A Security-enabled Safety Assurance Framework for IoT-based Smart Homes

Sohag Kabir, Prosanta Gope, *Senior Member, IEEE*, and Saraju P. Mohanty, *Senior Member, IEEE*

***Abstract*—The exponential growth of the Internet of Things (IoT) has paved the way for safety-critical cyber-physical systems to enter our everyday activities. While such systems have changed the way of our life, they brought new challenges that can adversely affect our life and the environment. Safety and security are two such challenges that can hamper the widespread adoption of new IoT applications. Due to a large number of connected devices and their ability to control critical physical assets, intended attacks on them and/or unintended failure events such as mechanical failure of devices, communication failure and unforeseen bad interactions between connected devices may cause an IoT-based system to enter into unsafe and dangerous physical states. By considering the importance of safety and security of IoT systems, in this article, we present a security-enabled safety monitoring framework for IoT-based systems. In the proposed framework, we utilise design-time system analysis to create an executable monitoring model that enables run-time safety assurance provision for a system via collecting and analysing operational data and evidence to determine the safety status of the system and then taking appropriate actions and securely communicating the safety status and recommended actions to the system users to minimise the risk of the system entering into an unsafe state.**

***Index Terms*—IoT, Safety Assurance, Security, Safety Monitoring, Smart Homes**

I. Introduction

People's lives have been changed dramatically due to technological advancement in smart and diverse types of consumer electronics. These devices, known as the Internet of Things (IoT), are connected by advanced communication technologies to the Internet to exchange information. Nowadays, IoT devices are widely deployed for various applications such as smart home, smart city, body networks, smart grid, and vehicular ad-hoc networks [1]. A smart home can be referred to as an internet-connected residence equipped with modern technologies and remotely controllable smart devices that allows monitoring of its residents and environment to provide residents with convenience, enhanced safety, and cost savings. In a smart home environment, smart devices can autonomously make their own decisions and take actions with minimal human intervention, for instance, can turn on sprinklers in the presence of fire, control the heating system of the home, locks of the doors, surveillance systems, and functionality of the connected devices. While such IoT systems bring several opportunities, they also raise concerns about the safety and security of IoT-enabled digital lives [2]–[5].

Due to a large number of connected devices and their ability to control critical physical assets, IoT systems can reach unsafe and dangerous physical states because of intended attacks on them and/or unintended random failure events such as failure of physical devices, failure or error in communication and unforeseen bad interactions between connected devices [6], [7]. Potential safety issues in IoT have been discussed in [8]. It was also noted that serious safety hazards could be caused by security attacks and physical failure of devices, which could cause injury to humans and damage to the environment and property.

In a smart home, multiple systems provided by different vendors are often installed in the same environment and are expected to work seamlessly without creating any issue. However, integrating systems from different providers is challenging because each individual system has its own policies to control the physical devices without much knowledge of the surrounding environment and other systems. Moreover, each system may operate under different assumptions. This may lead to conflicting situations when multiple systems work in the same environment. Such conflict could have catastrophic consequences. Apart from this, physical devices and/or the communication between the central hub and the user can fail, which can force the overall system to enter a hazardous state. Whether the failure of an IoT system is caused by intended cyber attacks or random failure of devices or communication, the failure has the potential to cause great harm, both to people and to the environment. For this reason, the development of these systems requires a rigorous assessment of system behaviour to ensure that they possess a high level of dependability.

A. IoT Safety and Security

Currently, the IoT industry has reached its "gold rush" state, where every manufacturer is competing to release their next innovative connected devices before their competitors do without thinking much about the non-functional properties of the system. Under such situations, the functionality of the connected devices becomes the major focus and the issues like safety and security take a back seat. However, safety and security are two imperative requirements to guarantee the availability and functionality of IoT-based applications. Guaranteeing both safety and security for IoT is challenging since miscellaneous IoT devices, communication interfaces, and applications lead to many different safety or security requirements and also increase the cost of deploying corresponding security protections. On the other hand, both safety

S. Kabir is with the Department of Computer Science, University of Bradford, Bradford, BD7 1DP, UK, E-mail: s.kabir2@bradford.ac.uk.

P. Gope is with the Department of Computer Science, University of Sheffield, Sheffield, S1 4DP, UK, E-mail:p.gope@sheffield.ac.uk.

S. P. Mohanty is with the Dept. of Computer Science and Engineering, University of North Texas, E-mail: saraju.mohanty@unt.edu.

and security in the IoT system have not been fully standardised due to the wide range of applications.

Security requirements in an IoT application should be considered through the following three aspects: hardware, communication, and system model. Here, hardware security means the physical security of IoT devices, while communication security of IoT applications means confidentiality and integrity of communications between IoT entities (e.g., end devices, network infrastructures, service providers, information processing systems) and application data in storage. The security of each IoT application may vary according to the system model.

In addition to security, safety issues in IoT systems are equally important to be addressed as such systems are increasingly being used to physically control critical devices both in homes and in industries. The safety issue caused by fire incidence in Samsung Galaxy Note smartphones shows us the importance of safety assurance in IoT devices and challenges making such devices safe even in the absence of security attacks. Assuring the safety of such devices in the presence of attackers will be more difficult. Therefore, to guarantee the safe operation of IoT systems, it is important to understand how such systems are designed, the behaviour of the systems and the potential causes of their failure. Through a rigorous safety assessment of systems, it is possible to identify the combination of events that can cause the systems to reach unsafe operational states, thereby, it is possible to define preventive measures to ensure safe operation of systems.

