Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

Issue 4/2021

THE RELIABILITY OF DATA-DRIVEN INTERNET OF THINGS SYSTEMS

Slavko POKORNI
Information Technology School, Cara Dušana 34, 11070 Belgrade, Serbia, Email: slavko.pokorni@its.edu.rs

How to cite: POKORNI, S. (2021). "The Reliability of Data-driven Internet of Things Systems." *Annals of Spiru Haret University. Economic Series, 21*(4), 43-52, doi: https://doi.org/10.26458/2141

Abstract

The goal of this paper is to show that reliability in the data-driven Internet of Things (IoT) must be taken into account. The reliability of data-driven IoT is a complex problem because such a system is comprised of hardware, software, human and data. The reliability of each of these elements is shortly analysed, and the equation for the reliability calculation of a ***data-driven*** *IoT system is proposed. Artificial intelligence is also included. Reliability is connected with availability and maintainability, and this is also explained. This paper is written mainly using two references recently published by the author of this paper.*

Keywords: *reliability; availability; maintainability; Internet of Things; data-driven; data.*

JEL Classification: C02, Y20

Introduction

In the 1950s, theories and practices of reliability began to emerge, and the Internet of Things (IoT) first started at the end of the last century. IoT is very complex and with many dependencies; as a result, new demands are placed on reliability research and education [Pokorni, 2016; Pokorni, 2019].

Everything on the Internet of Things (IoT) is interconnected and can communicate with each other usually without the need for human intervention. Due to the human element, the IoT relies on the reliability of both hardware and

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
Issue 4/2021

software in addition to human reliability. This calls for a discussion of these relationships.

A data-driven IoT system is more complex because data are an essential component of this system. So, the reliability of data must also be taken into account.

The issue of IoT availability and reliability is examined from the standpoint of the traditional reliability assessment method, which makes use of MIL-HDBK 217 in [Pokorni, 2019]. The reliability of data-driven IoT will be discussed in this paper.

1. Data-driven Internet of Things

Being data-driven means that all decisions and processes are based on the data. This is most evident in the field of big data [Technopedia, 2021]. It is connected with data science, data mining, etc. The term data-driven is used in many fields, also with the Internet of Things.

Being based on data means using data, and using data means at least collecting and analysing data. And this implies using some kind of communication. To achieve this, we as a person or organisation use technology (different devices, networks, software, Internet of Things, etc.), and anything of these can fail. Of course, we want to avoid failure and resolve it if they happen, and this is the task of reliability.

Before analysing reliability, we will, in short, explain the Internet of Things.

2. Internet of Things

The Internet of Things (IoT) aims to transform human society toward becoming intelligent, convenient, and efficient with potentially enormous economic and environmental benefits. Reliability is one of the main challenges that must be addressed to enable this revolutionised transformation [Xing, 2020].

The Internet of Things (IoT) is seen as the next step in the Internet's development. IoT is being driven by three main factors: miniaturisation of electronic components, rising electronic component costs, and a shift to wireless communications.

Many real-time monitoring applications, such as e-healthcare, home automation systems, environmental monitoring and industrial automation, will be transformed by the Internet of Things (IoT). This includes the economy as well.

The Internet of Things (IoT) and its applications and supporting hardware platforms have become a hot topic in academic and practitioner communities in recent years due to improvements in Internet connectivity and advances in smart

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

personal computing devices. The scale of IoT deployments can range from personal wearable to city-wide infrastructures, with the ability to deploy IoT systems in many different scenarios [Zhu et al., 2018; Pokorni, 2019].

The Internet of Things (IoT) is unquestionably complicated. An IoT system includes hardware, software, and human involvement on occasion [Pokorni, 2019]. So, the reliability of IoT depends not only on hardware but also on software and human reliability. And reliability is connected with availability and maintainability. Let us first define reliability, availability and maintainability.

3. Definition of reliability, availability and maintainability

It wasn't until the 1950s that reliability theory and practice began to take shape. Reliability means the likelihood that an item will meet certain standards of performance and deliver the desired results within a specified time period under specific environmental conditions.

A system's availability is measured by taking into account the component's reliability as well as the system's ability to be maintained. Availability is defined differently by different people, and it is calculated differently as well.

For instance, the probability that a system (or a component) will be operational at a specific point in time is defined as instantaneous availability (also known as availability).

Reliability and availability are the same for an unrepaired component or system, but availability is greater than reliability for a repaired component or system [Pokorni, 2014].

