UDC: 621.39(497.11)
DOI: http://dx.doi.org/10.7708/ijtte2023.13(1).08

PROTECTION OF TELECOMMUNICATION INFRASTRUCTURE USING IOT ECOSYSTEM OF TELEKOM SRBIJA

Vladan Nešić[1], Ljubomir Mrđenović[2], Ivan Petrović[3], Mirjana D. Stojanović[4]
[1,2,3] *Telekom Srbija a.d., Belgrade, Serbia*
[4] *University of Belgrade – Faculty of Transport and Traffic Engineering, Serbia*

Received 18 January 2023; accepted 26 February 2023

Abstract: Telekom Srbija is the first operator in the Western Balkan region with its own Internet of Things (IoT) ecosystem. The ecosystem is characterized by the following features: multitenant IoT platform; Long Range Wide Area Network (LoRaWAN) connectivity; technology proven through industry use cases with a large number of sensor devices and the associated application software; platform and application programming interfaces (APIs) for fast implementation and integration of new commercial use cases, and large capacity for fast network deployment. On that way, business partners are provided with a powerful environment for implementation of different use cases. The first use case based on this ecosystem referred to preventing theft of the company's underground telecommunication infrastructure. This article represented the state-of-the-art, the IoT ecosystem of Telekom Srbija, and the use case regarding protection of the underground cable infrastructure.

Keywords: application programming interface, IoT ecosystem, IoT platform, LoRaWAN, security.

1. Introduction

Development of advanced information and communication technologies (ICT) reduces the boundaries between traditional industrial sectors, which enabled the proliferation of the fourth industrial revolution (Industry 4.0) and implementation of the wide spectrum of innovative technical and technological solutions. New technologies are a driving force for telecommunication companies, which quickly adapt to changes, to explore new business areas, regarding ICT services and solutions, digital multimedia services, financial aspects, etc. The Internet of Things (IoT) has been defined by the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) in the Recommendation ITU-T Y.4000 (former Y.2060) as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (ITU-T, 2012, p. 1).

IoT applications include, but are not limited to: smart homes and smart buildings, agriculture, connected vehicles, traffic monitoring, asset tracking, supply chain management, manufacturing, smart grids, warehouse management, healthcare, wearables, pet tracking, alarm systems, etc.

[4] Corresponding author: m.stojanovic@sf.bg.ac.rs

Telekom Srbija, as a leader in the ICT field in Serbia, is the first telecom operator in the Western Balkan region, which in 2017 initiated the application of new technologies based on machine-to-machine (M2M) solutions, and commenced a series of workshops in order to implement the first project based on IoT, which nowadays has a significant practical application. A successful implementation of the first IoT project highlighted in the foreground the cooperation with start-up companies, which thereafter continued successful business ventures on the new use cases.

This article presents the main concepts of the initial IoT system of Telekom Srbija, which is applied daily, and is permanently developing and expanding. The use case presented in this article refers to implementing a reliable and robust protection system in order to prevent thefts of the underground cable infrastructure. Such an initiative has opened a treasure trove of ideas that can be realized in the IoT platform environment of Telekom Srbija.

The rest of the article is organized as follows. Section 2 describes the background and related work. The architecture of the IoT ecosystem of Telekom Srbija is presented in Section 3. Section 4 presents a use case, related to the application of the IoT ecosystem for protection of the Telekom Srbija telecommunication infrastructure. Section 5 concludes the article.

2. Background and Related Work

2. 1. Basic Features, Application and Expansion of IoT Systems

The reference model of IoT system is not yet standardized, although there are several proposals for layered system architectures, including three-layer architecture, five-layer architecture, cloud-based architecture and fog-based architecture (Sabry, Qarabash, & Obaid, 2019; Salih, Rashid, Radovanovic, & Bacanin, 2022). According to Rupareliya (2021), the IoT architecture "can be explained as a system in which there are various elements, protocols, sensors, cloud services, actuators and layers". Four interconnected stages of the IoT architecture are identified, as illustrated in Fig. 1. They include: (1) sensors and actuators; (2) gateways and data acquisition systems; (3) edge information technology and (4) data center and the cloud.

