applied sciences

MDPI

Article

An Accident Model with Considering Physical Processes for Indoor Environment Safety

Zhengguo Yang *, Yuto Lim and Yasuo Tan

School of Information Science, Japan Advanced Institute of Science and Technology 1-1 Asahidai, Nomi, Ishikawa 923-1292, Japan; ylim@jaist.ac.jp (Y.L.); ytan@jaist.ac.jp (Y.T.)

* Correspondence: yangzg@jaist.ac.jp

Received: 15 September 2019; Accepted: 1 November 2019; Published: 6 November 2019

Abstract: Accident models provide a conceptual representation of accident causation. They have been applied to environments that have been exposed to poisonous or dangerous substances that are hazardous in nature. The home environment refers to the indoor space with respect to the physical processes the of indoor climate, e.g., temperature change, which are not hazardous in general. However, it can be hazardous when the physical process is in some states, e.g., a state of temperature that can cause heat stroke. If directly applying accident models in such a case, the physical processes are missing. To overcome this problem, this paper proposes an accident model by extending the state-of-the-art accident model, i.e., Systems-Theoretic Accident Model and Process (STAMP) with considering physical processes. Then, to identify causes of abnormal system behaviors that result in physical process anomalies, a hazard analysis technique called System-Theoretic Process Analysis (STPA) is tailored and applied to a smart home system for indoor temperature adjustment. The analytical results are documented by a proposed landscape genealogical layout documentation. A comparison with results by applying the original STPA was made, which demonstrates the effectiveness of the tailored STPA to apply in identifying causes in our case.

Keywords: STAMP; STPA; physical process; indoor environment safety; smart home systems

1. Introduction

Accident models provide a conceptual representation of accident causation [1]. Their state-of-the-art development is on the phase of systemic models [1–3], i.e., accident models based on system theory rather than reliability. They were specifically applied to understand accidents in industrial areas, e.g., deepwater well control [4], railway [5], and aviation [6]. Some others relate to places that have been exposed to poisonous or dangerous substances, e.g., oil transportation [7] and nuclear power plants [8]. These poisonous or dangerous substances are hazards in nature, which can directly cause harm when leaked or released in workplaces. The workplace is a strictly managed environment for work. Safety-critical systems are taken as preventative measures for leakage and release.

The home environment refers to the indoor space with respect to physical processes of indoor climate, e.g., temperature change, which is different from safety-critical environments in workplaces. Hereafter, we use physical process to represent the physical process of indoor climate. The home environment is not a hazardous place in general. However, it can become hazardous when the physical process transfers from a normal state (e.g., temperature for thermal comfort), then through some intermediate states (e.g., temperature for thermal discomfort), finally reaching a hazardous state (e.g., temperature for heat stroke). The home environment is a place for everyday living, and it is not as strictly managed as that in workplaces. Smart home systems are developed to maintain the home environment in desired states, not only as preventative measures.

In systemic accident models [1–3], accidents are the result of the violation of a set of constraints on the behaviors of the system components, i.e., management, humans, and technology. If directly applying a systemic accident model to the smart home system, the information of physical processes is missing. For example, a smart home system violated its constraint on adjusting the indoor temperature for thermal comfort, and resulted in high temperature for heat stroke. The physical process of temperature change from one of thermal comfort, to some intermediate states for discomfort, then to a high-temperature state that can cause, e.g., heat stroke, is missing. This process is important. First, it assists in understanding how system behaviors could result in accident through intermediate state(s). Second, we need the anomalies' information of the physical process and their causes to deploy reactions and precautionary measures. We can take advantage of hazard analysis techniques to identify the causes in the system to the anomalies. When an intermediate abnormal state or hazardous state of the physical process is detected, with considering the corresponding causes in the system, an effective precautionary or reaction measures can be selected. Generally, if something undesired is not considered in the very beginning of risk analysis, the causes in the following analysis cannot be identified [2,9]. Therefore, it is necessary to extend the systemic accident model by including the physical process.

A newly developing systemic accident model, i.e., Systems-Theoretic Accident Model and Process (STAMP) [2], is considered in this paper, as its underlying rationale has been widely acknowledged by comparing with other systemic accident models [10]. It is based on general system theory for understanding accident causality of sociotechnical systems. A brief introduction of it is presented in Section 3.1. We extend it by considering the following facets. First, the home environment is not inherently hazardous. It can ensure a comfortable life in some physical process states and cause harms in others. Therefore, we take the physical process into account in understanding accident formation. Second, the indoor environment is greatly affected by the behaviors of smart home systems. This is because physical processes are the result of smart home systems and the outdoor climate. However, in a limited period, e.g., days, the outdoor climate can be considered with no big changes. Third, the role of people in the home environment. The characteristics of workers in workplaces and occupants in the home environment are different.

In this paper, we extend the STAMP model with considering physical processes (hereafter denoted by STAMP-PP) to understand accident formation. Smart home systems interact with the home environment through its behaviors, e.g., warm up and cool down. Thus, the STAMP-PP connects the physical world through the behaviors of the systems. Under this consideration, accidents are the result of the violation of a set of constraints on the behaviors of the systems to cause abnormal changes in physical processes, and finally result in personal harm. The extended STAMP-PP model demonstrates accident formation with respect to system behaviors and physical processes. The system behaviors can be controlled either by the smart home system directly or by occupants indirectly.

The information related to physical processes is important, and the abnormal behaviors of systems under specific operation scenarios must be known to select the appropriate reactions and precautionary measures. To this end, hazard analysis techniques [9,11] that can assist in analyzing potential causes of accidents are required. We adopted a hazard analysis technique to identify causes of abnormal system behaviors under related operation scenarios, which can result in abnormal changes in physical processes. A new approach to hazard analysis, called System-Theoretic Process Analysis (STPA) [2,9], is based on the STAMP model, and it is tailored and applied to the smart home system [12] for adjusting the indoor temperature, to demonstrate how to identify causes to abnormal system behaviors that result in physical process anomalies. The STPA can be used to identify unsafe control actions of a controller and are also the reasons why unsafe control actions can happen under specific scenarios. As abnormal behaviors of smart home systems that result in intermediate states of physical processes are also considered, the STPA is then tailored also for identifying causes to these abnormal behaviors. Landscape Genealogical Layout Documentation (LGLD) is proposed for documenting the analytical results, and the relations among the results are clearly and straightforwardly represented by comparing with conventional ways of documentation, i.e., tables and lists. We compared the results with that of

applying the original STPA, which demonstrate the effectiveness of the tailored STPA in identifying causes of abnormal system behaviors and the LGLD documentation in representing the relations among the results.

The contributions of this paper are as follows.

- We discussed the characteristics of the smart home in the viewpoint of occupants and the safety of the home environment.
- The concept of the Performers System, which emphasizes the behaviors performed by various home appliances, is proposed.
- We propose the STAMP-PP model for understanding accident formation, i.e., abnormal system behaviors that result in abnormal changes in physical processes and cause hazards.
- We tailored the STPA and applied it to a smart home system to identify inappropriate and unsafe control actions that cause abnormal system behaviors, which result in abnormal changes in physical processes, and hazards.
- An LGLD approach is proposed for documenting the STPA analytical results.

This paper extends a conference paper [13] that introduces the STAMP-PP model while considering physical processes. The application of the tailored STPA and the new way of documenting the results in this paper are novel.

The rest of this paper is organized as follows. Section 2 discusses some knowledge about smart home and home environment safety. Section 3 introduces the proposed accident model STAMP-PP. Then, the hazard analysis technique STPA is tailored and applied to a smart home system for indoor temperature adjustment in Section 4. In Section 5, a discussion is given. Section 6 introduces the related work. Finally, Section 7 concludes this paper and points out the future work.

2. Preliminaries

In this section, we discuss the characteristics of the smart home and home environment safety before introducing the STAMP-PP model and the application of the STPA.

2.1. Smart Home

A home is a place for people like individual or family members, etc. to live. It is the sum of the place where people live permanently and the social unit—family. Since the 20th century, with the introduction of electricity, informtion, and communication technologies, great changes have taken place in the home [14]. One representation of this change is the development of the concept of the smart home since the 1990s [15]. The primary objective of the smart home is to increase occupants' comfort and make daily life easier. An example of possible techniques that make a home smart is machine learning [16]. The smart home has certain characteristics [15,17], e.g., adaptability, connectivity, controllability, and computability. These are discussed from the viewpoint of technology. This section discusses the characteristics of the smart home from the viewpoint of occupants.

- Partial Automation: Although home life has been automated a lot more than ever before due to the development of electricity, electronics, and network technologies, there are still elements of our lifestyles that have been left unchanged in practice. For example, pots and pans are used for cooking with gas in everyday meals. Thus, contemporary homes are only partially automated in practice.
- Application Area: The home is a place where people live. Various off-the-shelf products are used to improve the quality of life. These are manufactured by different manufacturers for different purposes. Occupants are not professional in understanding their rationale, particularly that of high-tech products. Occupants only learn to use them through product instructions or other occupants.
- Complexity: The complexity of a home is owing to three aspects, i.e., variety of appliances and products; variety of occupants in terms of age, health condition, knowledge, gender, etc.;

and outdoor environment. Off-the-shelf appliances and products indoors have various purposes and are produced by different manufacturers. In smart homes, they are connected together by the smart home network to enable a variety of services [15,17]. Different from workers in workplaces which rely on skills, rules, and knowledge for a specific job [18], occupants are usually reliant on their own life experiences to lead their lives with respect to various indoor items. Outdoor climate, air quality, etc. can affect the indoor environment, which in turn impacts the working of indoor appliances or devices. All these add to the complexity of the smart home.

