

Review

An Overview of Safety and Security Analysis Frameworks for the Internet of Things

Alhassan Abdulhamid, Sohag Kabir *, Ibrahim Ghafir and Ci Lei

Department of Computer Science, University of Bradford, Bradford BD7 1DP, UK; a.abdulhamid2@bradford.ac.uk (A.A.); i.ghafir@bradford.ac.uk (I.G.); c.lei1@bradford.ac.uk (C.L.)
* Correspondence: s.kabir2@bradford.ac.uk; Tel.: +44-1274-232212

Abstract: The rapid progress of the Internet of Things (IoT) has continued to offer humanity numerous benefits, including many security and safety-critical applications. However, unlocking the full potential of IoT applications, especially in high-consequence domains, requires the assurance that IoT devices will not constitute risk hazards to the users or the environment. To design safe, secure, and reliable IoT systems, numerous frameworks have been proposed to analyse the safety and security, among other properties. This paper reviews some of the prominent classical and model-based system engineering (MBSE) approaches for IoT systems' safety and security analysis. The review established that most analysis frameworks are based on classical manual approaches, which independently evaluate the two properties. The manual frameworks tend to inherit the natural limitations of informal system modelling, such as human error, a cumbersome processes, time consumption, and a lack of support for reusability. Model-based approaches have been incorporated into the safety and security analysis process to simplify the analysis process and improve the system design's efficiency and manageability. Conversely, the existing MBSE safety and security analysis approaches in the IoT environment are still in their infancy. The limited number of proposed MBSE approaches have only considered limited and simple scenarios, which are yet to adequately evaluate the complex interactions between the two properties in the IoT domain. The findings of this survey are that the existing methods have not adequately addressed the analysis of safety/security interdependencies, detailed cyber security quantification analysis, and the unified treatment of safety and security properties. The existing classical and MBSE frameworks' limitations obviously create gaps for a meaningful assessment of IoT dependability. To address some of the gaps, we proposed a possible research direction for developing a novel MBSE approach for the IoT domain's safety and security coanalysis framework.

Keywords: Internet of Things; safety; security; analysis frameworks; model-based system engineering; safety and security coanalysis



Citation: Abdulhamid, A.; Kabir, S.; Ghafir, I.; Lei, C. An Overview of Safety and Security Analysis Frameworks for the Internet of Things. *Electronics* **2023**, *12*, 3086. <https://doi.org/10.3390/electronics12143086>

Academic Editors: Irfan Awan, Amna Qureshi and Muhammad Shahwaiz Afaqui

Received: 21 June 2023
Revised: 12 July 2023
Accepted: 13 July 2023
Published: 16 July 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

As the vision of an internet-centric and things-centric world for the near future has been progressively unfolding, numerous IoT applications across many domains have hitherto made successful market entries, or some of their prototypes have already been implemented [1]. This technological development underpins the projection that the IoT innovations will add about \$5.5 trillion to \$12.6 trillion in value to the global economy by 2030 [2]. Notably, some of the areas of modern life that have already witnessed the application of the IoT include smart homes and cities [3–5], Industrial IoT (IIoT) [6,7], smart agriculture [3,8], intelligent medicine [8–11], smart transportation and autonomous vehicles [3,4,12], and wearable fitness [4,8,10] among others.

The IoT innovation has transformed traditional electronics and mechatronics systems across many fields into smart and intelligent systems by integrating intelligence-driven applications into them. This technological progress has facilitated a seamless integration of

the sensing, processing, communication, reasoning, and actuation capabilities of modern systems [1]. The IoT has ushered humanity into a technological paradigm, which has created a more efficient, intelligent, and convenient environment [13]. 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 [14]. 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 [15]. 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 [14,16]. While system dependability deals with the system performing at its optimal functionality over a specified period [14], safety attributes entail that devices are devoid of harm to their users or damage to the environment [17–19]. Similarly, a system's security attributes concerns how it performs its intended functions and mission despite the risk posed by security threats [20–22]. 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 [23].

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 [5,16,24]. 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 [24].

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 [14,25–28]. 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 [29–32]. On the other hand, to meet the continuous requirements of systems development, some of the safety-critical domains, such as the automobile [33] and aerospace industries [34], as well as industrial control systems [35], have begun to explore the option of MBSE approaches. Notably, MBSE approaches have been used to analyse the various NFPs of system design, such as performance [36,37], safety [38–42], reliability [40,42], and security properties [43–45]. In the model-driven development paradigm, some of the

classical analysable models such as FTA, AT, Petri nets, and other artefacts are fully or semiautomatically generated using software-based approaches. These approaches generate the 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) [35,39], the Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS) [41,42,44,45], and the Architecture Analysis and Design Language (AADL) [34,36,45].

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 [46]. In the IoT environment, safety and security requirements are becoming increasingly interwoven, and the systems are increasingly given autonomous, adaptive, and evolving features [16]. 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. This research effort will support the actualisation of the IoT 2030 vision for tremendous global value addition to the international economy. The motivation of this review is to evaluate the safety and security requirements of IoT applications, as well as the existing analysis frameworks. Finally, based on our findings, we suggest future research trends for developing a trustworthy model-based safety and security analysis framework in the IoT domain. Specifically, the notable contributions of this article are summarised as follows:

- The performance of a review of salient issues surrounding the safety and security requirements of IoT systems.
- The provision of an overview and comparison of popular classical and MBSE approaches used for safety and security analysis and the discussion of their effectiveness in evaluating the dependability of IoT systems.
- The suggestion for future research directions in developing a viable dependability analysis framework for a unified treatment of safety and security requirements in the IoT environment.

After this brief introduction, the following section provides a conceptual overview of the IoT system dependability by critically examining safety and security attributes and their relationship. Next, Section 3 discusses the safety and security requirements of the IoT systems by evaluating the critical requirements of the two properties across the IoT architecture. Furthermore, Section 4 deals with the related works that have been conducted in areas of safety and security analysis frameworks. Finally, Section 5 is a discussion of the survey and offers further insight into future research directions, and Section 6 concludes the paper.

2. Background and Literature

This section describes some of the fundamental concepts that underpin our review. Dependability is the umbrella term that encompasses safety and security as its attributes. Accordingly, dependability, as well as safety and security attributes and their relationship, will be highlighted. Our aim in this section is not to be comprehensive, but rather to give a broad conceptual overview that will be used in the subsequent sections.

2.1. Dependability of the IoT System

Dependability is a broad term that deals relatively with the trustworthiness of a system to operate as expected. Conceptually, dependability is the ability of a system to reliably deliver the service it was designed to provide despite faults, failures, and errors [16]. Accordingly, a dependable system has been characterised as a system that can avoid failures

that are more frequent and severe than acceptable so that it can provide services that can justifiably be trusted [14,28,47]. Dependability attributes comprise safety, reliability, maintainability, and security properties (availability, confidentiality, and integrity) [16,28,47,48]. Although the IoT has remained a promising networking paradigm, it has to confront several dependability issues, due to a large number of different interconnected objects [49]. While this survey intends to dwell on only IoT dependability's safety and security attributes, some of the previous research on the IoT dependability have been covered in [14,16].

2.2. IoT Safety Attribute

Safety plays a vital role in internet-enabled systems. Primarily, safety failures of the IoT system or its components may result in risks to the users, the environment, reputation, and financial losses to the stakeholders in the technology [50]. Broadly, the safety of a system has to do with the freedom from unacceptable risks or damage due to malfunctioning behaviours of the technological systems [20,28]. Safety relates to ensuring that the device does not cause harm to its users or damage the environment [17]. Safety violations usually occur due to failures of the hardware, software faults, or errors that could be activated by hazards [28,51]. However, in the safety-critical domains, safety violations could result in hazardous situations that are capable of negatively impacting the environment and the users. For instance, autonomous vehicles could cause an accident due to a software malfunction; wearable medical devices could cause harm to a patient due to the malfunction of biosensors, and thermostat failure could cause overheating in smart homes [16,17,28]. The safety of IoT systems must therefore consider all issues that can cause the systems to enter an unsafe physical state. The safe use of IoT systems depends on the reliable operations of the system in its nominal behaviour, the safe management of un-intentional random hardware failures, malevolent threats against the system, systematic software, and hardware failures, as well as bad interactions among colocated IoT applications, operators' errors, and environmental changes [5,16,17].

2.3. IoT Security Attribute

Security is a crucial requirement in most of the embedded systems. Security problems have been acknowledged to be one of the most researched areas of IoT design due to its relevance in the design of dependable IoT solutions [17,52]. Broadly, security is one of the NFPs that deals with the system performing its intended functions and mission despite the risk posed by threats [7]. The security attributes of a dependable system are discussed based on security triads, including confidentiality, integrity, and availability (CIA) [47]. Confidentiality is the ability to protect data against unauthorised users and processes. In contrast, integrity is the ability to protect data from improper system modification over the entire system life cycle [48]. Similarly, availability is the system's ability to deliver services when requested, which technically describes the uptime and downtime of a system [14]. Various cyber-security threats are premeditated to compromise the system's CIA and eventually undermine the IoT system's dependability. For instance, critical IoT data can be altered, unauthorised access can be obtained, or the availability can be hampered through attacks such as spoofing (masquerading), traffic analysis attacks, malicious code injection, side-channel attacks, telnet attacks, and denial of service/distributed denial of service (DoS/DDoS), among others [37,53–55]. Some of these threats are significantly unpredictable, as various malicious agents can exploit several vulnerabilities before compromising a prized asset within the heterogeneous system, especially in IoT systems. To develop dependable IoT-Driven applications, the security attribute of the system must be well considered from the design stage of a system [26,56]. This effort is necessary to ensure that the systems are guarded against the exploitation of intended malicious agents from compromising the system's CIA and other security attributes [57].