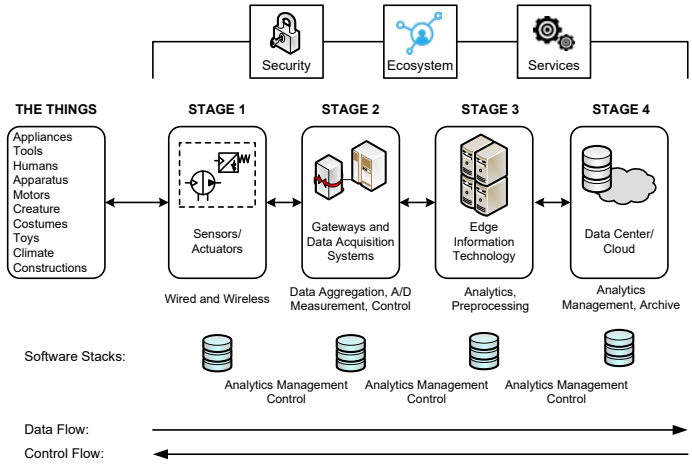


Fig. 1.
The Four-Stage IoT Solutions Architecture
Source: (adapted from Rupareliya, 2021)

Communication technologies and protocols play a significant role in IoT systems for the purpose of efficient and reliable data exchange in the network. Protocols specify data exchange formats, addressing mechanisms, coding, flow control, error control, and routing principles. Different "things" in the IoT system may pose different requirements for quality of service, security and reliability, typically with very low energy consumption in heterogeneous and/or variable working conditions. The main IoT standards include Radio Frequency Identification (RFID), Near-Field Communication (NFC), Wireless Fidelity (Wi-Fi, IEEE 802.11), Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4) and IPv6 for Low power Wireless Personal Area Networks (6LoWPAN). The aforementioned technologies are designed for short-range communications.

Low Power Wide Area Networks (LPWANs) have been designed for long-range communications in IoT systems, with the following features:

- Low energy consumption of IoT devices, which is of the crucial importance for the equipment without the external power source, to extend the battery lifespan;
- Large area coverage (focused or unfocused);
- Economic efficiency and availability to a broad range of users.

There are two key types of LPWAN technologies deployed on licensed spectrum, Long Term Evolution - Machine type communication (LTE-M) and Narrow Band IoT (NB-IoT). On the contrary, Long Range WAN (LoRaWAN) and SigFox have taken the top positions in the unlicensed spectrum band (Pena Queralta, Gia, Zou, Tenhunen, & Westerlund, 2019). The position of LPWAN in the world of wireless systems, regarding data rate and power consumption vs. range, is depicted in Fig. 2.

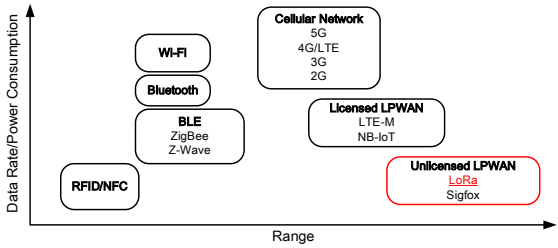


Fig. 2.
The Position of LPWAN in the World of Wireless Systems
Source: (adapted from Rajab, Ebrahim, & Cinkler, 2021)

LoRaWAN is a new industrial standard, proposed by LoRa Alliance, which demonstrates excellent performance and open network architecture as the main prerequisites for a cost-effective implementation of IoT systems. Main features of LoRaWAN include star topology, long range (several times higher than the cellular network) and excellent indoor coverage. End IoT devices experience a prolonged battery lifespan (from 10 to 20 years, depending on the traffic intensity and consumption optimization). LoRaWAN networks are cost effective, due to lower costs of the infrastructure in comparison with some previous solutions; besides, costs of the end equipment are also lower, thus making it available for a large number of end users. Detailed considerations on the LoRaWAN technology can be found in the literature (Ertürk, Aydın, Büyükakkaşlar, & Evirgen, 2019; Haxhibeqiri, De Poorter, Moerman, & Hoebeke, 2018).