2.2. Home Environment Safety

If we refer to a dictionary, the definition of safety could be the condition of being protected from or unlikely to cause harm, injury or loss. In system safety [2], safety is taken as an emergent property of systems. It is defined as freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [19]. However, it cannot be freedom from the conditions in practice. Safety is, thus, the condition of risk that has been reduced to an acceptable level, e.g., as low as reasonably practicable [20]. Home environment safety could be understood as that the risk of indoor climate has been reduced to a level of no harm to the health of occupants.

As is known to all, indoor climate is affected by outdoor climate. Bad weather such as heatwaves has been occurring frequently in recent years due to global warming and weather anomalies around the world. For example, many places globally experienced intense heat in the summer of 2018. It was observed that the highest temperature record in Japan was broken and reached a new level of 41.1 °C (Japan Meteorological Agency [visited 2018.10.03] http://www.jma.go.jp/jma/index.html). Indoor climate can thus be endangered by outdoor climate anomalies.

The indoor climate is adjusted by dedicated home appliances, e.g., use of air-conditioner to adjust indoor temperature. Different home appliances are integrated via home networks that yield value-added integrated services [21,22]. In order to ensure thermal comfort, an indoor temperature adjustment service is an example of the integrated service, which can potentially adopt a window, curtain, and air-conditioning unit. Each involved home appliance may have safety instructions. However, due to the complexity of the smart home, they still could be used in scenarios that cause safety problems. For example, the heating mode of an air-conditioner was used when it should not be. Since the smart home is an application area, appliances inside it may be replaced from time to time. Once an appliance is introduced into the smart home, it also brings about risk. For example, the predefined integrated service may not be aware of the new item and cause safety problems when using it. Therefore, home environment safety depends on the proper use of the indoor climate adjustment service with respect to related home appliances if they were properly designed and manufactured.

To understand home environment safety, we also need to discuss how people relate to the smart home. This is mostly because home appliances are produced and operated by people. One group of people are professionals. These relate to the activities of design, manufacture, transport, installation, and disposal of appliances, home networks, and so on. One distinguishing characteristic is that they have expertise in a certain field. The other group is occupants who are non-professionals. They are the customers who use the various home appliances. Both groups of people can affect home environment safety in different ways. Professionals are responsible for designing, manufacturing, etc. safe systems and home appliances. Occupants care more about operational safety, since they are more error-prone in operations. We talk about occupants in this paper.

3. Accident Model

As the smart home is an application area, the STAMP-PP model is discussed with respect to system operations rather than system development. It aims to understand how accident formation relates to system behaviors in adjusting the home environment, i.e., how abnormal system behaviors cause indoor climate anomalies. Concrete information about indoor climate anomalies can be used for

indoor climate anomaly detection [23], and abnormal system behaviors under operation scenarios can further be used in selecting reactions and precautionary measures when the corresponding indoor climate anomaly is detected.

The STAMP-PP model starts with system behaviors to describe accident formation. The behaviors can result in abnormal changes in physical processes, which can cause discomfort or harm. The connection between smart home systems and the home environment is the system behaviors. In this section, we first give a brief introduction of the STAMP model, then discuss in detail the proposed STAMP-PP model.

3.1. STAMP

In systems theory, systems are viewed as interrelated components kept in a state of dynamic equilibrium through feedback control loops. Figure 1 presents a standard contrl loop [2]. The STAMP model is based on system theory rather than the reliability that traditional accident models are grounded on. Safety, in STAMP, is an emergent property of systems. Accidents are the result of the lack of or inappropriate constraints imposed on the system design and operations. The STAMP model consists of three building blocks, i.e., safety constraints, a hierarchical safety control structure, and process models.

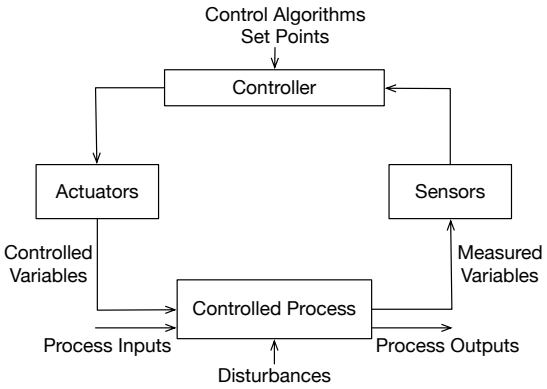

Figure 1. A standard control loop.

Safety constraints are a basic concept in the STAMP model. Losses occur only because safety constraints were not successfully enforced. Systems, in system theory, are viewed as hierarchical structures, where each level imposes constraints on the activity of the levels beneath it. Constraints are enforced by control actions of a higher-level system component (controller) to the lower-level one (controlled process).

The hierarchical safety control structure presents all stakeholders with their internal structures within the system under analysis, and the control actions and feedbacks that link the independent stakeholders and their internal components [6]. Control processes operate between levels of a system to control the processes at lower levels. The feedbacks provide information about how effectively the control actions ensure the constraints are enforced. The higher level uses the feedbacks to adapt future controls to more readily achieve its goals. An accident occurs when control processes provide inadequate control that violates safety constraints. Inadequate control comes from missing constraints, inadequate safety control commands, commands that were not executed correctly at a lower level, and inadequately communicated or processed feedback about constraint enforcement.

Process models are used by the controller to determine appropriate control actions. It is up to the type of the controller. For an automated controller, the process model is embedded in the control logic. For a human controller, the process model is the mental model. In both situations, it contains information of the required relationship among the system variables, the current system state, and the ways the process can change state. There are four conditions required to control a process, i.e., goal,

action condition, observability condition, and model condition. Accidents related to component interaction can usually be explained in terms of an incorrect process model. The process model used by the controller does not match the controlled process that results in interaction accidents.

In the STAMP model, safety is achieved when the behaviors of components of a system appropriately ensured safety constraints. Accidents are the results of flawed processes involving interactions among people, societal and organizational structures, engineering activities, and physical system components that lead to violating the system safety constraints. The process leading up to an accident is described in terms of an adaptive feedback function that fails to maintain safety as system performance changes over time to meet a complex set of goals and values.

3.2. STAMP-PP

Since the STAMP-PP model focuses on the behaviors of systems to affect physical processes, we first define the concept of systems that emphasize behaviors, i.e., Performers System. The reason for choosing the word "performer" is to highlight that the behaviors are performed by the systems. Then, based on the Performers System, we can describe accident formation considering physical processes.

3.2.1. Performers System

The indoor environment is adjusted by indoor environment adjustment services with respect to various home appliances. To differentiate the home appliances with other indoor items, e.g., router or furniture, we define the concept of Performer.

Definition 1 (Performer)**.** *A* performer *is a network-enabled home appliance that can adjust the indoor environment independently.*

There are two points to explain this definition. First, a Performer has networking capability so that it can be used by indoor environment adjustment services. Second, it has functions of adjusting the indoor environment, e.g., adjusting indoor temperature, or dehumidification.

There are two types of Performers based on the way it adjusts the indoor environment. One is direct adjustment, e.g., an air-conditioner which heats or cools indoor air directly; another is indirect adjustment, e.g., an electric window which adjusts, e.g., indoor temperature by introducing an air flow or solar radiation of the outdoor environment. In the latter case, the outdoor climate is passively used to adjust the indoor environment. Then, concept of Performer is used to define the Performers System.

Definition 2 (Performers System)**.** *It is a system of all installed* Performers *in a house that are connected to the same home network.*

By connecting to the same home network, we can ensure that the Performers System can be used by the same indoor environment adjustment service. The Performers System has a goal prescribed by the indoor environment adjustment service. The goal is achieved by taking advantage of the functions of the Performers of the Performers System. Each Performer is taken as a subsystem of the Performers System. However, there is no need to have all related Performers working at the same time. Figure 2 shows an example of the Performers System. It consists of an air-conditioner, an electric window, and an electric curtain, which are taken as Performers. They connect to the same network and have the ability to adjust the indoor temperature. When adjusting the indoor temperature for thermal comfort (the goal), the indoor temperature adjustment service could use any combination of the Performers, but not necessarily all of them. The indoor temperature adjustment service is executed in the smart home system core. The Performers can of course be operated by occupants who are also the beneficiaries of the adjustment.

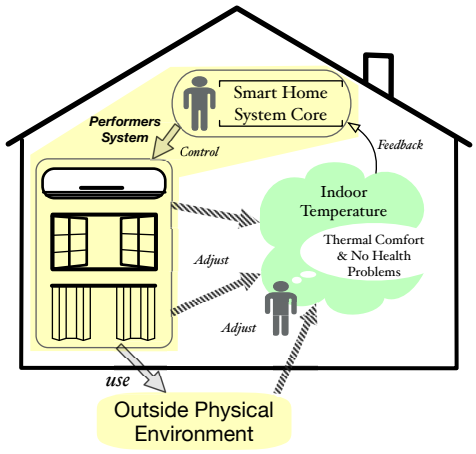

Figure 2. An example of the Performers System.

The Performers System can adjust physical processes with respect to various physical properties, e.g., temperature and humidity, by utilizing the functions the Performers provide. These physical processes may have different forms, for example, increasing or decreasing indoor temperature to the prescribed temperature level for thermal comfort.

3.2.2. Service

In this section, we discuss the behaviors of the Performers System, and when the behaviors can be taken as Services.

