva, da je na eni strani državna infrastruktura in na drugi strani zasebne družbe - prevozniki, ki delujejo na trgu prevoznih storitev. In ne tekmujejo samo med seboj v okviru železniških storitev ampak na globalnem trgu, kjer je konkurenca tudi cestni, vodni in letalski promet.

Kot že omenjeno, spremembe na infrastrukturi vplivajo na vozni park, tako da so prevozniki, torej zasebne družbe, če želijo še naprej voziti po tej infrastrukturi, prisiljeni v prilagoditev opreme na svojem voznem parku. Ob tem ni nepomembno dejstvo, da se večina investicij v infrastrukturo financira iz državnih proračunov. V primeru sistemov, ki jih je EU prepoznala kot ključne za interoperabilnost železniške infrastrukture, pa se financiranje zagotavlja tudi iz EU-virov. Na drugi strani pa finančno breme prilagoditev na voznem parku pade izključno na prevoznika. Ker so prilagoditve običajno relativno visok strošek, to predstavlja pomemben ekonomski učinek, ki na koncu vpliva tudi na konkurenčnost v primerjavi s prevozniki v drugih transportnih sistemih. Za primer vzamemo evropski sistem za nadzor vlakov ETCS (European Train Control System), ki je v EU prevzet kot standard na področju tovrstnih sistemov in je njegova vgradnja obvezna na infrastrukturi in na vozilih. Strošek vgradnje na vozilo se giblje med 200- in 300-tisoč evri. Če se pri nabavi novih vozil ta strošek še nekako izgubi, pa je pri vgradnji na obstoječ vozni park zadeva precej drugačna in neposredno zaje finančno substanco prevoznika. Da je problem za prevoznika še večji, pa mora k strošku opreme prišteti še stroške verifikacijskih postopkov s strani priglašenega organa, testiranja v realnem okolju v interakciji z infrastrukturo ter na koncu pridobiti še spričevalo o ustreznosti konkretnega tipa vozila za vožnjo na infrastrukturi določene države. Vse to zahteva čas, predstavlja izpad prihodkov iz prevozov, ker vozilo ni na voljo in zahteva dodatna usposabljanja strojevodij.

S tega vidika lahko razumemo zadržanost prevoznikov do tehnoloških sprememb, ki jih pogojuje infrastruktura. Še posebej to velja, ko se pred njih postavijo roki za implementacijo, ki so nerazumno kratki v primerjavi z običajno življenjsko/eksploatacijsko dobo voznega parka, ki je okrog 40 let. Kot učinkovit pristop se izkaže sinhronizacija med tehnološkimi spremembami na infrastrukturi in posodobitvami voznega parka [2].

Zakaj je vse to omenjeno? Ker gre za pomemben dejavnik in njegovo neupoštevanje. Nezavedanje ali ignoriranje pri uvajanju novih tehnologij pa vodi z visoko verjetnostjo k neučinkovitosti.

II. PRIMER PRISTOPA ŠVICARSKIH ŽELEZNIC

Kot primer prehoda v digitalne železnice izberemo Švico. Razlog je v celovitosti in sistematičnosti, ki izhaja iz njihovega pristopa. Svoj program so poimenovali Smartrail 4.0 [3].

Poglejmo na kratko.

1) V projekt so vključili vse deležnike, ki delujejo na področju železniškega prevoza s skupnim ciljem, pripraviti železnice na digitalno prihodnost. Jedro tako tvorijo vse železniške organizacije, ki delujejo na švicarskem železniškem omrežju (SBB, BLS, Schweizerische Südostbahn AG (SOB), the Rhaetian Railway (RhB) kot tudi Združenje javnih prevoznikov (UPT). Poleg teh so deležniki v projektu tudi železniška industrija ter znanstvene ustanove (raziskovalne in izobraževalne). Neke vrste vodilno vlogo v tem projektu ima železniško podjetje SBB kot največje in najpomembnejše v Švici.

   Ob zavedanju, da se železniški sistem ne konča na državni meji, temveč mora biti poenoten širše (globalno interoperabilen), so za to potrebne določene minimalne uskladitve osnovnih tehničnih rešitev, sistemov upravljanja prometa in določanja lokacije vlaka. V tem cilju švicarske železnice tesno sodelujejo z drugimi železniškimi organizacijami (DB, ÖBB, SNCF) in z organizacijami, ki delujejo na področju železniške standardizacije.
2) Cilje so postavili jasno in z merljivimi kazalci. Kot ključne so opredelili:
   a. zmanjšanje zunanjih naprav na progi za 70 %,
   b. prihranki z naslova projekta v višini 450 mio CHF na letni ravni,
   c. povečanje progovnih kapacitet na železniškem omrežju za 15 do 30 %,
   d. povečanje razpoložljivosti varnostnih naprav za 50 %,
   e. zmanjšanje nevarnosti nesreč (pri premiku in izvajanju del na progi) za 90 %,
   f. zagotavljanje visoko propustnega podatkovnega omrežja za uporabnike – zmogljivost >20 MBit/sec.
3) Postavili so jasne mejnike posameznih faz projekta:
   a. Načrtovanje projekta (obdobje 2017 do 2019) - izdeluje se konceptualno zasnovo ter tehnične in funkcijske zahteve prihodnjega sistema. Prav tako se izdelujejo analize tehnične izvedljivosti ter poslovni modeli, ki se morajo potrditi. Na tej podlagi se izdela potrebna dokumentacija za odločanje in razpise.
   b. Testno obdobje (obdobje 2020 – 2026) - sprejeta konceptualna rešitev se bo preizkušala v realnem okolju na eni ali več progah.
   c. Faza implementacije (obdobje 2027 – 2038).

Tehnološko načrtujejo prehod iz sedanjega radijskega železniškega omrežja GSM-R (2G), ki je že vgrajeno na železniškem omrežju, na prihodnje železniško radijsko omrežje (5G), in sicer z minimalnimi možnimi nadgradnjami infrastrukture ob progi. Ob tem so začetek prehoda na železniško omrežje 5G smiselno vezali na planirane aktivnosti standardizacijskih organov za železniški sektor, ki načrtujejo izdajo tehničnih specifikacij za omrežje 5G v letu 2022. Železniško omrežje 5G je trenutno poimenovano s kratico FRMCS (Future Railway Mobile Communication System). Več podatkov pa je na voljo na spletnih straneh Železniške organizacije UIC [4].

Projekt švicarskega železniškega sektorja Smartrail 4.0 je aktiven projekt, za katerega lahko verjamemo, da bo skozi faze doživel tudi določene smiselne prilagoditve, ki bodo izhajale iz spoznanj v fazi načrtovanja in testiranj. Na tem mestu zato ni smiselno dodatno izgubljati besed, vse ažurne informacije o projektu pa so dostopne na spletni strani [3].

III. DOMAČE OKOLJE

Morda je za slovensko železniško omrežje treba najprej ugotoviti, da ima dobro telekomunikacijsko podlago, saj ima sistem GSM-R (2G) zgrajen na vseh progah. Prav tako so vse proge opremljene z optičnimi kabli. V bližnji prihodnosti je načrtovana tudi izgradnja podatkovnih omrežij (IP MPLS) z visokimi zmogljivosti. Ob tem pa moramo dodati tudi, da je bila večina slovenskega železniškega omrežja zgrajena pred 150 leti. To predstavlja veliko omejitev pri zagotavljanju višjih progovnih hitrosti in propustnosti prog.

Na drugi strani, z vidika prevoznikov, lahko ugotovimo, da je vozni park star in potreben obnove in zamenjave.

Kot zadnje, nikakor pa ne manj pomembno, lahko ugotovimo, da nimamo pomembnejše domače železniške industrije in posledično to področju tudi v znanstvenem okolju ni posebej izpostavljeno.

Vse to pa še ne pomeni, da bi morali spregledati izzive in možnosti, ki jih prinašajo digitalne železnice in stati nekje ob strani te tehnološke revolucije. Verjetno ne moremo biti nosilci ali vodilni pri tovrstnih tehnoloških korakih, se pa odpirajo in ponujajo možnosti na področjih aplikativnih rešitev, ki se razvijajo na tej tehnološki platformi. Pri aplikativnih rešitvah gre namreč za prepoznanje potrebe na eni strani in na drugi za sposobnost izdelave enostavne, stroškovno sprejemljive rešitve. To sposobnost so naše znanstvene ustanove in tudi podjetja že večkrat dokazala.

Kot dodatni motiv pri tem lahko omenimo tudi dejstvo, da je železnica prepoznana kot eden ključnih transportnih sistemov prihodnosti, predvsem zaradi svoje okoljske sprejemljivosti in učinkovitosti v primerjavi z drugimi transportnimi sistemi. Tak položaj železnic pomeni zagotovilo za investicijska vlaganja, za vlaganja v raziskave in razvoj in tudi industrijo [5].

Da ne ostanemo zgolj pri bolj ali manj teoretičnih izhodiščih, navedimo dva primera, kjer bi lahko uporaba rešitev, ki jih omogočata digitalizacija železnic in internet stvari, imela neposredne in merljive učinke.

A. *Vzdrževanje infrastrukture*

Vzdrževalni pristop na železniški infrastrukturi temelji večinoma na rednem pregledovanju stanja le-te. Pri tem je pogostnost pregledov odvisna od vrste infrastrukture (tiri, kretnice, mostovi, tuneli, nasipi, brežine, vozna mreža, signalnovarnostne naprave, telekomunikacijske naprave itd.). Tak pristopu, ki je sicer povsem običajen tudi na drugih železnicah, ima vsaj dve bistveni pomanjkljivosti:

- v času med enim in drugim pregledom nimamo podatka o stanju dotične infrastrukture in
- vsak pregled zahteva dostop osebja na lokacijo, kjer je vgrajena oprema.

Posledica prve pomanjkljivosti je tveganje za nastanek izrednega dogodka zaradi napake, ki se je pojavila v vmesnem času med pregledi, in ima za posledico zmanjšanje razpoložljivosti proge, v skrajnem primeru pa je to lahko vzrok za nesrečo. Nerazpoložljivost proge pomeni izpad/zmanjšanje prihodkov za upravljavca infrastrukture, enako za prevoznike, za končne uporabnike storitev pa vsaj veliko nevšečnost.

Dostop do lokacije in izvedba pregleda pomeni neposredno strošek dela ob hkratnem dejstvu, da ni nikakršne garancije, da ne bo na ravnokar pregledani napravi, naslednji trenutek po odhodu vzdrževalca, nastala napaka.

Če vzdrževalni pristop spremenimo v »vzdrževanje po dejanskem stanju« (t.i. CBA, Condition Based Maintenance) se zgolj ob zgornjih dejstvih pojavijo bistveni prihranki[5]. Za uvedbo CBA pa potrebujemo podatke o infrastrukturi v realnem času. Le-te lahko pridobimo z vgradnjo ustrezne senzorike na ključnih mestih infrastrukture. Prav tako se lahko podatki pridobivajo tudi iz vozil ali iz naprav, ki so dodatno vgrajene na vozilih. Za realizacijo takšne senzorike je IoT nedvomno ustrezna in učinkovita rešitev.

B. *Spremljanje stanja ob progi*

Glede na konfiguracijo terena v Sloveniji, so proge na veliko mestih izpostavljene nevarnosti plazenja, padajočih skal ali dreves in tudi poplav. Prav tako je v času suše na veliko odsekih prog, velika požarna ogroženost. Za obe težavi je možna uporaba IoT-rešitev. Za spremljanje padajočih skal ali dreves so sicer na nekaterih odsekih prog uvedeni sistemi obveščanja, z IoT-rešitvami pa se lahko zagotovi realne podatke o stanju, kar prispeva k učinkovitejši sanaciji, saj intervencijske skupine že imajo podatke o vrsti, obsegu, mikrolokaciji dogodka in se lahko ustrezno pripravijo.

Naj omenimo še eno področje kot zanimivost - lahko pa tudi kot izziv za razmišljanje. Kraje bakrenih kablov ob progi so v Združenem kraljestvu velik problem, saj so se po zadnjih podatkih kraje v zadnjem letu povečale za 85 %![6] Posledično imajo kraje velik vpliv tudi na storitve, tako da ne predstavljajo zgolj tehničnega problema ampak še veliko bolj operativnega. Čeprav so za preprečevanje kraj uporabili vse znane metode, so se sedaj odločili za reševanje z izgradnjo infrastrukture IoT [7].

IV. ZAKLJUČEK

Digitalizacija železnic, katere sestavina je tudi IoT, je dejstvo. Izzivi, ki jih prinaša, so zanimivi in večplastni. Za slovensko okolje smemo reči, da so priložnosti, ki jih prinaša še veliko večje, kot to velja za Švico, ki smo jo v tem prispevku vzeli kot referenčni primer.

Izzivi in priložnosti v Sloveniji se dotikajo tako tehnologije kot tudi, in predvsem, področja strateških usmeritev, odločitev ter iz njih izpeljanih vseobsegajočih (glede na deležnike) projektov. Posamezniki brez državnega načrtovanja, gospodarskih virov in znanstvenih raziskav pri reševanju tovrstnih izzivov ne bodo prišli daleč[1].

Na najvišji ravni imamo na voljo Strategijo razvoja prometa v RS [8] in na njeni podlagi izdelan Nacionalni program razvoja prometa v RS za obdobji 2016–2022 ter 2022–2030. Na ravni operativnega načrtovanja, implementacije in vzdrževanja pa moramo vzpostaviti v Sloveniji multidisciplinarno platformo, v okviru katere bodo enakopravno sodelovale raziskovalno-izobraževalne ustanove, proizvodna podjetja, železniški sektor in izvajalci storitev.

[1] Harari v svoji knjigi Homo Deus (str.36; MK 2018) zapiše: »Posamezniki brez državnega načrtovanja, gospodarskih virov in znanstvenih raziskav v iskanju sreče ne bodo prišli daleč«.

LITERATURA

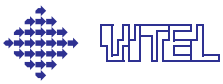
[1] http://shift2rail.org
[2] Global Rrailway Review; Volume 24, Issue 6, pages 1-4;
[3] http://www.smartrail40.ch.
[4] http://www. uic.org
[5] Ohoyun at all; Internet of Thinks for Smart Railway: Feasibility and Applications; IEEE Internet of Thinks Journal, 2017
[6] http://assets.publishing.service.gov.uk
[7] http://www.globalrailwayreview.com/article/64288
[8] http://www.mzi.gov.si/strategija_razvoja_prometa_v_rs

Jože Urbanc je na Slovenskih železnicah delal na različnih delovnih mestih, kot vzdrževalec signalnovarnostnih in telekomunikacijskih naprav, kot vodja oddelka za telekomunikacije in kot vodja službe za strategijo in razvoj. Sedaj je zaposlen v podjetju DRI, upravljanje investicij, d.o.o., z nalogami pri investicijskih projektih na železnicah in na DARSu ter strateških načrtih razvoja infrastrukture.

PRISPEVKI

ARTICLES

21. 5. 2019



Razvoj omrežja IoT Telekoma Slovenije

Andrej Kranjčević, Marjan Muršec, Telekom Slovenije, Ljubljana

Povzetek — Razvoj omrežja Telekoma Slovenije izhaja iz jasno definiranega poslanstva, vizije in vrednot. Pomemben vhodni podatek predstavljajo strateške smernice in globalni tehnološki trendi na področju IKT. Jedrno omrežje postaja jedrni oblak s centralizirano operativno in nadzorno funkcijo, na vse bolj virtualizirani platformi, vse za prilagodljivo zagotavljanje kakovostnih storitev na optimalen način. V povezavi z zanesljivim, varnim in stroškovno učinkovitim dostopovnim omrežjem ter aplikacijskimi rešitvami, omogoča sodobne NB-IoT in LTE-M1 storitve omrežja. Skupaj pa se z vse višjo stopnjo inteligence in avtomatizacije tehnološko postopoma razvijajo v platformo za celovite storitve in rešitve 4G/5G.

Ključne besede — Telekom Slovenije, LPWA, NB-IoT, LTE-M1, 4G, 5G, VoLTE

Abstract — The development of the Telekom Slovenije network is based on clearly defined mission, vision and values. Strategic development guidelines and global technological trends in the field of ICT are considered as important inputs. The core network of Telekom Slovenije is becoming core cloud with centralized operational and control function, on an increasingly virtualized platform, all devoted to agile provisioning of quality services in an optimal way. In conjunction with a reliable, secure and cost-effective access network, and application solutions, modern NB-IoT and LTE-M1 network services are provided. Together with the increasing level of intelligence and automation they are gradually developing into the end-to-end 4G/5G services and solutions platform.

Keywords — Telekom Slovenije, LPWA, NB-IoT, LTE M, 4G, 5G, VoLTE

I. UVOD

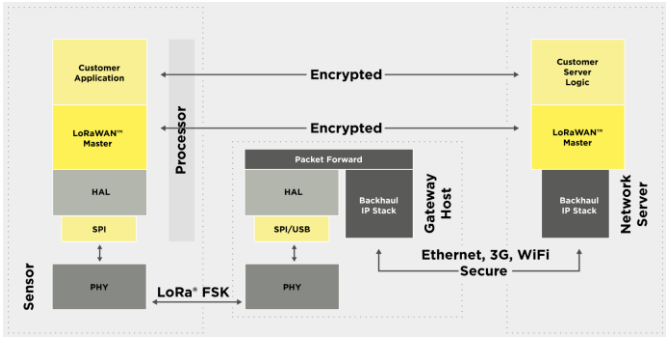
Razvoj mobilnega omrežja Telekoma Slovenije je vedno temeljil na jasno izraženi želji po zagotavljanju uporabnikom najboljšega mogočega mobilnega omrežja, tako glede pokrivanja s signalom, kot tudi podprtih tehnologij. S tem namenom smo med prvimi operaterji na svetu našim uporabnikom ponudili tretjo generacijo mobilnih telekomunikacij, nato četrto generacijo in sedaj si prizadevamo ponuditi tudi peto. A že četrta generacija LTE/4G je pokazala, da pri razvoju mobilnih telekomunikacij ne gre zgolj za oglaševanje novih generacij z namenom višanja hitrosti prenosa podatkov, tudi če uporabnike pravzaprav zanima ravno slednje, temveč gre tudi za velike tehnološke spremembe. Do četrte generacije smo za prenos govora uporabljali povezavno komutirano (CS – Circuit Switched) tehnologijo. Ta v 4G ni več podprta in govor se prenaša preko IP podatkovnega toka. V Telekomu Slovenije smo tako prvi v Sloveniji uporabnikom omogočili govor preko LTE oz. VoLTE (Voice over LTE).

A VoLTE ni končni cilj, temveč zgolj potreben pogoj za začetek veliko večje transformacije omrežja, ki operaterju, s selitvijo govornega prometa z 2G in 3G na 4G, omogoča, da začne s pripravami na ukinitev starejših, na povezavni tehnologiji temelječih radijskih omrežjih. A ni zgolj govor tisti, za katerega so danes uporabni radijski omrežji 2G in 3G. Uporabljajo ga tudi najrazličnejše obstoječe rešitve IoT (Internet of Things). Jasno je, da te z današnjega stališča zgodovinske rešitve, potrebujejo alternativo za priohodnost.

II. OMREŽJA LPWA

A. *LoRaWAN*

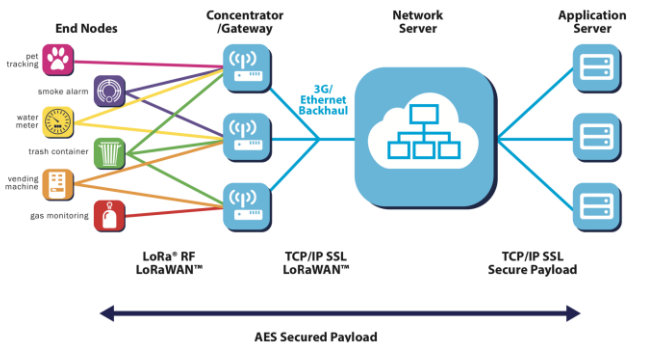
Morda najbolj razširjeno omrežje LPWA temelji na tehnologiji Wi-Fi. Prisotno je v Sloveniji – tudi pri Telekomu Slovenije. Gre za omrežni protokol z nizko porabo energije in širokim območjem pokrivanja, namenjen brezžičnemu povezovanju naprav interneta stvari z baterijskim napajanjem v regionalnih, nacionalnih ali globalnih omrežjih, ki pa temelji na odprtem frekvenčnem pasu. Naslavlja osnovne zahteve interneta stvari (IoT), kot so dvosmerna ozkopasovna komunikacija, varnost komunikacije, mobilnost in lokalizacija.



Slika 1: Komunikacijski protokol LoRaWAN

Omrežje LoRaWAN, tako kot veliko starejših brezžičnih sistemov, za fizično plast uporablja modulacijo frekvenčnega pomika (FSK), saj gre za zelo učinkovito modulacijo pri nizki oddajni moči. En sam prehod LoRa lahko pokriva celotna mesta ali stotine kvadratnih kilometrov velika področja. V praksi je pokrivanje seveda močno odvisno od konfiguracije terena, želenega namena uporabe, potrebnih kapacitet, ipd.

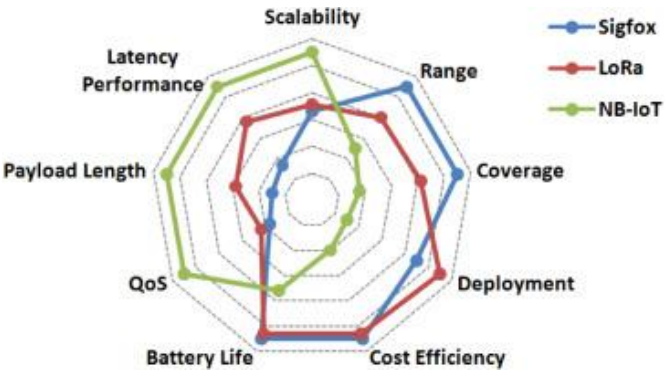
Omrežje LoRaWAN uporablja arhitekturo omrežja, v katerem posamezna končna vozlišča posredujejo informacije drugih vozlišč, da povečajo doseg komunikacije in velikost celice omrežja. Medtem, ko se doseg poveča, pa se doda kompleksnost, zmanjšuje zmogljivost in skrajšuje življenjsko dobo baterije, saj vozlišča prejemajo in posredujejo informacije iz drugih vozlišč. Dolgoročna zvezna arhitektura je najbolj smiselna za ohranjanje življenjske dobe baterije, ko je mogoče doseči dolgoročno povezljivost.



Slika 2: Mrežna arhitektura omrežja LoRaWAN

V omrežju LoRaWAN[1] končna vozlišča (ang. End Nodes) niso povezana le z določenim prehodom (ang. Gateway), temveč podatke, ki jih prenaša končno vozlišče, običajno sprejema več prehodov. Podatkovni paketi so preusmerjeni od končnega vozlišča do omrežnega strežnika (ang. Network Server) v oblaku, preko mobilne celične povezave (npr. LTE/4G), Ethernetne povezave ali Wi-Fi. Inteligentnost in kompleksnost je potisnjena na omrežni strežnik, ki upravlja omrežje, filtrira odvečne prejete pakete, izvaja varnostne preglede, razporeja potrditve prek optimalnega prehoda in prilagaja hitrost prenosa podatkov do ustreznega prehoda in seveda do aplikacijskih strežnikov.

Vozlišča v omrežju LoRaWAN uporabljajo asinhroni način delovanja in sporočajo, kdaj so podatki za pošiljanje na voljo, bodisi po vnaprej določenem razporedu ali glede na določen dogodek. V sinhronem načinu delovanja se vozlišča pogosto *prebudijo*, da se sinhronizirajo z omrežjem in preverijo, ali so na voljo sporočila. Ta sinhronizacija porabi precej energije in je poglavitni razlog za krajšanje življenjske dobe baterije. Primerjava različnih tehnologij LPWA, ki jih je razvila GSMA, kaže, da LoRaWAN v primerjavi z ostalimi tehnologijami obljublja od 3- do 5-krat daljšo življenjsko dobo baterije.



