A Markov Model of Healthcare Internet of Things System Considering Failures of Components

Anastasiia Strielkina[0000-0002-7760-7367], Vyacheslav Kharchenko[0000-0001-5352-077X] and Dmytro Uzun[0000-0001-5574-550X]

National Aerospace University "KhAI", Kharkiv, Ukraine
{a.strielkina, v.kharchenko, d.uzun}@csn.khai.edu

Abstract. An active infiltration of information technology in the healthcare sector has led to a fundamental change in people's quality of life. In this regard, the security and safety problems of this technology using increase rapidly. This paper touches upon the issue of the healthcare Internet of Things (IoT) infrastructure failures of components and complete system. The purpose of the paper is to develop and research an availability model of a healthcare IoT system regarding failures of components. A detailed analysis of an architecture of healthcare IoT infrastructure is given. The main causes of the healthcare IoT based system failures are considered. Much attention is given to developing and research of a Markov model of a healthcare IoT system considering failures of components. Some essential high-level requirements that such system must meet are presented. The analysis of obtained simulation results showed the rates that have the greatest influence on the availability function of the healthcare IoT system.

Keywords: Availability Function, Cloud, Failure, Insulin Pump, Internet of Things, Markov Model.

1 Introduction

1.1 Motivation

The paradigm of the Internet of Things (IoT) implies the possibility of massively and inexpensively connecting to an information network (for example, the Internet) any physical object and control systems for these objects. IoT in general promises textually to every citizen and every company, regardless of the industry - its own set of benefits and improvements, savings and growth, the release of time and new opportunities. On the basis of these statements, the IoT has already found applying in many industries. According to predictive forecasts [1-2], the number of networked and connected devices will increase to 25.6 billion. In 2017 IoT has been ranked as the first among the eight breakthrough technologies that can change the business model of companies or entire industries, advancing artificial intelligence, augmented reality, technology related to the creation and management of the drones, blockchain etc [3]. The IoT has

already a great impact in many economical areas [4] as transport, energy, healthcare, industry, agriculture, wearables, smart retails, smart homes, etc.

One of the most promising and already most advanced industries are medicine and healthcare. Networked medical and healthcare devices and their applications are already creating an Internet of Medical and/or Healthcare Things which is aimed at better health monitoring and preventive care for creating better conditions for patients who require constant medical supervision and/or preventive intervention. Healthcare and medical organizations (providers) also attempt to collect and analyze data that generate the IoT devices that are essential for prospective innovations.

One of the most sought-after fields in healthcare and medicine treatment, monitoring and prognosis is Diabetes. According to [5] an estimated 422 million adults were living with diabetes in 2014, compared to 108 million in 1980, the global prevalence of diabetes has nearly doubled since 1980, rising from 4.7% to 8.5% in the adult population, it caused 1.5 million deaths in 2012, and higher-than-optimal blood glucose caused an additional 2.2 million deaths and they predict that Diabetes will be the 7th leading cause of death in 2030.

But the new concepts and applying of new technologies bring certain risks including failures of devices, infrastructure which may lead to the worst outcome - the death of the user (patient). Hence to minimize such risks and assure required availability the system models and strategies of maintenance should be developed and researched.

1.2 State-of-the-Art

For today there are a lot of papers that describe opportunities and benefits of using smart and intellectual technologies in the field of healthcare and medicine and at the same time they describe the security and safety problems of this technology using.

One of the most famous and almost all covering paper is [6]. The authors tried to show all the healthcare IoT trends, solutions, platforms, services and applications. They outlined main problems during development and using of such devices related mostly to standardization and regulatory issues. In addition, that paper analyzed healthcare IoT security and privacy features, including requirements, threat models, and attack taxonomies and proposed an intelligent collaborative security model to minimize security risk. But the authors did not address the issues of reliability and safety analysis, did not consider the possible failures of the healthcare IoT system and its particular components and the influence on performance.

The authors of [7] presented three use cases for quality requirements for IoT in healthcare applications. One of them is for safety and violence. They gave a simple construct for a patient or caregiver safety use case. Also, they refer to the US Underwriters Laboratories [8] and as well recommended using “traditional techniques for defining misuse and abuse cases”.

Goševa-Popstojanova and Trivedi in [9] provided an overview of the approach to reliability assessment of systems. The architecture of system could be modeled as a discrete time Markov chain, continuous time Markov chain, or semi-Markov process.

The Markov model that takes into account the technical conditions of typical network components of the IoT-based smart business center was presented in [10].

In [11] was proposed a Markov Queuing approach to analyzing the Internet of Things reliability with some experimental results.

The paper [12] describes an approach to developing a Markov models' set for a healthcare IoT infrastructure that allows taking into account safety and security issues. It details the models sets for the healthcare IoT system based on Markov process approach.

