Safety and Security Issues in the IoT Domain

Subjects: Computer Science, Hardware & Architecture

Contributor: Alhassan Abdulhamid, Sohag Kabir, Ibrahim Ghafir, Ci Lei

The Internet of Things (IoT), which is developing quickly, has continued to provide humanity with many advantages, including many applications crucial for security and safety. The assurance that IoT devices will not pose a risk to people or the environment is necessary to realise the full potential of IoT applications, particularly in high-consequence areas. To develop safe, secure, and dependable IoT systems, it is necessary to comprehend a wide range of safety and security issues across the IoT's architectural frameworks and levels. As a result, among other attributes of dependable IoT systems, this research outlines safety and security features.

Keywords: Internet of Things ; safety ; security ; analysis frameworks ; safety and security coanalysis

1. Introduction

The Internet of Things (IoT) is evolving swiftly as numerous IoT applications have thus far made successful market entries or have already implemented some prototypes across various domains. By incorporating intelligence-driven applications into IoT innovation, conventional electronics and mechatronics systems across a variety of domains have been converted into smart and intelligent systems. The integration of current systems' sensing, processing, communication, reasoning, and actuation capabilities has been made possible by technological advancement [1]. The IoT has ushered humanity into a technological paradigm, which has created a more efficient, intelligent, and convenient environment [2]. While the breakthrough in IoT innovations has brought uncommon benefits for humanity, conversely, it has also opened new avenues for potential risk hazards capable of causing harm to the users and the environment. Some risks associated with intelligent and embedded internet-enabled systems were non-existent in traditional electronic or mechanical systems, which are not internet-enabled in their operations [3]. Also, given the increasing autonomy of IoT systems in making decisions, the safety, security and ethical use of these smart devices are increasingly becoming a concern across the board [4]. These and many other considerations underscore the need for the safety and security assurance of IoT innovations.

Safety and security are key non-functional properties (NFP) of IoT systems and constitute critical attributes of IoT dependability [3][5]. While system dependability deals with the system performing at its optimal functionality over a specified period [3], safety attributes entail that devices are devoid of harm to their users or damage to the environment [6][7][8]. Similarly, a system’s security attributes concern how it performs its intended functions and mission despite the risk posed by security threats [9][10][11]. Safety and security properties can affect one another in numerous ways. Notably, the two properties are both sources of hazards, and a breach of one can affect the other [12].

The safety and security of IoT systems could be compromised through random hardware faults and errors, conflicting interactions, human errors, and deliberate security attacks against a system, components, or its operations [5][13][14]. While it is difficult to guarantee a completely safe and secure system, it is a design requirement to ensure that safety and security thresholds are made to support the dependability of systems and certification standards. To meet these requirements, safety and security impediments, such as random and systematic system failures and security threats, need to be adequately identified, quantified, and mitigated. This analysis, if well carried out from the early stage of the system design, will guard against unacceptable levels of malfunctioning components and confer resilience against security threats that could adversely lead to a precarious and dangerous operating state of the systems [14].

2. Existing Safety and Security Analysis Frameworks

Based on the literature, numerous analysable models and tools have been developed to evaluate various safety and security metrics of mechatronics, industrial control systems, aerospace systems, automobile systems, and other embedded systems. The existing analysis methods derive their relevance based on their efficiency to identify, quantify, and mitigate various safety and security parameters of the systems [3][15][16][17][18]. Notably, during the system development life cycle (SDLC), systems undergo various testing and verification processes, and one of these is to

evaluate the functional safety and security properties of a proposed system. Based on this proactive system design philosophy, existing safety and security analysis models and frameworks provide insight into component failures, security threats, vulnerabilities, and other root causes of faults, errors, and failures. If effectively conducted with the right model or approach, this evaluation process can significantly ensure that design flaws are reduced so that the system development poses no safety or security hazards to its users, other stakeholders, or the environment.

