Doctoral Dissertation

Architecture and Platform for Safe Cyber-Physical Home System

Yang Zhengguo

Supervisor: Tan Yasuo

School of Information Science
Japan Advanced Institute of Science and Technology

Degree conferment March 2020

Advisor: Professor Tan Yasuo Yang Zhengguo

Architecture and Platform for Safe Cyber-Physical Home System

Abstract

Globe warming and weather anomalies, e.g., heatwaves, occur on this planet quite often in recent years, which affects the lives. These result in morbidities and mortalities. The indoor environment is, of course, affected in the viewpoint of safety. Moreover, people stay indoors for a large portion of their time. Therefore, safety problems related to abnormal indoor climate change have great affection for the indoor lives of occupants.

Conventionally, people take advantage of home appliances to adjust the indoor environment. With the development of home automation, networking, the introduction of the so-called artificial intelligence, and the smart grid, etc., the cyber world of smart homes becomes more and more complex. So, the indoor environment is adjusted by the cyber world may fail either due to its inability or malfunction. This cannot guarantee indoor environmental safety under the circumstance of weather anomalies. Thus, it is necessary to observe the indoor environment to detect or predict undesired safety events, based on which to design or select effective reactions to ensure the home environment safe.

The aim of this research focuses on home safety problem detection and prediction. Home safety problems in this work refer to indoor climate anomalies that will cause health problems to occupants. Thus, supportive architecture and platforms are necessary. To this end, a home safety architecture is proposed for supporting the observation of the indoor environment to detect and predict indoor climate anomalies. The architecture is based on Cyber-Physical Systems (CPS) and the Service Intermediary Model. For understanding the causality of home safety problem formation and identifying the causes of the indoor climate anomalies in the cyber world, I proposed an accident model and a hazard analysis technique, i.e., tailored STPA (System-Theoretic Process Analysis).

The proposed accident model is based on the STAMP (Systems-Theoretic Accident Model and Process) model. The accident model illustrates to connect the behaviors of smart home systems and the physical world to describe accident formation. To this end, I first proposed the concept of the Performers System, based on which to define terms like Behavior. Then I define terms and their relations to describe accident formation concerning the Performers System. I adopt indoor temperature data and empirical experience for demonstrating the validity of the proposed accident model.

For the tailored STPA, it mainly aims to also identify ICAs (Inappropriate Control Actions) of controllers. ICAs and UCAs (Unsafe Control Actions) are the causes of the occurrence of safety problems. I also proposed a procedure to identify system-level hazards and an LGLD (Landscape Genealogical Layout Documentation) approach for documenting the analytical results. The LGLD approach can

clearly and straightforwardly represent the relations of the results. Some examples are used to demonstrate the practical usefulness of our proposals. I also practiced applying an innominate approach for hazard identification and analysis, which is based on the goal-based requirement engineering, guide words, and item sketch.

Based on the above-discussed proposals, I proposed ways of safety problem detection and prediction. I proposed a multiple-conformance approach to check the indoor temperature for detecting thermal problems. Conformance testing is a formal approach to check the validity of an implemented system against its specification. It is applied to check whether the indoor temperature conforms to the requirements of no thermal problems. I model required changes in indoor temperature by hybrid automata. The practical usefulness and performance of the proposed multiple-conformance approach that takes the hybrid-automata-modeled requirement as the specification are demonstrated through experiments.

For the safety problem prediction, I take heat shock during the bath as an example. I adopt Bayesian networks for the prediction. The structure of the Bayesian network is built by the proposed procedure concerning surveyed knowledge of heat shock. The conditional probabilities are elicited by a proposed procedure that takes advantage of the probability scale method with the proposed concept of degree of influence. The results show that it is feasible to adopt Bayesian networks to predict heat shock based on partially observed evidence.

Keywords: Home Safety; Smart Home Environment; Accident Model; Hazard Analysis; Indoor Climate Anomaly Detection; Heat Shock Prediction.

Contents

Listing of figures

Listing of tables

To my parents, my sister, and my daughter.

Acknowledgments

My principal advisor Professor Dr. Yasuo Tan has been, and continuous to be the ideal advisor and supporter for the work I do. His intelligence, well-timed advice and altruistic support have much to do with my obstinate pursuit of this degree. I would like to express my greatest gratitude and respect to him for his kind, patient and ultimate supervise and support. He provided opportunities to me to be involved in research projects together with the *Graduate Research Program* (GRP) scholarship to allow me to carry on my research and to make a living here in Japan. After I applied the supplemental student status, he kindly hired me as a researcher at JAIST, so that I can finish my research to obtain the degree without worries.

I am also grateful to the support of Associate Professor Dr. Yuto Lim, who is my sub-advisor. He commented my research and gave me a lot of valuable and intellectual suggestions to improve my research during lab seminars. He spared his time to advise my research every time I went to his office. I thank what he did for me.

I would like to show my gratitute to Professor Dr. Toshiaki Aoki, who is my minor research advisor. His intelligence, profound knowledge, well-timed advices guided me to produce high quality publications. He supervised me not only in teaching me knowledge, but also the way of doing research, and of writing and publishing high quality publications. The latter will affect and guide me in my future research activities to avoid detours. This is the greatest part that I benifited while under his supervision. Professor Dr. Toshiaki Aoki is a kind, patient, well competent advisor that I show my respect with heart and soul.

My gratitude extends to the members of the lab. Dr. Marios Sioutis who used to be my tutor when I was a master student. He is a good friend and helped me a lot especially in revising english mistakes of my publications. Mr. Yoshiki Makino who helped me to translate documents into Japanese, to let me use his tool to acquire real data from iHouse (a testbed smart house). Dr. Saher Javaid, who is now a teaching assistant in the lab. She spared her time to revise the grammar and phrasing mistakes of my publications. I also show my thanks to other members of the lab for no matter what they did to help me. Also Ms. Ayako Tokuyama who is the research assistant of the lab who helped me dealing with a lot of trivia that related to like the procedure to attend a symposium. I would also like to thank the members that has left the lab. Mr. Hoaison Nguyen, Dr. Konlakorn Wongpatikaseree, etc. I spent a wonderful time to be in the lab. I will miss all of you.

A special thanks to the members of the Dissertation Defense Committee for Ph.D. Degree. Professor Yasuo Tan, who is the main committee member. The rest of the committee members are Professor Toshiaki Aoki, Professor Yoichi Shinoda, and Associate Professor Yuto Lim, who are from JAIST. The other one Professor Tomohiro Yoneda, who comes from the National Institute of Informatics, Japan. Thanks for the questions and constructive comments from all of you and the public audience.

Eight years have passed since the time I started pursuiting the Ph.D degree until the time I obtained

it. Great changes have taken place to me and my beloved and respective family. I am grateful to my parents and younger sister, they support me and help me to take care of my daughter so that I can devote most of my time to finish my research. Without them I cannot obtain the degree. Also, my deepest love and gratitude to my daughter, you are the source of the motivation for me to do my research. I spent less time to be with you which I should be. Fortunately, from now on, I can see you growing up.

Finally, I want to thank myself. When I look back, I am surprised that I managed to hang in there for the years to pursuit the degree. Without the faith of persisting in providing a good living for my daughter and my family, I would have given up long time ago. Even though I went through tremendous pressures, but I managed to survive. What could be a better result than this? I have to say no!

1 Introduction

Most of the time, people stay indoors. The home environment is of an extraordinarily important indoor environment to occupants. It is not only because it can provide a warm and comfortable place for people to live in, but also its safety property to occupants. The home is becoming a more and more intelligent place thanks to the development of the Internet of Things (IoT) in the home environment. As a result, new lifestyles are coming forth in combination with the legacy ones. Also, the home environment is an application area and a complex place for occupants. The working of smart home systems in a safe manner thus becomes critical. Other than this, climate anomaly like heatwaves occurs a lot in recent decades, which greatly affects indoor climate and in turn occupants' health. All these threaten indoor safety. So this research focuses on home safety related to the system safety of smart home systems and the safety of indoor climate change.

1.1 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 [222]. Empirically, the place could be a house, apartment, etc. to protect the family from unfavorable outdoor conditions like bad weather. Occupants vary in age, gender and knowledge, etc. and explicitly have requirements, like eating, sleeping. The dwelling provides the infrastructure to collaborate with occupants to achieve their requirements. For example, a kitchen for cooking, beds for sleeping.

According to [77], The concept of home has several connotations. First, the home is as security and control. The control means occupants should have control over their houses. Second, the home is a site of activity. All domestic activities, like eating, sleeping, etc., occur indoors. Third, the home is a place for relationships and continuity. The home is a place to strengthen relationships with people, e.g., families and friends one cares for. The continuity indicates that the home is a temporal process. It relates to the question of the family in the way houses have been handed from one generation to

another permanently. Fourth, the home is dealt with as identify and values. It has three meanings, i.e., a reflection of one's ideas and values, an indicator of social status, and being a property to own.

1.1.1 Smart Home Systems

Definition

With the introduction of electricity, information, and communication technologies, great changes have taken place in the home environment since the 20th-century [173]. One of the representations of this change is the development of the concept of *smart home* since the 1990s [131]. The main goal of smart homes is to increase the comfort of the occupants and make everyday life more convenient. There are two ways to achieve the goal as pointed by [131]. The first is to increase the automation of identified human activities. The second is to elevate comfort levels, security, energy management, reduce environmental emissions, and energy-saving through state-of-the-art techniques.

Some definitions of the smart home and explanations of smart have appeared in the literature [34, 38, 77, 103, 139, 159, 173, 208, 227]. Some emphasize the networking capability [77, 103]. A smart home should have a communication network that enables sensors, appliances, controls, and other devices to connect for remote monitoring and control. Some consider the computing ability [159] that residence should be equipped with technology to monitor the environment and provide advanced services. To the author's point of view, a smart home should have computing capability together with information communication technologies that enable networking capability. Also, the smart home is based on the definition of home, which means occupants and the house infrastructure are implicitly part of the smart home. It may have the following characteristics [131, 208]:

- Adaptability: the ability to learn, predict and satisfy the requirements of occupants through feedbacks, e.g., the sensor network, human inputs;
- Connectivity: the ability to allow interactions among appliances, devices and users is based on the communication network infrastructure;
- Controllability: the ability to control devices, home networks, appliances automatically and/or manually so that multiple functions can be performed to satisfy various needs;
- Computability: controllers, appliances, and devices should have computing ability;
- Safety: the ability to perform functions in a safe way.

The smart home is to promote occupants with comfort, convenience, security, and entertainment. It should adapt to occupants and avoid unnecessary work of occupants. The smart home can increase occupants' free time to do other things like entertainment or to improve the quality of life, e.g., intelligently adjust home environment by using an HVAC (Heating, Ventilation, and Air Conditioning) system [167, 173], so an occupant can enjoy thermal comfort and do other things.

Technologies

In this section, some smart home technologies will be briefly introduced. They include networking, control, Interfaces, e.g., human-system, object tracking, and that related to the buzz-words of the Internet of Things (IoT) and cloud computing.

The development of smart homes accompanies the development of automation, networking, and computing technologies. In the very beginning, home appliances were working independently to accomplish a single dull work at a time. Independence means the home appliances cannot communicate (neither receive commands nor feedback data like its working states) with others through a communication network. The control of these home appliances depend on press buttons or turn on/off switches manually. For example, to turn on the illumination, or to switch a washing machine to the wash mode.

As the development of networking technologies, home appliances, controllers, etc., are capable to be connected [12, 208]. Home network interconnection technologies are typically classified into two categories, i.e., wired and wireless, as shown in Figure 1.1. They enable the interconnection among controllers, appliances, sensors, devices, etc. inside the home. For the detail of these technologies, please refer to the relevant documents.

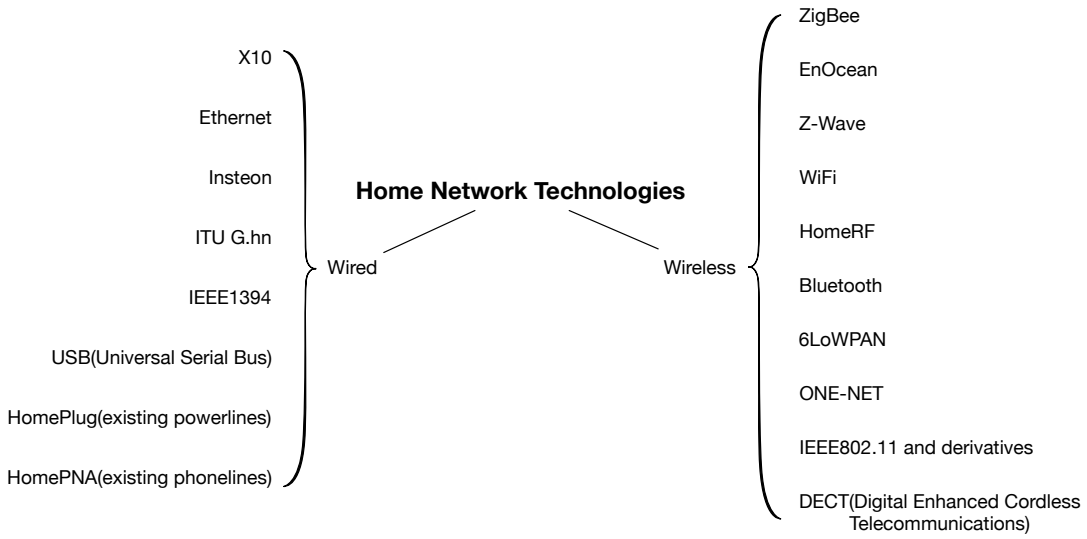


Figure 1.1: Classification of home network technologies.

Legacy home appliances cannot take advantage of these technologies since they do not have a network card. Legacy home appliances like microwave ovens, toasters, and consumer electronics are not intelligent and smart household devices. They have household functions to achieve for example cooking, washing, and entertainment, etc. [191]. To the author's viewpoint, the lack of intelligent and smart capabilities is due to the appliances that do not have computing and networking ability. [191]

figured out two characteristics of an appliance to be smart. First, an appliance can share its information, and its functions can be accessed, and its status and settings can be monitored and controlled by a user or an external device. Second, an appliance can automatically adjust and optimize its operation based on the commands issued by a user or a smart home controller or both.

A pervasive solution to connecting legacy home appliances to the home network is to use the so-called smart sockets or smart outlets. They are sockets or outlets that possess the following capabilities [52, 191]:

1. Computing capability that can, for example, to measure power consumption;
2. Networking capability that can transfer information, such as power consumption to and/or receive control commands from another device, e.g., smartphone.

Rely on the networking capability, controllers like smartphones can control (smart) home appliances. There are much work have appeared in the literature. [92] discussed a system that remotely controls electrical appliances in a house. The system employed Bluetooth and Java technology on a mobile phone that managed to eliminate the need to have various remote controls at home. [147] presented a framework that uses traditional home electric appliances with infrared remote controls for legacy home appliances. [52] discussed the integration of smart and legacy appliances into a generic system architecture. Authors of [196] proposed a method of home network formation by using Bluetooth devices and a method to control and monitor networked home appliances. [163] presented the design and implementation of SOAP-based (SOAP: Simple Object Access Protocol) residential management for home appliance control. [114] proposed a wireless network protocol called VSNP (Virtually Wired Sensor Network Protocol) and a control device, which makes it possible to control legacy home appliances interactively. The VSNP provides a bidirectional communication channel between a gateway and control devices. The control device that connects the wireless network to control a legacy home appliance on the request of a user. For managing the smart appliances, [182] proposed a system for recognizing electric appliances in-home networks, which can measure the power consumption of household appliances through a current sensing device. It transmits the current data back to the energy management platform, and identifies each electric appliance, then determines whether it is working normally according to its staged power consumption and various effects to avoid overloading problems. [198] proposed an appliance recognition method using current signals for an information-energy integrated network. The power-sensing data were measured by an intelligent outlet. [146] introduced software architecture to build ubiquitous computing environments. It assumes that every appliance, daily object, and even the occupant are equipped with pervasive services for communication. [191] integrated legacy appliances into the smart home through smart sockets.

There are two types of fundamental researches for the application of smart home systems. One is the interface between humans and the system. Another is the object or occupant tracking. To promote the convenience of the smart home for occupants to interact with it, human-system interfaces of the smart home are of particular importance. To our empirical experience, conventional interfaces of appliances to occupants are like a button of a table lamp and a switch of a washing machine. In the smart home environment, these become running short of ways in dealing with new situations. Newly

developing/developed ways take advantage of gesture, voice, face, etc. [118] proposed a method of the user-friendly interface that uses a natural language processing technique and an instant messaging system to control information appliances in smart homes. Information appliances are to perform the computation of predefined functions and to share information. To understand users' original intention by voice commands to proximately select devices. The authors of [119] proposed a method to select the most appropriate device among candidates by making use of complementary context feeding with incomplete interface information. It increased the accuracy of the smart home system to select the right device to perform the task of receiving a voice message command that may be incomplete to the system. [141] presented a system that extensively exploits uses' eye gaze information for operating services and appliances in-home network systems. A system called AXELLA (Adaptive and eXtensible Environment for Legacy and Leading Appliances) was designed and implemented to capture users' gaze, then invoke a service, and finally respond by voice. For the research of object tracking, it locates an object inside a room and tracks its moving trajectories. For example, [33] proposed an indoor tracking system based on common data mining techniques on radio frequency identification (RFID) tags readings. It can track several objects dynamically in the smart home context.

With the advent of IoT and cloud computing, the development of smart home systems has entered a new era. There are several definitions of IoT. For example, [95] defined it as a global infrastructure to support the information society. It enabled advanced services by interconnecting physical and virtual things based on existing and developing interoperable information and communication technologies. Another definition from [222] is that the network of things that embedded with electronics, software, sensors, and actuators, which enables these things to connect, collect, and exchange data, to integrate the physical world into cyber systems. The concept of the IoT is a result of the convergence of three visions [23], i.e., Things-oriented, Internet-oriented, and Semantic-oriented. Things have virtual personalities and identities operating in a smart environment connecting and communicating within the user, social, and environmental context. The Internet promotes the connection and interconnection among the "Things". The idea behind the semantic oriented IoT visions is that the number of things to be connected to the Internet will be huge in the future. Therefore, issues like the way to represent, search, store, interconnect, and organize information generated by the IoT becomes challenging.

The smart home is a promising application of the IoT. By integrating the IoT into the smart grid will benefit all involved parties, including the smart home due to a new way of managing electricity [188]. The IoT architectures, frameworks, and related technologies for applications bring great benefits to the smart home [16]. Four categories of benefits of smart home applications based on the IoT are identified in [16]. First, benefits related to smart home energy conservation. Second, reducing the cost of requirements like security and safety. Third, benefits related to healthcare, e.g., medical services, suitable living for the elderly, easy communication with health institutions, treatment alerts, and monitoring of elderly patients. The last is the entertainment and comfort. For instance, it provides comfortableness, easy to use and control, and pay bills easily.

The IoT-based smart home has the following characteristics [45, 129]:

1. Compatibility with different communication technologies;
2. Ubiquitous services;

3. Comprehensive perceptions;

4. Convenient controls.

There are many applications based on IoT. [22] proposed an IoT-based smart home system with several subsystems, e.g., energy-saving and home security. The authors of [51] explored the potential for exploiting information retrieved from two IoT devices that have limited storage capability. They focused on smart home devices to collect compromising information. [34] presented an IoT based smart home system for comfort, leisure, and security. [101] employed IoT technologies to propose an architecture of the smart home system. It enabled to integrate many applications into the system. Based on the Browse/Server module, [45] proposed a smart home system that enables remote control of household devices conveniently. An expansion of the smart home is the smart city. [236] focuses specifically on an urban IoT system. Urban IoTs are designed to support the smart city vision, which aims at exploiting the most advanced communication technologies to support value-added services for the administration of the city and the citizens.

[137] defined cloud computing as a model to enable network access to a shared pool of configurable computing resources, e.g., networks that service provider interaction or minimal management effort. It has three service models, i.e., software as a service (SaaS), platform as a service (PaaS), and Infrastructure as a service (IaaS). The application of cloud computing into a smart home can overcome the following limitations of conventional smart home systems [42]. First, there is no business model. Second, not smart. Third, security risks. Fourth, it cannot handle large amounts of data. To overcome these limitations, [42] proposed a smart home architecture based on cloud computing.

Some other researches take advantage of both the IoT and could computing to build a smart home system. [93] proposed an interoperable IoT platform for smart home systems by using cloud architecture and Web-of-Objects. The cloud is a central service and database to store the data acquired from the home and then for further analysis. [201] presented a multi-layer cloud architectural model that is developed to enable effective and seamless interactions/interoperations on heterogeneous devices/services provided by different vendors in the IoT-based smart home.

Architecture

In this section, a generic architecture of the smart home system will be introduced. It enables the implementation of various services, e.g., home energy management, multimedia entertainment, security, healthcare, and ambient assisted living. I summarized a generic architecture of smart home system from [15, 49, 64, 76, 103, 127, 148, 165, 187, 192, 214] that is shown in Figure 1.2.