Definition 3 (Behavior of the Performers System)**.** *The way the* Performers System *behaves to adjust the indoor environment.*

The Behaviors of the Performers System are the representation of the functions of related Performers. For example, the Performers System in Figure 2 has the ability to cool the temperature down (behavior), which could be achieved by setting a lower temperature level under the cool mode of the air-conditioner (function). The representation of the Behaviors is the physical process, e.g., temperature change.

Definition 4 (Service)**.** *The* Behavior of the Performers System *exhibited in order to fulfill occupants' comfort requirement.*

One example of the Service can be the Performers System in Figure 2, which increases the indoor temperature to 22 °C for thermal comfort. Comfort means psychological and physical satisfaction with the state of the indoor environment, e.g., thermal comfort. It is the way to evaluate the Behaviors of the Performers System, and thus implicitly constrain the Behaviors. The comfort has different contents for different goals of the Performers System, e.g., thermal comfort; comfort in terms of humidity levels.

There are two ways to evaluate comfort. Let us take thermal comfort as an example. The first is based on the perception of occupants. If occupants feel uncomfortable, one can manually set a desired temperature level to the Performers System. It is easy and accurate but limited in some scenarios. For example, babies and elderly people may not be sensitive to temperature change due to their nervous system not being well developed or being degenerated. The second way is for comfort to be automatically evaluated by the smart home system core. This depends on various indices [24,25] for evaluating the physical environment for thermal comfort. For example, the PMV–PPD (Predicted Mean Vote and Predicted Percentage of Dissatisfied) index [25] is used to evaluate thermal comfort with respect to environmental factors and personal factors. PMV and PPD are short for predicted mean vote and predicted percentage of dissatisfaction, respectively, and are calculated based on Fomulas (1)

and (2), where TS denotes the thermal sensation transfer coefficient and is determined by metabolic rate; MV means internal heat production in the human body and is determined by the metabolic rate and external work; and $HL1$, $HL2$, $HL3$, $HL4$, $HL5$, and $HL6$ represent heat losses through skin, sweating, latent respiration, dry respiration, radition and convection, respectively. Then combine with the ASHRAE (American Society of Heating, Regrigerating and Air-Conditioning Engineers) thermal sensation scale as shown in Table 1 to determine the comfortableness. The details are referred to in [25].

$$PMV = TS \times (WM - HL1 - HL2 - HL3 - HL4 - HL5 - HL6) \quad (1)$$

$$PPD = 100 - 95 \times e^{-0.03353 \times PMV^4 - 0.2179 \times PMV^2} \quad (2)$$

Table 1. ASHRAE thermal sensation scale.

Hot	Warm	Slightly Warm	Neutral	Slightly Cool	Cool	Cold
+3	+2	+1	0	−1	−2	−3

Environmental factors like humidity can be acquired through humidity sensors. Personal factors like metabolic rate can be roughly evaluated based on the occupant's activities, e.g., sedentary. Another way is to take advantage of wearable devices to measure personal information and send these data to the smart home system core to evaluate comfortableness. However, as far as the author is aware, cloth insulation cannot be evaluated through wearable devices for now. It can only be roughly evaluated through scenarios like in hot summer, where the value of cloth insulation is small, and an average value is assigned for the summer season.

Definition 5 (Service Manner)**.** *The* Service *under a specific condition is called a Service Manner.*

The condition can be personal or environmental. For a Service, e.g., adjust the indoor temperature for thermal comfort by an air-conditioner, changes in conditions result in different Service content. For example, compare a sweating man in summer and a sedentary man in winter. The conditions in the former are high metabolic rate, high outdoor temperature, etc., and he needs for the temperature to be cooled down. For the latter, the conditions may be low metabolic rate, low outdoor temperature, etc., and he needs for the temperature to go up.

Definition 6 (Critical Service Manner)**.** *The* Service Manner *in demand is called Critical Service Manner.*

This definition is given from the viewpoint of people who need the Service. In the example from Definition 5, the adjustment of indoor temperature to achieve a cool environment for thermal comfort is the Critical Service Manner for the sweating man; the adjustment of indoor temperature to achieve a warm environment for thermal comfort is the Critical Service Manner for the sedentary man.

3.2.3. Accident Formation

Accidents can be understood as the resilience [26] of the Performers System, i.e., adjusting indoor environment anomalies to maintain a normal performance has failed and resulted in undesired consequences. A Service may fail and result in uncomfortableness, then further evolve into hazards and cause harm to occupants. Accident formation is to describe how Services may fail and further evolve into a hazard to cause accidents. The causes on the system part, i.e., the Performers System, can be understood by the STAMP model. The relation between the Behaviors of the Performers System and the physical processes in accident formation is discussed in this section.

There are some considerations about physical processes from the viewpoint of engineering. Before a hazard is detected, physical process anomalies should be detected as early as possible so as to trigger precautionary measures. The information of hazards is also important for triggering reaction

measures. All in all, accident formation, which is shown in Figure 3 focuses on the physical process anomalies resulting from abnormal Behaviors.

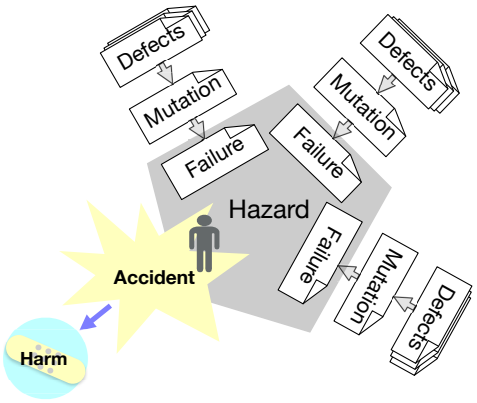

Figure 3. The accident causality model.

Next, let us discuss the terms and related rationales of the accident causality model in Figure 3.

Definition 7 (Defect)**.** Defects *are the direct causes of a* Mutation.

A Mutation (Definition 8) relates to abnormal Behaviors of the Performers System. Abnormal Behaviors are due to unexpected control actions of the Performers System. Thus, Defects are inappropriate control actions (ICAs) and unsafe control actions (UCAs) of the Performers System to the abnormal Behaviors in adjusting the home environment. ICAs occur when Mutations result in Service Failures (Definition 9), and UCAs occur when Service Failures evolve into Hazards (Definition 10). For example, an ICA can be wrongly setting the heating mode of a Performer in hot summer, which will cause thermal discomfort. To differentiate from causes introduced in the STAMP model, Defects refer to more superficial reasons. As the home environment is an application area, the deeper causes for system development defects are not considered here. When physical process anomalies are detected, the home environment is expected to react to them immediately with respect to Defects. Therefore, the Defects are the direct causes and should be controllable, e.g., through reconfiguration.

As discussed at the beginning of Section 3, the STAMP-PP model relates to system operations. The occurrence of Defects is under the scenarios of system operations. The operations can be categorized into three types. One is operations by occupants. Another is by some controllers, e.g., Performers. The other is a mixture of by occupants and the controller. To react to a physical process anomaly efficiently, it is necessary to know the Defect with its corresponding operation scenario. To identify Defects with respect to the scenarios, we applied the hazard analysis technique STPA [2,9] in Section 4.

Definition 8 (Mutation)**.** *A* Mutation *is the violation of constraint on the* Behavior of the Performers System.

Abnormal changes in physical processes are the representation of the abnormal Behavior of the Performers System. Therefore, the constraint on the Behavior of the Performers System is the prescription of changes in physical processes that satisfy the comfort purpose. Thus, the Mutation is the change of physical processes under adjustment unacceptably deviating from the prescribed curve(s), which results in uncomfortableness. For example, the amplitude of temperature fluctuation should not exceed a threshold value for thermal comfort [23]. The Mutation in this case is the amplitude of temperature fluctuation exceeding the threshold value.

The Mutation is a state of physical processes between the state that brings about comfort and the state that results in a hazard. This concept is important not only for the understanding of accident

formation, but also because the information can trigger precautionary measures. First, a Mutation indicates the current indoor environment adjustment is inefficient. Second, by combining the *Mutation* with Defects under certain operation scenarios, one can select appropriate precautionary measures to restore the state of physical processes that bring about comfort.

Definition 9 (Service Failure)**.** *The* Behavior of the Performers System *exhibits failed to fulfill occupants' comfort requirement.*

The concept of Mutation is related to physical processes, while Service Failure refers to both physical processes and the perception of occupants. The occurrence of Service Failure is when occupants perceive the uncomfortableness brought about by the Mutation.

There are two ways to determine whether a Service has failed. One is directly determined by the perception of occupants. Another one resorts to various indices [24,25], by which the smart home system core can conclude whether the home environment satisfies the comfort requirement with occupants on the scene.

Definition 10 (Hazard)**.** *It is an indoor environment state that will cause harm to occupants.*

A Hazard will harm the health condition of occupants who are on the scene. One or more Service Failures will form or further evolve into a hazardous situation. For example, a Service Failure for thermal discomfort evolves into a hazard if the indoor temperature reaches a level that can cause heat stroke if occupants are present.

Taking thermal related hazards as an example, the evaluation of a hazard depends on heat stress indices [27] and cold stress indices [28]. These indices are sophisticated techniques to represent thermal sensations to hot and cold conditions. Heat stress [27] is defined as the net heat load to which an occupant is exposed from the combined contributions of metabolic heat, environmental factors, and clothing that results in an increase in heat storage in the body. Cold stress [28] is the climatic condition under which the body heat exchange is just equal to or too large for heat balance at the expense of significant heat and sometimes heat debt. Similarly to the PMV–PPD index, they also have a complex relations with environmental and personal factors, which can be measured in practice.