The existing safety and security analysis methods and techniques in the literature have been categorised into informal manual frameworks and MBSE approaches. Some of the notable manual frameworks are the Failure Mode Effect Analysis (FMEA), Fault Trees Analysis (FTA), Dynamic Fault Trees, Petri Nets, Attack Trees (AT), Attack–Fault Trees, Attack–Defence Trees, Quantitative Attack Defence Trees, and Bowties, among others [19][20][21][22]. On the other hand, to meet the continuous requirements of systems development, some of the safety-critical domains, such as the automobile [23] and aerospace industries [24], as well as industrial control systems [25], have begun to explore the options of MBSE approaches. Notably, MBSE approaches have been used to analyse the various NFPs of system design, such as performance [26][27], safety [28][29][30][31][32], reliability [30][32], and security properties [33][34][35]. In the model-driven development paradigm, some of the classical analysable models such as FTA, AT, Petri nets, and other artefacts are fully or semi-automatically generated using software-based approaches. These approaches generate artefacts based on detailed modelling of the systems' static and dynamic behavioural patterns using methodologies drawn from the existing modelling languages (ML) functionalities. Existing MBSE frameworks have been developed using the unified modelling language/system modelling language (UML/SysML) [25][29], the Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS) [31][32][34][35], and the Architecture Analysis and Design Language (AADL) [24][26][35]. While research into safety and security analysis frameworks is fast progressing by the day, a most recent overview of the existing IoT-based safety and security (classical and MBSE) approaches can be found in ref.[36] .

While there are numerous classical and model-based analysis frameworks in the safety and security domains, their viability to critically evaluate the dependability of IoT applications needs to be further studied. Although separate analyses of the safety and security properties could suffice in other fields, the case differs in cyber-physical systems (CPS). The peculiarity of CPS, for which the IoT is at the centre stage, demands a high consideration of the safety and cyber-security properties to develop dependable systems [37]. In the IoT environment, safety and security requirements are becoming increasingly interwoven, and the systems are increasingly given autonomous, adaptive, and evolving features [5]. Therefore, to guarantee the smooth operations of the IoT systems, evaluating the existing safety and security analysis approaches is necessary vis-a-vis the unique nature of IoT systems.

3. Safety and Security Challenges of the IoT System

The freedom to innovate any technology comes with the inherent responsibility of safeguarding the users and the environment from its harmful effects [38]. With the greater acceptability of IoT in today's modern space, safety and security continue to remain paramount for various reasons. While the environment is permeated by the innovations of various applications of IoT systems, which are given the increasing autonomy of decision-making, the possibility of safety hazards should not be ruled out if the safety requirements of the systems are not adequately evaluated [13]. Moreover, in the area of standardisation, a functional safety threshold is a core prerequisite for the market entry and practical use of these modern devices, especially in safety-critical and mission-critical domains [10][39]. Therefore, for the IoT to be accepted and trusted, the systems must be relatively safe, secure, and devoid of harm to the users or harm to the environment [40]. Based on these considerations, the development of dependable IoT applications necessitates careful attention to safety issues. The safety requirements that are put into design consideration are meant to reduce the possibility that a device could malfunction or enter into harmful or hazardous operating conditions as a result of design flaws. To guarantee this in the IoT design, a vigorous analysis of various factors and conditions that can compromise the safety of the systems must be conducted. Thus, safety issues are crucial design requirements that need to be given due attention from the SDLC stage in order to guard against the possible negative consequences [13].

Conversely, security is a critical design challenge in the IoT domain for obvious reasons. The IoT technology extends internet connectivity to become pervasive, as everything (heterogeneous physical and virtual systems) with respect to the IoT systems will be connected to the internet and, at the same time, communicate with one another [41][42]. This makes the IoT ecosystem characterised by heterogeneity, the absence of defined limits regarding physical expansion, and the number and types of interconnected devices, all of which tend to create additional security risk hazards for the IoT systems [3][13]. The attack surfaces of IoT-Enabled applications tend to be higher due to the aforementioned reasons. Thus, the constraints open doors to increasing security breaches at a more significant proportion, which system developers need to cater to assure users of secure and dependable smart IoT-enabled applications [6][41]. Therefore, in the design of dependable IoT systems, it is imperative to conduct safety and security analyses iteratively throughout the

SDLC stage and to monitor the same processes during the operational stage to assure the safety and security of the end users and the environment [13]. To discuss the safety and security design requirements of the IoT system it is necessary to highlight the issues layer-wise, as each of the layers of the IoT architecture may have particular safety and security issues. Accordingly, the existing layers of the IoT architecture will be briefly highlighted prior to discussing their safety and security concerns.