The architecture consists of five parts, i.e., end items inside the home, home network connection, boundary devices, outer network connection, and outside facilities. End items include various meters, e.g., water meter and gas meter that measures the usages. Sensors are used to gather various indoor information, e.g., indoor temperature, humidity, and air velocity. Home appliances include smart appliances and legacy appliances that depend on the smart socket to connect to the home network. Renewable energy refers to energy sources like solar panels and batteries. The home network connection represents the home network that relies on home network technologies shown in Figure 1.1 to

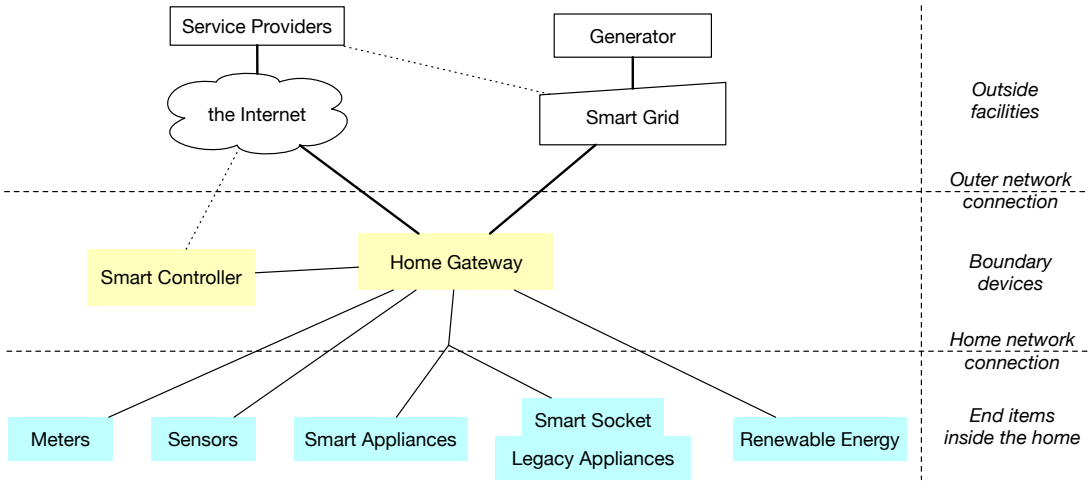


Figure 1.2: A generic architecture of samrt home system.

connect the end items. Boundary devices that joint the home network and the outside world. The home gateway is a pervasive concept to deal with the heterogeneous network protocols, end items, etc. Its fundamental function is to transform different network protocols between inside and outside the home. The smart controller means controller devices like handheld devices and smartphones. It has a friendly user interface that interacts with users. It can also connect to the Internet directly. The outer network connection denotes the outside network that refers to either the wide-area network or the grid network. Outside facilities roughly include two categories, i.e., the Internet and service providers connecting to the Internet, and the smart grid and the various generators. A service provider may take advantage of the smart grid to provide related services to the home environment. One possible implementation of the smart home system can rely on the multi-agent system platform [214].

Applications

There are many applications based on the smart home system. In this section, the home energy management system, healthcare, security, indoor environment adjustment, and ambient assisted living are going to be briefly introduced.

The smart home energy management system is defined as an optimal system that provides energy management services to monitor and manage electricity generation, storage, and consumption in smart homes [150, 238]. It monitors and arranges various home appliances dynamically to save electricity costs, and improves energy utilization efficiency. [130] surveyed and discussed five parts of the smart home energy management system, i.e., measuring devices, sensing devices, enabling ICT (Information and Communication Technology), smart appliances, and energy management systems. The advantages of the smart home energy management system are as follows [131]:

- The increased savings for both users and utilities providers;

- A reduced peak-to-average ratio and peak leads;
- They allows the household to be inserted in a systemic context, and allows it to be connected to the outside world so as to create the smart grid;
- They allow for historical comparison of home energy usage.

There are some researches relate to the home energy management system by considering demand response [181, 202]. Demand response can be defined as changes in the electric usage from normal consumption patterns in response to changes in electricity cost or incentive payments designed to induce low electricity usage during times of high wholesale market prices or suspected system reliability. [108] dealt with a comprehensive approach of a mixed-integer quadratic-programming model predictive control scheme based on the thermal building model and the building energy management system. This work demonstrates the optimal management of appliances such as heating, battery storage, a freezer, a dishwasher, a photo-voltaic system, and the opportunities to buy from and sell to the smart grid. [20] presented an Energy Management Algorithm for the smart home that is equipped with the fuel cell, battery, solar panel, and wind turbine. A fuzzy logic controller is designed for the energy management algorithm. To visualize the smart home energy management system, [63] proposed a visualization program of smart home energy based on smartphone APP.

Another application area of the smart home system is home healthcare [144]. Health smart home and healthcare monitoring systems are an integration of ubiquitous computing and communication technologies. It relates to like sensor systems, activities monitoring, and health monitoring. [164] presented a cloud-based smart home environment for home healthcare services. It includes a wearable unit, a private cloud, and a robot assistant in the smart home, which provides human contextual information and monitors the vital signs. One subset of this research area is the ambient assisted living. [73] presented a presence-aware smart home system based on the presence of information provided by all devices and objects in the home, which facilitates the daily living of private homes. [54] aimed to analyze the digital output signal of passive infrared sensors used in a configuration of smart home entrance called SmartGreeting. The system can be used to enable personalized services in an entire smart home environment. [98] proposed a resource-aware management system with a hierarchical smart home resource model by using the home context information. It accumulates home knowledge by analyzing and mapping the relations among objects. [213] proposed to use a context-sensitive and proactive fuzzy control system for controlling the home environment. A lighting control system was implemented by using a fuzzy control system design.

The security issue relates to several aspects, i.e., privacy, unauthorized access to smart devices, secure communication, misuse of information, system correctness, and existing malware attacks. Many works have contributed to smart home system security. [28] proposed a secure IFTTT-based smart home framework by incorporating a suitable captcha-based One Time Password (OTP) authentication scheme and Physical Unclonable Function (PUF). IFTTT (If This Then That) is an Internet service that integrates heterogeneous smart home devices and allows the user to customize smart home configurations via IFTTT recipes. The authors of [80] classified applicable threats according to a novel taxonomy. It focuses not only on the attack vectors that can be used but also on the potential

impact on the systems and ultimately on the occupants and their domestic life. An attack vector is a path or means by which a hacker or cracker can gain access to a computer or network to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities as well as human elements. They include, for example, viruses, email attachments, web pages, and instant messages. [128] presented a system that provides secure hierarchical identity encryption for the smart home to protect users' security and privacy. [84] provided a two-tier home automation network that provides a secure communication platform. For understanding the risks related to the use and misuse of information about homes and end-users, [96] examined 32 risks. [158] proposed an anomaly management framework for smart homes. The anomaly information is represented by Semantic Web ontologies. The framework can be used to detect anomalies related to hardware, software, network, operator, and context. [55] presented an approach for validating the Java implementation of a home network system to guarantee the correctness, safety, and the security of the system.

Other applications related to multimedia, e.g., [160] proposed a hybrid intelligent multimedia service framework that is mixed with application technologies like intelligent home infrastructure and multimedia protection/management through the ubiquitous sensor network-based technology to provide a proper multimedia service suitable for the Next Generation Home network Environment. [178] summarized current findings on the effect of measured environmental parameters on indoor air quality, individual thermal comfort, and living behavior in smart homes for the temperature climate zone.

The factors that affect the adoption and diffusion of smart homes are that compatibility, perceived ease of use, and perceived usefulness. They have significant positive effects on the purchase intention of a smart home system. Perceived usefulness was greater in the older and male groups, while compatibility was more important in the high education and female groups [30]. The authors of [183] found that highly-educated students seem ready to adopt the smart home concept, and the results highlight that smart home products could be targeted at this specific population.

1.1.2 Indoor Climate Changes

Due to global warming and weather anomalies around the world, bad weathers like heatwaves occur frequently in recent years. For example, many places in Asia, Europe, and North America had experienced the intense heat in the summer of 2018. It is observed that Japan had broken the highest temperature record in 2018 summer and the new record is $41.1°C$*. According to the record of this year, i.e., July and August of 2018 by the Ministry of the Environment of Japan†, the number of fatalities among heatstroke patients that sent to hospitals of 6 big cities of Japan had reached 151, while this number was just 42 in 2017. The statistical data by the National Meteorological Center of CMA‡ illustrates that China had experienced the hottest summer of 2018 since 1961. In northern Europe,

*Japan Meteorological Agency [Visited 2018.10.03] http://www.jma.go.jp/jma/index.html

†A dedicated website for *Heat Illness Prevention Information* of the Ministry of the Environment. [Visited 2018.10.03] http://www.wbgt.env.go.jp/

‡National Meteorological Center of CMA, China [Visited 2018.10.03] http://www.nmc.cn/

the 2018 heatwave had led to a record-breaking temperature and wildfire in many parts of Europe during the summer [§].

Climate changes like heatwaves and cold spells affect indoor climate [179]. [221] pointed out that indoor exposure to heat can be predicted using outdoor temperature and characteristics of the housing stock and surroundings. For example, indoor heat index can reach dangerous levels during heatwaves [166], and the high indoor temperature is indicated as a key cause of death [67].

Climate change and rapid population aging are significant public health challenges. Climate change causes mortality and morbidity due to heat and cold exposure. Heatwaves affect the elderly markedly more than younger people [67, 218]. Unfortunately, as reported in the *world population aging report 2013* [¶], the age group 60 years and older is expected to comprise 21.1% of the population by 2050. Heat exposure as identified to be associated with increased risk of cardiovascular, cerebrovascular, and respiratory mortality [185, 239]. Even a $1^{\circ}C$ temperature rise will increase cardiovascular, respiratory, diabetes mellitus, genitourinary, infectious disease, and heat-related morbidity [40]. Besides the easy affection to the elderly group, females are more sensitive to temperature changes [106]. In cold weather, people's chronic indoor thermal experience might be an important determinant of thermal adaptation [112].

In combining with weather anomalies, factors like economic, social, and health make elderly populations particularly vulnerable to exposure to temperature extremes and cause adverse consequences. This may limit their ability to mitigate or seek shelter from health-threatening conditions. The elderly, those in poor health, and the poor are especially at risk. Those populations experience temperature extremes almost exclusively in indoor environments [234].

1.2 Home Safety

With the transformation of home to the smart home, new forms of home safety problems have appeared. The time the home without the characteristics of automation, interconnection, smart, etc., the contents of home safety only focus on, for example, child neglect and abuse [203], accidents related to children [46, 143], and falls [102]. With the advent of the smart home system that was introduced in Section 1.1.1, system safety should be introduced into the home environment. As systems like cyber-physical systems interact with the physical environment, the hazard sources are the physical environment, e.g., indoor climate anomaly and the cyber world like the inability of systems.

1.2.1 System Safety

Earlier safety researches related to industrial safety to protect workers against industrial hazards. Later, it was applied to the engineering and operation of complex systems and called system safety [124]. Researches on system safety roughly include three big parts. First, the way to understand safety problems,

[§]Wikipedia: 2018 European heatwave. [Visited 2018.10.03] https://en.wikipedia.org

[¶]World population aging report 2013, Population Division, Department of Economic and Social Affairs, United Nations: [Visited 2018.10.04] http://www.un.org

which is called the accident model. Second, the way to evaluate the risk, e.g., fault tree analysis (FTA), event tree analysis (ETA), hazard and operability analysis (HAZOP), and system-theoretic process analysis (STPA). Third, the process of managing safety, which including risk management and safety case report.

For understanding why an accident could occur, a conventional way was the causality mechanism [24, 97, 123, 126], which are concerning reliability or dependability. A cause of an event is composed of a set of conditions, each of which is necessary and together are sufficient for the event to occur [123]. Given an event E, assume the sufficient set of conditions for E to occur is Z; the set of all necessary conditions for E to occur is Z'. Then Z' is the superset of Z. To illustrate the problem of causation and to investigate an event, a hierarchical approach to causality is shown in Figure 1.3 [126].

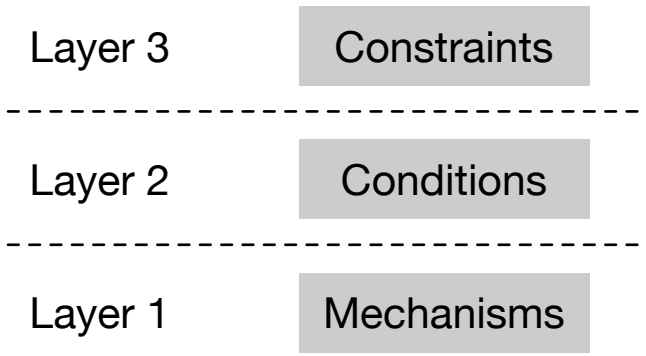


Figure 1.3: A hierarchical approach to causality.

The mechanism in the level 1 denotes a sequence of events until the accident, i.e., chain of events. The conditions in level 2 mean the satisfaction or lack of conditions that allowed the accident at the first level to occur. The constraints or lack of constraints in level 3 that allowed the conditions at the second level to cause the accident at the first level, or that allowed the conditions to exist at all. There are four types of constraints as follows.

1. Technical and physical conditions;
2. Social dynamics and human actions;
3. Management system, organisational culture;
4. Governmental or socioeconomic policies and conditions.

Causality has been applied to investigate accidents and various accident models, e.g., event-based models, chain-of-events models. Event-based models are also known as sequential accident models. It starts from a root cause, followed by a sequence of subsequent events to finally cause the accident. The root cause could be undesirable or expected event, e.g., a single unsafe act or condition. It works well for losses caused by failures of physical components or human errors in relatively simple systems. The

countermeasure to this accident causation is to identify and remove the single cause. Chain-of-events Models are timed ordered, multiple sequences of events in the form of hierarchies, e.g., event trees and networks. The events generally correspond to component failure, human error, or energy-related events. The countermeasure to this type of accident causation is to change individual events in the process.

Another chain-of-events model is from dependability. Dependability is defined as the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers [24, 97]. The impairments to dependability are faults, errors, and failures, which are undesired but not in principle unexpected circumstances causing or resulting from the undependability. A fault is active when it produces an error. An error may propagate to create another error. A failure occurs when an error reaches the system-user interface and affects service delivery. The failed component becomes fault types for components interacting with it.

The selection of the initiating event may be the event immediately preceding the accident or a particular event or condition. It should be familiar and acceptable to explain the occurrence of accidents. However, there are shortcomings for the above accident models. For event-based models, accidents always have more than one contributing factor. For the chain-of-events models, the development and analysis of such models are time-consuming and require significant analyst expertise.

With the rise of system safety, another type of model that is based on systems theory has been introduced. In this way, an accident is viewed as the interaction among humans, machines, and the environment. Models based on system theory usually related to one product of a set of hardware, software, and organizational factors. Accidents are the violation of a set of safety constraints on the behavior of system components. System models describe accidents in terms of dysfunctional interactions, control theory, or deviations and determining factors.

Many tools can be used to evaluate accidents and risk [125]. But they are all 40 to 65 years old, which some of them are shown in Figure 1.4. The FTA is a top-down and deductive failure analysis, in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. FMEA stands for Failure Models and Effect Analysis that was developed by reliability engineers to study problems that might arise from malfunctions of military systems. Event tree analysis (ETA) is a forward, bottom-up, and logical modeling technique for both success and failure. It explores through a single initiating event and then assesses the probabilities of outcomes. The HAZOP is a systematic way to identify possible hazards and operabilities problems in a work process. The bow tie analysis is a diagrammatic way of describing and analyzing the pathways of risk from hazards to outcomes and reviewing controls. It is the combination of the logic of a fault tree analyzing the cause of an event and an event tree analyzing the consequences. As with the advent of the introduction of computer control, exponential increases in system complexity, the introduction of new technology, and changes in human roles, conventional tools for evaluating methods may not apply to new systems. A new way of understanding accident causation that based on system theory called Systems-Theoretic Accident Model and Process (STAMP) and a new way of evaluating accident and risk called Systems-Theoretic Process Analysis (STPA) have been proposed [125].

There are engineering activities related to system safety as shown in Figure 1.5. All employers have the duty of caring for their employees, the general public, and the wider environment against occu-

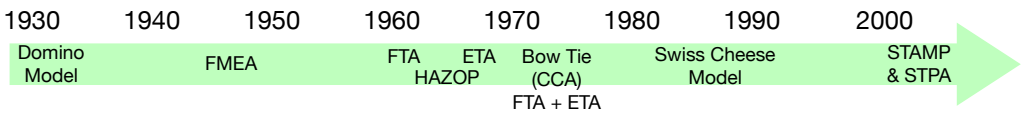


Figure 1.4: Chronology of tools of evaluating accidents.

pational diseases and accidents/incidents that result in injury/death or damage to the environment/equipment. Various safety standards like [2, 5, 6, 154, 155] establish many principles that need to satisfied to ensure the safety of products, processes, and services.

Safety management system standards provide the blueprint, or a framework, to help enable effective, robust, and sustainable programs to manage safety-related problems. Safety management system [11, 155] is the organizational structure, processes, procedures, and methodologies that enable the direction and control of the activities necessary to meet safety requirements and safety policy objectives. It provides a systematic way to control all processes relating to the management of safety for a system or organization. It also provides the means of managing safety and defining the processes to be followed to achieve the objective. Usually, the demonstration of safety is achieved via a Safety Case. Other definitions of the terms depicted in Figure 1.5 can be found in the related standards.

The components and process of a Safety Management System include four parts [4], i.e., safety policy and objectives, safety risk management, safety assurance, and safety promotion. The process of a Safety Management Process [204] starts with identifying and analyzing hazards under the predetermined scope, then evaluate the designed protective measures. If the desired safety level has achieved and then maintain the level, or re-assess and redesign the protective measures.

Risk Management is a systematic application of management policies, procedures, and practices to the tasks of hazard identification, hazard analysis, risk estimation, risk and ALARP evaluation, risk reduction, and risk acceptance [155]. It is important as it can ensure safety by identifying and managing hazards and potential accidents, risk management. A generic process can be summarized [6, 154] for managing risks is shown in Figure 1.6. The process for risk management is iterative.

Risk assessment is a series of logical steps to enable, in a systematic way, the analysis and evaluation of the risks associated with machinery [2, 6]. It is the overall process of risk identification, risk analysis, and risk evaluation. Risk assessment provides an understanding of risks, their causes, consequences, and their probabilities. The process of risk assessment is more or less the same concerning the relevant standards [2, 6]. The risk assessment is also an iterative process for evaluating risk.

Risk assessment is a part of risk management, which is a part of the safety management system. The process of risk assessment is always accompanied with products, processes, services, activities, etc., to understand the risk and as input for the selection of appropriate risk treatment.

1.2.2 Indoor Climate Safety

Globe warming and weather anomalies around the world have been discussed in Section 1.1.2. Abnormal weather affects indoor climate, which in turn causes health problems of occupants. People

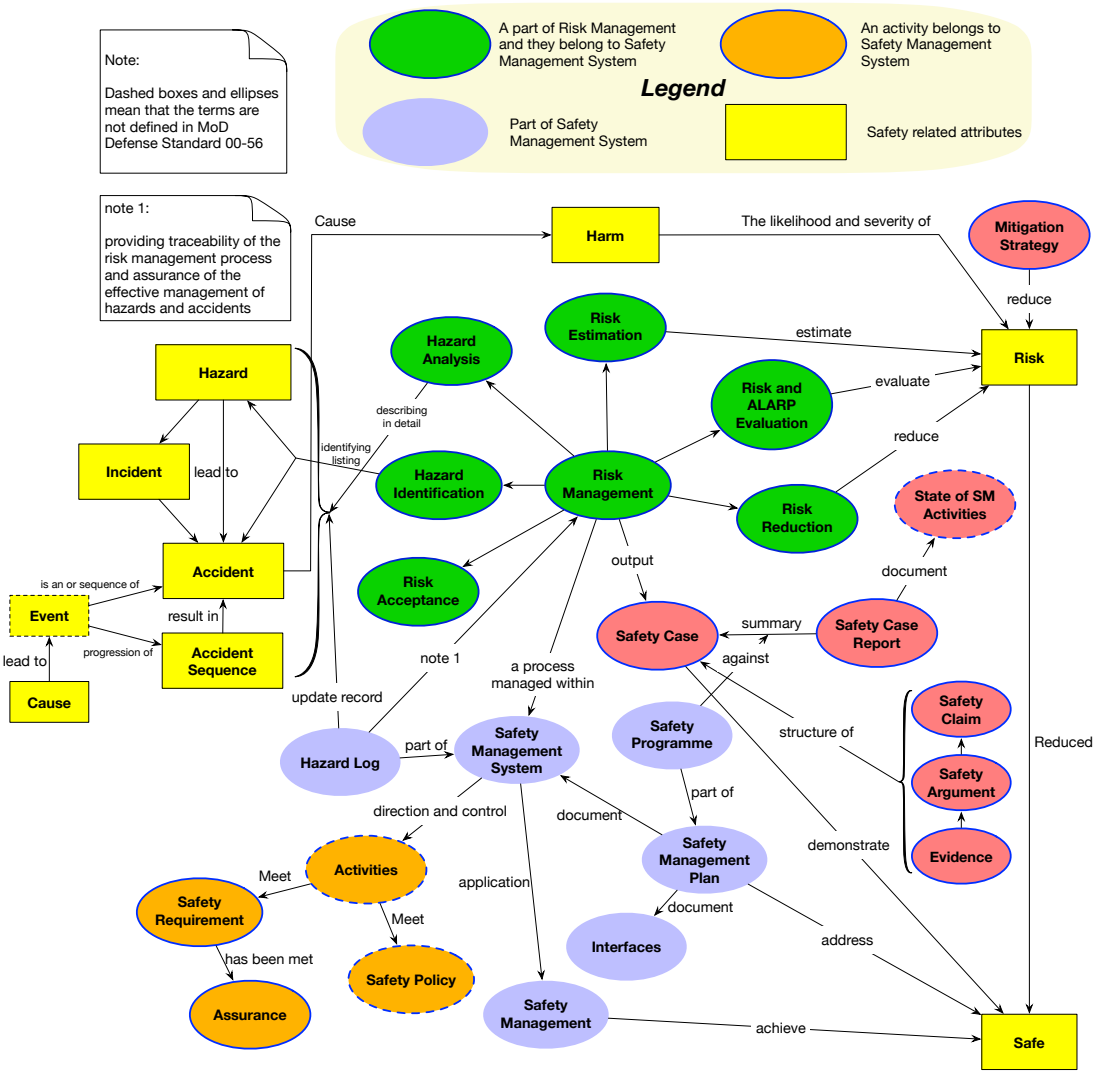


Figure 1.5: System safety engineering activities and their relationships and that with safety attributes.

stay indoors most of the time [110]. The indoor environment is thus important to the health and productivity [67, 68, 186]. In particular, indoor temperature anomalies can result in unfavorable thermal sensations. For instance, it is possible to cause heat illnesses or even death to like older people as a result of heat exposure [219, 221]. It can also affect sleep and circadian rhythm and result in cardiac autonomic response during sleep due to cold exposure [145, 156].

