Dependability of the Internet of Things: Current Status and Challenges

Alhassan Abdulhamid
Department of Computer Science
University of Bradford,
Bradford, UK
a.abdulh2@bradford.ac.uk

Sohag Kabir
Department of Computer Science
University of Bradford,
Bradford, UK
s.kabir2@bradford.ac.uk

Ibrahim Ghafir
Department of Computer Science
University of Bradford,
Bradford, UK
i.ghafir@bradford.ac.uk

Ci Lei
Department of Computer Science
University of Bradford,
Bradford, UK
c.lei1@bradford.ac.uk

***Abstract*— The advances in the Internet of Things (IoT) has substantially contributed to the automation of modern societies by making physical things around us more interconnected and remotely controlled over the internet. This technological progress has inevitably created an intelligent society where various mechatronic systems are becoming increasingly efficient, innovative, and convenient. Undoubtedly, the IoT paradigm will continue to impact human life by providing efficient control of the environment with minimum human intervention. However, despite the ubiquity of IoT devices in modern society, the dependability of IoT applications remains a crucial challenge. Accordingly, this paper systematically reviews the current status and challenges of IoT dependability frameworks. Based on the review, existing IoT dependability frameworks are mainly based on informal reliability models. However, these models are unable to effectively evaluate the unified treatment safety faults and cyber-security threats of IoT systems. Additionally, the existing frameworks are also unable to deal with the conflicting interaction between co-located IoT devices and the dynamic features of self-adaptive, reconfigurable, and other autonomous IoT systems. To this end, this paper suggested the design of a novel model-based dependability framework for quantifying safety faults and cyber-security threats as well as interdependencies between safety and cyber-security in IoT ecosystems. Additionally, robust approaches dealing with conflicting interactions between co-located IoT systems and the dynamic behaviours of IoT systems in reconfigurable and other autonomous systems are required.**

Keywords*— *Internet of Things, dependability analysis, safety, cyber-security, safety assurance, reconfigurable systems

I. INTRODUCTION

The IoT technology is a breakthrough that has penetrated most aspects of modern life. This breakthrough has remarkably digitised, transformed and revolutionised the world [1]. The paradigm of IoT advances the integration of various heterogeneous electronic devices and interconnected solutions which impact everyday life by connecting everyone and everything together [2]. Accordingly, the IoT is a paradigm shift of technology that intends to create an intelligent world where objects can communicate with each other through the internet platform [3, 4].

The breakthrough in IoT technology forms the centrepiece of the ongoing Cyber-Physical Systems (CPS), which integrates the interdependency of the physical objects in the environment with the cyber domain. Accordingly, the IoT and the CPS are inseparably the critical pillars of the ongoing fourth industrial revolution of the world [5, 6]. The applications of IoT technology cuts across several areas, such as home automation, smart cities, intelligent production systems, smart agriculture, smart health care and smart transportation, among others [1,7,49]. Moreover, IoT technology has an estimated economic impact which by 2025 would be about $3.9 to $11.1 trillion annually. This enormous economic projection underscores the importance of IoT innovations [50].

Albeit the widespread adoption of IoT systems is one of the most significant technological breakthroughs of the era, the requirement for highly dependable IoT devices has remained a challenge. For instance, high-consequence systems such as intelligent transportation systems, smart grids, and smart health services require highly secured and reliable systems [49]. Traditionally, the dependability of systems is estimated using reliability frameworks such as fault tree analysis (FTA), reliability block diagrams (RBD), model checking and Markov chain. However, unlike traditional mechanical systems, the IoT possesses both physical and cyber components, bringing numerous new issues cumulatively impacting its dependability [8]. Additionally, IoT applications have transcended to complex, connected, and evolving systems. Hence, these systems come with emerging dependability challenges which require new approaches [9].