To improve system safety and reliability, fault tolerance mechanisms are widely used to avoid hazardous situations during system operation. Safety monitors are widely used to observe the system and its operating environment to detect anomalies that may cause the system to enter an unsafe state. On detecting a fault, the safety monitor raises an alarm and triggers interventions to keep the system in a safe state [9]. Such interventions may include automatic action taken by the monitor and/or a manual action taken by human operators. For instance, in [10], monitoring knowledge is used to provide safety assurance for a robotic manufacturing system, whereas, safety assurance for a vehicle platooning system is provided in [11]. System monitoring has also been utilised to provide dynamic safety assurance in approaches like [12], [13].

B. Motivation and contributions of the current article

IoT-based monitoring has been successfully applied in many different domains such as smart health, smart cities, smart transportations, smart environments, smart manufacturing, smart agriculture, and so on [14]. In these applications, IoT-based solutions are used for device, infrastructure and environmental monitoring. The opportunities for using IoT-based monitoring in safety assurance provision for cyber-physical systems have been discussed in [15]. While it is evident that IoT-based monitoring systems have brought significant benefit in many domains, the fact that these monitoring systems themselves can fail to cause hazardous consequences is rarely considered.

To the best of our knowledge, there is no work on monitoring the safety status of IoT-based systems to provide continuous safety assurance. This motivates us to introduce a novel safety assurance framework that can provide safety assurance for IoT systems. The main contributions of this article are:

- A novel safety assurance framework that combines design-time safety analysis models and runtime evidence collected during system operation to provide continuous assurance for IoT-enabled systems.
- In addition to addressing safety concerns caused by system failures, we have identified and addressed safety concerns that are caused by conflicting interactions between multiple systems.
- Definition of recommended actions to avoid hazardous situations during system operation and communication of the system status with the users.
- Definition of security measures to ensure secure communication between the safety monitor and the users.

The rest of the article is organised as follows: Section II discusses the related prior works. The proposed framework is described in Section III. We then provide an illustrative example for the approach including a comparison with related approaches in Section IV, before summarising the key conclusions.

II. Related Works

The concept of smart homes has been around us for decades and their adoption by consumers has been increasing significantly. Different innovative ideas have been integrated into smart homes to improve the convenience and safety of the residents. Such ideas include, but are not limited to smart thermostat [16], smart locks [17], fire detection and prevention systems [18], [19], smart energy management system [20] and so on. Smart homes can be equipped with hundreds of heterogeneous devices and sensors for monitoring different physical parameters and the data generated by these sensors/devices can be processed to make intelligent decisions. In a recent work [21], state-of-the-art machine learning and data mining approaches used for learning from data generated in smart homes have been explored.

In the literature, it can be seen that the researchers are primarily concerned about the security, privacy and authentication issues in smart homes. Different research has been performed to address different cyber-security issues in smart homes. A survey on smart home security-related research can be found in [22]. Similar to security, safety is a critical non-functional property of a system. In many areas, such as the automotive and aerospace industries, significant efforts have been made to provide safety assurance. However, as mentioned in [23], despite the rapid growth of the IoT industry, the safety and reliability-related research for IoT is still in its early stage. Consequently, research on safety assurance in smart homes is a less explored area. There exists some related works such as fault diagnosis for smart homes [24]–[26]. In [27], fuzzy logic has been used in an agent-based approach for anomaly detection in sensor networks of smart homes. Doan *et al.* [28] described the cloud-based smart home platforms and then discussed the reliability, security and safety implications of the unavailability of the cloud services on smart home users.

Chen and Helal [29] proposed a device-centric, domain independent approach for addressing safety issues in IoT systems. In their approach, they proposed a domain independent ontology to define vocabulary relevant to safety and then used a device description language to define safety constraints for sensors and actuators. In [30], a tool has been presented based on fault tree analysis (FTA) [31] for dependability analysis of IoT in early planning and design phases. Among different attributes of dependability, their approach considers reliability and availability only. Concepts like safety and real-time monitoring for assuring safety were not considered. In a method called SOTERIA [32], the state-space model of an IoT app is extracted from the source code and then model checking is applied on the state-space model to find whether the app conforms to predefined safety and security properties. Similar to this approach, another model-checking-based approach was proposed in [7]. In [33], FTA has been used for risk assessment of a lighting system within a smart home environment. The primary focus of this study was the security attacks that can be performed on the studied system. Using traditional approaches, safety analysis of IoT-enabled systems is performed during development time based on static architectures of the systems. As new devices can be easily added or removed to/from IoT-based systems during operation, the architecture of such systems can change dynamically during system operation. Therefore, safety assurance for such systems needs to be provided continuously during runtime considering their evolving nature and dynamic operating environment.

III. Safety Assurance Framework for IoT-Enabled Smart Homes

Fig. 1 shows the proposed framework for safety assurance of IoT-enabled smart systems. The framework contains ten different steps. The first seven steps D1 to D7 are performed at system design and development time and the remaining three steps R1 to R3 are continuously carried out during system operation. In two stages, the steps are carried out as follows.

