doi: 10.36689/uhk/hed/2019-01-012

The Application of IoT in the Area of Detection

Petr DOUCEK, Milos MARYSKA, Lea NEDOMOVA

University of Economics Prague, Prague, Czech Republic
{doucek, maryska, nedomova}@vse.cz

Abstract. The article presents the application of Internet of Things (IoT) technologies in the distribution of utilities. The presented application – detection of the integrity of seals of meters of certain utilities (water, gas or electric power) - is based on an extensive analysis of opportunities in applying the IoT principles to the distribution of utilities, in particular the distribution of electric power. One of the opportunities with rather high expectations from distributors is detection of the integrity of meter seals. The article includes a proposal of the technical solution of such an IoT application and discusses the cost-effectiveness of the solution. We have reached the conclusion that an isolated implementation of IoT technology is much more expensive than the currently used solution, which is based on labor and on having meters checked by people. Another way to increase the cost-effectiveness of IoT devices is to add the function of remote meter reading and its follow-up interconnection with data mining technologies and the evaluation of a large volume of data. However, this addition goes beyond the scope of this article.

Keywords: Internet of Things, Energy Industry.

1 Introduction

The potential of applications that are generally referred to as Internet of Things (IoT) has developed gradually – from its use in detecting the level of beverage cooling [6], to its application in systems with Radio-Frequency Identification (RFID) technologies [1] all the way to nowadays its very important role in the world of information and communication technologies (ICT). By the year 2013, IoT had developed into a system that combines a very big quantity of different technologies with various functions and uses different communication protocols. For instance, sensors, GPS and mobile equipment, devices monitoring the movement of equipment, their remote switching off or on, etc. The definition of IoT as a dynamic global network infrastructure, with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information system, has been generally accepted during the past two years [7].

One of the areas of implementation of IoT technologies is their use in the production, services and distribution of gas, potable water and electric power – utilities in general [4]. We have conducted a survey concerning the applicability of individual solutions in

this area from a technological and economic perspective [8]. This article focuses on one application opportunity only, which is the detection of broken seals of utility meters. Broken seals are a critical problem especially when it comes to major customers but often also when it comes to small customers [2]. A typical example is the use of this technology in the case of problematic customers who have tried to commit fraud in the past, as well as customers inclined to commit fraud based on data mining results.

Electronic seals with remote detection help to reduce or mitigate non-technical losses caused by ignoring the fact that the seals were broken or that the sealed sensor or a part thereof was tampered with until such a fact is detected [11]. Non-technical losses, also referred to as commercial losses, include e.g. un-metered fixed takeoffs, metering mistakes, billing or recording mistakes, incorrect meter installation, takeoffs below the sensitivity limit of electrometers, etc.

The application opportunity of electronic seals is based on the principle of metering the resistance wire [3]; if it is damaged, interrupted or short-circuited, the sensor will immediately send information about such damage through the IoT network [5]. The resistance wire is either placed next to the mechanical seal, provided that there is enough room, or is a part of the mechanical seal and is placed in the fixed insulation. The purpose is to monitor on-line any seal breaking at the site of all customers [2].

2 Problem Formulation

The use of IoT in this industry is very topical. One of the important applications is monitoring whether or not seals on different devices, mainly on meters, have been broken [3]. The goal of this article is to propose and analyze the potential use of IoT solutions in monitoring the integrity of seals on meters of utilities (e.g. water, electric power, gas, etc.).

A similar principle can also be applied to other areas to detect the integrity of seals. For this reason, this is very topical because by solving this problem, companies may save a lot of money, mainly in case of dishonest customers.

3 Methodology

The basic data identified for this article mostly come from an extensive survey among experts from the energy supply industry [12] in the Czech Republic [10]. The survey among 50 experts from different business companies and universities was conducted at the turn of 2016 and 2017.

To obtain relevant data, over 67 two-round workshops were conducted. The first round included 50 structured workshops, using questionnaires. Our questionnaires' for asking questions and identifying technologies for IoT and business opportunities were based on the technique of guided questioning, with the use of open and closed questions [9].

Once all 50 workshops were finished, we processed and evaluated the data from the questionnaires that helped us to combine any identified duplicate application opportunities and to create a set of unique application opportunities.

In the second round of 17 workshops, experts and academicians evaluated 124 identified application opportunities and assigned to them priority from 1 to 3, where 1 was the most important and 3 the least important in terms of implementation [8].

It is important to add that the list of identified opportunities may always change, depending on workshop participants and actual changes of information technologies in IoT.

4 Results

A complete detailed overview of the results is provided and commented on in the article [8]. It is important to mention that we identified 16 application opportunities with priority 1, 20 application opportunities with priority 2 and 25 application opportunities with priority 3. The remaining 63 application opportunities were not assigned any priority due to differently evaluated factors, such as importance, costs, implementation speed, societal benefits, etc.

As already mentioned, in this article we focus on one of the application opportunities with priority 1, specifically on the implementation of the system detecting the integrity of seals [3].