The complex nature and heterogeneity of devices in the IoT ecosystem bring additional challenges to IoT dependability. Relatedly, conflicting interactions between co-located IoT systems and the evolving nature of modern IoT systems constrain existing informal manual reliability models [10-12]. To this end, to unlock the full potential of IoT applications, it has become expedient to reappraise the existing IoT dependability frameworks concerning their capacity to analyse IoT systems' complex and emerging features. Thus, this paper aims to conduct a systematic review of IoT dependability and suggests future work. Overall, the paper makes the following contributions:

- It provides a systematic review of the current trends in IoT dependability
- It examines emerging challenges in IoT dependability analysis.
- It draws open research issues in IoT dependability analysis.

After this brief introduction, the following Section conceptualised the IoT dependability and its attributes. Section III provides an overview of related work before Section IV covers emerging challenges in IoT dependability analysis. Finally, Section V concludes the paper and recommends future research direction.

II. IoT Dependability

Dependability is the ability of a system to reliably deliver the service it was designed to provide [13]. Accordingly, a dependable system should always be able to avoid failures that are more frequent and more severe than acceptable so that it can provide services that can justifiably be trusted [11, 12, 14, 15]. Generally, in the field of engineering, the concept of dependability has existed for decades. However, the concept has been more pronounced in the automotive and aerospace industries due to their safety criticalities [8, 14]. In the same view, over recent years, the rapid growth of CPS has contributed to the expansion of IoT applications into high-consequence domains that are either safety-critical or mission-critical [16]. Hence, the dependability of the IoT system started becoming a significant concern across the various stakeholders in the system. Appropriately, the system designers need to focus on developing IoT systems that should be relied upon and trusted under defined functional and environmental conditions. Based on the existing literature, the dependability of a system is evaluated based on six defined attributes: availability, integrity, reliability, confidentiality, safety, and maintainability [14]. Fig.1. depicted dependability attributes of a system.

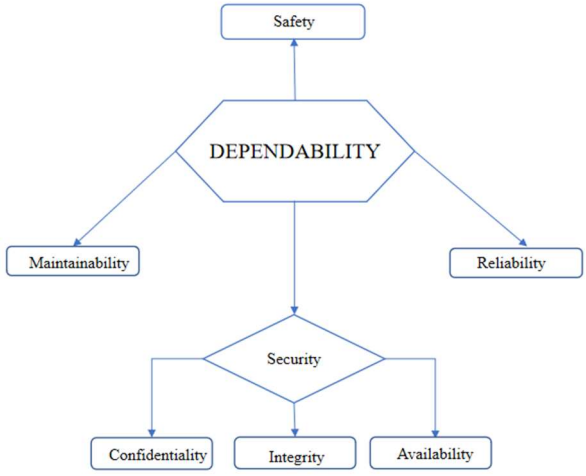

Fig. 1. Attributes of Dependability.

Dependability attributes of the IoT system could be affected by threats such as failures, faults, and errors, which could originate from deliberate malicious attacks, unintended random hardware failures, and possible conflicting interactions of devices, among others [12, 14]. To conduct dependability analysis, these attributes and their indices are modelled using various frameworks to quantify the overall system's dependability.

A. IoT Security

While IoT technology derives its value from the connectivity of the various pervasive systems and enables them to interact remotely over the internet connection, this comes with many security vulnerabilities that if exploited, can undermine IoT dependability [17]. In the case of simple mechanical or automobile systems which are not connected over the internet, their dependability can be easily predicted using existing traditional reliability approaches. These approaches evaluate the system dependability using established reliability indices of the sub-systems and components [11]. However, in the case of IoT systems, in addition to the components' reliability, the system's dependability is further affected by innumerable cyber-security threats. Moreover, a large volume of heterogeneous data, the complexity of IoT technology, and the absence of defined limits regarding the physical expansion of the systems, number, and types of interconnected devices were described as some of the common features of IoT systems [18]. These features, from cyber-security viewpoints, contribute to an increase in attack surfaces in IoT systems which open doors to security breaches at an unprecedented pace [18-19]. Consequently, security is considered a critical non-functional property of a dependable IoT system which is an imperative requirement to guarantee the system's confidentiality, integrity, and availability (CIA) [12, 20-22].