Definition 11 (Accident)**.** *It is an unintentional event where a* Hazard *results in harm of occupants.*

It involves both the home environment and occupants. The Hazard has harmed occupants. The Accident can be detected by evaluating the Hazard and the health condition of the occupants. The latter can be measured by taking advantage of wearable devices.

Definition 12 (Harm)**.** *Death, physical injury or damage to the health of occupants.*

It is the consequence of the Accident. It varies with respect to Hazards and the health conditions of occupants. For example, it may cause heat illnesses or even death to elderly people due to heat exposure [29]; it may also affect sleep and the circadian rhythm that can cause cardiac autonomic response during sleep due to cold exposure [30].

4. Application of STPA

To identify Defects under operation scenarios, the hazard analysis technique STPA is adopted. In this section, we first introduce the STPA steps, then discuss the way to tailor it and a new way of documenting the analytical results, and finally illustrate the application results and compare them with the application of the original STPA.

4.1. STPA

The Systems-Theoretic Process Analysis (STPA) [2,9] is a new hazard analysis technique based on the STAMP model. The goal is to identify causes that lead to hazards and result in losses so they can be eliminated or controlled. The STPA has three steps, the latter two of which are taken as the main steps.

The first step is to establish the system engineering foundation. Three things should be done in this step. The first is to define the interested accident and its related system hazards. They should be specific and concise. Then, the system level safety requirements and design constraints need to be specified to prevent system hazards from occurring. The last is to define the safety control structure that takes the system level safety requirements and design constraints as inputs.

The second step is to identify potentially unsafe control actions (UCAs). Every controller of systems usually has one or more control actions. System hazards thus result from inadequate control or enforcement of the safety constraints. Four taxonomies are provided to look for the UCAs:

1. A control action required for safety is not provided or not followed;
2. An unsafe control action is provide;
3. A potentially safe control action is provided too early or too late (at the wrong time or in the wrong sequence);
4. A control action required for safety is stopped too soon or applied too long.

Then, we translate the identified UCAs into safety requirement and designed constraints on system component behaviors.

The third step determines how each UCA identified in step two could occur. For each UCA, examine the parts of the control loop as shown in Figure 4 to see if they can cause the UCA under some scenarios. Then, design controls and mitigation measures if they do not already exist or evaluate existing measures.

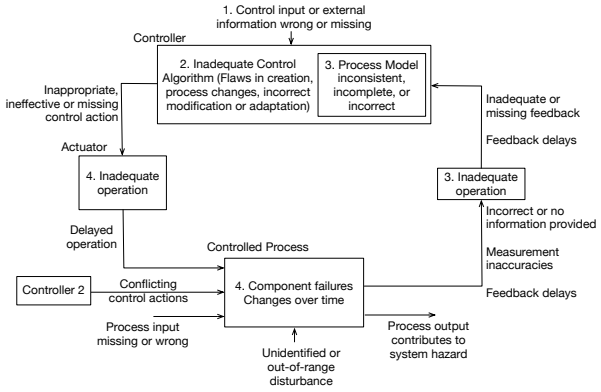

Figure 4. A classification of controls flaws leading to system hazards.

4.2. Tailor

The understanding of accident formation within the indoor environment has extended the STAMP model, i.e., the STAMP-PP model, by also considering physical processes. As disscussed in Section 3.2.3, abnormal Behaviors result in Service Failures, and abnormal Behaviors are due to inappropriate control actions of the Performers System. Thus, it is important to know what these inappropriate control actions are. Therefore, the STPA need to be tailored for this main purpose.

In the first step of STPA, in addition to the definition of accident, system hazard, and safety requirement, information about the Service Failure and requirements of no failure, i.e., the reliability of the Performers System to deliver Services, should also be provided. Design constraints are not required as this work is not for implementing a safe system.

When a Service Failure occurs, which means the corresponding control action is inappropriate, then precautionary measure(s) should be provided. Thus, in the second step of STPA, ICAs should

be identified with regard to the taxonomies provided in step two of STPA. Namely, given a state of physical processes, under a specific operation scenario, we need to consider whether a control action with respect to the taxonomies will cause a Service Failure. Precautionary measures are determined by considering the context information which consists of the ICAs, operation scenarios, and the Service Failure. The process of the determination heavily depends on the expertise of concerned areas, which is directed by the reliability requirements. The precautionary measures are also control actions. Ineffective precautionary measures will result in the occurrence of a Hazard (then, reaction measures are required). For each precautionary measure, UCAs are identified by considering the taxonomies provided in step two of STPA under the conditions of operation scenarios and of a state of physical processes. Safety requirements to the UCAs also need to be identified to guide the selection of reaction measures.

The third step of STPA is not necessary. This is because the analysis in our case is to identify Defects under operation scenarios, which can be utilized in selecting appropriate precautionary and reaction measures, but not in designing and manufacturing a system.

STPA adopted tables and lists for documenting analytical results [2,9]. After applying the tailored STPA, the results, i.e., control actions, ICAs, and their related reliability requirements and operation scenarios; and precautionary measures, UCAs, and their related safety requirements and operation scenarios, could be documented by that used by the STPA. However, the relations among them are not clearly represented. In this paper, we propose a Landscape Genealogical Layout Documentation (denoted as LGLD) for documenting the results, which is illustrated in Figure 5. The ancestor is a control action. The first generation illustrates ICAs and their related reliability requirements and operation scenarios. The second generation represents precautionary measures. The third generation represents UCAs and their related safety requirements and operation scenarios. These results can be numbered for better reference, e.g., ICA-m for an ICA, which means the inappropriate control action m. This way of documentation also implies the analysis direction, i.e., from control actions to ICAs, then to precautionary measures, and finally to UCAs.

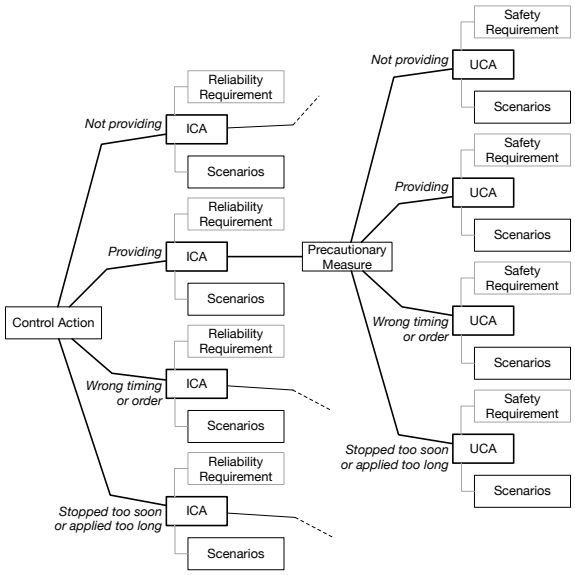

Figure 5. Documenting the analytical results by the Landscape Genealogical Layout Documentation (LGLD) approach.

For each control action, the taxomomies provided in step two of STPA to list the ICAs must be considered. Every ICA is attached with the reliability requirements and operation scenarios. Then, each ICA is connected with a precautionary measure. The precautionary measure is to prevent its connected ICA from changing the home environment from a Service Failure to a Hazard. For each

precautionary measure, it is important to list the UCAs attached with safety requirements and operation scenarios.

4.3. Results

As discussed in Section 2.2, weather anomalies affect indoor environment, e.g., the heatwave of summer 2018. Thus, we consider the example of the high-temperature results in heat stroke [31,32]. Heat stroke is clinically diagnosed as a severe elevation in body temperature (a core body temperature of 40°C or higher) that occurs in the presence of central nervous system dysfunction and a history of environmental heat exposure or vigorous physical exertion. It can be classified into nonexertional (classic) heat stroke and exertional heat stroke. The former occurs in very young or older people, or those with chronic illness when the environmental temperature is high. The latter happens to young fit people and involves prolonged excessive activities like sports. This paper focuses on the former case.

Heat stroke can be assessed by heat stress indices, among which the most widely accepted and used one is the wet bulb globe temperature (WBGT) [33]. The Ministry of the Environment of Japan (Ministry of the Environment, Japan: http://www.wbgt.env.go.jp/en/) has recommended a criterion for thermal conditions based on the WBGT as shown in Table 2.

Table 2. Recommended criteria for thermal conditions.

WBGT (°C)	Threat Level
∼21	Almost Safe
21∼25	Caution
25∼28	Warning
28∼31	Severe Warning
31∼	Danger

We applied the tailored STPA to a Performers System that is for indoor temperature adjustment for thermal comfort. The structure of the system consists of four parts, i.e., home, home gateway, service intermediary, and service provider [12], as shown in Figure 6. The home is the place that occupants live in, which is equipped with different kinds of items, e.g., home appliances, to meet everyday living requirements. The home gateway is the gateway of the networked Performers to the outside world of the home. The indoor temperature adjustment service is executed here to issue commands for the control of Performers. The service intermediary aggregates various services from different service providers and maintains them locally. It can also respond to service subscriptions from home gateways. The service provider designs, publishes, and updates concrete services to the service intermediary for future use. We applied STPA to investigate the Behaviors of the Performers System to elicit possible Defects under related operation scenarios. Thus, we focus on executing the indoor temperature adjustment service in the home gateway to adjust the indoor temperature. The home gateway, service intermediary, and service provider can be taken as the smart home system core.