Nevertheless, despite a large number of researches regarding healthcare IoT, there are no papers that consider safety and reliability issues of healthcare IoT systems taking into account failures of hardware and software components and system failures.

1.3 Objectives, Approach and Structure of Paper

The goal of the paper is to analyze and develop a model that describes the healthcare IoT system failures and their influence on availability indicators. Our approach is based on review of the variety of existing techniques and mathematical models for similar systems and step by step development of a set of states and transitions caused by failures of system components.

In this context, the paper proposes the Markov model describing possible failures of healthcare IoT system and recovery procedures. The remainder of this paper is organized as follows. The second section describes an architecture of healthcare IoT infrastructure and possible failures during its operation. The third is devoted to the development of the Markov model of a healthcare IoT system considering failures of components and analyzing simulation results. The last section concludes and discusses future research steps.

2 Analysis of Healthcare IoT Failures

2.1 The Architecture of Healthcare IoT Infrastructure

Analysis of the latest publications related to this topic [6, 11, 13] allows us to present a generalized architecture of the healthcare IoT infrastructure that can be seen in Fig. 1.

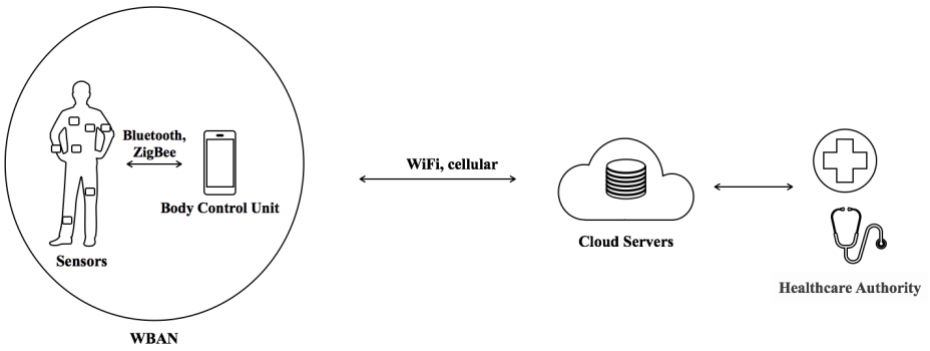

Fig. 1. The general architecture of healthcare IoT infrastructure.

Thereby it is possible to identify the main components and subcomponents of healthcare IoT system. They are:

- Wireless body area network (WBAN) consists of different sensors located in different parts of human's body and body control unit. Sensors are used to record physiological processes and convert the received data into a format convenient for perception and analysis. There are different kinds of medical sensors and first of all they are classified as consumer products for health monitoring, wearable external, internally embedded and stationary [14]. These sensors or even devices can capture such data as blood pressure, temperature, electrocardiogram (ECG), electroencephalogram (EEG), accelerometer, the global positioning system (GPS), electromyography (EMG), etc. Data collected by sensors are transmitted to the body control unit using e.g. Bluetooth or ZigBee protocols. The control unit is designed to read reports, monitor status, change settings, and update the device's firmware. It can directly connect to Cloud servers if it has WiFi or cellular interfaces or through monitoring unit using Bluetooth or WiFi;
- Cloud servers provide easy access to servers, storage, databases and a wide range of software services on the Internet. The main purposes of the cloud are storage, analytics, and visualization. Clouds provide reception of telemetry data in the required volume from the devices and determination of the way of processing and storing the obtained data, allow healthcare telemetry analysis to provide valuable information both in real time and later and send commands from the cloud or gateway device to a specific healthcare device. Also, the server part of the Internet of things' cloud should provide the device registration capabilities that allow preparation of the device and control which devices are allowed to connect to the infrastructure and device management for monitoring the status of devices and monitor their actions. Using cloud services, it is possible to effectively store and dynamically process data, interact and integrate data;
- A healthcare authority pulls an analytical report for each patient to check the patient's illness status. He evaluates the data and sends a notification. The patient receives a notification that advises whether to consult a doctor.

In this paper, the main subject of the study is an insulin pump operating in the infrastructure of the IoT. An activity diagram for the insulin pump operating independently without interaction with other devices or Internet was described in [15]. The author illustrated how the software transforms an input blood sugar level to a sequence of commands that drive the insulin pump. Fig. 2 shows an improved version for the insulin pump operating in the infrastructure of IoT and interaction with other components.