Previous work utilizes different indices to evaluate the indoor environment. These indices are sophisticated techniques to represent thermal sensations. They are calculated by concerning environmental and personal factors. For example, the PMV-PPD index [19] is used to evaluate the condition

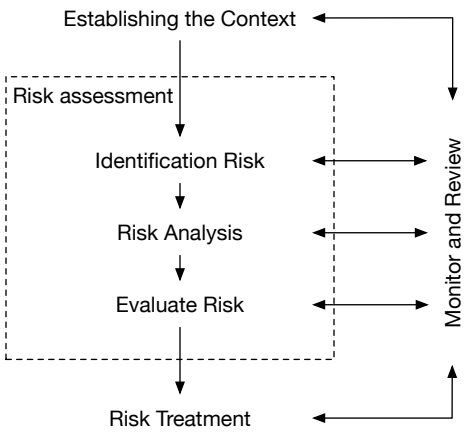


Figure 1.6: The process of risk management.

of the mind that expresses satisfaction with the thermal environment and is assessed by subjective evaluation. A cold index is an indicator to express the cooling effect on the body, which the cooling effect related to the cold stress. For example, a cold stress index called IREQ [1], which means the required clothing insulation of preserving body heat at defined levels of physiological strain. The heat index is widely used. It is an index that combines air temperature and relative humidity, in shaded areas, to posit a human-perceived equivalent temperature, as to how hot it would feel if the humidity were some other value in the shade. The widely used heat index is the wet bulb globe temperature (WBGT) in $^{\circ}C$ [37].

Various systems are designed to adopt these indices for evaluating the indoor environment. But to the best of my knowledge, they all focus on adjusting the indoor environment for thermal comfort. A field study was conducted in [168] in naturally ventilated office buildings to evaluate thermal comfort. The evaluation was based on the subjective judgments of occupants. Conventional on/off controllers are used to adjust the indoor temperature to approach desired levels. [70] took advantage of PMV index [19] for accurately adjusting the indoor temperature. It collects physical and personal data which are used to calculate the PMV-index to adjust the indoor temperature. We can understand this as dynamic desired levels. Some other work also considered energy saving. For example, [136] adopted fuzzy logic to represent different thermal sensations by linguistic variables to lead the air-conditioning unit to adjust the indoor temperature. A working state of the air-conditioning unit is when the indoor temperature belongs to a predefined interval that corresponds to a linguistic variable.

1.3 Problems and Contributions

Since the smart home system is getting more and more complex as discussed in Section 1.1.1, and the influence on the home environment due to like global warming and other weather anomalies discussed in Section 1.1.2. Home safety in this dissertation focuses on the indoor space, which reduces indoor

climate safety levels to an acceptable level concerning the smart home system.

The aim of this research is home safety problem detection/prediction. Home safety problems related to physical process anomalies occurred in the indoor space between occupants and home appliances. Physical process anomalies are due to the failed adjustment of indoor space, which causes hazardous situations and result in health problems of occupants. So, possible hazardous situations need to be identified, predicted, and detected to select appropriate precautionary or reaction measures to retain a normal adjustment of indoor physical processes that provide an indoor environment for the health of occupants.

Previous work only focuses on indoor temperature adjustment for thermal comfort as discussed in Section 1.2.1. The situations of heat and cold exposure should also be considered to ensure the safety of indoor space. To this end, an architecture is required, which supports the detection and prediction of safety problems. It is also necessary to understand how behaviors of the smart home system could cause hazardous situations. Furthermore, techniques for identifying the causes in the smart home system that result in abnormal system behaviors and cause physical process anomalies are also necessary. For hazard formation and cause identification, accident formation and hazard analysis techniques are for safety-critical systems, while the smart home system is generally not safety-critical only when working in situations of adjusting the heat or cold environment that causes health problems.

Home environment safety will be discussed in Section 2.2.2 of Chapter 2, which is the safety of indoor physical environment between occupants and home appliances. This research focuses on home safety problems detection/prediction based on the proposed home safety architecture. The proposed home safety architecture is based on Cyber-Physical Systems (CPS) and the Service Intermediary Model (SIM). The proposed architecture supports an event-based approach for the detection/prediction which has three levels of events to represent different semantic contexts. Safety problem refers to thermal related problems. The detection/prediction is based on the conformance of real data and its requirement by considering related thermal problems. The indoor environment is adjusted by the smart home system that involves various home appliances, e.g., window and air-conditioner for thermal comfort. Thus, an accident formation is required to consider physical processes and cyber systems. Also, hazard analysis techniques are required to look for the causes in cyber systems that result in physical process anomalies. The results of the analysis can further be taken as a theoretical basis for implementing a safer service for indoor environment adjustment. A more detailed discussion of problems will be at the beginning of each chapter of this dissertation. For the prediction, we will study the prediction of heat shock during a bath in Japan, which employed the technology of Bayesian networks.

The contributions of this research are briefly summarized as follows:

- For understanding accident formation of physical processes related to the smart home system, an accident model is proposed with respect to related definitions of concepts.
- To look for the causes of accidents, two hazard analysis techniques are adopted. One is called System-Theoretic Process Analysis (STPA) and will be tailored for this work. Another is an innominate approach that is based on the goal-based requirement engineering, guide words, and item sketch.

- To detect physical process anomalies that result in health problems, a home safety architecture is proposed that supports an event-based approach detection/prediction. Other activities like safety problem reactions are also possible to be performed based on this architecture.
- To perform the detection, a multiple-conformance approach is proposed, in which the required changes of indoor temperature are moded by hybrid automata.
- Temperature data were collected from a testbed smart house to verify the effectiveness of the multiple-conformance approach with respect to the hybrid-automata-modeled requirement.
- Bayesian network is adopted to predict heat shock during bath.

A detailed description of the contributions of this research is introduced in each chapter of this dissertation.

1.4 Scope of this work

I outline the scope of this work by comparing it with IEC 63168-2, -3, and -4 standards [7, 8, 9]. There are several reasons. First, the comparison can position this work in a product/system lifecycle, since the IEC 63168 series prescribe to cover all phases of a product/system lifecycle. Second, the IEC 63168 series can be taken as related work in the viewpoint of safety research activity[‖]. This is due to the IEC 63168 series specifies Active Assisted Living (AAL) specific functional safety requirements of electrical/electronic (E/E) safety-related systems for cooperative multiple systems that operated in a connected home environment. Third, it can distinguish this work with others, because the overlapped and unique considerations can be identified.

The comparison is at the abstract level because standards do not prescribe technique details. Table 1.1 outlines the comparison results. This work focuses on the concept and software design. The accident model and hazard analysis techniques adopted in this dissertation are state-of-the-art and based on system theory. Risk evaluation is not explicitly covered in this dissertation. However, there are two ways mentioned related to the evaluation of risk. First, I classify situations as normal, abnormal, and unsafe. Second, I pick up unsafe cases like the occurrence of heat shock for detection and prediction. This dissertation focuses on usage safety that related to the smart home system, so occupants are of main concern. IEC 63168, on the other hand, focuses on activities of the lifecycle of a product/system, so it concerns more on the professionals. The techniques mentioned in this dissertation aimed at software design and development, while the IEC 63168 focuses on both software and hardware.

1.5 Reading Guide

Chapter 2 introduces the way how a safety problem related to physical processes can occur, and this is represented by a proposed accident model. In Chapter 3, hazard analysis techniques are adopted to

[‖]Standards are typically aimed at supervising the activities related to a product/system in the lifecycle, while the research work like in this dissertation focuses on specific techniques.

Table 1.1: A comparison of this work with IEC 63168 to outline the scope of this work.

	Phase of lifecycle	hardware or software level	Accident model	Hazard identify or analysis	Risk evaluation	Human	Techniques
This work	Concept and design	Software	STAMP-PP (Ch. 2)	Tailored STPA (Ch.3)	Not covered	Mainly occupants	Softeware related (Ch. 4, 5, and 6)
IEC 63168	All	Hardware and software	Event based	Bottom-up methods like FMEA; Top-down methods like FTA	H-SIL	Mainly professionals	Only mention the work to be done; Related to software and hardware

analyze the causes of safety problems. Then, a home safety architecture is proposed in Chapter 4 for thermal problem detection. Based on the proposed home safety architecture, an event-based approach is proposed for detection. For the detection of thermal problems that occur in the physical world, a multiple-conformance approach is proposed in Chapter 5, which takes the required temperature change as the requirement. Chapter 6 introduces to employ Bayesian networks to predict heat shock during bath. Finally, Chapter 7 concludes this dissertation and points out some future work.

The relationships between the chapters of this dissertation are shown in Figure 1.7. The accident model introduced in Chapter 2 connects the physical world and the cyber world to understand the safety problem formation. Then to identify the causes in the accident model, Chapter 3 discusses to adopting hazard analysis techniques. Chapter 4 introduces a proposed architecture for physical problem detection. Based on the architecture, Chapter 5 proposes an approach for detecting undesired temperature change that causes health problems, and Chapter 6 introduces the way to build the Bayesian network for predicting heat shock during bath. Finally, Chapter 7 summarizes all these chapters and concludes this work.

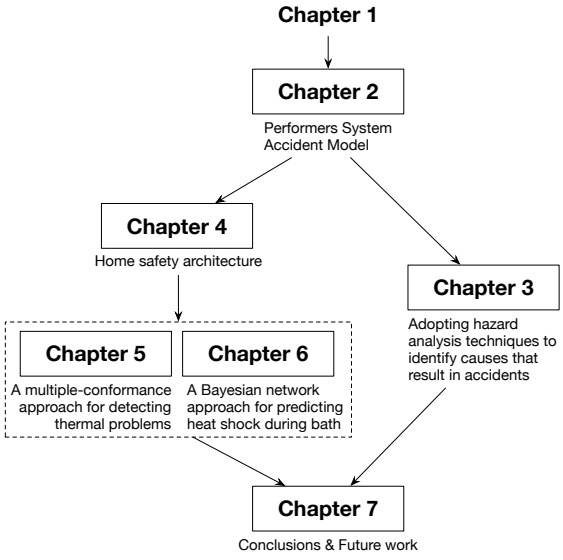


Figure 1.7: Relationships between chapters.

2
Safety Problem Formation

Home safety involves two parts, i.e., the safety of the cyber world (the safety of smart home systems) and the safety of the physical world (physical environmental safety). Conventionally, these two parts belong to two different research areas, i.e., system safety and meteorology. They are connected by the behaviors of smart home systems. For comprehensively understanding the relationship between the cyber and physical worlds, an accident model and its related terms are proposed in this chapter.

The contributions of this chapter are summarized as follows [228, 231]:

- The concept of Performers System that emphasizes the behaviors are performed by various home appliances is proposed.
- The definitions of Service and its derivative terms with respect to the Performers System are defined.
- I propose the accident model (denoted as STAMP-PP) for understanding accident formation, that is, abnormal system behaviors result in abnormal changes in physical processes and cause hazards.
- Validation of the accident model is by considering indoor temperature that was adjusted under the scenario of injecting control errors.

2.1 Introduction

Accident models provide a conceptual representation of accident causation [212]. The state-of-the-art development of them is on the phase of systemic models [85, 125, 212], i.e., accident models based on system theory rather than reliability. They have been applied to understand accidents in many areas, e.g., deepwater well control [138], railway [157], and aviation [17]. Some others relate to places periled by poisonous or dangerous substances, e.g., oil transportation [75] and nuclear power plants

[48]. The 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 means the indoor space regarding physical processes, e.g., temperature change, which is different from safety-critical environments in workplaces. The home environment is not a hazardous place in general. However, it could be when the physical process transfers from a normal state (e.g., temperature for thermal comfort), then go through some intermediate states (e.g., temperature for thermal discomfort), and finally reach a state of hazardous (e.g., temperature for heatstroke). The home environment is a place for everyday living and not 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 [85, 125, 212], 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 understanding accident formation. For example, a smart home system violated its constraint on adjusting the indoor temperature for thermal comfort, and result in high temperature for heatstroke. The physical process of temperature change from for thermal comfort to some intermediate states for discomfort, then to a high-temperature state that can cause, e.g., heatstroke is missing. This process is important due to not only the understanding of accident formation but also reactions and precautionary measures need this information. Because when an intermediate state of the physical process is detected, which indicates a possibility to transfer to a hazardous state. So, precautionary measures are needed to restore a normal state of physical processes. If a hazard is detected, which indicates reaction measures are required to restore a safe state of physical processes. 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 which is abbreviated as STAMP [125] is considered. It is based on general system theory for understanding accident causality of socio-technical systems. A brief introduction of it will be conducted in Section 2.3.1. I extend it by considering the following facets. First, the home environment is not inherently hazardous. It provides a comfortable environment in some physical process states and results in harm in some others. So I 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 due to physical processes are the results 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 chapter, I extend the STAMP model by 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; 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 the harms of people. 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.

2.2 Preliminaries

In this section, let us discuss the characteristics of the smart home based on the discussion in Section 1.1.1 and home environment safety before introducing the STAMP-PP model.

2.2.1 Smart Homes

A home* is a place for people like individual or family members, etc. to live. It is the place where the social unit, i.e., family lives permanently. Since the 20th century, with the introduction of electricity, informtion and communication technologies, great changes have been taken place in the home [173]. One representation of this change is the development of the concept of smart home since the 1990s [131]. The primary objective of the smart home is to increase occupants' comfort and make daily life easier. The smart home has some characteristics [131, 212], e.g., adaptability, connectivity, controllability and computability. These are discussed in the viewpoint of technology. This section discusses the characteristics of the smart home in the viewpoint of occupants.

- Partial Automation: Although the home lives have been automated a lot than ever due to the development of electricity, electronics, and network technologies, there are still lifestyles left unchanged in practice. For example, pots and pans are used for cooking with gas in everyday meals. So, the home nowadays is with partially automated in practice as shwon in Figure 2.1.

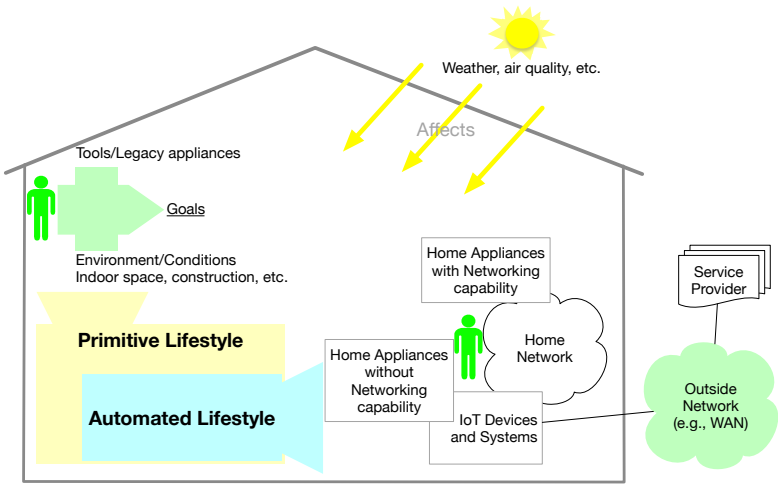


Figure 2.1: Lifestyles in a home.

*Wikipedia, keyword: home. https://www.wikipedia.org

- Application Area: The home is the place to live. Various off-the-shelf products are used to improve the quality of life. They 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 from product instructions or other occupants.

- Complexity: The complexity of home owing to three aspects, i.e., varity of appliances and products; occupants in ages, health conditions, knowledge, gender, etc.; and outdoor environment. The off-the-shelf appliances and products indoors are with various purposes and produced from different manufacturers. In smart homes, they are connected together by the smart home network to enable a variety of services [131, 208]. Different from workers in workplaces which are rely on skills, rules, and knowledge for a specific work [169], occupants are usually based on 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 impact the working of indoor appliances or devices. All these make the smart home complexity.

2.2.2 Home Environment Safety

If you look up 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 [125], 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 [140]. 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 [155]. 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 known to all that indoor climate is affected by outdoor climate. Bad weather like heatwaves occurs frequently recently years due to global warming and weather anomalies around the world. For example, many places globally had experienced intense heat last summer (2018). It is observed that Japan had broken the highest temperature record and reached a new level of $41.1\,^{\circ}C$[†]. Indoor climate can thus be endangered by the outdoor climate anomalies.

The indoor climate is adjusted by dedicated home appliances, e.g., use air-conditioners to adjust the indoor temperature. Integrated services [43, 149] are that provided by integrating various home appliances through home networks. For instance, an indoor temperature adjustment service that can possibly adopt a window, an air-conditioning unit, and a curtain for thermal comfort. 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 aware of the new item

[†]Japan Meteorological Agency [visited 2018.10.03] http://www.jma.go.jp/jma/index.html

and cause safety problems when using it. Therefore, the 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, it also needs to discuss people relate to the smart home. This is mostly because home appliances are produced and operated by people. One type of people belong to the professionals. They relate to the activities of design, manufacture, transport, installation, and disposal of appliances. One distinguishing characteristic is that they have expertise in a certain field. Another type is occupants who usually non-professionals. They are the customs that use various home appliances. Both types of people can affect home environment safety in different ways. For professionals, they 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. Let us talk about occupants in this paper.

2.3 Accident Model

Due to the smart home is an application area, the STAMP-PP model is discussed concerning system operations rather than system development. It aims to understand 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 [230], 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 uncomfortable or harm. The connection between smart home systems and the home environment is the system behaviors. In this section, let us first give a brief introduction of the STAMP model, then discuss in detail the proposed STAMP-PP model.

2.3.1 STAMP

In systems theory, systems are taken as interrelated components which kept in a state of dynamic equilibrium through feedback control loops. Figure 2.2 presents a standard control loop [125]. The STAMP model is based on the system theory and not reliability that traditional accident models ground on to understand accidents. Safety, in the STAMP model, is an emergent property of systems. Accidents are due to missing or inappropriate constraints of system design or operations. The STAMP model consists of three building blocks, i.e., a hierarchical safety control structure, safety constraints, and process models.

Safety constraints are basic building blocks in the STAMP model. Losses resulted from the unsuccessful enforcement of safety constraints. Systems, in system theory, are considered as multiple-levels of structures, where higher one prescribes constraints on the lower levels activities. Constraints are

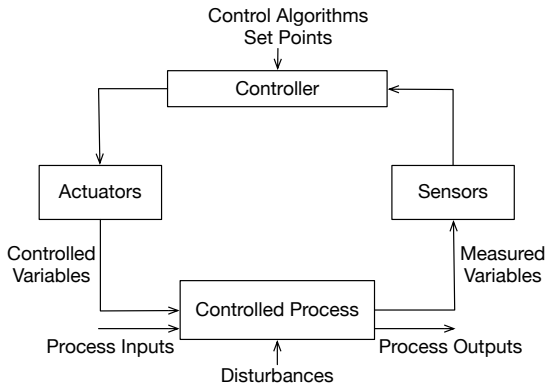


Figure 2.2: A standard control loop.

enforced by control actions of a higher-level system component (controller) to the lower level one (controlled process).

The layered safety control structure presents all stakeholders with their internal structures within the interested system, and control actions and feedbacks that connect the independent stakeholders and their internal components [17]. Control processes occur when a higher level of system controls lower-level processes. The feedbacks provide information about how effectively the control actions to ensure the constraints. 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, inappropriate safety control commands, incorrect execution of commands, and inappropriate feedback about the effects of constraints.

Process models are utilized by controllers to choose appropriate control actions. It is up to the type of controller. For an automated controller, the process model resides in control logics. For a human controller, the process model is the mental model. In both situations, it contains essential relationships among system variables, the current system state, and the ways to change states of the process. There are four conditions to control a process, i.e., goal, action condition, observability condition, and model condition. Accidents relate to component interactions are generally be explained as an incorrect process model. The process model 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 due to flawed processes that cause disobeying the system safety constraints. Flawed processes include interactions among societal and organizational structures, physical system components, operations, and engineering activities. Accidents caused by processes are characterized with respect to an adaptive feedback control loop that fails to retain safety as the dynamic system performance to achieve an intricate set of goals and values.

2.3.2 STAMP-PP

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

Performers System

Indoor environment adjustment services adjust the indoor environment with respect to various home appliances. To differentiate the home appliances with other indoor items, e.g., router or furniture, let us 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 the networking capability so that it can be used by indoor environment adjustment services. Second, it has functions of adjusting the indoor environment, e.g., to adjust the indoor temperature or dehumidification.

Let us classify two types of Performers concerning how to adjust the indoor environment. The first is the direct adjustment, e.g., an air-conditioner cools or heats the indoor environment directly. Second, indirect adjustments, e.g., an electric window introduces air flows or solar radiations of outdoors, which indirectly adjust the indoor temperature. In the latter case, the outdoor climate is passively used to adjust the indoor environment. Then let us define the Performers System based on the concept of Performer.

Definition 2 (Performers System)**.** *It is the system of all installed* Performer*s that are connected through the same home network.*

By connecting the Performers System to the same home network to ensure the utilization of the same integrated service of indoor environment adjustment. The Performers System has a goal that prescribed by the integrated service of indoor environment adjustment. The goal is achieved by taking advantage of the functions of the Performers of the Performers System. Each Performer is regarded as a component system of the Performers System. However, all related Performers may not work simultaneously. Figure 2.3 illustrates an example of the Performers System. It consists of an electric window, an air-conditioner, and an electric curtain. They are taken as Performers, which connect to the same network and are the capability of adjusting the indoor temperature. When adjusting the indoor temperature for thermal comfort (the goal), the integrated service of indoor temperature adjustment could use any combination of the Performers, but not necessarily them all. The indoor temperature adjustment service is embedded in the smart home system core. The Performers can, of course, be operated by occupants who are also the beneficiaries of the adjustment.