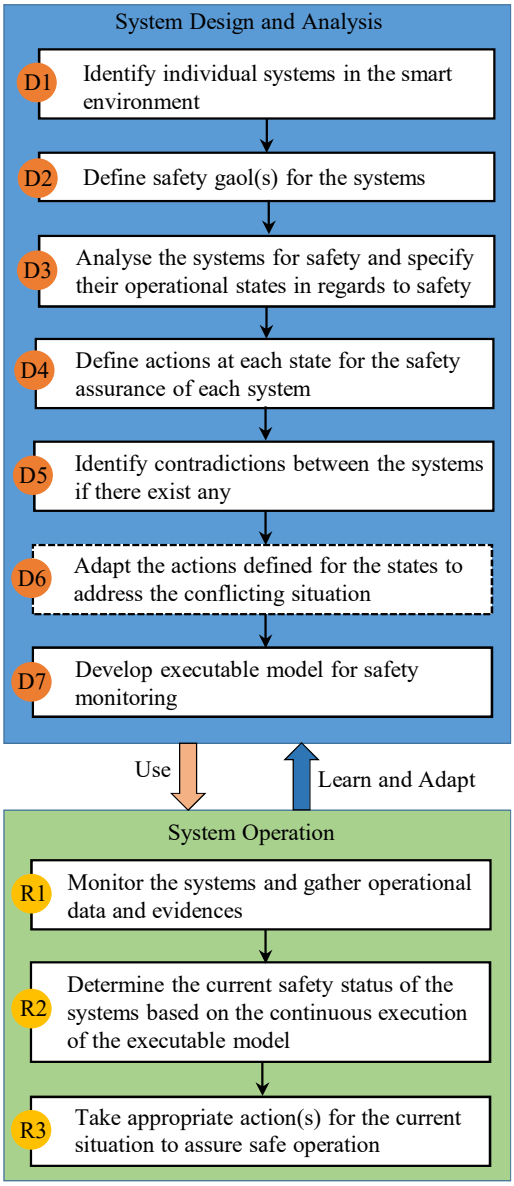

Fig. 1: Steps of the proposed framework

A. System Design and Analysis

Step D1: As multiple systems can operate simultaneously in a single smart environment, this step identifies the individual systems. These systems may work independently or they may work in collaboration to achieve some common goals.

Step D2: As the primary goal of the proposed framework is to provide safety assurance, this step defines the safety goal(s) for each of the systems residing in the smart environment.

Step D3: Once the safety goals are defined, in this step, the architecture of all systems and their nominal and failure behaviour are studied to specify the potential states that the system can be in during the operation with regards to safety. For architecture modelling and analysis, meta-models such as the one mentioned in [34] can be considered. For failure behaviour analysis, safety analysis artefacts like FTA can be used.

Step D4: In this step, concerning the predefined safety goals, safety statuses of the systems in each of the previously identified states are determined. In terms of safety, the system states can have varying levels of criticality, i.e., one state of a system can be more critical than another state. The criticality of a state can be determined based on the safety concerns in that state, i.e., what is the likelihood of reaching a hazardous situation from a particular state. Depending on the criticality of the states in terms of safety, actions are defined for each state such that safety can be assured in any system state. In other words, actions are defined to reduce or to eliminate unacceptable, i.e., unsafe risk of operation at any point in time. The nature of the execution of these actions largely depends on the specific application. For example, some actions may be provided as recommendations to human operators, others may be input for automated controls.

Step D5: Based on the outcomes of steps D1, D2, and D3, this step will identify the contradictions between the systems (identified in D1) by considering the smart environment as a system of systems. Note that multiple independent systems

may work simultaneously in a single environment without conflicting with each other. In such cases, this step will not find any conflict.

Step D6: This step depends on the outcome of step D5. If conflicts were identified in D5, this step will revisit the actions defined in step D4 to adapt them to address the conflicts while assuring the safety of the whole system.

Step D7: This step is to develop an executable model for safety monitoring such that it can be continuously executed during system operation to identify the system state given the inputs from the components. Therefore, the precondition of developing such an executable model is to identify necessary inputs/conditions that must be verified during system operation to determine the system state. Once such inputs/conditions are known, a logical model can be developed to process them to reach a decision.

Bayesian Network (BN) has been widely utilised for safety monitoring in different areas such as in [10], [11]. In the proposed framework, as an executable model, we utilise the modelling capacity of BN to form the logical structure of the safety monitor (see Fig. 2). Note that other state-space based models such as state machines, Markov chain, and Petri nets can also be used for the same purpose. Using BN, the conditional safety state probabilities of the IoT system are formed in terms of cause-effect relationships among the status of the components of the system, i.e., the monitored data. In the BN-based safety monitor, the root nodes (nodes without any parents) represent the operating status (working or failed) of the IoT devices or the output from these devices. For instance, a node may represent that a smoke detection sensor, *SD_Sensor*, is working and another node may represent whether smoke is detected by the *SD_Sensor*. The status of these nodes affects the status of their child nodes. In this way, the effects are propagated towards the top node (node without any child) to signify the effects of the operating state of the components on the operating state of the whole system.

B. System Operation

In an IoT-enabled environment, smart sensors report their observations about the environment (e.g. temperature reading) and their health status to a central hub. The hub processes the information to determine the actuation actions, e.g., turn on/off the central heating system of a smart home based on the temperature of the home. In this article, we consider that the executable safety monitoring model developed in step D7 will reside in the hub. Note that the safety monitor will only be responsible for safety assurance, whereas the hub will be responsible for all other functional and non-functional requirements of the system. Following are steps that are repetitively performed during system operation to provide continuous safety assurance.

Step R1: During operation, the safety monitoring system will monitor the health and the output of IoT devices. As seen in Fig. 2, during system operation, inputs are provided by the IoT devices to the safety monitor (represented by the green arrow). These inputs are considered as runtime evidence and are used in the next step to determine the safety status of the systems.