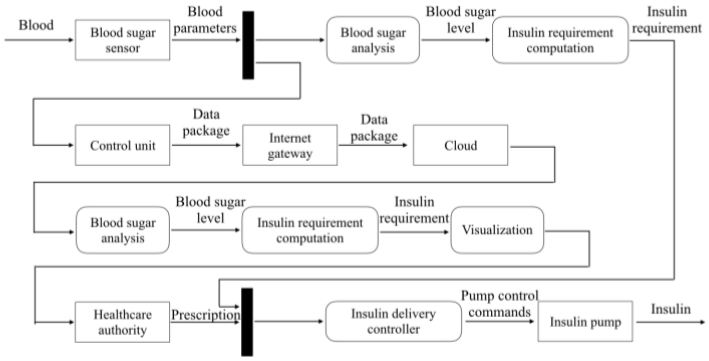

Fig. 2. High-level processes for the insulin pump in the context of IoT.

The data from the blood sugar sensor send to the blood sugar analysis and insulin requirement computation what is carried out by integrated technical possibilities and tools of the insulin pump and/or sends to the Cloud servers via the Internet gateway for further processing, storage, and visualization. The patient's data can be analyzed using e.g. artificial intelligence tools in the Cloud. The decision made by artificial intelligence tools sends to the healthcare authority for the conclusive prescription and finally to the patient or insulin pump user. In more details, decisions that were made by the healthcare authority are also loaded into the Cloud, and then insulin pump user (control unit) downloads prescriptions.

2.2 Analysis of Failures

It is clear that the healthcare IoT based system is a safety-critical system. If the pump or any other significant element fails to operate or does not operate correctly, then the patients' health may be damaged or they may fall into a coma because their blood sugar levels are too high or too low, or the doctor's prescription is not received by the patient, etc. There are, therefore, some essential high-level requirements that such system must meet:

1. The system shall be available to deliver insulin when required.
2. The system shall perform reliably and deliver the correct amount of insulin to counteract the current level of blood sugar.
3. Any component of the IoT system shall interact with any other when required.
4. The system shall be able to scale.
5. The Cloud component shall be able to process, storage and visualize all patients' data when required.
6. The healthcare authority component shall be able to respond to all patient requests when required, etc.

Thereby as in any other information and technology systems, failures also may occur in the IoT based systems. Fig. 3 depicts in outline the main causes of healthcare IoT based system failures.

In papers [14 - 20] were described failures of insulin pumps that were caused by different reasons (e.g. sensors failure, control unit failure due to hardware and/or software, etc.). Analysis of papers [21 - 24] shows the possible failures of Cloud servers. These failures are caused due to software failure, hardware failure, scheduling, service failure, power outage, denser system packaging, etc. Accordingly, it is possible to assert that the reasons of failures may be variable and depend on failures of healthcare IoT infrastructure each component.

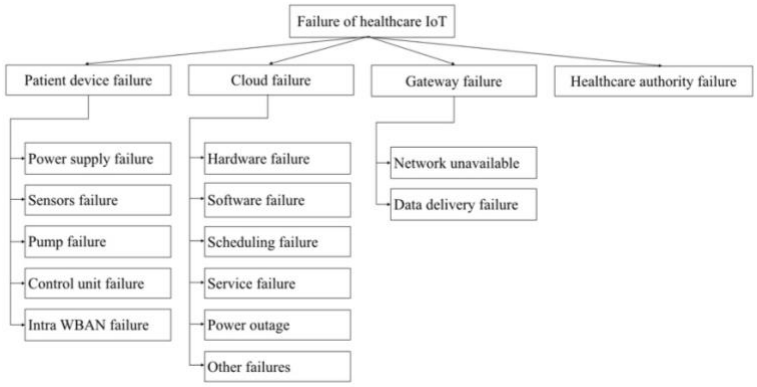

Fig. 3. Classification of healthcare IoT failures.

3 Case Study: A Markov Model of Healthcare IoT System

3.1 Markov Model Development

In [11] basic models were described, in details, simple cases with a few models of healthcare IoT system based on the queueing theory. These models describe streams of the requests and attacks on vulnerabilities and procedure of recovery by a restart and eliminating of ones. In this paper, the model of the functioning of the main components of healthcare IoT system is proposed. The assumptions in the development of the model are the failure of rate is constant, the model does not take into account eliminating of any reasons because of what failures caused.

In general, in the healthcare IoT system, the failures of single subcomponents are possible. These failures may lead to the failures of the main components of infrastructure (i.e. insulin pump, cloud, etc.). In its turn, the failures of main components may lead to failure of the whole healthcare IoT system. Fig. 4 shows the dependence of the healthcare IoT system failures, where 0 – there is no any failure in the system, 1 – there is one failure (of subcomponent), 2 – there are two failures (subcomponent and main element), 3 – there are three failures (the failure of the whole healthcare IoT system).

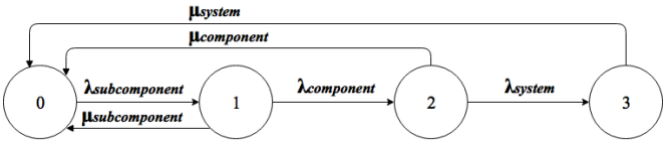

Fig. 4. Dependence of the healthcare IoT system failures.