The Performers System can adjust the physical processes of various climatic properties, e.g., temperature and humidity, through functions provided by the Performers. These physical processes may

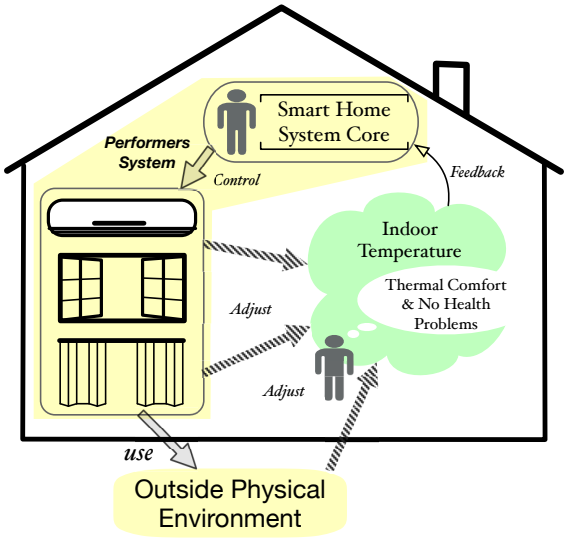


Figure 2.3: An example of the Performers System.

have different forms. For example, increase or decrease the indoor temperature to the prescribed temperature level for thermal comfort.

Service

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

Definition 3 (Behavior)**.** *The behavioral representations of the functions of* Performers System *in adjusting the indoor environment.*

The Behaviors are the representation of the functions of related Performers. For instance, the Performers System in Figure 2.3 can cool the temperature down (behavior), which could be achieved by setting a lower temperature level under the cool mode of air-conditioner (function). The representation of the Behaviors is the physical process, e.g., temperature change.

For the Behavior to adjust physical processes, e.g., changes in indoor temperature, humidity, and wind speed, expected behaviors can be divided into two phases, i.e., approaching behavior and maintenance behavior. Approaching behavior means a physical process approaches the desired level. After reaching the desired level, the physical process should be stable at the desired level. To maintain a stable level is called maintenance behavior. Next, let us formally represent the Behaviors of the Performers System with respect to indoor temperature, humidity, and wind speed.

For the indoor temperature (*Temp*) that is adjusted by a Performers System (*Per*), given a point p in the useful space (US) that will be introduced in Section 2.3.2, the approaching behavior to ad-

just the indoor temperature within the time interval $[t_1, t_2]$ is represented in Formula 2.1 ($\rightarrow$ denotes approaching). $E(p)$ denotes the effect of the adjustment, i.e., the approaching behavior at the point p.

$$\bigcup_{p}^{US} E_{(Per,Temp)}(p)|_{t_1}^{t_2} \rightarrow \pm V_{Temp}) \tag{2.1}$$

After reaching the desired level, the Behavior of the Performers System became maintenance behavior. It maintains the temperature to stabilize at the desired level. The maintenance behavior is represented by using the Formula 2.2 ($\approx$ means stable at).

$$\bigcup_{p}^{US} (E_{(Per,Temp)}(p)|_{t_3}^{t_4} \approx V_{Temp}) \tag{2.2}$$

Then let us consider the Behavior of the Performers System to adjust indoor humidity to the desired level. Humidity is the degree of moisture in the air. One way to measure the humidity is the humidity ratio, which is the radio of the mess of water vapor to the mess of dry air in a given volume [19]. The representation is similar to that of the indoor temperature. However, the Performers System is used for humidity adjustment, and it takes a different time interval to reach the desired level. The approaching behavior is represented by using Formula 2.3.

$$\bigcup_{p}^{US} (E_{(Per,Humid)}(p)|_{t_5}^{t_6} \rightarrow \pm V_{Humid}) \tag{2.3}$$

Maintenance behavior maintains indoor humidity by the Performers System is similar to that of the maintenance of the indoor temperature. And it is represented by the Formula 2.4.

$$\bigcup_{p}^{US} (E_{(Per,Humid)}(p)|_{t_7}^{t_8} \approx V_{Humid}) \tag{2.4}$$

The last is for wind speed. It is the rate of air movement at a point in disregarding its direction. Similarly, it is similar to that of the adjustment of the indoor temperature. However, the Performers System is used for wind speed adjustment. The approaching behavior is represented by Formula 2.5, and the maintenance behavior is shown in Formula 2.6.

$$\bigcup_{p}^{US} (E_{(Per,Airspeed)}(p)|_{t_9}^{t_{10}} \rightarrow \pm V_{Airspeed}) \tag{2.5}$$

$$\bigcup_{p}^{US} (E_{(Per,Airspeed)}(p)|_{t_{11}}^{t_{12}} \approx V_{Airspeed}) \tag{2.6}$$

Choose the right Performers to work is important. There are some criteria on how to choose the appropriate Performers. Choose the ones near the useful space, especially the anchor point, i.e., either

occupant location or a designated indoor location. The concept anchor point will be introduced in Section 2.3.2. From the viewpoint of energy saving, choose the minimum Performers (at least one) to work.

Definition 4 (Service)**.** *The* Behavior*s of* Performers System *that can satisfy comfort requirements of occupants.*

One example of the Service can be the Performers System in Figure 2.3 increases the indoor temperature to 22 $^{\circ}C$ for thermal comfort. Comfort is that the state of the indoor environment satisfies physical and psychological perceptions, e.g., thermal comfort. Let us use it to evaluate Behaviors that can be taken as Services, and thus implicitly constraint on the Behaviors. The comfort has different contents for different goals of the Performers System, e.g., thermal comfort and comfort to the humidity.

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. This way is easy to be implemented but is limited in some situations. For instance, a baby or elderly person may not sensitive to temperature change due to the nervous system is not well developed or is degenerated. The second way is to automatically evaluated by algorithms embedded in smart home systems. This depends on various indices [18, 19] for evaluating the physical environment for thermal comfort. For example, the PMV-PPD index [19] is used to evaluate thermal comfort by considering environmental factors and personal factors. PMV and PPD means predicted mean vote and predicted percentage of dissatisfied, respectively, and are calculated based on Formulas 2.7 and 2.8, where TS means thermal sensation transfer coefficient and depends upon the metabolic rate, MV represents the internal heat production in human body and is calculated concerning external work and metabolic rate, and $HL1$, $HL2$, $HL3$, $HL4$, $HL5$, and $HL6$ represent heat losses through skin, sweating, latent respiration, dry respiration, radiation, and convection, respectively. Then combine with the ASHRAE thermal sensation scale as shown in Table 2.1 to determine the comfortableness. The details refer to [19].

$$\begin{aligned} PMV = TS \times (WM - HL1 - HL2 - \\ HL3 - HL4 - HL5 - HL6) \end{aligned} \tag{2.7}$$

$$PPD = 100 - 95 \times e^{-0.03353 \times PMV^4 - 0.2179 \times PMV^2} \tag{2.8}$$

Data on environmental factors, e.g., humidity are collected by (e.g., humidity) sensors. Data related to personal factors, e.g., metabolic rate, one can evaluate based on occupant's activities. Another way is to make full use of wearable devices to gather personal data and evaluate the comfortableness at places like smart home systems. However, to the best of author's knowledge, wearable devices are unable to collect data of cloth insulation. One can only manually evaluate various clothes. Then to scenarios like in hot summer, one can evaluate the wearing clothes by looking up their corresponding insulation values and add them together.

Table 2.1: ASHRAE thermal sensation scale.

hot	warm	slightly warm	neutral	slightly cool	cool	cold
+3	+2	+1	0	-1	-2	-3

A Service can be to satisfy occupants' other requirements. Even though these requirements are not the main concern of this dissertation, it is worth discussing here. The requirements could be providing occupants a theater circumstance, room cleaning, ventilation, etc. Occupants are also the beneficiaries of the Services, which therefore promoting living qualities. There are many Services in the home environment. Empirically, different rooms have different functionality and are deploying specific home appliances that can be used in that room. For example, an example of the room layout is depicted in Figure 2.4. The room has an entrance hall, a kitchen, a living room, a bedroom, a toilet, a washroom, and a bathroom. Each room is used for a different purpose and thus equipped with different home appliances with various functions.

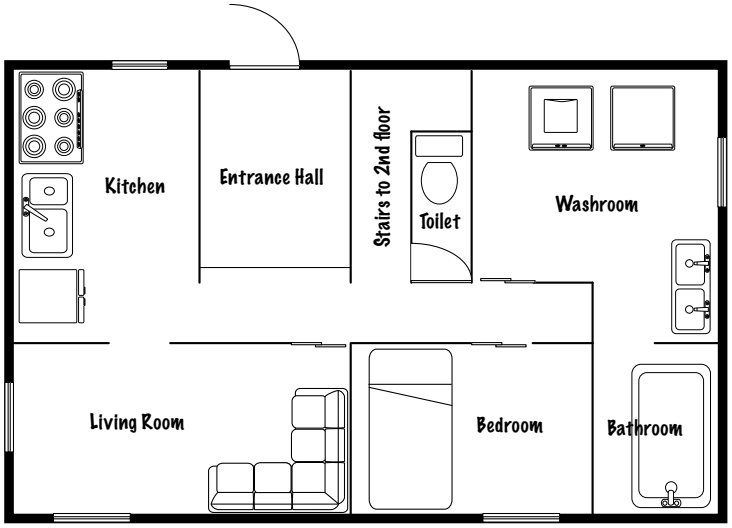


Figure 2.4: An example of layout of a room.

Possible functions of home appliances for each room is shown in Figure 2.5. For example, the living room requires security, entertainment, lighting. I surveyed the home appliances from Amazon[‡], and listed the functions of each home appliances, then summarized the services based on these functions

[‡]Amazon is an American electronic commerce and cloud computing company based in Seattle, Washington, that was founded by Jeff Bezos on July 5, 1994, .https://www.amazon.com/

that are required by each room[§]. Finally, I classified the services into different categories as shown in Table 2.2.

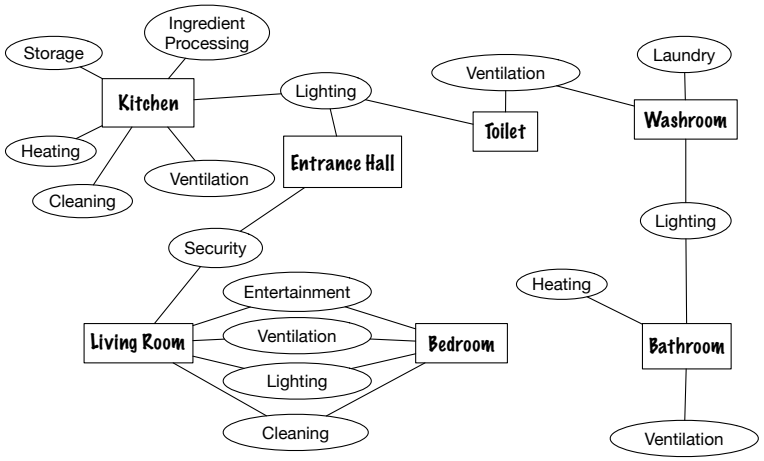


Figure 2.5: An example of home appliance categories w.r.t. the functions.

Definition 5 (Service Manner)**.** *The* Service *is delivered in a particular condition.*

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 person in hot weather with a sedentary person in winter. Conditions about the sweating person are high outdoor temperature, high metabolic rate, and requires cool the temperature down. For the sedentary person, the conditions can be low outdoor temperature and metabolic rate and require warm the temperature up.

Indoor activities are performed under various conditions, thus require different contents of Services. Indoor activities are to satisfy either physiological needs, e.g., sleep or that related to occupants' living habits, e.g., cleaning the floor. One classification of human activities is conducted by NHK[¶] in their time use research. They are necessary activities, e.g., eating and sleeping, restriction activities, e.g., social event participation, go to school, and work, and free movement activities, e.g., conversation with people and take a rest. This classification concerns not only indoor activities but also outdoors'. In this work, indoor activities are of main concern. By considering indoor activities and the services been classified, some activities may not affect the service delivery, e.g., sleep, some activities may have an affection for the service delivery, e.g., cooking. Therefore, the services can be classified into passive activities and active activities. Passive activities are that when performing an activity the service

[§]Please refer to the Appendix A.1 and A.4 for the details of the functions of home appliances and their services.

[¶]It is the Japan Broadcasting Corporation, which is a publicly owned corporation funded by viewers' payments of a television license fee. https://www.nhk.or.jp

Table 2.2: Classification of home appliance services.

L1 Service Classification	L2 Service Classification	Service Details
Ambient Regulation	Volume Control	Volume up
		Volume down
		Maintains a volume level
	Luminance Adjustment	Increases brightness
		Decreases brightness
		Maintains a certain brightness
	Air Purification	Removes airborne pollutants
		Reduces odors
		Absorbs volatile airborne pollutants
		Kills microorganisms that cause disease
		Eliminates musty odor
		Exhausts heat, steam, odors, fumes, etc.
		Filtrates airborne grease, smoke, combustion products
	Humidity Regulation	Reduces humidity level
		Increases humidity level
	Temperature Control	Cool down
		Warm up
		Maintains a certain temperature
	Ventilation	Increases airflow rate
		Decreases airflow rate
		Change airflow direction
Housekeeping	Housekeeping	Heat up for cook
		Clean dust and dirt
		Washing-up
		Shreds food waste into pieces
		Make coffee
		Wash clothes
		Spin-dry
		Authenticates the "keys"
		Open the door
		Close the door
Entertainment and Telehealth	Entertainment and Telehealth	Image display
		Volume up
		Volume down

delivery will be of little or no affection. Active activities are that when performing an activity the service delivery will be affected. Service delivery is the process of delivering a service while performing a specific activity. There are three ways to deliver a service by the Performers System. Based on this, I classified indoor activities into three categories as shown in Figure 2.6.

Definition 6 (Critical Service Manner)**.** *In a specific time, the* Service Manner *is required to deliver.*

This definition is given in the viewpoint of people who need the Service. It considers the timeliness property of Services. In the example when explaining the Definition 5, the adjustment of indoor temperature to achieve the cool effect for thermal comfort is the Critical Service Manner to the sweating man; the adjustment of indoor temperature to achieve the warm effect for thermal comfort is the Critical Service Manner to the sedentary man.

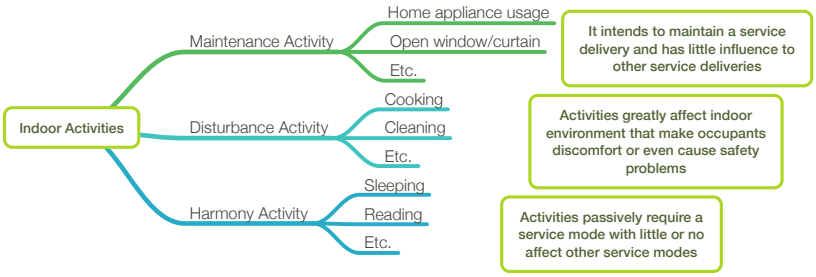


Figure 2.6: The classification of indoor activities.

Figure 2.7 illustrates the abstract structure of a Performers System for service delivery. Figure 2.8 shows examples of the corresponding concepts introduced in this section. The relationships among the concepts of Behavior, Service, and Service Manner are depicted in Figure 2.12.

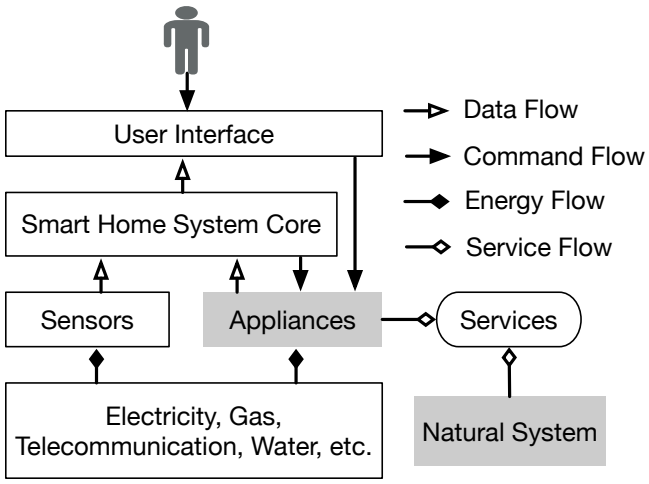


Figure 2.7: An abstract structure of the Performers System for service delivery.

Useful Space

Usually, due to the contact area, heat conduction, and the effects of working on home appliances, the Critical Service Manner has varied effects in different locations of a room. Space is the indoor physical space between occupants and home appliances. By considering energy saving, the ability to adjust physical processes, and occupant's will, it is better to divide the space into different subspaces for better understanding the effects on them.

Concepts	Examples
Performers System	Combine air-conditioner, window and curtain for indoor temperature adjustment
Behavior	Temperature adjustment
Service	Temperature adjustment to satisfy thermal comfort
Service Manner	Cool the room to decrease indoor temperature for thermal comfort Warm the room to increase indoor temperature for thermal comfort
Critical Service Manner	In hot summer, cool the room for thermal comfort is currently required

Figure 2.8: Examples of these concepts.

The Area of Effect (AoE) [133] of a home appliance is the physical space, over which the considered physical process can be adjusted by the home appliance. The intensity of a climatic property at a certain point in the space is the intensity of the desired effect. The intensity of an AoE of a home appliance should be within a certain threshold interval. The measurement unit of the intensity differs up to the measured climatic property. Unfortunately, [133] did not define other related subspaces. In this section, I will define other spaces based on the AoE.

The first term is Ineffective Space. It is an indoor space that the adjustment of a home appliance in this space beyond its desired effect. The desired effect can be understood in the occupants' viewpoint. It is a beneficiary centered requirement on a Critical Service Manner of a specific physical property. The beneficiary includes occupants and an indoor place that is designated by an occupant. For example, a warm bathroom is required before taking the bath in winter. Then a new concept comes, i.e., Demand Space (DS), which is the space where a required service is designated by an occupant. The DS has some characteristics. First, it is the requirement of occupants. Second, the required Critical Service Manner is achieved in the DS by the Performers System. Third, space may be a part of a room or the whole room that depends on the occupants' will. In contrast, no matter the required Critical Service Manner is achieved or not, the complement space of the DS is the Undesired Space.

Part or all of the AoE of a home appliance of the Performers System that a required service is designated by an occupant is called the Useful Space (US). It is the intersection of the AoE and the DS. The complementary space of the US is Blind Space (BS). It is a DS, but the required Critical Service Manner is hard to be achieved due to the ability of the Performers System. For example, the indoor temperature in the BS cannot be adjusted to a prescribed level.

Figure 2.9 is used for better understanding these concepts and their relationships. The home appliance is part of the Performers System. The DS is the place where an indoor activity is performing. Otherwise, it is the undesired space. The US is the space where the demand is designated, and the Performers System can adjust to the desired level. The DS is where the Performers System cannot adjust

is the BS. The Ineffective Spaces are adjacent to the AoE. So, the designated Critical Service Manner can be achieved in the US. The situation is not desired when the DS does not in conjunction with the AoE. If the AoE and the DS are partially in conjunction with each other (the conjunction part is the US), it is a degraded form. The perfect situations are that the AoE and the DS are conjugated, and the conjugated space is the superset of the US.

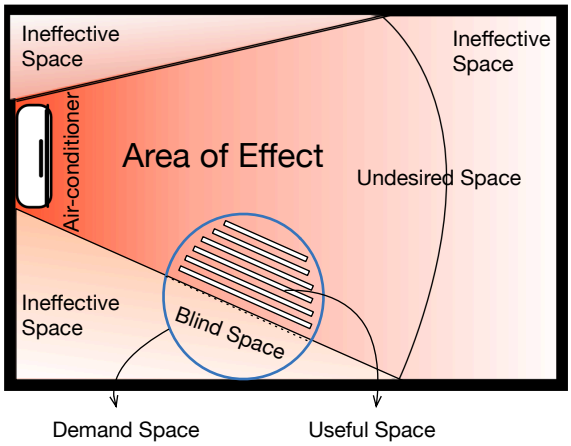


Figure 2.9: The relationships among the terms related to space.

Another situation is that when the AoE intersects with multiple DSs. The intersection space is the union of each DS intersects with the AoE. Assume that a set of AoE is

$$AoE = AoE_1, AoE_2, ..., AoE_n, n \in \mathbb{N},$$

and the set of DS is that $dS = dS_1, dS_2, ..., dS_m, m \in \mathbb{N}$. The intersection spaces becomes $(dS_1 \cap (AoE_1 \cup AoE_2 \cup ... \cup AoE_n)) \cup (dS_2 \cap (AoE_1 \cup AoE_2 \cup ... \cup AoE_n)) \cup ... \cup (dS_m \cap (AoE_1 \cup AoE_2 \cup ... \cup AoE_n))$. That is to say the US becomes the following fomula (Fomula 2.9).

$$US = \bigcup_{i=1}^{m} (dS_i \cap (\bigcup_{j=1}^{n} AoE_j)) \tag{2.9}$$

The spaces can be calculated. The space calculation is the way to compute or designate the size and location of a space. Based on the introduction of these definitions above, not all space needs to be calculated. Only the US is needed to be calculated. [133] used anchor points combine with distance specifiers to designate the size and location of the AoE. Any object can be placed somewhere indoor, which is taken as an anchor point. It can be a static or moving physical objects or even an abstract point in the space. However, the distance specifier was not given in [133].

The distance specifier can be designated by the capability of the Performers System to adjust the corresponding physical property. The Performers System can adjust a limited space with respect to its capability as introduced earlier in this section. Before introducing how to determine the distance

specifier, let us discuss the concept of the effect of home appliances (of the Performers System) at a given point in the space [133]. For a physical property *Phy* and a home appliance *HA* to adjust it. The effect E of *HA* at a given point p in the space is $E_{HA,Phy}(p)$. Assume the capability of *HA* to adjust *Phy* is $[low, up]$, the distance specifier can be determined by using the algorithm described in Algorithm 1.

Algorithm 1: The determination of the distance specifier.