4. The IoT System Architecture

A generic IoT system is represented using a layer architectural framework that uses various standards and layer structures [2]. Some of the most common frameworks are three-layer, four-layer, and five-layer architectures [2][43][44][45]. **Figure 1** presents the IoT four-layer architecture. The layers are the perception, network, processing, and application layer.

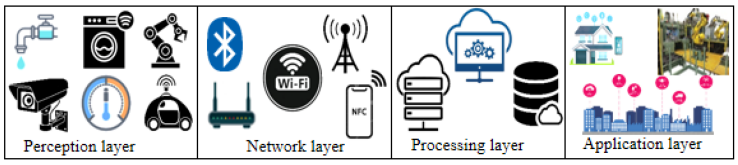

Figure 1. IoT Four-Layer Architecture.

4.1. Perception Layer

The perception layer of the IoT architecture is composed of various devices that primarily deal with the sensing of the environment and the actuation of physical processes. These devices, including sensor nodes and actuators, are expected to have high reliability, ease of use, a higher resolution, high sensitivity, smart detection, and minimum power consumption, among others [46]. In this layer, various sensor nodes perform sensing measurements of the environment and other physical parameters [2][46]. Data acquisition of physical parameters, such as object properties, biometrics, and physiological or environmental conditions, is made by various sensor nodes and data acquisition devices.

4.2. Network Layer

The network layer is the second layer in the IoT architecture, which is responsible for the reliable transmission of sensing data generated from the perception layer to the computational unit for information processing [2][42][47]. The network layer conveys data across interfaces and gateways using communication technologies and protocols, especially the Internet protocol [42]. This layer of IoT architecture sets the rules for data aggregation. The network layer integrates devices, such as hubs, switches, and gateways, as well as communication technologies such as Bluetooth, Wi-Fi, and Long-Term Evolution (LTE) [2].

4.3. Data-Processing Layer

The data-processing layer is the IoT system's event-processing layer, which ensures seamless software interaction for the storage and processing of IoT data [2][43][44][47]. This layer leverages many connected computing technologies in the form of cloud technology to store, compute, secure, and process various sensing data. The processing layer bridges the application and network layer, which is responsible for data accumulation, abstraction, and analysis [47][48]. Data processing is carried out via cloud computing and multiparty computation, where mass data processing and intelligent processing are conducted [42]. The layer processes the data obtained from the perception layer through numerous machine learning, deep-learning algorithms, and data processing elements to generate new insight and, in some cases, make projections and provide useful warnings of impending hazards and situations. Various types of technologies of the processing layer include wired, wireless, and satellite technologies, as well as cloud and other third-party computational systems [37].

4.4. Application Layer

The application layer is the top layer of the IoT architecture that is responsible for providing personalised services according to the relevant needs of the end-users [47]. The application layer acts as an interface between third-party applications. The layer serves as the primary link between the users and the applications. The layer receives the data sent through the network layer and uses it to perform the necessary activities or services that the customer needs. The layer is involved in decoding patterns in the IoT data and computing them into summarised patterns that are easily understandable by the users in the form of graphs, tables, and pictorial displays.

5. Safety and Security Issues across IoT Layered Architecture

The IoT system architecture comprises various layers. Remarkably, there are a range of safety and security issues associated with each of these layers. A systematic survey of these safety and security studies gathered from various existing research is provided in this section. A summary of the notable safety and security issues across the IoT layered architecture is depicted below in **Figure 2** [5][27][42][47][48].