Slika 3: Primerjava različnih tehnologij LPWA

B. *NB-IoT*

NB-IoT je nova radijska tehnologija, katere lastnost je, da uporablja poseben ozek del spektra omrežja LTE, omogoča preproste, poceni in hkrati energijsko varčne modeme [3]. Tako omogoča povezavo tudi tistih naprav, ki jih tradicionalno do zdaj nismo povezovali v internet, ker z obstoječimi tehnologijami to ni bilo možno ali gospodarno.

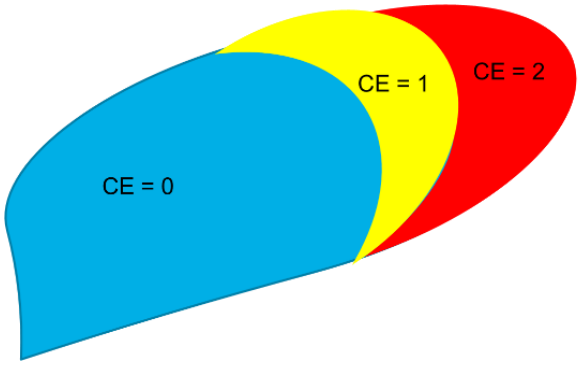
Tukaj je posebej treba izpostaviti senzorje, števce, in naprave, ki s podatki, ki jih generirajo, postanejo uporabnejše po povezavi v omrežje.

Tabela 1: Zahteve organizacije 3GPP za tehnologijo NB-IoT

Zahteve	*NB-IoT*
Cena	Nizka cena modulov, 5-10 $ na modul
Pokrivanje	Izboljšano pokrivanje, največja dovoljena izguba 164 dB
Življenjska doba baterije	10 let delovanja s zmogljivostjo baterije 5 Wh
Gostota naprav/celico	Najmanj 50.000 na celico
Varnost	Varnost glede avtentikacije in šifriranja, ki temelji na LTE varnosti

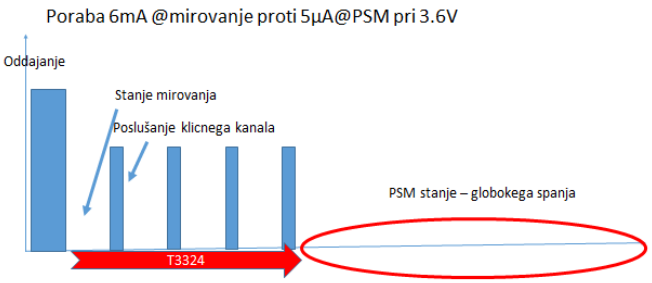
Uporabljamo lahko različne protokole, katerih nabor je velik. Zato je glede na vrsto aplikacije/uporabe mogoče izbrati najboljšo možnost, kjer izbor učinkovitejše in preproste rešitve v večini primerov zagotavlja najboljše rezultate. Preprosta struktura naprav pomeni, da trenutna generacija modulov ne uporablja hkratne dvosmerne komunikacije, ampak enosmerno. Za doseganje nizke cene IoT-modulov je navadno najpomembnejša cenovna optimizacija. Velika konkurenca med različnimi proizvajalci modulov je že danes omogočila, da so moduli NB-IoT cenovno ugodnejši od UMTS- in LTE-modulov in zelo primerljivi z moduli, ki podpirajo le tehnologijo GSM in so s tem cenovno v skladu z željeno ceno (glej tabelo 1).

Tehnologija NB-IoT z uporabo dodatnih izboljšav (s kontrolo različnih časovnikov in kontrolo moči glede na zahteve aplikacije IoT) skupno doprinese do 20 dB dodatne pokritosti. Tako je v standardu predvideno območje normalnega pokrivanja do izgub na poti 144 dB, robustnejšega pokrivanja pri izgubah na poti med 145 in 154 dB in območje ekstremnega pokrivanja do izgub na poti do 164 dB. Različna območja se razlikujejo med drugim v odzivnosti, različnem uporabljenem kodiranju, času komunikacije in posledično v porabi energije – vse to je optimizirano glede na zahteve aplikacij IoT.



Slika 4: Primerjava različnih območij pokrivanja

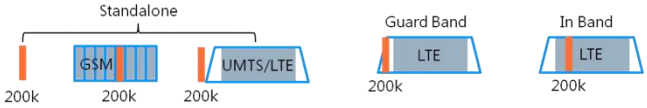
Pri razvoju naprav moramo upoštevati tudi vpliv različnih vrst pokrivanja na porabo energije in posledično na življenjsko dobo baterije. Mnogo naprav, ki uporablja tehnologijo NB-IoT, uporablja lastno baterijsko napajanje, zato je zelo pomemben podatek življenjska doba naprave z uporabljeno baterijo. Možnosti za varčevanje je več. Začne se že z načrtovanjem same naprave in vključuje tako izbiro protokola za komunikacijo kot izbiro časa, ki ga naprava preživi v stanju globokega mirovanja.



Slika 5: Različna stanja modula NB-IoT [4]

Zelo pomembno je iskanje pravega razmerja med pogostostjo oglašanja in velikostjo prenesenih sporočil. Tako dosežemo življenjsko dobo baterije 10 let pri porabi 10 Wh energije na robu pokrivanja (največja poraba energije pri prenosu) in prenosu 10 bajtov enkrat na 24 ur [5]. Pri prenosu 1000 bajtov enkrat na dan se razmere močno spremenijo.

Ena od lastnosti tehnologije NB-IoT je tudi možnost različne izbire postavitve omrežja glede uporabljenih frekvenc. Skupna možnost z LTE-M je tako uporaba frekvence za NB-IoT znotraj že delujoče LTE-celice, druga možnost je uporaba frekvence iz območja varnostnega pasu ali nazadnje možnost samostojne postavitve nosilca NB-IoT na prostem delu frekvenčnega spektra. Večina postavitev NB-IoT uporablja prvo možnost.



Slika 5: Položaj NB-IoT v frekvenčnem pasu LTE

C. *LTE-M*

Razlika med LTE-M in NB-IoT je večja hitrost prenosa podatkov pri LTE-M, boljša podpora mobilnosti v povezanem stanju in v tem, da LTE-M podpira tudi VoLTE. Sama življenjska doba baterije je v primeru LTE-M [6] primerljiva z zgoraj podanim primerom za NB-IoT, ob primerljivem prometnem profilu - poslanih 200 bajtov na 24 ur.

Trenutno je večina komercialno dobavljivih modulov LTE-M kombinirana z NB-IoT. Zahteve za tehnologijo LTE-M so zapisane v standardu 3GPP, verzije 13 [3] in so podobne kot za NB-IoT – povzete so v tabeli 2.

Tabela 2: Zahteve 3GPP za tehnologijo LTE-M

Zahteve	*LTE-M*
Življenjska doba baterije	10 let delovanja s 5 Wh baterijo
Cena	Nizka cena modulov, primerljiva z GSM/GPRS
Pokrivanje	Izboljšano pokrivanje, največja dovoljena izguba 155,7 dB
Spremenljiva hitrost	Najmanj 10 kb/s do 1 Mb/s v odvisnosti od zahtev po pokrivanju

Primerjava med tehnologijama NB-IoT in LTE-M pokaže veliko skupnih točk in tudi v praksi bo uporabniška izkušnja podobna. Seveda pa je omrežje, ki uporablja LTE-M, namenjeno senzorjem oziroma aplikacijam, ki zahtevajo nekaj več podatkovne hitrosti in manjše zakasnitve, še posebej v smeri od naprave v omrežje (tipično za nadzorne kamere ali naprave, kjer je zahtevana relativno nizka zakasnitev). Trenutno je v produkciji preko 120 omrežij NB-IoT/LTE-M [7]. Obstaja preko 200 naprav, ki za komunikacijo uporabljajo ali tehnologijo NB-IoT ali tehnologijo LTE-M, njihovo število pa se je samo v zadnjem letu dni več kot podvojilo in hitro raste.

III. REŠITVE IOT

A. *Pametna mesta*

V sklopu strategije Telekoma Slovenije na področju interneta stvari smo vzpostavili prvi referenčni projekt *Pametno mesto Novo mesto*, s katerim se umeščamo kot prepoznaven ponudnik celovitih rešitev za pametna mesta, kot tudi ponudnik posameznih rešitev, ki sestavljajo celoto.

Referenčni projekt pametnega mesta vključuje obširno okoljsko senzoriko (temperatura, vlaga, zračni pritisk, NO2, CO2, O3, PM10, PM2.2, PM1 in SO2), pametne obcestne svetilke z možnostjo dinamičnega prilagajanja svetilnosti, senzorje zasedenosti parkirnega mesta, polnilne postaje za električna vozila ter merilnike pretoka vode in plina. Rešitve za povezljivost uporabljajo omrežje prehodov in zaledno platformo LoRaWAN, na kateri so realizirane različne aplikacije tako za potrebe mesta kot občanov. Tudi obstoječe rešitve za eZdravje in eOskrbo bomo razvijali na tehnologiji LTE IoT.

Skupaj s tehnološkimi, razvojnimi in infrastrukturnimi partnerji smo razvili tudi osrednjo komunikacijsko postajo, ki je zasnovana kot pametna ulična svetilka, a nadgrajena tako, da omogoča spremljanje ključnih dogodkov na lokaciji. Prek komunikacijske postaje se lahko opravijo storitve polnjenja električnih vozil, lokacijske informacije (točke zanimanja v bližini) in okoljske informacije (kakovost okoliškega zraka in vremenska napoved) ali upravljavcu posredujejo povratne informacije (kako so zadovoljni z dostopom, kdaj najlažje opravijo obisk/nakup, ali potrebujejo parkirno mesto ipd.).

B. *»Massive IoT« oziroma množični IoT*

Druga kategorija, kateri posvečamo veliko pozornosti, je tako imenovani *Massive IoT* oziroma množični IoT. Sem spadajo vse rešitve, kjer gre za množico podobnih naprav razpršenih na širokem geografskem področju ali različnih naprav na ozkem področju - na eni lokaciji. Gre predvsem za najrazličnejše oblike merjenja in nadzor porabe energentov (plin, elektrika, toplotna energija) in vode. To področje želimo razviti s pomočjo partnerjev, lokalnih komunalnih podjetij in proizvajalcev senzorike, kjer bomo za povezljivost uporabili omrežje NB-IoT ali LTE-M. V veliki meri bo razvoj na tem področju temeljil tudi na naših obstoječih platformah (Neo, eOskrba, eZdravje).

IV. OMREŽJE NB-IOT TELEKOMA SLOVENIJE

Svoje mobilno omrežje, ki so ga neodvisni zunanji strokovnjaki na nedavnem testu ocenili kot najboljšega v Sloveniji, smo že v celoti nadgradili s tehnologijo NB-IoT. Nadgradnja obstoječega omrežja LTE s podporo tehnologiji NB-IoT odpira nove priložnosti za razvoj inovativnih rešitev z visoko dodano vrednostjo za optimizacijo procesov, upravljanje z viri, zagotavljanje visoke stopnje varnosti, pa tudi višje kakovosti bivanja. Hkrati predstavlja nadaljnji mejnik v smeri razvoja pete generacije mobilnih omrežij

(5G). Prve projekte s tovrstnimi rešitvami že izvajamo na področju pametnih mest, e-mobilnosti in e-zdravja.

Razvoj infrastrukture in rešitev interneta stvari je skladen z razvojno strategijo, zato svoje omrežje že več let postopoma nadgrajujemo in pripravljamo na uvedbo pete generacije mobilnih omrežij (5G). Tako z omrežjem LTE/4G pokrivamo že več kot 98 %, z omrežjem LTE-Advanced (4G+) pa že več kot 68 % prebivalstva. Skladno s tem vse več naših uporabnikov prehaja na novejše tehnologije, ki zagotavljajo boljšo povezljivost in višje prenosne hitrosti, poslovnim uporabnikom pa je na voljo tudi možnost sklenitve dogovora o ravni storitev (ang. SLA – Service Level Agreement) in zagotavljanje kibernetske varnosti.

V našem podjetju vzpostavljamo odprt ekosistem razvoja celovitih rešitev IoT, pri čemer se na podlagi izkušenj in kompetenc umeščamo kot vodilni integrator in upravljavec celovitih rešitev IoT, ki so sestavljene iz ekosistema naprav IoT, varnega omrežja in aplikacij.

LITERATURA

[1] LoRa Alliance, What is LoRaWAN, https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

[2] Huawei, NB-IoT – Enabling New Business Opportunities, https://www.huawei.com/minisite/hwmbbf15/img/nb-iot-white-paper-mbb-forum-2015.pdf

[3] Philippe Reininger, 3GPP Standards for the Internet-of-Things, stran 9, https://www.3gpp.org/images/presentations/2016_11_3gpp_Standards_for_IoT.pdf

[4] https://www.quectel.com/UploadFile/Product/Quectel_BC95_NB-IoT_Specification_V1.2.pdf

[5] El Soussi, Mohieddine & Zand, Pouria & Pasveer, Frank & Dolmans, Guido. (2017). Evaluating the Performance of eMTC and NB-IoT for Smart City Applications.

[6] Olof Liberg, Mårten Sundberg, Y.-P. Eric Wang, Johan Bergman, Joachim Sachs, Cellular Internet of Things, Chapter 6 - LTE-M Performance,

[7] https://www.gsma.com/iot/mobile-iot-commercial-launches/, stanje april 2019

[8] https://docbox.etsi.org/Workshop/2018/201810_IoTWEEK/02_IoTWORKSHOP/S04_IoT_CONNECTIVITY/IoT_5G_ERA_GSMA_PAREGLIO.pdf, stran 10

Andrej Kranjčević je diplomiral na Fakulteti za elektrotehniko v Ljubljani. Leta 2009 se je zaposlil v družbi Mobitel d.d., danes pa je na Telekomu Slovenije d.d. vodja raziskovalnih in razvojnih projektov v razvoju tehnologije.

Marjan Muršec je diplomiral na Fakulteti za matematiko in fiziko v Ljubljani. Leta 1997 se je zaposlil v družbi Mobitel d.d., danes pa je na Telekomu Slovenije d.d. vodja razvoja in načrtovanja radijskih komunikacij.

Mobilni internet stvari

Božo Mišović, Andrej Souvent, EIMV, Ljubljana

Povzetek — V podporo nadalje širitve in razvoja področja Interneta stvari (IoT) je mobilna industrija razvila in standardizirala razrede namenskih mobilnih-celičnih tehnologij. Takšna mobilna omrežja IoT podpirajo naprave, ki zahtevajo širokopasovno pokrivanje, dolgo življenjsko dobo baterij in nizke cene, s poudarkom na varnosti in povezljivost tako v mestih kot zunaj njih.

Ključne besede — 2G, 3G, 4G, 5G, eMTC, LPWA, LTE-M, NB-IoT, 3GPP - različica 13

Abstract — To support further expansion and evolution of the Internet of Things (IoT) the mobile industry has developed and standardized a class of dedicated cellular technologies. These Mobile IoT networks support devices requiring broad coverage, a long battery life and low cost, yet secure, connectivity across both rural and urban locations.

Drawing on interviews with 24 mobile operators, this article outlines how LTE-M and NB-IoT networks are being rolled out around the world, what operators and their partners have learnt so far and what they plan to do next. It explains how the Mobile IoT is creating value in commercial settings, while outlining initial tariff plans and the availability of modules, chipsets and other equipment.

The contribution also provides an overview of the features of LTE-M and NB-IoT, which have been standardized by the 3rd Generation Partnership Project (3GPP) for use in licensed spectrum. Together, these technologies are enabling mobile operators to address a very wide range of potential use cases, ensuring customer choice and helping the IoT to flourish globally.

Keywords — 2G, 3G, 4G, 5G, eMTC, LPWA, LTE-M, NB-IoT, 3GPP-Release 13

I. UVOD

V prispevku so podane značilnosti naprav IoT, ki delujejo v omrežjih LTE-M in NB-IoT, so že standardizirane v 3GPP in so namenjene uporabi v licenčnih spektrih. Obe omenjeni tehnologiji omogočata mobilnim operaterjem, da lahko pokrijejo široko paleto storitev - uporabniških primerov (slika 1).

Slika 1: Nabor storitev IoT

Ta prispevek opisuje, kako so se omrežja LTE-M in NB-IoT začela uveljavljati po svetu, kaj so se mobilni operaterji in njihovi partnerji že morali naučiti in kaj imajo v planu v prihodnje.

Razloženo je tudi, kako so v mobilnih omrežjih ovrednotili postavitev komercialnih parametrov IoT, kot povzetek prvotnih planov, razpoložljivosti modelov, razvoja integriranih vezij in drugih naprav.

II. LONG TERM EVOLUTION FOR MACHINES (LTE-M)

Slika 2: Tehnologija LTE-M

LTE-M (ang. Long Term Evolution - Machine) je poenostavljen naziv za tehnologijo eMTC (Enhanced Machine-Type Communication) LPWA (Low Power Wide Area), ki je je standardizirala organizacija 3GPP.

Bolj natančno je specificirana kot tehnologija LTE CatM1, ki je načrtovana za podporo IoT.

LTE-M je široko-prostorna tehnologija majhnih moči (LPWA), majhne kompleksnosti in podaljšanega pokrivanja (glede na klasično pokrivanje LTE), ki deluje na obstoječih baznih postajah LTE.

Opisana tehnologija omogoča delovanje naprav z življenjsko dobo baterij do 10 let, v raznolikih primerih uporabe, ki ceno modema zmanjša od 20 do 25 % glede na klasične modeme EGPRS. LTE-M lahko podpira relativno hitre prenose, mobilnost, gostovanje (ang. roaming) in govorne storitve VoIP/VoLTE.

Tehnologijo LTE-M podpira večina mobilnih naprav. Tovarniško podprte *chipsete* in module podpirajo javna mobilna omrežja naslednjih generacij: 2G, 3G in 4G.

Tehnologija vsebuje ustrezne varnostne mehanizme in funkcije, ki so značilne za mobilna omrežja, kot so podpora zaupnosti uporabniške identitete, avtentikacija, integriteta podatkov in identifikacija mobilnih naprav, uporabnih v javnih službah, prenosnih sistemih in industriji.

Komercialno naj bi bila omrežja LTE-M omogočena že v tem obdobju.

III. NARROW BAND – INTERNET OF THINGS (NB-IOT)

Slika 3: Tehnologija NB-IoT

NB-IoT (ang. Narrow Band Internet of Things) je tehnologija, ki jo je standardizirala organizacija 3GPP. Gre za naprave majhnih moči (tehnologijo LPWA), ki omogočajo široko razprostrto pokrivanje za nove naprave in storitve IoT. NB-IoT minimizira porabo povezanih naprav, povečuje sistemsko kapaciteto in spektralno učinkovitost, še posebej na lokacijah, ki omogočajo pokritost z mobilnimi celičnimi tehnologijami. Povezljive naprave NB-IoT ohranjajo, v širokem spektru uporabe, življenjsko dobo baterij tudi več kot 10 let.

NB-IoT uporablja novi fizični nivo s signali in kanali, ki lahko demantirajo zahteve širokega pokrivanja ruralnih področji, ter globino pokrivanja znotraj objektov, z uporabo zelo majhne kompleksnosti naprav. Tehnološko so naprave NB-IoT bolj enostavne v primerjavi z obstoječimi moduli GSM/GPRS, kar zelo zmanjša njihovo ceno. Glede na povečan interes se cena hitro zmanjšuje.

Tehnologija NB-IoT je podprta večinoma v vseh mobilnih napravah, ki uporabljajo mobilna omrežja 2G, 3G in 4G. Podprta je tudi z ustreznimi varnostnimi mehanizmi ter ostalimi lastnostmi mobilnih omrežij, kot so podpora zaupnosti uporabniške identitete, avtentikacija, integriteta podatkov in identifikacija mobilnih naprav, uporabnih npr. v aplikacijah za pametno parkiranje, javnih službah, prenosnih sistemih in industriji.

Komercialno so bila omrežja NB-IoT omogočena že v letu 2018.

IV. PRIMERJAVA TEHNOLOGIJ NB-IOT IN LTE-M

	NB-IOT	LTE-M
Bandwidth	180 KHz 3GPP Licensed	1.4 MHz 3 GPP Licensed
Peak data rate	<100	384 Kbps
Uplink / Downlink speed	27.2 / 62.5 Kbps (DL / UL)	Up to 1 Mbps
Latency	1.5 - 10 sec.	50 - 100 ms.
Battery life	+ 10 years (depending on the use case)	10 years (depending on the use case)
Power consumption	Best at low data rates	Best at medium rates
Cost per module	5 - 10 dollars	10 - 15 dollars
Frequency deployment	Flexible	In LTE band
Penetration in indoors	Excellent	Good
Voice	No	Yes. VoLTE

Slika 4: Primerjava tehnologij NB-IoT in LTE-M

Mobilne tehnologije (2G/3G/4G/5G), ki se uporabljajo tudi za dostop do interneta, so del IoT zgodbe, v kateri imajo svoj delež ustrezno pripravljene naprave LPWAN, tipa; LTE Cat-1, LTE-M in NB-IoT z namenom zmanjšanja porabe in cene prenosa podatkov po tipalu/napravi.

V. ZAKLJUČEK

Najnovejši dosežki razvoja na področju interneta stvari so vključeni v zadnjo generacijo mobilnega omrežja 5G. Slednja ima možnost uporabe velikih hitrosti (10 Gb/s in več) in zelo majhne zakasnitve (3 do 4 ms, URLLC 1 ms) za aplikacije IoT, kot so npr. UHD TV (4K), avtonomna vozila ali droni,aplikacije navidezne/obogatene resničnosti (VR/AR) in drugo.

Božo Mišović je rojen v Ljubljani leta 1952. Fakulteto za elektrotehniko v Ljubljani, smer telekomunikacije, je končal leta 1977. Prvo delovno razmerje je nastopil leta 1976 v podjetju Iskra Elektrozveze, kjer je deset let delal na področju domače proizvodnje naprav za podatkovni prenos – modemov. V času tržne transformacije podjetij je pomagal pri ustanovitvi podjetja SMARTCOM, kjer je bil tehnični direktor in nadaljeval deset let v podjetju SRC.SI, kot vodja programa za WAN-komunikacije. Nato se je zaposlil v podjetju MOBITEL kot tehnični strokovnjak, kjer je uvajal tehnologije GPRS/UMTS/HSPA/LTE za končne uporabnike. Leta 2015 je zaključil delo v Telekom. Sedaj dela kot zunanji svetovalec EIMV. Je aktiven predavatelj na številnih dogodkih s področja podatkovnih komunikacij.

Andrej Souvent je diplomiral in magistriral na Fakulteti za elektrotehniko Univerze v Ljubljani. Zaposlen je na Elektroinštitutu Milan Vidmar, kjer vodi Oddelek za vodenje in delovanje elektroenergetskih sistemov. Je član organizacij IEC, IEEE, CIGRÉ, SIST in Inženirske zbornice Slovenije. Ima več kot 20 let izkušenj na področju informacijskih tehnologij, sistemov vodenja in procesne informatike, predvsem za podjetja splošne in elektro-energetike. Področje njegovega dela so sistemi nadzora in vodenja elektroenergetskih sistemov, koncepti, tehnologije in rešitve pametnih elektroenergetskih omrežij, procesna informatika in integracija sistemov.

Critical Machine Type Communication in 5G Networks

Benedek Kovács, Ericsson Hungary, Budapest

Abstract — This article presents a few examples of critical machine type communication in 5G networks. Typical use cases for critical machine type communication will be introduced and then it will be explained how 5G networks will enable these. The first use case presented is related to automotive and will describe the problem of high bandwidth uplink V2X data. The second use case is related to de-wiring the factories and explaining basics of 3GPP Ultra Reliable Low Latency Communication. The third use case that will be discussed in detail explains how machine intelligence and neural networks will be enabled in 5G networks and support digital environments with Edge Computing.