2.4. Relationship between IoT Safety and Security Analysis

Historically, various research projects in safety and security have been conducted independently by separate communities, each with unique mindsets, approaches, and standards [20,58]. Safety analysis is more pronounced in traditional safety-critical domains, such as automotive, aviation, and industrial control designs, where safety considerations are given a higher premium. In the safety analysis, the likelihood, causes, and severity of a potential system element's fault or error are evaluated at the design stage using the reliability data of various components based on their configuration in the system [16,17]. Based on the outcome of the safety analysis, necessary amendments are made in terms of the components' specifications or system configuration to meet a defined threshold of safety standards.

Contrarily, the security attributes of systems such as the CIA of data and processes are more considered in the computing and CPS domain, where internet connections are applicable. In these domains, cyber-security threats are premeditated to compromise the system's CIA and eventually undermine the IoT system's dependability [7]. Accordingly, the security analysis is conducted from the viewpoint of intentional threats that are orchestrated for malicious purposes to exploit the system's vulnerabilities, thereby leading to breaches. Thus, security analysis identifies threats regarding potential attack steps, the possibility of exploitation of an information system, and the potential impacts on a system's operations. Therefore, the difference between the two analysis perspectives is that the security property of a system is more subjective and dynamic, which cannot be easily evaluated at the design stage based on established data such as system safety [17,20,59]. However, the evolving nature of system design and ubiquitous computing systems in almost every domain of today's innovations have created interactions between the safety and security properties in most of the aforementioned safety-critical domains. The interaction of computational components, which are internet-enabled, with the physical hardware components creates a nexus where security issues can influence the safety considerations of the systems and vice versa. For instance, cyber attacks against IoT systems can cause negative consequences in the physical world and, thus, compromise the safety of the user and the environment. In this regard, several studies have attested that, despite the differences and dichotomies between the safety and security properties, they still share several commonalities, interdependence, and relationships, which make them closely intertwined for a viable analysis of many systems, including the IoT [18–20,23,58–60].

Some existing studies have identified the safety and security relationship in terms of their interdependence. Based on the literature, safety and security share four types of interactions: conditional dependency, mutual reinforcement, antagonistic relationship, and independent relationship [12,20,58]. In conditional dependence, safety and security requirements are required and necessitate one another. In the case of mutual reinforcement relationships, safety requirements enhance the security of the system and vice-versa. Conversely, the two properties conflict in the antagonistic relationship. Lastly, no interaction between safety and security properties occurs in the case of an independent relationship. A high-level overview of the interdependence between safety and security properties and the impact of their coanalysis is illustrated in Figure 1.

Exploring the interplay between security and safety in IoT dependability is imperative for guaranteeing the safe operations of IoT innovations. Based on the established relationship, the dependency and interactivity between safety and security in the IoT domain, new risks could emanate if the two properties continue to be evaluated independently. Therefore, the assurance of dependability of the IoT applications will be highly dependent on efficient frameworks that rigorously coanalyse safety and security relationships in IoT systems. Accordingly, there is a need for a common framework to evaluate the crossfertilisation of the two properties and develop an integrated approach for their analysis. Research efforts in this direction will translate into more cost-effective design, reduce delays in independent analysis, and assist in developing more viable, safe, secure, and dependable IoT systems. This will eventually assist the systems' developers in developing reliable, generally more trusted systems that support the expected certification standards.

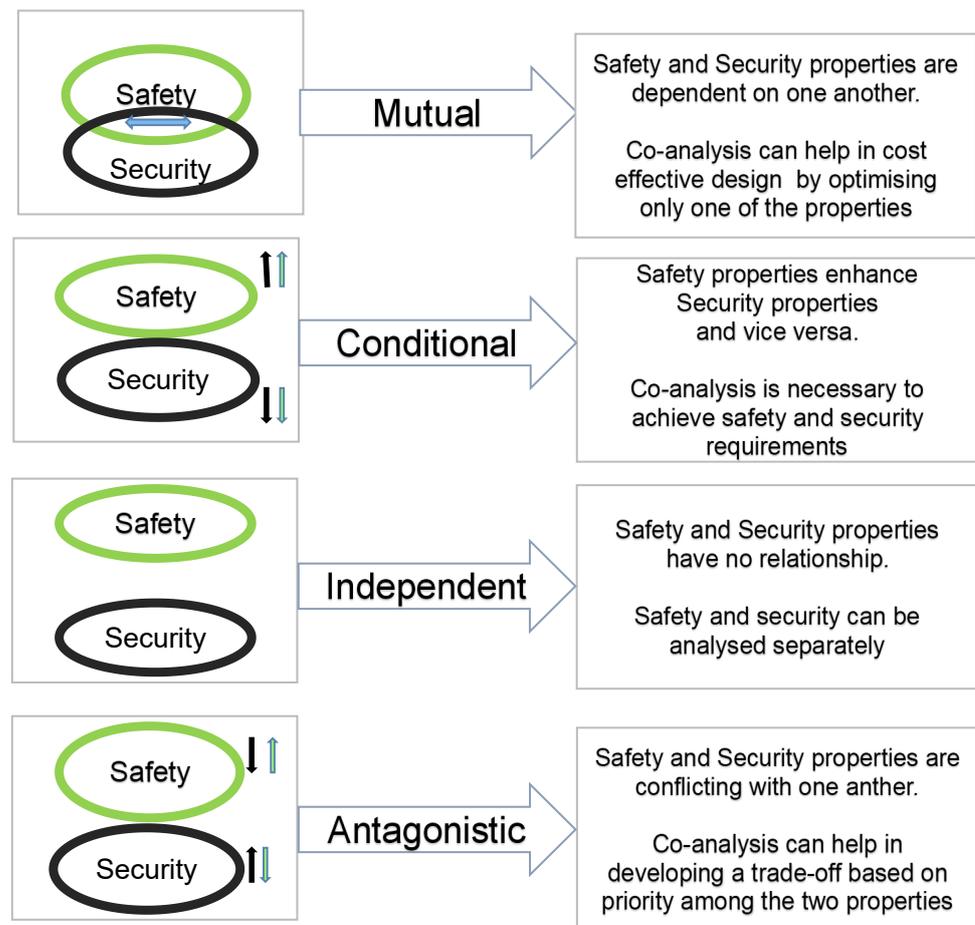


Figure 1. Safety and security relationship.

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 [61]. 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 pervaded 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 [5]. 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 [21,62]. 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 [51]. 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 [5].

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 [55,63].

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 [5,14]. 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 [17,55]. 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 [5]. 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.

3.1. The IoT Model

A generic IoT system is represented using a layer architectural framework that uses various standards and layer structures [13]. Some of the most common frameworks are three-layer, four-layer, and five-layer architectures [3,13,64,65]. Accordingly, a four-layered IoT architecture is considered in this survey. Figure 2 presents the IoT four-layer architecture. The layers are the perception, network, processing, and application layer.

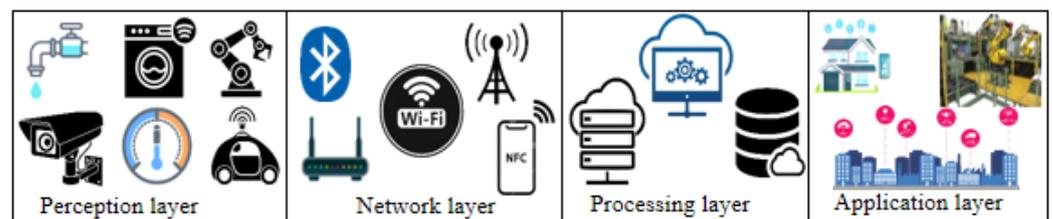


Figure 2. IoT Four-Layer architecture.

3.1.1. 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 a high reliability, an ease of use, a higher resolution, a high sensitivity, smart detection, and minimum power consumption, among others [66]. At this layer, various sensor nodes perform sensing measurements of the environment and other physical parameters [13,66]. The 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.

3.1.2. 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 [13,63,67]. The network layer conveys data across interfaces and gateways using communication technologies and protocols, especially the internet protocol [63]. This layer of the IoT architecture sets the rules for data aggregation. The network layer integrates devices, such as hubs, switches, gateways, as well as communication technologies such as Bluetooth, Wi-Fi, and Long-Term Evolution (LTE) [13].

3.1.3. 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 the IoT data [3,13,64,67].

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 is a bridge between the application and network layer, which is responsible for data accumulation, abstraction, and analysis [67,68]. Data processing is carried out via cloud computing and multiparty computation, where mass data processing and intelligent processing are conducted [63]. 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 [46].

3.1.4. 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 [67]. 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.

3.2. Safety and Security Issues across IoT Layered Architecture

As discussed in Section 3.1, 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 3 [16,37,63,67,68].

3.2.1. 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 [67]. On the other hand, regarding safety issues, there is the 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 [69] 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 [13]. 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 have negative effects on the overall safety of the IoT system [13].

3.2.2. 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 [14]. Notably, attacks such as phishing site access, man-in-the-middle attacks, selective forwarding, replay attacks, DoS/DDoS, data transmission errors, data inconsistency, and routing attacks are most prevalent at this layer [67,70]. 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 [50]. 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 [13]. These issues could affect the efficient performance of the IoT system and, thus, could hinder the trustworthiness of the IoT applications.