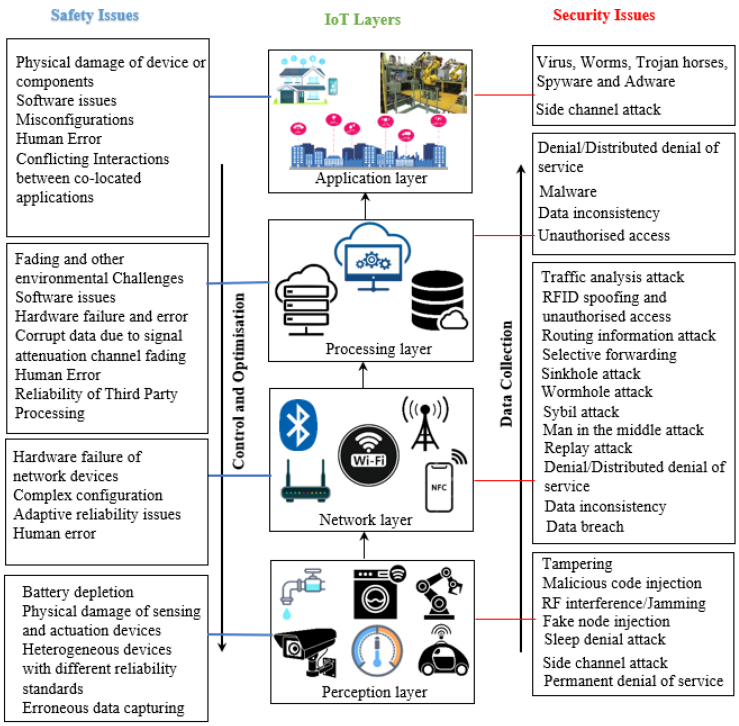

Figure 2. Safety and security issues across IoT layers.

5.1. Safety and Security Issues in the Perception Layer

The smooth operation of IoT systems demands that security and safety issues associated with the perception layer enabling technologies must be well taken into account. There are numerous security attacks associated with the perception layer. Notably, denial/distributed denial of service (DoS/DDoS), malicious code injection, false data injection, eavesdropping/interference, jamming, sleep deprivations, booting attacks, and side-channel attacks are some common examples of security threats associated with the perception layer [47]. On the other hand, regarding safety issues, there is a risk of hardware failure of large networks in some circumstances. Additionally, the heterogeneity of devices that have different flexibility on many occasions and are manufactured with different standards, failures, and reliability behaviours [49] poses a safety risk. Furthermore, the resource-constrained nature of IoT systems often tends to affect some design considerations, especially those which could have enhanced the system's safety [2]. This challenge is affecting the safety consideration of the systems. Additionally, depending on the application domain, IoT applications can be deployed in harsh operating and unattended environments. This constraint makes the perception layer technologies more prone to failures, which has negative effects on the overall safety of the IoT system [2].

5.2. Safety and Security Issues in the Network Layer

The network layer in an IoT architecture is prone to security issues, such as intended malicious cyber attacks against the confidentiality, integrity, and availability of sensing or actuation data [3]. Notably, attacks such as phishing site access, man-in-the-middle attacks, selective forwarding, replay attacks, DoS/DDoSs, data transmission errors, data inconsistency, and routing attacks are most prevalent at this layer [47][50]. On the contrary, the safety issues are unintended environmental and climatic hazards, such as atmospheric fading, which could hinder the free flow of data communication in IoT systems [51]. Likewise, human error, unauthorised access, restricted computing resources shared by IoT systems, and the challenging operating circumstances of specific IoT applications pose constraints to their safety and reliability [2]. These issues could affect the efficient performance of the IoT system and, thus, could hinder the trustworthiness of the IoT applications.

5.3. Safety and Security Issues in the Processing Layer

The data processing layer is critical to providing reliable IoT applications. It is susceptible to threats that are capable of affecting the integrity and quality of data processing, among others. The safety challenges in the data processing layer

include but are not limited to third-party processing reliance, corrupt data due to noise, signal attenuation, and hardware failure. Some of the identified cyber-security attacks in the middle layer are SQL injection, signature wrapping, man-in-the-middle, cloud malware injection, and flooding attacks, among others [47].