Keywords — 5G, IoT, Artificial Intelligence, Edge Computing

I. INTRODUCTION

5G Mobile Networks currently under development promise low latency and high bandwidth enabling the 4th industrial revolution, the digital transformation for industries, cities, infrastructure and for the everyday life. However, it is also a common opinion that most of the imagined use cases can be served and implemented using wireless technologies of today such as 4G, WiFi, Bluetooth, etc. In the present article we present some use cases that would be very challenging to implement using existing technologies and will emphasize the key features in 5G that enable these challenging use cases. According to this paper, critical IoT use cases cover all use cases where reliability, latency or security is critical or if the failure of the use case would result in harm in human, expensive infrastructure or would result in critical loss of business.

Three main use cases will be introduced:

1. The automotive industry is introducing new mobility services that place high demands on network capacity due to the extreme amount of data that must be transported to and from highly mobile devices, often with near-real-time characteristics. Data needs to be transported within a limited time window (~30 min/day), with a varying geographical concentration of vehicles using a multitude of different network technologies and conditions.
2. The 4th industrial revolution is happening and one of the major steps to be taken is the total digitalization of factories. The challenge today is that even at evolved production sites there are diverse systems installed. It is still wire that connects programmable logic controllers to robotic arms at a production chain while radio technologies are being experimented for production monitoring, logistics and communication today. Therefore, a major challenge is to remove the wires and introduce an ultra-reliable very low latency communication that can meet the demanding requirements of these cyber physical systems.
3. One driver of 5G mobile networks is consumer media, where high definition, 4K and 8K video will dominate bandwidth consumption. Augmented reality, holographic calls and virtual reality are applications existing today but the full potential will be exploited using by high bandwidth 5G system. Many of these systems will be used for use cases like transport safety, augmentation of engineering, etc. and therefore considered critical not only in their field of application but also by latency. These applications utilize the power of artificial intelligence (e.g. for image recognition) which requires high computation capacity and low latency. The computational power needed for artificial intelligence will not drop even with the development of purpose build hardware chipsets, rather it will enable a wider usage and therefore cloud based implementation of server backend will be used (not only for cooperating systems). On the other hand, we cannot challenge the law of physics (speed of light) and therefore the execution shall be close to maintain low latency. As an answer to these challenges, edge computing is heavily discussed in the industry and will be introduced in 5G networks.

In Section II we will describe the automotive use case and formulate the challenges and the requirements on the 5G network. Section III introduces the industrial use case characteristics and describes what technologies will be used to provide implementation for these. Section IV discusses the use case of digital environment and 5G support for edge computing.

II. AUTOMOTIVE USE CASES

This section is based on the article “Distributed cloud – a key enabler of automotive and industry 4.0 use cases” [1].

According to market forecasts, the global number of connected vehicles will grow to approximately 700 million by 2025 and the data volume transmitted between vehicles and the cloud will be around 100 petabytes per month. Gartner recently raised the expectations further in its report from June 2018, estimating the volume to be as high as one terabyte per month per vehicle [1]. Such massive amounts of data will place new demands on the radio network, as the main part is UL data.

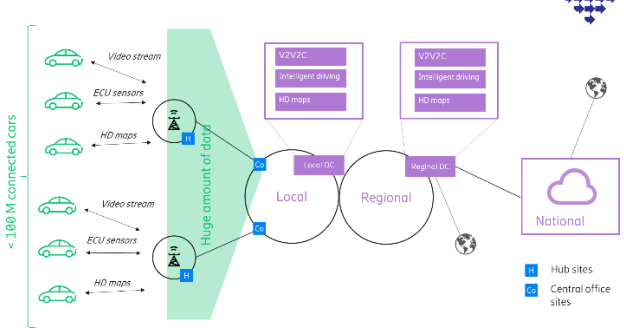


Figure 1: Uplink data and edge analytics for automotive use cases

As explained in the AECC (Automotive Edge Computing Consortium) white paper [2], optimizations are required for the uplink data based using network edge analytics (see Figure 1.) One of these optimizations is edge computing and analytics services on the network edge.

III. INDUSTRIAL NETWORKING

It is digitalization that drives the 4th industrial revolution which in general means the convergence between the IT and Operations with automation of operations. Systems are introduced to control and monitor production and logistics processes. Communication of components is a fundamental part of these systems. There are multiple communication technologies installed in a typical state-of-the art or experimental production sites of today.

1. Especially for critical situations *4G/3G mobile network* services are used to manage human to human communication, for example Mission Critical Push to Talk.
2. *WiFi* is often used as a primary access to company data, databases and some sensors may also communicate using the industrial version of it.
3. Other radio technologies such as *Bluetooth, LoRa, Sigfox* and sometimes *NB-IoT* are used to connect sensors and devices.
4. Regular *IT wiring* is used for safety systems and cameras.
5. Profinet is a common solution for connecting Programmable Logic Controllers.

The challenge the industry digitalization faces is to select an optimal yet consolidated set of access technologies that are integrated in order to provide a manageable production environment. We envision that the network of the future factories is built using a combination of broadband 5G, critical 5G based on 5G NR and NB-IoT wireless access technologies served by a common single core network technology providing security, authentication, quality of service and the necessary mobility, communication and platform features.

The typical day of the worker of tomorrow may look something like this:

She receives the call from the company that predictive analytics on production chain Alpha at Atlantis factory site II fails. After preliminary analysis she decides to examine the industrial robot on site, using AR glasses and augmented operational data. She is able to access operation information of a particular instalment (and not others) in a secure way. She is able to seamlessly connect to secure network to run some diagnosis and propose and immediate re-configuration of the production chain. The reconfiguration would be managed by her engineering colleague in the company remote central office who overview the completed production system. Then the robot is replaced by another with no manual interaction and production continues in a safe way.

In the next two sub chapters we present the current situation and then discuss some 5G technologies that might help to improve towards the visionary situation.

A. *De-wiring the industry sites*

A main use case for de-wiring an industrial site is to remove the expensivae cables that connects industrial robots with control machines and control centres.

Today Profinet [3] is a commonly used technology to connect a robotic arm to a controller. Even if the industry trend is going towards the commoditization of Profinet with technologies like Time Sensitive Networking (TSN) using Ethernet, the costs of installation and reconfiguration of such systems is significant and shall be reduced to make production environment flexible. Deterministic networks today are defined at both Layer 2 and Layer 3 by IEEE and IETF, while, in a cellular 5G network context, TSN may be considered as a control layer over end-to-end Ultra Reliable Low Latency Communication (URLLC) [4].

These deterministic networking technologies require L2 and L3 features that are only available as an overlay with 4G or WiFi technologies. However, 5G Next Generation Radio (5G NR) standard will support ethernet bearers and there is a package for Ultra Reliable Low Latency Communication (see e.g. [5]) under standardization that will enable 5G to meet the requirements of deterministic networking.

Key features of the Ultra Reliable Low Latency Communication include e.g. Frame Replication and Elimination. This feature requires n+1 physically disjunct paths between the communicating parties which implies that there is a redundancy in the mobile communication network starting from the modem to the network service point. Another difficult problem is clocks synchronization (IEEE802.1AS, [6]) and enabling scheduled traffic for quality of service and bandwidth guarantee (802.1Qbv [7]).

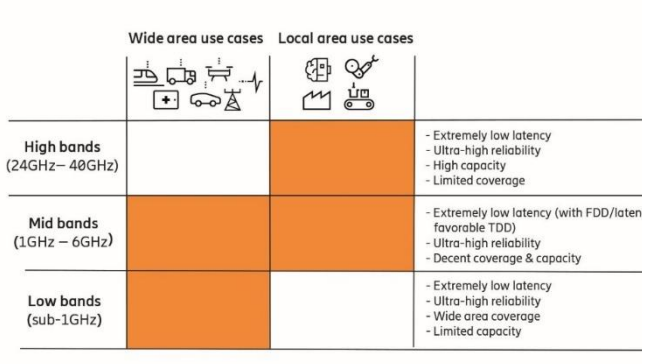
B. *Next generation radio*

Another problem area is to identify the right radio access configuration. This subchapter is based on the Ericsson Review Article on Cellular IoT Evolution for Industry Digitalization [4].

NR Frequency Division Duplex (FDD) achieves extremely low latencies and ultra-high reliability with large coverage areas per base station because of favourable radio wave propagation. However, the channel bandwidths are limited in the low bands and therefore these bands should primarily target wide area users.

For unpaired spectrum allocations in the mid bands, NR Time Division Duplex (TDD) achieves ultra-high reliability with advanced antenna solutions. However, it may not be possible to achieve extremely low latencies with a downlink-heavy static TDD transmission pattern typically optimized for downlink-heavy enhanced Mobile broadband (eMBB) traffic. For certain localized deployments such as factories with sufficient isolation, a low-latency favourable transmission pattern can be a viable option. In the high frequency mmWave bands, NR TDD achieves extremely low latencies with its ultra-short transmission capability.

NR provides a great degree of freedom to optimize these trade-offs. 3GPP Rel-15 evaluations have already confirmed that the NR radio-interface can deliver a small sized message with 99.999% reliability within a 1 ms latency bound in both uplink and downlink. 3GPP Rel-16 is further evaluating 99.9% to 99.9999% reliabilities within 1ms to 7 ms latency bounds at various data rates from Kbps to Mbps.



Picture 2: 5G NR Trade-offs for low latency, coverage and capacity

IV. EDGE COMPUTING AND ARTIFICIAL INTELLIGENCE USE CASES

Digital infrastructure and environment are emerging due to a wide range of technologies already available and under development. A waste number of connected devices and sensors are being installed such as remote monitoring of power consumption, connected street lamps etc. These isolated solutions contribute to our digital environment where machine to machine communication is just as important as human to machine a.k.a. cyber physical systems.

A. Example: The Internet of eyes use case

The typical mobile applications used today have components on the client and server side. The server components are either deployed at private locations and private cloud or at public web scale data centers such as Amazon, Azure and Google cloud, etc…

The Internet of Eyes use case is designed to demonstrate a typical edge computing application. Multiple cameras are streaming high definition video uplink to the central component of the application that is able to detect events like movements, objects and estimate the position of the moving objects creating the digital environment. Actuators might react on the observations immediately but in our case we have implemented an augmented reality service that can track objects in a real time. Sensor actuation might be useful to intercept in critical situations such as accidents in an intersection since the cameras are able to see objects that may be out of site for others. In the most popular example a car approaches the intersection and signals the driver that there is a bicyclist coming from a non-visible area.

Main components of the system:

a) Data source (cameras) streaming high definition video continuously using RTP with GStreamer.

b) Video processing with OpenCV for to decrease the noise in the video stream and to detect movements.

c) Object recognition, inference with a neural network using TensorFlow. Teaching the neural network is a lengthy process and thus executed in central data centers while inference is done at the network edge using GPU HW acceleration. However, even with GPU HW acceleration, inference is a complex method and therefore the component with the highest latency in the system.

d) Position estimation: possible if at least two cameras identify the same object.

e) Reaction in our basic example is to stop a model train to avoid collision, so latency is a key.

This use case requires central cloud for training the network but a powerful local edge cloud to run application components that are both latency critical but require high capacity so running on the devices is not feasible or would consume too much batter and produce heat.

B. Edge computing for critical applications

Modern 4G networks are built using a centralized core network, local breakout is difficult to configure and limited in functionality. A typical middle European operator has one or two central datacenters where 3rd party applications may also be installed. Since Amazon and other web scales operate a few large datacenters worldwide only therefor the packets has to travel a significant distance to reach the application. If we are to deploy an application with low latency requirement then we have to take into account physical limits. Light with the wavelength of 1310 nm on a commonly used Brand B (G.652) fibre travels with speed of 489.34µs/100km [8]. The closest datacenter of Amazon (in Western Europe) may be reached in 20 ms from Slovenia or Hungary without taking any bit error, switches or routers into account. The typical delay of commonly used network nodes is around 1 ms. Typical country level data centers can be reached around 50 ms in 4G networks. (This data is an average and may be significantly influenced by the exact location, the quality of the access channel and the purpose of usage.) This implies that the typical augmented reality applications with a maximum latency requirement of 10-30 ms where the network contribution should be even below needs an application component deployed closer to the end devices. This is the technology we call *edge computing* enabled by distributed cloud infrastructures providing virtualization environments on the network edges with high level of automation.

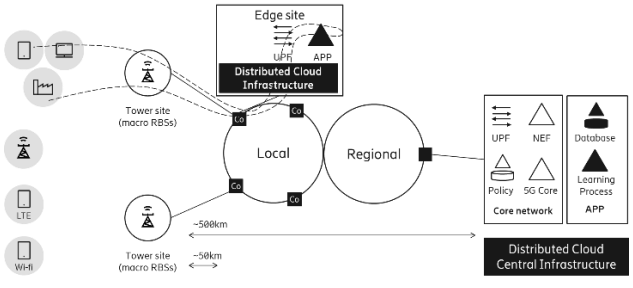


Figure 2: Edge computing: the application components with critical response time are deployed on the network edge depicted by a dashed line. Distributed cloud: the management and orchestration of the edge site is integrated party of the cloud infrastructure

Figure 2 describes how an edge computing application will be deployed in 5G networks with distributed cloud. Potential deployment options for the HW infrastructure of the edge networks can be different based on network structure and availability. The most typical deployments will be the existing telecommunication sites e.g *Central office*s (Co) on city level. The typical size of such a small cloud is 5-25 pizza box server capacity. Due to the limited resources available,

management and monitoring functionalities are supposed to be lightweight. According to opensource projects like Linux Foundation Edge, Akraino [9] these sites will provide similar IaaS environments as the central cloud (VM and Container) combined with some PaaS elements. It will provide runtime environment for both Virtual Network Functions (VNFs) for the 5G networks e.g. User Plane Function for local breakout and applications or application platforms developed by 3rd parties.

3GPP improves *local breakout* functionality in 5G to make sure that the right application data gets connected with the right application on the network edge. It also adds flexibility to switch the traffic between edge sites and the central locations and adds flexibility to provide additional edge services defined in the standard as *flexible mobile service steering*. A simple uplink video might skip *deep packet inspection* (DPI). The services of *User Plane Function* may be distributed across edge sites (e.g. depending on HW availability) and be provided as a service chain according to the definition in 3GPP *flexible mobile service steering*.

The *5G Core* network is responsible for most of the services above radio access such as security, authentication, mobility management, location services and all the mentioned packet processing capabilities. The *5G Core* network architecture is significantly different from 4G *Evolve Packet Core*. All network nodes are implemented as so-called Virtual Network Functions specified by ETSI Network Function Virtualization and 3GPP designed the architecture using the *service oriented architecture* principle. The *5G Core* architecture is therefore referred as *service based architecture* where the aim is improved flexibility and programmability. A special element of this is the *Network Exposure Function* that exposes service interfaces internally and externally for trusted 3rd party applications. This exposure is a key element of edge computing since it provides higher level of automation by enabling 3rd party applications to configure the network directly. One of these configuration options is *application influence on traffic routing* that sets up the local breakout on the network edge but also allows the configuration of *flexible mobile service steering* services. It provides a rest API based on HTTP.

One of the central questions of edge computing applications is the optimal selection of locations for module runtimes. Simple applications might use static configurations but in the future applications will use intelligent optimization systems to determine their distribution of modules e.g. for cost saving reasons while keeping the user experience high. Such algorithms are discussed in [10].

V. CONCLUSIONS AND TAKE AWAY

The 5G networks under development - including not only the 5G radio (5G NR) but also the corresponding Ultra Reliable Low Latency Communication, Core Network and virtualization, Edge Computing standard - will be able to provide the infrastructure for digitalization enabling the 4th industrial revolution, significant revolution of automotive and transportation, cyber physical systems and our digital environment.

The motivation may be critical by economical just as it is described in the case of high bandwidth uplink video for automotive, can be security, latency and reliability critical in extreme cases such as manufacturing or application in critical infrastructure situations and for user experience of augmented reality and virtual reality applications. Edge computing is a key enabler making artificial intelligence applications feasible on 5G networks with enabling application workload on the network edge. 3GPP 5G standard is developed in a way that it supports all kinds of edge computing requirements.

ACKNOWLEDGMENTS

The author would like to acknowledge the colleagues he is working with in Ericsson worldwide, Budapest University of Technology and Economics (BME), Eötvös Lóránd Science University (ELTE) and EIT Digital.

LITERATURE

[1] Malgorzata Svensson, Christofer Boberg, Benedek Kovács, Distributed cloud – a key enabler of automotive and industry 4.0 use cases, Ericsson Technology Review, 2018, https://www.ericsson.com/en/ericsson-technology-review/archive/2018/distributed-cloud

[2] AECC White Paper, 2017, https://aecc.org/home/whitepaper/

[3] Profinet, Wikipedia, https://en.wikipedia.org/wiki/PROFINET

[4] Ali Zaidi, Yasir Hussain, Marie Hogan, Christian Kuhlins, Cellular IoT Evolution for Industry Digitalization, 2019, https://www.ericsson.com/assets/local/trends-and-insights/consumer-insights/reports/wp_evolving-iot-forindustrialdig_jan-312019_revised.pdf

[5] 3GPP TS 38.824, Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3498

[6] IEEE802.1AS, https://www.deterministicethernet.com/time-synchronization

[7] IEEE802.1Qbv, http://www.ieee802.org/1/pages/802.1bv.html

[8] Calculating Optical Fiber Latency, K. Miller, 9 Jan 2012, M2 optics inc., http://www.m2optics.com/blog/bid/70587/Calculating-Optical-Fiber-Latency

[9] Linux Foundation Edge, Akraino, https://www.lfedge.org/projects/akraino/

[10] A. Reale, Kiss P., C. Ferrari, Kovacs B., Szilagyi L., Toth M., "Application Functions Placement Optimization in a Mobile Distributed Cloud Environment", In: Studia Informatica, no 2, pp. 37-52, 2018, http://www.studia.ubbcluj.ro/arhiva/cuprins_en.php?id_editie=1155&serie=INFORMATICA&nr=2&an=2018

Benedek Kovács joined Ericsson in 2005 as a software developer and tester, and later worked as a system engineer. He was the innovation manager of the Budapest R&D site 2011-13, where his primary role was to establish an innovative organizational culture and launch internal startups based on worthy ideas. Kovács went on to serve as the characteristics, performance management and reliability specialist in the development of the 4G VoLTE solution. Today he is working on 5G networks and distributed cloud, as well as coordinating global engineering projects. He holds an M.Sc. in information engineering and Ph.D. in mathematics from the Budapest University of Technology and Economics in Hungary.

Ugotavljanje skladnosti naprav z vgrajenim radijskim oddajnikom

Andrej Škof, Slovenski institut za kakovost in meroslovje, Ljubljana

Povzetek — Članek opisuje postopek ugotavljanja skladnosti z evropsko Radijsko direktivo 2014/53/EU za elektronske naprave, ki vsebujejo radijski oddajnik ali sprejemnik.

Ključne besede — Direktiva 2014/53/EU, radijski modul, radijski oddajnik, radijski sprejemnik, kombinirana naprava, CE oznaka, EMC direktiva 2014/53/EU

Abstract — This article explains how to show compliance of electronic devices with integrated radio module with European Directive 2014/53/EU.

Keywords — Directive 2014/53/EU, radio module, radio transmitter, radio receiver, combined equipment, CE marking, EMC directive 2014/53/EU

I. UVOD

V zadnjih letih se množično povečuje število elektronskih naprav, ki imajo vgrajen radijski modul (npr. gospodinjski aparat z vgrajenim WiFi oddajnikom), vendar njihova primarna funkcija ni radijska komunikacija. Vgradnja takšnega modula lahko v določenih primerih vpliva na primarno funkcijo elektronske naprave, prav tako pa lahko sama naprava vpliva na parametre radijskega modula in posledično na njegovo skladnost z evropsko *Radijsko direktivo 2014/53/EU* kot tudi na skladnost celotne naprave z *EMC direktivo 2014/30/EU*.

V trenutku, ko se proizvajalec odloči, da bo svoji napravi dodal radijsko funkcijo, se zahteve ugotavljanja skladnosti za te naprave spremenijo. Zaradi radijske komunikacije mora naprava ustrezati zahtevam evropske *Radijske direktive 2014/53/EU*, ki pokriva vse elektronske naprave, ki sprejemajo in/ali oddajajo radijske valove za namene radijske komunikacije ali radijske determinacije. Osnovni namen radijske direktive je zagotavljanje učinkovite rabe radijskega spektra in preprečitev škodljivega motenja [1].

Treba je poudariti, da radijska direktiva ne pokriva samo učinkovite rabe radijskega spektra, ampak zahteva, da radijska naprava zagotavlja [1]:

- varovanje zdravja ter varnosti ljudi in domačih živali ter zaščite premoženja, vključno s cilji v zvezi z varnostnimi zahtevami iz *Direktive 2014/35/EU*, vendar brez uporabe napetostne meje;
- ustrezno raven elektromagnetne združljivosti iz *Direktive 2014/30/EU*;
- Radijska oprema iz določenih kategorij ali razredov je izdelana tako, da izpolnjuje naslednje bistvene zahteve:
  (a) radijska oprema medsebojno deluje z dodatno opremo, zlasti z univerzalnimi polnilniki;
  (b) radijska oprema prek omrežij medsebojno deluje z drugo radijsko opremo;
  (c) radijsko opremo je mogoče povezati z vmesniki ustreznega tipa po vsej Evropski uniji;
  (d) radijska oprema ne škoduje omrežju ali njegovemu delovanju ter ne zlorablja sredstev omrežja in s tem povzroča nesprejemljivo poslabšanje storitev;
  (e) radijska oprema ima vgrajeno zaščito za zagotavljanje varstva osebnih podatkov ter zasebnosti uporabnikov in naročnikov;
  (f) radijska oprema podpira določene funkcije za zaščito pred goljufijami;
  (g) radijska oprema podpira določene funkcije za dostop do storitev reševanja;
  (h) radijska oprema podpira določene funkcije, ki invalidom olajšujejo uporabo;
  (i) radijska oprema podpira določene funkcije, ki zagotavljajo, da se v radijsko opremo lahko naloži programska oprema, kadar je kombinacija radijske opreme in programske opreme dokazano skladna.

Ker se *Radijska direktiva* v členu 3.1.a sklicuje na *Nizkonapetostno direktivo 2014/35/EU* brez napetostne meje, to pomeni, da je treba preveriti tudi skladnost vseh naprav, ki delujejo pod 50 V in nad 1.000 V za izmenični tok, ter pod 75 V in nad 1.500 V za enosmerni tok. V realnosti to pomeni velik vpliv na postopek ugotavljanja skladnosti za baterijsko napajanje naprave in naprave, ki so tipično napajane z enosmerno napetostjo 5 V ali 12 V. Pred vgradnjo radijskega modula te naprave ne spadajo v obseg *Direktive 2014/35/EU*.

Poudariti je treba, da *Direktiva 2014/35/EU* pokriva tudi zahteve vezane na omejevanje izpostavljenosti ljudi elektromagnetnim sevanjem. Če je namen uporabe elektronske naprave z radijsko komunikacijo neposredno na osebi ali njeni bližini, ne smemo pozabiti tudi na zahteve tega dela direktive.

Velika večina zahtev, ki izhajajo iz člena 3.3 *Direktive 2014/53/EU* ni delegiranih in zato za te točke ni specifičnih zahtev [3]. Izjema je točka 3.3.g, ki se nanaša na radijsko opremo, ki podpira določene funkcije za dostop do storitev reševanja. Primer take opreme so plazovne žolne.