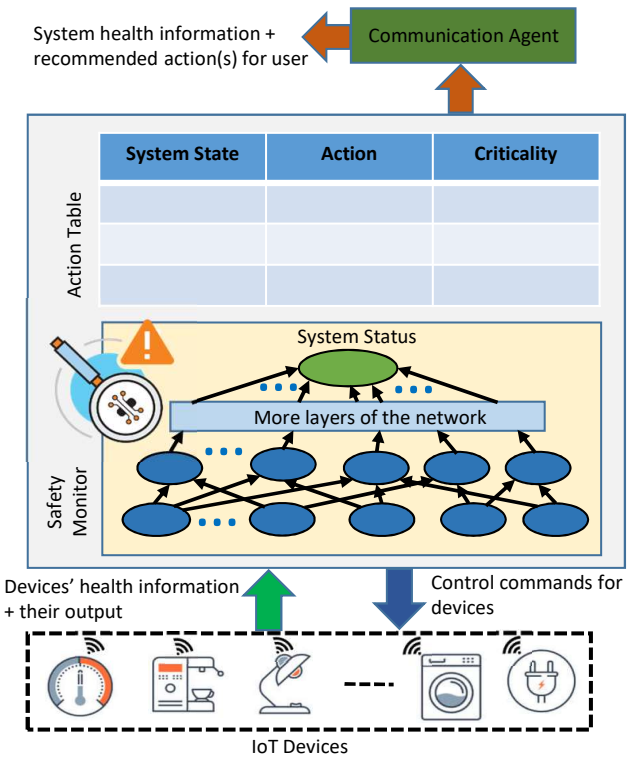

Fig. 2: Online monitoring and assurance provision process

Step R2: In this step, the executable model will be executed at a regular interval utilising the evidence collected in step R1 to update the knowledge about the current operational state of the system.

Step R3: Based on the safety status of the system, the monitor will trigger interventions to ensure the safety of the system. When the current operational state of the system is known to the monitor, it will select appropriate action(s) for the current state from the predefined set of actions. As seen in Fig. 2, these actions can either be some controlled command to the IoT devices or some recommendations to the user external to the system.

C. Security Consideration in the proposed safety monitoring framework

Usually, we need support from a communication agent for any external communication. Different security issues can be raised during external communications. In this context, an attacker may try to gain access to the system by using a false identity (spoofing) or may try to alter the messages communicated between a legitimate user and the IoT system. For instance, a successful alteration of any critical message related to the safety status of the IoT system and/or recommended urgent actions communicated by the safety monitor to the user may lead to unexpected hazardous situations. Therefore, it is important that security measures are put in place to avoid any safety issues caused by security breaches. At the same time, to ensure security against some internal threats, physical security of the IoT devices is also required to be considered. In this section, we describe some of the imperative security

measures (such as resilience against impersonation or message tampering attacks etc.) to prevent various security attacks in the proposed safety monitoring framework.

To ensure security against any spoofing attack in the proposed framework, a secure authentication mechanism is required. In general, there are two roles in the authentication protocol, namely the sender (prover, denoted as P) and the receiver (verifier, denoted as V). P authenticates a message m to V. The fundamental security requirements of the authentication protocol are the *Completeness* and *Unforgeability*.

- *Completeness:* V accepts the authentication for the message m with overwhelming if both P and V follow the authentication protocol honestly.
- *Unforgeability:* This property states that an attacker $\mathcal{A}$ can not pretent to be the sender P to complete authentication. Consider the propabilistic polynomial time attacker $\mathcal{A}$ trying to forge a message . It adaptively chooses a sequence of arbitary messages m_1,m_2,... and asks some good participant P_i to validate m_i. We say that $\mathcal{A}$ succeeds if V accepts $\mathcal{A}$'s authentication message $m \notin m_i$ as P_i and $\mathcal{A}$ does not have P_i's secret. The authentication (unforgeability) requirements is that the probability of success of $\mathcal{A}$ is negligible.

On the other hand, to ensure security against any message tampering attacks, a secure message authentication code (MAC) or key-hashed can be applied. In this regard, both the MAC and key-hash are expected to generate an unforgeable tag based on a given data/message. The receiving end needs to verify the tag to find any alteration of the original message. Finally, to ensure security again any physical tampering of the IoT devices, we suggest using the PUF (physically unclonable function)-enabled devices [35], where PUF can be considered as a digital fingerprint and defined as a unique identity for a device. In this regard, any changes in device settings will significantly affect the PUF-circuit of the device and after that, the device will not be able to generate the intended output. In this way, any legitimate user of the device will be able to identify the issue. However, PUFs are vulnerable to machine learning based modeling attacks that can mathematically clone the PUFs in order to impersonate them. In order to resolve such issues, the concept of reconfigurable one-time PUF [35] [36] can be adapted.

IV. Illustrative Example

A. System model and description

To illustrate the effectiveness of the proposed safety monitoring framework, we use the example of an IoT-enabled smart home environment shown in Fig. 3. In this system, we considered two distinct cases. In the first case, we consider that the smart home environment contains a Fire Detection System (FDS). The FDS has separate battery-powered smoke and temperature sensing units. These sensing units report their observations to the smart hub. The behaviour of the FDS is defined as such that if smoke is detected by the smoke sensor, then the smart hub will raise an alarm and notify the user about this. In conjunction with the smoke, if the temperature of the room is detected to be higher than a predefined threshold, then the smart hub considers there is a fire, thus turning on the sprinkler system to stop the fire. At the same time, an alarm is raised and the user is notified. Note that in normal operating conditions, the water shut off valve is always open to maintain the water supply to different parts of the home. However, the sprinkler system is off by default but can be turned on when necessary. In this case, the inclusion of the water sprinkler system in the smart home environment is a safety measure (i.e. protection method) to prevent the fire from spreading. In the second case, we consider that there exists a leak detector system (LDS) together with the FDS in the smart home. The task of LDS is to detect leaks in the home and report them to the smart hub. Upon detection of a leak, in addition to notifying the user, the smart hub turns off the water shut off valve to stop water dripping by stopping the water supply to the whole house.