The use experience points to conclusions that IoT technology enables creation of the business value through reduction of operational expenses, better risk management, as well as increase of new sources of income through digital business models and the next generation technologies. Market research companies forecast a tremendous growth of IoT connections in the next years (IoT Analytics, 2020; Nešić, Mrđenović, Petrović, & Stojanović, 2022; Rupareliya, 2021).

Besides sensors and applications, the IoT interconnects heterogeneous entities, such as mobile devices, computers and all types of objects that can be connected to the Internet and mutually interact under automatic control or human control. The IoT concept evolves in several directions, including the industrial IoT, Internet of vehicles, Internet of energy, Internet of nano-things, towards a paradigm of mutually connected people, data, processes and things, which is known as the "Internet of Everything" (IoE) and illustrated in Fig. 3 (Farias da Costa, Oliveira, & de Souza, 2021; Miraz, Ali, Excell, & Picking, 2018).

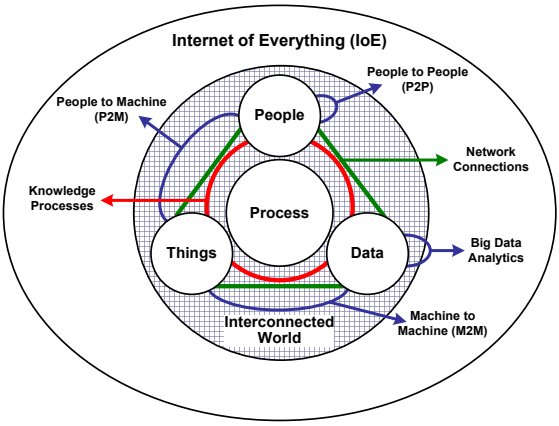


Fig. 3.
Illustration of the IoE Concept

2.2. Related Work

IoT platforms are applied in different use cases and for various business goals. Among the global telecom players that have already experienced the benefits of implementing IoT-based end-to-end solutions are O2, AT&T, Telefónica, NTT Docomo, SK Telecom, Vodafone, Deutsche Telekom, and others. The best IoT use cases across the industry are illustrated in Fig. 4, and include IoT connectivity services, data analytics, asset monitoring, solutions for cloud services such as PaaS (Platform as a Service) and SaaS (Software as a Service), as well as data storage and management (Epam Anywhere, 2022).

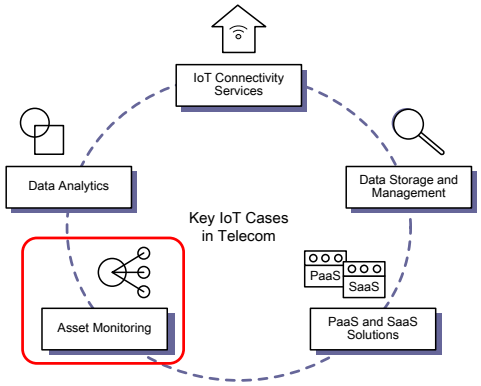


Fig. 4.
Key IoT Cases in Telecom

Asset monitoring is one of the crucial IoT use cases, because telecom operators use a huge amount of heterogeneous equipment. Hence, it is necessary to: (1) quickly track system failures and serious interruptions in work; (2) be able to response to global catastrophes and (3) implement reliable and robust protection systems in order to prevent theft of expensive and critical equipment. The capabilities of IoT can help in meeting these challenges. IoT sensors collect and analyze data from various sources, and also allow identifying the problems, responding to them, and carrying out a real-time surveillance. IoT devices allow efficient management of facilities, monitoring incidents, and detecting disasters in time. Besides, IoT technologies offer a strong potential to improve physical security, including IoT-based smart cameras and different types of special-purpose devices.

An IoT platform is a set of components that allows developers to deploy the applications, remotely collect data, secure connectivity, and execute sensor management. It also allows developers to build new desktop and mobile software applications. There are more than 1000 open-source and commercial IoT platforms on the market today, most of them providing services such as device, data and connection management.

Some authors distinguish four types of IoT platforms, namely IoT cloud platforms, IoT connectivity platforms, IoT device platforms and IoT analytics platforms (Murphy, 2021). Their main features are as follows:

- *IoT cloud platforms* provide a number of cloud services, from collecting and transmitting IoT data from end devices to storage and analysis. They are also known as end-to-end platforms because of the capability to provide all the services for the particular use case including connectivity and device management;
- *IoT connectivity platforms* (also known as mediation platforms) typically provide specific support for devices that rely on cellular or LPWAN technologies, meaning the data must flow through a wireless WAN before reaching the Internet. Such platforms manage data flows and often include services like geo-location, over-the-air updates and remote provisioning;
- *IoT device platforms* provide the hardware components needed to design and develop IoT devices.
- *IoT analytics platforms* typically provide a number of machine learning or artificial intelligence methods to enable a comprehensive support for big data processing and analytics.

Rupareliya (2021) provided an exhaustive list of the most popular IoT platforms together with the description of their main features. Some of them are Google Cloud Platform, IRI Voracity, Particle, Salesforce IoT Cloud, IBM Watson IoT, ThingWorx, Amazon AWS IoT Core, Microsoft Azure IoT Suite, Samsung Artik Cloud, Oracle IoT, Cisco IoT Cloud connect, Altair SmartWorks, Raspberry Pi, etc. Guth *et al.* (2016) provided a detailed comparative analysis of open-source platforms OpenMTC4, FIWARE2, and SiteWhere5, and the proprietary solution of Amazon Web Services, especially with regards to their architectures. Mineraud, Mazhelis, Su, and Tarkoma (2016) reviewed 39 platforms regarding seven criteria, including support of heterogeneous devices, type and architecture of the platform, open source, APIs, data access control and service discovery. El-Shweky *et al.* (2018) provided a comparative analysis of IoT architectures, platforms and applications, with a case study to illustrate the

main IoT concepts and levels of abstraction. Further, a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis was conducted to assess the present and the future use of IoT solutions. Toutsop, Kornegay, and Smith (2021) presented a comparative analysis of several commercial and open-source IoT platforms, including Arm Pelion, Microsoft Azure cloud, ThingWorx, FIWARE, and ThingSpeak. The analysis encompassed system architecture, management schemes, protocols, interoperability, and security, based on the experimentation with real-world IoT devices.

Among IoT connectivity platforms, the most widespread is the ThingPark Wireless, which is a multi-technology, open, hardware agnostic IoT platform developed by the French vendor Actility (Actility, 2023). It allows to deploy LPWAN worldwide, and integrates the most advanced LoRaWAN network server, as well as low-power cellular networks (LTE-M, NB-IoT) and satellite radio networks. LoRaWAN and the ThingPark Wireless platform cover a wide spectrum of use cases, creating value from disruptive IoT solutions. Examples of use cases are: Industry 4.0, smart cities, energy and utilities, logistics and supply chains, smart buildings, precision agriculture, etc.

SourceForge ranks the best alternatives to ThingPark Wireless in 2023 (SourceForge, 2023). Some of them are: akenza, QlikTag Platform, EMnify, Sigfox, ZohoIoT, mimic edgeEngine, myDevices, Nubix, Insight Connected Platform, Kazuhm, Eclipse Kura, Things5, Journeyware, Qopper, Embiot, Thingstream, etc. However, to the best of our knowledge, comparative studies regarding the features of those platforms have not yet been published.

3. IoT Ecosystem of Telekom Srbija

According to Narayan (2022), the IoT ecosystem can be defined as "a network of interconnected devices existing in a specific environment that collects data and transmits it to people who use modern technologies". The seven major components of an IoT ecosystem are: IoT devices, security, network, gateway, cloud, application and users. The IoT ecosystem of Telekom Srbija has been developed as a result of the strong motivation for implementing the innovative standards, especially when the innovation allows for the development of partner's ecosystem and specific solutions – use cases with optimization/combination of technological modules of different vendors (Telekom Srbija, 2020). Such openness to partnership in finding and developing new use cases and new customers is enabled by the availability of all IoT components.

The basic system elements are as follows:

- Sensors – class A, B or C (Fig. 5), with the battery lifespan from 10 to 20 years and activation using over-the-air-authentication (OTAA) or activation-by-personalization (ABP) procedures;
- LoRaWAN network, consisting of the omnidirectional base stations and gateways, with the range 2-3 km in urban areas (densely populated) and 15-20 km in the rural areas. The network covers large cities as well as most of communication lines on the territory of Serbia;
- IoT platform for system monitoring and management, as well as development of simple applications;
- Application for monitoring and management of devices.

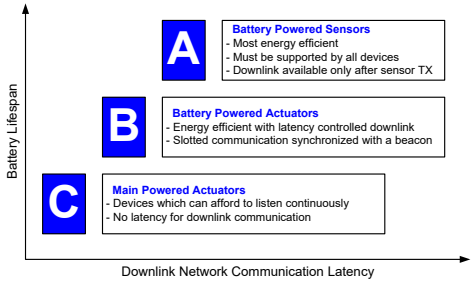


Fig. 5.
Sensor Classes: Battery Lifespan vs. Downlink Network Communication Latency

The IoT platform of Telekom Srbija consists of the two basic components: (1) ThingPark Wireless platform at the network layer and (2) Application Enabled Framework (AEF) – a platform intended for management and development of applications, as well as big data analytics, as illustrated in Fig. 6. This composite software platform is located in the company's cloud and implements standardized solutions for cyber security. The system is elastic, which means that it is adaptable to changes of workload by dynamic provisioning of the required resources in an autonomous way. Open services of other subsystems and platforms may enrich particular use cases in the sense of billing system, sales support, etc.

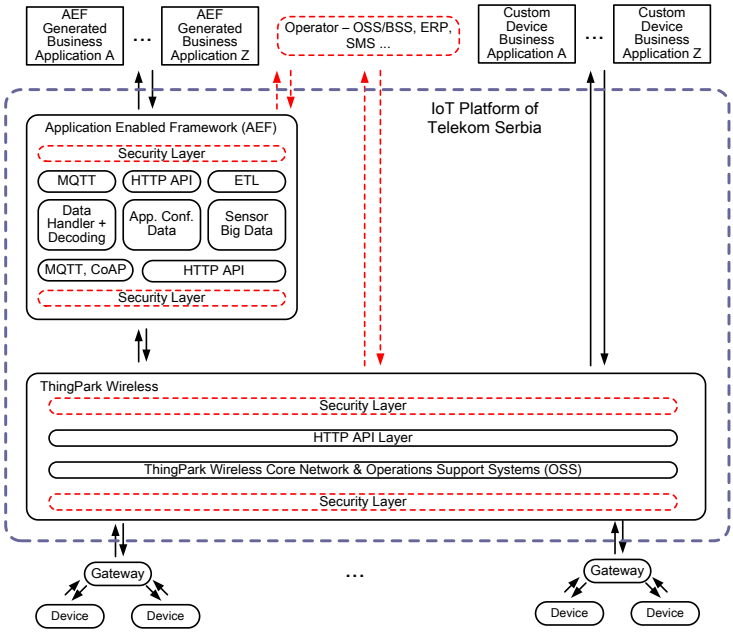


Fig. 6.
The IoT Platform of Telekom Srbija

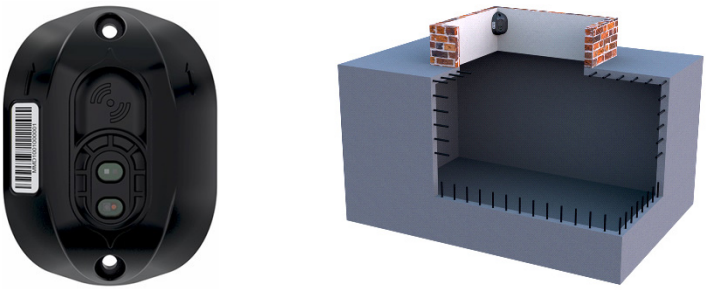
As already mentioned, the ThingPark Wireless is one of the most powerful and advanced IoT connectivity platforms. Specifically designed for telecom operators and service providers, this platform meets all requirements for connectivity, security, management and monetization of public LPWANs. Some more features will be listed here:

- ThingPark Wireless is fast to deploy, fully scalable, and able to manage unlimited numbers of sensors;
- The platform is fully modular, and intended for the unlimited number of use cases;
- Large capacity of interconnected devices and users is supported;
- Open interfaces are available through different web services, primarily the Representational State Transfer (REST) API, which uses the standard HyperText Transfer Protocol (HTTP) methods for API calls;
- A suitable graphical user interface (GUI) simplifies implementation of different use cases;
- The platform is agnostic, i.e., it enables different types of connectivities;
- The platform interacts with the edge gateways, as well as with the AEF platform, operator's software and enables creation of custom device business applications.

The AEF is based on the IoT analytics platform of the French vendor BUSIT, and performs data handling and decoding, application configuring, and big data analytics. The ETL module extracts, transforms, and loads data from multiple sources to a unified data repository. The AEF implements standard IoT protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP). The use of AEF platform enables a standardized way of service development and provisioning, i.e., a relatively simple development of different business applications. This platform also interacts with operator-specific applications such as operations support system/business support system (OSS/BSS), enterprise resource planning (ERP), short message service (SMS), etc. Thus, a basis is provided for fast implementation and integration with the other internal and/or external platforms.

4. Use Case: A System for Telecommunication Infrastructure Protection

The goal of the project was to solve problems such as: long-term theft of copper cables, multi-million damage, risk of violating reputation, collateral damage due to traffic loss and user dissatisfaction due to service interruptions. A special emphasis is on service interruption of business customers. It should be noted that the problem of telecommunication infrastructure protection could not be solved earlier, mainly because of technical reasons, including lack of power supply for detecting devices and their weak autonomy (up to one year).



(a) (b)

Fig. 7.
A Multi-Sensor IoT Device for Telecommunication Infrastructure Protection: (a) Appearance of the Device; (b) Mounting of the Device in the Cable Manhole

The designing task (Telekom Srbija, 2021) encompassed the following requirements:

- The position of the cable manhole, as an element of the cable canalization, is under the ground, with low signal availability, which required a more dense network;
- Dimensions of the manhole entrance are 60 cm x 60 cm, which required that the IoT device be as small as possible, and positioned in the corner of the manhole.;
- Place of installation of the device is often exposed to unfavorable atmospheric conditions such as moisture, large temperature range, mud, ice, etc. IoT device has to be hermetically sealed, with independent power supply, cooling and heating;
- Quick and easy installation is needed, regarding large number of devices;
- Guaranteed battery lifespan should be more than 10 years;
- Security mechanisms are needed to prevent theft, equipment damage or disabling, and to reliably detect intrusions;
- A layered approach to system management is required, with the reporting subsystem which provides short-term and long-term analytics, while the management process is achieved through a multi-level access control (administrator, read-only, control center, supervisory center, maintenance, security agency);
- Definition of process and procedural reaction mechanisms of different entities is required (procedures for regular entrance, irregular entrance, maintenance, etc.).

The design was done in cooperation with the start-up company Bitgear. As a result, the original and unique multi-sensor IoT device was created. The appearance of the device is presented in Fig. 7a, while the place of installation of the device in the cable manhole is presented in Fig. 7b.

The main features of the multi-sensor IoT device for telecommunication infrastructure protection are as follows:

- Ambient light – minimum threshold sensitivity of 0,045 lux enables detection of the opening of the manhole cover, even in the dark chamber;
- Proximity – the device detects the presence of an obstacle and is activated when entering the manhole;
- The magnetometer detects the change of magnetic field and is activated when the magnetic field above the manhole is disturbed;
- The anti-masking sensor reacts to masking trials, e.g., in the case when the intruder tries to misuse entering to the manhole and to disable the sensor;
- The accelerometer detects move along three axes, and is activated due to vibrations, for example, opening of the manhole cover, drilling a hole, etc;
- The temperature sensor detects increase in temperature, for example in the case of the fire nearby;
- The moisture sensor alerts that the place is flooded;
- The device is resistant to impacts and fully compliant with the IK10+ standard (IEC, 2002);
- The device is waterproof and fully compliant with the IP67 standard (IEC, 2001).

The functional architecture of the system for cable infrastructure protection is depicted in Fig. 8.

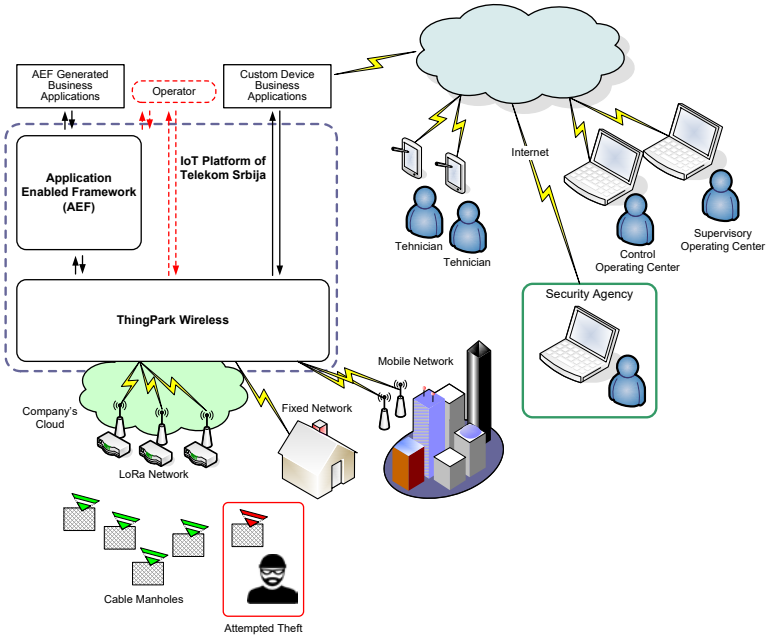


Fig. 8.
The Functional Architecture of the System for Cable Infrastructure Protection

The attempted theft is registered by the multi-sensor IoT device, and the alert message is generated and forwarded to the IoT platform, using LoraWAN infrastructure. Using IoT platform, the user-oriented desktop application is

developed and integrated with the local geographic information system (GIS) for easier viewing. Besides, the application for mobile devices is developed for the purpose of terrain works. After receiving the alarm message, several organizational entities react in accordance with the predefined procedures, including control operating center, supervisory operating center and security agency. Particularly, the security agency (as a trusted third-party entity) goes to the terrain, equipped by navigation with all relevant information about the alarm type. After identifying the perpetrator of theft, the appropriate legal procedures are initiated.

5. Conclusion

Today, the IoT market is developing intensively and is bringing a number of benefits regarding the improvement of quality in different areas of human activity. This article presented the IoT ecosystem of Telekom Srbija, based on the powerful composite IoT connectivity and analytics platforms. Moreover, the article described one of the first use cases implemented using the ecosystem in order to protect the underground telecommunication infrastructure of the company. As a result, the original and unique multi-sensor IoT device was created, together with control desktop and mobile applications based on the IoT platform. In this way, a decades-long problem of cable theft was successfully solved. This pioneering venture shows that large projects can be successfully implemented in cooperation of telecom operators and business enterprises. The project also represents a driving force and provides a technological basis for implementation of other IoT systems, such as smart homes, smart cities, industrial IoT, etc.

References

Actility. 2023. ThingPark®, the leading IoT Mediation Platform. Available from Internet: < https://www.actility.com/>.

El-Shweky, B. E.; El-Kholy, K.; Abdelghany, M.; Salah, M.; Wael, M.; Alsherbini, O., et al. 2018. Internet of Things: A comparative study. In *Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 622-631. DOI: 10.1109/CCWC.2018.8301678.

Epam Anywhere. 2022. Internet of Things in Telecom: How your business gains revenue growth with IoT. Available from Internet: <https://anywhere.epam.com/business/iot-in-telecommunications>.

Ertürk, M. A.; Aydın, M. A.; Büyükakkaşlar, M. T.; Evirgen, H. 2019. A Survey on LoRaWAN architecture, protocol and technologies, *Future Internet* 11(10): 216. DOI: 10.3390/fi11100216.

Farias da Costa, V.C.; Oliveira, L.; de Souza, J. 2021. Internet of Everything (IoE) taxonomies: A survey and a novel knowledge-based taxonomy, *Sensors* 21(2): 568. DOI: 10.3390/s21020568.