In more details Fig. 5 shows a Markov graph of the functioning of the main components of healthcare IoT system during failures, λ - the failure rate, μ - the recovery rate. Thereby, the basic states of the healthcare IoT system are: 1 - normal condition (upstate) system; 2 - failure due to the power supply (battery) pump causes discharge, recharging and/or causing damage; 3 - failure of any one and/or more sensors of the insulin pump due to the out-of-order, does not deliver any output to inputs, delivers null output values and/or no meaningful values and/or impurity etc.); 4 - pump failure (inaccurate size/rate of insulin dose) due to the components defects, improper position of pump, ambient temperature, air pressure and/or design errors etc.; 5 - software of insulin pump control module failure due to buffer overflow or underflow, incorrect libraries, wrong algorithms or programming, threshold setting error etc.; 6 - hardware of insulin pump control module failure due to overheating, short or open circuit, high leakage current, high or low impedance, missed alarm, false alarm, fail to read/write data and/or design error etc.; 7 - intra wireless body area network (WBAN) communication failure due to the packet loss, isolation, a communication module failure (e.g., L2CAP, BNEP etc.), header corruption and/or length mismatch and/or payload corruption etc.; 8 - insulin pump (as the patient's complex) failure due to the failure of any one or more main components; 9 - extra gateway communication partial failure due to data delivery failures; 10 - extra gateway communication partial failure due to Bluetooth/cellular/WiFi network unavailable; 11 - partial failure due to the refusal of the mobile application of the reader (control unit); 12 - cloud software failure due to planned or unplanned reboot, software updates and/or complex design; 13 - cloud hardware failure due to hard disk failures, RAID controller, memory and/or other devices; 14 - cloud scheduling failure due to overflow and/or timeout; 15 - cloud service failure due to request stage and/or execution stage; 16 - cloud failure due to power outage; 17 - cloud failure due to the failure of any one and/or more cloud components; 18 - failure due to incorrect assignment or programming of the device by a healthcare authority related to device functions or lack of functions; 19 - failure of the IoT healthcare system.

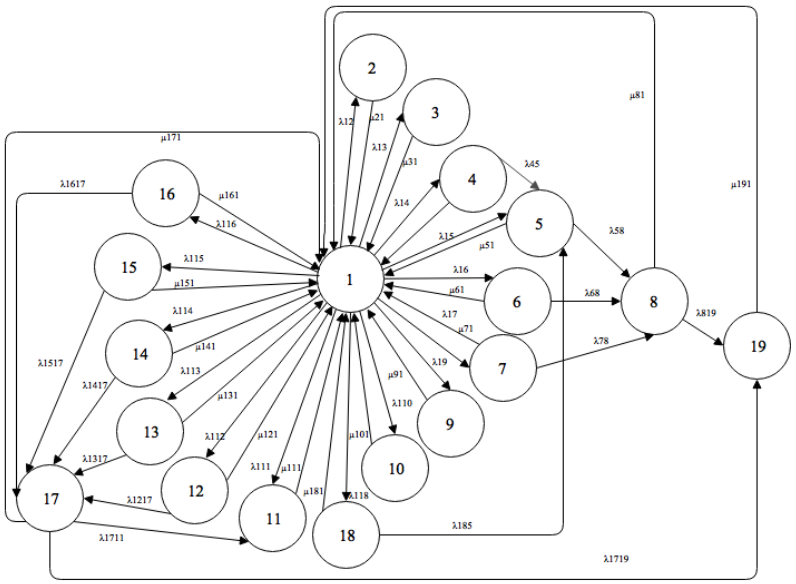

Fig. 5. A Markov's graph of healthcare IoT failures.

A system of Kolmogorov differential equations for presented Markov model is:

$$dP_1 / dt = -(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15} + \lambda_{16} + \lambda_{17} + \lambda_{19} + \lambda_{110} + \lambda_{111} + \lambda_{112} + \lambda_{113} + \lambda_{114} +$$
$$+\lambda_{115} + \lambda_{116} + \lambda_{118})P_1(t) + \mu_{21}P_2(t) + \mu_{31}P_3(t) + \mu_{41}P_4(t) + \mu_{51}P_5(t) + \mu_{61}P_6(t) +$$
$$+\mu_{71}P_7(t) + \mu_{81}P_8(t) + \mu_{91}P_9(t) + \mu_{101}P_{10}(t) + \mu_{111}P_{11}(t) + \mu_{121}P_{12}(t) + \mu_{131}P_{13}(t) +$$
$$+\mu_{141}P_{14}(t) + \mu_{151}P_{15}(t) + \mu_{161}P_{16}(t) + \mu_{171}P_{17}(t) + \mu_{181}P_{18}(t) + \mu_{191}P_{19}(t);$$

