RELIABILITY AND AVAILABILITY OF THE INTERNET OF THINGS

Slavko J. Pokorni

Information Technology School, Belgrade, Republic of Serbia,
e-mail: slavko.pokorni@its.edu.rs,
ORCID iD: http://orcid.org/0000-0002-3173-597X

Abstract:

The problem of reliability and availability of the Internet of Things (IoT) from the point of view of the classical approach of reliability assessment using MIL-HDBK 217 is discussed in this paper. With the classical approach of reliability assessment using MIL-HDBK 217, only hardware reliability can be assessed, and the situation with the IoT is more complicated: billions of different things (devices), software programs, and human users are involved (networked). The reliability and availability of the IoT is not only a matter of a failure rate of elements (things), but also protocols, standardization, logistics support and other influences. The relation for the reliability calcuation of an IoT system is proposed.

Key words: reliability, availability, maintainability, Internet of Things.

Introduction

Reliability as theory and practice began to develop in the 50s of the last century. Very soon MIL-HDBK-217 appeared. Reliability prediction by MIL-HDBK-217 has been done for about 60 years. By the time it has been shown that this manual, which is essentially based on an exponential distribution of failure, has a number of limitations, and that other approaches are needed (Pokorni, 2016).

Besides this, new challenges in reliability appeared in recent years. They are Cloud Services and the Internet of Things, and since they are very complex and with many dependencies, this puts new requirements on research and education in reliability and reliability culture (Pokorni, 2016), (Pokorni, 2018).

The Internet of Things (IoT) consists of hardware and software which can communicate without human intervention (in that case we can consider it to be machine to machine (M2M) communication); sometimes the human factor is involved, so hardware reliability is connected not only

to software reliability, but also to human reliability, thus creating a need to discuss these relations.

The problem of reliability and availability of the Internet of Things from the point of view of the classical approach of reliability assessment using MIL-HDBK 217 is discussed in this paper. With the classical approach of reliability assessment using MIL-HDBK 217, only hardware reliability can be assessed, and the situation with the IoT is more complicated: billions of different things (devices), software programs, and human users are involved (networked). The reliability of the IoT is not only a matter of a failure rate of elements (things), but also of software, human factor, logistics support, standardization and other influences, such as, for example, energy efficiencies (green), security (hacking, etc.).

Definition of reliability and availability

Reliability is defined as a probability that a component or a system will meet certain performance standards in yielding correct output for a desired time duration in certain environmental conditions.

Availability is a metric used to assess the performance of repairable systems, incorporating both the reliability and maintainability properties of a component or a system. There are different definitions of availability and different ways to calculate it.

Instantaneous availability (usualy called availability) is defined as the probability that a system (or a component) will be operational at a specific point of time.

For an unrepaired component or system, reliability and availability means the same, but for a repaired component or system, availability is bigger than reliability (Pokorni, 2014).

Internet of Things

A growing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the IoT (Popa et al, 2017), (Prasad & Kumar, 2013), Figure 1. The IoT first started in 1990s with industrial automation systems (Prasad & Kumar, 2013).

The Internet of Things will soon, if not already, permeate to all industries and have influence in everyone's life (Rohde & Schwarz, nd).

The IoT is regarded as the next phase in the evolution of the Internet. Electronic miniaturization, cost of electronic components, and the trend towards wireless communications are the three main drivers for the IoT (Ryan & Watson, 2017).

The Internet of Things is going to change a wide variety of real-time monitoring applications, for example, E-healthcare, homes automation system, environmental monitoring and industrial automation (Popa at al, 2017).

It is stated in (Andersen, 2018) that a lot of attention in recent time seems to be on building highly reliable (up to carrier grade) clouds, but another area is the IoT.