The entire systematic solution for detecting the integrity of seals can be divided into five steps:

- Technical solution;
- Sensors;
- Communication in the IoT network;
- Work with data prior to transmission;
- Power supply.

4.1 Technical Solution – Description

An electronic seal is a simple device that measures the resistance of the resistance wire. This resistance wire responds not only to its interruption but also to its short-circuit or crossover. It also responds to any attempt to break it by dropping it or tampering with it. Based on the aforesaid, we can say that the transmission of information about a broken seal does not require any major data flow (alarm message, daily heartbeat device – a heartbeat is a simple message that is regularly sent to confirm that the device is properly working). In view of this fact, a low-energy IoT network can be used for transmission [12]. The message is sent on a one-off basis – it is not a regular transmission.

4.2 Sensors

A sensor means a general device that can be used to detect any seal tampering and that transmits information about a broken seal.

Different types of sensors can be used to detect a broken seal. One of them is a sensor that uses the resistance wire. The resistance wire can usually also recognize a short-circuit caused by a person trying to break the seal and to overcome its protection by causing a short-circuit on metering terminals.

A sensor can also be used to monitor several different circuits. Each of them is then monitored by a separate circuit with the resistance wire. In such a case, each circuit is connected to a single shared sensor and if the seal is broken, we know that it was broken on some of the connected circuits. However, we cannot tell which seal was broken. This is how we can secure several separate parts of metered devices. But it requires that the devices (seals) are not too far from each other. As an example, we can mention a breaker panel with circuit breakers on a floor in a block of flats or an office building. Let's assume that there are four apartments on one floor whose electrometers are in a shared breaker panel in the hallway. In such a case, it is possible to connect the seals on each of the four electrometers to one sensor. In the case that one of the seals is broken, we will know the location and will check only those four seals.

We propose e.g. SIGFOX as a transmission IoT network because, based on conducted tests, it is much more resistant against tampering than other low-energy IoT networks and also is the only network with sufficient all-state coverage (resistance citation).

What is also important about these solutions is that the device sends a heartbeat message with information about battery voltage both during transmission and in the idle state together with the chip temperature on a regular basis, usually every 24 hours. Another important part is the unique identification of the sensor (its ID). Every sent message is signed and encoded into a hash message by the algorithm AES128. This guarantees the integrity of the transmitted message.

4.3 Communication in the IoT Network

The device in IoT networks usually does not register in the network when sending data. The device sends the message immediately upon the data transmission request. No confirmation of message receipt is usually required in the IoT network. The robustness and guaranteed likelihood of message delivery is achieved by the following mechanisms:

- The message is typically sent three times in a row. This minimizes the risk that the message will not be delivered;
- IoT networks are usually designed in a way to make sure that the sent message could be received by the maximum number of base stations;
- An identifier is automatically assigned to every message by a protocol implemented in the modem. The identifier is automatically escalated to easily and quickly find out that some message was not delivered. In such a case, the receiving device can generate a defined event and inform the user about lost data;
- In the case that no message from the end equipment is received for a certain time, the data receiving system can regenerate the event and forward it to the user in a standard way.

4.4 Work with Data Prior to Transmission

It is often discussed whether or not it is necessary to process the data prior to transmission. In the case of this type of message and communication, it is not necessary to process the data in any major way. A defined information message is transmitted from the sensor only if the status changes (a specific event occurs), e.g. the resistance wire is interrupted, the seal is tilted or opened, etc.

4.5 Power Supply

Power supply is another important parameter of IoT solutions. A battery is usually used for this type of sensor. Considering how it is used (sending a heartbeat message once every 24 hours), its useful life is at least 7 years. The device is designed as low-energy because it is independent of any external source of energy to ensure that the seal could not be tampered with during a power outage.

5 Discussion

The survey among sensor manufacturers showed that the price of an IoT device with an electronic seal is about 2,500 CZK. The cost of device installation and operation in the given IoT network must be added to this price.

When speaking of costs, we must always take into consideration benefits, proceeds or the reduction of other related costs.

When there are no technologies or no technologies are used that inform the utility provider about a problem on the device, the device must be checked by a person. Let's assume that during a work shift one person can check 80 meters on average (10 meters per hour during an 8-hour work shift). It is an average value; more meters can be checked in a housing development in Prague than in the countryside where it takes several or even dozens of minutes to get from one meter to another.

Therefore, one person can check about 1,600 meters per month and thus about 19,000 meters per year. If we assume about 500,000 apartments, we will need at least 27 employees who will check and monitor the situation once a year. Considering the average wage in Prague, which is about 40,000 CZK, it amounts to 19 million CZK in annual costs (when considering the company's costs and disregarding bonuses). To this amount, we must add the employee's cost of transportation between metering stations and the ineffective loss of his time, etc. The annual costs will be about 25 million CZK.

If we implement seals for all users, the cost will be extreme. It will be about 1,5 billion CZK. Therefore, this solution does not seem profitable when considering the annual savings of about 20 million CZK (the checking of broken seals will continue). However, we must also take into account the potential savings resulting from a timely detection of fraud, the consequent cost of collecting the due amount or potential court fees and legal costs, etc. This part, however, is hard to estimate at this moment without having detailed knowledge of the data.

This situation could be resolved by a combination of advanced data analysis technologies and behavior pattern identification, based on which it would be possible

to identify the customer groups with a higher risk of fraud. In such a case, seals could be installed only on these devices, which would considerably reduce costs. There could be a marketing campaign communicating that the given company started using modern methods of detecting fraud and that these methods will be used for certain customer groups. This will raise general awareness about how easy it is to detect fraud, which will further reduce the potential risk of losses caused by fraud.

6 Conclusions

There are a lot of IoT devices that can be applied in different areas of human activities, e.g. an IoT device monitoring the movement of vehicles to prevent unnecessary trips, a device monitoring parking lot occupancy, a device monitoring excessive noise and many others.

In this article, we focused on one specific application opportunity, which is the use of IoT sensors to monitor the integrity of seals. Seals in general are devices that protect service providers against unauthorized use. It could be a provider of some utility, such as water, electric power or gas. In these cases, end customers have a meter with a seal installed to protect utility providers against unauthorized takeoffs.

In the context of our article, unauthorized takeoffs are identified thanks to a broken seal that is connected to a sensor. In case the seal is broken, the sensor will identify this fact and will alert the service provider. This way the provider is immediately informed about the problem and can appropriately respond.

The main benefits of these solutions are as follows:

- Immediate detection of a broken seal;
- Identification of the location where the seal was broken;
- Easy installation;
- Low operating costs;
- Low investment costs – seals can be installed only at the site of customers who - based on other analyses - were identified as potentially risky.

Negative factors include the limited useful life of the device, which is usually up to seven years thanks to the installed battery. This disadvantage is however compensated by the fact that e.g. water meters are replaced once every five years. Gas meters and electrometers are replaced about this often as well.

Acknowledgements. Paper was processed with contribution of long term support of scientific work on Faculty of Informatics and Statistics, University of Economics, Prague (IP 400040).

References

1. Ashtone, K.: Ashton, K.: That 'Internet of Things' Thing. RFID Journal 2009. June 22. https://www.rfidjournal.com/articles/view?4986, last accessed 2018/10/26.
2. Childs, P.R.N.: Mechanical Design Engineering Handbook. Butterworth-Heinemann, (2014).
3. Dolan, P J.: Mechanical Seal Review Fluid Sealing. pp. 413-427. Springer, Dordrecht (1992).
4. Doucek, P., Pavlíček, A., Luc, L.: Internet of Things or Surveillance of Things? In: Tjoa A.M. et al. (eds.), Proceedings of the 11th IFIP WG 8.9 Working Conference, CONFENIS 2017 Research and Practical Issues of Enterprise Information Systems, LNBIP, vol. 327, pp. 45–55. Springer, Cham (2018). DOI: 10.1007/978-3-319-94845-4_5.
5. Espinoza, F., Maryska, M.: Low Power Wide Area Networks, Comparison in the Context of the Czech Republic. In: Doucek, P. Chroust G., Oškrdal V. (eds.), Proceedings of the 26th Interdisciplinary Information Management Talks IDIMT-2018 Strategic Modeling in Management, Economy and Society, pp. 65–72. Trauner Verlag Universität, Linz (2018).
6. Foote, K., D.: A Brief History of the Internet of Things, Data Education for Business and IT Professionals, http://www.dataversity.net/brief-history-internet-things/, last accessed 2018/11/10.
7. van Kranenburg, R.: The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID. Institute of Network Cultures, Amsterdam (2008).
8. Maryska, M., Doucek, P., Nedomova, L., Sládek, P.: The Energy Industry in the Czech Republic: On the Way to the Internet of Things. Economies, 6(2), 1-13 (2018). DOI: 10.3390/economies6020036
9. Řezanková, H.: Analýza dat z dotazníkových šetření. 2nd ed. Praha: Professional Publishing, Czech Republic (2010).
10. Sládek, P., Maryska, M.: The Business Potential of Emerging Technologies in the Energy Industry, In: Doucek, P. Chroust G., Oškrdal V. (eds.), Proceedings of the 26th Interdisciplinary Information Management Talks IDIMT-2018 Strategic Modeling in Management, Economy and Society, pp. 57–64. Trauner Verlag Universität, Linz (2018).
11. Yibo E.F., Fengshou G., Andrew B.: A review of the condition monitoring of mechanical seals, In: Proceedings of the ASME 7th Biennial Conference on Engineering Systems Design and Analysis, pp. 179-184. American Society of Mechanical Engineers (ASME), (2004).
12. Yuan, H., Zhao, J., Li, Y., Zhang, J., Mei, N.: 2017 : Energy analysis of a subsea steam Rankine cycle for the subsea power supply. In: Caetano, N.D.; Felgueiras, M.C. (eds.), Proceedings of the 4th International Conference on Energy and Environment Research, ICEER 2017, pp. 444-449. Elsevier (2017).