$$dP_2 / dt = -\mu_{21}P_2(t) + \lambda_{12}P_1(t);$$

$$dP_3 / dt = -\mu_{13}P_3(t) + \lambda_{13}P_1(t);$$

$$dP_4 / dt = -(\mu_{41} + \lambda_{45})P_4(t) + \lambda_{14}P_1(t);$$

$$dP_5 / dt = -(\mu_{51} + \lambda_{58})P_6(t) + \lambda_{16}P_1(t) + \lambda_{45}P_4(t) + \lambda_{185}P_{18}(t);$$

$$dP_6 / dt = -(\mu_{61} + \lambda_{68})P_6(t) + \lambda_{16}P_1(t);$$

$$dP_7 / dt = -(\mu_{71} + \lambda_{78})P_7(t) + \lambda_{17}P_1(t);$$

$$dP_8 / dt = -(\mu_{81} + \lambda_{819})P_8(t) + \lambda_{58}P_5(t) + \lambda_{68}P_6(t) + \lambda_{78}P_7(t);$$

$$dP_9 / dt = -\mu_9P_9(t) + \lambda_{19}P_1(t);$$

$$dP_{10} / dt = -\mu_{101}P_{10}(t) + \lambda_{110}P_1(t);$$

$$dP_{11} / dt = -\mu_{111}P_{11}(t) + \lambda_{111}P_1(t) + \lambda_{1711}P_{17}(t);$$

$$dP_{12} / dt = -(\mu_{121} + \lambda_{1217})P_{12}(t) + \lambda_{112}P_1(t);$$

$$dP_{13} / dt = -(\mu_{131} + \lambda_{1317})P_{13}(t) + \lambda_{113}P_1(t);$$

$$dP_{14}/dt = -(\mu_{141} + \lambda_{1417})P_{14}(t) + \lambda_{114}P_1(t);$$
$$dP_{15}/dt = -(\mu_{151} + \lambda_{1517})P_{15}(t) + \lambda_{115}P_1(t);$$
$$dP_{16}/dt = -(\mu_{161} + \lambda_{1617})P_{16}(t) + \lambda_{116}P_1(t);$$
$$dP_{17}/dt = -(\lambda_{1711} + \lambda_{1719} + \mu_{171})P_{17}(t) + \lambda_{1217}P_{12}(t) + \lambda_{1317}P_{13}(t) + \lambda_{1417}P_{14}(t) +$$
$$+\lambda_{1517}P_{15}(t) + \lambda_{1617}P_{17}(t);$$
$$dP_{18}/dt = -(\mu_{181} + \lambda_{185})P_{18}(t) + \lambda_{118}P_1(t);$$
$$dP_{19}/dt = -\mu_{191}P_{19}(t) + \lambda_{919}P_8(t) + \lambda_{1719}P_{17}(t).$$

Initial values are:

$$P_1(0) = 1, Pi(0) = 0, i = 2,3, \ldots, 19.$$

To solve a system of the linear Kolmogorov differential equations it is necessary to carry out the collection and analysis of statistics on failures of healthcare IoT systems.

3.2 Simulation of the Developed Markov Model

Hence the initial data for Markov model simulating were taken from [16, 18-20] for the insulin pump failures, for the Cloud failures [22-24] and experts' assessments. Due to the heterogeneous nature and complexity of statistical data, and not to overflow with excess information, the sequence of rates' calculations and the rates are not given in this paper.

The working state is state 1, and eighteen others are states with failures of different components and parts of the healthcare IoT system. The obtained probabilities of finding the healthcare IoT system in each state of Markov model are shown below (stationary values):

P1 = 0.9853745;	P2 = 0.000103622;	P3 = 0.003330566;
P4= 0.000251795;	P5 = 0.001162896;	P6 = 0.0003859747;
P7 = 0.006145591;	P8 = 0.0009757008;	P9 = 0.001486934;
P10 = 0.0006328081;	P11 = 3.207395e-05;	P12 = 3.070724e-05;
P13 = 1.056492e-05;	P14 = 2.90451e-05;	P15 = 2.596815e-05;
P16 = 5.734457e-06;	P17 = 3.038937e-08;	P18 = 1.545724e-05;
P19 =2.957985e-08.		

Hence A(t) = P1(t). Fig. 6 shows the availability function changing before a transition to the stationary value ($A_{stationary}$ = 0.9853745). According to the simulation results the function gets a qua approximately at step 2300 h, i.e. 3 months later after beginning of work.

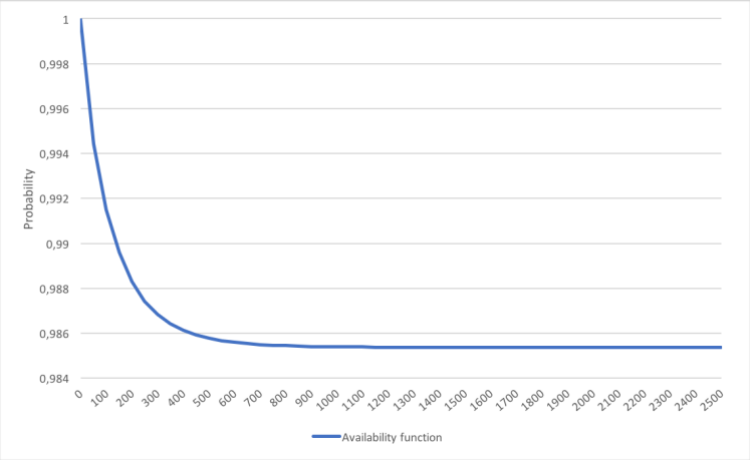

Fig. 6. Availability function changing before a transition to the steady-state value.

Fig. 7 – 10 show the dependence of the availability function changing depending on the different types of failures changing on the healthcare IoT systems rates.

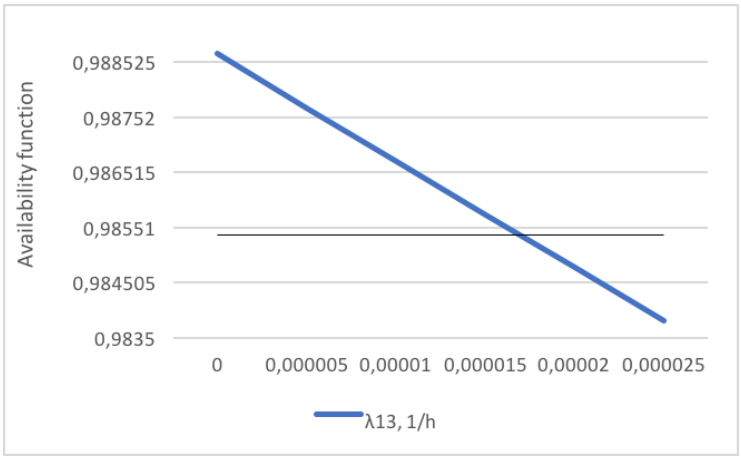

Fig. 7. Dependence of the availability function changing depending on the changing λ13 rate.

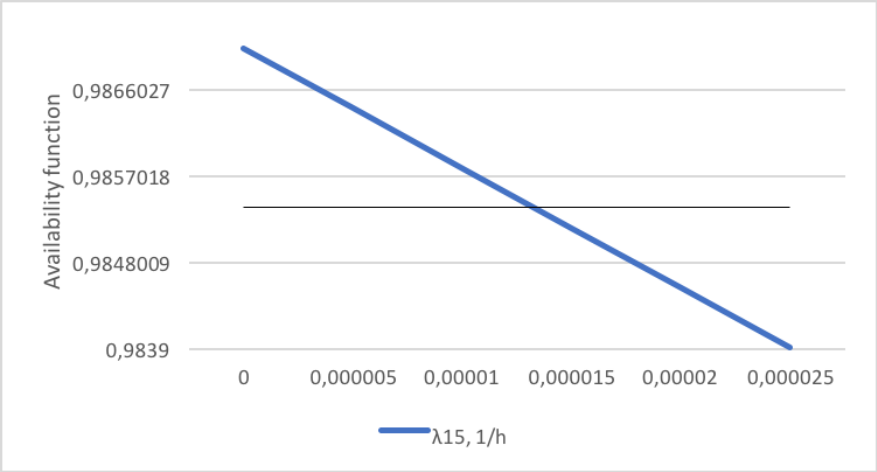

Fig. 8. Dependence of the availability function changing depending on the changing λ15 rate.