Maintainability is linked to both reliability and availability. Maintainability must be taken into account during the design phase of the IoT in order to achieve optimal cost over the IoT's lifespan.

Maintainability is now defined as an intelligent system's ability to be easily uncoupled, fixed, and modified without interfering with the system's normal operations or functionalities in any significant way. When evaluating the IoT system's maintainability, look for components that can be easily replaced if something goes wrong. IoT systems must be able to complete maintenance tasks effectively, efficiently, and with satisfaction, before they can be described as highly maintainable [Thomas & Rad, 2017; Pokorni, 2019].

Repairing the system changes availability from reliability. The following relation can be used to calculate availability (inherent availability) [Pokorni, 2014]

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
Issue 4/2021

$$A = \frac{MTBF}{MTBF + MTTR} \quad (1)$$

where
- *MTBF* is mean time to failure, and
- *MTTR* is mean time to repair.

For example, replacing an exhausted battery in an IoT device can reduce availability if the IoT system is supposed to work during the replacement.

Now we will analyse the reliability of a data-driven Internet of Things system in more detail, keeping in mind that the system is composed of elements: hardware, software, human and data.

4. Reliability of data-driven IoT elements

Unreliable sensing, processing, and transmission can lead to erroneous monitoring data reports, long delays, and even data loss, which reduce people's interest in IoT communication and their confidence in data. To keep pace with IoT's rapid growth, it needs a high level of reliability [Prasad & Kumar, 2013].

So, if the organisation is based on data-driven IoT, then the reliability of such a system depends on IoT components (elements) and data.

4.1 IoT hardware reliability

Until now, military manual MIL-HDBK-217 has been primarily used to calculate the reliability of electronic devices. In 1961, the first version of this product was created (version A). More than 80% of engineers still use MIL-HDBK-217 to calculate reliability, despite its shortcomings. Other standards for calculating reliability exist in the industrial and commercial sectors, of course. MIL-HDBK-217 has been replaced by RIAC's 217PlusTM methodology and a software tool, but it is no longer available for free. Unlike the previous MIL-HDBK-217, this one is considerably more difficult to understand [Pokorni, 2016].

In addition to this, determining hardware reliability has a number of challenges. Elerath & Pecht (2012) state that there is no standard method for creating hardware reliability predictions, which means predictions vary widely in terms of methodological rigour, data quality and the extent of analysis and uncertainty. Documentation of the prediction process is often not provided. The IEEE has responded by creating a standard in 2009 called IEEE Std.1413 (Standard Framework for Hardware Reliability Prediction). The IoT consists of a variety of

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

hardware with varying levels of quality and reliability. The commercial hardware often lacks established reliability and lacks any data on the failure rate or the mean time to failure (MTTF), or the mean time between failures (MTBF), making it difficult to calculate exact reliability.

4.2 IoT software reliability

The reliability of the software as a product is an important criterion to consider. Software reliability assessment models abound, but none is universally accepted [Kapur, 2014; Pokorni, 2016]. Except for that, software reliability requirements are rarely, if ever, adequately specified. This is especially true for the Internet of Things (IoT). The issue is exacerbated by the fact that software is fundamentally different from hardware. Software reliability is not a time-dependent function, despite the fact that it is a probabilistic one. It's also true that methods for predicting software reliability aren't routinely implemented in software engineering practices. Software and reliability experts must work together to take the necessary steps to include software in the system's reliability case [Kapur, 2014; Pokorni, 2016].

The real problem with dependable software is when a feature that's critical to the system doesn't work. When people hear the phrase "failing safe," they often think it means "never failing." Because they share the same goal of creating secure and dependable software, software safety and reliability are natural partners. Again, software and reliability engineers must work together. The basics of software reliability and its reliance on software safety are, however, rarely taught in educational institutions or by industry professionals. [Pokorni, 2014].

Enhancing reliability by redundant software presents a unique set of challenges because it differs from hardware in that the error appears in every copy [Pokorni, 2014].

4.3 IoT human reliability

As we stated in the introduction, a human can be involved in the IoT system. So, human action can influence the reliability of the IoT.

Accident prevention and damage reduction are two key components of human dependability. These things can happen when working with data in addition to hardware and software alone. Whether or not people decide to act has an impact on the technological systems in which they live. Frequently, disasters and major system failures are the results of a series of decisions or actions taken by one or more people while using, maintaining, or fixing a technological system. As long as

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900
Issue 4/2021

these potential consequences are significant, reliability engineers working with others (such as risk managers, environmentalists, and life safety engineers) can have a significant impact on the outcome. [Pokorni, 2016]. Human error in working with data can also have significant consequences.