II. POSTOPKI UGOTAVLJANJA SKLADNOSTI

Ko imamo napravo, ki ima radijsko funkcijo, ugotavljamo skladnost po zahtevah Radijske direktive. Ne glede na pomembnost radijskega modula in njegovo vlogo v elektronski napravi, se postopek ugotavljanja skladnosti izvede po *Radijski direktivi*. Če je narava produkta takšna, da spada pod obseg več direktiv, npr. *Strojne direktive* ali

Direktive o medicinskih pripomočkih, je treba izvesti tudi vse postopke ugotavljanja skladnosti vezanih na ti direktivi.

Radijska direktiva predvideva dokazovanje skladnosti z bistvenimi zahtevami po treh poteh [1]:

- notranja kontrola proizvodnje;
- EU-pregled tipa, ki mu sledi skladnost s tipom, na podlagi notranje kontrole proizvodnje;
- skladnost na podlagi popolnega zagotavljanja kakovosti.

A. Notranja kontrola proizvodnje

Kadar se proizvajalec odloči za dokazovanje skladnosti z notranjo kontrolo proizvodnje - modula A za ugotavljanje skladnosti - mora pripraviti tehnično dokumentacijo in zagotoviti, da s proizvodnim procesom in njegovo kontrolo zagotovi skladnost radijske opreme. Tehnična dokumentacija mora vključevati vse pomembne podatke, ki so pomembni za zagotavljanje skladnosti. Ena izmed pomembnejših vsebin tehnične mape je seznam uporabljenih harmoniziranih standardov in poročila o preskusih. Poročila, ki izkazujejo skladnost proizvoda s harmoniziranimi standardi služijo kot osnova za izjavo o skladnosti, ki jo izda proizvajalec na lastno odgovornost in s katero zagotovi, da njegova naprava izpolnjuje bistvene zahteve *Radijske direktive*. Proizvajalci se, če je to le mogoče, večinoma odločijo za ugotavljanje skladnosti po modulu A, ker je ta postopek najenostavnejši. Če proizvajalec pri ugotavljanju skladnosti ne uporabi harmoniziranih standardov, jih uporabi samo delno, ali pa primerni standardi še ne obstajajo. Za ugotavljaje skladnosti ni mogoče uporabiti postopka notranje kontrole proizvodnje.

B. Postopek EU-pregled tipa

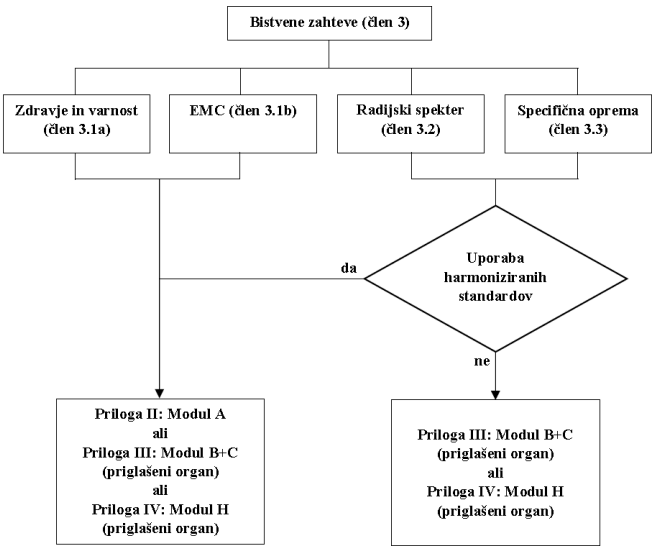
V postopku EU-pregled tipa - modul B za ugotavljanje skladnosti - priglašeni organ pregleda tehnično zasnovo radijske naprave na podlagi dokumentacije in dokazil. Tukaj so pomembna predvsem dokazila o ustreznih tehničnih rešitvah, če niso bili uporabljeni harmonizirani standardi. Če priglašeni organ ugotovi skladnost z *Radijsko direktivo*, izda certifikat o EU-pregledu tipa. Proizvajalec izvede vse potrebne ukrepe, da proizvodni proces in njegovo spremljanje zagotovita skladnost proizvedene radijske opreme z odobrenim tipom, opisanim v certifikatu o EU-pregledu tipa, in z zahtevami iz te direktive, ki zanjo veljajo (modul C za ugotavljanje skladnosti) [1].

C. Popolno zagotavljanje kakovosti

Redkeje pa se proizvajalci odločijo za postopek dokazovanja skladnosti na podlagi popolnega zagotavljana kakovosti - modul H ugotavljanja skladnosti.

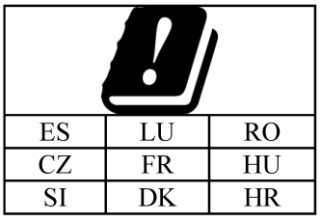
V tem postopku proizvajalec uporablja odobren sistem kakovosti za oblikovanje, proizvodnjo, končni pregled in preskušanje zadevne radijske opreme ter je nadzorovan s strani priglašenega organa. Priglašeni organ opravlja redne revizije, da ugotovi, če proizvajalec vzdržuje primeren sistem kakovosti. Priglašeni organ lahko izvede tudi nenapovedane obiske.

Na vsako napravo, ki je v skladu z Radijsko direktivo, proizvajalec namesti CE oznako in za vsako napravo sestavi pisno izjavo EU o skladnosti.



Slika 1: Postopki dokazovanja skladnosti z direktivo 2014/53/EU [3]

V primerih, ko za radijsko napravo obstaja omejitev uporabe v določeni članici Evropske unije (slika 2), je treba na embalažo proizvoda dodati opozorilo in v navodilih za uporabo razložiti, za kakšno omejitev gre. Primer take omejitve je 5G WiFi, ki se sme uporabljati samo v notranjih prostorih.



Slika 2: Piktogram za pritrditev na embalažo v primeru omejitve uporabe radijske naprave [3].

III. KOMBINIRANE NAPRAVE

Z razvojem novih tehnologij in željo po čim večji medsebojni povezljivosti naprav je na tržišču vedno več naprav, katerih osnovna funkcija ni radijska komunikacija, vendar se jim vseeno doda radijski modul in s tem omogoči večjo funkcionalnost, npr. pralni stroj z vgrajenim modulom WiFi. Za neko napravo rečemo, da je kombinirana naprava, ko je sestavljena iz vsaj dveh delov, pri čemer je vsaj en del naprave radijski in vsaj en del ne radijski [4]. Zaradi specifike kombiniranih naprav je ETSI (European Telecommunications Standards Institute) pripravil nov standard EMC *ETSI EN 303 446-1*, ki podaja zahteve za preskušanje elektromagnetne združljivosti kombiniranih naprav. Čeprav standard še ni bil dokončno potrjen in je na voljo samo osnutek standarda, se v praksi po njem že izvaja preskušanje EMC kombiniranih naprav. Razlog, da se že uporablja, čeprav še ni na seznamu harmoniziranih standardov je v tem, da do zdaj ni bilo standarda, ki bi pokrival tovrstne naprave. Leta 2016 je bilo sicer izdano vodilo *ETSI TG 203 367 V.1.1.1* kot pomoč pri uporabi harmoniziranih standardov po zahtevah *Radijske direktive* za pokritje zahtev iz točk 3.1b ter 3.2., vendar gre v tem primeru samo za vodilo in ne standard. Če se proizvajalce drži zahtev standarda *Draft ETSI EN 303 446-1* priglašeni organ potrdi skladnost produkta za tisti del, ki ga pokriva standard.

Pri kombiniranih napravah je treba biti pri preverjanju skladnosti EMC pozoren na dva vidika:

– Na funkcijo naprave, ki spada pod *ne radijski del* (npr. predvajanje video vsebine, regulacija ogrevanja prostora, pomivanje posode). Skladnost tega dela naprave se preveri po ne radijskem standardu EMC, pod katerega spada naprava.
– Za *radijski del* naprave pa se preverjanje elektromagnetne združljivosti opravi po zahtevah standardov serije *ETSI EN 301 489-x*. Izbira standarda je odvisna od frekvenčnega pasu, v katerem deluje naprava. Če naprava to omogoča, je možno tudi simultano preskušanje radijskega dela in ne radijskega dela naprave.

IV. UPORABA CERTIFICIRANIH RADIJSKIH MODULOV

Zelo pomembna odločitev, s katero se mora spoprijeti proizvajalec kombinirane naprave je, ali bo uporabili že preverjen radijski modul, ki je v skladu z *Radijsko direktivo* in ima za to tudi ustrezna potrdila, ali pa bo sam razvil radijski modul in potem izvedel ustrezne postopke preverjanja skladnosti. Na odločitev vpliva kar nekaj dejavnikov, o katerih mora proizvajalec temeljito premisliti.

Prednosti uporabe certificiranega modula so:

- velik prihranek časa in denarja pri razvoju,
- preverjanja učinkovite rabe radijskega spektra ni treba izvesti ali pa se izvede samo delno,
- možnost uporabe radijskega modula v več produktih.

Na drugi strani pa uporaba že certificiranega modula prinaša tudi slabosti v primerjavi z razvojem lastnega modula:

- radijskega modula ni mogoče poljubno prilagoditi potrebam proizvajalca (zasnova, oblika, funkcije, oddajna moč, poraba),
- omejeno poznavanje delovanja modula,
- višja nabavna cena,
- v primeru potrebnih modifikacij modula zaradi sprememb standardov ali potreb proizvajalca odvisnost od proizvajalca modula,
- delovanje modula v gostitelju (naprava v katero je vgrajen radijski modul) ni takšno, kot je bilo predvideno.

Če naprava to dovoljuje, se večina manjših proizvajalcev odloči za uporabo že certificiranih radijskih modulov zaradi prihrankov pri stroških razvoja in omejenih kapacitet v razvoju.

Treba pa je biti zelo pozoren, ko imamo produkt, v katerega vgradimo več radijskih modulov, ki bodo delovali istočasno. Tudi, če se uporabi certificirane module, se le-ti lahko med sabo motijo in pride do slabšega delovanja, kot se je pričakovalo. Treba se je zavedati, da je bil vsak certificiran modul preskušan samostojno. V takih primerih je treba biti zelo pozoren, da produkt ne presega dovoljene oddajne moči, če delujejo moduli v skupnem frekvenčnem območju in na kakovost sprejema. Tudi, če radijski moduli delujejo v različnih frekvenčnih pasovih, lahko njihova majhna medsebojna oddaljenost negativno vpliva na kakovost sprejema.

Pri uporabi certificiranih modulov je treba natančno preveriti tudi karakteristike in omejitve, ki jih predpiše proizvajalec, npr. temperaturno območje delovanja, razred sprejemnika, oddaljenost od človeškega telesa. Če je kombinirana naprava namenjena nošenju na osebi, je treba preveriti, ali ima radijski modul določeno minimalno oddaljenost od človeškega telesa in je morda zaradi tega treba ponovno oceniti ali izmeriti izpostavljenosti ljudi elektromagnetnim sevanjem.

V. ZAKLJUČEK

Postopek dokazovanja skladnosti z zahtevami Evropske unije za naprave, v katere je vgrajen radijski modul, je opredeljen v *Radijski direktivi 2014/53/EU*. V primeru kombiniranih naprav je treba preveriti dva vidika - radijski del naprave in ne radijski del. Uporaba certificiranih modulov olajša postopke dokazovanja skladnosti, če je uporaba takšnih modulov možna in smiselna.

VIRI

[1] Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014
[2] Direktiva 2014/35/EU Evropskega parlamenta in Sveta z z dne 26. februarja 2014
[3] Guide to the Radio Equipment Directive 2014/53/EU, Version of 05 June 2018
[4] Draft ETSI EN 303 446-1 (V.1.1.0) (3-207): "ElectroMagnetic Compatibility (EMC) standard for combined and/or integrated radio and non-radio equipment; Part 1: Requirements for equipment intended to be used in residential, commercial and light industry locations Harmonised Standard covering the essential requirements of article 3.1(b) of Directive 2014/53/EU"

Andrej Škof je produktni vodja za preskušanje radijskih in medicinskih proizvdov v EMC laboratoriju v podjetju SIQ Ljubljana. Ima 11 let delovnih izkušenj z meritvami elektromagnetne združljivosti (EMC) in preskušanji radijskih modulov. Diplomiral je leta 2008 na Fakulteti za Elektrotehniko.

Merjenje ključnih parametrov naprav IoT

Mirko Ivančič, Amiteh, Ljubljana

Povzetek – Hitro naraščajoče število IoT, pogojeno z novimi tehnologijami in novimi priložnostmi na trgu, postavlja pred razvijalce in načrtovalce nove izzive tudi na področju preskušanja teh naprav v vseh korakih njihove poti, od zamisli do uporabnika. Članek poskuša osvetliti ključne izzive pri preskušanju naprav IoT.

Ključne besede IoT, merilni izzivi, merjenje porabe, simulacija baterije

Abstract — This article explains how to use a style that produces an article for the Proceedings of the workshops VITEL. Style is a good approximation to the style used in the IEEE Transactions. The article is itself an example of the VITEL_G_SVN.dotx style in action.

Keywords — template, MS Word, VITEL 2003

I. UVOD

V prihodnjih letih bodo napredek na področju računalništva (AI, Artificial Inteligence), komunikacij (5G NR, 5G New Radio), avtomatizacije naprav (IoT, Internet of Things) in avtomatizacije v industriji (IIoT, Industry IoT) pospešili hitrost sprememb in inovacij. V industriji bodo uporabljeni številni senzorji interneta stvari za avtomatiziran prenos podatkov in daljinski nadzor naprav. V dobi interneta vsega bo povezljivost postala običajna. Podjetje Gartner, Inc. napoveduje, da bo do leta 2020 v uporabi več kot 20 milijard naprav IoT, kar je bistvena rast v primerjavi z letom 2017, ko jih je bilo 8,4 milijarde.

Kmalu bo zaživela tehnologija 5G. V povezavi z napravami IoT bodo povečana pasovna širina, večja hitrost in nižje zakasnitve omogočile nastanek aplikacij, za katere smo nekoč menili, da niso mogoče. Teoretična največja hitrost 5G (10 Gb/s) in pričakovana 10-letna življenjska doba baterij za senzorje majhnih moči in naprav bosta zahtevali analizo in obravnavo velike količine podatkov. V obdobju interneta stvari in omrežij 5G bo treba preizkusiti številne nove proizvode, kar bo skupinam za raziskave in razvoj in njihovo preskusno opremo prineslo nove izzive.

V nadaljevanju si bomo ogledali, kakšni izzivi čakajo snovalce in načrtovalce novih naprav IoT, nekoliko bolj poglobljeno pa se bomo posvetili izzivom na področju ugotavljanja življenjske dobe baterij in s tem povezanim upravljanjem porabe.

II. IOT IZZIV ŠTEVILKA 1 - INTEGRITETA SIGNALOV IN MOČI

Integrirana vezja za mešane (analogne in digitalne) signale, ki lahko vključujejo senzorje/MEMS, kateri delujejo na sorazmerno nizki moči, pogosto uporabljamo pri načrtovanju naprav IoT. Izredno so dovzetna za presluhe. Vezja za distribucijo moči imajo običajno zelo majhne tolerance, kar poveča možnost, da valovitost in šum, ki se pojavita na močnostni zbiralki, negativno vplivata na uro (takt) in digitalne podatke. Majhna fizična struktura mnogih naprav IoT zahteva tudi, da so poti signalov visoke hitrosti zelo skupaj, kar povečuje možnost presluhov in sklopa.

Skrbno načrtovanje vezij lahko zagotavlja integriteto signala z ukrepi, kot so usmerjanje signalov od točke do točke, nadzor impedance povezav v vezju za distribucijo moči in na medsebojnih povezavah, ohranjanje kratkih povratni poti in skrb za ustrezen prostor med sosednjimi povezavami. Čeprav je pomembno upoštevanje naštetih dobrih načel oblikovanja vezij za doseganje zanesljive zasnove, je ključna predvsem možnost preskušanja električnega delovanja struktur, ki prenašajo signale v napravi.

Slika 1: Naprave IoT

Vektorski analizatorji vezij (VNA) so med najpogostejšimi orodji za opisovanje električnih lastnosti vsakega povezovalnega ali prenosnega voda. Z njimi lahko izmerimo pomembne značilnosti, ki vplivajo na celovitost signala, kot so vstavitveno slabljenje, slabljenje, odboji, presluhi in zakasnitve. Poleg tega imajo nekateri analizatorji (običajno z uporabo programske opreme) možnost meritev v časovnem prostoru in s tem impulznega odziva kanala.

Eno od najnovejših orodij, razvitih za analizo integritete moči, so sonde za močnostne zbiralke, ki omogočajo merjenje ultra nizkih šumov na močnostnih zbiralkah. Uporabljajo se z osciloskopom. Lastnosti teh sond so odvisne od proizvajalca, na splošno vključujejo:

– odmik (offset) do 60 V, ki zagotavlja, da je napetost močnostne zbiralke popolnoma prestavljen na zaslon osciloskopa;
– dinamično območje do 1 V;
– gigahertzne delovne pasovne širine, ki zagotavljajo, da visokofrekvenčni šum ne ostane neopažen;
– razmerje dušenja 1:1 za zmanjšanje šuma merilnega sistema;
– 50 kΩ impedanco za zmanjšanje obremenitve.

Izbira pravih orodij za zaznavanje težav z integriteto signala in moči je pomembna za ustrezno zaznavo in odpravljanje vzrokov slabega delovanja ter za potrditev resničnih zmogljivosti. VNA, sonde za močnostne zbiralke in osciloskopi so le nekatera orodja, ki so na voljo za doseganje tega cilja.

III. IoT izziv številka 2 - Skladnost z brezvrvičnimi standardi

Izbrani brezvrvični protokol bo narekoval, kako se naprava poveže in deli podatke s svetom. Zagotavljanje interoperabilnosti z upoštevanjem specifikacij brezvrvičnega standarda je ključnega pomena. Preskušanje na začetku načrtovanja lahko pomaga odkriti težave, ki lahko povzročijo zamude in povečajo stroške razvoja naprave.

Generatorji vektorskih signalov z zmožnostjo generiranja standardnih signalov in analizatorji spektra/signalov z zmožnostjo demoduliranja teh signalov so idealna orodja za ocenjevanje delovanja naprave z brezvrvičnim standardom po izbiri.

IV. IoT izziv številka 3 - EMI/EMC in preskus soobstoja

EMC (Electromagnetic Compatibility) lahko definiramo kot merilo, ali izdelek deluje kot je bilo predvideno, istočasno pa ne ovira drugega izdelka v skupnem okolju pri njegovem delovanju. EMI (Electromagnetic Interference) lahko definiramo tudi kot katero koli elektromagnetno energijo, ki ovira napravo, da bi delovala tako, kot je bilo predvideno. Ker se število naprav, ki komunicirajo brezvrvično, še naprej povečuje eksponentno, se ustrezno povečuje elektromagnetni šum v delovnem okolju in tudi tveganje, da se bo delovanje poslabšalo zaradi motenj.

Uporaba predhodno certificiranih RF modulov lahko pomaga zmanjšati verjetnost, da dokončana naprava ne bo opravila predpisanih preskusov skladnosti z EMC, ne zagotavlja pa, da bo končni izdelek skladen.

Tako uporaba dobrih konstrukcijskih protiukrepov za izogib motnjam (EMI) od začetka oblikovanja kot preskus dejanske učinkovitosti naprave (EMC) pred preskusom skladnosti (predhodno preverjanje skladnosti) pomagata preprečiti drago preoblikovanje in zamude.

Spektralni/signalni analizatorji ter antene so ključni del preskusne opreme za EMC za preskušanje sevalnih in prevajalnih motenj. Za preskus imunosti so dodatno potrebni viri RF signalov in ojačevalniki, ki zagotavljajo potrebno poljsko jakost. Vektorski generatorji signalov se uporabljajo za generiranje signalov, kot so WiFi in Bluetooth, ki se bodo pojavili v pričakovanem delovnem okolju naprave, katerega s tem simuliramo.

Predhodno preverjanje skladnosti EMC lahko izvajamo v običajnem okolju, boljša (in dražja) možnost pa je preskušanje v (brezodbojnih) Faradayevih kletkah/sobah.

V. IoT izziv številka 4 - RF zmogljivost za brezvrvično povezljivost

Čeprav bodo nekatere naprave IoT uporabljale vrvično komunikacijo, se bo večina za dostop do omrežja zanašala na brezvrvične tehnologije. Načrtovalci naprav IoT se soočajo s številnimi dilemami pri določanju, kako najbolje izvesti brezvrvično povezavo. Najpomembnejša med njimi je odločitev, katero brezvrvično komunikacijsko tehnologijo in protokol uporabiti (npr. WiMax, Wi-Fi, Zigbee, BLE, LoRaWan, Z-Wave, in NB-IoT), in ali naj uporabimo vnaprej pripravljen RF brezvrvični modul ali lasten dizajn. Ne glede na to, kako so ta vprašanja oblikovanja rešena, je treba uspešnost RF-komunikacije preskusiti v realnih razmerah z ustrezno opremo. Preskusi, ki jih je treba opraviti, so običajno:

A. Na oddajniku:

– oddajna moč,
– moč sosednjega kanala,
– natančnost modulacije,
– spektralna maska,
– neželene emisije.

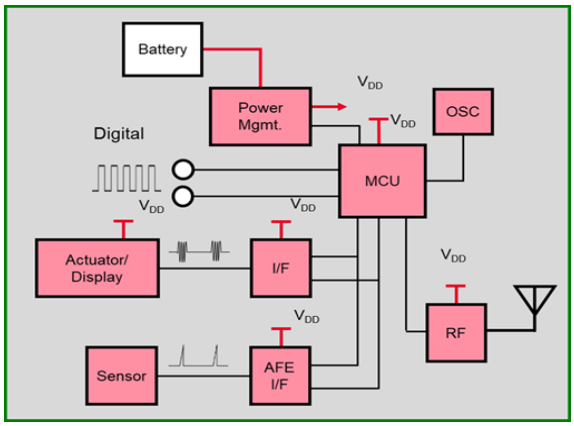
B. Na sprejemniku:

– občutljivost,
– najvišja vhodna moč,
– selektivnost sosednjega kanala,
– imunost na intermodulacijske motnje,
– presih (angl. fading) in aditivni beli Gaussov šum (angl. Additive White Gaussian Noise – AWGN).

Analizatorji spektra oz. analizatorji signalov so pogosto najprimernejše orodje za preskuse oddajnika, za meritve sprejemnika pa se uporabljajo (vektorski) generatorji signalov.

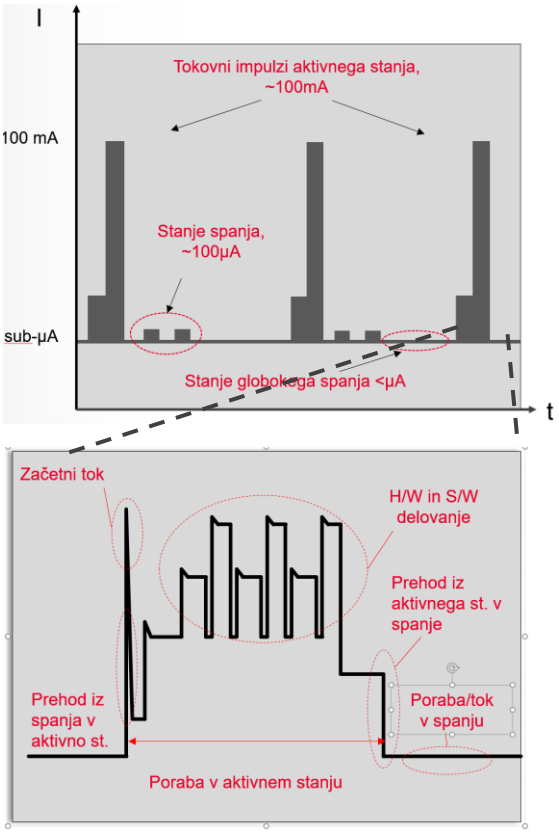
VI. IoT izziv številka 5 - Upravljanje porabe

Ker so naprave interneta stvari pogosto nameščene oddaljeno ali v mobilnem okolju, jih bo večina za glavni vir energije uporabljala baterijo. Razumevanje profila porabe energije naprave je ključnega pomena za zagotavljanje največje zanesljivosti in učinkovitosti med življenjsko dobo naprave.