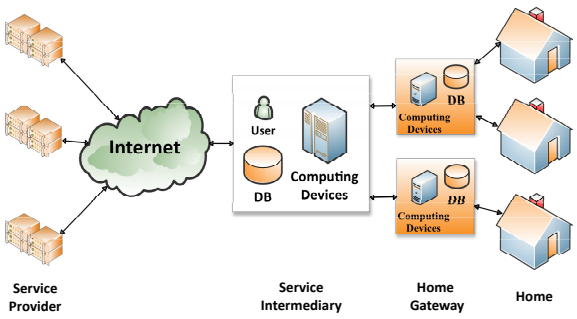

Figure 6. The structure of the Performers System.

In order to apply STPA, an assisting tool, i.e., STAMP Workbench (the STAMP Workbench is an open-source, free, easy-to-use tool for people who are interested in system safety analysis by using the STAMP/STPA. It was developed by the IT Knowledge Center of Information-Technology Promotion Agency, Japan. https://www.ipa.go.jp/english/sec/complex_systems/stamp.html) is adopted for the analysis. The STAMP Workbench is claimed to include features such as concentration on thinking and help analysis and is not just an editing tool, or guide analysis procedure, but an unlimited and intuitive operation. Analytical results can be exported into Excel files and images.

In the first step of STPA, we prepared some concepts for further analysis as shown in Table 3. For demonstration, Service Failure is defined as when the indoor WBGT temperature is adjusted within (25,28] °C, and the Hazard is when the indoor WBGT temperature is adjusted over 28 °C. The reliability requirement corresponds to the Service Failure, which represents the requirement to ensure a Service will not fail.

Table 3. Preparation for the tailored System-Theoretic Process Analysis (STPA).

Accident	Physical harm of occupants due to heat stroke
Service Failure	Indoor WBGT temperature is within (25,28] °C
Reliability Requirement	Indoor WBGT temperature should be adjusted bellow 25 °C
Hazard	Indoor WBGT temperature is over 28 °C
Safety Requirement	Indoor WBGT temperature should be adjusted bellow 28 °C

Figure 7 illustrates the safety control structure for indoor temperature adjustment. The Home Gateway is the controller, which is responsible for executing the indoor temperature adjustment service. The controlled process is the Home Environment. Performers are taken as actuators. We consider an air-conditioner and a window here as Performers. Empirically, for energy saving, these two cannot work at the same time. The control actions are listed on the arrow from the Home Gateway to the Performers. The control action "set to X °C" means to set Performers to adjust the indoor temperature to X °C. The feedback to the Home Gateway is the indoor temperature. Indoor temperature can be adjusted by the indoor temperature adjustment service that is executed in the Home Gateway, or by occupants to issue commands, i.e., control inputs to the Home Gateway.

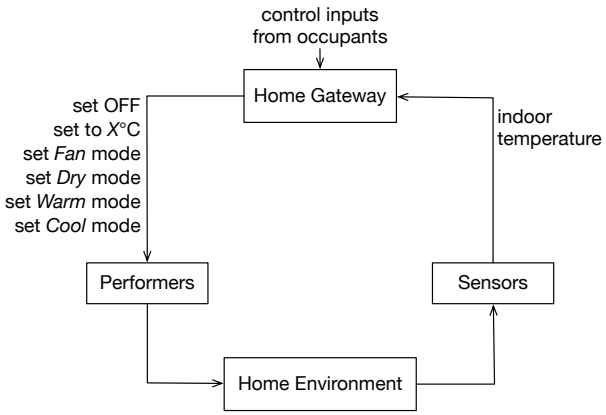

Figure 7. The safety control structure for indoor temperature adjustment.

Next, based on the results of the first step, we identifies ICAs and UCAs and elicited their related requirements and operation scenarios. Part of the results are shown in Figures 8 and 9, which adopted the LGLD approach introduced in Section 4.2 for the documentation. They illustrate the results of analyzing the control actions “set OFF” and “set to X °C”. “N/A” denotes the taxonomy is not applicable to the corresponding control action. In Figure 8, the second “set OFF” can be considered as a reconfiguration compared with the first one. The precautionary measure “set Cool mode” can be deployed for the two ICAs that relate to the “set OFF”. One reason could be that a different configuration has a higher possibility to restore the physical process to a comfortable state, as the “set

OFF" has caused the ICA. For the second operation scenario, not-providing ICA, it is because people are not sensitive to temperature change and thus did not issue the "set OFF" command manually.

For the results as shown in Figure 9, X satisfies $X < 25$ °C. There are two reasons for the not-providing ICA and UCA to say that the Performers System is working in the Fan mode. The first is if it works in the Warm mode, which in this case is inappropriate or hazardous, and we cannot make a solemn vow to conclude that not providing "set to X °C" is inappropriate or hazardous. Second, the other working modes, i.e., Dry and Cool, have a cooling effect based on our experience, which may not be an ICA or UCA even when "set to X °C" is not provided. One more thing that needs to be explained is that providing "set to X °C" at the "wrong time" is neither inappropriate nor hazardous. If it is not provided in time, the home environment would experience Service Failure or Hazard for some time. However, providing "set to X °C" at a different time should not be inappropriate or hazardous. Conversely, since "set to X °C" is provided, the home environment could be restored to a safe level, even though later than expected. In this case, providing "set to X °C" can be thought of as a precautionary or reaction measure, rather than an inappropriate or hazardous control action.

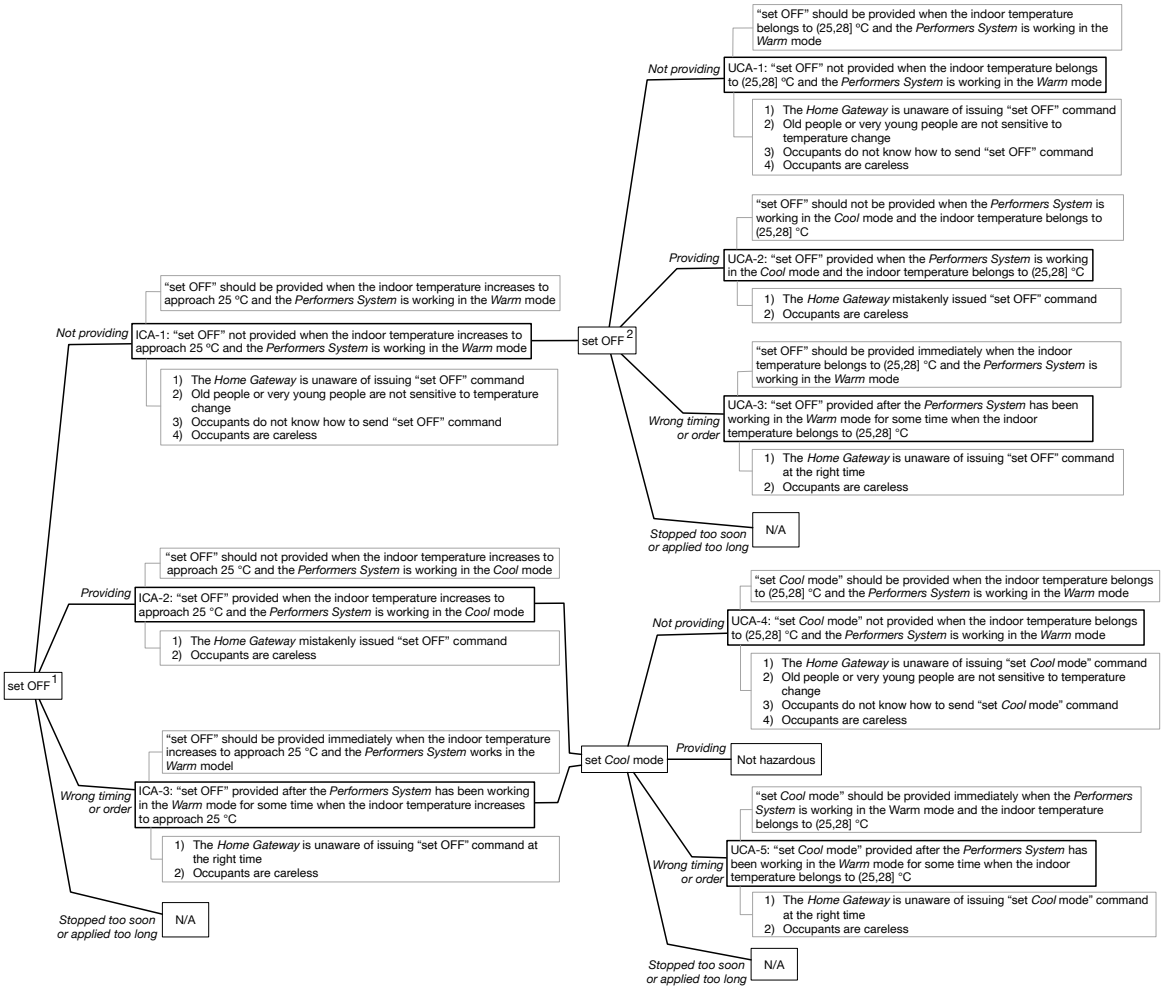

Figure 8. The analysis results for the control action "set OFF".