There are different approaches and models to human reliability [Pokorni, 2016].

System failures cannot be completely prevented by procedures, rules, codes, standards, or laws, but in the author's experience, they can be reduced by those same measures.

Human reliability has always been an important consideration for this author, and as a result, it is included in all of his textbooks [Pokorni, 2014].

4.4 Reliability of data

In order to build trust in data, it's critical that it's reliable, which means that it's complete and accurate. Data integrity initiatives, which are used to maintain data security, data quality, and regulatory compliance, have as one of their primary goals the assurance of data reliability [Talend, 2021].

Business leaders need reliable data to make reliable decisions. So, in data-driven organisations, data reliability is of crucial importance. Data reliability is not the same as data validity. The reliability of the data is based on the validity, completeness, and uniqueness of the data. Because of unreliable IoT, data can be missing, incomplete and/or corrupted.

4.5 Reliability of artificial intelligence

Artificial intelligence (AI) is being applied more and more in various fields, and data-driven IoT is not an exception.

Even artificial intelligence (AI) can go horribly wrong. As with human reasoning, artificial intelligence (AI) has the potential to fail in the same way if it tries to replace human intelligence with machine intelligence. Then why do people make mistakes in their reasoning (erroneous conclusions, decision-making)? Or, can we bring up the issue of AI's dependability or how to prevent AI failures [Pokorni, 2021]?

This is an important question that attracted the attention of ISO/IEC. In [ISO, 2020], there are surveys of topics related to the so-called trustworthiness in AI systems, including the following: (1) approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; (2) engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and (3) approach to assess and achieve

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

availability, resiliency, reliability, accuracy, safety, security, and privacy of AI systems. In this document, trustworthiness is defined as an ability to meet stakeholders' expectations in a verifiable way, including the characteristics of trustworthiness such as reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, and usability.

Just like any other product, AI requires maintenance to remain robust and valuable.

4.6 Is there anything else?

Yes, there is. The failure rate of hardware and software is only one factor in determining IoT reliability. Other factors include protocols and energy efficiency (green), standardisation and other influences, such as, for example, security, etc.

Let us mention something about protocols. A reliable protocol in computer networking refers to a protocol that informs the sender if the delivery of data to the intended recipients was successful or failed.

Reliability depends on the type of users. Different users can expect different levels of reliability and availability. So, approaches to designing an IoT system can be different depending on the types of users. And this also stands for data-driven IoT.

Google service availability targets are typically determined by the function they provide and their market positioning. There are a number of things to think about [Alvidrez, 2017]: What level of service can customers reasonably expect from your company?

- Exactly what level of service can customers hope to get from you?
- Is there a direct link between the revenue generated by this service and the revenue generated by our customers?
- Is this a for-profit or non-profit service?
- What level of service do competitors provide if they exist in the market?
- Is this service geared toward individuals or businesses?

5. Reliability of data-driven IoT system

Because of the complexity of the data-driven IoT system, and because the IoT includes hardware, software, sometimes humans, and data-driven IoT system includes data, we suggest assessing the reliability of the data-driven IoT system by changing the equation from the [Pokorni, 2019], to next

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

$$R_S(t) = R_{HW}(t)R_{SF}(t)R_H(t)R_D(t) \quad (2)$$

where R_{HW}, R_{SF}, R_H and R_D are reliability of hardware, software, human and data subsystem, respectively.

The above formula is valid if failures of hardware, software, human and data subsystems are mutually exclusive.

Due to the IoT's obvious complexity, finding an analytical solution for the reliability of such a complicated system is difficult, if not impossible.

Our recommendation is to use simulation to test the IoT's reliability because of its complexity. We simulated a few complex systems and found that the results were insightful [Pokorni & Janković, 2011; Pokorni et al., 2011].

If artificial intelligence is implemented in a data-driven IoT system, it can be treated as a subsystem also and included in equation (2) in the same way as other subsystems.

Conclusion

Reliability assessment and the analysis of the data-driven Internet of Things elements and system require knowledge from many different technical and other areas and teamwork.

Data-driven IoT system is complex and includes hardware, software, sometimes humans, and also data. The reliability of all these elements must be taken into account. Artificial intelligence can also be a component of this system, and its reliability must be analysed.

Reliability of the data-driven Internet of Things is not always of the primary concern in IoT practice, but understanding reliability can help in case of failure, i.e., where to look for a failure, and how series consequences of failure can happen during decision making because of incomplete or corrupted data.