Slika 2: Tipična zgradba naprave IoT

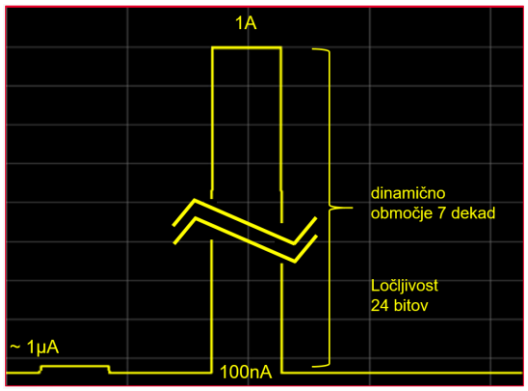
Za popolno karakterizacijo porabe energije naprave IoT se morajo meritve izvesti v vseh pogojih delovanja naprave. Zaradi varčevanja z energijo so naprave v aktivnem način delovanja le kratek čas, preostali čas pa v stanju pripravljenosti ali popolnega mirovanja (»spanja«).



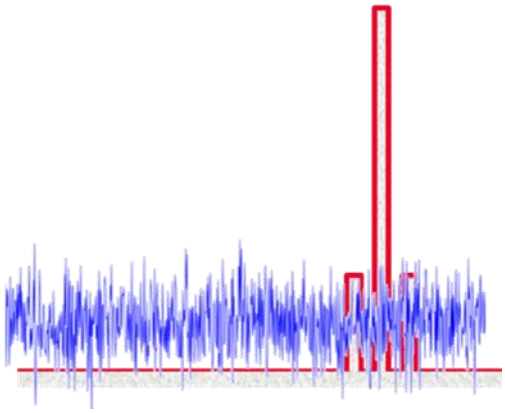
Slika 3: Dinamika toka

Glavni izzivi, ki jih je treba premagati, da bi lahko natančno količinsko opredelili moč, ki jo porabi naprava IoT, ali potrdili optimalno zmogljivost in velikost baterije, ki je potrebna za določeno dolgoročno prenosno rešitev, so našteti v nadaljevanju, prikazani pa na slikah od 3 do 5.:

– Potreben je širok dinamični razpon za stalno merjenje majhnih tokov v mirovanju (spanje), ki jim sledijo tokovni impulzi velikih amplitud v aktivnem stanju naprave (na primer prenos podatkov ali komunikacija z bazno postajo).
– Povprečen ali integriran pogled na porabo energije ni dovolj. Namesto tega zahteva smiselna kvantitativna karakterizacija natančno sliko trenutnega profila. Tokove v mirovanju (spanje) in v aktivnem delovanju naprave (prenos podatkov) je treba meriti z enako natančnostjo.
– Za natančno določanje tokov v mirovanju sta potrebna ločljivost merjenja reda nano amperov in nizek lasten šum merilnika.
– Za zajem hitrih vhodnih tokov in konice, je potrebna zadostna pasovna širina in dovolj velika hitrost vzorčenja.
– Za oceno porabljene energijo v daljšem časovnem obdobju in izvedbo izčrpne analize, mora biti instrument zmožen zabeležiti podatke skozi daljši čas in zato imeti dovolj velik pomnilnik.



Slika 4: Možno razmerje med tokom spanja in aktivnim stanjem



Slika 5: Mali tokovi merjeni na območju za velike tokove so skriti v šumu

Pomembna je natančna meritev napetosti, sinhronizirana z dinamičnim merjenjem toka.

Natančno merjenje profila porabe naprave v vseh načinih delovanja lahko predstavlja izziv za običajne tehnike merjenja toka z digitalnimi multimetri (DMM), tokovnimi sondami ali soupori. V mirovanju so lahko tokovi reda nA ali µA, medtem ko v aktivnih načinih, na primer pri prenosu podatkov, lahko dosežejo območja mA ali A. Ta velika povečanja toka se pogosto pojavljajo v zelo kratkih obdobjih, ki so lahko dolga le nekaj µs, kar predstavlja hud izziv za preskusne instrumente.

Soupori so lahko zelo natančni, vendar njihova uporaba za te vrste meritev, kjer potrebujemo veliko dinamiko, zahteva večje število souporov. Tudi z uporabo več souporov je morda treba ločeno preskusiti aktivne načine in načine mirovanja, zaradi česar je zelo težko dobiti pravo sliko trenutne porabe. Z uporabo večjih souporov, ki nam povečajo dinamiko meritev, lahko padec napetosti na souporu vpliva na preskušanca.

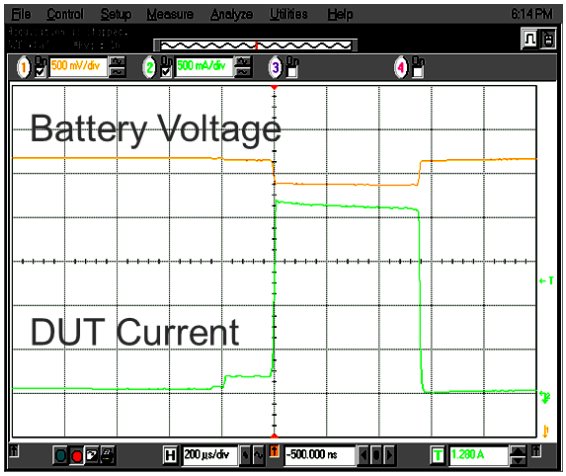
Tabela 1: Odvisnost merilnega šuma od merilnega območja

Območje	Merilni šum	Ločljivost meritve (18 bitov)
3A	400 µA	25 µA
100 mA	20 µA	1 µA
1 mA	2 µA	10 nA
10 µA	20 nA	0,1 nA

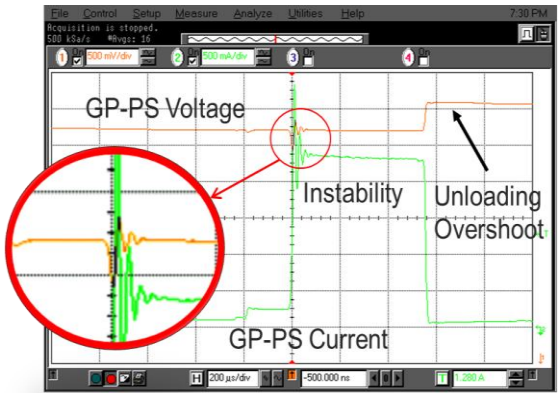
DMM, ki se pogosto uporabljajo v povezavi s soupori, lahko tudi omejijo natančnost meritve. Nekateri so prepočasni pri meritvah in obdelavi podatkov za natančno in popolno sliko hitro spreminjajočih se trenutnih vrednosti v napravah IoT. Uporaba fiksnih merilnih območij lahko pomaga ublažiti zamudo, ki jo povzroči DMM med samodejnim določanjem območja, vendar to omejuje dinamični razpon. Uporaba avtomatične izbire območja poveča dinamiko, vendar pa obstaja tveganje izgube podatkov med t.i. *slepim* obdobjem DMM, ko preklaplja iz enega območja v drugega.

Tok lahko merimo tudi z uporabo osciloskopov in tokovnih sond, ki običajno ponujajo veliko pasovno širino in s tem večjo verjetnost, da bodo zaznane hitre spremembe toka. Vendar pa večina sond ne ponuja dinamičnega razpona, ki je potreben pri meritvah toka, prav tako pa niso tako natančne kot soupori. Dinamiko meritev navzdol običajno omejuje tudi osciloskop z lastnim šumom, ki ga določata kakovost vhodne stopnje z ojačevalnikom in slabilniki in kakovost analogno-digitalnega pretvornika, ki ima omejeno ločljivost.

VII. IoT IZZIV ŠTEVILKA 6 – NAPAJANJE NAPRAVE



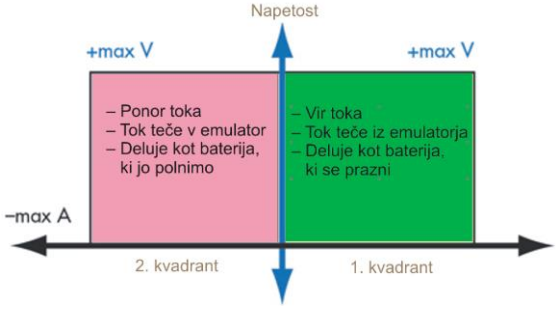
Slika 6: Napetost in tok baterije mobilnika



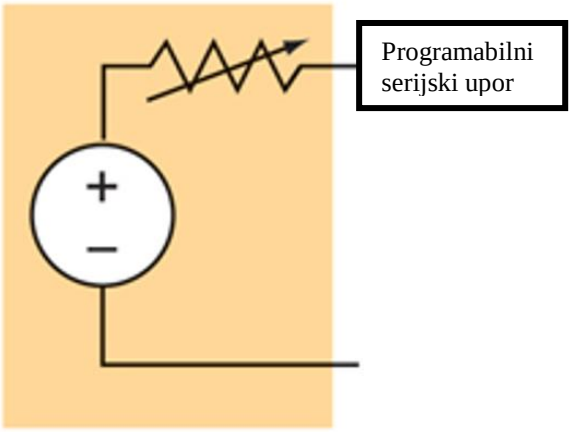
Slika 7: Napetost in tok napajalnika mobilnika

Naprave IoT želimo preskušati pri različnih napajalnih napetostih in ugotoviti, kako sprememba napetosti vpliva na delovanje naprav. Zato moramo baterijo nadomestiti z enosmernim virom. Ugotovimo lahko, da vsak vir ni dobra zamenjava za baterijo. Oglejmo si primer, ki je prikazan na slikah 6 in 7.

Na sliki 6 vidimo, da se pri napajanju iz baterije napetost nekoliko zniža, ko se tok poveča, in zopet naraste, ko tok pade. Potek napetosti in toka pri napajanju iz napajalnika (slika 7) se s tem posnetkom ne ujema in sicer prihaja ob spremembah toka do nestabilnosti napetosti in tok je večji, kot pri napajanju iz baterije. Torej bodo rezultati meritev porabe pri obeh virih različni, nestabilnosti napetosti pa lahko vnesejo motnje v delovanje naprave.



Slika 8: Emulator baterije kot pametni dvokvadrantni napajalnik



Slika 9: Model baterije

Kakovosten emulator baterije (slika 8) ima nekaj prednosti pred običajnim enosmernim virom. Te so naštete v nadaljevanju:

– Napetost in notranja upornost vira se spreminjata tako, da vir simulira napolnjenost baterije.
– Emulator je vir in ponor toka.
– Vir ima lahko vgrajeno prenapetstno in pretokovno zaščito, tako da lahko varuje preskušanca v primeru napak in preprečuje njegovo poškodovanje ali uničenje. Ker pri preskusu ni prave baterije, odpadejo tudi vse nevarnosti, vezane na baterijo (eksplozija, požar). Uporaba emulatorja baterije tako zagotavlja večjo varnost preskusov.
– Emulator baterije zagotavlja enostavnejšo pripravo preskusa z različnimi stanji napolnjenosti baterije in s tem hitrejše preskušanje. Tudi ponovljivost takih testov je neprimerno večja.

VIII. Sklep

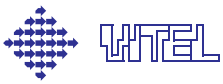
Z razvojem novih tehnologij se spreminjajo standardi preskušanja, povečuje se povpraševanje po preskušanju in validaciji, zlasti za podporo obstoječim in še neznanim izzivom upravljanja z energijo.

Upravljanje moči za naprave IoT je zahtevna naloga, saj morajo biti naprave vedno vklopljene in delujejo s polno zmogljivostjo tudi v najbolj zahtevnih okoljih.

Literatura

[1] Keysight Technologies: Five Tips for Optimizing Battery Drain on IoT Devices - Application Note, https://literature.cdn.keysight.com/litweb/pdf/5992-1810EN.pdf?id=2792264

Mirko Ivančič je diplomiral leta 1978 na ljubljanski Fakulteti za elektrotehniko, smer telekomunikacije in se zaposlil v podjetju Iskra Elektrozveze, kjer je vodil oddelek merilne tehnologije. Leta 1984 se je kot inženir za podporo tehničnih računalnikov zaposlil v Hermesu, v sektorju zastopstva za Hewlett-Packard. Od 1986 do 1992 je bil odgovoren za prodajo testno-merilne opreme za področje Hrvaške, nato je postal vodja servisa in leta 1993 član uprave Hermes Plus, d. d. in direktor podpore za vse HP-jeve izdelke za področje Slovenije, Hrvaške, Makedonije in delno Slovaške. Leta 1996 je postal direktor merilne skupine za prodajo in podporo elektronske, medicinske in kemijsko-analitske merilne opreme. Leta 1997 je zapustil Hermes in po letu dni dela v podjetju Spes postal direktor Venture, podjetja za razvoj, proizvodnjo in trženje plovil. Leta 2002 se je pridružil Avektisu, takratnemu slovenskemu zastopniku podjetja Agilent Technologies (bivši HP), kot vodja prodaje elektronske merilne opreme. Od leta 2010, ko je Agilentov partner za Slovenijo postal Amiteh d.o.o., pa dela pod okriljem tega podjetja, specializiranega za trženje visokokakovostne merilne opreme priznanih proizvajalcev Keysight Technologies, Rigol, Itech in ostalih.



Referenčno pametno mesto Novo mesto in osrednja komunikacijska postaja za pametna mesta

Gregor Grkman in Robert Richter, Telekom Slovenije, Ljubljana

Povzetek — Trg interneta stvari (Internet of Things - IoT) se kaže kot zelo obsežen in raznolik, predvsem zaradi večjega števila vertikal - posameznih tržnih področij (kot so pametna mesta, e-mobilnost, pametne stavbe, pameten dom, e-zdravje, agrikultura ...). Velikost posamezne vertikale je odvisna od geografske lege in gospodarske razvitosti države ter vsaka zase za operaterja predstavlja svojevrsten izziv. Sam nastop na posamezni vertikali od operaterja zahteva najprej njeno razumevanje in nato učinkovito popolnitev manjkajočih kompetenc na trgu posamezne vertikale, s čimer operater zagotavlja konkurenčno prednost svoje ponudbe. Ob takšnem pristopu pa se pojavlja tudi vprašanje, ali ob takem specifičnem nastopu lahko operater ponudi nekaj več kot samo povezljivost ter se poskusi premakniti višje v IoT-vrednostni verigi in tako s celostnimi rešitvami zasesti dodatno pozicijo na trgu interneta stvari (naprave, povezljivost, IoT platforma in obdelava podatkov, aplikacije).

Ključne besede – IoT-sistemi, NB-IoT, pametno mesto, osrednja komunikacijska postaja

I. UVOD

Telekom Slovenije kot vodilni ponudnik celovitih in najsodobnejših komunikacijskih rešitev skladno s svojo usmeritvijo širi portfelj storitev tako na področja izven osnovne komunikacijske dejavnosti kot IT-rešitev. Med novejša področja sodijo tudi rešitve interneta stvari in pametnih mest. Naše podjetje je v aprilu 2019 svoje mobilno omrežje, ki so ga nemški strokovnjaki na neodvisnem testu ocenili kot najboljšega v Sloveniji, že v celoti nadgradil s tehnologijo NB-IoT (Narrowband Internet of Things). Gre za standardizirano tehnologijo za učinkovito množično komunikacijo naprav (povezanih v internet stvari), ki ustvarjajo majhen podatkovni promet. Tehnologija odpira nove priložnosti za razvoj inovativnih rešitev z visoko dodano vrednostjo za optimizacijo procesov, upravljanje z viri, zagotavljanje visoke stopnje varnosti, pa tudi višje kakovosti bivanja.

Rešitve interneta stvari (IoT) lahko koristijo posameznikom, podjetjem in družbi. Za posameznike je ta koncept uporaben na številnih področjih, vključno z zdravjem, varnostjo, finančnimi storitvami in vsakodnevnim načrtovanjem. Tako, na primer, sistem hišne varnosti posameznikom omogoča, da svoje domače prostore spremljajo preko pametnih naprav, spet drugi sistemi pa so lahko vgrajeni v vozila, namenjeni pa so spremljanju gibanja, pomoči pri vožnji, v primeru trkov lahko prožijo klic v sili in podobno. Rešitve interneta stvari so lahko koristne pri nadzoru stroškov v gospodinjstvih ipd.

Rešitve interneta stvari bodo pomembne tudi pri razvoju mest, saj ta s tehnološkim razvojem mesta postajajo vse bolj pametna in povezana. Pametno mesto je urbani center, ki tehnologijo uporablja za boljšo kakovost življenja prebivalcev, za upravljanje virov (ceste, vode, promet) na ekonomičen in trajnostni način ter zmanjšanje okoljske onesnaženosti.

II. OPIS STORITVE

Za delovanje IoT-sistema za izvajanje storitev in pripravo rešitev pametnih mest je potrebno najprej vzpostaviti celoten sistem strojne in programske opreme ter aplikacijskih komponent, ki so običajno razvrščene v naslednje skupine:

- *Senzorji* – merijo različne parametre na objektih, v prostoru, na strojih in napravah, sistemih in telesih. Parametri so lahko preprosti (npr. temperatura) ali bolj kompleksni (npr. geolokacija, značilnosti gibanja, snovi v vodi ali zraku ipd.) Senzorji izvedejo digitalizacijo podatkov o objektih, kar je prvi korak pri zasnovi podatkovnega modela opazovanega objekta.
- *Komunikacijska infrastruktura* – brezžična komunikacijska infrastruktura prenaša podatke iz senzorjev v centralni sistem na varen in zanesljiv način, kjer so na razpolago za nadaljnjo obdelavo v okviru aplikacij.
- *Hramba podatkov in uporaba aplikacij* – veliko število senzorjev lahko ustvari ogromno količino podatkov, platforma pa podatke zbira, jih konsolidira in hrani. Poleg tega omogoča preprosto povezavo aplikacij z uporabo vnaprej opredeljenega modula za programiranje pravil obdelave na višji ravni in brez kodiranja.
- *Aplikacije* – pridobivajo podatke iz vmesne programske opreme in izvajajo analize na različnih ravneh. Vmesna programska oprema in aplikacije so lahko na isti platformi, vendar so ločene in uporabljajo standardizirane API-je za medsebojno komunikacijo.

Vse navedene komponente lahko zagotovi naše podjetje, s čimer zagotavljamo celovito rešitev za mesta in njihove prebivalce.

III. VSEBINA STORITVE

V septembru 2018 smo Mestna občina Novo mesto, Telekom Slovenije in podjetje SAP Slovenija podpisali sporazum o sodelovanju v sistemu pametno mesto (ang. Smart City). Gre za referenčno postavitev pametnega mesta, ki predstavlja naslednjo fazo razvoja mest v okviru rešitev, ki jih omogoča internet stvari. Rešitve so namenjene povečevanju kakovosti življenja v mestih.

Za referenčno postavitev pametnega mesta Novo mesto smo predvideli naslednje storitve:

- zasedenost javnih parkirnih prostorov,
- meritve kakovosti zraka,

– zajem in meritev porabe vode in energentov,
– pametna ulična razsvetljava,
– merjenje zadovoljstva občanov.

Celotna rešitev je povezana v enotno platformo za upravljanje in spremljanje različnih dejavnikov.

Ob tem smo v Telekomu Slovenije skupaj s tehnološkimi, razvojnimi in infrastrukturnimi partnerji za pametna mesta razvili tudi osrednjo komunikacijsko postajo, ki omogoča spremljanje ključnih dogodkov na lokaciji (število pešcev ali vozil, frekvenca obiskovalcev ipd.), kar omogoča njihovo nadaljnjo analizo za učinkovitejše načrtovanje logistike, delovnih procesov, lokalne ponudbe itd. Poleg tega pa lahko občani in ostali prek komunikacijske postaje opravijo tudi določene storitve (napolnijo e-vozilo, pridobijo informacijo o lokaciji in načrtujejo nadaljnjo pot, preverijo vremensko napoved, poiščejo najbližjo lekarno ipd.) ali upravljavcu posredujejo povratno informacijo (kako so zadovoljni z dostopom, kdaj najlažje opravijo obisk/nakup, ali potrebujejo parkirno mesto ipd.).

IV. OSREDNJA KOMUNIKACIJSKA NAPRAVA

Osrednja komunikacijska postaja (slika 1) je zasnovana kot pametna ulična svetilka, poleg ulične razsvetljave pa vključuje še številne dodatne funkcije, kot so:

– tipala za spremljanje ozračja,
– možnost polnjenja električnih vozil,
– možnost spremljanja zasedenosti parkirnih mest,
– videonadzorni sistem,
– sistem za merjenje zadovoljstva občanov,
– WiFi-oddajnik ter
– komunikacijsko opremo, ki omogoča nizanje dodatnih modulov za zbiranje drugih relevantnih podatkov (glede na namen) v radiju do 8 km.

Slika 1: Osrednja komunikacijska postaja za pametna mesta

Osrednja komunikacijska postaja uporablja skupno implementacijo IoT-platforme, ki omogoča krmiljenje storitev, zbiranje podatkov, upravljanje z napravami in obračunavanje storitev. Ima interaktivni zaslon, ki se ga upravlja na daljavo. V zaledju je mogoče nastaviti in slediti zastavljenim ciljem ter določati parametre, ki jih lahko uporabniki spremljajo na zaslonu, kot so zasedenost parkirnih mest, polnjenje električnih vozil, spremljanje mestnih projektov, podajanje mnenj itd.

A. Polnilnica električnih vozil

Osrednji del komunikacijske postaje za pametna mesta predstavlja funkcionalnost polnjenja električnih vozil. Status polnjenja spremljamo na zaslonu polnilne postaje in v mobilni aplikaciji.

B. Povezljivost

Integrirano brezžično omrežje je zaradi svoje umeščenosti vizualno zlito z ulično svetilko ter zaščiteno pred vandalizmom in okoljskimi dejavniki. Za spremljanje slednjih v premeru 5 do 8 km je v uporabi prehod LoRaWAN, ki je umeščen v samo postajo. Na vrhu postaje je antena za povezljivost z omrežjem WiFi.

C. Spremljanje/nadzor

Na drogu osrednje komunikacijske postaje je nameščena visoko resolucijska kamera za zagotavljanje varnosti, uporablja pa se lahko tudi za namene promocije, štetje prometa, prepoznavo registrskih tablic, spremljanje razpoložljivosti parkirišč, dvigovanje/spuščanje zapornic itd.

D. Razsvetljava

V sklopu napredne ponudbe lahko uporabniki izbirajo med različnimi možnostmi integracije omrežja javne in zasebne razsvetljave s sistemi za krmiljenje, ki delujejo v korelaciji s tipali ali na podlagi strojnega učenja. Razsvetljava je LED z nizko porabo električne energije.

E. Interaktivnost

Na osrednjem delu postaje je interaktiven zaslon, ki omogoča prikaz praznih parkirnih mest v bližini, prikazuje stanje polnjenja električnega vozila, generira geslo za omrežje WiFi, pregleduje okoljske podatke itd. Prek mobilne ali spletne aplikacije lahko prebivalci izrazijo tudi svoje mnenje oz. (ne)zadovoljstvo z aktualnimi mestnimi projekti.