According to ITU-T, the IoT is defined as (Popa at al, 2017) „In a broad perspective, the IoT can be perceived as a vision with technological and societal implications. From the perspective of technical standardization, IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, while maintaining the required privacy.“

In recent years, with the improvement in Internet connectivity and advances in smart personal computing devices, the IoT, along with its applications and supporting hardware platforms, has become a hot topic in both academic and practitioner communities. IoT systems can be deployed in many scenarios, where the scale of IoT deployments can vary from personal wearables to city-wide infrastructures (Zhu et al, 2018).
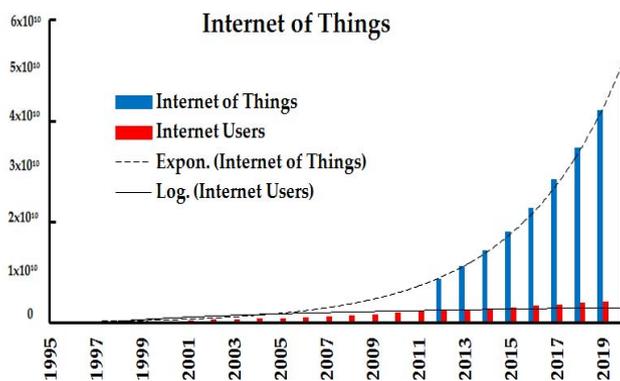

Figure 1 – Internet of Things growth (Ryan & Watson, 2017)
Рис. 1 – Рост интернета вещей (Ryan & Watson, 2017)
Слика 1 – Раст интернета ствари (Ryan & Watson, 2017)

The architecture of the Internet of Things consists of sensor nodes, the network domain, and application domains, Figure 2, (Popa et al, 2017), (Prasad & Kumar, 2013).

The Sensor Node domain is the same as the M2M node domain in M2M communication. After collecting the packets from the nodes, the gateway GW is able to intelligently manage the packets and provide efficient paths for forwarding these packets to the remote back-end server (BS) via wired/wireless networks. The network domain provides cost-effective and reliable channels for transmitting sensory data packets from the sensor domain to the application domain. The application domain is the last part with BS as the key component for the whole IoT communication.

Reliability of the IoT elements

Reliability is defined as the ability of an item to perform a required function under stated conditions for a stated time period (Bauer & Adams, 2012), (Pokorni, 2014). Quantitatively, it is expressed in probability.

Reliability is critical for efficient IoT communication, because unreliable sensing, processing, and transmission can cause false monitoring data reports, long delays, and even data loss, which would reduce people's interest in IoT communication. Therefore, the rapid growth of IoT communication demands high reliability (Prasad & Kumar, 2013).
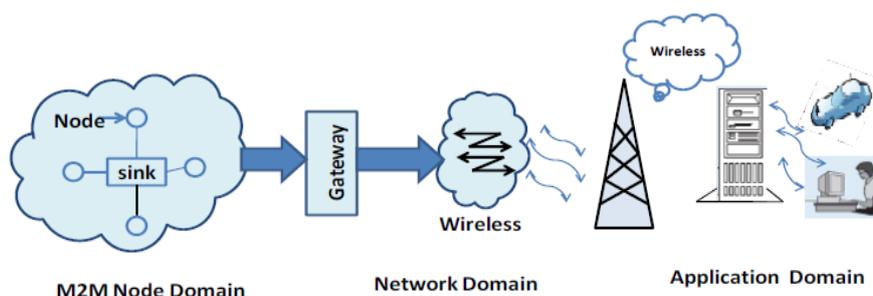

Figure 2 – Architecture of the IoT (Popa et al, 2017), (Prasad & Kumar, 2013)
Рис. 2 – Архитектура интернета вещей (Popa et al, 2017), (Prasad & Kumar, 2013)
Слика 2 – Архитектура интернета ствари (Popa et al, 2017), (Prasad & Kumar, 2013)

However, these deployments, as IoT implementations, depend heavily on the Internet connectivity, therefore on the network

infrastructure. In large-scale IoT deployments like those in smart cities and smart communities, failures in the network infrastructure can be fatal to the operation when large events or emergencies stress or strike the public network facilities. Enabling the reliability and resilience of large-scale IoT deployments is critical in these scenarios and promising for further research (Zhu et al, 2018).

There are several research challenges that must be resolved to support the operation of IoT systems for communities (Zhu et al, 2018). The first challenge is that of scale, i.e. the huge number of devices. In community-wide IoT systems, the number of participating devices can make a big difference in the design of system architecture and influence the network infrastructures. Bring-in mobility and crowd participation can make a bigger challenge. The second challenge is that of the dynamics. Both the physical and networking environment in communities can change. Mobility brings in more changes and adaptation to changes is important. The third challenge is that of the inter-operability. With the growing number and heterogeneity of IoT devices, the interoperation and coordination are keys to make all these devices, platforms, and their supporting software an integrated system instead of a pile of independent pieces (Zhu et al, 2018).