5.4. Safety and Security Issues in the Application Layer

The most crucial requirement of the application layer in the IoT ecosystem is the ability to provide reliable services to meet the end-users' personal or business needs. The security issues in the application layer are sometimes specific to different applications [47]. In general, the major security issues in the application layer include malicious code injection, access control, service interruptions, data theft, snipping, and reprogram attacks [47]. Conversely, the safety challenges arising from this layer include the possibility of conflicting interactions among various co-located IoT applications, as well as human errors and the performance of the software aspect of the application [2][13]. For instance, the potential for conflicting interactions between two IoT applications, namely, the smart flood detection system and fire detection system in a smart home system, were illustrated in the literature [13]. This conflicting interaction could jeopardise safety, even while the two IoT applications are within their nominal behaviours. Therefore, beyond device failure and unintended cyber attacks as sources of hazards to the environment, the conflicting relationship of IoT systems also brings an emerging challenge to the safety of the IoT ecosystem.

6. Conclusion

IoT systems are emerging in a way that has never been seen before due to technological advancement in numerous engineering and computer science areas. According to the review, IoT systems' safety and security standards are crucial to this advancement. An effort to address safety and security issues in the IoT domain will contribute to state-of-the-art development in the IoT ecosystem. Thus, research in this direction will serve as a pivotal driver to manage and reduce adverse events and avoid impact on Health Safety and Environment (HSE) while maintaining a productive process in compliance with local and global regulations. Thus, this will support the rapid pace of the design of IoT-enabled applications, which requires a high level of safety and security thresholds.

References

1. Dawid, H.; Decker, R.; Hermann, T.; Jahnke, H.; Klat, W.; König, R.; Stummer, C. Management science in the era of smart consumer products: Challenges and research perspectives. Cent. Eur. J. Oper. Res. 2017, 25, 203–230.
2. Xing, L. Reliability in Internet of Things: Current status and future perspectives. IEEE Internet Things J. 2020, 7, 6704–6721.
3. Frühwirth, T.; Krammer, L.; Kastner, W. Dependability demands and state of the art in the internet of things. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–4.
4. Kabir, S. Internet of things and safety assurance of cooperative cyber-physical systems: Opportunities and challenges. IEEE Internet Things Mag. 2021, 4, 74–78.
5. Abdulhamid, A.; Kabir, S.; Ghafir, I.; Lei, C. Dependability of The Internet of Things: Current Status and Challenges. In Proceedings of the 2nd International Conference on Electrical, Computer, Communications and Mechatronics Engineering, Malé, Maldives, 16–18 November 2022; pp. 2532–2537.
6. Kriaa, S.; Bouissou, M.; Colin, F.; Halgand, Y.; Pietre-Cambacedes, L. Safety and security interactions modeling using the BDMP formalism: Case study of a pipeline. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Florence, Italy, 10–12 September 2014; pp. 326–341.
7. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 2015, 139, 156–178.
8. Kumar, R.; Stoelinga, M. Quantitative security and safety analysis with attack-fault trees. In Proceedings of the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 12–14 January 2017; pp. 25–32.
9. Bakirtzis, G.; Carter, B.T.; Elks, C.R.; Fleming, C.H. A model-based approach to security analysis for cyber-physical systems. In Proceedings of the 2018 Annual IEEE International Systems conference (SysCon), Vancouver, BC, Canada, 23–26 April 2018; pp. 1–8.
10. Sasaki, R. A Risk Assessment Method for IoT Systems Using Maintainability, Safety, and Security Matrixes. In Information Science and Applications; Springer: Singapore, 2020; Volume 621, pp. 363–374.