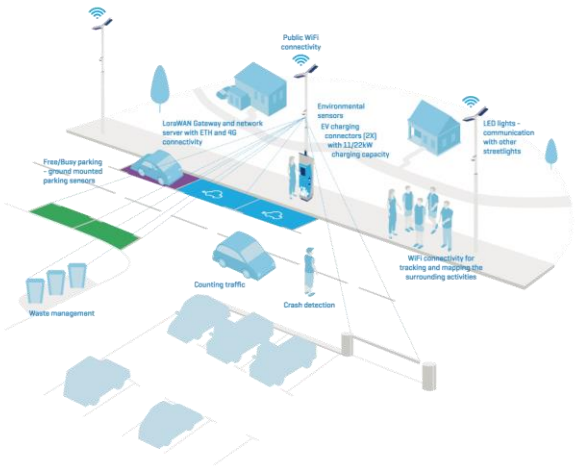
F. Okoljski senzorji

Osnovni nabor okoljske senzorike vključuje spremljanje temperature, vlage in pritiska ter nivo ogljikovega monoksida, žveplovega in dušikovega dioksida in ozona. Nabor tipal senzorike je poljubno razširljiv na zvočno in svetlobno onesnaženost ter na druga področja meritev kakovosti zraka.

G. Prilagodljivi elementi

Z osnovnimi komunikacijskimi elementi (WiFi, 4G, LoRaWAN, NB–IoT) lahko postajo prilagajamo za katerokoli področje mestnega upravljanja. Načrtujemo širok nabor, trenutno pa so možnosti naslednje:

– nadzor polnosti zabojnikov za smeti,
– napovedi poplav,
– pametno kmetovanje,
– pametna industrija,
– spremljanje porabe vode.



Slika 2: Urbano pohištvo

V. RAZVOJNE SMERNICE

Dodatni primeri uporabe platforme interneta stvari, ki jih lahko na isti platformi zagotovimo v našem podjetju, so:

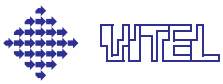
- *Energija* – v energetskem segmentu lahko internet stvari omogoči merjenje energije na različnih mestih, spremljanje prevodnosti, opredelitev lokacije preloma električnega voda in zaznavanje ledu, zaščito pred krajo, geo-ograje itd.
- *Kmetijstvo* – kmetijska podjetja so zainteresirana za spremljanje okoljskih in vremenskih podatkov, spremljanje živali (na primer pri govedu spremljanje temperature, srčnega utripa, geo-lokacije), spremljanje temperature tal, spremljanje strojev pri obdelavi površin itd.
- *Zaščita pred krajo* – zaznavanje gibanja sicer nepremičnih stvari, kot so podzemni kabli, geo-ograje.
- *Upravljanje prometa* – upravljanje voznega parka ali skupine vozil vključno s sledenjem in načrtovanjem poti, načrtovanjem in predvidevanjem vzdrževanja vozil, pametnimi prometnimi znaki, ki nakazujejo ovinek na podlagi prezasedenosti, štetje prometa z namenom pridobitve realnega časa in zgodovinske informacije o gostoti prometa itd.
- *Logistična veriga* – sledenje palet in kontejnerjev, sledenje vozil, spremljanje stanja okolja z namenom zagotavljanja zahtevanih pogojev, nadzor nivoja in tlaka za spremljanje cistern.
- *Pametni dom* – zaznavanje prisotnosti in gibanja v domu, opozorilo v primeru dima, opozorilo v primeru varnostnih težav z vrati oz. okni itd.
- *Električne polnilnice* za električna prevozna sredstva.

VI. ZAKLJUČEK

Pametno mesto je razvojna vizija kako integrirati informacijsko komunikacijske tehnologije (IKT) in tehnologije interneta stvari (IoT) za upravljanje mestne infrastrukture na varen način. Mestna infrastruktura vsebuje informacijske sisteme, šole, knjižnice, promet, bolnišnice, oskrbo z elektriko, vodo, upravljanje z odpadki, varnost in druge storitve za občane. Naše podjetje je ponudnik na področju IoT (Internet of Things) in IoE (Internet of Everything), ki je osnovni gradnik za formiranje ponudbe na področju upravljanja z viri urbanih okolij. Inicialna oblika ponudbe bo urbanim okoljem (občinam) omogočila osnovno merjenje kakovosti bivalnega okolja, polnilnice za električna vozila ter upravljanje z javno razsvetljavo in parkirnimi površinami. Sklop obsega prvotne ponudbe pa občinam zagotovi predpogoje za sodelovanje na razpisih za financiranje razvoja pametnih mest in se uporablja za izboljšanje produktivnosti in večjo interaktivnost storitev, za zmanjšanje stroškov, za izboljšanje porabe virov ter za boljšo komunikacijo med občani in mestno/občinsko upravo.

Gregor Grkman v Telekomu Slovenije kot produktni vodja skrbi za razvoj ponudbe storitev v oblaku ter storitev na področju pametne infrastrukture. Njegova karierna pot ga je z mesta načrtovalca in skrbnika informacijskega sistema podjetja Elektro Ljubljana vodila do takratnega sistemskega integratorja Avtenta. Ob nenehni strokovni rasti v vlogi načrtovalca, implementatorja in SLA-skrbnika ter s širokim poznavanjem IKT-tehnologij se je leta 2012 odločil za prestop na področje razvoja in trženja produktov, kjer je s celostnim poznavanjem kompleksnosti rešitev pripomogel k svežemu pristopu oblikovanja ponudbe takratnega portfelja storitev Avtenta.now. S prenosom dejavnosti podjetja Avtenta na Telekom Slovenije, se je ponudila priložnost širšega nastopa skupine na področju zunanjega izvajanja storitev v oblaku, z letom 2018 pa tudi strateški nastop na področju IoT. Trenutno kot del skupine za razvoj poslovanja v okviru strateške poslovne enote Poslovni trg v Telekomu Slovenije skrbi za kontinuiran razvoj ponudbe ter pravočasen odziv podjetja na tem segmentu trga.

Robert Richter ima na področjih, kot so telekomunikacije in prodaja, že več kot 20-letne izkušnje. Zaposlen je pri telekomunikacijskem operaterju Telekomu Slovenije. Trenutno je vodja ekipe za upravljanje s projekti in razvoj v strateški poslovni enoti Poslovni trg Telekoma Slovenije.



Gradniki pametnih mest prihodnosti

Janez Križan, A1 Slovenija

Povzetek — Ta članek opisuje uporabno vrednost elementov, ki jih ponudniki predstavljajo v sklopu ekosistema pametnih mest.

Ključne besede — trajnostni razvoj, tehnologije prihodnosti

Abstract — This article explains what is the useful value of elements that are usually presented within ecosystem of smart cities.

Keywords — sustainable development, future technologies

I. UVOD

Bistvo iniciativ s področja pametnih mest bi vedno morali biti napredni projekti, s katerimi lahko lokalne skupnosti/občine izboljšajo kakovost bivanja na območju mest in okolice, spodbujajo trajnostni razvoj, obvladujejo in znižajo obratovalne stroške ter učinkovito obvladujejo vplive na okolje.

A. Centraliziran pogled na delovanje mesta

Napredna rešitev za pametno mesto občinam in mestom zagotavlja centraliziran nadzor nad vsemi relevantnimi deli javne infrastrukture, omogoča avtomatizacijo internih procesov in enostavno integracijo že obstoječih rešitev, kot so izposoja koles, upravljanje parkiranja, uporaba javnega transporta in drugih.

Takšna rešitev tako omogoča povezovanje vseh deležnikov v enoten ekosistem, s čimer je omogočena nemotena interakcija med občani, lokalnim gospodarstvom, turisti, obiskovalci in občino ter njenimi službami.

Centralizirana platforma pametnega mesta je stičišče vseh obstoječih tehnologij in omogoča enostavno vpeljavo tehnologij prihodnosti. Platforma prav tako omogoča hrambo in dostopnost do vseh zbranih podatkov naprav IoT, ki lahko tako služijo kot osnova za izgradnjo novih rešitev in izboljšave v drugih dejavnostih.

Posamezna občina z uvedbo dobi dostop do digitalne platforme, preko katere lahko spremlja podatke zajete s pomočjo senzorjev in kamer za različne primere uporabe npr.

- Spremljanje okolja z nadzornimi postajami, ki merijo specifične koncentracije plina in koncentracije delcev. Postaje so lahko nameščene v mirujočem položaju ali na vozilih;
- Pametni promet, ki temelji na video analitiki in štetju prometa. Video viri, usmerjeni na prometne poti, se analizirajo v realnem času in štejejo vozila v vnaprej določenih prometnih tokovih;
- Upravljanje z odpadki s senzorji nameščenimi na smetnjake, ki merijo raven napolnjenosti zabojnikov za odpadke. Zagotavljajo vpogled, katere zabojnike je treba izprazniti, da bi se izognili nepotrebnim odvozom smeti ali preveč napolnjenim smetnjakom;
- Pametna razsvetljava, s pomočjo katere se lahko zagotavlja najbolj optimalno razsvetljavo javnih površin. Svetilke se opremi z radarskim senzorjem, ki lahko zazna prisotnost in hitrost predmetov, ki se nahajajo oziroma gibljejo v neposredni bližini posameznega droga. Dodatno se lahko (glede na tip svetilke) omogoči vgradnjo ustreznih polnilcev za električna vozila, klice v sili in podobno;
- Pametno parkiranje s parkirnimi senzorji. Video viri, usmerjeni na parkirišča, se analizirajo v realnem času, da se ugotovi zasedenost posameznih parkirnih mest.

Modularen uporabniški vmesnik za uporabnike obsega uporabniški vmesnik, na katerem lahko posamezniki dostopajo to relevantnih podatkov v občini, prijavljajo napake in potrebe po vzdrževanju … Tako se jim omogoči dostop do podatkov o prireditvah in dogodkih ter dostop do podatkov o javnem transportu, parkirnih mestih, nakup vozovnic, turistom pa dostop do podatkov o lokalni ponudbi, znamenitostih v občini, interaktivno vodenje po občini z uporabo obogatene resničnosti, nakupovanje kart, izposojo koles, plačilo parkirnine, rezervacijo gostinskih storitev in podobno.

B. Trajnostna energetska učinkovitost mesta in skrb za okolje

Napredna rešitev za pametno mesto občinam in mestom z uvedbo spremljanja pretočnosti in klasifikacije vozil v realnem času omogoča optimizacijo pretočnosti prometa in načrtovanje potreb po izboljšavi infrastrukture, voznikom pa skrajša čas potovanja in iskanja parkirnega mesta.

Z vzpostavitvijo merjenja kakovosti okoljskih parametrov, na primer zraka, je vzpostavljen temelj, ki omogoča transparentno komunikacijo vplivov industrije in prometa na kakovost bivanjskega okolja ter posledično dolgoročno načrtovanje ukrepov in izboljšav.

S storitvijo upravljanja z odpadki, ki deluje na osnovi spremljanja ravni napolnjenosti zabojnikov za odpadke s senzorji, se vzpostavi sodoben sistem za učinkovitejše načrtovanje praznjenja omrežja zabojnikov. Ta pristojnim službam omogoča optimizirano upravljanje omrežja zabojnikov. Na ta način posamezna občina lahko zasleduje cilje družbe brez odpadkov (angl. Zero Waste) in zmanjša stroške praznjenja zabojnikov.

Pametno upravljanje javne razsvetljave je pomembna komponenta pri uresničevanju ciljev za večjo energetsko učinkovitost in zmanjševanje svetlobne onesnaženosti mest. Z njegovo uporabo lahko občina zagotavlja najbolj optimalno in racionalno razsvetljavo javnih površin, saj so svetilke opremljene s tehnologijo zaznavanja prisotnosti in hitrosti predmetov, ki se nahajajo oziroma gibljejo v neposredni bližini.

II. MESTO PO MERI PREBIVALCEV

Poleg že navedenih nekaterih primerov uporabe pa je potrebno poudariti, da rešitev *A1 Pametno mesto* omogoča tudi funkcionalnosti digitalnega upravljanja z mestnimi dovolilnicami, od zaprosila, odobritve in končne uporabe pri vstopu v mestno jedro, kot tudi integracijo sistemov plačevanja storitev, vpeljave mestne kartice in mnogih drugih.

Sistem digitalne dovolilnice zagotavlja učinkovito uravnavanje prometa v starih mestnih jedrih in modrih conah. Spletna aplikacija omogoča, da upravičenci zlahka pridobijo dovolilnico, upravljavci pa obdelujejo podatke in dokumente oddanih vlog ter dovolilnic.

Celovita rešitev za plačevanje in upravljanje parkirnin ponuja možnost podaljševanje parkirnine na daljavo in sklenitev brez parkirnega listka, uporabnika opozori o izteku parkirnine, hkrati pa je njen del tudi nadzor sistema upravljalca, ki nadzornikom omogoča enostaven način preverjanja parkirnin. Plačevanje je omogočeno preko SMS sporočil, mobilne aplikacije (ki predstavlja enostaven način plačila parkirnine tudi za tujce, tako na iOS kot Android napravah in z vsemi bolje zastopanimi plačilnimi sredstvi) in preko spletne strani.

Dodatno komponento rešitve *A1 Pametno mesto* predstavljajo avtomatizirani in avtonomni sistemi pristopne kontrole, parkirni sistemi in sistemi za kontrolo in umirjanje prometa. Nadzorni center za kontrolo in upravljanje omenjenih naprav ter sistemov omogoča uporabo na namiznem računalniku, tablici ali na mobilnem telefonu in na ta način upravljalcem nudi možnost oddaljenega spreminjanja nastavitev in parametrov za povečano učinkovitost in ekonomičnost sistemov.

III. PRIHODNOST MEST IN DIGITALIZACIJA

Trajnostni razvoj, stroškovna vzdržnost, transparentna komunikacija in izgradnja ekosistema, ki povezuje vse deležnike na tehnološko neodvisni platformi so osnovni gradniki pametnih mest prihodnosti že danes.

LITERATURA

[1] T. M. Vinod Kumar, Smart Economy in Smart Cities: International Collaborative Research, 2016

Janez Križan je direktor razvoja novih poslovnih modelov in inovacij v podjetju A1 Slovenija. Je vizionar, ki neprestano išče nove izzive in nove poslovne priložnosti, z več kot 19 leti izkušenj iz področij informatike, informacijske varnosti, telekomunikacij in razvoja produktov.

Razvoj enotne platforme gradnikov za podporo aplikacije 'pametni dom'

Andrej Volčjak, ISKRA, d.o.o., PE MIS, Kranj

Povzetek — Namen tega dokumenta je zgoščena predstavitev različnih aktivnosti, ki jih podjetje Iskra, d.o.o. vlaga v razvoj in raziskave na področju vsak dan večjih izzivov učinkovitega nadzora in obvladovanja različnih proizvodnih virov energije (lastna PV proizvodnja, kogeneracija, drugi obnovljivi viri na objektih), ter učinkovite oz. *pametne* porabe energije na različnih porabnikih objekta (pametni dom) oz. večjih in kompleksnejših obratih, kot so npr. večji poslovni kompleksi oz. dislocirane poslovne enote v družinah podjetij. Znotraj takšnih t.i. *energetskih ekosistemov* se lahko srečujemo z zelo različnimi segmenti in kombinacijami proizvodnih virov lastne energije in energije iz javnih distribucijskih omrežij, ter različnimi energetskimi porabniki (strojna oprema, ogrevanje, hlajenje, el. vtičnice, e-polnilnice …). Sodobna energetska infrastruktura objektov v večini primerov bazira na sistemu energetske samozadostnosti, kjer primarni vir oskrbe zagotavljajo lastni obnovljivi viri in se energija iz omrežja preliva le v izrednih primerih, kadar samooskrba ni zadostna. Zato imajo naprave in sistemska orodja oz. sodobne aplikacije (mobilne) za učinkovit in zanesljiv sistemski nadzor nad proizvodnjo in porabo energije izredno velik pomen.

Ključne besede — »pametni dom«, mobilne aplikacije, nadzor, regulacija, poraba energije, proizvodnja energije, objekti

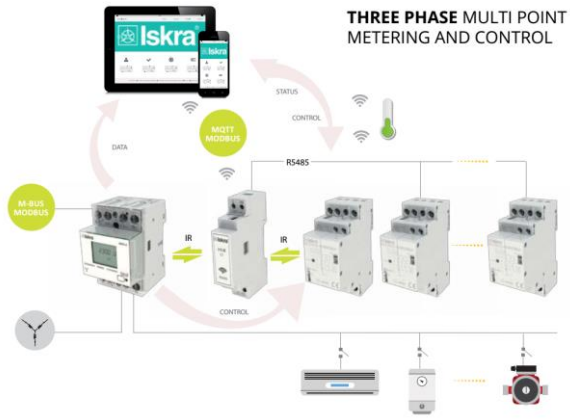
Abstract — The purpose of this document is a concise presentation of the various activities that company Iskra d.o.o. invests in a development and research in the field of daily challenges for an effective control and monitoring applications above the different energy production sources (PV production, cogeneration, other renewable resources at the facilities), and an efficient, "Smart power usage" of all produced energy on a different customers' objects ("smart home") or even larger - more complex plants such as for example big business complexes or different dislocated business units. Within all these so-called "energy ecosystems" we are confronted with a very different segments and combinations of production sources as own production, energy from the public distribution networks, and various energy consumers (hardware, heating, cooling, electrical outlets, e-vehicle charging ...) on the other side. Modern energy infrastructure inside facilities are in most cases based on a system of energy self-sufficiency, where the primary source of supply is considered to provide own renewable resource and the energy from the network is poured added only in exceptional cases, when self-sufficiency is insufficient. Therefore all in-built measuring devices, sensors, communicators and modern applications (mobile) for an effective and reliable system control above energy production and consumption have a great significance.

Keywords — "Smart home", mobile applications, control, regulation, energy consumption, energy production, facilities

I. UVOD

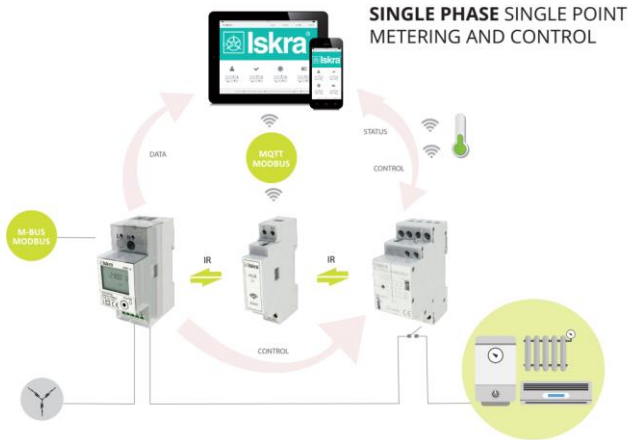
Osnovna ideja enotne platforme gradnikov aplikacije »Pametni dom« oz. »Pametni Objekt« je namenjena razvoju in integraciji naprav, komunikacijskih vmesnikov in sistemskih *cross-platform* aplikativnih rešitev za pridobivanje, prenos in prezentacijo podatkov o proizvodnji in porabi energije, ter krmiljenju različnih bremen preko poljubno nastavljivih vmesnikov WiFi, LoRa ali BlueTooth v lokalnem sistemu objekta ali oddaljeno preko strežnikov Cloud/IoT/MQTT (s pomočjo web-servisov REST API oz. mehanizma *publish/subscribe* uporabljenega protokola MQTT). Dve trenutno najbolj tipični povezavi naprav in aplikacij, ki kot osnovna gradnika lahko tvorita enostavne ali kompleksnejše aplikativne sistemske rešitve spremljanja, nadzora ter krmiljenja proizvodnje in porabe energije sistema, sta naslednja:

– *Three Phase – MultiPoint Metering And Control System*



Slika 1. Osnovni gradnik 3-faznega sistema

– *Single Phase - SinglePoint Metering And Control* System



Slika 2. Osnovni gradnik 1-faznega sistem

II. OSNOVNE KOMPONENTE SISTEMA

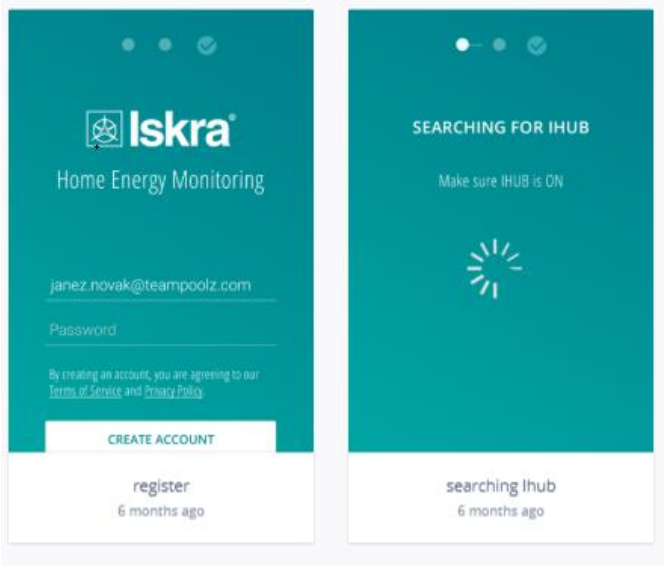
Glavne komponente sistema, ki v različnih oblikah medsebojnih povezav in podprtih komunikacijskih kanalov lahko tvorijo celovito sistemsko rešitev, po željah končnega uporabnika ali poznanih infrastrukturnih omejitvah objekta oz. vhodnih zahtevah topološke strukture vseh povezanih enot v večje kompleksnejše sisteme poslovnega okolja, so naslednje:

- iHUB (gateway) - komunikacijski modul,
- WM3-6 - trifazni števec,
- WM1-6 - enofazni števec,
- BICOM32 - komunikacijsko kontrolno stikalo,
- WTS100 – WiFi-senzorji temperature, vlage, gibanja,
- Smart Home Energy Monitoring - mobilna aplikacija,
- Cloud/Backend - *docker engine* administracija sistema.

III. FUNKCIJSKE LASTNOSTI SISTEMA

Funkcijske lastnosti kompletne sistemske rešitve vseh uporabljenih komponent in mobilne aplikacije, ki skrbi za prikaz in grafično korelacijo trenutnih ter zgodovinskih trendov proizvodnje oz. porabe ter ON/OFF funkcionalnosti krmiljenja različnih porabnikov preko komponent BiCOM, vezanih v sistemu, so naslednje:

- prikaz kumulativnih podatkov energetske porabe,
- prikaz tarifnih podatkov energetske porabe,
- prikaz kumulativnih podatkov energetske proizvodnje,
- prikaz tarifnih podatkov energetske proizvodnje,
- prikaz trenutnih moči porabnikov,
- zgodovinski grafi porabe (tedenski, mesečni, letni),
- primerjave zgodovinskih trendov,
- alarmiranje izrednih dogodkov v sistemu,
- cenovni primerjalnik SLO ponudnikov energentov,
- »Carbon footprint« [1] prihranki lastne PV proizvodnje.

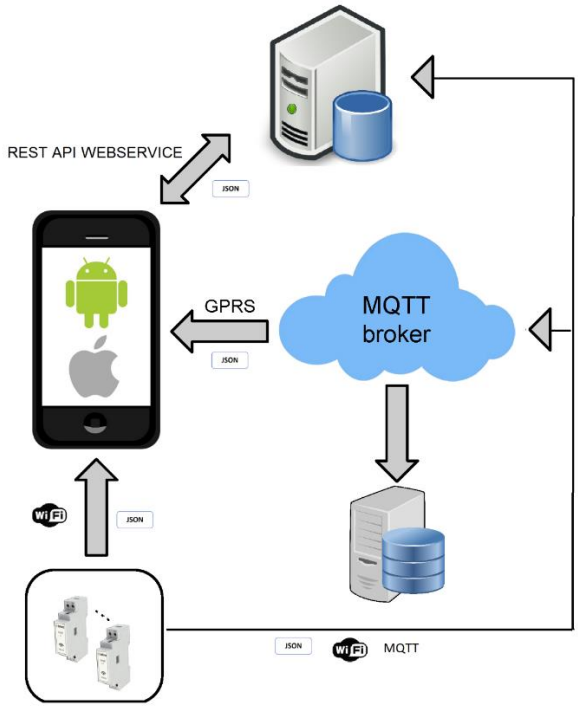


Slika 3. Prijava v aplikacijo in iskanje vmesnikov iHub v sistemu

A. *Branje oz. način pridobivanja podatkov*

Načini branja oz. transporta podatkov od števcev preko komunikacijskih vmesnikov v sistemu (iHUB) do mobilnega klienta in naprej do administrativnega vmesnika oz. zaledne t.i. »Cloud« sistemske rešitve, so naslednji:

- preko Wi-Fi-vmesnika (GET,SET ukazi) in MQTT–brokerja oz. odjemalca podatkovnih sporočil v obliki JSON,
- podatki, zbrani v bazi sistema MiSMART, z uporabo web-servis klicev REST API do mobilnega klienta.