Obviously, the IoT is very complex. It comprises hardware, software, and sometimes a human is envolved in an IoT system. Since the IoT is regarded as the next phase in the evolution of the Internet, and the iInternet is a network of networks, and the functioning of networks is based on protocols, then, except hardware and software, protocols also must be considered in the reliability of the IoT. Although protocols are esentially realized in software, there is a need to consider them separately because there are reliable and unreliable protocols.

IoT hardware reliability

Up to now, hardware reliability has been calculated mostly using MIL-HDBK-217, military manual, for the calculation of the reliability of electronic devices. The first version was developed in 1961 (version A). But MIL-HDBK-217 has limitations, and has not been updated since 1995 (the last version F). In spite of its limitations, MIL-HDBK-217 is still used by more than 80% of engineers in calculating reliability. Of course, there are other industrial and commercial standards for calculating reliability. RIAC's 217Plus™ methodology and a software tool is a replacement for MIL-HDBK-217, it is no longer free, it is more complex, and, at least, this methodology is the same as with former MIL-HDBK-217 (Pokorni, 2016).

Besides this, the calculation of hardware reliability is also faced with a number of problems. In (Elerath & Pecht, 2012), it is stated that there is no standard method for creating hardware reliability prediction, so predictions vary widely in terms of methodological rigor, data quality, extent of analysis, and uncertainty, and documentation of the prediction process employed is often not presented. Because of that, the IEEE has created a standard, IEEE Std.1413 (Standard Framework for the Reliability Prediction of Hardware) in 2009.

The IoT comprises different hardware concerning quality and reliability: very often this hardware is of a commercial type, without established reliability, and very often without any data about the failure rate or the mean time to failure (MTTF), or the mean time between failures (MTBF), so exact reliability calculation is very difficult.

IoT software reliability

Software reliability is an important attribute determining the quality of the software as a product. There are many models of software reliability assessment, but none of them is generally accepted (Pokorni, 2016, Kapur, 2014). Except that, the requirements for the reliability of software are often not adequately specified if specified at all, especially for the IoT.

The problem also lies in a different nature of software compared to hardware. Although defined as a probabilistic function, software reliability is not a direct function of time. Another problem is that techniques for software reliability prediction are rarely used as routine software engineering practices. It calls for collaboration between software and reliability subject matter experts to take appropriate steps to include software into the reliability case for the system (Pokorni, 2016), (Kapur, 2014).

The real issue with reliable software is that the critical function fails safe. Failing safe is often misunderstood and is often misinterpreted as never failing. Software safety and software reliability are allies in the realization of their mutual goal of developing safe and reliable software. Again, there is a need for a cooperation between software and reliability engineers. However, few educational institutions or industry professionals teach the basics of software reliability and its dependence upon software safety to be effective (Pokorni, 2014).

Enhancing reliability by redundant of software is a special problem, because it is different from hardware, and every copy of software has the error at the same place (Pokorni, 2014).

IoT human reliability

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

Human reliability can mean preventing accidents and minimizing the consequences of accidents that do occur. The effects of decisions made by people to act or not to act have consequences for the technological systems they operate. Disasters and major system failures are frequently a sequence of events where one or more people have made a decision or taken some action while operating, maintaining or repairing some technological system. When these potential consequences are significant, such as catastrophic loss of equipment, long term damage to the environment, or loss of life, then reliability engineers working collaboratively with others (such as risk management, human factors and safety engineers) can have an important impact (Pokorni, 2016).

There are different approaches and models to human reliability (Pokorni, 2016).

Procedures, rules, codes, standards and laws cannot completely prevent system failures, but, in this author's experience, they can reduce system failures.

This author has considered human reliability important from the beginning of his work in reliability, so human reliability is included in his textbooks (Pokorni, 2014).

About reliable and unreliable protocols

In computer networking, a reliable protocol is the name for a protocol which notifies the sender whether or not the delivery of data to intended recipients was successful.

For example, the TCP (Transmission Control Protocol), the main protocol used on the Internet, is a reliable protocol, and the UDP (User Datagram Protocol) is unreliable (because there is no guarantee of delivery of data, as in the TCP). Therefore, the UDP can be used in situations where some data loss may be tolerated.

There are also the Hot Standby Router Protocol (HSRP), the Virtual Router Redundancy Protocol (VRRP), and the Gateway Load Balancing Protocol (GLPB) used to enchance availability of computer networks providing redundancy. The HSRP provides routing redundancy for routing IP traffic without being dependent on the availability of any single router. The GLBP provides routing redundancy similar to that of the

HSRP and also provides load balancing over multiple routers by using a single virtual IP address and multiple virtual MAC addresses.

Maintainability and availability

Reliability is connected with maintainability. In order to achieve optimal cost in the life cycle of the IoT, maintainability must be considered in the design phase of the IoT. Maintainability refers to the ability for an intelligent system to be seamlessly and easily uncoupled, fixed and modified without causing an obstruction in the system processes or functionality. To evaluate the maintainability property of the IoT system, in case of a problem, the system should allow easy replacement of faulty components without loss of service. Therefore, to characterize IoT systems as highly maintainable, they have to enable maintenance tasks to be completed effectively, efficiently and with satisfaction (Thomas & Rad, 2017).

If we include maintainability, we speak about availability instead only of reliability. Availability is defined as the probability that the system or element is in a functional state at the moment the user needs it. If the system is unrepaired, then reliability and availability are the same. If the system is repaired, then availability is not the same as reliability. Availability (inherent availability) can be calculated using the next relation (Pokorni, 2014)

$$A = \frac{MTBF}{MTBF + MTTR} \tag{1}$$

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

Obviously, for example, replacing an exhausted battery in an IoT device can reduce availability if the IoT system is not in the working state during the replacement.

Other influences on the IoT reliability

The reliability of IoT is not only a matter of a failure rate of hardware and software, but also of protocols, energy efficiencies (green), standardization and other influences, such as, for example, security, etc.

The energy efficiency, reliability and security issues in the IoT (M2M communications) have not been well explored. The energy efficiency (green) becomes a challenging issue especially in the IoT sensor domain. IoT communications dominates energy consumption. There are

measures with which energy efficiency can be increased (Al-Fuqaha et al, 2015).

In (Higginbotham, 2018), it is stated that the IoT makes systems vulnerable to new security treats: consequences of failure are more dire (when car or infusion pumps are hacked people can die); today adversaries to the IoT security are not only hackers, but nation states; software and hardware vendors nowadays do not provide support as before; many IoT devices are built with software, hardware and firmware created by different companies and the problem can appear if some of these companies does not update its software; and many IoT devices live in environments unlike any IT systems.

Reliability and availability policies

Different users can expect different levels of reliability and availablity. So, aproaches to design an IoT system can be different depending of types of users. For example, the target level of availability for a given Google service usually depends on the function it provides and how the service is positioned in the marketplace. The following list includes issues to consider (Alvidrez, 2017):

What level of service will users expect?

Is this service directly connected to the revenue (either our revenue, or our customers' revenue)?

Is this a paid service, or is it free?

If there are competitors in the marketplace, what level of service do these competitors provide?

Is this service targeted at consumers or at enterprises?

Reliabilityof the IoT system

Because of a complexity of the IoT and because the IoT includes hardware and software and sometimes humans, we suggest assessing the reliability of hardware, the reliability of software and the reliability of the human factor, and then the reliability of the IoT system is calculated by the formula

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

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

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

The IoT is obviously very complex, so it is difficult, almost impossible, to determine the analytical solution for the reliability and availability of such a complex system.

Because of the complexity of the IoT, we suggest using simulation to asses the reliability of the IoT. We used simulation for some examples of complex systems and showed that simulations can give useful results (Pokorni & Janković, 2011), (Pokorni et al, 2011), (Ostojić et al, 2012).

Conclusion

The problem of the reliability of the Internet of Things from the point of view of the classical approach of reliability assessment using MIL-HDBK 217 is discussed in this paper. Because of the complexity of the IoT (the IoT includes hardware, software and sometimes human users), and because data in MIL-HDBK 217 are obsolete, the classical approach of reliability assessment of hardware using MIL-HDBK 217 is not appropriate, so we need other approaches for assessing reliability of hardware (for example RIAC's methodology, based on PRISM and new MIL-HDBK-217Plus), and of course adequate approaches for the assessment of reliability of software and the human factor. There are also other influences such as protocols, energy efficiencies, standardization security, etc.

Reliability assessment and the analysis of the IoT require knowledge from many different technical and other areas and team work.

Reliability of the IoT is not always of the primary concern in the IoT, but understanding reliability can help in case of failure, i.e. where to look for a failure.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communication Surveys & Tutorials,* 17(4), pp.2347 - 2376. Available at: https://doi.org/10.1109/COMST.2015.2444095.

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. Accessed: 20.04.2018.

Andersen, J. 2018. *What Does Reliability Have to do with the Internet of Things*? [online] Available at: https://www.stratus.com/stratus-blog/what-does-reliability-have-to-do-with-the-internet-of-things/. Accessed: 20.04.2018.

Bauer, E., & Adams, R. 2012. *Reliability and Availability of Cloud Computing*. Hoboken, NJ, USA: Wiley. Available at: https://doi.org/10.1002/9781118393994.

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.

Higginbotham, S. 2018. Internet of everything: 6 ways IoT is vulnerable. *IEEE Spectrum,* 55(7), p 21.

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.

Ostojić, D., Pokorni, S., Rakonjac, P., & Brkić, D. 2012. Accuracy of reliability calculated by Monte Carlo simulation method. *Vojnotehnički glasnik/Military Technical Courier,* 60(4), pp 47-58. Available at: https://doi.org/10.5937/vojtehg1204047O.

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

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.

Pokorni, S. 2018. Reliability of Internet of Things. In: 8th *International Scientific Conference on Defensive Technologies OTEH,* Belgrade*,* pp.567-570. October 11-12, ISBN 978-86-81123-88-4.

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.

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.

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. Accessed: 20.04.2018.

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.

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.

-Rohde & Schwarz GmbH & Co.*Testing IoT Devices: Battery Life, Application Note.* Munich, Germany.

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.

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.

НАДЕЖНОСТЬ И ДОСТУПНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ

Славко Й. Покорни
Колледж информационных технологий, г. Белград, Республика Сербия

Резюме:

В данной статье обсуждается проблема надежности и доступности Интернета вещей (IoT) с точки зрения классического метода оценки надежности с помощью MIL-HDBK 217. Однако при применении классического метода оценки надежности с помощью MIL-HDBK 217 можно оценить только надежность аппаратного обеспечения, в то время как ситуация с IoT намного сложнее, так как задействованы (объединены в сеть) миллиарды различных факторов: вещей (устройств), программных обеспечений, включая и людей. Надежность и доступность интернета вещей зависит не только от частоты отказов элементов (вещей), но также и от протоколов, стандартизации, логистической поддержки и других факторов. Предложено соотношение для расчета надежности системы IoT.

Ключевые слова: надежность, доступность, ремонтопригодность, интернет вещей.

ПОУЗДАНОСТ И РАСПОЛОЖИВОСТ ИНТЕРНЕТА СТВАРИ

Славко J. Покорни
Висока школа струковних студија за информационе технологије,
Београд, Република Србија

Сажетак:

У раду се разматра проблем поузданости и расположивости доступности интернета ствари (ИоТ) са становишта класичног приступа процене поузданости помоћу МИЛ-ХДБК 217. Коришћењем класичног приступа процене поузданости помоћу МИЛ-ХДБК 217 може се проценити само поузданост хардвера, а ситуација са ИоТ-ом је сложенија: милијарде различитих ствари (уређаја), софтвера, укључујући људе, укључено је (умрежено). Поузданост и доступност интернета ствари није само питање степена отказа елемената (ствари) већ и протокола, стандардизације, логистичке подршке и других утицаја. Предложена је релација за израчунавање поузданости ИоТ система.

Кључне речи: поузданост, расположивост, погодност одржавања, интернет ствари.