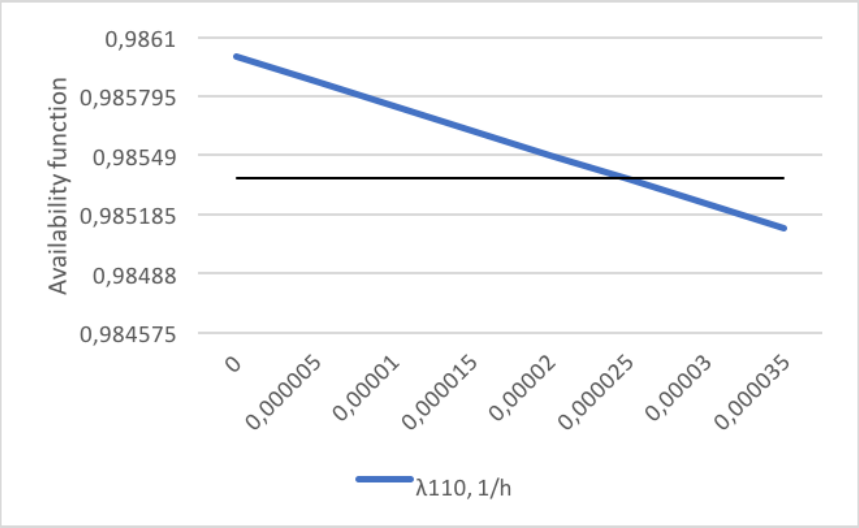

Fig. 9. Dependence of the availability function changing depending on the changing λ110 rate.

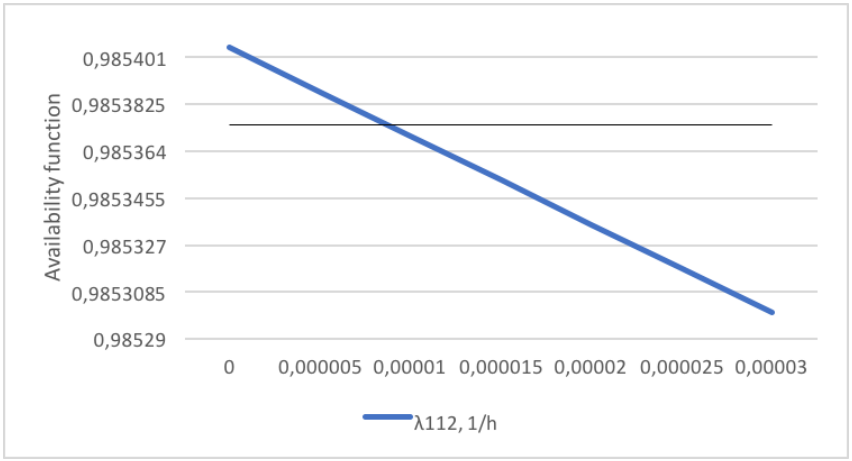

Fig. 10. Dependence of the availability function changing depending on the changing λ112 rate.

The obtained results analysis shows that the greatest influence on the change in the availability function is the λ15 rate and the next is the λ13 rate (i.e. different components of the patient device (for our case of insulin pump) failures). The least influence has the failures of cloud components due to the rapid recovery time. These results are confirmed by statistical data.

The analysis of obtained results shows that the complete failure of the healthcare IoT system does not happen too often (one case on the analyzed time interval due to the complete failure of the Cloud). Nevertheless, failures of constituent elements of the system arise quite often that may affect the performance of mission-critical functions of the healthcare IoT system and in the worst case, lead to the death of the patient. The most often failures are due to the failure of the insulin pump and its particular elements and components and some components of the Cloud.

Availability of the system can be improved by more fast recovery (repair) of the equipment and system resources and application of more reliable devices.

4 Conclusions and Future Work

Due to the use of the IoT technologies, the interaction of objects, environment, and people will be extremely active, and it is making it possible to hope that the world will be "smart" and a well-appointed for a person. However, at the same time, the IoT faces a number of problems that can prevent us from taking power of its potential advantages.

In this paper, the overview of the healthcare IoT system failures is presented. Based on the conducted analysis and classification of the main possible failures of healthcare IoT infrastructure a Markov model considering failures of components is constructed. For the developed model probabilities of finding IoT system in each state of Markov model are shown. The obtained results show possible most frequent failures of healthcare IoT system. The presented Markov model can be used not only for the

availability evaluation of insulin pumps but for other healthcare devices operating in IoT system.

Next steps of research will be dedicated to a development of more general dependability models for healthcare IoT systems and combining results of this paper and models taking into account both the reliability, safety and security requirements and issues.

Acknowledgements

This paper implies results obtained during involvement in the Erasmus+ programme educational project ALIOT «Internet of Things: Emerging Curriculum for Industry and Human Applications» (reference number 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, web-site http://aliot.eu.org) in which the appropriate course is under development (ITM4 - IoT for health systems). Within its framework, the teaching modules related to IoT systems modelling were developed. The authors would like to thank colleagues on this project, within the framework of which the results of this work were discussed.

The authors also would like to show deep gratitude to colleagues from Department of Computer Systems, Networks and Cybersecurity of National Aerospace University n. a. N. E. Zhukovsky «KhAI» for their patient guidance, enthusiastic encouragement and useful critiques of this paper.