Slika 4. Podprti komunikacijski kanali in logični protokoli

Aplikativna rešitev, ki skrbi za prikaz in analitično obdelavo podatkov z vseh osnovnih gradnikov sistema, temelji na t.i. zasnovi *cross-platfor*[2], kar predstavlja prihranek časa pri razvoju za vse naprave (mobilne, statične) z različnimi vgrajenimi operacijskimi sistemi (Android/iOS/WIN). Nekateri tipični pogledi na izrise podatkov v aplikaciji so podrobneje predstavljeni v nadaljevanju.

B. *Prezentacija podatkov in meritev energentov sistema*

Izgled in funkcionalne možnosti za čim učinkovitejšo prezentacijo različnih podatkov v aplikaciji so bili definirani s pomočjo orodja *UX design.ea*, kjer so bili vsi znani sodobni principi prikaza in interpretacije podatkov na sodobnih napravah temeljito preučeni in izbrani v prototipni fazi razvoja.

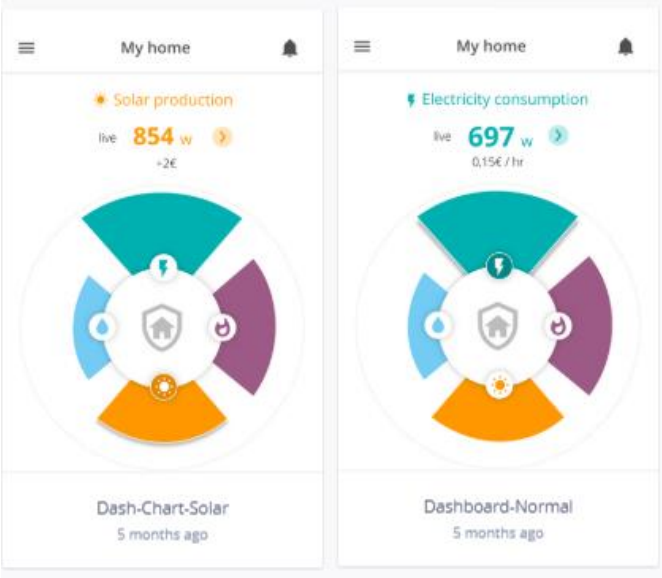
Zato lahko trdimo, da zahtevan uporabniški nivo izkušenj za koristno uporabo in razumevanje aplikacije pokriva vse stopnje zahtevnosti od osnovnega do zelo zahtevnega končnega uporabnika, ki s tem orodjem lahko nadzoruje in upravlja kompleksnejši energetski sistem poslovnega okolja.

[1] Kumulativni letni prihranek CO2 emisije zaradi PV proizvodnje električne energije

[2] Programska oprema za več različnih platform (*multi-platform*) oz. programsko neodvisna oprema – aplikacija.

C. *Prikaz trenutnih vrednosti porabe in smeri energij*

Prikaz trenutnih vrednosti porabe in smeri pretoka energij v sistemu je namenjen spremljanju vrednosti in smeri pretoka moči na objektu (PV-proizvodnja vs. distribucijsko omrežje). V primeru, ko je PV-proizvodnja sistema večja kakor trenutna poraba, je možno proizvedeno moč oz. energijo pošiljati v omrežje. Spodaj so prikazani možni prikazi podatkov, ki lahko nastopijo.

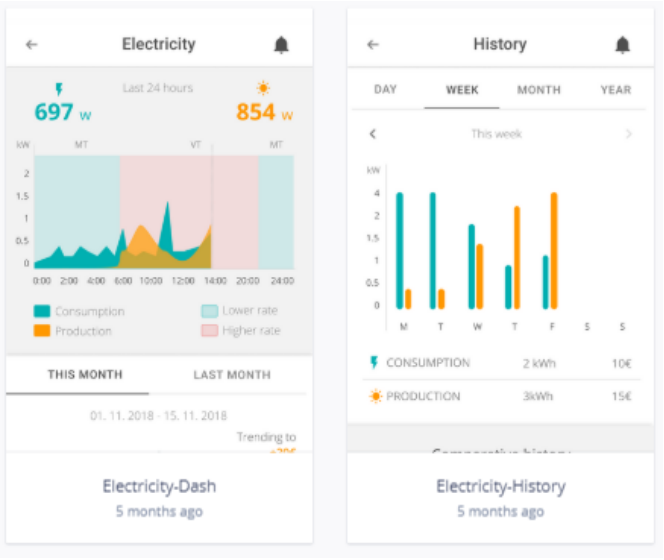


Slika 5. Trenutna vrednost PV-proizvodnje in porabe električne energije objekta

Slika 6. Trenutna vrednost porabe plina in vode na objektu

D. *Prikaz zgodovinskih vrednosti in trendov porabe*

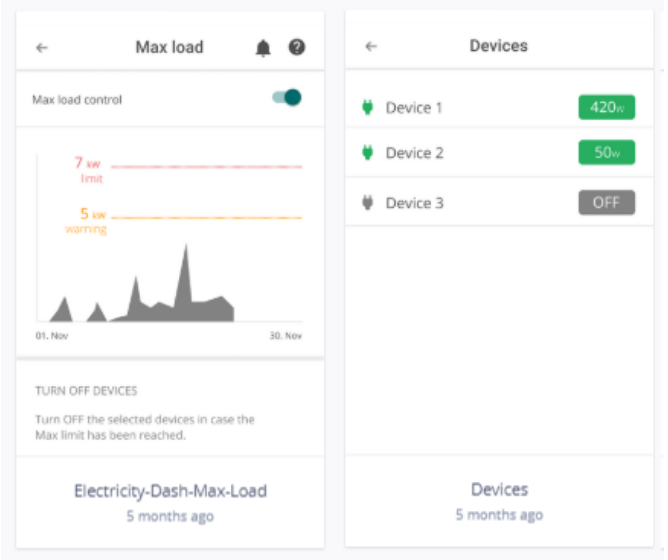
Prikaz zgodovinskih vrednosti oz. trendov porabe in PV-proizvodnje je namenjen prezentaciji tedenske, mesečne in letnih kumulativnih vrednosti energij (proizvedena energija vs. porabljena energija).



Slika 7. Zgodovinski prikaz in trendi porabe in proizvodnje električne energije na objektu

E. *Prekoračitev porabe v sistemu – Max Load*

Namen funkcije *Prekoračitev porabe* oz. opozorila *Max Load* je prikazati, da se trenutna moč bliža mejni vrednosti sistema oz. je le-ta že prekoračena. Na podlagi tega podatka se uporabnik lahko odloči za intervencijo oz. nastavitev avtomatskega odklopa porabnika.

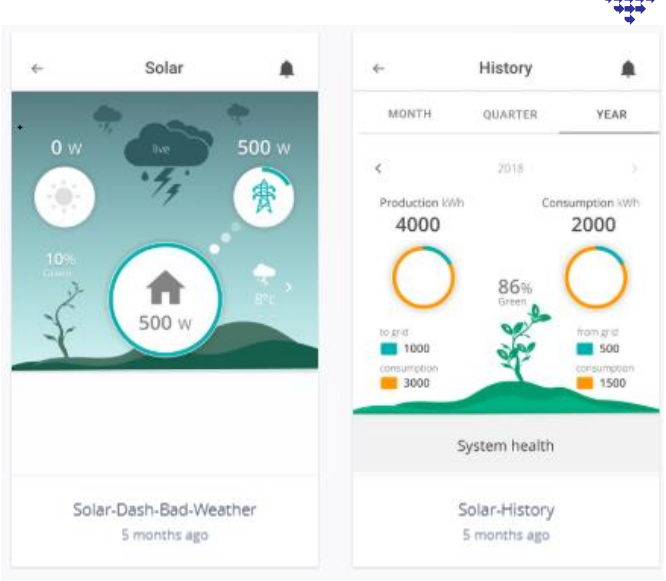


Slika 8. Prikaz prekoračitve porabe v sistemu

F. *Prihranki zaradi lastne proizvodnje - Carbon footprint*

Namen te funkcije oz. prikaza *zdravja sistema* je uporabniku nazorno predstaviti vzroke (subjektivne zaradi pomanjkljivosti sistema ali objektivne zaradi, npr., vremenskih pogojev) oz. efektivno uspešnost ali neuspešnost delovanja pod-sistema za proizvodnjo el. energije. (PV oz. vgrajen solarni sistem).

S tem podatkom je neposredno povezan naš letni prihranek oz. emisije CO2 zaradi brezhibnega delovanja sistema PV.



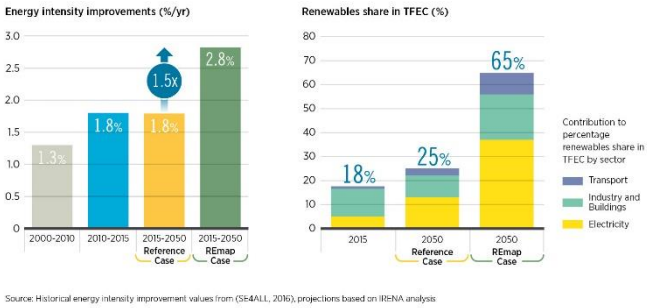
Slika 9. *Carbon footprint* oz. *zdravje sistema* PV-proizvodnje

IV. GLOBALNI KAZALCI PORABE ENERGIJE

Vse globalne raziskave kažejo na zelo očitno rast trendov porabe energentov do leta 2050. Zato v podjetju Iskra upravičeno posvečamo vedno večjo skrb in pozornost v raziskave in razvoj modernih sistemskih rešitev, kakršna je opisana zgoraj. Te nam omogočajo varčevanje energije, povečajo varnost ter udobje bivanja in dela v prostorih, ter nam hkrati na drugi strani omogočajo prihranke energije oz. čim večjo energetsko samozadostnost objektov.

Z vpeljavo vse večjega števila različnih obnovljivih virov se sicer zmanjšujejo potrebe po energiji iz javnih distribucijskih omrežjih in se s tem posledično manjšajo obremenitve le-teh, a hkrati s tem postajajo zahteve v prenosnih (TSO[3]) in distribucijskih omrežjih (DSO[4]) po večji sistemski obvladljivosti vse večjega števila takšnih malih oz. t.i. samozadostnih mikro energetskih virov iz dneva v dan večje.

Zaradi širokih znanj in bogatih izkušenj naših strokovnjakov v podjetju, lahko aktivno sodelujemo pri različnih projektih in sistemskih rešitvah, tako na strani učinkovite vpeljave energetsko samozadostnih stavb oz. lastnih virov oskrbe, kakor tudi na strani sistemskih rešitev TSO in DSO operaterjev prenosnih in distribucijskih omrežij.



Slika 10. Globalni trendi rasti obnovljivih virov in porabe

[3] Transmision System Operator – sistemski operater prenosnega omrežja
[4] Distribution System Operator – sistemski operater distribucijskega omrežja

LITERATURA

[1] MQTT: http://mqtt.org/
[2] MQTT broker: https://www.hivemq.com/
[3] JSON (JavaScript Object Notation): http://www.json.org/
[4] Docker Engine: https://docs.docker.com/engine/
[5] Global Energy Transition | A Roadmap to 2050: https://www.irena.org/publications/2018/Apr/Global-Energy-Transition-A-Roadmap-to-2050

AVTOR

Andrej Volčjak je produktni vodja v podjetju Iskra, d.o.o., PE MIS, Kranj.

Smart system of integrated health and care

Marjeta Pučko, Bojan Jurca, Telekom Slovenije, Ljubljana

Abstract — This paper presents intermediary results of the EkoSMART Research and Development project 5 (RDP5) with the aim to develop and test a smart system of integrated health and care in Slovenia in a real environment. Focus is given to the ICT and IoT (Internet-of-Things) aspect of the project providing the technological base for telemedicine and integrated care services.

Keywords — smart systems, internet of things, telemedicine, integrated health care systems

Povzetek — V članku predstavljamo vmesne rezultate projekta *EkoSmart RRP5* s ciljem razviti in v realnem okolju preveriti pametni sistem integriranega zdravstva in oskrbe v Sloveniji. Fokus je usmerjen v IKT in IoT vidik projekta, ki zagotavlja tehnološko osnovo za storitve telemedicine in integrirane oskrbe.

Ključne besede — pametni sistemi, internet stvari, telemedicina, integrirana zdravstvena oskrba

I. INTRODUCTION

A. Background

The Internet-of-Things (IoT) concept is coming up for practical use with applications in different domains as traffic, energetics, health care and smart cities overall. Smart systems in health and care have been actively researched and developed during last five years and have proven to bring benefits for different stakeholders. In the domains of health and care, pilot or regular use in many countries resulted in remarkable effects as better accessibility of health and care services for patients, reducing deaths caused by elderly falls, preventing critical health condition for patients with chronic diseases, cost savings for medical treatment etc. [1,2,3]

B. About EkoSMART and RDP5

The main objective of *EkoSMART* programme is to develop a smart city ecosystem with all the support mechanisms necessary for efficient, optimized and gradual integration of individual areas into a unified and coherent system of value chains. The program focuses on three key domains of smart cities: health, active living and mobility; and forms strategic relationships with municipalities and other areas of smart cities, such as energy, smart buildings, involvement of citizens, smart communities, etc. *EkoSMART* introduces the universal architecture of a smart city, based on the combination of self-learning and self-optimizing agents able to find a common Nash equilibrium even between inhomogeneous sources. This architecture enables the realization of all the concepts of smart cities, such as interoperability, self-adaptivity and self-configurability, open data, semantic interoperability, and integration of social capital. In terms of economy, the vision of the *EkoSMART* programme is to launch Slovenian solutions in the field of smart cities on the world market [4].

The aim of the *EkoSMART RDP5* project is to develop approaches and prototypes that ensure the basic conditions for an efficient transformation of Slovenian health system. By developing the prototypes for the use of modern ICT technology and telemedicine in managing chronic diseases, a comprehensive integration of individual levels of health care is performed. In addition, an efficient and safe exchange of information between various stakeholders at the national level is developed (national register, accounting system, analyses of large data volumes) and the basic conditions for development and sustainability of the health and social systems are provided.

For the purpose of testing the prototypes in a real environment, the *EkoSMART RDP5* project is connected with the *EkoSMART RDP6* project. The testing is being currently executed to carry out at the level of subsystems and smart city ecosystem as a whole. For the telemedicine prototype testing, clinical pathways for five chronic diseases have been defined (chronic obstructive pulmonary disease - COPD, asthma, chronic cardiac failure - CHF, type 2 diabetes and arterial hypertension), and a telemedicine services prototype developed with integration to telecare services, including telemedicine infrastructure, processes and knowledge. The technological solution is already in the production phase able to provide full support for telemedicine services testing in a real environment, conducted as a clinical study.

C. Focus and contribution of the paper

Besides a brief presentation of our integration concept and the complete technological framework, we concentrate in the paper on intermediate results of the integrated telemedicine prototype testing from the technological point of view. Some attention is given to description of principles of integrated health and care to provide basic understanding of requirements for supporting ICT infrastructure and multidisciplinary scope of the prototype testing. After the prototype testing is finished, the complete evaluation will be done and final results available.

II. SMART SYSTEMS IN THE DOMAINS OF HEALTH AND CARE

A. Basic Definitions

- **Smart city:** The *smartness* of a city describes its ability to bring together all its resources, to effectively and seamlessly achieve the goals and fulfil the purposes it has set itself. The role of Smart City standards is focused on enabling the integration and interoperability of city systems in order to provide value, both to the city as a whole, and to the individual citizen [5].
- **Internet-of-Things (IoT):** IEEE distinguishes between *small environmental scenario* and *large environmental scenario*. Use of IoT in our use case of integrated care requires the *large environment*

scenario according to which IoT envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration [6].

- **Telemedicine services:** Telemedicine is viewed as a cost-effective alternative to the more traditional face-to-face way of providing medical care (e.g., face-to-face consultations or examinations between provider and patient). This definition is modelled on Medicare's definition of telehealth services (42 CFR 410.78) [7].
- **Integrated health and care:** Integration is a coherent set of methods and models on the funding, administrative, organizational, service delivery and clinical levels designed to create connectivity, alignment and collaboration within and between the cure and care sectors. The goal of these methods and models is to enhance quality of care and quality of life, consumer satisfaction and system efficiency for people by cutting across multiple services, providers and settings. Where the result of such multi-pronged efforts to promote integration leads to benefits for people, the outcome can be called integrated care [8].

B. Need for Integration and Related Work

The need to integrate health and care for elderly has been well researched so far by different authors. Although national health and social care systems remain, at best, loosely coupled systems that are facing increasing difficulties, given the current challenges, in particular in long-term care for older persons: increasing marketization, lack of managerial knowledge (co-operation, co-ordination), shortage of care workers and a general trend towards down-sizing of social care as stated in the EU Fifth Framework Project *Providing integrated health and social care for older persons (PROCARE)* that took under consideration 9 EU countries (Austria, Denmark, Finland, France, Germany, Greece, Italy, the Netherlands, and the UK) [9].

On the other hand, only integrated care provides optimum outcomes of treatment and helps the (type 2 diabetes in particular) patient to take control over his or her health. From the perspective of health professionals, the greatest obstacles to a well-integrated care (in Slovenia) are of systemic and organizational nature [10].

An obvious link exists between aging and chronical disease development. Aging itself is the predominant risk factor for most diseases and conditions that limit health span [11].

According to National Institute for Public Health of Republic of Slovenia (NIJZ), the reasons for the increase in diabetes can be attributed to the aging of the population only partly, even though the high prevalence of type 2 diabetes is attributed to a long-living society.

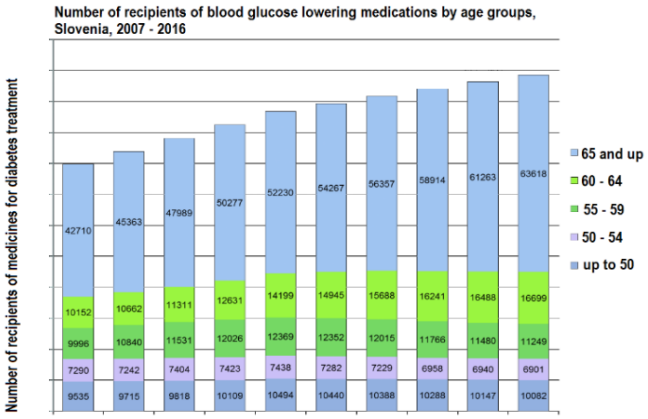


Figure 1: Number of recipients of blood glucose lowering medications by age [10]

There have been previous attempts to overcome some of the difficulties with the use of state-of-the art technology like IoT. For example, the UK National Health Service (NHS) started project named *Technology Integrated Health Management (NIHM)* for people with dementia and their caregivers [12]. In the UK, Governmental Department of Health & Social Care has recognized importance of integrated care approach and has published their vision for digital, data and technology in health and care including guiding principles to make this work [13].

C. Integration Principles

The principle of integrated care, used in *RDP5*, basically follows the chronic care model [8] which brings together 6 elements for treatment of a patient with a chronic disease: community, health system, self-management support, delivery system design, decision support, and health information systems. As one of results of *RDP5*, the strategy and development plan of the original integrated health and care model [14] was adopted to Slovenian health system and based on three key approaches:

- tele-monitoring,
- tele-interventions,
- integration and coordination including cooperation with home care providers in local communities.

The developed model of integrated health care directly imposes requirements for integration on the architecture and service level including system management, data, processes and use cases.

D. Requirements for Technology

Defining requirements for technology, we started analysis and requirements specification with consideration of best practices and experiences in other EU countries, for example in the UK and Denmark. The UK has after several pilots clearly defined the vision of future digital architecture together with guiding principles to make it real, with focus on getting the basics right: the digital architecture of the health and care system – the building blocks. Open standards, secure identity and interoperability are critical to the safe and successful use of technology, ensuring that systems talk to

each other and that the right data gets to the right place at the right time. At the heart of this vision are 4 guiding principles to make this work: user need, privacy and security, interoperability and openness, inclusion as declared in [13]. In Denmark a few subsequent pilots were executed gradually collecting requirements for different populations, chronic diseases, increasing number of patients and improving the smart system [1].

Learning from their experiences, we made a careful analysis of requirements in the following categories:

- basic functionality of a smart system regarding health and care,
- data processing and exchange,
- end user requirements,
- interoperability, legacy and information security.

Hereby, a classification of smart healthcare is used as defined by [15].

E. Implemented ICT Infrastructure and IoT

The *EkoSMART* telemedicine infrastructure consists, as shown in Figure 2, of medical sensors, a HUB and a telemedicine platform. This relatively simple infrastructure supports implementation of key elements of telemedicine services: telemonitoring, teleconsulting, telediagnostics and patient empowerment. Most common technology used for transferring measurement results from medical sensors to the HUB is Bluetooth Low Energy (BLE). The HUB, whether a smartphone or tablet, then transmits measurement results via 4G to the telemedicine cloud platform, implemented as PaaS.

The infrastructure for telecare services is similar, consisting of home unit gateway installed in a patient's home connected over xDSL or GSM and communicating with assistance centre and telecare cloud. PIR motion, personal and ambient sensors are used to detect falls or danger for patients as for example fire. An advanced AI based data analytics of collected movement data is used to recognize patient falls and alarm the assistance centre. Telecare (E-care) itself is a standalone product of Telekom Slovenije integrated with telemedicine for the purpose of *EkoSMART* system of integrated health and care.

The system is also integrated with public health information systems and some hospital information systems for purposes of prototype testing in a complete health and care ecosystem.

The complete *EkoSMART* system architecture is shown in Figure 2.

III. PROTOTYPE TESTING IN A REAL ENVIRONMENT

A. Prototype Testing Framework

Although the main focus of this article is more on the technological aspect of a smart system of integrated health and care, the purpose of *RDP5* is much broader, i.e. to develop models and prototypes that ensure the basic conditions for an efficient transformation of Slovenian health system.