Input: points in the space and $p \in Space$
Output: the value of distance specifier and denoted by *dSpecifier*

```
1  d = 0
   /* the maximum distance between a point in the space and the HA
      that is initialized by 0                                    */
2  L_low = 0
   /* the distance between a point in the space and the HA when it
      works in its low capability                                 */
3  pause(t)
   /* wait until the physical property is adjust to the desired
      level                                                       */
4  while p do
5  |  E_{HA,Phy}(p) = low
6  |  d = distance(p, HA)
7  |  if d > L_low then
8  |  |  L_low = d
9  |  end
10 end
11 L_up = 0
   /* the distance between a point in the space and the HA when it
      works in its best capability                                */
12 pause(t)
13 while p do
14 |  E_{HA,Phy}(p) = up
15 |  d = distance(p, HA)
16 |  if d > L_up then
17 |  |  L_up = d
18 |  end
19 end
20 dSpecifier = (L_low + L_up)/2
```

The calculation of the AoE can be applied to a single home appliance or multiple home appliances

of the Performers System. In the case of a single home appliance, it can either directly adjust a physical process or indirectly take advantage of the natural system for the adjustment. In the case of multiple home appliances, [133] described AoE as the effect of a service, which it defines service is an executable file designated to control multiple home appliances to adjust a specific physical property. It is the union of all the AoEes of the considered home appliances to adjust the same physical property, e.g., indoor temperature.

Next is to determine how to calculate the DS. The DS is defined based on the occupants' will. The anchor point of it can be determined by either the location of a beneficiary, i.e., the location of an occupant in the room, or manually specify a point in the space. There are two cases of the distance specifier of the demand space. For an occupant, it is the occupant centered, enough for a static activity. E.g., 1m around a sedentary occupant. For a designated space, it can be manually specified for an activity area. E.g., in winter, it requires a warm bathroom before taking a bath.

Figure 2.10 is used to illustrate the concepts of the anchor point and the distance specifier both in the cases of an occupant as an anchor point and a designated point as an anchor point.

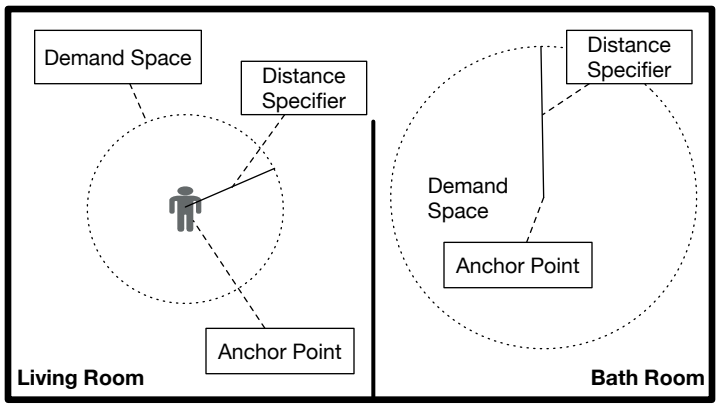


Figure 2.10: Terms related to anchor point and distance specifier.

Assume the Performers System includes a set of home appliances $HA_1, HA_2, ..., HA_n$ that adjusts the same physical process *Phy*, e.g., indoor temperature variation. The AoEes of these home appliances are denoted by $AoE_1, AoE_2, ..., AoE_n$. The DS is represented by *DS*. Then the US can be calculated by Formula 2.10. The shape of the US may be an irregular space.

$$US = DM \cap (\bigcup_{i=1}^{n} AoE_i) \tag{2.10}$$

It may become meaningless in the case of a degraded form of the intersection, i.e., an occupant is out of the US. This may be due to the distance specifier of the demand space is too long. And this meaningless case should be avoided.

The US is not a fixed space. Rather, it dynamically changes due to the dynamic of the AoE or the DS or both. The dynamic of the AoE is due to like a portable home appliance moves from one location

to another, or the anchor point moves. But the distance specifier may not be changed. The dynamic of the DS may be because of a movable beneficiary especially an occupant that means the anchor point can move. Also, distance specifier does not change. In the case of both the home appliance and the occupant move, the US must be recalculated when these conditions changed. The relationship of the terms can be found in Appendix B.1.

2.3.3 Accident Formation

Accidents can be understood as the resilience [223] of the Performers System, i.e., to adjust 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. The 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, the physical process anomalies should be detected as early as possible to trigger precautionary measures. The information about hazards is also important for triggering reaction measures. All in all, the accident formation that is shown in Figure 2.11 focuses on the physical process anomalies resulted from abnormal Behaviors.

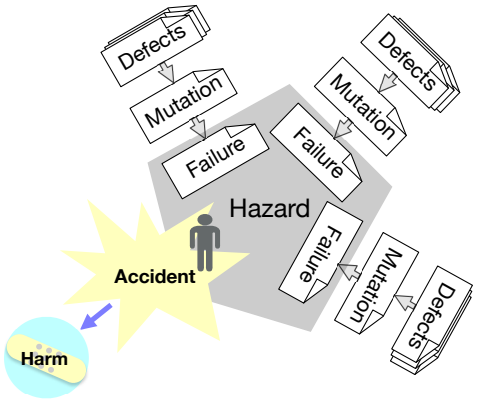


Figure 2.11: The accident causality model.

Next, let us discuss the terms and related rationales of the accident causality model in Figure 2.11.

Definition 7 (Defect)**.** *Direct causes that reside in the* Performers System *to give rise to a* Mutation.

A Mutation (Definition 8) relates to abnormal Behaviors of the Performers System. The 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 are that when Mutations resulted in Service Failures (Definition 9), and UCAs are that when Service Failures evolved into Hazards (Definition 10). For example, an ICA can be mistakenly set the heat mode of an air-conditioner in hot summer, which will cause thermal discomfort. To differentiate from causes that introduced in the STAMP model, Defects refer to more superficial reasons. This is due to that the home environment is an application area, the deeper causes for system development defects are not considered here. When physical process anomalies are detected, it is expected to react to that immediately concerning Defects. Therefore, the Defects are the direct causes and should be controllable, e.g., through reconfiguration.

As discussed in Section 2.1, 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. For reacting 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, let us apply the hazard analysis technique STPA [122, 125] in Chapter 3.

Definition 8 (Mutation)**.** *Abnormally* Behavior*s that cannot be taken as* Service*s.*

Abnormal changes in physical processes are the representation of abnormal Behaviors. So, the constraint of the Behavior is the prescription of variations in physical processes that satisfy the comfort purpose. Thus, the Mutation is the change of physical processes under adjustment unacceptably deviated from the prescribed curve(s), which results in uncomfortableness. For example, the amplitude of temperature fluctuation cannot greater than a threshold value for thermal comfort [230]. The Mutation in such circumstances is the undesired amplitude of temperature fluctuation.

The Mutation is a state of physical processes, which between the state that brings about comfort and the state that results in a hazard. This concept is important due to not only the understanding of accident formation but also the information that 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*s of* Performers System ***failed*** *to fulfill occupants' comfort requirement.*

The concept Mutation 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 perceived the uncomfortableness the Mutation brought about.

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 [18, 19], by which smart home systems can conclude whether the home environment satisfies the comfort requirement with occupants on the scene.

Definition 10 (Hazard)**.** *A state of indoor environment which will cause harm of 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 evolved into a hazard due to the indoor temperature reached a level, which if occupants on the scene will cause heatstroke.

Take thermal related hazards for example, the evaluation of a hazard depends on cold stress indices [37] and heat stress indices [1]. They are proved techniques to evaluate different thermal sensations to hot and cold conditions. Heat stress [37] is defined as the net heat load to which a person is exposed to the combined contributions of environmental ingredients, metabolic heat, and clothing that cause an increase in body heat storage. Cold stress [1] 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 and sometimes heat debt. Similarly, the PMV-PPD index also has an intricate relation with environmental and personal ingredients, which can be measured in practice.

Definition 11 (Accident)**.** *An unintentional event which a* Hazard *resulted in the 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 occupants. The latter can be measured by taking advantage of wearable devices.

Definition 12 (Harm)**.** *Damage to the health of occupants, physical injury, or even death.*

It is the consequence of the Accident. It varies with respect to Hazards and health conditions of occupants. For example, it can result in heat illnesses or death to old people due to heat exposure [219]; it can also affect sleep and circadian rhythm that result in cardiac autonomic response during sleep as a result of cold exposure [156].

In summary, Figure 2.12 illustrates the relationships among the terms introduced in this chapter. the reasons why an accident model is required was discussed first. Then, to propose the accident model, I proposed the concept of the Performers System. The discussion of the accident model is ground on the Performers System. During the introduction, various terms have been defined and explained. Based on the accident model, the causation of how system Behaviors affect physical process anomalies can be comprehensively understood. Furthermore, the accident model connects the physical world and the cyber world.

2.4 Experiment

This section describes the experiment that validates the proposed accident model by acquiring real data of temperature from an experimental smart house. The testbed smart house that is located at the Nomi city of Ishikawa prefecture, Japan is for smart home services. It is named by iHouse. Temperature data were acquired from the western style room 1 of the iHouse.

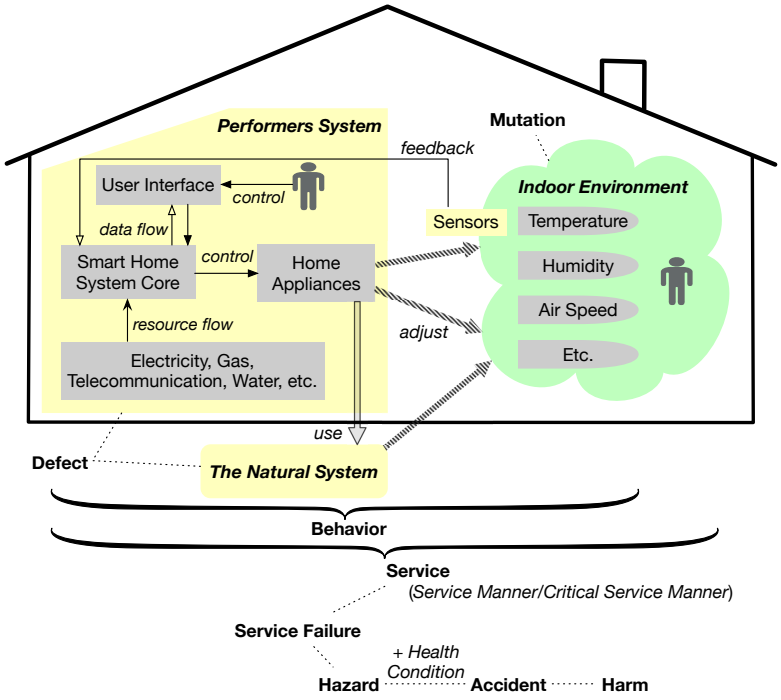


Figure 2.12: Terms related to service delivery and the risk model.

The Performers System includes an air-conditioner, a curtain, and a controller, which controlled remotely from our lab. The scenario is as follows to acquire real data. The weather was sunny and the indoor temperature was high (between $27°C$ and $28°C$). I used the cool mode of the air-conditioner to cool the room from 12:08. Then the indoor temperature dropped. Next, the curtain was opened from 12:46. Unfortunately, after opening the curtain the indoor temperature increased due to more radiant heat was introduced.

The real data acquired from iHouse is shown in Figure 2.13. In the beginning, the air-conditioner (AC) was turned on. The Behavior of AC is to cool down the indoor temperature. The Service is thus to cool down indoor temperature that satisfies thermal comfort. Under the sunny hot weather to use the cool mode of the AC to cool down the indoor temperature to satisfy thermal comfort is the Service Manner. As it is required at that time, it is also the Critical Service Manner. Since the curtain was opened, the temperature increased again. From this, the open curtain can be identified as the Defect. Since 12:46 indoor temperature unexpectedly increased and this process can be taken as the Mutation. If to somebody, temperature over $24°C$ would cause heat stroke to them, a hazardous situation has been caused by this circumstance. If this type of person happens in the room and caused heatstroke, that is an Accident that has happened. The consequence is a health problem for this type of people and thus harm occurred. In the real data shown in Figure 2.13, the curve finally dropped. This is because the outside climate changed that less radiant heat was introduced to the room. Also,

the cool mode of the AC affects the room.

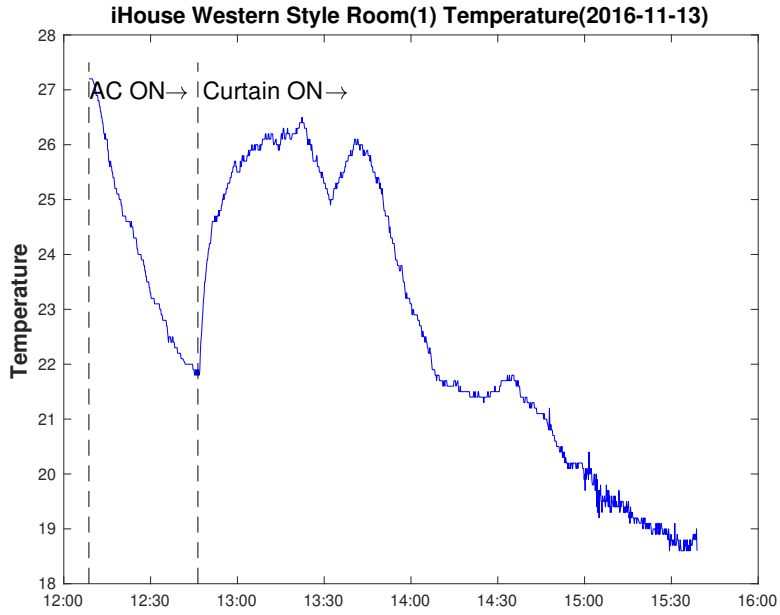


Figure 2.13: Temperature data that gathered from iHouse.

2.5 Discussion

As one of our everyday living experiences, physical processes could be in hazardous states that cause harm to occupants [156, 219]. The occurrence of hazardous states can be transferred from a normal state of 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 deviated from expectations, the above transformation will occur. Thus, this living experience and the results from the experiment in Section 2.4 validate the proposed STAMP-PP model.

For validating the terms defined in the STAMP-PP model, let us consider the eight abnormal indoor temperature situations that were discussed in our previous work [230]. 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. Based on the information of Service Failure combines with ICAs under related operation scenarios, one can predict

whether Hazards would happen before providing precautionary measures. Because Service Failures and 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 sensors. For example, it can be known whether the temperature is increasing to approach 25 $^{\circ}C$ through temperature sensors. Then precautionary measures can be selected under the direction of reliability requirements. If unfortunately, a Hazard is detected, reaction measures have to be selected based on the operation scenarios and the Hazard, which are guided by safety requirements.

The purpose of precautionary measures is to retain Service delivery. It is achieved by reconfiguration of the Performers System. The reconfiguration includes two forms. One is to reset the working Performer(s). Another is to reconfigure standby Performers. The purpose of reactions is to retain a safe home environment state, which could be a Service Failure (that need further interference) or the process of normal Service delivery. It is also achieved by reconfiguring the Performers System, which has the same contents as introduced for precautionary measures. The reactions should have other content that precautionary measures do not have, i.e., a warning system. The warning system is activated 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 safe. If the reconfiguration in the reaction stage cannot restore to a safe situation, the warning mechanism will inform an emergency, e.g., a hospital, through networks.

Accident models can be roughly classified into three categories [125, 212], i.e., sequential models, epidemiological models, and systemic models. The 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 analogous to the spreading of 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 grounded on general system theory, and so does the STAMP-PP model. It describes the 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 relationship 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.

2.6 Related Work

The systems approach is considered as the dominant paradigm in safety research [174]. It views accidents as unexpected interactions among system components, i.e., technical, social, and human elements. Among various systemic models, there are three most cited models [211], that is, STAMP [125], Functional Resonance Analysis Method (FRAM) [85], and Accimap [170, 195].

STAMP has been briefly discussed in Section 2.3.1. According to [211], over half of the reviewed papers were about the STAMP related, which indicates a pervasive acknowledgment of its underlying rationale. The application of it has attracted researchers from a broad field. [17] adopted it to investigate aircraft rapid decompression events. [138] applied it for the analysis of deepwater well con-

trol safety. In the field of railway, [157] investigated a railway accident, and an accident spreading by taking the China Jiaoji railway accident as an example. It has also been applied to the field related to poisonous or dangerous substances. [75] adopted it in analyzing the China Donghuang oil transportation pipeline leakage and explosion accident. [48] applied it to Fukushima Daiichi nuclear disaster and to promote the 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 a risk assessment tool [211]. The FRAM model graphically describes systems as interrelated subsystems and functions that will exhibit varying degrees of performance variation. The accident results from that emergent variation produced from the performance variability of any system component to "resonate" with that the rest 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 [35]. The FRAM also has applications in different fields, e.g., [31] applied it to the railway traffic supervision to investigate interdisciplinary safety analysis of complex socio-technological systems. [205] extended the FRAM by including a framework with steps to support hazard analysis. Some efforts have been tried to quantify it, e.g., [161] developed a semi-quantitative FRAM based on Monte Carlo Simulation.

The Accimap method is a graphical representation of a particular accident scenario that relates to system-wide failures, decisions and actions [85, 170]. Accimap is a generic approach and does not use taxonomies (that is different from that of the STPA [122, 125]) of failures across the different levels of considered [175]. The Accimap produces less reliable accident analysis results by comparing it with the STAMP [66].

The selection of accident analysis techniques depends on the system characteristics, i.e., manageability and coupling [212]. The systemic approaches are usually adopted by systems with low manageability and tight coupling. Systemic approaches relate to complex socio-technical systems have their strengths. For one such system, it is better to adopt multiple approaches for supplementary to each other, even though the STAMP is considered much more effective and reliable in understanding accidents and hazard analysis [66, 175, 211].

2.7 Conclusion

I extended the accident model STAMP by considering physical processes in the home environment. Due to the home environment is adjusted by behaviors of the smart home system, I first proposed the notion of the Performers System that emphasizes the behaviors that are performed by various home appliances. Then based on the Behavior of the Performers System, the accident formation concerning physical processes from the normal state to some intermediate states that result in uncomfortableness, and finally to states that cause harm. The accident model is validated by experimental results and empirical experience.

3

Operational Safety of Smart Home Systems

An accident model, i.e., STAMP-PP has been proposed in Chapter 2, which provides a conceptual representation of how abnormal system behaviors result in physical process anomalies. In this chapter, let us discuss how to identify the causes, i.e., Defects that resides in the Performers System. To this end, two hazard analysis techniques are employed. One is called System-Theoretic Process Analysis (STPA) that will be tailored and applied to a smart home system that is for indoor temperature adjustment. Another one is an innominate approach proposed in the literature, which is based on the goal-based requirement engineering, guide words, and item sketch. Finally, a comparison of these two approaches is going to be made.

I summarized the contributions of this chapter [231]:

- A procedure to identify system level hazards is proposed.
- I applied the innominate approach for safety problem analysis.
- I proposed a tailored STPA approach for hazard analysis.
- A Landscape Genealogical Layout Documentation (LGLD) is proposed for documenting the analytical results of the tailored STPA.
- A comparison of the above two approaches.

3.1 Introduction

Besides the information related to physical processes is important, the abnormal behaviors of systems under specific operation scenarios are also necessary to be known for selecting appropriate reactions and precautionary measures. To this end, hazard analysis techniques [60, 122] that can assist in analyzing potential causes of accidents are required. I adopt hazard analysis techniques to identify the

causes of abnormal system behaviors under related operation scenarios. Abnormal system behaviors can result in abnormal changes in physical processes. A pervasive approach to hazard analysis named System-Theoretic Process Analysis (STPA) [122, 125] that based on the STAMP model is tailored and applied to the smart home system [227] that for is adjusting the indoor temperature, to demonstrate the way 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 also the reasons why unsafe control actions can happen under specific scenarios. Since 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 of these abnormal behaviors. A Landscape Genealogical Layout Documentation (that is denoted as LGLD) is proposed for documenting the analytical results, in which the relations among the results are clearly and straightforwardly represented by comparing with conventional ways of documentation, i.e., tables and lists. I compared the results with that of applying the original STPA, which demonstrates the effectiveness of the tailored STPA in identifying causes of abnormal system behaviors and the LGLD documentation in representing the relations among the results.

For comparison, I also adopt an innominate approach [94] that based on goal-based requirement engineering, guide words, and item sketch. First, let us explore the feasibility to adopt it for identifying the causes of abnormal system behaviors. Second, it is to learn more knowledge in requirement engineering due to system safety techniques that may have a connection with it.

3.2 System Safety

System safety is part of system engineering that supports risk management. It calls for a risk management strategy based on the application of engineering and management principles, criteria and techniques to optimize safety through a system-based approach. The goal of system safety is to improve safety by identifying risks, then eliminating and controlling them by design and/or procedures based on system safety precedences. This is different from conventional safety tactics that rely on control of conditions and causes of an accident based on either epidemiological analysis or investigations of individual past accidents. System safety encompasses safety in system development and system operation [125], which this chapter focuses on the latter.

In this section, basic concepts relate to risk assessment and risk analysis will be introduced. These are mainly referenced from [2, 5, 6, 62, 153, 154, 155, 204].

3.2.1 Risk Assessment

Risk assessment is the systematic approach of finding and recognizing reasonably foreseeable hazards, hazardous situations, and/or events. This supports to understand risks, their causes, consequences, and the probabilities of occurrence. The purpose of risk assessment is to identify events or situations that affect to achieve the objectives of safety, to provide evidence-based information and analysis to make decisions on how to select options to those risks.

Risk assessment consists of five parts:

1. The scope
2. Hazard identification in risk analysis
3. Hazard analysis in risk analysis
4. Risk estimation in risk analysis
5. Risk evaluation

Step 1 prescribes the reason and scope of the assessment and other related issues about the assessment. The others include the research background, the context, risk criteria, and the subject of risk assessment. The context of the risk assessment includes the goal, the extent including depth and breadth of the risk assessment activities, methodologies of risk assessment, and ways of evaluating the performance/effectiveness. Risk criteria are defined as references to quantitatively or qualitatively evaluate the significance of risk, e.g., unacceptable, tolerable, or broadly acceptable. The subjects are the body of the risk assessment. It is necessary to make it clear what subjects should be included in the assessment, for example, a process, an activity, or a service.

The aim of step 2 is to identify a set of accidents and related hazards. Comprehensive identification using a well-structured systematic process is important. This is due to a hazard will not be further analyzed if it was not identified at this stage. Unidentified hazards may have potential dangers. There are questions may need to be answered, i.e., what can happen, where and when, and why and how it can happen.

Step 3 provides the process of investigating contributing factors to the identified hazards and accidents. Hazard analysis involves the identification of causes of hazard, the consequences, and the likelihood of that consequences. It is also necessary to identify factors that affect consequences and likelihood.

Step 4 systematically uses available information from hazard analysis to estimate risk by evaluating the level of risk concerning the severity, range, and likelihood of the consequences. The way to represent consequences and likelihood can determine the level of risk. If sufficiently accurate, suitable and complete data is available, a quantitative methodology may be adopted, otherwise, a qualitative methodology is used.

The risk evaluation in step 5 systematically determines whether a risk is broadly acceptable, tolerable, or unacceptable based on tolerability criteria and if it is necessary to reduce the risk. Risk evaluation encompasses comparing estimated levels of risk with risk criteria when the context was established to determine the significance of the level and type. Finally, it can be determined if the risk reduction or treatment is required or not. The purpose of this step is to make decisions about if treatment and treatment priorities are needed to risks based on the outcomes of risk analysis.

3.3 System Level Hazard Identification

In this section, a procedure for identifying the system-level hazard is proposed. The first step in safety engineering usually is to determine the interested accident. It is up to various many reasons. As [122]

pointed:

> The determination of what is to be considered as a loss or accident in a particular system has to be made by those assigned such responsibility because it involves the allocation of resources and effort, and these things are never unlimited. For some types of extremely dangerous systems, such as nuclear weapons, the government usually makes this determination. In some industries where safety is critical to the survival of the industry, such as commercial aviation, often the decision is made by national or international associations. Alternatively, the decision may simply be local to a particular company, it may be a requirement imposed by insurance companies, or it may result from liability concerns.

After the accident is determined, the next step is to derive appropriate and holistic system-level hazards that can further be analyzed to identify the corresponding causes. Unfortunately, there seem no tools for identifying system-level hazards [125]. As quoted above, it depends on domain expertise and subjective evaluation. A set of hazards should be avoided by system stakeholders. Some government agencies have mandated the hazards for the systems they regulated or certified. For most systems, the hazards to be considered are up to the developers and their customers. This section proposes a procedure that as guidance for system-level hazard identification regarding domain expertise.

The accident is defined in the STAMP model [125] as an unexpected or hit-or-miss event that results in a loss, including death or injury, property damage, environmental pollution, mission loss, etc. The event is the occurrence or change of a particular set of circumstances [79]. Hazard is a combination of system state or set of conditions with a particular set of worst-case environmental conditions, which will cause an accident. So, an accident is an unexpected or planless occurrence or change of a particular set of circumstances that result in a loss. The undesired or unplanned occurrence or change of a particular set of circumstances is due to a hazard. Because system-level hazards are derived from the accident, the procedure is thus proposed as follows.

There are five steps of the proposed procedure, as shown in Figure 3.1. In step 4, if there exist unidentified undesired, unplanned occurrence, change, or the identified system-level hazards seem not to comprehend and holistic, it will go to step 0 to go through the procedure again for the identification.

To demonstrate this procedure, two examples are used that referenced from [122] as shown in Table 3.1. The n/a denotes the corresponding condition is irrelevant in contributing to the occurrence or change. One is the chemical plant. Another is the train door controller. In step 0, it is required to identify the undesired or unplanned occurrence or change. Based on the given accident to identify what has occurred or changed by comparing with the situation where the accident has not occurred. The occurrence or change should relate to the system or the relationship between the system and its environment (or other systems).

The purpose of step 1 is to find out the relative factors to the occurrence or change identified in step 0. They should be at the system level, not related to the component of the system. The results of this step can provide informative and comprehensive knowledge for system-level hazard identification in the next step. The factors include possible system states and conditions when the occurrence or change is happening. The system states are that may prior to the occurrence or change. The conditions encompass the following two types:

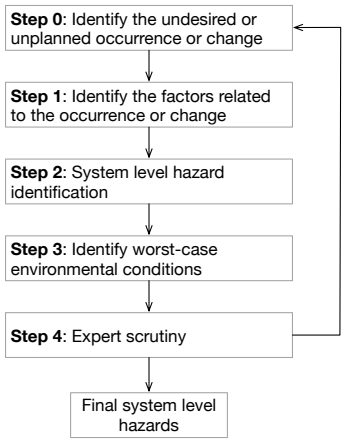


Figure 3.1: A procedure for identifying high level hazards.

A. The relationship between the system and other system(s) or its working environment;

B. The adverse environmental factors the system is supposed to control.

Step 2 is to identify system-level hazard identification. A hazard should be controllable and within the system boundaries [122] by considering the results from step 1. For example, a hazard for an airplane is not bad weather because the designer of the airplane or the air traffic control system cannot control the weather. On the contrary, the hazard could be the airplane being in an area of bad weather. This definition gives potential ways to avert the hazard when designing the system. Synthesize the results from conditions A and B of step 1 to generate hazards. Then rephrase the statement of the hazard by eliminating the state(s) information if only the condition A or B appears the hazard still holds. Multiple hazards can be identified when the identified conditions belong to a different context.

Then, it is required to identify worst-case environmental conditions in step 3 to verify the identified hazard(s) in step 2 are hazard(s). This is due to a set of worst-case conditions in the environment that will cause losses [122, 125]. For example, the pilots of two airplanes may see each other when they violate the minimum distance and avoid a collision. However, there exist worst-case conditions so that the accident may not be avoided, for example, low visibility.

The last step is expert scrutiny that examines whether the identified hazards would cause the identified accident under the worst-case environmental conditions. Also, it is necessary to check whether the identified hazards within the system boundary over which can be controlled. Moreover, to check whether hazards are holistically identified. Other questions may be added if they are relevant and necessary. If there exits conditions that need to be considered or other hazards are thought to be missing, then go to step 0 to check again, else to generate the final system-level hazards.

To validate the proposed procedure, three example cases are employed to apply the procedure for identifying system-level hazards. The first is the Yong-Tain-Wen railway train rear-end accident that happened in China [193]. The detailed description of the accident can be found in [193]. The accident is used by applying the procedure to elicit system-level hazards.

Table 3.1: Examples of applying the procedure.

System	Accident	Step 0		Step 1			Step 2	Step 3
		If No Accident	Occurrence or Change	System State	Conditions A	Conditions B		
Chemical Plant	People die or are injured due to exposure to chemicals	People are not exposed to chemicals	Chemical density or its appearance	At work; shutdown; unknown	n/a	Chemicals in air; chemicals in ground	Chemicals in air or ground after release from the plant	People in the vicinity
Train Door Controller	Passenger falls out of train	Passengers are not fall out of train through the doorway	Door status	Open; close	Train starts; train is moving; someone in the door way	n/a	Door is open when train starts; door is opened when train is moving; door closing on someone in the doorway	Passengers near the doorway

The accident happened when the fast-moving train D301 rear-ends the D3115 with a speed of 99 *km/h*. Thus, the accident is described as *The D301 crashed into the D3115 at the same section of TC-5829*. After applying the proposed procedure, the results were derived and shown in Table 3.2. From [193], the hazard was identified as *Two trains on the same section of track traveling at different speeds*. Therefore, it can be concluded that the identified hazard by using the procedure is equivalent to the hazard in [193].

Table 3.2: Apply the procedure to the example of the train accident.

System	Accident	Step 0		Step 1			Step 2	Step 3
		If No Accident	Occurrence or Change	System State	Conditions A	Conditions B		
D301	The D301 crashed into the D3115 at the same section of TC-5829	D301 and D3115 maintain a certain distance in the same section	The distance between the D301 and D3115	Running at the speed of 99 km/h	The D301 is running in the same section with D3115; The D301 is running faster than the D3115 behind it	n/a	The D301 were running faster than the D3115 in the same section	The driver of D301 did not see the D3115 in front of it

The second example is the cruise control of a vehicle [87]. An Adaptive Cruise Control (ACC) is a driver assistance system that can help to improve driving safety. It senses the presence of a leader vehicle and adjusts the vehicle's speed to keep a safe distance with the leading vehicle. The accident identified in [87] is that *vehicle occupants are injured while ACC is engaged*. Then, the proposed procedure is applied to identify system-level hazards, which is shown in Table 3.3. Finally, two hazards are identified by using the proposed procedure. The first is that the ACC failed to maintain a safe distance that may cause a collision. It is equivalent to the one provided by [87] that the ACC did not maintain a safe distance from the object in the front and lead to the collision. The second is the ACC caused a sudden slow down of the vehicle, which may cause a rear-end collision. It is equivalent to the one provided by [87] that the ACC slows down the vehicle suddenly, and the vehicle is rear-ended.

Table 3.3: Apply the procedure to the example of the ACC.

System	Accident	Step 0		Step 1			Step 2	Step 3
		If No Accident	Occurrence or Change	System State	Conditions A	Conditions B		
ACC	Vehicle occupants are injured while ACC is engaged	Vehicle occupants are not injured while ACC is engaged	The distance between the vehicle and the one in front	The ACC failed to maintain a safe distance; The ACC caused a sudden slow down of the vehicle	The vehicle is equipped with the ACC	n/a	The ACC failed to maintain a safe distance that may cause a collision; The ACC caused a sudden slow down of the vehicle which may cause a rear-end collision	The driver did not have an in time interfere to apply the brake; A vehicle in back drives at a high speed

The final example is a Lane Keeping Assist (LKA) system that detects lane departure, i.e., deviate from the driving lane, and steers the car back into the lane when necessary (corrective action may

be taken by a driver) [132]. The accident is given as *a collision is occurred when the LKA system is engaged*. Table 3.4 shows the identification results by using the proposed procedure. A comparison with the hazards provided in [132] is shown in the Table 3.5. An inconsistency has appeared between *H2* and *h4*. By using the procedure, *h4* has not been identified, and one more hazard *H2* was identified. The reason for this can be that the author is not an expert of the LKA system. He only identified by using the procedure based on his experience. Therefore, there may be a discrepancy between expert examination.

Table 3.4: Apply the procedure to the example of LKA system.

System	Accident	Step 0		Step 1			Step 2	Step 3
		If No Accident	Occurrence or Change	System State	Conditions A	B		
LKA	A collision is occurred when LKA system is engaged	A collision is occurred when LKA system is not engaged	The distance between the vehicle and an object (that can be another vehicle or immobile items)	LKA enabled	Lack of warning information; wrong warning information; failed to steer vehicle back into lane; corrective action is provided when no need to do so	n/a	Lack of warning information; wrong warning information; failed to steer vehicle back into lane; corrective action is provided when no need to do so	Driver did not see the warning signal; driver did not provide corrective action

Table 3.5: A comparison the results hazards with the provided ones.

Identified Hazards	Hazards [132]
H1: lack of warning information	h1: absence of warning when vehicle moves out of lane
H2: wrong warning information	h2: no corrective action provided by the system when the car moves out of lane
H3: failed to steer vehicle back into lane	h3: corrective action provided when it isn't required
H4: corrective action is provided when no need to do so	*h4*: corrective action (torque to the steering) provided in the wrong direction

For a given accident, the proposed procedure guides in identifying system-level hazard(s). The statement of the interested accident should strictly follow the definition of an accident. If an accident is defined as a consequence like serious injury or fatality to personnel, it will be very difficult to know what has happened. The identification process requires domain expertise, especially in step 1 of the procedure. In case 3, inconsistency occurred due to a lack of expertise. The more concrete the context in which the accident occurs, the easier the hazard(s) can be identified.

Application

This section introduces the application of the procedure to identify system-level hazards relate to indoor temperature adjustment by the Performers System. As discussed in Section 1.1.2, weather anomalies affect indoor environment. So let us consider the example of the high-temperature results in heat stroke [74, 120]. Heatstroke is defined as a severe elevation in body temperature (a core body temperature of $40^{\circ}C$ or higher) accompany with the occurrence of central nervous system dysfunction under the condition of environmental heat exposure or vigorous physical exertion. It can be classified into nonexertional (classic) heatstroke and exertional heatstroke. The former occurs to very young or older people, or those with chronic illness when the environmental temperature is high. The latter happens to young fit people that involve prolonged excessive activities like sports. This section focuses on the former case.

Heatstroke can be assessed by heat stress indices, among which the most widely accepted and used one is the wet bulb globe temperature (WBGT) [39]. The Ministry of the Environment of Japan* has recommended criteria for thermal conditions based on the WBGT, as shown in Table 3.6.

Table 3.6: Recommended criteria for thermal conditions.

WBGT ($^{\circ}C$)	**Threat Level**
$\sim$21	Almost Safe
21 $\sim$25	Caution
25 $\sim$28	Warning
28 $\sim$31	Severe Warning
31 $\sim$	Danger

The accident is defined as *physical harm of occupants due to heatstroke when the Performers System is engaged*. According to the results shown in Table 3.7 after applying the procedure, the system level hazard became that the room WBGT temperature is over 28$^{\circ}C$.

Table 3.7: Applying the procedure to identify hazards related to heat stroke.

System	**Accident**	**Step 0**		**Step 1**			**Step 2**	**Step 3**
		If No Accident	**Occurrence or Change**	**System State**	**Conditions** **A**	**B**		
Performers System	Physical harm of occupants due to heat stroke when the Performers System engaged	Heat stroke of occupants due to heat exposure is not occurred when the Performers System engaged	Room heat accumulation	turn off; heating; fan; dehumidification	n/a	Heatwave; hot weather	Room WBGT temperature is over 30oC	Very young children or old people with chronic illness in the room

3.4 Safety Problem Analysis

This section will introduce the innominate approach [94] to identify low-level hazards based on a goal-based approach [217], item sketch, and guide words [50]. And an approach called STPA [125] for hazard analysis is tailored applied to the Performers System. The latter is based on a basic system theory to understand accidents. The aim to apply them is to identify Defects that cause abnormal system behaviors. Finally, a comparison is made from the viewpoint of hazard identification.

3.4.1 Hazard Identification by Using the Innominate Approach

Four steps are used for hazard identification [94]. The first is to build item sketches, which is to clarify the structure of a system, behavior, and the boundary of an item. Then, build a goal model of items, meanwhile, detail item sketches. Third, apply the guide words [50] to each goal description statements to generate the possibilities. Finally, let us identify hazards by using the item sketches.

*Ministry of the Environment, Japan: http://www.wbgt.env.go.jp/en/

Goal-oriented Requirements Engineering

The goal-based approach in the requirements engineering field is used to elicit requirements of various kinds, e.g., system requirements. This section will introduce the basics of the goal-oriented approach. A goal prescribes the intent of a system, which is satisfied by the collaboration of its agents. An agent is an active system component playing a specific role in goal satisfaction. There are many kinds of agents, e.g., human agents, devices such as sensors and actuators, existing software components, and new software components.

The goals have granularities. At a higher level, coarser-grained goals stating strategic objectives. At a lower level, finer-grained goals stating technical objectives. The coarser-grained goals can be refined into finer-grained goals. The finer-grained goals are the abstracts towards the coarser-grained goals. Goals are classified along two dimensions. A goal of one type when it prescribes intended system behaviors or preferences among alternative behaviors. A goal belongs to one category when it prescribes a functionality or a quality constraint. There are two types of goals, i.e., behavioral goal and soft goal.

Behavioral goals implicitly define a maximal set of admissible system behaviors. The system behaviors related to the state variables and a sequence of state transitions of items. A behavior goal can be defined in a clear-cut sense. Achieve goals prescribe expected behaviors, where a target condition must sooner or later hold whenever some other condition holds in the current system state. The specification has the following informal temporal pattern:

> Achieve[TargetCondition]: [If CurrentCondition Then] sooner-or-later TargetCondition

For example, *Achieve*[BookRequestSatisfied]: if a book is requested then sooner-or-later a copy of the book is borrowed by the requesting patron.

Maintain goals prescribe intended behaviors when a good condition must always hold. Its specification takes the following informal temporal pattern:

> Maintain[GoodCondition]: [if CurrentCondition Then] always GoodCondition, in particular: always (if someCondition then Good Condition)

For example, *Maintain*[DoorsClosedWhileMoving]: always (if a train is moving then its doors are closed).

Soft goals prescribe preferences among alternative system behaviors. It cannot be provided in a clear-cut sense. Prefix a soft goal name by a keyword indicating a corresponding pattern. For example, *Improve*[TargetCondition]; *Increase*[TargetQuantity]; *Reduce*[TargetQuantity]; *Maximize* [ObjectiveFunction]; *Minimize*[ObjectiveFunction].

Goals are categorized into function goals and non-functional goals. A functional goal states the intent underpinning a system service, e.g., satisfaction, information, and stimulus-response. A non-functional goal states a quality or constraint on service provision or development, e.g., quality of service, compliance, architecture, and development.

A goal model shows how the system's functional and non-functional goals contribute to each other through refinement links down to software requirements and environment assumptions. Each goal

in a goal model annotated by a number of features to characterize the goal individually. A goal has two mandatory features, i.e., name and specification. The name uniquely identifies the goal throughout all views of the entire system model. The specification precisely defines, in natural language, what the goal prescribes in terms of phenomena that are monitorable and controllable in the system. There are other optional features like type, category, source, and priority.

Each goal in a goal model is graphically represented by a parallelogram. An example of this graphical representation is shown in Figure 3.2. The goal is represented in a parallelogram that attached with an annotation that provides feature information of the goal.

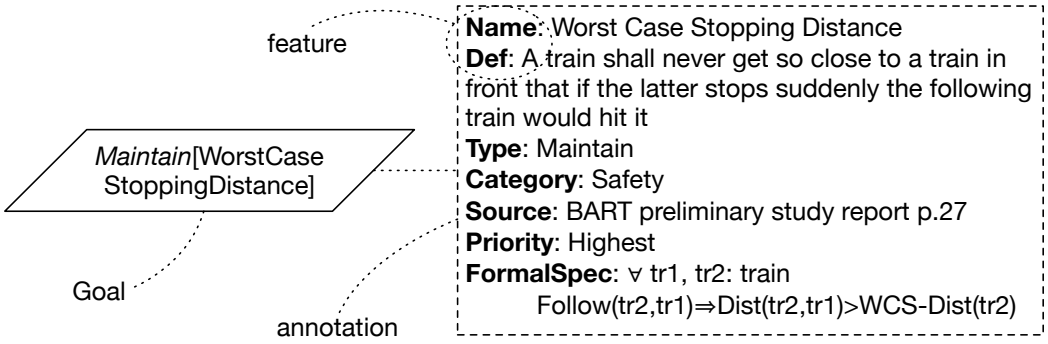


Figure 3.2: An example of the graphical representation of a goal.

There are two types of goal refinements, i.e., AND-refinement and alternative refinement. ADN-refinement connects a goal with a set of sub-goals. The parent goal is satisfied by satisfying all sub-goals in the refinement. The refinement should be consistent, complete, and minimal. Leaf nodes in refinement trees are node that need not be refined further. The graphical representation of the AND-refinement is illustrated in Figure 3.3. The solid circle denotes arguably complete refinement, and the hollow circle may need further argument. The black frame parallelogram means leaf goals.

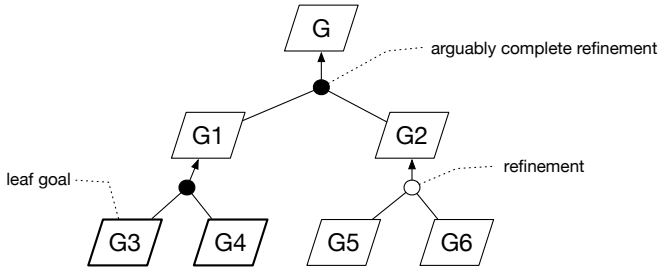


Figure 3.3: Graphical representation of AND refinement.

Alternative goal refinements focus on sets of sub-goals that each of them AND-refines the parent goal. The parent goal is achieved by achieving all sub-goals from any of the alternative refinements.

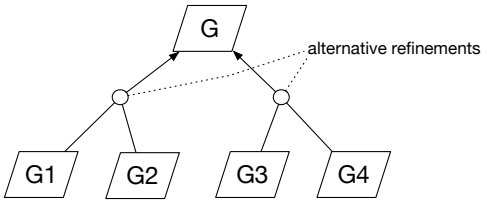


Figure 3.4: Graphical representation of alternative refinement.

Each alternative results in different system designs that will produce different versions of the system. Figure 3.4 presents a graphical representation of the alternative refinements.

The way to build goal models can either by heuristic rules or reusable patterns. For heuristic rules, several heuristics are available for eliciting individual goals to start with. For example, analyze the current objectives and problems, and search for goal-related keywords in elicitation material. There are some reusable patterns, e.g., the milestone-driven refinement pattern, case-driven refinement pattern that includes decomposition-by-case pattern and guard-introduction pattern, and the divide-and-conquer pattern.

Guide Words

Guide words are a part of the HAZOP (Hazard And Operability Study) [50]. The HAZOP is a highly disciplined procedure intend to identify how a process may depart from its design intent. Guide words are words or phrases which express and define a particular type of departure from the design intent of an element. An element is a component of a part to identify the essential features of the part. Examples of features like involved material, e.g., data, software, the activity being carried out, and employed equipment.

The role of guide words is to stimulate imaginative thinking and enable a comprehensive hazard identification. They can be classified into temporal and spatial and should be devised adequately corresponding to the system. An example of guide words can found in Table 3.8.

Then apply guide words to the goals to identify hazards. This process is to examine all possible deviations of goals, which is a prerequisite for hazard identification. Goals and guide words can be regarded as a matrix, as shown in Figure 3.5. Each cell represents a possible deviation of a goal.

Figure 3.5: The guide word/goal matrix.

Table 3.8: Example of guide words.

Guide Word	Meaning	Type
NO or NOT	Complete negation of the design intent	Spatial
MORE	Quantitative increase	
LESS	Quantitative decrease	
AS WELL AS	Qualitative modification/increase	
PART OF	Qualitative modification/decrease	
REVERSE	Logical opposite of the design intent	
OTHER THAN	Complete substitution	
EARLY	Relative to the clock time	Temporal
LATE	Relative to the clock time	
BEFORE	Relative to order or sequence	
AFTER	Relative to order or sequence	

There are two possible sequences to examine the cells of the matrix, i.e., column by column, e.g., element first, and row by row, e.g., guide word first.

Item Sketch

An item [58, 94] is an abstract representation of a system, which uses functional and non-functional requirements to define its boundaries. The item sketch is to clarify the structure, behavior, and the boundary of the item. The representation of item sketch can be a static representation or dynamic representation. The static representation is given by like UML class diagram, while the dynamic representation is given by a finite state machine. They show two facets of the same object.

Accompany with goal refinement, there two ways of combing item sketches, i.e., refinement and composition. For refinement, high-level goal uses AND-refinement to get multiple sub-goals, accompany this process to describe item sketches that are attached to each level of goals. In the goal refinement, their corresponding static representation of item sketches have the same basic structure. The composition combines goals that do not have a direct refinement relationship. It usually considers the meaning of combination to describe a more detailed scenario. Dynamic representations will be combined in this case.

The item sketches and the goal model have some relationships. Each goal in the goal model has its corresponding item sketches. The corresponding relationship between goal and item sketch is maintained by using the goal statement. The goal and its corresponding item sketches have the same level granularity. The goal model takes charge of the functional and nonfunctional requirements of items. Item sketches can be used to represent the achievement of the corresponding goal.

Hazard Identification

Hazard identification includes four parts. The basic idea is to operate on item sketches to interpret the goal description that applied guide words. Thinking about the change in descriptions or values of items to see what is going to happen. The goal of hazard identification is to produce a set of hazards, accidents, and their possible sources. In this case, the inputs to the hazard identification are item sketches and goal description statements that applied guide words.

Indoor temperature adjustment by the Performers System for thermal comfort without causing heat exposure or cold exposure. So, this section introduces hazard identification about indoor temperature adjustment by the Performers System that will cause heat exposure and result in health problems.

Heat transfer depicts thermal energy exchange between physical systems in regarding temperature and pressure [222]. It tries to reach a state of thermal equilibrium. Two mechanisms of heat transfer affect indoor temperature, i.e., convection and radiation. The convection means heat transfer from one place to another by fluid movements (liquids or gases). It is used to refer to the sum of the advective and diffusive transfer. Thermal radiation refers to electromagnetic radiation produced by the thermal motion of charged particles in matter. All matters with a temperature greater than absolute zero emit thermal radiation.

Indoor temperature is affected by multiple mechanisms of heat transfer while being dominated by one. For example, variations of indoor temperature through air exchange between outdoor and indoor. If there is a temperature difference between indoor and outdoor, the indoor temperature would be changed by diffusion and radiation. The indoor temperature would be changed by advection due to the bulk air movement.

Normally, in naturally ventilated spaces, it takes a long time for the outdoor climate to change the indoor temperature a lot, e.g., season changes. Some other physical processes take a shorter time for the indoor temperature to change a lot, for example, indoor heat sources and opening windows when indoor and outdoor temperature difference is big. So, when a physical process takes a long time to change the indoor temperature a lot, say days. In a short time during that long time, assume this physical process has a constant affection for indoor temperature.

Then to identify the items. An identified item should affect a physical process to change the indoor temperature in one or more mechanisms of heat transfer. The indoor space should be naturally be conditioned. It is primarily regulated by occupants through the opening and closing of the window. And indoor heat sources are not related to HVAC systems nor other electric devices. So items that affects indoor temperature are as follows:

1. Indoor items
    - windows
    - curtains
    - heat sources
2. Outdoor items

- sunlight
- exterior construction

3. occuapnts (can also be taken as heat sources)

Goals are elicited from heat transfer, e.g., maintain thermal radiation, and empirical, e.g., maintain air exchange through the window. Ways of top-down fashion, divide and conquer patter, and heuristic rules from [217] can be used to build the goal model.

Next is to build the goal model. The goal model is used to analyze how does an indoor temperature adjustment service can be supported by a bunch of sub-goals. Then assigning each leaf goal with a corresponding identified item that takes the responsibility to achieve the goal. The root goal is that the indoor temperature is adjusted by the Performers System for thermal comfort without causing heatstroke. But, thermal comfort is determined by not just the indoor temperature, others like metabolic rate, clothing insulation, etc. also affect it. However, the usual way to satisfy thermal comfort is to adjust the indoor temperature. If in a certain condition like a sedentary in the summer season, other factors are taken as the constant condition and to only focus on indoor temperature adjustment. So, the root goal is denoted as *maintain*[IndoorThermalComfort].

To satisfy the root goal, two situations should be taken into consideration under naturally conditioned indoor space, i.e., the indoor temperature is greater than the outdoor temperature and is smaller than the outdoor temperature. When the indoor and outdoor are thermally equilibrium, the time the root goal lasts in each scenario should be as long as occupants stay indoor.

As discussed that heat transfer includes radiation and convection that includes diffusion and advection. Radiation includes solar radiation and man-made radiation. Solar radiation refers to sunlight that affects the indoor temperature through a window with a curtain opening and the walls. The curtain is just a representative, others like similar functionality are also taken into account. Man-made radiation means indoor heat sources to keep warm, e.g., fireplace. The diffusion of heat takes place in exterior construction to affect indoor temperature. The requirement of this is that the temperature difference between interior and exterior construction exists. Once the above condition satisfied, it can happen all year round. Advection happens when the air carries heat from the outdoor to the indoor. Wind speed is not zero and there exists an air temperature difference between indoor and outdoor. The goal models are built and shown in Figures 3.6 and 3.7. The goal annotations in the goal models refer to Appendix C.

Verification of the Goal Model

The goal model is taken as a precondition and base for the following hazard identification. All scenarios considered in building the goal model are reasonable and comprehensive based on the physical processes of heat transfer. The building of the goal model should be correct. For one thing, the goal model is built strictly follows the goal refinement patterns introduced in [217]. For another, the formal approach is used to verify goal refinements. A set of goals $G_1, G_2, \ldots, G_n$ correctly refines a goal G in a domain theory *Dom*, if and only if:

Figure 3.6: The goal model when the indoor temperature is smaller than the outdoor temperature.

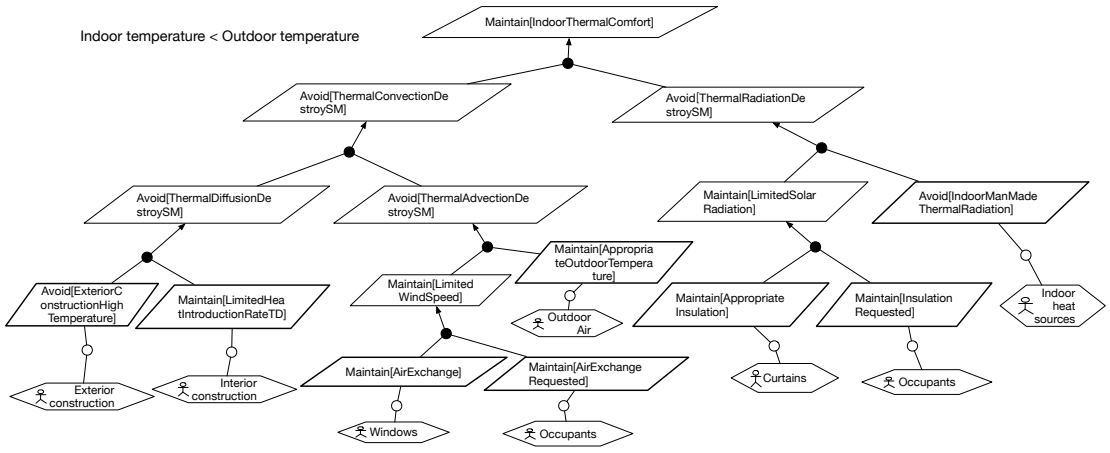
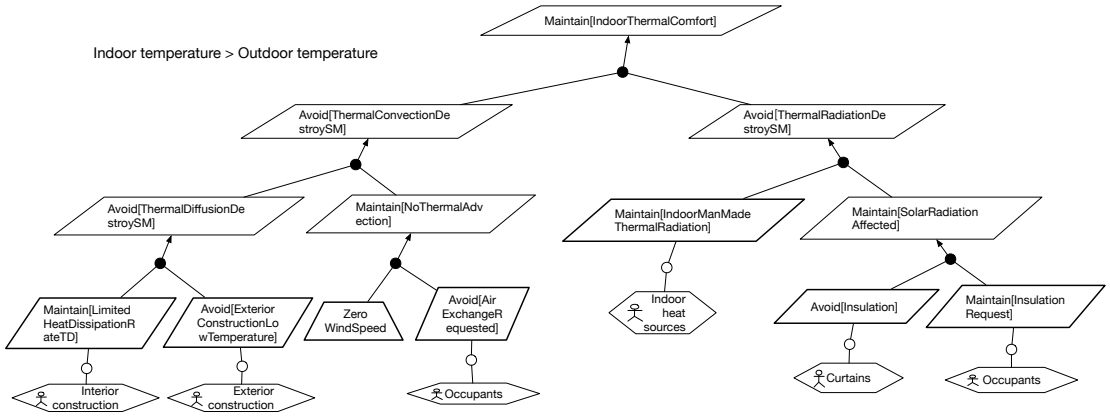


Figure 3.7: The goal model when the indoor temperature is greater than the outdoor temperature.



- $G_1, G_2, ..., G_n, Dom \models G$ completeness
- $G_1, G_2, ..., G_n, Dom \not\models false$ consistency
- $\{\wedge_{j \neq i}, G_j, Dom\} \not\models G$ for any $i \in [1, ..., n]$ minimality

where $S \models A$ means the statement A is satisfied in any circumstance where all statements in S are satisfied. In other words, no subgoal is missing for the parent goal to be satisfied. There are several ways for formal verification, e.g., formal refinement patterns, theorem prover, and bounded SAT solver. Formal refinement patterns are used here for some nodes (from top to bottom, the first node adjacent to the goal of Maintain[Indoor ThermalComfort] and the second node bellow the goal Avoid[ThermalConvectionDestroySM], both in Figures 3.6 and 3.7), because they are easy to use and more efficient. [217] has introduced a set of common refinement patterns. Each of them has

been proved formally correct and completed once for all. For example, the divide-and-conquer pattern as shown in Figure 3.8. For the rest nodes, the bounded SAT solver is used.

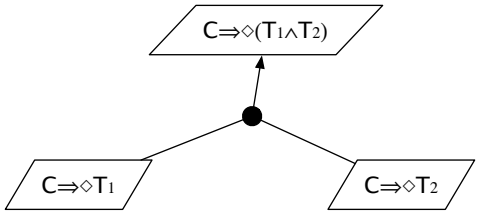


Figure 3.8: The divide-and-conquer pattern.

SAT Solvers are efficient tools for determining whether a given propositional assertion is satisfiable. Bounded SAT Solvers allow some user-defined upper bound to be imposed on the length of satisfying histories. Because the goals and their refinement are formally described in linear temporal logic (LTL), a tool used to verify LTL formulas is required.

NuSMV is a symbolic model checker that can be used to verify LTL formulas. It stands for New Symbolic Model Verifier[†]. It is an open-source product and can be used for model checking. The NuSMV provides a language for describing a model and the LTL specifications. The way to use it is depicted in Figure 3.9.

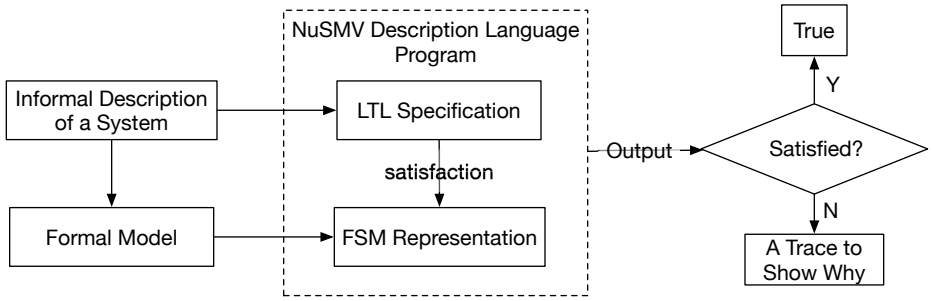


Figure 3.9: Use NuSMV to formally check the goal refinement.

The model of the indoor temperature adjustment by the *Performers System* is described by Finite State Machine (FSM). The LTL specifications describe the relationship between a parent goal with its sub-goals to see whether the FSM represented model satisfies these LTL specifications. If yes, print true, else print a trace to show why it was failed.

The grammer is the NuSMV program is follows:

Program :: module_list
module_list :: module | module_list module

[†]NuSMV: a new symbolic model checker. http://nusmv.fbk.eu/

The program has one module named *main* with no formal parameters.
The grammer of the LTL specifications is as follows:

ltl_specification :: **LTLSPEC** ltl_expr [;]
LTLSPEC NAME name := ltl_expr [;]

The detailed introduction of the grammer can refer to the website of the NuSMV.

In this case, a model for how the indoor temperature is affected should be setup. Heat sources, no matter from natural or man-made, affect the object, including occupants through transmission media. Heat sources include the indoor space may from exterior construction, outdoor air, solar, and home appliances for heating. The transmission media encompasses interior construction and airflow, in which the transfer mechanisms include thermal convection (thermal diffusion and advection) and thermal radiation.

The FSM represents the model of indoor temperature change. The inputs are various heat sources and the output is the indoor temperature. The FSM should be levels of FSMs to represent how heat is transferred to affect indoor temperature. The model of levels of FSMs is shown in Figure 3.10.

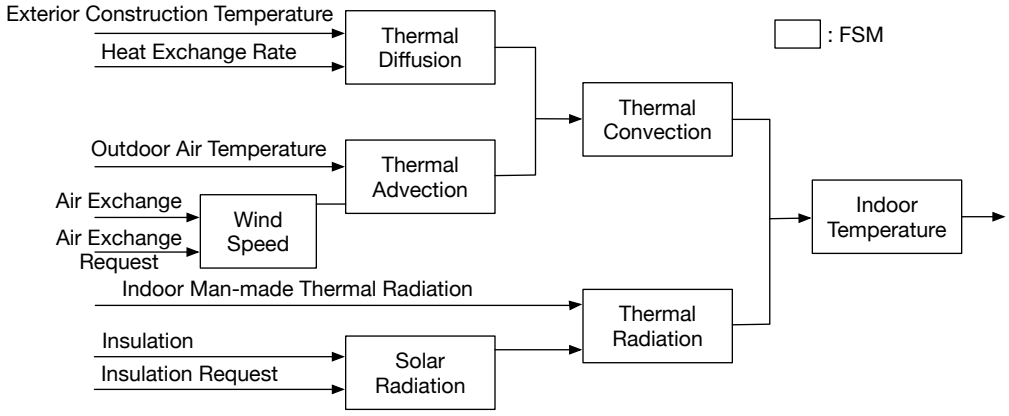


Figure 3.10: Model of indoor temperature adjustment by levels of FSMs.

Based on the levels of FSMs, the modules and their relationships are listed bellow and are represented in class diagrams, as illustrated in Figure 3.11. The NuSMV program code (includes the levels of FSMs and LTL specifications) can be found in Appendix D.

To achieve the verification of the correctness of goal refinements, let us reformulate the problem by applying *refutation principle* in logic. Consider the refinement of a goal G into subgoals $G_1, G_2, ..., G_n$ in a domain theory Dom. The problem is to determine whether Formula 3.1 is satisfiable or not. If yes, the refinement is not complete. The proof of this principle is shown below. The consistency and minimality conditions for refinement correctness are used as additional constraints in this process.

$$G_1 \wedge G_2 \wedge ... \wedge G_n \wedge Dom \wedge \neg G \tag{3.1}$$

Proof. $G_1 \wedge G_2 \wedge ... \wedge G_n \wedge \neg G$
$\Leftrightarrow G_1 \wedge G_2 \wedge ... \wedge G_n \wedge \neg(G_1 \wedge G_2 \wedge ... \wedge G_n)$
$\Leftrightarrow G_1 \wedge G_2 \wedge ... \wedge G_n \wedge (\neg G_1 \vee \neg G_2 \vee ... \vee \neg G_n)$
$\Leftrightarrow [(G_1 \wedge G_2 \wedge ... \wedge G_n) \wedge \neg G_1] \vee [(G_1 \wedge G_2 \wedge ... \wedge G_n) \wedge \neg G_2] \vee ... \vee [(G_1 \wedge G_2 \wedge ... \wedge G_n) \wedge \neg G_n]$
$\Leftrightarrow [(G_1 \wedge \neg G_1) \wedge G_2 \wedge ... \wedge G_n] \vee [(G_1 \wedge (G_2 \wedge \neg G_2) \wedge ... \wedge G_n)] \vee ... \vee [G_1 \wedge G_2 \wedge ... \wedge (G_n \wedge \neg G_n)]$
$\Leftrightarrow F \wedge F \wedge ... \wedge F$
$\Leftrightarrow F$ □

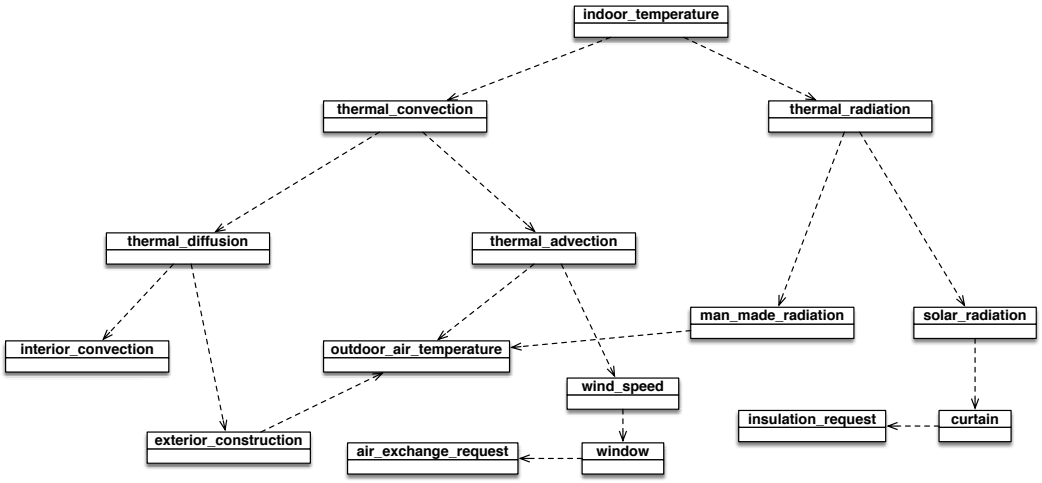


Figure 3.11: The class diagram of the MuSMV program.

Two forms of formal goal specification are employed. They are the goals of *Maintain* and *Avoid* as illustrated as:

> Maintain[GoodCondition]: CurrentCondition ⇒ GoodCondition **W** NewCondition
> Avoid[BadCondition]: CurrentCondition ⇒ ¬BadCondition **W** NewCondition

Then, translate each goal into the NuSMV readable format, next to apply refutation principle, finally, run the NuSMV program to verify the LTL specifications. Part of the verification result and the annotations are illustrated in Figure 3.12. The results show that all the refinements shown in Figures 3.6 and 3.7 are correct and reasonable.

Defect Elicitation

This section tries to explain how to elicit Defects from hazards. To this end, first, to apply the guide words to leaf goals, which generate a series of goal variations. Then, based on expertise to examine the result to generate hazards. Finally, for the corresponding item sketch to see how control actions can result in an identified hazard.

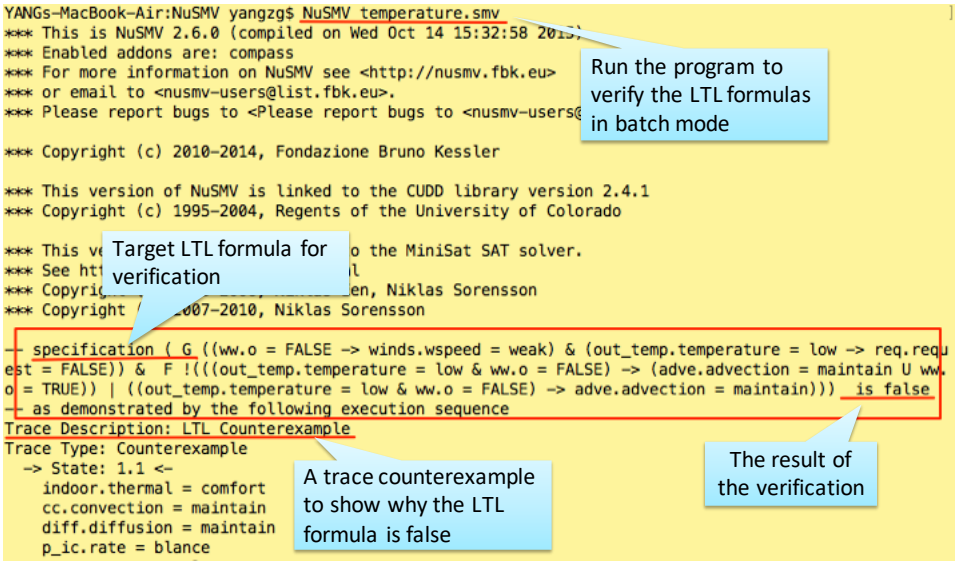


Figure 3.12: Part of the running results of the NuSMV program to verify the LTL specificatioins.