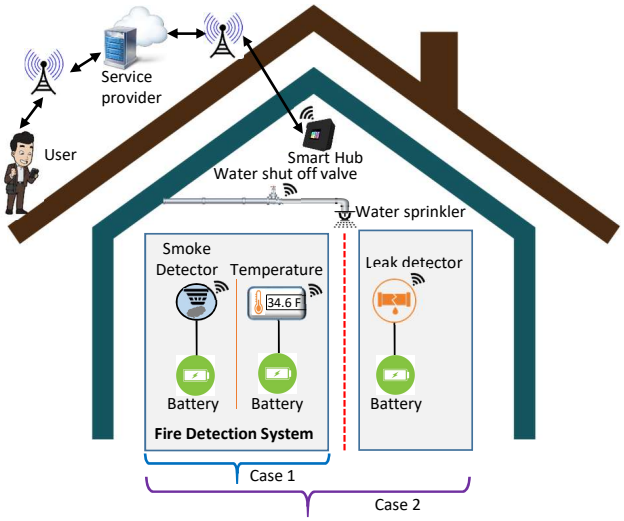

Fig. 3: IoT-based Smart Home Environment

B. Design Time Analysis and Monitor Design

While designing a safety monitor for the above-mentioned IoT-based smart home environment, we assume that the communications between the sensor devices and the smart hub within the home are secure, and the water shut off valve and the sprinkler system are reliable, thus not considered during the monitor design. According to the process described for step D2 in section III-A, we defined the following two safety goals.

1) When there is a fire, it should be detected and the sprinkler system should be turned on to stop the fire.
2) If a leak is detected, the water shut off valve should be closed to stop the water leak.

The first safety goal is for the FDS and the second one is for the LDS. With respect to these safety goals, we have analysed the architecture and the nominal and the failure behaviour of these systems separately to identify the states that they can be in during operation. Tables I and II show the states and their description for the FDS and LDS, respectively. Safety goals can be violated for many different reasons, including

random hardware failure and/or bad interactions between the applications. For instance, a failure of the FDS will cause a fire incidence to go undetected, leading to a non-activation of the sprinkler system, thus violating the first safety goal. Similarly, the failure of the LDS will violate the second safety goal. Note that the two potential reasons for safety goals violation are due to the physical failure of the system components. In such cases, the safe operation of the system can only be guaranteed by restoring the functionality of the failed component either by repairing or replacing them.

TABLE I: States and actions for the fire detection system

State	Description	Action
S0	Both smoke and heat detector units are working. Nothing detected.	If either the alarms or the sprinkler or both were on, then turn them off.
S1	Both units are working and smoke detected.	Turn on the smoke alarm and notify the user.
S2	Both units are working, and smoke and heat detected.	Turn on the fire alarm and sprinkler, and notify the user. Note: this case may find that the alarm is already on, so keep it on.
S3	Only the smoke detector is working and nothing detected.	Inform the user about the failure of the heat detector.
S4	Only the smoke detector is working and smoke detected. As smoke is detected, there is a very high chance that there is fire, but as the heat detector has failed, the fire will go undetected. Hence, sprinkler would not be turned on.	Turn on the smoke alarm and **urgently** informthe user about the failure of the heat detector.
S5	Only the heat detector is working and nothing detected.	Inform the user about the failure of the smoke detector.
S6	Only the heat detector is working and heat detected. As the smoke detector was failed, there is a high chance that there was smoke which gone undetected.	Turn on the fire alarm and sprinkler, and notify the user.
S7	Both units failed. No detection possible.	Urgently inform the user to restore devices' functionality.

To ensure the safe operation of the FDS and LDS, actions are defined for each state to ensure that safety goals are satisfied in each of them. Actions defined in Table I are to assure safe operation of FDS, whereas actions in Table II are for safety assurance of LDS. For instance, in Table I, state S0 represents a scenario where both smoke and heat (temperature) detection units within the FDS are working, hence the criticality of this state is very low as there is no chance of violating the safety goal. Therefore, in this state, no critical action is recommended. On the other hand, in state S7, both smoke and heat detectors are not working, meaning that any fire in this state will not be detected, thus will violate the safety goal. Therefore, urgent action is recommended to the user to restore the functionality of the sensors so that the safety goal can be guaranteed. Similarly, according to the criticality of the states concerning the safety goals, appropriate actions are defined for all states. For LDS, state LS2 is the most critical one because in this state the leak detector sensor is in the failed state, thus will not be able to detect any leak, which will lead to the violation of safety goal 2. It can be seen that in the states where any system component is in a failed state, it is possible to provide the user with the exact information about the failed component, therefore, the user can instantly know which parts of the system require a repair.

TABLE II: States and actions for the leak detection system

State	Description	Action
LS0	Leak detector is working and no leak detected.	No action required by the leak detector system.
LS1	Leak detector is working and a leak is detected.	Close the water shut off valve and inform the user.
LS2	Leak detector failed.	Notify the user about the failure.

As seen in Tables I and II, the violation of safety goals is due to hardware failures. However, if there exist contradictory goals among the subsystems, then even the nominal behaviour of system components can cause the violation of safety goals. If this is the case, the safety monitor should give priority to the most critical goals and take action accordingly. According to step D5 shown in Fig. 1, we have identified a contradiction between FDS and LDS. According to the states tables, there will be a contradiction when the FDS is in state **S2** and LDS is in state **LS1**. In S2, due to the detection of a fire, the FDS will turn on the sprinkler. At the same time, the LDS will be in LS1 because it will detect a leak due to the sprinkling of water and LDS will shut off the water valve causing the sprinkler to stop working. This will cause a violation of the safety goal 1. In this case, the safety assurance process has to make a trade-off between the goals and prioritise the action of FDS and keep the sprinkler on, while suppressing the action of LDS. To automatically address this conflicting situation, we have adapted some actions and created some additional sub-states as shown in Table III.

An executable model of the monitor is formed as a BN and shown in Fig. 4. In this model, the sub-models within the red and purple boundaries are for determin-

TABLE III: Supplementary sub-states and actions to address conflicting situations

State	Description	Action
SS0	Leak detector is working. Either no leak is detected or a leak is detected because of the activation of the sprinkler system by the fire detection system.	No action is required by the leak detector system. Follow the state and action suggested for the fire detection system.
SS1	Leak detector is working and a leak is detected. This leak is not due to the activation of the sprinkler system.	Turn off the main valve and inform the user. Additionally, follow the state and action suggested for the fire detection system.
SS2	Leak detector failed.	In addition to following the state and action suggested for the fire detection system, inform the user about the failure of the leak detector.

ing the states of the FDS and LDS, respectively. For instance, in the sub-model for the FDS system, the top node `(FireDetectionSystemStates)` represents the states of the FDS system. The state of this node is dependent on the states of nodes `SmokeStatus` and `TemperatureStatus`, i.e., the status of the smoke and heat detection units. The state of the node `SmokeStatus` depends on the states of nodes `IsSmokeDetected?` and `StatusOfSDUnit` (a short form of status of smoke detection unit). The state of `IsSmokeDetected?` node can either be *YES* or *NO* depending on whether smoke is detected by the smoke sensor. On the other hand, the node `StatusOfSDUnit` can either be in *Working* or *Failed* state depending on whether the `StatusOfSmokeDetector` (operating status of the smoke sensor within the smoke detection unit) and `StatusOfSDBattery` (operating status of the battery within the smoke detection unit) are in *Working* or *Failed* state.

C. Online Monitoring

During system operation, the readings obtained from the sensors and their health statuses are used as inputs in the executable model of Fig. 4 to determine the status of the system and take appropriate actions to ensure safe operation. In the illustrative scenario shown in Fig. 4, the FDS is in state **S2** and LDS is in state **LS1**. According to Table I, state S2 refers to a scenario when both smoke and heat detector sensors are working, and both smoke and heat are detected by the respective sensor. According to the predefined action for state S2, the monitor will raise the fire alarm, notify the user, and turn on the sprinkler. On the other hand, as seen in Table II, the state LS1 of LDS refers to a case where the leak detector is working and detected a leak. Action for this state recommends shutting off the main water valve. As mentioned before, it is a contradiction between the FDS and LDS. In other words, one action recommends turning on the sprinkler (open water shut off valve is a precondition for the success of this action), whereas the other action recommends shutting off the water valve. In this case, if the water valve is closed eventually then safety goal 1 will be violated, whereas if the water valve is open then safety goal 2 will be violated. As mentioned before, this is a case when the nominal behaviour of subsystems causes safety goal violation and the monitor should take care of this case by making a trade-off between the goals by utilising the supplementary states shown in Table III. In the BN model, the supplementary states are represented by node `SystemSubStates`. As mentioned in table III, these supplementary states will supersede the states for LSD. Therefore, for the demonstrated scenario in Fig. 4, the FDS system is in state S2 and the system sub-state is SS0. Because of this, according to the actions defined in tables I and III, the sprinkler system will be turned on and the leak detection will take no action, even if it detects a leak because a fire hazard is more dangerous than a hazard caused by a water leak.

To test whether the monitor can detect different scenarios based on its monitoring knowledge and recommend appropriate actions, we randomly populated several test cases and tested the proposed monitor. For the sake of brevity, in Table IV, we reported the results of ten of those test cases (C1 to C10). For instance, case 1 (C1) represents a scenario when both FDS and LDS are working and in terms of detection, the smoke sensor detects smoke, the temperature reading is below the threshold value and no leak is detected. The monitor determines the states of the system as **S1** and **SS0**, and suggests action(s) based on predefined actions for these states. According to the description of the states in tables I and III, the monitor correctly identifies the scenario and makes the correct decision to assure safe operation. Similar to this case, as can be seen in Table IV, the monitor was able to detect the states of the system with respect to the defined safety goals in all the illustrated cases, thus was able to take appropriate actions.

D. Comparison with other approaches

As explained in II, although there exist several studies to address security, privacy and authentication issues in smart homes, there are very few studies on safety assurance of IoT-enabled smart homes. Most of these studies are performed at design/development time, hence, are not applicable to provide continuous safety assurance based on online monitoring. The proposed approach alleviates this issue by enabling continuous safety assurance through real-time monitoring of different system parameters. Although the existing approaches were not developed for the same purposes, and they have their own strengths and weaknesses, Table V shows a high-level comparison between different existing approaches based on their features. As seen in the table, the proposed approach

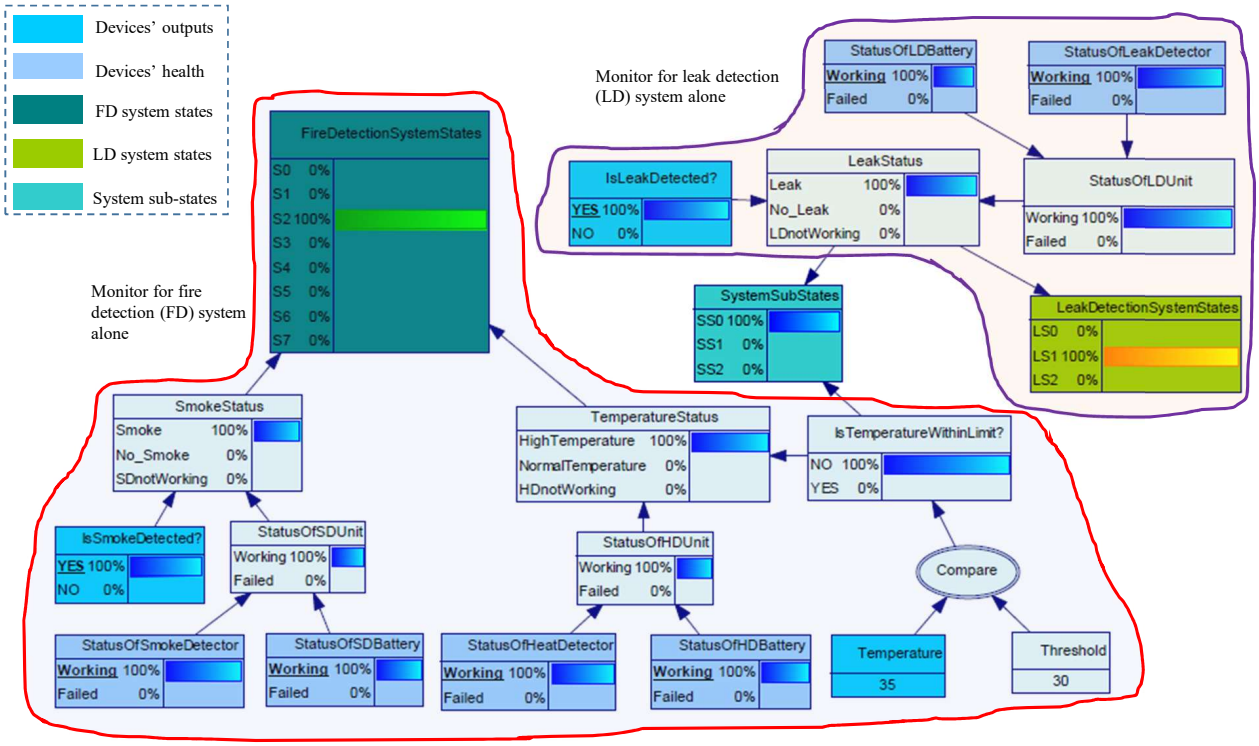

Fig. 4: BN model of the safety monitor of the IoT-enable smart home environment

TABLE IV: Results of the testing of the safety monitor

Parameters	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**
StatusOfSmokeDetector	W	W	F	W	W	W	W	W	W	W
StatusOfSDBattery	W	F	W	W	W	W	F	W	W	W
IsSmokeDetected?	Y	N	N	Y	Y	N	N	N	Y	Y
StatusOfHeatDetector	W	W	W	W	F	F	W	W	W	W
StatusOfHDBattery	W	W	F	W	W	W	W	W	W	F
Temperature (°C)	25	25	27	42	29	27	45	25	30	25
TemperatureThreshold (°C)	35	35	35	35	35	35	35	35	35	35
StatusOfLeakDetector	W	W	W	W	W	W	W	W	W	W
StatusOfLDBattery	W	W	W	F	W	W	W	F	W	W
IsLeakDetected?	N	Y	N	N	N	N	Y	N	Y	Y
States determined	**S1 SS0**	**S5 SS1**	**S7 SS0**	**S2 SS2**	**S4 SS0**	**S3 SS0**	**S6 SS0**	**S0 SS2**	**S1 SS1**	**S4 SS1**

*W: Working, F:Failed, Y:YES, N:No

is the only approach that provides runtime safety assurance. Compared to some approaches, the proposed approach currently does not have a dedicated tool support to perform the analysis. In the future we will consider developing a dedicated tool to facilitate the analysis.

V. Conclusion

Due to design flaws, failure of hardware and/or software, undesired interactions between installed devices and/or apps, and communication failure can cause an IoT-enabled smart environment to reach hazardous states. In this article, we presented a novel safety assurance framework that can continuously monitor the states of the IoT devices to ascertain the safety status of the systems and thereby recommends appropriate actions to ensure the safe operation of the systems. Our evaluations show that the proposed approach can successfully identify the states of the system based on the monitoring knowledge. The monitor can detect hazardous states that can be reached either due to the failure of devices or due to conflicting goals of the devices. Currently, in the proposed framework, actions to address safety issues are organised in a tabular format. The action rules may become more complicated as the system becomes larger, which may undermine the scalability of the proposed approach. We are currently working on a more efficient representation of actions so that the scalability of the proposed approach can be improved.

TABLE V: Comparison of features of existing approaches and the proposed approach

Approaches	Features				
	F1	**F2**	**F3**	**F4**	**F5**
Nguyen *et al.* [7]	✔	✗	✔	✔	✔
Celik *et al.* [32]	✔	✗	✔	✔	✔
Silva *et al.* [30]	✔	✗	✔	✗	✗
Chen and Helal [29]	✔	✗	✔	✗	✗
Wongvises *et al.* [33]	✔	✗	✔	✔	✗
Proposed Approach	✔	✔	✔	✔	✔

F1: Offline Failure Analysis; **F2:** Runtime monitoring and assurance; **F3:** Device centric approach; **F4:** Security awareness; **F5:** Resolution for contradiction between subsystems

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 195–212.

[3] K. Fu, T. Kohno, D. Lopresti, E. Mynatt, K. Nahrstedt, S. Patel, D. Richardson, and B. Zorn, "Safety, security, and privacy threats posed by accelerating trends in the internet of things," *Computing Community Consortium (CCC) Technical Report*, vol. 29, no. 3, 2017.

[4] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 636–654.

[5] M. Orcutt, "Security experts warn congress that the internet of things could kill people," *MIT Technology Review*, vol. 15, p. 2019, 2016.

[6] M. Machin, J. Guiochet, H. Waeselynck, J.-P. Blanquart, M. Roy, and L. Masson, "SMOF: A safety monitoring framework for autonomous systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 702–715, 2016.

[7] D. T. Nguyen, C. Song, Z. Qian, S. V. Krishnamurthy, E. J. Colbert, and P. McDaniel, "IoTSAN: fortifying the safety of IoT systems," in *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*. ACM, 2018, pp. 191–203.

[8] B. Bisenius, "Product Safety of the Internet of Things [Product Safety Perspectives]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 137–139, 2017.

[9] T. Kohda and W. Cui, "Risk-based reconfiguration of safety monitoring system using dynamic bayesian network," *Reliability Engineering & System Safety*, vol. 92, no. 12, pp. 1716–1723, 2007.

[10] S. Kabir and Y. Papadopoulos, "Computational intelligence for safety assurance of cooperative systems of systems," *Computer*, vol. 53, no. 12, pp. 24–34, 2020.

[11] S. Kabir, I. Sorokos, K. Aslansefat, Y. Papadopoulos, Y. Gheraibia, J. Reich, M. Saimler, and R. Wei, "A Runtime Safety Analysis Concept for Open Adaptive Systems," in *International Symposium on Model-Based Safety and Assessment*. Springer, 2019, pp. 332–346.

[12] R. Calinescu, D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli, and T. Kelly, "Engineering Trustworthy Self-Adaptive Software with Dynamic Assurance Cases," *IEEE Transactions on Software Engineering*, vol. 44, no. 11, pp. 1039–1069, 2018.

[13] D. Schneider and M. Trapp, "Conditional Safety Certification of Open Adaptive Systems," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 8, no. 2, pp. 1–20, 2013.

[14] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[15] S. Kabir, "Internet of Things and Safety Assurance of Cooperative Cyber-Physical Systems: Opportunities and Challenges," *IEEE Internet of Things Magazine*, vol. 4, no. 2, pp. 74–78, 2021.

[16] J. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben, J. Stankovic, E. Field, and K. Whitehouse, "The smart thermostat: using occupancy sensors to save energy in homes," in *Proceedings of the 8th ACM conference on embedded networked sensor systems*, 2010, pp. 211–224.

[17] Y.-C. Yu, "A practical digital door lock for smart home," in *IEEE International Conference on Consumer Electronics*, 2018, pp. 1–2.

[18] F. Saeed, A. Paul, A. Rehman, W. H. Hong, and H. Seo, "Iot-based intelligent modeling of smart home environment for fire prevention and safety," *Journal of Sensor and Actuator Networks*, vol. 7, no. 1, p. 11, 2018.

[19] K. C. Lee and H.-H. Lee, "Network-based fire-detection system via controller area network for smart home automation," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 4, pp. 1093–1100, 2004.

[20] J. Han, C.-s. Choi, and I. Lee, "More efficient home energy management system based on zigbee communication and infrared remote controls," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 1, pp. 85–89, 2011.

[21] M. Antić, I. Papp, S. Ivanović, and M. Matić, "Learning from smart home data: Methods and challenges of data acquisition and analysis in smart home solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 3, pp. 64–71, 2020.

[22] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[23] L. Xing, "Reliability in internet of things: Current status and future perspectives," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6704–6721, 2020.

[24] J. Lee, J. Kim, J.-Y. Son, and J.-H. Park, "Autonomous fault diagnosis for smart home network services," in *Second International Conference on Consumer Electronics*, 2012, pp. 216–217.

[25] J. Son, J. Lee, J. Kim, J. Park, and Y. Lee, "RAFD: Resource-aware fault diagnosis system for home environment with smart devices," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1185–1193, 2012.

[26] J. Liao, C. Zhang, T. Li, and X. Zhu, "An efficient fault diagnosis technique for home unified service system," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1487–1494, 2010.

[27] M. Usman, V. Muthukkumarasamy, and X. Wu, "Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 2, pp. 197–205, 2015.

[28] T. T. Doan, R. Safavi-Naini, S. Li, S. Avizheh, and P. W. Fong, "Towards a resilient smart home," in *Proceedings of the 2018 Workshop on IoT Security and Privacy*, 2018, pp. 15–21.

[29] C. Chen and S. Helal, "A Device-Centric Approach to a Safer Internet of Things," in *Proceedings of the 2011 International Workshop on Networking and Object Memories for the Internet of Things*, 2011, p. 1–6.

[30] I. Silva, R. Leandro, D. Macedo, and L. A. Guedes, "A dependability evaluation tool for the internet of things," *Computers & Electrical Engineering*, vol. 39, no. 7, pp. 2005–2018, 2013.

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

[32] Z. B. Celik, P. McDaniel, and G. Tan, "SOTERIA: Automated IoT Safety and Security Analysis," in *Proceedings of the 2018 USENIX Annual Technical Conference*, 2018, pp. 147–158.

[33] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, "Fault tree analysis-based risk quantification of smart homes," in *2nd International Conference on Information Technology (INCIT)*. IEEE, 2017, pp. 1–6.

[34] J. Rauscher and B. Bauer, "Safety and security architecture analyses framework for the internet of things of medical devices," in *IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2018, pp. 1–3.

[35] P. Gope and B. Sikdar, "A comparative study of design paradigms for puf-based security protocols for iot devices: Current progress, challenges, and future expectation," *Computer*, vol. 54, no. 11, pp. 36–46, 2021.

[36] ——, "A privacy-aware reconfigurable authenticated key exchange scheme for secure communication in smart grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5335–5348, 2021.