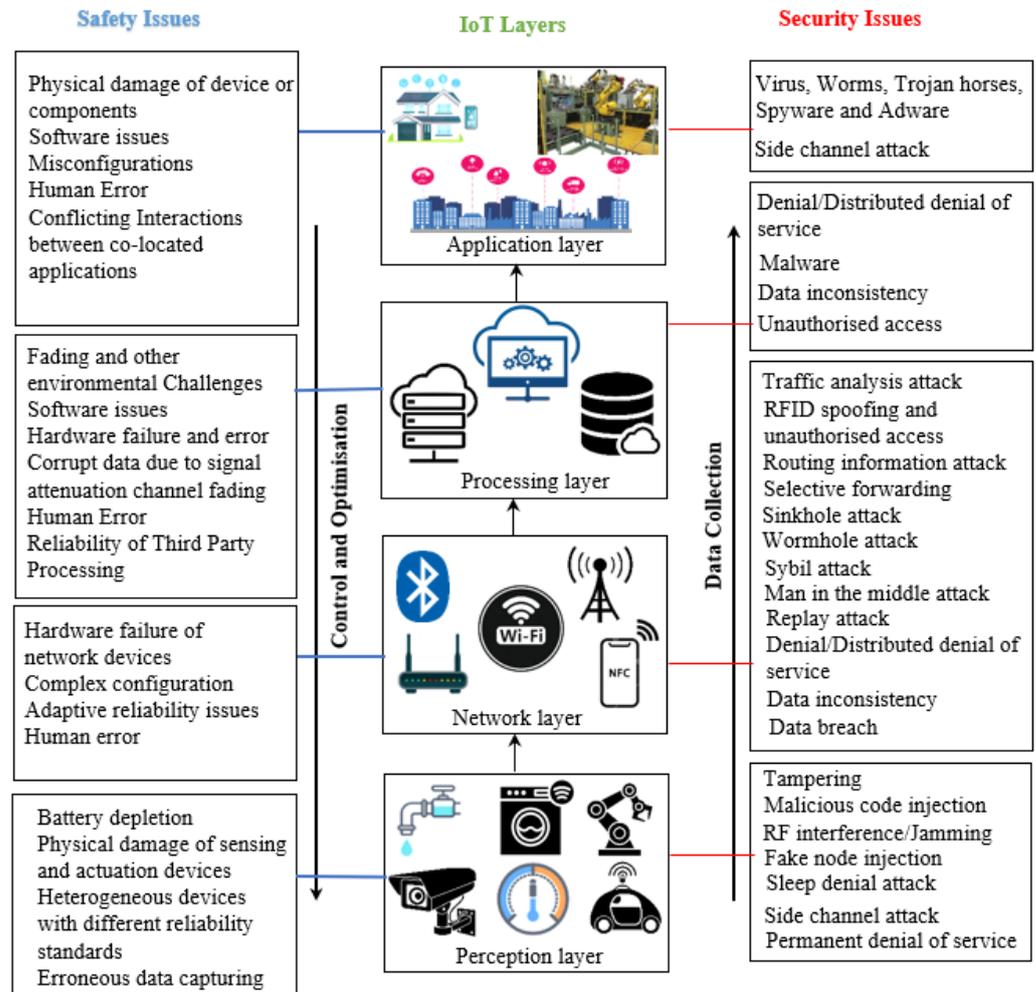


Figure 3. Safety and security issues across IoT layers.

3.2.3. 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 [67].

3.2.4. 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 [67]. In general, the major security issues of the application layer include malicious code injection, access control, service interruptions, data theft, sniffing, and reprogram attacks [67]. Conversely, the safety challenges arising from this layer include the possibility of conflicting interactions among various colocated IoT applications, as well as human errors and the

performance of the software aspect of the application [5,13]. For instance, the potential for conflicting the 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 [5]. 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.

4. Safety and Security Analysis Frameworks and Related Work

This section reviews notable analysable models for safety and security analysis across various domains. Basically, these analysis models are grouped as classical safety and security analysis approaches, unified safety and security analysis approaches, and MBSE approaches. Based on these frameworks, some of the recent surveys conducted in both safety and security domains will also be highlighted.

4.1. Classical Safety Analysis Methods

There are numerous approaches used for the safety and security evaluation of systems. In the safety domain, some of the most common and widely used approaches are FTA, FMEA, the Reliability Block Diagram (RBD), Event Tree Analysis (ETA), and the Markov Chain (MC), among others. Some of the prominent safety analysis approaches in the various literature are described as follows.

4.1.1. Fault Tree Analysis

The FTA is one of the most widely used approaches for evaluating systems' safety and reliability in different domains, including the IoT [71,72]. Bell Phone Laboratories developed the approach in 1962 [73]. The FTA is a deductive approach that quantifies and evaluates the combination of basic component failures that can lead to a top event (critical events that can cause the overall system failure upon its occurrence). The tree starts with the system's undesired state, represented as the top event, and deductively identifies all the possible paths leading to this undesired state. A graphical illustration of the FT diagram is shown in Figure 4.

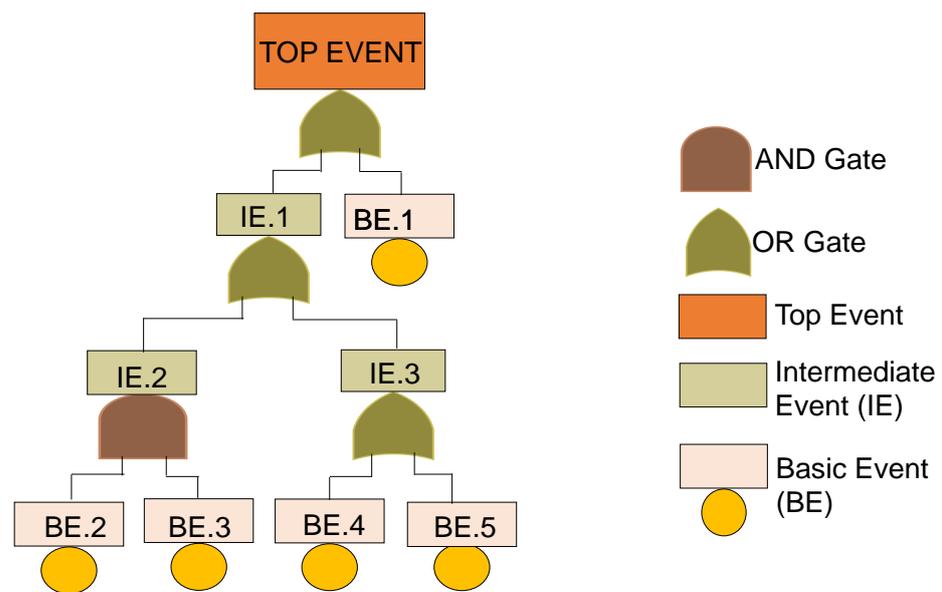


Figure 4. Fault Tree framework.

The main cause of a system failure is the top event in the FT structure. The preceding branches and leaves of the tree are represented as the intermediate and basic events, respectively. The basic faults, which are represented as basic events in the tree, are linked

together by Boolean logic gates, such as *AND* and *OR* gates, based on how the subsequent events can cause the occurrence of proceeding events in the tree [29].

The relevance of the FT to the safety analysis of IoT systems is in the expressiveness of the technique for both qualitative and quantitative analyses. These two analyses, which are possible via the FT framework, can help design engineers ascertain the safety of a proposed system and ensure that a minimum safety threshold is achieved to guarantee the safe use of the system and also meet the certification standards of various IoT design innovations. The qualitative analysis helps establish the minimal cut sets, which represent all the basic events for the top event. On the other hand, the quantitative analysis provides probabilistic assessments of the system's safety based on the failure probability of the basic events (components). These two analyses support the iterative system design, where configuration modification or a change in the proposed components can be suggested based on safety considerations.

In the existing literature, various extensions and modifications of the FTA have been developed over the years. These extensions involve the addition of other gates to depict different fault behaviours and operating states of the systems. Notable extensions include the Dynamic FT, Component FT, Pandora Temporal FT, and State/Events FT [28,74–76]. The FTA framework has been used extensively across various safety-critical domains for safety analysis. In the IoT domain, the FTA framework was used in the safety analysis of smart homes [71], smart grid system [77], smart aquaculture [78] and CPS, in general [46,79]. Although the studies of IoT safety design evaluation using FTA are in progress, the manual process of the approach still needs to be improved. This has been characterised as time-consuming and being performed based on cumbersome informal system models that are subject to human errors, thereby leading to inconsistency or incompleteness [28,75]. Another limitation of the FTA framework is that its combinatorial approach is mostly represented using the Boolean gates 'AND' and 'OR'. Some of the modifications, such as the Dynamic Fault Tree [80] and Pandora Temporal FT [81,82], have added such gates as the functional dependency ('FDEP'), priority AND ('PAND') gate, and a host of others to represent the various dynamic behaviours of modern system [28,75,83]. Nevertheless, despite the relevance of the FT as one of the famous safety analysis approaches, its manual nature has left much to be desired in the analysis of IoT systems [16]. Additionally, the basic events in the tree are assumed to be statistically independent, which, in some dynamic IoT system configurations, may not be the case [28]. These challenges suggest further research into IoT safety.

4.1.2. Failure Mode Effect Analysis

The Failure Mode Effect and Criticality Analysis (FMECA) approach is a classical inductive safety assessment framework developed by the US military in 1980 to systematically identify potential failures in a system in addition to their causes and effects [28]. Unlike FTA, in the FMECA framework, the process starts from the root causes of the failure (basic component failure) and proceeds bottom-up to establish the undesired event or events (overall system failure). The FMEA framework is organised in a tabular form containing columns such as Function, Failure Mode, Cause, Effect, Severity, and Detection, among others. Systematically, the technique considers all the possible combinations of effects of a single component mode [84,85]. By using FMEA, system safety engineers can determine the effects of various components and the criticality of failure modes in a system. Similar to FTA, the FMEA approach is also a manual process that inherently has the disadvantages of reusability constraints, incorrectness, and an informal nature, among others.

4.1.3. Reliability Block Diagram

As with the FTA, the Reliability Block Diagram (RBD) is also a deductive and graphical safety analysis framework that is used to find the reliability of the overall system from the reliability of its constituent units. Using the RBD framework, safety, alongside other attributes such as reliability, availability, and maintainability, are modelled based on failure

relationships between the systems and components. The overall system is modelled into several blocks and connectors (lines), which denote system components and their configurations, respectively. The components are represented either in a series or in parallel configurations [86]. As the safety of a system can be deduced from the reliability of the components, the RBD gives the failure characteristics of a system based on the failure rate of the components parts that make the system and the design configuration of the system [86]. The relevance of the RBD in safety analysis is similar to FTA. System development can be analysed to evaluate the impact of component failures on overall system safety. Furthermore, it enables safety design optimisation and trade-offs based on the components' specifications and system configurations. However, the approach also suffers the manual-based limitations of the safety analysis process.

4.1.4. Markov Chain Analysis

The Markov Chain Analysis (MCA) framework is also an inductive safety analysis technique, which is based on stochastic models [87]. The MCA is based on mathematical modelling, wherein the failure states of a system are dependent only on the current state and time lapsed [88]. Despite MCA being stochastic in nature, the state of the systems is assumed to be memoryless, because the probability of future states is not dependent upon steps that led to the present states. The initial state and the probability represent the starting state and the transition probability from state to state, respectively. In MCA, a transition matrix is formed that correlates the past state and the next future state with constant failure and repair rates. Notably, in IoT-based systems, as with other electronic systems, the components fail at a constant rate that is effectively modelled by MCA. The two categories of MCA in the literature include Discrete Time Markov Chain Analysis (DTMCA) and Continuous Time Markov Chain Analysis (CTMCA). In the literature, the life cycle of a CPS was characterised on the basis of CTMCA and derived reliability metrics, therein deriving the mean time to failure (MTTF) of the system [87]. Unlike FTA or RBD, the MCA can be used in safety analysis to evaluate system failure or availability at any point along the system. Therefore, this is one of the advantages of MCA, which gives both the reliability and the availability of repairable components in a system.

4.2. Classical Security Analysis Frameworks

At the conceptual phase of the IoT design, systematic security analysis, validation, and verification are conducted by the security team to develop a robust and resilient system against security attacks [44]. Accordingly, various threat modelling frameworks were developed to identify, quantify, and address vulnerabilities and threats against the systems to handle the cyber-security challenges of IoT systems [52]. Based on the various threat models, some of these attributes, such as availability and reliability, are defined quantitatively, and their analyses are conducted accordingly [14,27,89]. The common security analysis frameworks in various studies include attack trees, attack–defence trees and quantitative attack–defence trees.

4.2.1. Attack Trees

The attack tree (AT) was developed by Schneier in 1999 to model threats against a system using a deductive tree-like structure similar to FTA [90]. The AT framework depicts various ways in which a system can be compromised by a malicious agent [90]. The approach decomposes the various possibilities for a system's attack in multi-level steps. The different ways to compromise a system are represented as the root, leaves, and children nodes. These nodes intuitively indicate various hierarchies of attacks against a system. The root node corresponds to an attacker's overall goal. The lower nodes in the tree represent the refinement of the root node's goals, which involves some basic actions to be executed by the attacker to achieve his main goal [31,91]. The dependencies between different nodes on the same level of the tree are modelled using Boolean 'AND' and 'OR' gates. In the 'AND' conditions, the attackers set goals, which must all be achieved to

compromise its parent node, whereas the ‘OR’ conditions could be achieved if any one of the goals is accomplished. Quantitatively, the overall security metrics of the system can be estimated from the values of the children nodes and their various Boolean logic conditions. Consider the example attack tree adapted from [92], which is illustrated in Figure 5. The tree deductively illustrates how cyber-security threats could be premeditated to compromise one of the system’s CIA triads and eventually undermine the IoT system’s dependability. Step by step, the framework establishes the steps needed to be followed by malicious agents to exploit several vulnerabilities before compromising the confidentiality of the IoT data. Furthermore, subjective quantitative metrics can be added to each step based on various known techniques, such as fuzzy logic and vulnerability quantification. This approach can assist security engineers in evaluating and prioritising security design to develop safe and dependable systems.

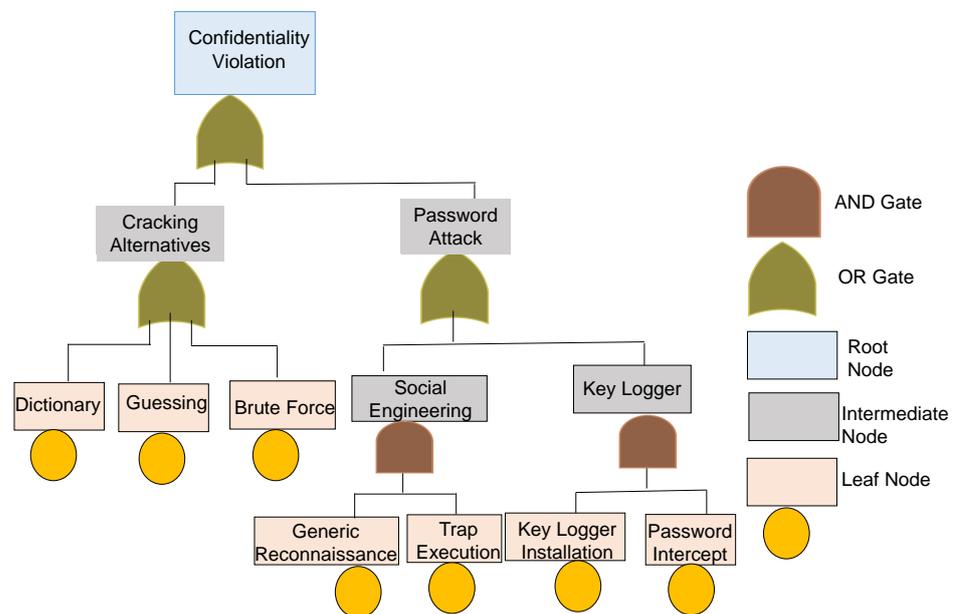


Figure 5. Example of attack tree.

Based on the AT framework, the necessary steps that malicious agents require to compromise the system can be developed. Accordingly, the framework will help determine where it is necessary to make design modifications and improvements to strengthen the system’s security. In general, the AT gives a clue as to the attack vector optimisation, which can help develop stronger built-in security mechanisms from the design abstraction stage of the system. In addition, through the various amendments of the AT approach, the quantitative analysis of potential attack scenarios can be conducted to evaluate the feasibility of a successful attack against a system. Insight into the likelihood of an attack, cost, and the impact of an attack can be ascertained. This useful information can help determine the low or high probability of attacks against a system, as well as the appropriate resources that can be channelled towards the countermeasures.

4.2.2. Attack–Defence Trees

Attack–Defence trees (ADT) involve a deductive node-labelled rooted tree, which extends the AT framework with defensive measures [90]. Basically, the framework models the security of a system using two types of nodes: the attack nodes and defence nodes. The attack nodes represent the measures an attacker might take to compromise the system, while the defence nodes are the actions defenders can employ to protect the system [63]. The unique features of ADT are, therefore, the representations of refinement and countermeasures. The basic nodes are the nonrefined nodes, which are similar to basic events in the FTA framework. In the ADT framework, the attack nodes are graphically represented

as circles, while the defence nodes are depicted as rounded rectangles. The refinement relationships are represented using the solid edges of trees, and countermeasures are represented by the dotted edges. The same refinement relationship using Boolean logic ‘AND’ and ‘OR’ conditions, as with AT, are used to systematically map the relationship between leaf nodes, intermediate nodes, and root nodes. The parent node attack is considered successful if at least one of its children’s conditions is true [93].

4.2.3. Quantitative Attack–Defence Trees

Quantitative attack–defence trees (QADT) entail a further refinement that was proposed to extend the qualitative description of ADT with quantitative metrics. Basically, some degree of quantitative information, such as the likelihood and impact of security impingement vis-a-vis the cost, skills, and benefits an attacker might derive from compromising a system, can be computed with some level of subjectivity. Some metrics for the quantification of the system vulnerability can be factored into quantitative ADT to enrich the validation of the subjective nature of cyber-security attacks [93]. In the IoT environment, attack risk attributes on attack–defence nodes were developed to quantitatively evaluate the risk of smart systems being attacked [94].

The various threat modelling frameworks discussed, including AT, ADT, and quantitative ADT approaches, contribute to the security analysis of dependable systems in general, including the IoT systems. Some of the studies conducted using the AT framework and its extensions in evaluating the IoT security vulnerabilities are found in [29,95,96]. In general, across the two domains, classic analysis frameworks tend to inherit one or more limitations, such as a manual nature, a state-based nature, a static nature, being time-consuming, being prone to errors, and lacking of reusability, which make them not the most viable option for the analysis of IoT-Based systems [16,42,44]. In areas of security analysis, the approaches only provide static analysis primarily using the Boolean logic conditions ‘AND’ and ‘OR’. Other dynamic conditions, such as dependencies between security attacks, sequencing, and the conditional characteristics of complex security environments, are yet to be captured. Additionally, unlike FTA, in which the reliability of the failure of the basic component event can be obtained from its design specification, security quantification, on the other hand, is subject to various subjective opinions. Furthermore, the threat modelling frameworks discussed are manual and informal analysis systems, which are inherently deficient due to the cumbersome nature of the manual process and their being subject to human errors. Accordingly, computerised model-based approaches are needed to describe the behaviour of the systems and the attack patterns in order to develop fully or semiautomatic frameworks. Efforts in this direction are ongoing in academia and in the industry. However, an integrated approach that brings new constructs to evaluate the coanalysis of safety and security in the IoT environment is yet to be established.

4.3. Unified Safety and Security Analysis Frameworks

Several studies have been conducted, and frameworks have been proposed for safety and security coanalysis. Notably, safety and security interactions were evaluated using Boolean Logic-Driven Markov Processes (BDMP) formalism through a case study of the hypothetical pipeline control system and emergency lock door [17]. The study demonstrated conflicting interactions between safety and security properties. However, the approach over-simplified these complex dependability interactions. For instance, the case study of the emergency door was used to depict conflicting interactions between safety and security. However, while this is a good illustration, it only looks at the physical security instead of the cyber-security properties of the system. In the case of the IoT systems with both physical components and cyber elements, thorough analyses of both components are essential.

Furthermore, a unified framework called the attack fault tree (AFT) was proposed in [17]. The approach attempts to unify safety and security properties by using the traditional reliability framework based on the fault tree analysis framework and the security formalism based on the attack tree analysis framework. The observed limitations of the ap-

proach are based on its manual nature and, at the same time, that it only gives a qualitative analysis. Similarly, Kumar et al. [19] developed the qualitative and quantitative analysis of the AFT using stochastic model-checking techniques. Nonetheless, no new construct was created to handle complex interactions, and the quantitative analysis was only for a few aspects of cyber-security properties. Alternatively, for instance, the authors could have achieved a critical analysis of the CIA properties and the reliability of the components parts. Similarly, an attack–defence tree framework was developed for the risk quantification of IoT-Based smart-grid systems [94]. The framework modelled the system and enabled the computation of the proposed risk attributes that assessed the system risks by propagating the risk attributes in the tree nodes. While the study captured security strategies concerning risk minimisation, the work can be extended to evaluate the safety attributes of the same IoT-Based safety-critical system. However, that is yet to be achieved.

The noncoherent fault tree approach was proposed for modelling safety and security coanalysis [97]. The authors considered stochastic safety events such as random component failures, human error, and intentional cyber-security events. As with coherent FTA, this approach deals with the modelling and quantification of top events. The authors used the binary decision diagram (BDD) approach to validate the approach. Nevertheless, the interactions and interdependencies between the two properties need to be adequately analysed to define the accurate dependability of the system. Similarly, attempts were made to integrate cyber attacks within fault trees as a framework [61,91,98]. The works qualitatively integrated attack trees into preexisting FTA structures, thereby increasing the framework’s usability to consider potential intentional attacks. In [98], the authors introduced a new concept of the macroattack tree, thereby allowing a multilayered view of the attack process. The integration followed conventional FTA methods, and the probability of a top event was computed when one or more events were outcomes of malicious attacks. However, the framework needed to address the quantitative analysis of the unification comprehensively. Furthermore, no new constructs were developed to evaluate the interactions of the properties. Similarly, the component fault trees approach was developed for security and safety coanalysis [99]. The authors extended the statistical FTA, wherein they focused on the system components and reusability to analyse safety and security qualitatively. However, an extension of their work to quantify the system’s dependability has yet to be achieved. Another related work has been presented recently by Stoelinga et al. [51], which discussed the significant challenges in unifying the safety and security properties. Some of the highlighted challenges include the complex interaction between safety and security, the lack of practical algorithms to compute system-level risk metrics, and the lack of proper risk quantification methods. A summary of a comparison of widely used manual approaches for safety and security analysis is presented in Table 1. In the table, QL and QT denote qualitative and quantitative, respectively. The approaches were compared in terms of their expressiveness of analysis, their capacity to evaluate qualitative and quantitative safety and security parameters, and their major weaknesses in adaptation to the IoT dependability analysis.

Table 1. Notable classical safety and security manual analysis approaches.

Framework	Studies	Analysis	QL and QT	Limitations
FTA	[29,71,77–79]	Static failure	Both	Static and manual-based
AT	[31,91]	Threat modelling	Both	Static and manual-based
ADT	[31,91]	Attack and defence	QL only	Static and manual-based
QADT	[93,94]	QT threat modelling	Both	Static and manual-based
DFT	[80]	Dynamic failure	Both	Manual-Based
PT FT	[81]	Dynamic failure	Both	Manual-Based
FMEA	[28,84,100]	Static failure	QL Only	Static and manual-based
RBD	[86]	Static failure	Both	Manual-Based
MCA	[87,88]	Reliability and availability	QT Only	Manual-Based

4.4. Model-Based Safety and Security Analysis Frameworks

As part of the development of model-based system engineering (MBSE), several approaches were developed for modelling systems' safety and security properties using domain-specific models or general models with domain-specific profiles. The MBSE approaches involve more formal computer-based system design and verification approaches, which are used to model both the functional and nonfunctional properties of systems [39]. Various studies have been conducted using MBSE to develop methodologies for the analysis of performance [36,37], safety [39–42], reliability [40,42], and security properties [43–45]. In the realm of model-driven development, classical analysable models such as fault trees, attack trees, Petri nets, and other artefacts are automatically or semiautomatically generated using software-based approaches. The software-driven approaches generate the artefacts based on painstaking modelling of systems' static, dynamic, and behavioural patterns using methodologies drawn from the existing modelling languages' (ML) functionalities. Subsequently, the modelled system is further transformed or mapped into safety and security analysis models. The MBSE approaches can be used to manage a system's complexity and to perform formalised, structured, and rigorous system design evaluations. In exploring the richness of MBSE methodologies, various studies have been conducted to automate analysable safety and security artefacts such as FT, Component FT, and Petri nets among others. Notably, studies [101–105] used UML functionalities, namely, the activity, class, sequence, and used-case diagrams (AD, CD, SD, UCD) to automate FMEA, FT and GSPN. The methodologies were evaluated using automotive, control systems, and generic case studies. In close comparison to UML-based methodologies, SysML was used in both the safety and security domains. For instance, refs. [33,39–42] used SysML and BDD, IBD, AD, SMD to develop FT and FMEA safety analysis frameworks using embedded systems and generic system case studies. Conversely, an attack tree was generated for security analysis based on industrial control case studies using SysML BDD, IBD, and SMD by [35].

Furthermore, refs. [34,36,45] developed an FT and an FMEA using AADL for aircraft digital system safety analysis. In another research conducted by [43], the AADL methodology was used to automate an attack tree for the evaluation of a patient-controlled analgesic pump. The HiP-HOPS was used by [41,42,45] to automate FT, Pandora FT, and DFT frameworks, as well as evaluate the safety analyses of automotive and embedded systems. Lastly, research by [44] used Digital Dependability Identities [106] for offline security analysis, and an attack tree was developed based on HiP-HOPS; the approach was evaluated using a web-based medical application. Notably, the MBSE approaches continue to address some of the limitations of informal system modelling, such as the lack of reusability, time consumption, and human errors. However, the existing semiautomated dependability assessment approaches in IoT environments, which are still in their infancy, focus more on the qualitative and independent analysis of safety and security properties. Furthermore, some MBDA approaches focus more on the physical security properties of systems design, and some of the studies often tend to oversimplify the interactions between the safety and cyber-security properties of IoT systems. To the best of our knowledge in this review, the existing MBSE approach has not developed a viable safety and security assessment methodology that has adequately captured cyber security, safety quantification, and the coanalysis of a robust IoT case study. Therefore, we consider the existing work in safety and security to be less viable for useful assessment in modern, dynamic, and evolving system design processes such as those found in IoT environments. A summary of comparisons of notable MBSE approaches for safety and security analysis is presented in Table 2. The approaches were compared in terms of the analysable artefacts generated, the expressiveness to evaluate qualitative and quantitative safety and security parameters, the case studies applied, and their major weaknesses in the coanalysis of the two properties.

Table 2. Notable model-based safety and security analysis frameworks.

Approach	Studies	Artefact	Analysis	Case Study
UML	[101–105]	FMEA, FT, GSPN	Qualitative Safety Analysis	Automotive and control systems
SysML	[33,39–42]	FT, FMEA	Qualitative Safety Analysis	Embedded systems and generic systems
SysML	[35]	Attack Tree	Qualitative Security Analysis	Industrial control systems
AADL	[34,36,45]	FT, FMEA	Qualitative Safety Analysis	Aircraft digital systems
AADL	[43]	Attack Tree	Qualitative Security Analysis	Patient-controlled analgesic pump
HiP-HOPS	[41,42,45]	FT, Pandora FT, and DFT	Qualitative Safety Analysis	Automotive, Aerospace, and Embedded systems
HiP-HOPS	[44]	Attack Tree	Qualitative Security Analysis	Web-Based medical application

4.5. Related Work

Researchers have conducted notable surveys on safety and security analysis frameworks across many domains. Some surveys were based on individual safety or security analysis approaches; few considered their coanalysis. Regarding IoT safety, a recent and comprehensive survey was conducted by Xing [13]. The author discussed various state-of-the-art reliability issues across the IoT model. These reliability issues directly impact the safe operation of the IoT device. The survey acknowledges that research in IoT safety is at its early stage, and much research is required to address the unexplored behaviour of current and emerging IoT innovations. This research exploration supports the safe operation of the IoT system. Contrarily, there are many surveys in the areas of IoT security frameworks that have more of a focus on IoT security than safety. The survey of Ammar et al. [107] extensively elaborated on the existing frameworks and approaches used in evaluating IoT security. The survey discussed some of the relevant pros and cons of some frameworks to fulfil the security requirements and meet the standard guidelines.

Furthermore, other surveys review the coanalyses of safety and security properties. A prominent survey was made by Kriaa et al. [18]. Although the work raised awareness regarding the safety and security convergence in industrial control systems, there was less emphasis on the IoT systems. Nevertheless, it remarkably discussed the interdependence of the two properties and highlighted a possible way forward to their coanalysis. An insight into model-based analysis approaches for safety and security was also made. However, further exploring these complex interactions to analyse their impact on the IoT domain is relevant. Some challenges in quantifying safety and security, standardisation, and new constructs when modelling the safety and security of IoT systems' design and operational phases need further studies. Furthermore, the survey did not capture new challenges to safety and security that modern IoT systems have brought. A few of these challenges include bad interactions between colocated IoT devices, the dynamic behaviour, and the reconfigurable and adaptive nature of IoT systems [16,108]. More recently, Lisova et al. [109] proposed a systematic literature review regarding safety and security coanalysis. In their survey, in addition to safety and security interactions and relationships, which were covered in Kriaa et al. [18], they went further to give an insight into the impact and influence of safety considerations on the security properties of systems and vice versa. Accordingly, they highlighted new insights on safety-informed security approaches and security-informed safety approaches, which, in both ways, are important for achieving dependable IoT systems. The survey attested that there is no existing approach so far that has addressed the impact of device safety on its security properties. The review also elaborated that several existing approaches lack extensive evaluation and involve an oversimplification of security problems, as was earlier highlighted. The authors' view has reinforced an existing gap in the field of dependability, and their survey should have considered the growing dynamism of MBSE with regard to addressing safety and security coanalysis and verification. A summary of some of the notable surveys based on their focus is depicted in Table 3.

Table 3. Survey distribution based on their focus.

Approach	Studies	Domain of Application	Limitation
Safety Analysis	[13]	IoT	Emphasis on reliability only
Security Analysis	[107]	IoT	Emphasis on threat modelling only
Coanalysis	[18,109]	Industrial control systems	Less insight into MBSE approaches

So far, from the existing surveys, there needs to be more insight into the review of approaches that consider both safety and security analysis in manual and MBSE studies. This survey attempts to address this observed gap in the literature. Additionally, the survey also looks at some of the existing safety and security issues across the IoT architecture.

5. Discussion and Future Outlook

IoT systems are evolving unprecedentedly due to the general technological progress across various engineering and computer science domains. From the review conducted, the safety and security requirements of IoT systems are critical to this progress because of the increasing concerns across various stakeholders in the IoT systems. Remarkably, most of the existing safety and security analysis frameworks discussed in this survey have been accepted over the years and have been used in many safety-critical industries to evaluate static, dynamic, and modern systems. While for typical mechanical or electronics systems, the classical informal analysis frameworks can provide useful insight into the safety and security requirements, these approaches must meet the demand for the rigorous safety and security analysis of complex and emerging IoT systems.

From our review, it has been established that the limitations of the classical approaches are centred on their informal manual processes of the evaluation of safety or security properties. Manual frameworks tend to inherit the natural limitations of informal system modelling, such as human error, time consumption, and a lack of reusability. Additionally, their independent approach to evaluating safety and security properties could be less viable for modern systems. Although some studies have been conducted on a unified safety and security treatment, most studies were conducted using short and oversimplified case studies for other domains that did not have complex safety and cyber-security requirements. The prominent approach so far developed for the unified safety and security approach is available in [18]. The case studies on the scenarios involved a simple industrial control system and an emergency door system which were conducted using a classical manual approach. As stated earlier, the manual approach inherits several limitations, which can not guarantee the safety and security of the IoT systems. Additionally, the study failed to adequately address the cyber-security requirements, which are critical issues in the IoT environment. Thus, the safety and security coanalysis of IoT systems has not been exhaustively modelled using a viable unified framework in the studies evaluated.

Furthermore, any independent or incomplete analysis of safety and security properties in the IoT environment using an informal approach is unlikely to adequately capture the four established safety and security interactions discussed in Section 2.4. The implication behind the dependable IoT system design is that the system developers may not consider the criticality of these interactions if the two properties are evaluated independently. For instance, when safety and security requirements serve the same purpose, their coanalysis could lead to cost-effectiveness. Conversely, in the case of conflicting safety and security design parameters, the coanalysis of the two properties can suggest the need for a trade-off based on the system requirements. Moreover, the independent analysis of safety and security properties goes contrary to international risk recommendations such as the ISO 31004, IEC 64443, ISO 26262, and European research projects, which have all acknowledged the need for safety and security to be coanalysed in order to develop more trustworthy systems [18,20,80].

Additionally, the existing studies on safety and security analysis in the IoT domain have yet to adequately address the safety/security interdependencies, cyber-security prop-

erties, and quantification. These limitations make the existing approaches less viable for a useful assessment of the safety and security requirements of modern, dynamic, and iterated system design processes such as those found in IoT environments. This development underpins research gaps in the existing dependability frameworks for assessing interactions and quantifying IoT systems' safety and cyber-security properties. An effort to address some of these gaps will contribute to state-of-the-art dependability analysis in the IoT environment. Thus, research in this direction will serve as a pivotal driver to manage and reduce adverse events and avoid impact on health safety and the environment (HSE) while maintaining a productive process in compliance with local and global regulations. This effort will support the rapid pace of the design of IoT-Enabled applications, which requires a high level of safety and security thresholds.

In our future roadmap to address some of these identified gaps, we will explore existing modelling language methodologies to develop a software-based analysis framework for the robust analysis of IoT systems' safety and security requirements. We will rely on some of the studied functionalities of UML/SysML frameworks, such as internal block, activity, and state-machine diagrams, to model the static and behavioural patterns of complex IoT case studies. Additionally, domain-specific profiles, such as DAM, MARTE, and DICE, will be helpful in annotating failure and security parameters such as the fault, error, hazards, and probability of occurrences of some of the requirements. These profiles have reached stereotypes, and tag values, which are parts of their extension mechanisms to model desired system features. Therefore, with further refinement of the existing methodologies, the profiles can aid in threat and failure annotations, thereby leading to new constructs, which could be used to model and quantify the safety and security requirements of the IoT environment. A careful design of a good IoT system source model developed using this novel approach can be transformed into state-based or stateless analysable and formal artefacts such as dynamic FTA, Petri net, or Bayesian Network. This effort will contribute to developing a more viable and trustworthy safety and security coanalysis in the IoT domain. Thus, it will provide remarkable opportunities for automation and integration with design models to simplify the analysis of IoT systems' complex safety and security-critical requirements. The intended approach will further support reusability, reduce human error, increase robustness to perform complex dependability analysis unambiguously, and support the heterogeneity of IoT systems' designs. Consequently, efforts to explore the features of these MBDA techniques to develop a safety and security coanalysis framework will be worthwhile.

6. Final Remarks

Given the widespread use of IoT systems in private and public domains, it is evident that the safety and security of IoT systems must be given appropriate consideration to avoid the catastrophic consequences of their aftermath. Safety and security as the NFPs of dependable IoT systems are traditionally viewed by different communities, with each focusing on different problems, methodologies, causes, and consequences. However, unlike traditional mechatronic systems, this approach is less viable in the IoT domain due to the complex interaction and interdependencies between the safety and security properties. Albeit research on the unified treatment of the safety and security of IoT systems is in the infancy stage, some modest contributions to investigating these complex interactions are ongoing in other domains.

The survey has shown that most existing safety and security analysis frameworks are centred on classical manual approaches, which independently evaluate the two properties. However, these approaches come with inherent limitations regarding informal system modelling, such as human error, time consumption, and a lack of support for reusability. On the other hand, the existing model-based safety and security approaches have been based on limited scenarios, which independently assess safety and security properties. Furthermore, the existing studies are yet to adequately address the safety/security interdependencies, cyber-security properties, quantification, and coanalysis of the safety and

security properties of IoT applications. These limitations make the existing approaches less viable for a valuable assessment of the safety and security requirements of dynamic and iterated system design processes such as those found in IoT environments. These under-explored gaps present a viable research opportunity in the design of safety and security analysis frameworks.

In our future roadmap to address some of these identified gaps, we intend to explore modelling language methodologies to develop a software-based analysis framework for IoT systems' robust safety and security requirements. We will rely on some of the studied functionalities of UML/SysML, such as internal block, activity, and state-machine diagrams, to model the static and behavioural patterns of complex IoT case studies. Additionally, three domain-specific profiles, which are DAM, MARTE, and DICE, will be helpful in annotating failure and security parameters such as fault, error, hazards, and their probabilities of occurrence. However, these profiles have reached stereotypes, and tag values, which are part of their extension mechanisms to model desired system features. Therefore, with further refinement, these profiles can aid annotations leading to new constructs, which could be used to model and quantify the safety and security coanalysis of the IoT environment. This will contribute to developing a more viable and trustworthy safety and security coanalysis in the IoT domain.

Author Contributions: Conceptualization, A.A. and S.K.; methodology, A.A., S.K., C.L. and I.G. writing—original draft preparation, A.A., S.K., C.L. and I.G.; writing—review and editing, S.K., C.L. and I.G.; problem space and formalization, S.K., C.L. and I.G.; supervision, S.K., C.L. and I.G.; project administration, S.K., C.L. and I.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AADL	Architecture Analysis and Design Language
AD	Attack–Defence Tree
AT	Attack Trees
AFT	Attack Fault Trees
DAM	Dependability Analysis Modelling
FTA	Fault Tree Analysis
FMEA	Failure Mode Effect Analysis
HiP-HOPS	Hierarchically Performed Hazard Origin and Propagation Studies
IoT	Internet of Things
MBSE	Model-Based System Engineering
MCA	Markov Chain Analysis
SDLC	System Development Life Cycle
RBD	Reliability Block Diagrams
DFT	Dynamic Fault Tree
UML	Unified Modelling Language
QAD	Quantitative Attack–Defence Tree
QT	Quantitative Analysis
QL	Qualitative Analysis
SysML	System Modelling Language.

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. [[CrossRef](#)]
2. Fizza, K.; Banerjee, A.; Jayaraman, P.P.; Auluck, N.; Ranjan, R.; Mitra, K.; Georgakopoulos, D. A Survey on Evaluating the Quality of Autonomic Internet of Things Applications. *IEEE Commun. Surv. Tutor.* **2022**, *25*, 567–590. [[CrossRef](#)]
3. 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.
4. Udoh, I.S.; Kotonya, G. Developing IoT applications: Challenges and frameworks. *IET Cyber-Phys. Syst. Theory Appl.* **2018**, *3*, 65–72. [[CrossRef](#)]
5. 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. [[CrossRef](#)]
6. Raza, U.; Lomax, J.; Ghafir, I.; Kharel, R.; Whiteside, B. 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, Cambridge, UK, 19–20 July 2017; pp. 1–8.
7. Hammoudeh, M.; Ghafir, I.; Bounceur, A.; Rawlinson, T. 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, Paris, France, 1–2 July 2019; pp. 1–5.
8. Wu, F.; Wu, T.; Yuce, M.R. Design and implementation of a wearable sensor network system for IoT-connected safety and health applications. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 87–90.
9. Bhushan, D.; Agrawal, R. The Internet of Things: Looking beyond the hype. In *An Industrial IoT Approach for Pharmaceutical Industry Growth*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 231–255.
10. Wu, F.; Redouté, J.M.; Yuce, M.R. We-safe: A self-powered wearable iot sensor network for safety applications based on lora. *IEEE Access* **2018**, *6*, 40846–40853. [[CrossRef](#)]
11. Gope, P.; Gheraibia, Y.; Kabir, S.; Sikdar, B. A secure IoT-based modern healthcare system with fault-tolerant decision making process. *IEEE J. Biomed. Health Inform.* **2020**, *25*, 862–873. [[CrossRef](#)]
12. Patel, P.; Narmawala, Z.; Thakkar, A. A survey on intelligent transportation system using internet of things. *Emerg. Res. Comput. Inf. Commun. Appl.* **2019**, *1*, 231–240.
13. Xing, L. Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet Things J.* **2020**, *7*, 6704–6721. [[CrossRef](#)]
14. 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.
15. Kabir, S. Internet of things and safety assurance of cooperative cyber-physical systems: Opportunities and challenges. *IEEE Internet Things Mag.* **2021**, *4*, 74–78. [[CrossRef](#)]
16. 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.
17. Kriaa, S.; Bouissou, M.; Colin, F.; Halgand, Y.; Pietre-Cambacédes, 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.
18. Kriaa, S.; Pietre-Cambacédes, 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. [[CrossRef](#)]
19. 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.
20. 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.
21. 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.
22. Brunner, M.; Huber, M.; Sauerwein, C.; Brey, 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.
23. Cerf, V.G.; Ryan, P.S.; Senges, M.; Whitt, R.S. Iot safety and security as shared responsibility. *Bus. Inform.* **2016**, *1*, 7–19. [[CrossRef](#)]
24. 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.
25. Aven, T. A unified framework for risk and vulnerability analysis covering both safety and security. *Reliab. Eng. Syst. Saf.* **2007**, *92*, 745–754. [[CrossRef](#)]

26. 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. [[CrossRef](#)]
27. 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.
28. Kabir, S. An overview of fault tree analysis and its application in model based dependability analysis. *Expert Syst. Appl.* **2017**, *77*, 114–135. [[CrossRef](#)]
29. 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.
30. 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.
31. 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.
32. 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. [[CrossRef](#)]
33. Wang, H.; Zhong, D.; Zhao, T.; Ren, F. Integrating model checking with SysML in complex system safety analysis. *IEEE Access* **2019**, *7*, 16561–16571. [[CrossRef](#)]
34. 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. [[CrossRef](#)]
35. 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.
36. Ahamad, S.; Gupta, R. Performability modeling of safety-critical systems through AADL. *Int. J. Inf. Technol.* **2022**, *14*, 1–14. [[CrossRef](#)]
37. 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. [[CrossRef](#)]
38. 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.
39. 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.
40. 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.
41. Papadopoulos, Y.; Walker, M.; Parker, D.; Rude, 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. [[CrossRef](#)]
42. 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. [[CrossRef](#)]
43. 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.
44. 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.
45. 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. [[CrossRef](#)]
46. 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. [[CrossRef](#)]
47. Edifor, E.; Gordon, N.; Walker, M. Dependability Analysis Using Temporal Fault Trees and Monte Carlo Simulation. In Proceedings of the International Conference on Dependability and Complex Systems, Wroclaw, Poland, 28 June–2 July 2021; pp. 86–96.
48. Avizienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. Basic Concepts and Taxonomy of Dependable Secure Computing. In *A Process for Developing a Common Vocabulary in the Information Security Area*; IOS Press: Amsterdam, The Netherlands, 2007; pp. 10–51.
49. Ştefan, V.K.; Otto, P.; Alexandrina, P.M. Considerations regarding the dependability of Internet of Things. In Proceedings of the 2017 14th International Conference on Engineering of Modern Electric Systems (EMES), Oradea, Romania, 1–2 June 2017; pp. 145–148.

50. 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.
51. 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.
52. Wach, P.; Salado, A. Model-Based Security Requirements for Cyber-Physical Systems in SysML. In Proceedings of the 2020 IEEE Systems Security Symposium (SSS), Crystal City, VA, USA, 1 July–1 August 2020; pp. 1–7.
53. Ghafir, I.; Kyriakopoulos, K.G.; Aparicio-Navarro, F.J.; Lambotharan, S.; Assadhan, B.; Binsalleeh, H. A basic probability assignment methodology for unsupervised wireless intrusion detection. *IEEE Access* **2018**, *6*, 40008–40023. [[CrossRef](#)]
54. Diab, D.M.; AsSadhan, B.; Binsalleeh, H.; Lambotharan, S.; Kyriakopoulos, K.G.; Ghafir, I. Denial of service detection using dynamic time warping. *Int. J. Netw. Manag.* **2021**, *31*, e2159. [[CrossRef](#)]
55. 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. [[CrossRef](#)]
56. Ghafir, I.; Prenosil, V.; Svoboda, J.; Hammoudeh, M. A survey on network security monitoring systems. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 77–82.
57. Papakonstantinou, N.; Linnosmaa, J.; Bashir, A.Z.; Malm, T.; Van Bossuyt, D.L. Early combined safety-security Defense in Depth assessment of complex systems. In Proceedings of the 2020 Annual Reliability and Maintainability Symposium (RAMS), Palm Springs, CA, USA, 27–30 January 2020; pp. 1–7.
58. Zalewski, J. IoT safety: State of the art. *IT Prof.* **2019**, *21*, 16–20. [[CrossRef](#)]
59. Draeger, J. Roadmap to a unified treatment of safety and security. In Proceedings of the 10th IET System Safety and Cyber-Security Conference, Bristol, UK, 21–22 October 2015; pp. 1–6.
60. Kriaa, S.; Bouissou, M.; Laarouchi, Y. A new safety and security risk analysis framework for industrial control systems. *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.* **2019**, *233*, 151–174. [[CrossRef](#)]
61. 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. [[CrossRef](#)]
62. Bisenius, B. Product safety of the internet of things [product safety perspectives]. *IEEE Consum. Electron. Mag.* **2017**, *6*, 137–139. [[CrossRef](#)]
63. 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.
64. 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.
65. 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. [[CrossRef](#)]
66. 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.
67. 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. [[CrossRef](#)]
68. 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.
69. 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. [[CrossRef](#)] [[PubMed](#)]
70. Sontowski, S. Exploration and Detection of Denial-of-Service Attacks on Cyber-Physical Systems. Ph.D. Thesis, Tennessee Technological University, Cookeville, TN, USA, 2022.
71. Wongvises, C.; Khurat, A.; Fall, D.; Kashiara, S. Fault tree analysis-based risk quantification of smart homes. In Proceedings of the 2nd International Conference on Information Technology (INCIT), Nakhonpathom, Thailand, 2–3 November 2017; pp. 1–6.
72. Kabir, S.; Azad, T.; Walker, M.; Gheraibia, Y. Reliability analysis of automated pond oxygen management system. In Proceedings of the 2015 18th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 21–23 December 2015; pp. 144–149.
73. Bhattacharyya, S.; Cheliyan, A. Optimization of a subsea production system for cost and reliability using its fault tree model. *Reliab. Eng. Syst. Saf.* **2019**, *185*, 213–219. [[CrossRef](#)]
74. Ruijters, E.; Stoelinga, M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Comput. Sci. Rev.* **2015**, *15*, 29–62. [[CrossRef](#)]
75. Aslansefat, K.; Kabir, S.; Gheraibia, Y.; Papadopoulos, Y. Dynamic fault tree analysis: State-of-the-art in modeling, analysis, and tools. In *Reliability Management and Engineering*; CRC Press: Boca Raton, FL, USA, 2020; pp. 73–112.
76. Kabir, S. Compositional Dependability Analysis of Dynamic Systems with Uncertainty. Ph.D. Thesis, University of Hull, Hull, UK, 2016.