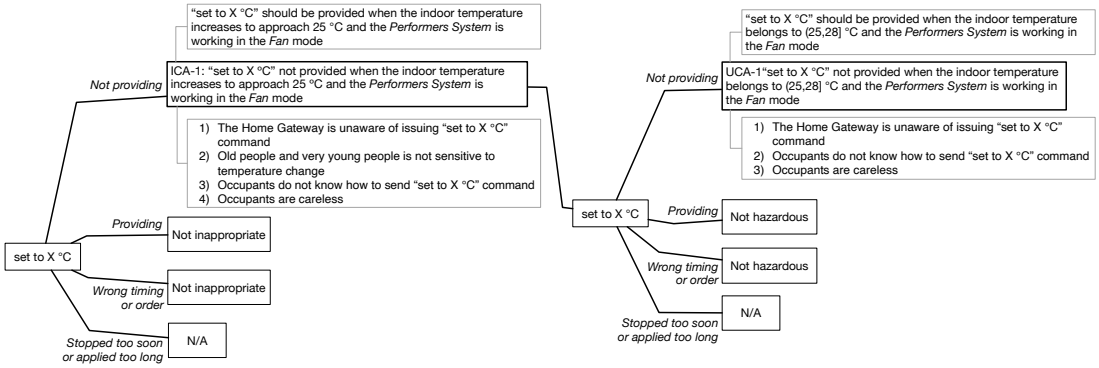

Figure 9. The analysis results for the control action "set to X °C".

4.4. Comparsion of Results

Originally, the STPA is the only hazard analysis technique was based on the STAMP model [2]. Thus, in this section, let us compare the results presented in Section 4.3 with those by adopting the original STPA. Since the third step of STPA was not taken into account, the comparison only considers the results that derived from the first two steps of STPA. For comparability, the temperature issue discussed in Section 4.3 is still part of our focus when adopting the original STPA.

As discussed, the goal of STPA is to identify causes that lead to hazards and result in losses, so they can be eliminated or controlled. The causes to be identified are UCAs, and flaws in the control loop (as shown in Figure 4) under some scenarios which are different from our case. The elimination or control usually resorts to designing and implementing a safe system, while in our case, the aim is to select appropriate precautionary and reaction measures which can restore a safe Service delivery.

The system engineering foundation is given first. The prepared definitions are illustrated in Table 4. The design constraint is system level constraint and is expected to further decompose into constraints that can be assigned to system components as the analysis evolves. Compared with what is shown in Table 3, Service Failures and reliability requirements to the system are gone, which indicates ICAs will not be identified afterward. This is because ICAs are supposed to result in Service Failure, and reliability requirements of ICAs can be taken as the decomposition of the system level reliability requirement. The safety control structure as shown in Figure 7 can also be used here.

Table 4. Preparation for the STPA analysis.

Accident	Physical harm of occupants due to heat stroke
Hazard	Indoor WBGT temperature is over 28 °C
Safety Requirement	Indoor WBGT temperature should be adjusted bellow 28 °C
Design constraint	The Performers System is capable of adjusting the indoor WBGT temperature bellow 28 °C

Next, the UCAs identified in step two of STPA are shown in Tables 5 and 6 for control actions "set OFF" and "set to X °C", respectively. Then, for each UCA, safety requirements and design constraints can be derived. For example, the safety requirement for UCA-1 in Figure 5 could be:

- "set OFF" should be provided when the indoor temperature belongs to (25,28] °C and the Performers System is working in the Warm mode.

The design constraints for UCA-1 could be:

- The Performers System should be accurately aware of the indoor temperature change;
- "set OFF" should be provided when needed.

Table 5. UCAs for the control action "set OFF".

Hazard: Indoor WBGT temperature is over 28 °C				
Control Action	**Not Providing**	**Providing**	**Wrong Timing or Order**	**Stopped Too Soon or Applied Too Long**
set OFF	UCA-1: "set OFF" not provided when the indoor temperature belongs to (25,28] °C and the Performers System is working in the Warm mode	UCA-2: "set OFF" provided when the Performers System is working in the Cool mode and the indoor temperature belongs to (25,28] °C	UCA-3: "set OFF" provided after the Performers System has been working in the Warm mode for some time when the indoor temperature belongs to (25,28] °C	N/A

Table 6. UCAs for the control action "set to X°C".

Hazard: Indoor WBGT Temperature Is over 28 °C				
Control Action	**Not Providing**	**Providing**	**Wrong Timing or Order**	**Stopped Too Soon or Applied Too Long**
set to X °C	UCA-4: "set to X °C" not provided when the indoor temperature belongs to (25,28] °C and the Performers System is working in the Fan mode	Not hazardous	Not hazardous	N/A

There are some differences in the comparison with the results derived in step two of STPA. The ICAs, operation scenarios for ICAs, reliability requirements, precautionary measures, and operation scenarios for UCAs cannot be obtained by adopting the original STPA. However, the design constraints can be derived. The UCAs identified by adopting the original and tailored STPA are equivalent. The results documented by tables and lists are separated. It is a trivial problem when checking the relations between the results that were documented by the conventional approach. The LGLD approach integrated the results and overcame this problem. We discuss the advantages of the tailored STPA at the end of Section 5.

5. Discussion

As one of our everyday living experiences, physical processes could be in hazardous states that cause harm to occupants [29,30]. The occurrence of hazardous states can be transferred from a normal state of a physical process that brings about comfortableness, through some intermediate states for uncomfortableness. The normal state is maintained by the smart home system, which takes advantage of home appliances or the outdoor climate. When the behaviors of the smart home system deviate from expectations, the above transformation will occur. Thus, this living experience validates the proposed STAMP-PP model.

To validate the terms defined in the STAMP-PP model, let us consider the eight abnormal indoor temperature situations that were discussed in our previous work [23]. Mutations can be undesired fluctuation, constantly cooler/warmer than expectation, undesired duration of the temperature that results in discomfort, and Service Failures when combining the Mutations with the feeling of occupants on the scene. Hazards can be unbearable hot/cold and undesired duration in hot/cold situations.

Mutations and Hazards provide detectable evidence of physical process anomalies. The information of Service Failure combines with ICAs under related operation scenarios—e.g., as depicted in Figures 8 and 9, one can predict whether Hazards would happen before providing precautionary measures, because Service Failures and the ICAs under related operation scenarios can be the context, in which a Hazard could occur if time goes on. This context information can be acquired from various sensors (e.g., temperature sensor), system states, etc. For example, in Figure 9, we can know whether the temperature is increasing to approach 25 °C through temperature sensors. Then, precautionary measures can be selected under the direction of reliability requirements. If a Hazard is unfortunately detected, reaction measures have to be selected based on the UCAs under operation scenarios and the Hazard, which are guided by safety requirements.

The purpose of precautionary measures is to restore Service delivery. This is achieved by reconfiguration of the Performers System. The reconfiguration has two forms. One is to reset the current working Performer(s), e.g., the precautionary measure "set OFF" (the second one) as shown

in Figure 8, which is achieved by resetting the OFF command to the same Performer. Another is to reconfigure ready-to-use Performers to achieve the goal, e.g., the "set Cool mode" in Figure 8, which could be reconfigured to a standby Performer to the Cool mode. The purpose of reactions is to restore a safe home environment state, which could be a Service Failure (that needs further interference) or the process of normal Service delivery. It is also achieved by reconfiguring the Performers System, which has the same contents as those introduced for precautionary measures. The reactions should have another content that precautionary measures do not have, i.e., a warning mechanism. The warning mechanism is triggered when a Hazard is detected that implies precautionary measures have failed. In the very beginning, the warning signals will be sent to occupants who could leave the scene or do something else to ensure safety. If the reconfiguration in the reaction stage cannot restore the system to a safe situation, the warning mechanism will inform an emergency department, e.g., a hospital, through networks.

Accident models can be roughly classified into three categories [1,2], i.e., sequential models, epidemiological models, and systemic models. Sequential models describe accidents as the result of time-ordered sequences of discrete events. Epidemiological models view accidents as a combination of latent and active failures within a system, which is analogous to the spreading of a disease. Latent conditions, e.g., management practices or organizational culture, can lie dormant within a system for a long time, which can finally create conditions at a local level to result in active failures. The STAMP model is based on system theory and so is the STAMP-PP model. It describes physical process anomalies that cause uncomfortableness and health problems as a result of abnormal Behaviors of the Performers System. Furthermore, to better understand the causal relation between the Performers System and physical processes and better represent the time order of physical process evolvement, the terms in the STAMP-PP model can be taken as events.

Hazard analysis techniques are devised based on accident models. The STPA was invented based on the STAMP model to identify causes that conventional approaches overlooked [2,9]. We found it is an efficient tool for assisting in the identification of Defects, i.e., ICAs and UCAs (e.g., the results shown in Figures 8 and 9). However, hazard analysis heavily depends on expertise in a specific area. Accident models and hazard analysis techniques are to assist in understanding accidents and guiding for causal analysis. The STAMP-PP model offers a way to understand physical process anomalies with respect to the behaviors of smart home systems. To apply the tailored STPA to that in our case (some results of which are shown in Figures 8 and 9), one may need to possess knowledge in at least the fields of computer science, software engineering, computer networks, and even physics. This makes the authors feel that safety research in different areas is like different research fields.

In the first step of STPA, the accidents and system hazards provided mostly depend on the interest of an organization or the government [2]. For example, in this paper, Accident is defined as physical harm of occupants due to heat stroke, as illustrated in Table 3. It can also, however, encompass other symptoms aside from heat stroke, e.g., severe cold. Concrete accidents are different due to the variety of environments, e.g., workplaces and the home environment. It is also determined by budget, severity of occurrence, and frequency of occurrence [2].

In step two of STPA, originally, the taxonamies were provided to identify UCAs with respect to control actions. Physical process anomalies (not Hazards) are the result of abnormal Behaviors of the Performers System. The behaviors are the representations of the functions which are achieved by the control actions issued by the Performers Sytem. For example, stopping the Performers System from working is achieved by the control action "set OFF" as shown in Figure 8. Thus, the taxonomies are applicable for identifying ICAs. This ensures that all possible ICAs can be effectively identified.