11. Brunner, M.; Huber, M.; Sauerwein, C.; Breu, R. Towards an integrated model for safety and security requirements of cyber-physical systems. In Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Prague, Czech Republic, 25–29 July 2017; pp. 334–340.
12. Cerf, V.G.; Ryan, P.S.; Senges, M.; Whitt, R.S. Iot safety and security as shared responsibility. Bus. Inform. 2016, 1, 7–19.
13. Kabir, S.; Gope, P.; Mohanty, S.P. A Security-enabled Safety Assurance Framework for IoT-based Smart Homes. IEEE Trans. Ind. Appl. 2022, 59, 6–14.
14. Nguyen, D.T.; Song, C.; Qian, Z.; Krishnamurthy, S.V.; Colbert, E.J.; McDaniel, P. IotSan: Fortifying the safety of IoT systems. In Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies, Heraklion, Greece, 4–7 December 2018; pp. 191–203.
15. Aven, T. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab. Eng. Syst. Saf. 2007, 92, 745–754.
16. Nicol, D.M.; Sanders, W.H.; Trivedi, K.S. Model-based evaluation: From dependability to security. IEEE Trans. Dependable Secur. Comput. 2004, 1, 48–65.
17. Mahak, M.; Singh, Y. Threat Modelling and Risk Assessment in Internet of Things: A Review. In Proceedings of the Second International Conference on Computing, Communications, and Cyber-Security, Delhi, India, 3–4 October 2020; pp. 293–305.
18. Kabir, S. An overview of fault tree analysis and its application in model based dependability analysis. Expert Syst. Appl. 2017, 77, 114–135.
19. Asif, W.; Ray, I.G.; Rajarajan, M. An attack tree based risk evaluation approach for the internet of things. In Proceedings of the 8th International Conference on the Internet of Things, Santa Barbara, CA, USA, 15–18 October 2018; pp. 1–8.
20. Gao, X.; Shang, T.; Li, D.; Liu, J. Quantitative Risk Assessment of Threats on SCADA Systems Using Attack Countermeasure Tree. In Proceedings of the 2022 19th Annual International Conference on Privacy, Security & Trust (PST), Fredericton, NB, Canada, 22–24 August 2022; pp. 1–5.
21. Neha; Maurya, A. Cyber Attack Modeling Recent Approaches: A Review. In Proceedings of the Third International Conference on Computing, Communications, and Cyber-Security, Virtual, 26–28 May 2023; pp. 871–882.
22. Anand, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Ghafoor, K.Z. IVQFIoT: An intelligent vulnerability quantification framework for scoring internet of things vulnerabilities. Expert Syst. 2022, 39, e12829.
23. Wang, H.; Zhong, D.; Zhao, T.; Ren, F. Integrating model checking with SysML in complex system safety analysis. IEEE Access 2019, 7, 16561–16571.
24. Stewart, D.; Liu, J.J.; Cofer, D.; Heimdahl, M.; Whalen, M.W.; Peterson, M. AADL-Based safety analysis using formal methods applied to aircraft digital systems. Reliab. Eng. Syst. Saf. 2021, 213, 107649.
25. Lemaire, L.; Lapon, J.; Decker, B.D.; Naessens, V. A SysML extension for security analysis of industrial control systems. In Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research. BCS Learning & Development, St. Pölten, Austria, 11–12 September 2014; pp. 1–9.
26. Ahamad, S.; Gupta, R. Performability modeling of safety-critical systems through AADL. Int. J. Inf. Technol. 2022, 14, 1–14.
27. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481.
28. Kabir, S.; Sorokos, I.; Aslansefat, K.; Papadopoulos, Y.; Gheraibia, Y.; Reich, J.; Saimler, M.; Wei, R. A runtime safety analysis concept for open adaptive systems. In Proceedings of the International Symposium on Model-Based Safety and Assessment, Thessaloniki, Greece, 16–18 October 2019; pp. 332–346.
29. Nordmann, A.; Munk, P. Lessons learned from model-based safety assessment with SysML and component fault trees. In Proceedings of the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems, Copenhagen, Denmark, 14–19 October 2018; pp. 134–143.
30. de Andrade Melani, A.H.; de Souza, G.F.M. Obtaining fault trees through sysml diagrams: A mbse approach for reliability analysis. In Proceedings of the 2020 Annual Reliability and Maintainability Symposium (RAMS), Palm Springs, CA, USA, 27–30 January 2020; pp. 1–5.
31. Papadopoulos, Y.; Walker, M.; Parker, D.; Rüde, E.; Hamann, R.; Uhlig, A.; Grätz, U.; Lien, R. Engineering failure analysis and design optimisation with HiP-HOPS. Eng. Fail. Anal. 2011, 18, 590–608.