References

1. Understanding the Internet of Things (IoT). London: GSM Association , p. 14 (2014)
2. Press Release: Global Internet of Things market to grow to 27 billion devices, generating USD3 trillion revenue in 2025, https://machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/, last accessed 2018/03/02.
3. A decade of digital: Keeping pace with transformation, 10th ed. PwC's Digital IQ research, p. 30 (2017).
4. Vermesan, O., Friess, P.: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, (2013).
5. World Healthcare Organization, Global report on diabetes (2016).
6. Islam, S. M. R., Kwak, D., Kabir, MD. H., Hossain, M., Kwak, K.-S.: The Internet of Things for Health Care: A Comprehensive Survey, IEEE Access, vol. 3, 678-708 (2015). DOI: 10.1109/ACCESS.2015.2437951.
7. Laplante, P. A., Kassab, M., Laplante, N. L., Voas, J. M.: Building Caring Healthcare Systems in the Internet of Things. IEEE Systems Journal, 1-8 (2017). DOI: 10.1109/JSYST.2017.2662602.
8. Applied Safety Science and Engineering Techniques. Taking Hazard Based Safety Engineering (HBSE) to the Next Level. IEEE, p. 11 (2010).
9. Goševa-Popstojanova, K., Trivedi, K. S.: Architecture-based approach to reliability assessment of software systems. Performance Evaluation 45 (2-3), 179-204 (2001). DOI: 10.1016/S0166-5316(01)00034-7.
10. Kharchenko, V., Kolisnyk, M., Piskachova, I., Bardis, N.: Reliability and Security Issues for IoT-based Smart Business Center: Architecture and Markov Model. In: 2016 Third

International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), pp. 313-318. Chania (2016). DOI: 10.1109/MCSI.2016.064.
11. Strielkina, A., Uzun, D., Kharchenko, V.: Modelling of healthcare IoT using the queueing theory. In: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 313-318. Bucharest (2016). DOI: 10.1109/IDAACS.2017.8095207.
12. Strielkina, A., Kharchenko, V., Uzun, D.: Availability Models for Healthcare IoT Systems: Classification and Research Considering Attacks on Vulnerabilities. In: 2018 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018. Kyiv, Ukraine (in press).
13. Maksimović, M., V. Vujović, V., Perišić, B.: A custom Internet of Things healthcare system. In: 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6. Aveiro, (2015). DOI: 10.1109/CISTI.2015.7170415.
14. Malik, M. A.: Internet of Things (IoT) Healthcare Market by Component (Implantable Sensor Devices Wearable Sensor Devices System and Software) Application (Patient Monitoring Clinical Operation and Workflow Optimization Clinical Imaging in Fitness and Wellness Measurement) - Global Opportunity Analysis and Industry Forecast 2014–2021. Alied Market Research, p. 124 (2016).
15. Sommerville, I.: Software Engineering. 9th edn. Pearson (2010).
16. Yi Zhang, Y., Jones, P. L., Jetley, R.: A Hazard Analysis for a Generic Insulin Infusion Pump. Journal of Diabetes Science and Technology 4 (2), 263-283 (2010). DOI: 10.1177/193229681000400207.
17. Wetterneck, T.B., Skibinski, K.A., Roberts, T.L., et al : Using failure mode and effects analysis to plan implementation of smart i.v. pump technology. Smart i.v. pump technology 63, 1528-1538 (2006).
18. Rafeh, R., Rabiee, A.: Towards the Design of Safety-Critical Software. Journal of Applied Research and Technology 11 (5), 683-694 (2013). DOI: 10.1016/S1665-6423(13)71576-1.
19. Klonoff, D. C., Reyes, J. S.: Insulin Pump Safety Meeting: Summary Report. Journal of Diabetes Science and Technology 3(2), 396-402 (2009). DOI: 10.1177/193229680900300224.
20. Guenego, A., Bouzillé, G., Breitel, S., Esvant, A., Poirier, J.-Y., et al.: Insulin Pump Failures: Has There Been an Improvement? Update of a Prospective Observa-ional Study. Diabetes Technology and Therapeutics 18 (12). Mary Ann Liebert, 2016, pp.820-824 (2016). DOI: 10.1089/dia.2016.0265.
21. Sharma, Y., Javadi, B., Si, W., Sunb, D.: Reliability and energy efficiency in cloud computing systems: Survey and taxonomy. Journal of Network and Computer Applications 74, 66-85 (2016). DOI: 10.1016/j.jnca.2016.08.010.
22. Reliability Pillar. AWS Well-Architected Framework. Amazon Web Services, p. 45 (2018).
23. Yanovsky, M., Yanovskaya, O., Kharchenko, V.: Analysis of Methods for Providing Availability and Accessibility of Cloud Services. In: 2016 12th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, pp. 414-426. Kyiv (2016).
24. Cloud Computing Vulnerability Incidents: A Statistical Overview. Cloud Vulnerabilities Working Group, p. 21 (2013).