The states of physical process change from a state of comfort to one of discomfort, then to one of hazard. When a state of discomfort is detected, precautionary measures are adopted to prevent the physical process from transferring into a state of hazard. Precautionary measures refer to control actions achieved by reconfigurations. Thus, the taxonomies are also applicable to the precautionary measures. For example, the control action "set OFF" in Figure 8 can both be the original control action

and the precautionary measure. The same applies to the control action "set to X °C" as shown in Figure 9.

The purpose of adopting the hazard analysis technique is to identify Defects, so as to select appropriate precautionary and reaction measures for adjusting home environment anomalies to maintain a normal performance. By checking the comparison presented in Section 4.4, we found the tailored STPA can satisfy this purpose, while the original STPA cannot. First, ICAs under operation scenarios and the reliability requirements of the ICAs can be identified by the tailored STPA. This is due to Service Failure, and the system level reliability requirement is provided in the first step of STPA. Naturally, precautionary measures are not necessarily identified in the original STPA, because precautionary measures are selected for ICAs. Second, even though UCAs can be identified by both the original and tailored STPA, the operation scenarios have different contents. For the tailored STPA, the operation scenarios refer to occupants or controllers or both as discussed when introducing the concept of Defect. For the original STPA, the operation scenarios refer to the control flaws as shown in Figure 4, which are identified in step three of STPA.

As discussed in Section 4.2, the STPA takes advantage of tables and lists to document the analytical results (see the results shown in Tables 5 and 6). We proposed the LGLD approach to document the analytical results. The advantage of comparing tables and lists is that it can clearly represent the relations among the results in a straightforward way. For example, in Figures 8 and 9, the relations among control actions, ICAs, precautionary measures, and UCAs are clear. Further, it is clear to see the (reliability or safety) requirements attached to each ICA and UCA, and the related operation scenarios under which the ICA and UCA can occur. This kind of relations is not explicitly represented using tables and lists such as the ones presented in Section 4.4. To build such documentation, one can build along the way of analysis, because the analysis starts from control actions to identify ICAs under related operation scenarios, and reliability requirements, then to determine precautionary measures, and finally to identify UCAs under related operation scenarios, and safety requirements.

When applying the STAMP-PP model to understand accident formation, the Performers System has to fully control the home environment, or its behaviors may not be the "only" reason to cause Service Failure, then Hazard. This can be the limitation of the proposed STAMP-PP model.

6. Related Work

This section includes two parts. The first is about accident models based on system theory. The second discusses safety-related research in the smart home environment.

6.1. Accident Models

The systems approach is considered as the dominant paradigm in safety research [34]. It views accidents as the unexpected interactions among system components, i.e., technical, social, and human elements. Among various systemic models, there are three most cited models [10], that is, STAMP [2], Functional Resonance Analysis Method (FRAM) [3], and Accimap [35,36].

The concept of STAMP has been briefly introduced in Section 3.1. According to [10], over half of the reviewed papers were STAMP-related, which indicates a pervasive acknowledgement of its underlying rationale. Its application has attracted researchers from a broad field. The authors of [6] adopted it to investigate aircraft rapid decompression events. The authors of [4] applied it in the analysis of deepwater well control safety. In the field of railway, the authors of [5] investigated railway accidents and accident spreading by taking the China Jiaoji railway accident as the example. It has also been applied to the field related to poisonous or dangerous substances. The authors of [7] adopted it in analyzing the China Donghuang oil transportation pipeline leakage and explosion accident. The authors of [8] applied it to the Fukushima Daiichi nuclear disaster and to promote safety of nuclear power plants. Smart home systems are generally not considered as safety-critical systems. However, as weather anomalies, e.g., heatwaves, occur regularly due to global warming, smart home

systems for indoor environment adjustment, in this context, can be taken as safety-critical. Thus, the STAMP model can be adopted for understanding accident formation in the home environment.

FRAM was developed to act as both an accident analysis and risk assessment tool [10]. The FRAM model graphically describes systems as interrelated subsystems and functions that will exhibit varying degrees of performance varation. Accidents result from the fact that the emergent variation produced from the performance variability of any system component to "resonate" with that of the rest of the elements is too high to control. It has been discussed that the FRAM and STAMP approaches focus better on qualitative modeling and description of systemic behavior and accidents [37]. FRAM also has applications in different fields, e.g., the authors of [38] applied it to railway traffic supervision to investigate interdisciplinary safety analysis of complex sociotechnological systems. The authors of [39] extended FRAM by including a framework with steps to support hazard analysis. Some efforts have been tried to quantify it, e.g., the authors of [40] developed a semiquantitative FRAM based on a Monte Carlo simulation.

The Accimap method is a graphical representation of a particular accident scenario that relates to systemwide failures, decisions, and actions [3,36]. Accimap is a generic approach and does not use taxonomies (that is different than that of the STPA [2,9]) of failures across the different levels of considered [41]. The Accimap produces less reliable accident analysis results compared to STAMP [42].

The selection of accident analysis techniques depends on the system characteristics, i.e., manageability and coupling [1]. The systemic approaches are usually adopted by systems with low manageability and tight coupling. Systemic approaches related to complex sociotechnical systems have their own strengths. For one such system, it is better to adopt multiple approaches which supplement each other, even though STAMP is considered much more effective and reliable in understanding accidents and hazard analysis [10,41,42].

6.2. Smart Home Safety

In the past, safety research inside the home environment used to be based on events or chains-of-events. With the emergence of the so-called smart homes, safety research inside the home environment also has new forms. Some of it refers to monitoring the home environment. With the purpose of detecting safety problems of indoor climate abnormal variations, the authors of [12] proposed a CPS (cyberphysical system) home safety architecture to support an event-based detection. The authors of [43] presented a method that maps the real home connection to a virtual home environment, together with related policies to ensure remote monitoring, to ensure home safety. Elderly safety in the smart home environment was achieved by analyzing and inferring locations, time slots, and periods of stay of elderly people [44]. Robot techniques were also employed, e.g., the authors of [45] developed a robot which can, for example, sense gas leakage and shut off the gas valve. Others focus on a specific part of the home. The authors of [46] proposed risk analysis and assessment when cooking to prevent potential risks. This is because the kitchen is also prone to safety problems like gas leakage and fire accidents. Electricity is also an important risk factor. The authors of [47] adopted an alert circuit with a voltage level indicator to prevent the smart solar home system from being overloaded and damaged. With cloud computing techniques becoming pervasive in implementing smart home systems, risks like cloud service unavailability have also been introduced. To overcome this, the authors of [48] discussed home resilience in the presence of possible unavailability and proposed RES-Hub, i.e., a standalone hub to ensure the continuity of required functionalities.

Most of the studies like those discussed above focus on implementing systems to deal with home safety problems. If not properly designed and implemented, the system itself can be a risk factor. Thus, requirement elicitation becomes critical. Conventional safety-related techniques are applied to safety-critical areas, e.g., aviation [6]. Our work employed these techniques to the smart home systems.

7. Conclusions and Future Work

We extended the accident model STAMP by considering physical processes in the home environment. As the home environment is adjusted by behaviors of the smart home system, we first proposed the concept of Performers System that emphasizes the behaviors performed by various home appliances. Then, based on the Behavior of the Performers System, we proposed accident formation with respect to physical processes going from normal state to some intermediate states that result in uncomfortableness, and finally to states that cause harm. In order to identify the Defects, i.e., ICAs and UCAs that result in abnormal system behaviors, the hazard analysis technique STPA was tailored and applied to the smart home system for indoor temperature adjustment. After comparison with the results derived by adopting the original STPA, we found that the tailored STPA is an efficient tool to assist in identifying the Defects. The analytical results of applying STPA were used to adopt tables and lists for documentation, but the relations among the results were not straight-forward and unclear. We then proposed the LGLD approach, whose advantages are demonstrated by the comparison of results.

For future work, we aim to map the context information in which physical process anomalies occurred in the cyber world, such that precautionary measures and reactions can be effectively selected in real time. This brings about the problem of how to parameterize the STPA analytical results, i.e., ICAs, operation scenarios, and reliability requirements; and UCAs, operation scenarios, and safety requirements.

Author Contributions: Conceptualization, Z.Y., Y.L., and Y.T.; methodology, Z.Y. and Y.T.; validation, Z.Y. and Y.T.; writing—original draft preparation, Z.Y.; writing—review and editing, Z.Y. and Y.T.; supervision, Y.T.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank Toshiaki Aoki who gave constructive comments.

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

References

1. Underwood, P.; Waterson, P. *Accident Analysis Models and Methods: Guidance for Safety Professionals*; Loughborough University: Loughborough, UK, 2013; p. 28.
2. Leveson, N.G. *Engineering a Safer World: Systems Thinking Applied to Safety*; The MIT Press: Cambridge, MA, USA; London, UK, 2011.
3. Hollnagel, E. *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*, 1st ed.; CRC Press: Boca Raton, FL, USA; London, UK; New York, NY, USA, 2012.
4. Meng, X.; Chen, G.; Shi, J.; Zhu, G.; Zhu, Y. STAMP-based analysis of deepwater well control safety. *J. Loss Prev. Process Ind.* **2018**, *55*, 41–52. [CrossRef]
5. Ouyang, M.; Hong, L.; Yu, M.H.; Fei, Q. STAMP-based analysis on the railway accident and accident spreading: Taking the China—Jiaoji railway accident for example. *Saf. Sci.* **2010**, *48*, 544–555. [CrossRef]
6. Allison, C.K.; Revell, K.M.; Sears, R.; Stanton, N.A. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Saf. Sci.* **2017**, *98*, 159–166. [CrossRef]
7. Gong, Y.; Li, Y. STAMP-based causal analysis of China-Donghuang oil transportation pipeline leakage and explosion accident. *J. Loss Prev. Process Ind.* **2018**, *56*, 402–413. [CrossRef]
8. Daisuke, U. STAMP Applied to Fukushima Daiichi Nuclear Disaster and the Safety of Nuclear Power Plants in Japan. Master's Thesis, School of Engineering, Massachusetts Institute of Technology, Cambridge, MA, USA, 2016.
9. Leveson, N.G.; Thomas, J.P. *STPA Handbook*; Massachusetts Institute of Technology: Cambridge, MA, USA, 2018.
10. Underwood, P.; Waterson, P. A critical review of the STAMP, FRAM and Accimap systemic accident analysis models. In *Advances in Human Aspects of Road and Rail Transportation*; CRC Press: Boca Raton, FL, USA, 2012; pp. 385–394.

11. Ericson, C.A., II. *Hazard Analysis Techniques for System Safety*; John Wiley and Sons, Inc.: Hoboken, NJ, USA, 2005; Chapter 3, pp. 31–54.
12. Yang, Z.; Lim, A.O.; Tan, Y. Event-based home safety problem detection under the CPS home safety architecture. In Proceedings of the 2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE), Tokyo, Japan, 1–4 October 2013; pp. 491–495. [CrossRef]
13. Yang, Z.; Lim, Y.; Tan, Y. A risk model for indoor environment safety. In Proceedings of the 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 24–27 October 2017; pp. 1–5. [CrossRef]
14. Harper, R. *Inside the Smart House*; Springer: Berlin/Heidelberg, Germany, 2003.
15. Lobaccaro, G.; Carlucci, S.; Löfström, E. A Review of Systems and Technologies for Smart Homes and Smart Grids. *Energies* **2016**, *9*, 1–33. [CrossRef]
16. Djenouri, D.; Laidi, R.; Djenouri, Y.; Balasingham, I. Machine Learning for Smart Building Applications: Review and Taxonomy. *ACM Comput. Surv.* **2019**, *52*, 24:1–24:36. [CrossRef]
17. Toschi, G.M.; Campos, L.B.; Cugnasca, C.E. Home automation networks: A survey. *Comput. Stand. Interfaces* **2017**, *50*, 42–54. [CrossRef]
18. Rasmussen, J. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Trans. Syst. Man Cybern.* **1983**, *SMC-13*, 257–266. [CrossRef]
19. MIL-STD-882E. *Department of Defense Standard Practice: System Safety*; Standard, Department of Defense: Washington, DC, USA, 2012.
20. Defence Standard 00-56. *Safety Management Requirements for Defence Systems, Part 1, Requirements*; Standard, Ministry of Defence: London, UK, 2007.
21. Chemishkian, S. Building smart services for smart home. In Proceedings of the 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525), Gaithersburg, MD, USA, 15–16 January 2002; pp. 215–224. [CrossRef]
22. Nakamura, M.; Tanaka, A.; Igaki, H.; Tamada, H.; Matsumoto, K. Constructing Home Network Systems and Integrated Services Using Legacy Home Appliances and Web Services. *Int. J. Web Serv. Res. (IJWSR)* **2008**, *5*, 82–98. [CrossRef]
23. Yang, Z.; Aoki, T.; Tan, Y. Multiple Conformance to Hybrid Automata for Checking Smart House Temperature Change. In Proceedings of the 2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Madrid, Spain, 15–17 October 2018; pp. 1–10. [CrossRef]
24. Anderson, G.B.; Bell, M.L.; Peng, R.D. Methods to Calculate the Heat Index as an Exposure Metric in Environmental Health Research. *Environ. Health Perspect.* **2013**, *121*, 1111–1119. [CrossRef]
25. ANSI/ASHRAE Standard 55-2010. *Thermal Environmental Conditions for Human Occupancy*; Standard, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.: Atlanta, GA, USA, 2010.
26. Woods, D.D.; Hollnagel, E.; Leveson, N. *Resilience Engineering: Concepts and Precepts*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2006.
27. Jacklitsch, B.; Williams, W.J.; Musolin, K.; Coca, A.; Kim, J.H.; Turner, N. *NIOSH Criteria for a Recommended Standard: Occupational Exposure to Heat and Hot Environments*; Recommended Standard 2016-106; U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health: Cincinnati, OH, USA, 2016.
28. ISO 11079. *Ergonomics of the Thermal Environment—Determination and Interpretation of Cold Stress When Using Required Clothing Insulation (IREQ) and Local Cooling Effects*; Standard, International Organization for Standardization: Geneva, Switzerland, 2007.
29. van Loenhout, J.; le Grand, A.; Duijm, F.; Greven, F.; Vink, N.; Hoek, G.; Zuurbier, M. The effect of high indoor temperatures on self-perceived health of elderly persons. *Environ. Res.* **2016**, *146*, 27–34. [CrossRef] [PubMed]
30. Okamoto-Mizuno, K.; Mizuno, K. Effects of thermal environment on sleep and circadian rhythm. *J. Physiol. Anthropol.* **2012**, *31*, 14. [CrossRef] [PubMed]
31. Leon, L.R.; Bouchama, A. Heat Stroke. In *Comprehensive Physiology*; American Cancer Society: Atlanta, GA, USA, 2015; pp. 611–647, doi:10.1002/cphy.c140017. [CrossRef]
32. Gaudio, F.G.; Grissom, C.K. Cooling Methods in Heat Stroke. *J. Emerg. Med.* **2016**, *50*, 607–616. [CrossRef] [PubMed]

33. Budd, G.M. Wet-bulb globe temperature (WBGT)—Its history and its limitations. *J. Sci. Med. Sport* **2008**, *11*, 20–32. [CrossRef] [PubMed]
34. Salmon, P.; Williamson, A.; Lenné, M.; Mitsopoulos-Rubens, E.; Rudin-Brown, C. Systems-Based Accident Analysis in the Led Outdoor Activity Domain: Application and Evaluation of a Risk Management Framework. *Ergonomics* **2010**, *53*, 927–39. [CrossRef] [PubMed]
35. Svedung, I.; Rasmussen, J. Graphic representation of accident scenarios: Mapping system structure and the causation of accidents. *Saf. Sci.* **2002**, *40*, 397–417. [CrossRef]
36. Rasmussen, J. Risk management in a dynamic society: A modelling problem. *Saf. Sci.* **1997**, *27*, 183–213. [CrossRef]
37. Bjerga, T.; Aven, T.; Zio, E. Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliab. Eng. Syst. Saf.* **2016**, *156*, 203–209. [CrossRef]
38. Belmonte, F.; Schön, W.; Heurley, L.; Capel, R. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 237–249. [CrossRef]
39. Tian, J.; Wu, J.; Yang, Q.; Zhao, T. FRAMA: A safety assessment approach based on Functional Resonance Analysis Method. *Saf. Sci.* **2016**, *85*, 41–52. [CrossRef]
40. Patriarca, R.; Gravio, G.D.; Costantino, F. A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems. *Saf. Sci.* **2017**, *91*, 49–60. [CrossRef]
41. Salmon, P.M.; Cornelissen, M.; Trotter, M.J. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Saf. Sci.* **2012**, *50*, 1158–1170. [CrossRef]
42. Filho, A.P.G.; Jun, G.T.; Waterson, P. Four studies, two methods, one accident—An examination of the reliability and validity of Accimap and STAMP for accident analysis. *Saf. Sci.* **2019**, *113*, 310–317. [CrossRef]
43. Yang, L.; Yang, S.H.; Yao, F. Safety and Security of Remote Monitoring and Control of intelligent Home Environments. In Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics, Taipei, Taiwan, 8–11 October 2006; Volume 2, pp. 1149–1153. [CrossRef]
44. Kim, S.C.; Jeong, Y.S.; Park, S.O. RFID-based Indoor Location Tracking to Ensure the Safety of the Elderly in Smart Home Environments. *Pers. Ubiquitous Comput.* **2013**, *17*, 1699–1707. [CrossRef]
45. Lee, K.H.; Seo, C.J. Development of user-friendly intelligent home robot focused on safety and security. In Proceedings of the ICCAS 2010, Gyeonggi-do, Korea, 27–30 October 2010; pp. 389–392. [CrossRef]
46. Yared, R.; Abdulrazak, B.; Tessier, T.; Mabilleau, P. Cooking Risk Analysis to Enhance Safety of Elderly People in Smart Kitchen. In *Proceedings of the 8th ACM International Conference on PErvasive Technologies Related to Assistive Environments*; ACM: New York, NY, USA, 2015; pp. 12:1–12:4. [CrossRef]
47. Hasan, T.; Nayan, M.F.; Iqbal, M.A.; Islam, M. Smart Solar Home System with Safety Device Low Voltage Alert. In Proceedings of the 2012 UKSim 14th International Conference on Computer Modelling and Simulation, Cambridge, UK, 28–30 March 2012; pp. 201–204. [CrossRef]
48. Doan, T.T.; Safavi-Naini, R.; Li, S.; Avizheh, S.; K., M.V.; Fong, P.W.L. Towards a Resilient Smart Home. In Proceedings of the 2018 Workshop on IoT Security and Privacy, Budapest, Hungary, 20–20 August 2018; ACM: New York, NY, USA, 2018; pp. 15–21. [CrossRef]