32. Kabir, S.; Walker, M.; Papadopoulos, Y. Dynamic system safety analysis in HiP-HOPS with Petri nets and Bayesian networks. Saf. Sci. 2018, 105, 55–70.
33. Thiagarajan, H. Supporting Model Based Safety and Security Assessment of High Assurance Systems. Ph.D. Thesis, Department of Computer Science, Kansas State University, Manhattan, KS, USA, 2022.
34. Whiting, D.; Sorokos, I.; Papadopoulos, Y.; Regan, G.; O'Carroll, E. Automated model-based attack tree analysis using HiP-HOPS. In Proceedings of the International Symposium on Model-Based Safety and Assessment, Thessaloniki, Greece, 16–18 October 2019; pp. 255–269.
35. Mian, Z.; Bottaci, L.; Papadopoulos, Y.; Biehl, M. System dependability modelling and analysis using AADL and HiP-HOPS. IFAC Proc. Vol. 2012, 45, 1647–1652.
36. Abdulhamid, A.; Kabir, S.; Ghafir, I.; Lei, Ci.; An Overview of Safety and Security Analysis Frameworks for the Internet of Things. *Electronics* **2023**, *12(14)*, 3086, .
37. Musa, A.A.; Hussaini, A.; Liao, W.; Liang, F.; Yu, W. Deep Neural Networks for Spatial-Temporal Cyber-Physical Systems: A Survey. Future Internet 2023, 15, 199.
38. Guzman, N.H.C.; Kozine, I.; Lundteigen, M.A. An integrated safety and security analysis for cyber-physical harm scenarios. Saf. Sci. 2021, 144, 105458.
39. Bisenius, B. Product safety of the internet of things . IEEE Consum. Electron. Mag. 2017, 6, 137–139.
40. Stoelinga, M.; Kolb, C.; Nicoletti, S.M.; Budde, C.E.; Hahn, E.M. The Marriage Between Safety and Cybersecurity: Still Practicing. In Proceedings of the International Symposium on Model Checking Software, Virtual, 12 July 2021; pp. 3–21.
41. Lefoane, M.; Ghafir, I.; Kabir, S.; Awan, I.U. Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks. IEEE Trans. Ind. Inform. 2022, 19, 921–929.
42. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 3, pp. 648–651.
43. Tiwary, A.; Mahato, M.; Chidar, A.; Chandrol, M.K.; Shrivastava, M.; Tripathi, M. Internet of Things (IoT): Research, architectures and applications. Int. J. Future Revolut. Comput. Sci. Commun. Eng. 2018, 4, 23–27.
44. Kakkar, L.; Gupta, D.; Saxena, S.; Tanwar, S. IoT architectures and its security: A review. In Proceedings of the Second International Conference on Information Management and Machine Intelligence, Jaipur, India, 24–25 July 2020; pp. 87–94.
45. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. 2017, 4, 1125–1142.
46. Rayes, A.; Salam, S. The things in iot: Sensors and actuators. In Internet of Things From Hype to Reality; Springer: Cham, Switzerland, 2022; pp. 63–82.
47. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access 2019, 7, 82721–82743.
48. Aswale, P.; Shukla, A.; Bharati, P.; Bharambe, S.; Palve, S. An overview of internet of things: Architecture, protocols and challenges. Inf. Commun. Technol. Intell. Syst. 2019, 1, 299–308.
49. Djedouboum, A.C.; Abba Ari, A.A.; Gueroui, A.M.; Mohamadou, A.; Aliouat, Z. Big data collection in large-scale wireless sensor networks. Sensors 2018, 18, 4474.
50. Sontowski, S. Exploration and Detection of Denial-of-Service Attacks on Cyber-Physical Systems. Ph.D. Thesis, Tennessee Technological University, Cookeville, TN, USA, 2022.
51. Hussaini, A.; Qian, C.; Liao, W.; Yu, W. A Taxonomy of Security and Defense Mechanisms in Digital Twins-based Cyber-Physical Systems. In Proceedings of the 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Espoo, Finland, 22–25 August 2022; pp. 597–604.