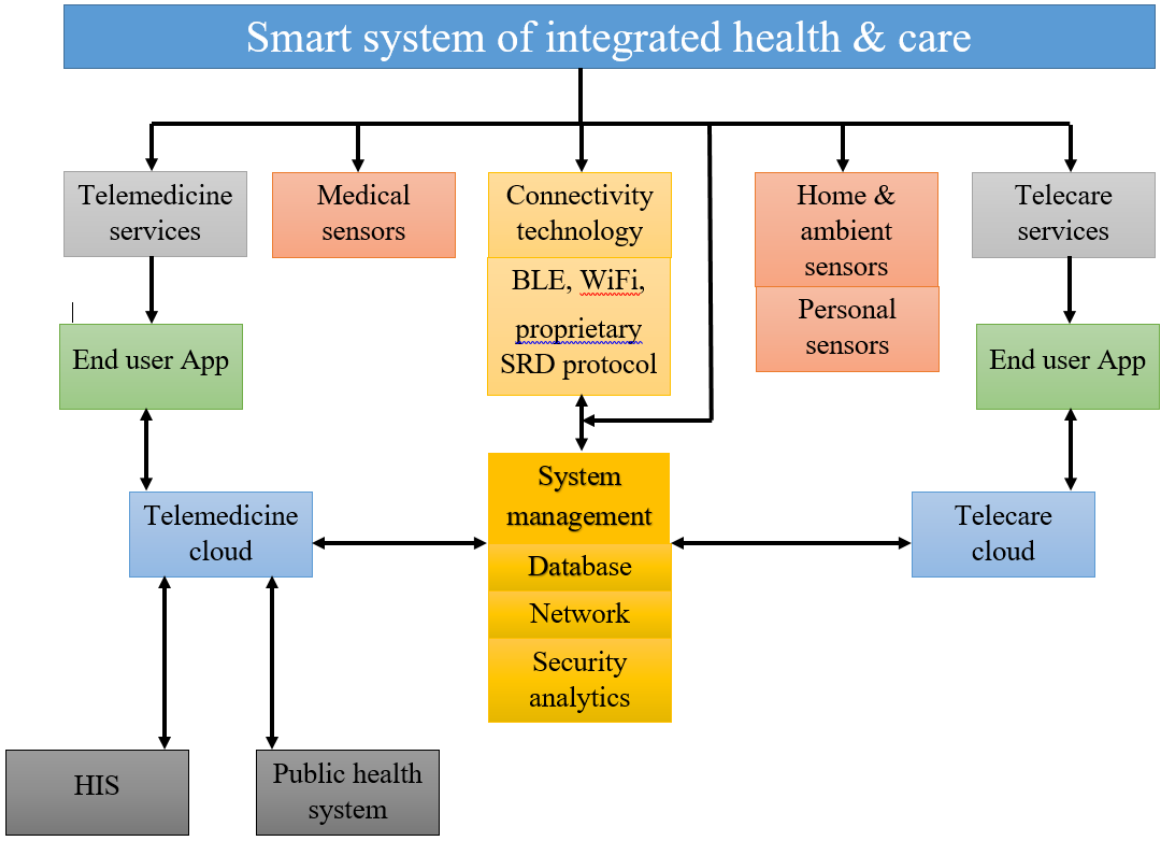


Figure 2: Architecture of the EkoSMART RDP5 system of integrated health & care

The RDP5 project is divided into four work packages that holistically address a smart system of integrated health and care from different aspects, as shown in Figure 3.

Therefore in the prototype testing, the complete integrated framework is tested from different aspects and as a whole in order to evaluate how successful and efficient is in comparison to traditional health treatment and care methods.

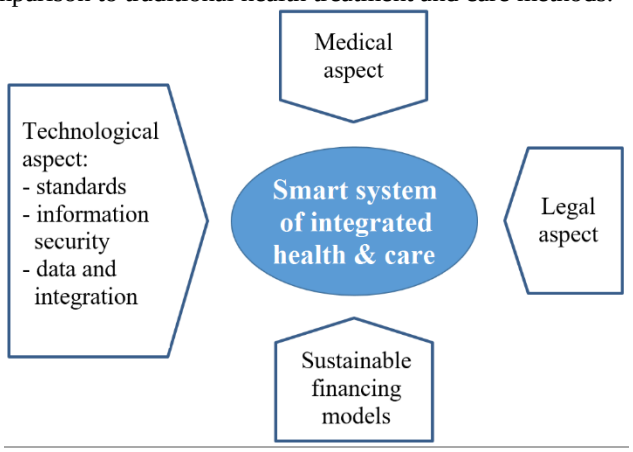


Figure 3: Aspects of development and prototype testing of the EkoSMART RDP5 system of integrated health & care

B. *Prototype Testing Ecosystem*

The RDP5 project is, by its very nature and objectives, multidisciplinary bringing together partners from research, health sector, public health ICT infrastructure, and telemedicine and telecare services provider:

- Telekom Slovenije d.d.,
- University Medical Centre Ljubljana,
- University Clinic of Respiratory and Allergic Diseases Golnik,
- Health Center Trebnje,
- National Institute of Public Health,
- Anton Trstenjak Institute of Gerontology and Intergenerational Relations,
- University of Ljubljana - Faculty of Medicine,
- University of Ljubljana - Faculty of Electrical Engineering.

C. *Prototype Testing Objectives*

Models and prototypes developed in *RDP5* are being tested in *RDP6*. The main purpose of prototype testing of the smart system of integrated health and care in a real environment is to prove its efficiency in addressing problems the health system is currently facing with and anticipating as a result of an aging population. Main operative goals of the prototype testing are to prove that:

- the supporting technology is efficient,
- integrated health treatment and care has a positive effect for treatment of patients,
- the use of integrated health and care brings a financial benefit for public health system.

A thorough analysis will be performed at the end of the prototype testing, evaluating clinical effects using MAST methodology [16]. However, we have already collected some useful intermediate results.

D. *Intermediate results and experience*

The testing of a smart system prototype of integrated health and care in a real environment started in October 2018 as a clinical study involving patient groups with chronic obstructive pulmonary disease (COPD), asthma, chronic cardiac failure (CHF), type 2 diabetes and arterial hypertension. Multimorbidity is also included, as a patient can belong to several groups due to his/her different chronic diseases. Before involvement of patients into the clinical study, the supporting ICT infrastructure and telemedicine treatment processes have been previously proven by beta testing. The patients that after that got medical sensors, connected to smart phones or tablets, are being treated according to clinical pathways developed and supported by the smart system of integrated health and care. A subset of telemedicine patients also uses telecare with a home unit/gateway, PIR and ambient sensors, primarily to early detect falls and to prevent critical health conditions of patients at their homes.

We are currently in the middle of the prototype testing phase involving patients. Five patients have already finished telemedical treatment whereas approximately one half of the planned population is still waiting to start. Some important quantitative results are presented in Table 1 and Table 2.

Table 1: Scope of the prototype testing

	Planned	*Actual (so far)*
Project duration	9 months	6 months
Duration of telemedical treatment	3–9 months	
Number of enrolled patients	200	81
Number of patients that have already finished telemedical treatment		5
Drop out		1*
Number of patient data transmittions		1.615

*due to death of a patient

Table 2: IT service KPIs

Availability	99,91 % **
Number of upgrades	2
Number of incidents	28

**240 minutes downtime during 2 upgrades

As shown in Figure 4, altogether the patients have performed 1.615 data transmissions. The frequency of transmissions increases with the number of patients enrolled into the clinical study.

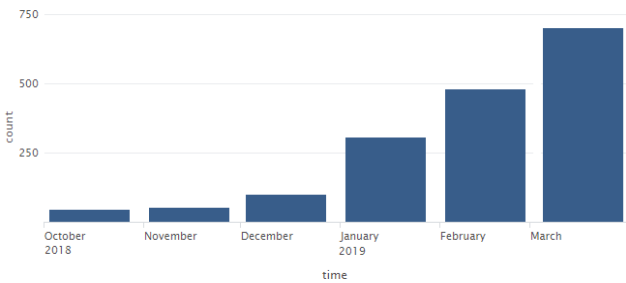


Figure 4: Dynamics of patient data transmissions

Generally, the alternative way of chronic diseases treatment supported by the smart system of integrated health and care, in comparison to classical medical treatment, has been well accepted by medical personnel and patients. Many benefits have been identified [17]. For that reason, there is no drop out of patients, except death of one patient. The complete model of integrated health and care with the supporting smart system and intermediate results of prototype testing have already been presented to Ministry of Health of Republic of Slovenia and National Institute for Public Health [18].

IV. CONCLUSIONS

Development and introduction of a smart system of integrated health and care, which would fulfil requirements and needs of all stakeholders in a national health system, is a challenging task. Despite learning from many foreign experiences, models and tools cannot directly be transferred from one country or use case to another. In the case of *EkoSMART RDP5*, the technology part was not trivial, but it could not succeed without considering all other aspects enabling it to work in the complete health ecosystem.

For the future work, we will continue to collect user feedback and evaluate the whole project after its end. The evaluation will provide directions for further enhancement. Considering only the intermediate results of prototype testing, we can conclude that use of a smart system of integrated health and care in Slovenia has a great potential.

ACKNOWLEDGMENTS

We would like to thank dr. Dominika Oroszy from University Medical Centre Ljubljana for her valuable input enabling us to provide the implemented ICT infrastructure well-tailored to actual medical and patient needs.

The EcoSmart programme is co-financed by the Republic of Slovenia and the European Union from the European Regional Development Fund.

LITERATURE

[1] TelecareNord Hjertesvigt, Afslutningsrapport for det telemedicinske hjertesvigtprojekt I Nordjylland, Denmark, 2019, https://issuu.com/telecarenord/docs/tcn_afslutningsrapport_2019_issuu?e=36851858/67585331

[2] World Health Organization (WHO), WHO Global Report on Falls Prevention in Older Age, 2007

[3] Jonathan Neufeld, Financing Telehealth: A National Perspective, Upper Midwest Telehealth Resource Center, USA, 2014

[4] About the EkoSMART program, http://ekosmart.net/en/about/

[5] ISO/IEC JTC1, Smart cities, Preliminary report, 2014 https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf

[6] IEEE, Towards a definition of Internet of Things (IoT), May 2015, https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[7] Medicaid.gov, Medicare's definition of telehealth services (42 CFR 410.78) https://www.medicaid.gov/medicaid/benefits/telemed/index.html

[8] World Health Organization (WHO) - Regional Office for Europe, Health Services Delivery Programme, Division of Health Systems and Public Health, Integrated Care Models: An Overview, Working Document, Copenhagen, Denmark, October 2016

[9] Kai Leichsenring, Developing integrated health and social care services for older persons in Europe, International Journal of Integrated Care, Jul-Sep 2004, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1393267/

[10] National Institute for Public Health (NIJZ), Pomen integrirane oskrbe pri obvladovanju sladkorne bolezni, http://www.nijz.si/sl/pomen-integrirane-oskrbe-pri-obvladovanju-sladkorne-bolezni

[11] Brian K. Kennedy et al., Aging: a common driver of chronic diseases and a target for novel interventions, PubMed Central, U.S. National Library of Medicine, National Institutes of Health, May, 2016, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4852871/

[12] NHS, Technology Integrated Health Management (TIHM) Project, https://www.england.nhs.uk/ourwork/innovation/test-beds/tihm/

[13] GOV.UK, Department of Health & Social Care, The future of healthcare: our vision for digital, data and technology in health and care, Policy paper, The UK, October 2018, https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care

[14] Dominika Oroszy, Strategy and development plan of telemedicine treatment model (in Slovene), EkoSMART Project Documentation, 2017

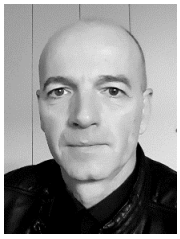
[15] Prabha Sundaravadivel, Elias Kougianos, Saraju P. Mohanty, and Madhavi Ganapathiraju, Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health, IEEE Consumer Electronics Magazine, January 2018

[16] A. Kotzeva on behalf of MAST Working Group, MAST – a model for HTA-based assessment of telemedicine, HTAi Annual Meeting, June 2012, Bilbao, https://www.slideshare.net/HtaiBilbao/mast-a-model-for-htabased-assessment-of-telemedicine-applications

[17] Irena Dolschon, Zdravje na daljavo (Telehealth), Oddaja Preverjeno, POP TV, in Slovene, February 2019, https://media.klipingmap.com/html/view?filePath=2019/02/27/1edbd370-8440-469c-8008-8cd6254e6c5f&language=sl&topicGroupId=829826a3-0221-3b41-8364-102835c4dfb7&showHighlights=true&purpose=2&summaryType=auto_generated&iT=2e63f76a-475c-4998-b9ac-a84dde9a39c0&iT=5232286c-85a9-4c9e-a695-29c2ea7bf199&iT=3bc1be82-fa0a-4d99-965e-b9073496085e&iT=c43d0752-10a1-41ea-913b-ea0fc6381d4b&iT=d2a0cdcc-e774-4cad-8035-6296f0a53ef2&iT=2783176f-31e1-4873-b673-9a34b7ca2cc8

[18] Dominika Oroszy, Peter Pustatičnik, Presentation of integrated health and care for Ministry of Health of Republic of Slovenia and National Institute for Public Health, February & March 2019

Marjeta Pučko received Ph. D. in computer science from the University of Ljubljana, Slovenia. She was a researcher at Jožef Stefan Institute and a visiting researcher at Technical University of Munich. After that she joined IskraTEL, Telecommunicatins Systems, Ltd., as expert for telecommunications systems and later held different management positions in research, development and business improvement. Next she was with Vzajemna health mutual insurance as head of IT services department, information security manager and CIO deputy. Currently, consulting and managing different research and applicative projects, also with Jožef Stefan Institute and Telekom Slovenije, her interests concern information and communication technologies and systems, e-health, business intelligence and data, e-learning systems, information security and process management.



Bojan Jurca graduated in computer and information science in 1990 at the Faculty of Electrical Engineering and Computer Science at the University of Ljubljana. From 1992 to 1995, he was a researcher at this faculty and gained the title of Master of Science in 1995. He worked in various IT and healthcare companies on different positions, as a

programmer, database architect, CIO, BI consultant, assistant director of a hospital. He is currently working for Telekom Slovenije, where he is responsible for managing RDP5 project of EkoSmart programme.

The Experience Economy – Unlocking New Business Value with Intelligent Technology

Jelena Ilić, SAP SEE

Abstract — The Experience Economy has reshaped how CEOs are thinking about running their business. With feedback coming from various channels, there is a tremendous potential to leverage these insights in a meaningful way to drive business model innovation, process optimization and reimagine how work is done.

Linking operational data with experience data in the moment, will enable agile responses to shifting trends, better service to customers and employees, and the ability to quickly adopt innovative business models and processes.

This article is aimed to provide a perspective of how to accelerate journey to the Intelligent Enterprise, by bringing experience and operations together.

Key Words — Intelligent Enterprise, experience, operations, insight, outcomes, process, value.

I. INTRODUCTION

"Change has never been this fast, but it will never be this slow again".

Evolving Experience Economy is shaping the enterprise strategic priorities to generate new revenues streams and services, lead in customers' experiences, and simplify and automate processes.

Companies are beyond the stage of awareness when it comes to digital technologies. They already understand the power of AI, IoT, cloud, robotics, and mobile, while block chain and augmented reality are more and more appearing on the radar.

All of this innovation is fuelled by data, from having the right intelligence to capture, combine, enrich and execute. We are entering the era of intelligent mega-processes, which start by combining the right data sets and converting them into intelligent insights. These insights then trigger automated transactions across the process.

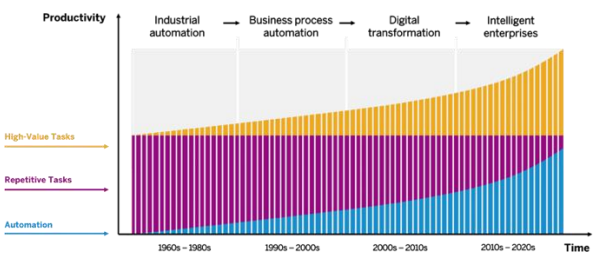
Leading companies that are making digital transformation a reality are putting customer, data and intelligence at the centre of their future. They are building new capabilities, skills, and technology, and evolving their culture to transform into an 'Intelligent Enterprise'.

These companies are not only delivering short-term value to shareholders but are also positioned to thrive and transform their industries in the future.

II. WHAT IS THE INTELLIGENT ENTERPRISE?

The Intelligent Enterprise is not yet another buzzword but logical consequence of what is possible today.

The Intelligent Enterprise delivers new capabilities that enable the workforce to focus on higher-value outcomes.



The Intelligent Enterprise builds upon the promise of digital transformation by applying data-driven intelligence to drive automated actions and decisions based on superior insights. Today, the ability to automate is much more sophisticated than in prior years. Furthermore, this automation can be achieved far more cost-effectively than before. Embedding the intelligence within the business processes makes emerging technologies much more consumable and scalable.

When many routine activities are automated, the workforce can focus on higher-value activities such as customer success, strategic planning, and innovation.

III. ROLE OF IOT IN INTELLIGENT ENTERPRISE

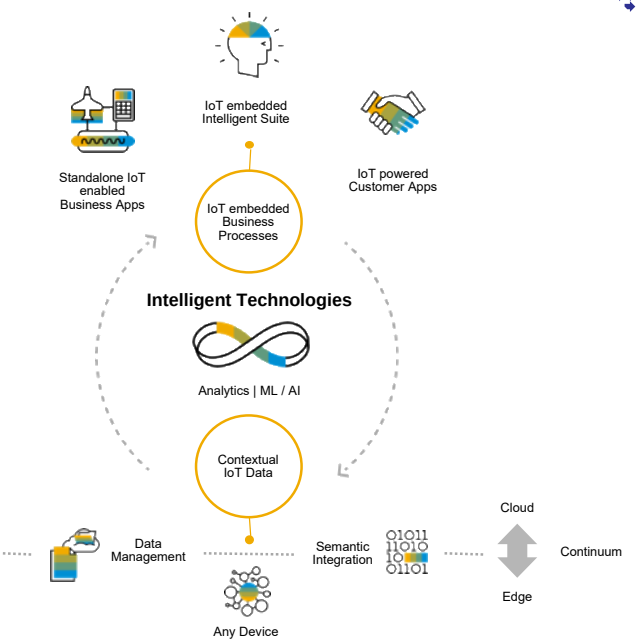
In combination with innovative technologies such as machine learning and AI, IoT has been a driving force of the Intelligent Enterprise.

Advances in ubiquitous connectivity and edge computing are driving a step change in business productivity. Connectivity, coupled with IoT, artificial intelligence and machine learning, enable us to analyse petabytes of data and affect business outcomes.

As an example: although manufacturers have been using the Internet of Things for some time, now the entire value chain can be connected – from development to production to supply chain. Data-driven insights can drive customer-centric innovation, lower material costs, and reduce risk. Remote assets condition monitoring provides real-time data, to predict maintenance needs and identify potential quality problems before they occur. Assets can be jointly managed as digital twins by manufacturers, customers, and partners, thereby improving asset utilization and reliability.

Advanced analytics enables business users to analyse data on the fly and drives better decision-making. Empowered users, benefiting from embedded analytics and IoT in business processes, can get real-time visibility into their changing environment, simulate the impact of business decisions, mitigate risk, and achieve better customer outcomes.

It's clear that truly powerful outcomes arise when intelligent technologies are brought together with business processes already in play or are aimed to support new ones.



Typically, IoT data is made available to different applications across departments within a company, for a variety of decisions to be made or actions to be performed.

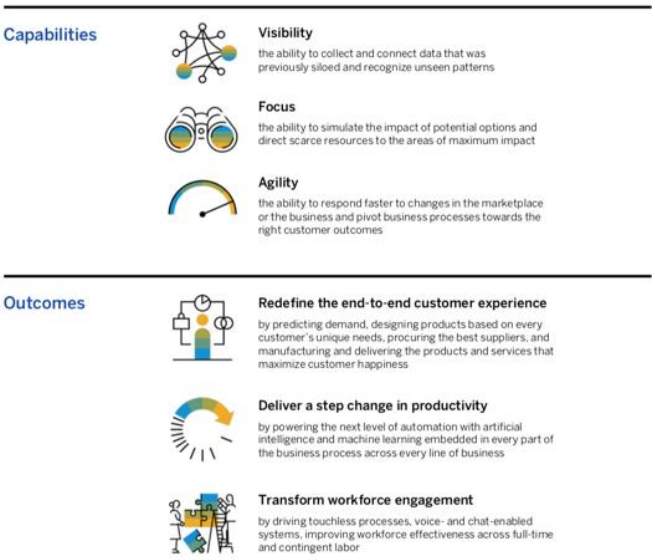
- Remaining lifetime calculations create a dynamic maintenance scheduling process. It includes time-of-arrival forecasts to improve logistics operations, and early detection of product issues to increase service delivery effectiveness and customer satisfaction.
- Information on product usage and quality is used by engineering, manufacturing, field services, maintenance, and sales teams.
- In connected hydrocarbon logistics, a product planner and scheduler might learn that a jobber is lifting less than forecasted. This will affect revenue and create a containment issue at the terminal if the product isn't moved. In the connected world, the system will automatically generate a number of cost-ranked options to move product. The product scheduler can then look on the network to identify potential transportation assets that can be employed in the movement.
- Real-time monitoring of temperature, humidity, and location of goods that are in transit as well as those stored in warehouses serve to optimize Cold chain logistics, as well as overall supply chain planning.
- Supporting technology, such as sensors, speech recognition, and automated documentation, releases nurses from traditional, routine tasks, freeing them up for more time with patients. They can focus on value-adding activities, such as interaction, providing advice, and planning recovery, making for an improved patient experience.

Therefore, IoT projects focus less on technology and more on ways to enable desired outcomes.

IV. What Is the Value?

In today's world, the concept of best practices is becoming increasingly outdated. Winners are characterized by one main characteristic: speed. First mover advantage in creating new markets and capturing mindshare is more critical than ever. These winners have adopted a set of "next practices" that help them innovate faster than the competition.

These next practices are defined by a set of capabilities and outcomes that are made possible by disruptive technologies. While the capabilities themselves may not be new aspirations for the enterprise, the Intelligent Enterprise delivers these capabilities better, faster, and more completely than ever before.



In speaking with CEOs today, they see significant business implications across three dimensions:

- **Drive customer experience** – Reimagine end-to-end customer journeys from the point of first interaction to fulfilment to post-sales and boost loyalty across complete customer lifetime.
- **Deliver step change in productivity** – Through a combination of digital technologies and process simplification and automation, companies can achieve 15 – 20 % productivity gains. This completely transforms the cost structures and value chains across industries.
- **Transform the way we work and engage employees** – Touchless systems, automated processes, and other similar technologies will become the norm. These will augment human capabilities and enable employees to focus on value-added work and manage exceptions and innovation.

V. How to Get There

It's better to change while you can, rather than when you have to.

Speed matters.... The first companies that lead the move will have an edge. They can keep on improving their processes with more data and intelligence, while their competitors try to catch up.

Most companies are adopting the change in a step manner, instead of waiting for proven end-to-end solutions and technology stack. It is a long journey, so the sooner you start, the sooner you will be able to compete in the experience economy.

However, transformation to an intelligent enterprise requires an end-to-end plan. This includes creating an intelligent enterprise roadmap and implementation plan.

Proven best practices, industry-specific expertise and optimal deployment options, should ensure continuous innovation with a focus on intelligent outcomes.

VI. CONCLUSION

Intelligent enterprises empower employees through process automation. This empowered workforce will be able to focus on high-value activities like customer success, strategic planning, and innovation.

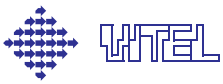
When interaction shifts to digital, it becomes far easier for customers to switch to other providers, especially with new disruptive market entrants. New approaches and business models are required to attract and retain customers. Companies will need to anticipate and proactively respond to customer needs, creating personalized and unique customer experiences using AI, chatbots, and voice technologies to deliver best in class customer service. The imperative for change is clear and the difference between winners and losers will be their ability to digitally transform and embrace intelligent technologies and major trends shaping the future of the industry.

REFERENCES

[1] SAP® Leonardo Internet of Things: Business Outcomes in a Connected World
[2] SAP References, Performance Benchmarking and Industry Whitepapers
[3] Mckinsey (Digital Quotient)
[4] Mckinsey (Industry 4.0)
[5] WEF/AT Kearney

ABOUT THE AUTHOR

Jelena Ilic is industry value advisor at company SAP SEE, helping companies to realize value of SAP solutions and run at their best. She is consulting professional with long track in enterprise software and telecommunication industry.



Podporniki

Sponzors

TelekomSlovenije

ISKRATEL

ERICSSON

arnes

Iskra

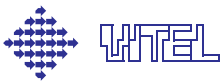
AMITEH

ROHDE&SCHWARZ

Univerza v Mariboru

Fakulteta za elektrotehniko, računalništvo in informatiko

Univerza v Ljubljani
Fakulteta za elektrotehniko



Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije