Type of the Paper: Review paper
Received: 22.01.2021.
Accepted: 28.01.2021.
DOI: https://doi.org/10.18485/edtech.2021.1.1.1
UDC: 004.78:004.35

Problems of Reliability Assessment in Data-Driven Internet of Things

Slavko Pokorni[1]*

[1] Information Technology School, ITS-Belgrade, Belgrade, Serbia; slavko.pokorni@its.edu.rs

Abstract: There has been an increase in interest in the Internet of Things (IoT) research endeavour. New concepts were discovered or existing ones were improved or fixed due to many novel research studies and IoT technologies in various sectors. There was also a focus on IoT security and standards for the Internet of Things. IoT applications that serve other industries, such as smart-living, industry 4.0, and e-health, are still relevant today. This paper aims to demonstrate that the Internet of Things (IoT) must be considered reliable, especially if it is data-driven IoT. Reliability of data-driven IoT is a complicated issue to solve because it involves hardware, software, people, and data, and today artificial intelligence. It is possible to calculate the reliability of an IoT system using a simple equation proposed in this paper. But the main problem is how to calculate the reliability of subsystems in this equation. Additionally, reliability is linked to availability and maintenance. The author of this paper primarily relies on two of his recent publications for the bulk of this paper's content.

Keywords: reliability, availability, maintainability, Internet of Things, data-driven, data

1. Introduction

The Internet of Things (IoT) was first introduced at the end of the twentieth century, and reliability theories and practices began to emerge in the 1950s. However, the Internet of Things (IoT) is a very complex and interdependent system, and as a result, new demands are placed on reliability research and education.

In the Internet of Things, all devices are interconnected and can communicate with each other often without the intervention of a human being. Since the Internet of Things relies on people, hardware, and software, it must have high reliability. A discussion of these relationships is warranted.

A data-driven IoT system is more complex since data are an important, integral part of this system. As a result, the reliability of data must be considered. In [1], the traditional reliability assessment method is used to examine the issue of IoT availability and reliability. This paper will focus on the reliability of data-driven IoT.

2. The Internet of Things

Human society will be transformed by the Internet of Things, thus becoming more innovative, more accessible and efficient with potentially enormous economic and environmental advantages. However, one of the most pressing issues is reliability, which must be addressed for this revolutionary transformation to occur [2].

There is much hype around the Internet of Things. Electronic components are getting smaller and more expensive, and wireless communications are becoming more commonplace. These three factors are driving the Internet of Things.

Applications such as electronic health care, home automation, and environmental sensors will be transformed by the IoT. Even the economy is a part of this discussion. Recent advances in Internet connectivity and intelligent personal computers have made the Internet Things and its applications and supporting hardware platforms a hot topic among academic and professional communities. It is possible to deploy IoT systems in many different scenarios, from personal wearables to city-wide infrastructures [3,1].

The Internet of Things is undeniably complex. IoT systems include hardware and software as well as humans at times [1]. Because IoT relies on more than just hardware, software, and humans, its reliability is affected by all three factors. Availability and maintainability are also linked to reliability. Defining reliability, availability and maintainability is the first step in this discussion.

3. Reliability, availability, and maintainability

As recently as the 1950s, the field of reliability theory and practice began to emerge. If an item is expected to meet a certain standard of performance and deliver the desired results within a specific time frame, it is considered reliable.

Component reliability and system upkeep are two factors determining a computer system's availability. However, availability is defined and calculated in various ways by different people.

For example, immediate availability can be defined as the probability that a system (or a component) will be operational at a given time (also known as availability).

Reliability and availability are equal for an unrepaired component or system, but availability is more significant than reliability for a repaired component or system [4].

Both reliability and availability are linked to maintainability. Therefore, to keep the IoT's cost as low as possible, the design phase of the IoT must include consideration for maintainability.

Being maintainable means that an intelligent system can be easily uncoupled, fixed, and modified without affecting the system's normal operations or functions in any significant way. To ensure the IoT system can be easily repaired or replaced in case of a malfunction, look for easily replaceable components. A highly maintainable IoT system can only be described as one that can effectively and efficiently complete maintenance tasks [5,1].

Information on how to calculate a system's or component's availability can be found in [4].

IoT device replacements, for example, can reduce availability if the IoT system is supposed to function while the battery is being replaced. As a result, data-driven IoT systems will be scrutinised in greater detail now, focusing on the system's dependability across hardware, software, people, and data.

4. The Internet of Things is a data-driven system

The term "data-driven" refers to all the decisions and processes based on the available information. This is most apparent when it comes to big data [6]. It has ties to data science, data mining, and other related fields. Many fields, including the Internet of Things, use the term "data-driven" to describe their work.

In order to be a data-driven organisation, you must first collect and analyse data. As a result, some form of communication must be employed. We use various devices, networks, software, and the Internet of Things to achieve this, but any of these can fail. We want to keep things working and fix them when they go wrong, and that is the job of reliability. While discussing reliability, we will briefly explain the Internet of Things.

The heterogeneity of an end-to-end IoT system presents reliability challenges. Much attention must be paid to the interface between subsystems to ensure compatibility, and it can also influence reliability. The IoT's most critical component is the physical system, which might lead to unanticipated system failures. Engineers and mathematicians have spent a long time analysing these systems as part of hardware reliability to lower accident rates and preserve human life [7].

5. Elements of a data-driven IoT system

Erroneous reports of data monitoring, long delays, and even data loss can diminish people's interest in IoT communication and their trust in data. The Internet of Things requires a high level of reliability to keep up with its rapid growth [8].

As a result, an IoT-based system's reliability depends on the IoT components (elements) and data that make up the system.

5.1. Reliability of IoT hardware

MIL-HDBK-217 has been used to determine the reliability of electronic devices since the sixties of last century. The first version of this product (version A) was developed in 1961. Despite its shortcomings, more than 80% of engineers still use MIL-HDBK-217 to determine reliability. In addition, of course, the industrial and commercial sectors have their standards for calculating reliability. However, MIL-HDBK-217 has been replaced by RIAC's 217PlusTM methodology and a software tool, and it is no longer available for free use. In addition, this new MIL-HDBK-217 is significantly more difficult to comprehend than the previous one [9].

In spite of having MIL-HDBK-217, determining the reliability of hardware is a difficult task. Because there is no standard method for creating hardware reliability predictions, the results can vary widely in terms of methodological rigour, data quality, and the extent to which analysis and uncertainty are taken into account [10]. Furthermore, not all prediction processes are documented. IEEE Std.1413 was established in 2009 as a response (Standard Framework for Hardware Reliability Prediction). The Internet of Things comprises a wide range of hardware components of varying quality and dependability. To accurately calculate the reliability of commercial hardware, there is often no established reliability and no data on the failure rate, the mean time to failure (MTTF), or the mean time between failures (MTBF).

5.2. Reliability of IoT software

An important criterion to consider is the quality of the software as a finished product. There are numerous models for assessing software reliability, but none are universally accepted [11,9]. For the most part, it is difficult to define the requirements for software reliability. This is especially the case in the Internet of Things. Because software is fundamentally different from hardware, the problem is made worse. Even though software reliability is probabilistic, it is not a time-dependent function. It is also true that there are not any standard practices for predicting software reliability. Reliability and software experts must ensure that software is included in a system's reliability case.

There is a real problem with reliable software when a critical feature fails. "Failing safe" is often misunderstood to mean "never failing." Software safety and reliability go hand in hand because they aim to create secure and dependable software. Engineers who specialize in both software and reliability must collaborate once more. Despite this, few educational institutions or industry professionals devote adequate time to teaching the fundamentals of software reliability and safety [4].

It is challenging to improve reliability by using redundant software because the error is present in every copy [4].

5.3. Reliability of humans in IoT

As we stated in the introduction, a human can participate in the IoT system. As a result, the Internet of Things is susceptible to human error.

A person's dependability can be improved by preventing accidents and minimising damage. In addition to working with hardware and software, these issues can arise solely with stored data. People's actions impact the technological systems in which they live. There are many instances where a series of decisions or actions taken by one or more individuals while using, maintaining or repairing a technological system results in disasters and major system failures. Reliability engineers

can significantly impact the outcome if they work with others, such as risk managers, environmentalists, and life safety engineers. The consequences of human error in handling data can be pretty severe. Human reliability can be approached in various ways and with a variety of models [9]. Procedures, rules, codes, standards, and laws cannot prevent all system failures, but they can be made less likely in the author's opinion.

When it comes to the author of this paper, reliability has always been an important consideration, taking humans into account as well, and as a result, it is included in all of his textbooks.

5.4. Reliability of data in the IoT or data trustworthiness

It is essential that data is reliable, which means that it is complete and accurate to build trust in it. Therefore, to maintain data security, data quality, and regulatory compliance, the primary goal of data integrity initiatives is to ensure data reliability [12].

To make sound decisions, business leaders need accurate information. As a result, in data-driven organisations, data reliability is essential. However, data validity and reliability are not the same thing. A dataset's trustworthiness is based on the dataset's validity, completeness, and uniqueness. Data can be missing, incomplete, or corrupted due to the unreliability of the Internet of Things.

Unfortunately, there is no adequate theory and practice on how to assess reliability of data.

5.5. Reliability of artificial intelligence in IoT

The data-driven Internet of Things is no exception to the trend of using artificial intelligence (AI). Machine learning (ML) and AI are changing many aspects of the economy, education, and people's lives. A vital area for detecting cyber-attacks on the Internet of Things, ML is becoming increasingly significant. ML can also detect sophisticated assaults using knowledge-based strategies. However, the lack of publicly accessible and regularly updated data sets is the most severe issue with IoT security [13].

AI has evolved from ML through deep learning to practical AI. AI allows a machine to learn from experience, adapt to new inputs, and perform specific jobs without human involvement. Face recognition, speech recognition, and chess game triumph are all feasible. It is currently seeing the most use due to the recent surge in IoT data, fast internet, and high-performance computers. Statistical and computational techniques are currently used in AI research [14].

AI detects patterns and abnormalities in data from intelligent sensors and devices without being told where to look. In addition, ML algorithms "learn" to give increasingly accurate results over time. As a result, ML outperforms traditional business intelligence tools in speed and accuracy. Deep learning, computer vision, natural language processing, and ML in time-tested prediction or optimization are AI technologies that complement the Internet of Things [15].

It is possible that even artificial intelligence (AI) can go disastrously wrong. Artificial intelligence has the potential to fail in the same way that human reasoning has if it attempts to replace machine intelligence with human intelligence. Then why do people make erroneous conclusions (decisions) in their reasoning? Is there a way to raise the issue of AI's reliability or how to avoid AI failures?

Considering the importance of this issue, ISO/IEC decided to look into it. AI systems' so-called trustworthiness is surveyed in [16], including the following: AI systems trustworthiness can be established through transparency, (1) controllability and other means; (2) engineering pitfalls and associated threats and risks to AI systems, along with possible mitigation techniques and methods; and (3) a method for achieving availability, resiliency, reliability, accuracy, safety, security, and privacy of AI systems. Many characteristics make something trustworthy, including reliability, availability, resilience, security, privacy, safety, accountability, integrity, authenticity, quality, and usability. These attributes are all included in this definition of trustworthiness. Like any other product, AI needs to be maintained to continue to be valuable and robust.

One factor in determining IoT reliability is the rate of hardware and software failure. In addition, protocols, energy efficiency (green), standardisation, and other influences, such as security, are also necessary. For example, regarding the protocols, a reliable protocol lets the sender know whether or not data was successfully delivered to the intended recipients in computer networking [17].

The type of user determines the reliability of a product it is being used by. The reliability and availability of a service can vary widely depending on who uses it. This means that IoT system design approaches can vary depending on the type of user. The Internet of Things is also data-driven.

According to Google services' function and market position, their availability targets are typically set. However, several factors need to be considered [18]. If the question is what customers can reasonably expect from the company in terms of customer service, then the answer must be:

Do the customers' purchases of this service directly translate into revenue for the company; this service is for-profit; if there are competitors on the market, what is their level of service; does this service cater to individuals or companies, and the reliability of data-driven IoT systems is number five.

6. Reliability of the IoT system

A data-driven IoT system is more complicated than an IoT system, which includes hardware, software and sometimes humans and artificial intelligence, which can be seen as subsystems of an IoT system, so we recommend changing the equation in [1,19]

$$R_S(t) = R_{HW}(t)R_{SF}(t)R_H(t)R_D R_{AI} \tag{1}$$

where R_W , R_S , R_H , R_D and R_A stand for reliability of hardware, software, human, data, and the artificial intelligence subsystems, respectively.

The above-mentioned formula looks simple, but it is valid only if failures of hardware, software, human, and data subsystems are mutually exclusive. In the reliability block diagram, this represents the series model. Calculation of reliability of these subsystems is another problem which depends on the type of subsystem.

In the aforementioned equation, reliability means probability. If we can consider that a subsystem is reliable, we can put in the formula that probability for that subsystem is 1.

As we mentioned before, there is theory and practice of calculating reliability of hardware and software, and it is not simple, especially if hardware comprises many components (elements). Calculating reliability of software is another problem, and there is no adequate theory and practice on how to calculate reliability of human, data, and AI.

There is no easy way to analyse the reliability of the Internet of Things because of its apparent complexity. Because of the IoT's complexity, we recommend testing its reliability through simulation. Pokorni and Janković [20] and Pokorni et al. [21] conducted simulations of complex systems and found that the results were insightful. As with other subsystems, artificial intelligence can be treated as a subsystem in an IoT data-driven system and included in equation (1).

7. Five IoT reliability research directions

Reliability of data-driven Internet of Things is obviously an open area for research. There are a number of papers dealing with it. For example, [22] points out five critical features for an IoT dependability management system as follows:

1. Measurement in the vertical and time
   If the IoT is to manage critical infrastructure like security and traffic systems, we need to be able to assess the system's resilience in real time or near real time. We must pay special attention to apps that operate emergency services and demand swift and dependable responses. Moreover, each domain's reliability criteria must be defined. For example, a smart-building solution may tolerate a few seconds of delay. On the other hand, a manufacturing process can likely only tolerate microsecond delays. As a result, conducting research is essential so as to categorise these needs and build appropriate solutions for each vertical domain.
2. All devices, all protocols
   A wide range of protocols and devices connect to and use IoT services. Many research groups are working to build more lightweight and efficient communication protocols. Every day, new IoT gadgets and hardware hit the consumer market. So a reliable solution must be independent of hardware, software, and communication protocols.
3. Full-stack awareness
   The literature review concluded that, while many researchers have solved a specific problem or group of problems in IoT reliability research, no study has addressed end-to-end reliability. In light of the scope and complexity of emerging IoT deployments, that does not mean researchers should try to create a one-size-fits-all reliability method, as that would go against the first research objective stated above. Instead, they should propose dependability solutions custom-made for each IoT vertical. Making the IoT more reliable would be an essential and innovative research finding that might tremendously benefit IoT end users.
4. Using anomalies to get dependability data
   Anomalies in IoT services have been detected and reported extensively. While this kind of work is valuable and required, it does not necessarily improve reliability. An anomaly does not warn the user if the IoT system is less trustworthy. So we need to explore ways to synthesise information about emerging abnormalities in IoT systems into knowledge about dependability. For example, if a sensor in an intelligent house is monitoring assisted living malfunctions, there may not be a life-threatening situation. In a smart factory, faulty heat sensors can cause the dangerous gear to malfunction.
5. Anticipate and manage failure
   This feature discusses measuring reliability extensively. However, predictive maintenance can be considered as an option if the research goes beyond this. For example, can we derive an exact maintenance date from a system's quantifiable reliability? Furthermore, is it possible to classify this as a dynamic process based on real-time dependability data rather than a history of past failures to predict future failures? Solving this research challenge would be an essential milestone in IoT reliability research.

8. Conclusions

Traditional offline businesses will be able to turn into digital businesses owing to new industries and technology like cloud computing, artificial intelligence, and the Internet of Things. This necessitated an overhaul of business models. This will become vital for companies that wish to survive the increasingly intense market rivalry. However, the Internet of Things elements and system's reliability assessment and analysis all require knowledge from various technical and non-technical areas, so teamwork must be provided.

Data-driven Internet of Things is a multifaceted system that includes hardware, software, humans, and data. The reliability of each of these subsystems should be considered, and for some of them there is no adequate theory and practice. As a possible subsystem, artificial intelligence must be tested for resiliency.

Reliability is not always a top priority when it comes to data-driven Internet of Things. However, knowing what to look for and how a series of failure consequences can occur during decision making because of incomplete or corrupted data can help in the event of a failure.

There has been a dramatic shift in how we interact with technology in the modern world due to the Internet

of Things. Low-cost devices can connect flexibly and widely thanks to the notion of the Internet of Things, which is employed in crucial applications, such as traffic infrastructure, health care, and home security. Being able to quantify the reliability of these IoT devices because of their limited resources is a vital function. Following an in-depth analysis of the current state of the art in dependability quantification in the IoT, this study looks at the many problems connected with this undertaking. Key research directions for IoT reliability have been identified following an in-depth examination.