Among the multiple issues concerning IoT design, researchers viewed security at the forefront of the challenges of IoT systems [12, 23]. Based on the literature, the CIA triad, which was considered the core foundation of data security, is, at the same time crucial attributes of a system's dependability [8, 14]. Thus, security threats against CIA of IoT data, if exploited, could result in abnormal behaviour of the system and, consequently, affect its dependability. For instance, an alteration of IoT sensing or actuation data which is a security breach against data integrity could cause deviation from the nominal behaviour of the IoT system and, thus, negatively affect its dependability [24]. Likewise, a denial-of-service attack, which is a breach of the system availability, could constitute system downtime, which impedes the system's dependability, especially in safety or mission-critical services [25]. Hence, a comprehensive analysis of the CIA triad must be conducted alongside the other dependability attributes to safeguard IoT dependability. However, ensuring CIA of sensing and actuation data between various IoT entities is a considerable challenge to system designers [18, 26]. Accordingly, various threat analysis frameworks and models were developed to evaluate cyber-security threats and help the system designers to develop secured and reliable IoT applications

B. IoT Safety

Safety is the absence of catastrophic consequences on the user(s) and the environment [14]. Like the security artefacts discussed, safety as an attribute of dependability is also crucial, especially with the increasing applications of IoT systems in safety-critical domains such as biosensor systems, and autonomous vehicles, among others. Safety violations in IoT design and operations may cause harm to the users, other systems, or the environment in which the IoT operates. In safety-critical domains, failures, or abnormal behaviours of IoT systems or components at some critical moments could result in catastrophic consequences, which could be fatal to the users, other systems or the environment. Therefore, a safety analysis of IoT systems is necessary to ensure that the systems do not pose threats or cause physical harm to the users and the environment [27]. This is achieved by evaluating unintended random failures of hardware, cyber-security threats and conflicting interactions between IoT applications. An effective safety analysis framework should safeguard the IoT system from entering unsafe or dangerous physical states during its operations.

C. IoT Reliability

The reliability and safety of IoT systems are closely related as both are essential design goals in IoT architecture. The reliability of a system is the probability of a system running without failure for a defined period [11, 19].

Reliability analysis is carried out to investigate the degree a system will require to meet specific performance standards in delivering correct, desired, and intended output over a given period. The reliability of IoT could be affected not only by the random failure of components but also by deliberate cyber or physical attacks [28]. Therefore, rigorous dependability analysis techniques are employed to ensure the safety and reliability of IoT systems. Various reliability frameworks were developed and modified to ascertain the probability that a system could remain dependable over time. These frameworks are used to analyse the reliability properties of the system's components and evaluate their nominal as well as failure behaviours over defined operating periods and conditions. Indices used to quantify system reliability include but are not limited to failure rate, average time out, and average unavailability, among others.

D. IoT Maintainability

Maintainability is the ability of a system to undergo repairs and modifications [14]. Maintainability is a measure that shows the probability that a failing system can be repaired and returned to service in a specific period. The Mean Time to Repairs (MTTR) and Mean Time Between Repairs (MTBR) are indicators measuring a system's maintainability. In the context of IoT dependability, maintainability involves the capacity of an IoT device(s) while undergoing repairs to keep working to meet its intended functionality [13]. Broadly, maintainability also relates to the system's continued operation, which may involve duties like accommodating new requirements, re-organising code and other maintenance tasks which extend the applicable life period of IoT devices [29].