References

[1] Alvidrez, M. (2017) *Embracing Risk*. [e-book] Sebastopol, CA: O'Reilly Media, Inc. Available at: https://landing.google.com/sre/sre-book/chapters/embracing-risk/#risk-management_measuring-service-risk_time-availability-equation.

[2] Elerath, J.G., & Pecht, M. (2012) IEEE 1413: A Standard for Reliability Predictions. *IEEE Transactions on Reliability*, 61(1), pp.125-129. Available at: https://doi.org/10.1109/TR.2011.2172030.

[3] ISO. 2020. *ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence* [online]. Available at: https://www.iso.org/standard/77608.html?browse=tc

[4] Kapur, K.P. (2014) Measuring Software Quality (State of the Art). In: *5th DQM International Conference Life Cycle Engineering and Management ICDQM*, Belgrade, pp.3-45. June 27-28.

[5] Pokorni, S. (2014) *Reliability of information systems, textbook*. Belgrade: Information Technology School (in Serbian).

[6] Pokorni, S. (2016) Reliability prediction of electronic equipment: Problems and experience. In *7th International Scientific Conference on Defensive Technologies OTEH*, Belgrade, pp.695-700. October 06-07, ISBN 978-86-81123-82-9.

[7] Pokorni, S. (2019) Reliability and Availability of the Internet of Things, *Vojnotehnički glasnik/Military Technical Courier*, pp. 588-600, 67(3), https://doi.org/10.5937/vojtehg67-21363

[8] Pokorni, S. (2021) Current State of the Artificial Intelligence in Reliability and Maintainability, *Vojnotehnički glasnik/Military Technical Courier*, 2021, Vol. 69, Issue 3, pp. 578-593, DOI: 10.5937/vojtehg69-30434, https://doi:10.5937/vojtehg69-30434, ISSN 0042-8469, UDC 623 + 355/359

[9] Pokorni, S., & Janković, R. 2011. Reliability Estimation of a Complex Communication Network by Simulation. In: *19th Telecommunication forum TELFOR*, Belgrade, pp.226-229, November 22-24, IEEE 978-1-4577-1500-6/11.

[10] Pokorni, S., Ostojić, D., & Brkić, D. 2011. Communication network reliability and availability estimation by the simulation method. *Vojnotehnički glasnik/Military Technical Courier*, 59(4), pp.7-14. Available at: https://doi.org/10.5937/vojtehg1104007P.

[11] Popa, D., Popa, D.D. & Codescu, M.M. (2017) Reliability for a green internet of things. *Buletinul AGIR*, 2017(1). Available at: https://www.buletinulagir.agir.ro/articol.php?id=2824.

[12] Prasad, S.S., & Kumar, C. (2013) A Green and Reliable Internet of Things. *Communications and Network*, 5(1B), pp.44-48. Available at: https://doi.org/10.4236/cn.2013.51B011.

[13] Ryan, P.J., & Watson, R.B. (2017) Research Challenges for the Internet of Things: What Role Can OR Play. *Systems*, 5(1), 24. Available at: https://doi.org/10.3390/systems5010024.

[14] Technopedia. Available at https://www.techopedia.com/definition/18687/data-driven (Seen 28.10.2021)

[15] Thomas, M.O., & Rad, B.B. (2017) Reliability Evaluation Metrics for Internet of Things, Car Tracking System: A Review. *International Journal of Information Technology and Computer Science (IJITCS)*, 9(2), pp.1-10. Available at: https://doi.org/10.5815/ijitcs.2017.02.01.

[16] Talend. Available at https://www.talend.com/resources/what-is-data-reliability/ (Seen 28.10.2021)

Annals of Spiru Haret University.
Economic Series
Since 2000
ISSN:2393-1795 ISSN-L:2068-6900

[17] Zhu, Q., Uddin, M.Y.S., Venkatasubramanian, N., Hsu, C-H., & Hong H-J. (2018) Poster abstract: Enhancing reliability of community Internet-of-Things deployments with mobility. In: *IEEE INFOCOM 2018-IEEE Conference* on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu. April 15-19. Available at: https://doi.org/10.1109/INFCOMW.2018.8406922

[18] Xing, L. (2020) Reliability in Internet of Things: Current Status and Future Perspectives. *IEEE Internet of Things Journal*, Volume: 7 Issue: 8. **DOI:** 10.1109/JIOT.2020.2993216