References

1. Pokorni S. Reliability and Availability of the Internet of Things. Vojnotehnički glasnik/Military Technical Courier. 2019; 67(3):588-600. Available from: https://doi.org/10.5937/vojtehg67-21363.
2. Xing L. Reliability in Internet of Things: Current Status and Future Perspectives. IEEE Internet of Things Journal. 2020; 7(8). Available from: https://ieeexplore.ieee.org/document/9089244.
3. Zhu Q, Uddin MYS, Venkatasubramanian N, Hsu CH, Hong HJ. 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. [Internet]. 2018 April 15-19. Available from: https://doi.org/10.1109/INFCOMW.2018.8406922.
4. Pokorni S. Reliability of information systems, textbook. Belgrade: Information Technology School (in Serbian); 2014.
5. Thomas MO, Rad BB. Reliability Evaluation Metrics for Internet of Things, Car Tracking System: A Review. International Journal of Information Technology and Computer Science (IJITCS) [Internet]. 2017;9(2):1-10. Available from: https://doi.org/10.5815/ijitcs.2017.02.01.
6. Technopedia [Internet]. Available from https://www.techopedia.com/definition/18687/data-driven (Seen 28.10.2021)
7. Azghiou K, El Mouhib M, Koulali M, Benali A. An End-to-End Reliability Framework of the Internet of Things. Sensors (Basel) 2020 May; 20(9): 2439. Published online 2020 Apr 25. doi: 10.3390/s20092439.
8. Prasad SS, Kumar C. A Green and Reliable Internet of Things. Communications and Network [Internet]. 2013;5(1B):44-48. Available from: https://doi.org/10.4236/cn.2013.51B011.
9. Pokorni S. Reliability prediction of electronic equipment: Problems and experience. In: 7th International Scientific Conference on Defensive Technologies OTEH. Belgrade; 2016;695-700. October 06-07, ISBN 978-86-81123-82-9.
10. Elerath JG, Pecht M. IEEE 1413: A Standard for Reliability Predictions. IEEE Transactions on Reliability [Internet]. 2012;61(1):125-129. Available from: https://doi.org/10.1109/TR.2011.2172030.
11. Kapur KP. Measuring Software Quality (State of the Art). In: 5th DQM International Conference Life Cycle Engineering and Management ICDQM. Belgrade; 2014 June 27-28;3-45.
12. Talend [Internet]. [cited 28.10.2021]. Available from https://www.talend.com/resources/what-is-data-reliability/.
13. Charlesworth A. Absolute Essentials of Digital Marketing; Routledge: London, UK; 2020.
14. Hassanien A, Darwish EH. Machine Learning and Data Mining in Aerospace Technology. Cham, Switzerland: Springer Nature Switzerland AG; 2020.
15. Kuleto V, Ilić M, Dumangiu M, Ranković M, Martins OD, Păun D, Mihoreanu L. Exploring Opportunities and Challenges of Artificial Intelligence and Machine Learning in Higher Education Institutions. Sustainability 2021, 13, 10424. Available from: https://doi.org/10.3390/su131810424.
16. ISO. 2020. ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence [Internet]. Available from: https://www.iso.org/standard/77608.html?browse=tc.
17. Pokorni S. Current State of the Artificial Intelligence in Reliability and Maintainability. Vojnotehnički glasnik/Military Technical Courier. 2021;69(3):578-593, DOI: 10.5937/vojtehg69-30434. Available from: https://doi:10.5937/vojtehg69-30434, ISSN 0042-8469, UDC 623 + 355/359
18. Alvidrez M. Embracing Risk. [e-book] Sebastopol, CA: O'Reilly Media, Inc.; 2017. Available from: https://landing.google.com/sre/sre-book/chapters/embracing-risk/#risk-management_measuring-service-risk_time-availability-equation.
19. Pokorni S. Reliability of Data-driven Internet of Things Systems. 6th International Conference on Economic Sciences and Business Administration BIG DATA-DRIVEN SMART URBAN ECONOMY. ICESBA 2021. Romania. 2021 26-27 November.
20. Pokorni S, Janković R. Reliability Estimation of a Complex Communication Network by Simulation. In: 19th Telecommunication forum TELFOR. Belgrade; 2011 November 22-24;226-229. IEEE 978-1-4577-1500-6/11.
21. Pokorni S, Ostojić D, Brkić D. Communication network reliability and availability estimation by the simulation method. Vojnotehnički glasnik/Military Technical Courier [Internet]. 2011;59(4):7-14. Available from: https://doi.org/10.5937/vojtehg1104007P.
22. Moore SJ, Nugent CD, Zhang S. et al. IoT reliability: a review leading to 5 key research directions. CCF Trans. Pervasive Comp. Interact. 2020;2:147–163. Available from: https://doi.org/10.1007/s42486-020-00037-z.