77. Bilgen, M.; Altin, N. An Overview on reliability analysis and evaluation methods applied to smart grids. *Gazi Univ. J. Sci. Part C Des. Technol.* **2021**, *9*, 645–660. [[CrossRef](#)]
78. Chen, Y.; Zhen, Z.; Yu, H.; Xu, J. Application of fault tree analysis and fuzzy neural networks to fault diagnosis in the internet of things (IoT) for aquaculture. *Sensors* **2017**, *17*, 153. [[CrossRef](#)]
79. Niloofar, P.; Lazarova-Molnar, S. Fusion of data and expert knowledge for fault tree reliability analysis of cyber-physical systems. In Proceedings of the 2021 5th International Conference on System Reliability and Safety (ICSRS), Palermo, Italy, 24–26 November 2021; pp. 92–97.
80. Zhou, S.; Ye, L.; Xiong, S.; Xiang, J. Reliability analysis of dynamic fault trees with Priority-AND gates based on irrelevance coverage model. *Reliab. Eng. Syst. Saf.* **2022**, *224*, 108553. [[CrossRef](#)]
81. Kabir, S.; Walker, M.; Papadopoulos, Y. Quantitative evaluation of Pandora temporal fault trees via Petri nets. *IFAC-PapersOnLine* **2015**, *48*, 458–463. [[CrossRef](#)]
82. Kabir, S. A fuzzy data-driven reliability analysis for risk assessment and decision making using Temporal Fault Trees. *Decis. Anal. J.* **2023**, *8*, 100265. [[CrossRef](#)]
83. Kabir, S.; Papadopoulos, Y.; Walker, M.; Parker, D.; Aizpurua, J.I.; Lampe, J.; Rude, E. A model-based extension to HiP-HOPS for dynamic fault propagation studies. In Proceedings of the Model-Based Safety and Assessment, Trento, Italy, 11–13 September 2017; pp. 163–178.
84. Mikulak, R.J.; McDermott, R.; Beauregard, M. *The Basics of FMEA*; CRC Press: Boca Raton, FL, USA, 2017.
85. Korsunovs, A.; Doikin, A.; Campean, F.; Kabir, S.; Hernandez, E.M.; Taggart, D.; Parker, S.; Mills, G. Towards a Model-Based Systems Engineering Approach for Robotic Manufacturing Process Modelling with Automatic FMEA Generation. *Proc. Des. Soc.* **2022**, *2*, 1905–1914. [[CrossRef](#)]
86. Kim, M.C. Reliability block diagram with general gates and its application to system reliability analysis. *Ann. Nucl. Energy* **2011**, *38*, 2456–2461. [[CrossRef](#)]
87. Brameret, P.A.; Roussel, J.M.; Rauzy, A. Preliminary system safety analysis with limited markov chain generation. *IFAC Proc. Vol.* **2013**, *46*, 13–18. [[CrossRef](#)]
88. Agrawal, A.K.; Murthy, V.; Chattopadhyaya, S. Investigations into reliability, maintainability and availability of tunnel boring machine operating in mixed ground condition using Markov chains. *Eng. Fail. Anal.* **2019**, *105*, 477–489. [[CrossRef](#)]
89. Casola, V.; De Benedictis, A.; Rak, M.; Villano, U. Toward the automation of threat modeling and risk assessment in IoT systems. *Internet Things* **2019**, *7*, 100056. [[CrossRef](#)]
90. Gabbay, D.M.; Horne, R.; Mauw, S.; van der Torre, L. Attack-defence frameworks: Argumentation-based semantics for attack-defence trees. In Proceedings of the Graphical Models for Security: 7th International Workshop, GramSec 2020, Boston, MA, USA, 22 June 2020; pp. 143–165.
91. Brooke, P.J.; Paige, R.F. Fault trees for security system design and analysis. *Comput. Secur.* **2003**, *22*, 256–264. [[CrossRef](#)]
92. Kumar, R.; Ruijters, E.; Stoelinga, M. Quantitative attack tree analysis via priced timed automata. In Proceedings of the Formal Modeling and Analysis of Timed Systems: 13th International Conference, FORMATS 2015, Madrid, Spain, 2–4 September 2015; pp. 156–171.
93. Muller, S.; Harpes, C.; Muller, C. Fast and optimal countermeasure selection for attack defence trees. In Proceedings of the Risk Assessment and Risk-Driven Quality Assurance: 4th International Workshop, RISK 2016, Held in Conjunction with ICTSS 2016, Graz, Austria, 18 October 2016; pp. 53–65.
94. Rios, E.; Rego, A.; Iturbe, E.; Higuero, M.; Larrucea, X. Continuous quantitative risk management in smart grids using attack defense trees. *Sensors* **2020**, *20*, 4404. [[CrossRef](#)]
95. Ge, M.; Hong, J.B.; Guttman, W.; Kim, D.S. A framework for automating security analysis of the internet of things. *J. Netw. Comput. Appl.* **2017**, *83*, 12–27. [[CrossRef](#)]
96. Ge, M.; Kim, D.S. A framework for modeling and assessing security of the internet of things. In Proceedings of the 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS), Melbourne, Australia, 14–17 December 2015; pp. 776–781.
97. Contini, S.; Cojazzi, G.; Renda, G. On the use of non-coherent fault trees in safety and security studies. *Reliab. Eng. Syst. Saf.* **2008**, *93*, 1886–1895. [[CrossRef](#)]
98. Fovino, I.N.; Masera, M.; De Cian, A. Integrating cyber attacks within fault trees. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1394–1402. [[CrossRef](#)]
99. Steiner, M.; Liggesmeyer, P. Combination of safety and security analysis-finding security problems that threaten the safety of a system. In Proceedings of the ERCIM/EWICS Workshop on Dependable Embedded and Cyber-Physical Systems, Toulouse, France, 24–27 September 2013; pp. 1–8.
100. Oliveira, J.; Carvalho, G.; Cabral, B.; Bernardino, J. Failure mode and effect analysis for cyber-physical systems. *Future Internet* **2020**, *12*, 205. [[CrossRef](#)]
101. David Deji, P. Derivation of Failure Mode and Effects Analysis (FMEA) Table from UML Software Model by Epsilon Model Transformation. Ph.D. Thesis, Carleton University, Ottawa, ON, Canada, 2016.
102. Mohrle, F.; Zeller, M.; Hofig, K.; Rothfelder, M.; Liggesmeyer, P. Automated compositional safety analysis using component fault trees. In Proceedings of the 2015 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Gaithersburg, MD, USA, 2–5 November 2015; pp. 152–159.

103. Zhao, Z. UML Model to Fault Tree Model Transformation for Dependability Analysis. Ph.D. Thesis, Carleton University, Ottawa, ON, Canada, 2014.
104. Rodriguez, R.J.; Gomez-Martinez, E. Model-based safety assessment using OCL and Petri nets. In Proceedings of the 2014 40th EUROMICRO Conference on Software Engineering and Advanced Applications, Verona, Italy, 27–29 August 2014; pp. 56–59.
105. Grant, E.S.; Datta, T. Roadmap to a DO-178C formal model-based software engineering methodology. In Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, China, 18–20 March 2015; Volume 1.
106. Armengaud, E.; Schneider, D.; Reich, J.; Sorokos, I.; Papadopoulos, Y.; Zeller, M.; Regan, G.; Macher, G.; Veledar, O.; Thalmann, S.; et al. DDI: A novel technology and innovation model for dependable, collaborative and autonomous systems. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 1–5 February 2021; pp. 1626–1631. [[CrossRef](#)]
107. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27. [[CrossRef](#)]
108. Riaz, S.; Kabir, S.; Campean, F.; Mokryani, G.; Dao, C.; Marquez, J.A.; Al-Ja' Afreh, M.A.A. Challenges with Providing Reliability Assurance for Self-Adaptive Cyber-Physical Systems. In Proceedings of the 6th International Conference on System Reliability and Safety (ICSRS), Venice, Italy, 23–25 November 2022; pp. 1–6.
109. Lisova, E.; Šljivo, I.; Čaušević, A. Safety and Security Co-Analyses: A Systematic Literature Review. *IEEE Syst. J.* **2019**, *13*, 2189–2200. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.