III. Related Works

To evaluate the dependability of IoT, various attributes that constitute the system's dependability are analysed using one framework or the other. However, reliability and availability are the most analysed using a quantitative approach, among other dependability attributes [30]. From the literature, reliability analysis is conducted using various quantitative and qualitative frameworks to evaluate system reliability. Some of the existing frameworks used for reliability analysis are RBD, FTA, Markov chain, and model checking, among others. However, the most widely accepted technique of conducting dependability analysis is based on FTA and its extensions [11, 21, 30-32]. FTA is a graphical risk assessment technique developed by Bell Laboratories in the early 1960s, which is used to determine how the occurrence of a component failure in a system can propagate to cause complete system failure [30]. The technique is used in system safety and reliability to determine the combination of basic component failures that can lead to an overall system failure using the traditional Boolean logic gates 'AND' and 'OR' [11]. The FTA technique is a systematic, graphical, and deductive process that explores logical connections between faults and their causes in a system using various events and gate symbols [21, 31]. Accordingly, dependability analysis is conducted using FTA in two folds. Namely, the qualitative approach involves reducing the FTA to minimum cut sets (MCSs) using various algorithms such as the Method of Obtaining Cut Set (MOCUS) [11]. This approach gives the basic events that must happen for the system to go down. Therefore, critical components of the system could be identified, and necessary redundancy will be built to ensure the system's dependability [11]. On the contrary, the quantitative approach in FTA involves probabilistic estimation of the reliability of the top event from the reliability of the basic events. The probability of primary events is derived from external information, e.g., components specification and reliability data. For all other events, their probability is calculated based on their immediate descendant events and gate symbol, which define their logical connection. Over time, FTA has been further modified and extended to capture various dynamic behaviours of systems. From the literature, various modifications of FTA were developed, such as dynamic FTA and non-coherent FTA, which added one or more functional gates to cater to various dynamic operational circumstances of systems [11, 21, 30-33].

Additionally, various threat modelling frameworks were developed within the security domain. Cyber security threat models such as STRIDE, CORAS and attack trees are some of the common threat modelling frameworks used in the IoT domain [18, 21, 26, 32, 34]. Like FTA, which is based on the component failure, the attack tree frameworks evaluate potential attacks and threats against the IoT system. While probabilistic techniques are used in FTA to determine the root cause of system failure, the attack trees explore a similar approach to determine the likelihood of a specific class of attack succeeding [32].

Recently, as the research in dependability studies continues to evolve. Accordingly, in responding to the emerging features of modern technological systems, new approaches were developed, which tend to unify cyber-security threats and system reliability. Notably, the attack tree and fault tree were combined as an attack-fault tree (AFT) framework and others such as non-coherent FT [21, 28, 31, 32, 35-39]. While such approaches open research prospects in the unified treatment of safety and security, the efforts have so far been at the infancy stage in the IoT domain.

From the assessment of extant literature, the existing approaches of IoT dependability analysis are oversimplified and unable to effectively evaluate the complex nature of IoT systems. While most of the dependability frameworks focus on only the reliability analysis of the system, others consider either reliability and physical security or selected properties of cyber-security. So far, based on the extant literature surveyed, there have not been any robust unified frameworks that effectively model the impact of reliability, availability, confidentiality, and integrity as well as their interdependencies in IoT dependability analysis. Therefore, the existing frameworks are inadequate to address the complex physical and cyber-physical interactions of IoT systems. To this end, several challenging areas are yet to be addressed in IoT dependability.

IV. Challenges in IoT Dependability Analysis

In this Section, we present some pertinent challenges affecting IoT dependability analysis.

A. Unified Treatment of Safety and Security Analysis of IoT

As earlier stated, safety and security are both critical attributes of a dependable IoT system and, indeed, intertwined in so many ways. The consequence of safety is related to risks that could have a potential impact on the system environment, while security is related to risks that can have consequences on the system itself or its

environment [27, 40]. Security property allows the system to perform its mission or critical functions despite risks posed by threats, while the safety property guards against the risk of harm due to malfunctioning behaviour of the systems. Therefore, the inability to ensure safety and security properties in IoT design can hamper the widespread adoption of the technology. Accordingly, these properties deserve ample consideration as the key drivers to managing and reducing adverse events and avoiding impact on health, safety, and the environment [41]. Safety and security are related, and their interdependence needs to be analysed in a unified approach. This study of the relationships between safety and security in CPS is an ongoing issue, as well as research in the unified analysis of their interdependence [12, 15, 16, 38-44].

Based on the literature, similarities between safety and security and their associated risk analysis techniques make their integration a reasonable and achievable goal [28, 45, 46]. Accordingly, unifying a safety and security framework using a single methodology could result in a single set of requirements describing the safety and security functions of the IoT system. Furthermore, by harmonising safety and security frameworks, their interdependencies and conflicts could become more apparent. Notably, there are four established interdependencies between safety and security in CPS. Firstly, conditional dependency in which safety and security requirements are conational to one another. Second is mutual reinforcement, in which safety requirements contribute to security or vice-versa. On the other hand, antagonistic relationships between safety and security requirements which are considered jointly, lead to conflicting situations. Lastly, the independence relationship implies that there is no interaction between safety and security properties [38, 39]. Therefore, there is a need to exploit the complex interaction between safety and security systematically. Undoubtedly, these interdependences could only be analysed effectively using a unified framework. The unified framework will enhance a better understanding of the IoT system and its environment. This would facilitate recognition of conflicts and trade-offs and allow judgement-based decisions to be made. Consequently, the results of safety and security co-analyses could facilitate better dependability analysis of IoT systems [41].

To the extent of this survey, the research in the unified treatment of safety and security has so far mainly focused on reliability, and physical security, while few others considered reliability and cyber security. For instance, Karia et al. in [38] and [39] attempted to quantify reliability and security in a unified framework using case studies of smart pipeline leak detection systems and emergency exit doors. The analysis combined accidental and malicious disruption scenarios yielding probabilistic estimates over time. However, the framework failed to sufficiently quantify confidentiality, availability, integrity, and reliability in the same environment. Similarly, Kabir et al. in [12] developed a framework that considers security and safety in IoT-smart-based systems. However, the framework aptly captured novel safety concerns such as design and operations time safety monitoring and the example of conflict of interaction between co-located IoT systems but failed to address the safety and security interactions in the model. Therefore, it is evident from the state-of-the-art dependability analysis of IoT systems that there are insufficient frameworks that quantify and unify the complex interactions and interdependencies between the safety and security of the IoT ecosystem. Consequently, this creates novel opportunities for further research.

B. Informal Modelling of Dependability Analysis of IoT

As discussed in Section III, FTA can help system engineers determine how the occurrence of basic component faults in a system can propagate to cause a total system failure. Furthermore, it also assists in determining critical components of the system from qualitative analysis using the MCSs technique [11]. However, in the context of IoT, there are some identified constraints associated with FTA which could impede reliability and safety analysis. For instance, FTA is a manual process that is often time-consuming, performed based on an informal system model that is cumbersome and subject to a human error leading to inconsistency or incompleteness [11]. This could affect IoT system dependability analysis, especially in complex systems.

Additionally, the FTA technique is based on static system conditions and, at the same time, lacks support for reusability. As the IoT system is getting more complex by the day due to its greater applicability in numerous domains, this brings the need to develop a robust model-based dependability framework that would enhance the dependability analysis of the IoT systems. To this end, research on model-based dependability frameworks is considered a research direction in IoT dependability analysis.

C. Conflicting Interactions Between Multiple Co-located IoT Systems

It is vital to appreciate that different manufacturers are developing various IoT systems, and without proper analysis of the possibility for the users to have incompatible systems within the same environment. The goal of dependability analysis of the IoT ecosystem is to ameliorate the risk of the system entering an unsafe or dangerous physical state which could be counter-productive to its purpose. However, these states could occur not only because of unintended hardware failures or intended cyber security threats but even in the interaction between the various co-located IoT systems [12, 47]. For instance, authors in [12] demonstrated an example of conflicting interaction of co-located IoT systems where safety could be compromised due to bad interaction between smart flood detection and smart fire detection systems. The authors demonstrated that the nominal behaviour of smart fire detection and prevention IoT systems is to turn on the sprinkler system in a smart home to extinguish a fire in the event of a fire incident. However, if at the same smart home there is another smart flood detection system, it would detect the activation of the sprinkler system by the smart-fire detection system as a flooding hazard and trigger the shut-off valves. Consequently, this negative interaction might result in safety hazards despite both systems being within their dependable state. Accordingly, this creates an avenue for further research in IoT dependability frameworks to develop a model that can cater for dependability issues resulting from bad interactions between co-located IoT systems.

D. *Dependability of Self-Adaptive and Increasing Autonomous IoT Systems*

IoT systems have constantly been evolving due to advancements in knowledge of the domain. Accordingly, modern IoT systems are evolving with various dynamic behaviours which were not considered in traditional dependability analysis. For instance, reconfigurable, self-adaptive and cooperative behaviours of CPS have posed challenges to existing traditional dependability analysis frameworks of IoT systems [9, 48]. These modern and emerging IoT systems have different nominal and failure behaviours. For instance, to illustrate this problem, a phase-mission CPS-like aircraft contains various smart components which are subject to different conditions during different phases of the aircraft movements. This resultantly subjects the various smart components to undergo different environmental conditions that might result in varying failure rates. This is a challenge to the notion of fixed design time dependability analysis earlier discussed. Furthermore, IoT applications are also expanding in scope, especially in Industry 4.0, which comprises interconnected mainly and increasingly autonomous systems [10]. In these domains, some of the IoT systems are self-adaptive, reconfigurable, and even cooperative. These autonomous and other dynamic behaviours of modern IoT systems bring emerging issues of their dependability which have not been well understood. Additionally, loosely connected, or temporary configurable systems could not be effectively analysed with the existing dependability analysis frameworks that mainly focus on the design time analysis of fixed IoT systems. Therefore, further research is required to guarantee IoT dependability vis-a-vis the evolution of increasingly autonomous systems.

V. Conclusion and Future work

In this paper, we provided an overview of IoT dependability, which is critical to IoT systems' evolving nature and rapid development. The IoT dependability was discussed based on dependability attributes and existing approaches. Traditionally, existing dependability analysis frameworks focused more on evaluating the reliability and safety attributes of systems. However, in the paradigm of IoT, the systems' dependability is affected not only by reliability, safety, and maintainability attributes but heavily by the CIA due to its cyber-components. These systems' security attributes and interdependencies between safety and security must be exploited in IoT dependability to mitigate their risks. Based on this, current challenges of IoT dependability were analysed. Notably, there are insufficient frameworks that vigorously co-analysis random hardware failures and intentional cyber-security threats against IoT data. Similarly, most of the existing informal reliability frameworks are based on manual FTA, and they lack the flexibility to evaluate complex IoT architecture effectively. Lastly, conflicting interactions between co-located IoT systems and the dependability of reconfigurable and other autonomous systems are emerging challenges in IoT dependability that need further research attention.

Based on the gaps identified in this survey, our future work will focus on extending the existing FTA, AT, and AFT frameworks to model the unified treatment of reliability, availability, confidentiality, and integrity of IoT systems. Additionally, we plan to extend our proposed framework to a model-based dependability approach that enables a formal, computerised, and more dynamic dependability analysis, thereby enabling the design of highly dependable IoT systems.

Acknowledgement

This work has been supported by the SURE project BA237 (023000/66005).

References

[1] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," Computer Networks, vol. 148, pp. 241-261, 2019.

[2] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," IEEE Access, vol. 8, pp. 138406-138446, 2020.

[3] S. Agrawal and M. L. Das, "Internet of Things—A paradigm shift of future Internet applications," in 2011 Nirma University International Conference on Engineering, 2011: IEEE, pp. 1-7.

[4] U. Raza, J. Lomax, I. Ghafir, R. Kharel, and B. Whiteside, "An IoT and business processes-based approach for the monitoring and control of high value-added manufacturing processes," in Proceedings of the International Conference on Future Networks and Distributed Systems, 2017, pp. 1-8.

[5] K. Schwab, The fourth industrial revolution. Currency, 2017.

[6] M. Hammoudeh, I. Ghafir, A. Bouncer, and T. Rawlinson, "Continuous monitoring in mission-critical applications using the internet of things and blockchain," in Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, 2019, pp. 1-5.

[7] A. Khanna and S. Kaur, "Internet of things (IoT), applications and challenges: a comprehensive review," Wireless Personal Communications, vol. 114, no. 2, pp. 1687-1762, 2020.

[8] T. Frühwirth, L. Krammer, and W. Kastner, "Dependability demands and state of the art in the internet of things," in 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), 2015: IEEE, pp. 1-4.

[9] S. Kabir et al., "A runtime safety analysis concept for open adaptive systems," in International Symposium on Model-Based Safety and Assessment, 2019: Springer, pp. 332-346.

[10] E. E. Alves, D. Bhatt, B. Hall, K. Driscoll, A. Murugesan, and J. Rushby, "Considerations in assuring the safety of increasingly autonomous systems," 2018.

[11] S. Kabir, "An overview of fault tree analysis and its application in model-based dependability analysis," Expert Systems with Applications, vol. 77, pp. 114-135, 2017.

[12] S. Kabir, P. Gope, and S. P. Mohanty, "A Security-enabled Safety Assurance Framework for IoT-based Smart Homes," IEEE Transactions on Industry Applications, 2022.

[13] A. Avizienis, J.-C. Laprie, and B. Randell, "Fundamental concepts of computer system dependability," in Workshop on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments, 2001: Citeseer, pp. 1-16.

[14] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE transactions on dependable and secure computing, vol. 1, no. 1, pp. 11-33, 2004.

[15] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: from dependability to security," IEEE Transactions on dependable and secure computing, vol. 1, no. 1, pp. 48-65, 2004.

[16] E. Araujo, J. Dantas, R. Matos, P. Pereira, and P. Maciel, "Dependability evaluation of an IoT system: A hierarchical modelling approach," in 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), 2019: IEEE, pp. 2121-2126.

[17] N. Papakonstantinou, J. Linnosmaa, A. Z. Bashir, T. Malm, and D. L. Van Bossuyt, "Early combined safety-security Defense in Depth assessment of complex systems," in 2020 Annual Reliability and Maintainability Symposium (RAMS), 2020: IEEE, pp. 1-7.

[18] M. Mahak and Y. Singh, "Threat Modelling and Risk Assessment in the Internet of Things: A Review," in Proceedings of Second International Conference on Computing, Communications, and Cyber-Security, 2021: Springer, pp. 293-305.

[19] L. Xing, "Reliability in the Internet of Things: Current status and future perspectives," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6704-6721, 2020.

[20] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," IEEE Internet of things journal, vol. 5, no. 4, pp. 2483-2495, 2017.

[21] R. Kumar and M. Stoelinga, "Quantitative security and safety analysis with attack-fault trees," in 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), 2017: IEEE, pp. 25-32.

[22] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE internet of things journal, vol. 4, no. 5, pp. 1125-1142, 2017.

[23] M. Wolf and D. Serpanos, "Safety and security in cyber-physical systems and internet-of-things systems," Proceedings of the IEEE, vol. 106, no. 1, pp. 9-20, 2017.

[24] I. Ghafir, K. G. Kyriakopoulos, F. J. Aparicio-Navarro, S. Lambotharan, B. Assadhan, and H. Binsalleeh, "A basic probability assignment methodology for unsupervised wireless intrusion detection," IEEE Access, vol. 6, pp. 40008-40023, 2018.

[25] D. M. Diab, B. AsSadhan, H. Binsalleeh, S. Lambotharan, K. G. Kyriakopoulos, and I. Ghafir, "Denial of service detection using dynamic time warping," International Journal of Network Management, vol. 31, no. 6, p. e2159, 2021.

[26] G. Kavallieratos, V. Gkioulos, and S. K. Katsikas, "Threat analysis in dynamic environments: The case of the smart home," in 2019 15th international conference on distributed computing in sensor systems (DCOSS), 2019: IEEE, pp. 234-240.

[27] J. Zalewski, "IoT safety: state of the art," IT Professional, vol. 21, no. 1, pp. 16-20, 2019.

[28] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," Reliability engineering & system safety, vol. 139, pp. 156-178, 2015.

[29] R. Sasaki, "A Risk Assessment Method for IoT Systems Using Maintainability, Safety, and Security Matrixes," in Information Science and Applications: Springer, 2020, pp. 363-374.

[30] E. Editor, N. Gordon, and M. Walker, "Dependability Analysis Using Temporal Fault Trees and Monte Carlo Simulation," in International Conference on Dependability and Complex Systems, 2021: Springer, pp. 86-96.

[31] C. E. Budde, C. Kolb, and M. Stoelinga, "Attack trees vs fault trees: two sides of the same coin from different currencies," in International Conference on Quantitative Evaluation of Systems, 2021: Springer, pp. 457-467.

[32] I. N. Fovino, M. Masera, and A. De Cian, "Integrating cyber-attacks within fault trees," Reliability Engineering & System Safety, vol. 94, no. 9, pp. 1394-1402, 2009.

[33] M. Jablonowski, D. Wijesekera, and A. Singhal, "Generating Cyber-Physical System Risk Overlays for Attack and Fault Trees using Systems Theory," in Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2022, pp. 13-20.

[34] M. S. Lund, B. Solhaug, and K. Stølen, Model-driven risk analysis: the CORAS approach. Springer Science & Business Media, 2010.

[35] P. Anand, Y. Singh, A. Selwal, P. K. Singh, and K. Z. Ghafoor, "IVQFIoT: An intelligent vulnerability quantification framework for scoring internet of things vulnerabilities," Expert Systems, vol. 39, no. 5, p. e12829, 2022.

[36] M. Brunner, M. Huber, C. Sauerwein, and R. Breu, "Towards an integrated model for safety and security requirements of cyber-physical systems," in 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2017: IEEE, pp. 334-340.

[37] N. H. C. Guzman, I. Kozine, and M. A. Lundteigen, "An integrated safety and security analysis for cyber-physical harm scenarios," Safety Science, vol. 144, p. 105458, 2021.

[38] S. Kriaa, M. Bouissou, F. Colin, Y. Halgand, and L. Pietre-Cambacedes, "Safety and security interactions modelling using the BDMP formalism: a case study of a pipeline," in International Conference on Computer Safety, Reliability, and Security, 2014: Springer, pp. 326-341.

[39] S. Kriaa, M. Bouissou, and Y. Laarouchi, "A new safety and security risk analysis framework for industrial control systems," Proceedings of the Institution of Mechanical Engineers, Part O: Journal of risk and reliability, vol. 233, no. 2, pp. 151-174, 2019.

[40] J. Draeger, "Roadmap to a unified treatment of safety and security," 2015.

[41] M. Stoelinga, C. Kolb, S. M. Nicoletti, C. E. Budde, and E. M. Hahn, "The Marriage Between Safety and Cybersecurity: Still Practicing," in International Symposium on Model Checking Software, 2021: Springer, pp. 3-21.

[42] R. Winther, "Qualitative and Quantitative Analysis of Security in Safety and Reliability Critical Systems," London, 2004: Springer London, in Probabilistic Safety Assessment and Management, pp. 2345-2351.

[43] G. Bakirtzis, B. T. Carter, C. R. Elks, and C. H. Fleming, "A model-based approach to security analysis for cyber-physical systems," in 2018 Annual IEEE International Systems Conference (SysCon), 2018: IEEE, pp. 1-8.

[44] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modelling and risk assessment in IoT systems," Internet of Things, vol. 7, p. 100056, 2019.

[45] S. Chockalingam, D. Hadžiosmanović, W. Pieters, A. Teixeira, and P. v. Gelder, "Integrated safety and security risk assessment methods: a survey of key characteristics and applications," in International Conference on Critical Information Infrastructures Security, 2016: Springer, pp. 50-62.

[46] S. Max, "Lot safety and security as a shared responsibility," Бизнес-информатика, no. 1 (35), pp. 7-19, 2016.

[47] D. T. Nguyen, C. Song, Z. Qian, S. V. Krishnamurthy, E. J. Colbert, and P. McDaniel, "IotSan: Fortifying the safety of IoT systems," in Proceedings of the 14th International Conference on emerging Networking Experiments and Technologies, 2018, pp. 191-203.

[48] S. Kabir, "Internet of Things and safety assurance of cooperative cyber-physical systems: opportunities and challenges," IEEE Internet of Things Magazine, 2021.

[49] A. Hussaini, C. Qian, W. Liao, and W. Yu, “Taxonomy of Security and Defense Mechanisms in Digital Twins-based Cyber-Physical Systems,” IEEE International Conferences on Internet of Things (iThings), 2022.

[50] Manyika, Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D, Unlocking the Potential of the Internet of Things. McKinsey Global Institute, 2015.