Guth, J.; Breitenbücher, U.; Falkenthal, M.; Leymann F.; Reinfurt, L. 2016. Comparison of IoT platform architectures: A field study based on a reference architecture. In *Proceedings of the 2016 Cloudification of the Internet of Things (CIoT)*, 1-6. DOI: 10.1109/CIOT.2016.7872918.

Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. 2018. A survey of LoRaWAN for IoT: From technology to application, *Sensors* 16(18): 3995. DOI: 10.3390/s18113995.

International Electrotechnical Commission (IEC). 2001. *Degrees of protection provided by enclosures (IP Code)*. IEC 60529:2001. Geneva, Switzerland: IEC.

International Electrotechnical Commission (IEC). 2002. *Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code).* IEC 62262:2002. Geneva, Switzerland: IEC.

International Telecommunication Union – Telecommunication Standardization Sector (ITU-T). 2012. *Overview of the Internet of Things. ITU-T Recommendation Y.4000/Y.2060*. Geneva, Switzerland: ITU-T.

IoT Analytics. 2020. Cellular IoT & LPWA connectivity market tracker. Available from Internet: <https://iot-analytics.com>.

Mineraud, J.; Mazhelis, O.; Su, X., Tarkoma, S. 2016. A gap analysis of Internet-of-Things platforms, *Computer Communications* 89-90: 5-16. DOI: 10.1016/j.comcom.2016.03.015.

Miraz, M. H.; Ali, M.; Excell, P. S.; Picking, R. 2018. Internet of Nano-Things, Things and Everything: Future growth trends, *Future Internet* 10(8): 68. DOI:10.3390/fi10080068.

Murphy, M. 2021. What is an IoT platform and how do you choose the right one for your business? Available from Internet: <https://www.hologram.io/blog/iot-platform-overview/>.

Narayan, V. 2022. IoT ecosystem – what is it & what are its key elements. Available from Internet: <https://thinkpalm.com/blogs/iot-ecosystem-what-is-it-what-are-its-key-elements/>.

Nešić, V.; Mrđenović, Lj.; Petrović, I.; Stojanović, M. D. 2022. IoT ecosystem of Telekom Srbija. In *Proceedings of the XL Symposium on Novel Technologies in Postal and Telecommunication Traffic – PosTel 2022*, 259-268. (In Serbian). DOI: 10.37528/FTTE/9788673954165/POSTEL.2022.027.

Pena Queralta, J.; Gia, T. N.; Zou, Z.; Tenhunen, H.; Westerlund, T. 2019. Comparative study of LPWAN technologies on unlicensed bands for M2M communication in the IoT: beyond LoRa and LoRaWAN, *Procedia Computer Science* 155: 343-350. DOI: 10.1016/j.procs.2019.08.049.

Rajab, H.; Ebrahim, M.; Cinkler, T. 2021. Reducing power requirement of LPWA networks via machine learning, *Pollack Periodica – An International Journal for Engineering and Information Sciences* 16(2): 86-91. DOI:10.1556/606.2020.00263.

Rupareliya, K. 2021. Top IoT development tools & platforms with comparison. 2022. Intuz. Available from Internet: <https://www.intuz.com/blog/top-iot-development-platforms-and-tools>.

Sabry, S. S.; Qarabash, N. A.; Obaid, H. S. 2019. The road to the Internet of Things: A survey. In *Proceedings of the 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)*, 290-296. DOI: 10.1109/IEMECONX.2019.8876989.

Salih, K. O. M.; Rashid, T. A.; Radovanovic, D.; Bacanin, N. 2022. A comprehensive survey on the Internet of Things with the industrial marketplace, *Sensors* 22(3): 730. DOI: 10.3390/s22030730.

SourceForge. 2023. Alternatives to ThingPark Wireless. Available from Internet: <https://sourceforge.net/software/product/ThingPark-Wireless/alternatives>.

Telekom Srbija. 2020. *IoT Ecosystem of Telekom Srbija*. Internal technical documentation.

Telekom Srbija. 2021. *The System for Protection of the Underground IT Infrastructure*. Internal technical documentation.

Toutsop, O.; Kornegay, K; Smith, E. 2021. A comparative analyses of current IoT middleware platforms. In *Proceedings of the 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud),* 413-420. DOI: 10.1109/FiCloud49777.2021.00067.