Goal variations can be generated by take advantage of that in Figure 3.5. For example, by applying the guide word **MORE** to the goal Maintain[AirExchange] to generate:

> **MORE** outdoor air has been introduced which undesirable heat is accumulated in the room.

A hazard here is an obstacle to the corresponding goal. It results from inappropriate or unsafe control actions of item sketches. The control actions are elicited from the way to achieve the corresponding goal with respect to item sketches. Then let us define appropriate guide words, by which to examine control actions to check whether a control action can cause a hazardous situation.

3.4.2 Application of STPA

To identify Defects under operation scenarios, the hazard analysis technique STPA [125] is adopted. In this section, let us 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 that with the application of the original STPA.

System-Theoretic Process Analysis

The STPA (Systems-Theoretic Process Analysis) is a novel hazard analysis technique to identify scenarios that cause identified hazards and then to losses. Therefore, one can eliminate or control them. There are several reasons to develop STPA. First, the new causal factors identified based on the STAMP

model that are not handled by the conventional techniques should be included. Second, it is expected to guide users in getting good results. It can also be used before a design has been created and to provide necessary information related to the process of safe design.

The STPA has three steps as shown in Figure 3.13, in which the latter two are taken as the main steps.

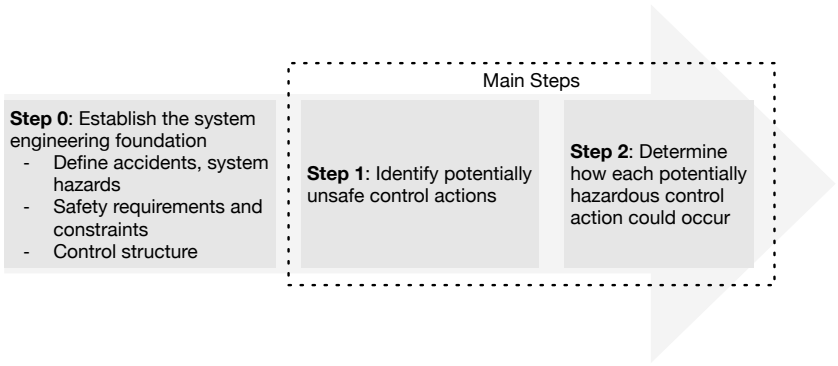


Figure 3.13: The STPA process.

The first step is to establish the system engineering foundation. [125] gave general definitions of accidents and hazards. They should be more specific, e.g., the definitions in Section 2.3.3. If multiple accidents are defined for analysis, it is better to prioritize or assign a level of severity to the identified losses. In the system level, given an accident, how to derive the corresponding system level hazard can be found in Section 3.3.

The system-level safety requirements and design constraints need to be specified to prevent the hazards from happening. Then, the constraints are refined and assigned to every component during the system engineering decomposition.

The safety control structure takes high-level safety requirements and constraints as input. It provides appropriate documentation and a graphical illustration of system functional design. It starts from a simple, high-level model, and further refine the model in steps. For example, only a controller and a controlled process, or a couple of levels of the controller, e.g., human and automated. [122, 125] give detailed and illustrative examples to demonstrate how to construct safety control structures.

Step 1 is to identify possible unsafe control actions (UCA) of the system that could cause a hazardous state. Every controller usually has one or more control actions. Hazardous states are due to inappropriate control or enforcement of the safety constraints, which can result from the following four taxonomies:

1. No provision or follow of a safe control action;
2. An unsafe cotnrol action is provided;
3. Provision of a safe control action at the wrong timing or in the sequence of unexpected;

4. Stop of a safe control action too soon, or apply of it is too long.

Then, let us translate the identified UCAs into safety constraints and requirements on system component behaviors. Generally, the right side of the loop of Figure 3.14 represents the causes of unsafe control action, while the left side of it illustrates the cause of not (or properly) executing a control action.

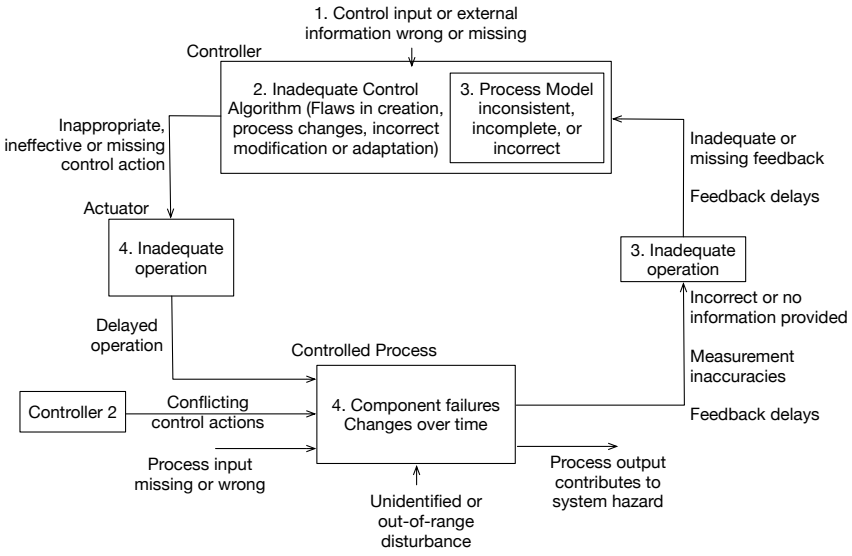


Figure 3.14: A classification of control flaws leading to system hazards [125].

Step 2 looks for the reasons for the possible occurrence of the identified hazardous control actions in step 1. Let us check every piece of the control loop, as shown in Figure 3.14 to see if every identified unsafe control action could occur. Then try to control and mitigates them by designing measures or evaluating measures that already exist. For multiple controllers of the same controlled process, identify potential coordination problems and conflicts.

Another problem is to think about the degradation of designed controls over time, and how to design protections. This may include the management of planned changes, performance audits, and analysis of accidents and incidents. The first is to ensure safety constraints are enforced dynamically. Performance audits ascertain unplanned changes that violation of the safety constraints can be detected. The last is to trace anomalies relate to hazards and system design. Once the causal analysis is completed. Check if they are properly tackled in design, or design features added to control the developed design.

There are several ways to document the results of the analysis, e.g., a control loop with the results in each part, tables, and lists.

Tailor

The understanding of accident formation within the indoor environment has extended the STAMP model, i.e., the STAMP-PP model, with considering physical processes. As discussed in Section 2.3.2 of Chapter 2, abnormal Behaviors result in Service Failures, and the abnormal Behaviors are due to inappropriate control actions of the Performers System. Thus, it is expected to know what are the inappropriate control actions. Therefore, the STPA needs to be tailored for this main purpose.

In the step of establishing the system engineering foundation of STPA, Besides the definition of accident, system hazard, and safety requirement, the 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 due to this work is not for implementing a safe system.

When a Service Failure occurred which means the corresponding control action is inappropriate, then precautionary measure(s) should be provided. Thus, in the first step of STPA, ICAs should be identified concerning the taxonomies provided in step one of STPA. Namely, given a state of physical processes to consider that under specific operation scenarios whether a control action concerning 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 controlling 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 a state of physical processes. Safety requirements for the UCAs also need to be identified for guiding the selection of reaction measures.

The second step of STPA is not necessary. This is due to 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 [122, 125]. After applying the tailored STPA, the results, i.e., control actions, ICAs with their related reliability requirements, operation scenarios for ICAs, precautionary measures, UCAs with their related safety requirements, and operation scenarios for UCAs, could be documented by that used by the STPA. However, the relations among them are not represented. In this paper, I propose a Landscape Genealogical Layout Documentation (that denoted as LGLD) for documenting the results, which is illustrated in Figure 3.15. 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.

For each control action, by considering the taxonomies provided in step two of STPA to list the ICAs. Every ICA is attached with the reliability requirements and operation scenarios. Then, connecting each ICA with a precautionary measure. The precautionary measure is to prevent its connected

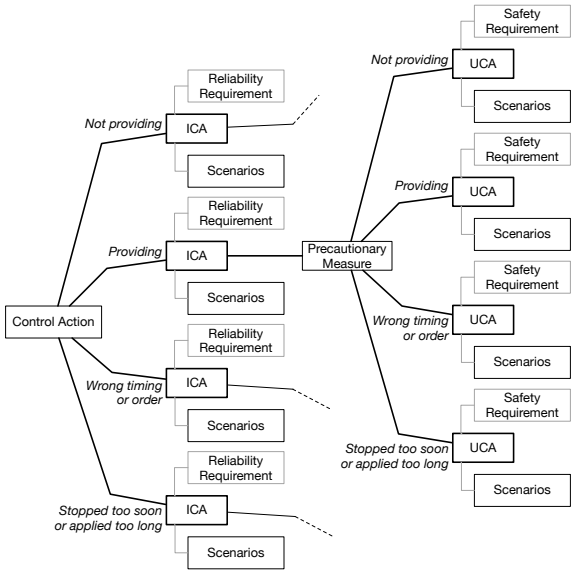


Figure 3.15: Documenting the analytical results by the LGLD approach.

ICA from changing the home environment from a Service Failure to a Hazard. For each precautionary measure to list the UCAs that attached to safety requirements and operation scenarios.

Results

In this section, the STPA is adopted to analyze the hazard identified in Section 3.3. To apply STPA, there are assisting tools to exist to guide the analysis. For example, a tool called XSTAMPP[‡]. Another tool is called STAMP Workbench[§] is adopted for the analysis. The STAMP Workbench is claimed to have features of concentrate on thinking, help analysis and not just an editing tool, guide analysis procedure, but not limit operation, and intuitive operation. Analytical results can be exported into Excel files and images.

In the first step of STPA, let us prepare some concepts for further analysis as shown in Table 3.9. For demonstration, the Service Failure is defined 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

[‡]XSTAMPP (eXtensible STAMP Platform) is a software tool developed to serve the widespread adoption and use of STAMP methodologies in different domains. [visited 2018.10] https://sourceforge.net/projects/stampp/

[§]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 is developed by the IT Knowledge Center of Information-Technology Promotion Agency, Japan. https://www.ipa.go.jp/english/sec/complex_systems/stamp.html

a Service will not fail.

Table 3.9: Preparation for the tailored STPA analysis.

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

The Performers System adjusts the indoor temperature for thermal comfort. The levels of controls for the adjustment is as illustrated in Figure 3.16. The controlled processes and the responsibilities of these controllers are shown in Table 3.10. The control structure is shown in Figure 3.17. The detailed explanation will be discussed when introducing the home safety architecture in the next chapter.

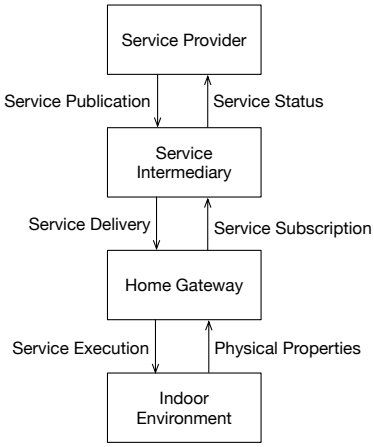


Figure 3.16: Levels of controllers of the Performers System.

Table 3.10: Controllers and their responsibilities.

Controller	**Controlled Process**	**Responsibilities**
Home Gateway	Service Execution	Adjust indoor temperature; Subscribe services
Service Intermediary	Service Delivery	Service distribution; Service management
Service Provider	Service Publication	Service design; Service publish; Service revoke

Due to system operation for indoor temperature adjustment is of the main focus in this dissertation, let us discuss the safety control structure of the Home Gateway to adjust the indoor temperature as shown in Figure 3.18. The Home Gateway is the controller, which is responsible for executing the indoor temperature adjustment service. The controlled process is the Home Environment. Performers

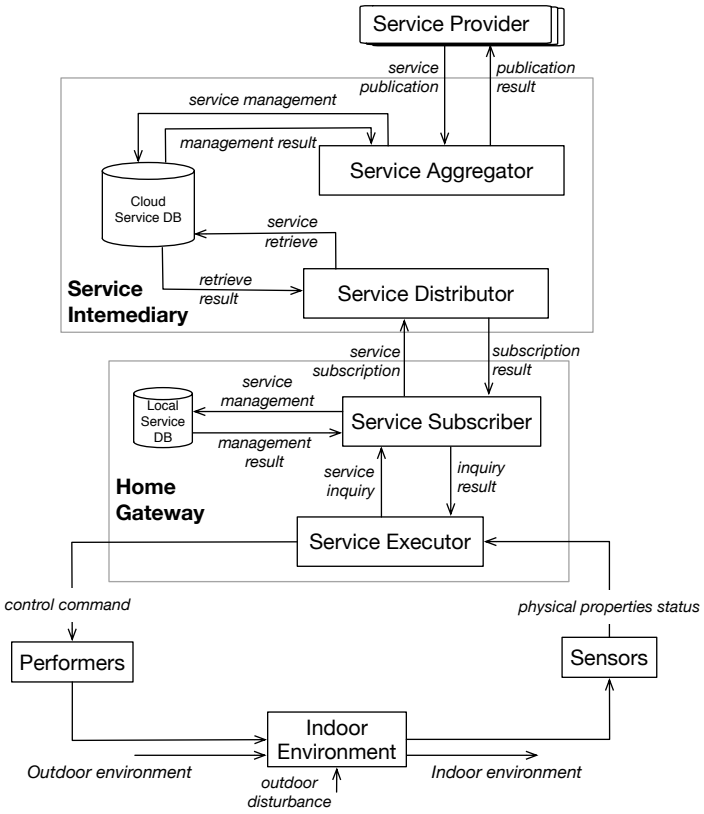


Figure 3.17: The control structure of the Performers System for indoor temperature adjustment.

are taken as actuators. Let us consider an air-conditioner and a window here as Performers. Empirically, for energy saving, these two can not 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.

Next, based on the results of the first step, let us identify ICAs, UCAs, and elicit their related requirements and operation scenarios. Part of the results are shown in Figures 3.19 and 3.20 that are for the control actions of "set OFF" and "set to X °*C*". "N/A" denotes the taxonomy is not applicable to the corresponding control action. In Figure 3.19, 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 of the not providing caused ICA, this is due to people are

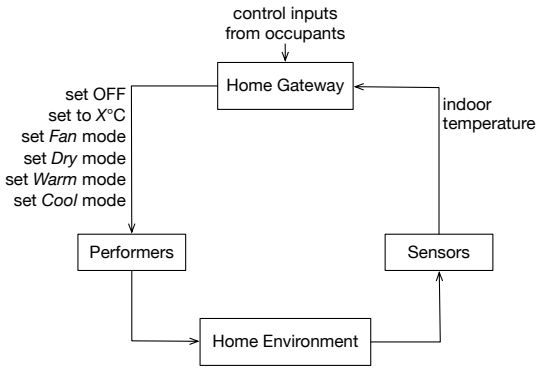


Figure 3.18: The safety control structure of home gateway for indoor temperature adjustment.

not sensitive to temperature change, and thus did not issue the "set OFF" command manually.

For the results as shown in Figure 3.20, 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 that if it works in the Warm mode, which in this case is inappropriate or hazardous, and one 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, it may not be an ICA or UCA even "set to X $°C$" is not provided. One more thing that needs to be explained is that providing "set to X $°C$" at "wrong time" is not inappropriate nor hazardous. If it is not provided in time, the home environment would experience Service Failure or Hazard for some time. But providing "set to X $°C$" at a different time should not be inappropriate nor 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.

Comparsion of Results

Originally, the STPA is the only hazard analysis technique based on the STAMP model [125]. Thus, in this section, let us compare the results presented in Section 3.4.2 with that by adopting the original STPA. Since the second step of STPA did not take into account, the comparison only considers the results derived from the step of establishing the engineering foundation and the first step of STPA. For comparability, the temperature issue discussed in Section 3.3 is still focused on when adopting the original STPA.

As discussed that 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 3.14 under some scenarios which are different from our case. The elimination or control usually resorts to design and implement a safe system, while in our case is to select appropriate precautionary and reaction measures that can restore a safe Service delivery.

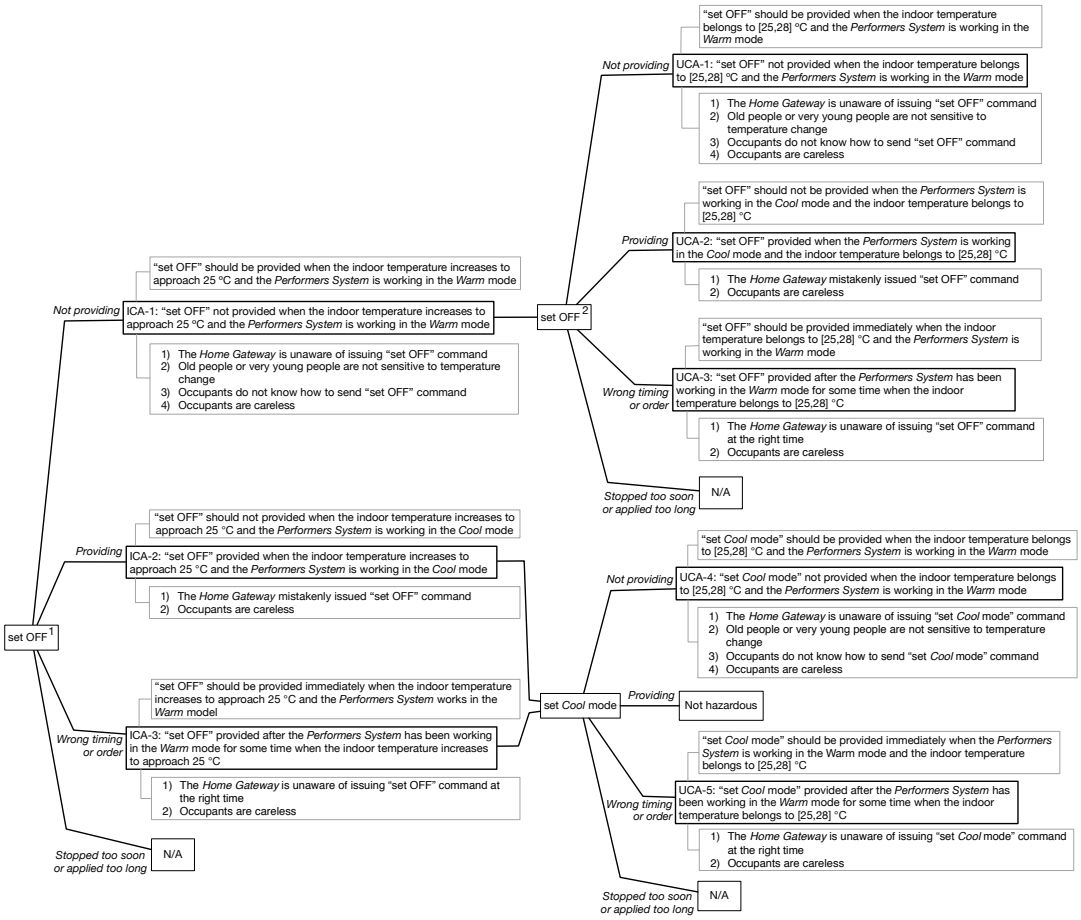


Figure 3.19: The analysis results for the control action "set OFF".

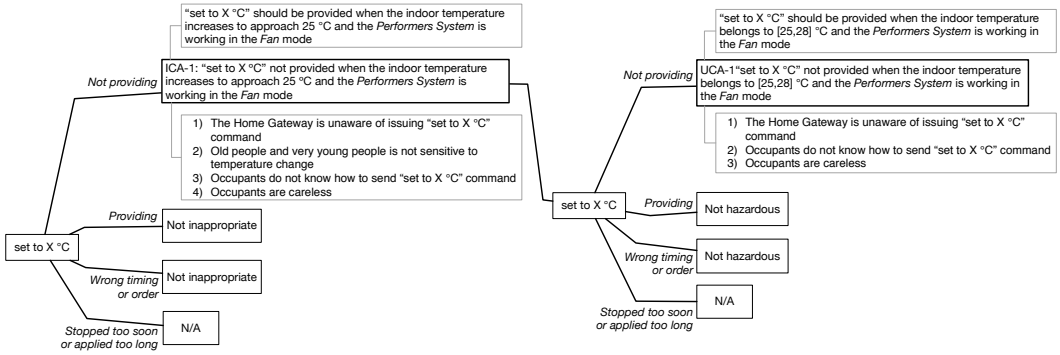


Figure 3.20: The analysis results for the control action "set to X $^{\circ}C$".

The system engineering foundation is given first. The prepared definitions are illustrated in Table 3.11. The design constraint is a system-level constraint and is expected to further decompose into constraints that can be assigned to system components as the analysis evolves. Compare with that of Table 3.9, 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 the reliability requirements of ICAs can be taken as the decomposition of the system-level reliability requirement. The safety control structure as shown in Figure 3.18 can also be used here.

Table 3.11: 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 3.12 and 3.13 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 Table 3.12 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 accurately aware of the indoor temperature change.
- "set OFF" should be provided when needed.

Table 3.12: 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

There are some differences by comparing with the results derived in step two of STPA. The ICAs, operation scenarios for ICAs, reliability requirements, precautionary measures, and operation scenarios for UCAs can not be obtained by adopting the original STPA. However, the design constraints can be derived. The UCAs identified by adopting the original STPA is equivalent to that identified by the tailored STPA.

Table 3.13: 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

3.5 Discussion

The discussion includes two parts. The first is a comparison of the two hazard analysis techniques, i.e., the tailored STPA and the innominate approach. The second part of this section discusses the effectiveness of the tailored STPA due to the tailored STPA has better performance in identifying Defects.

3.5.1 A Comparison

In this section, let us compare the two techniques, i.e., STPA [125] and the innominate approach [94] in identifying Defects. Defects include ICAs and UCAs. The comparison is based on several criteria. The first and important one is that whether Defects can be identified. Second is the effort in the identification, that is, the work to prepare for the identification and the complexity of steps in the identification. A brief comparison of the two techniques is shown in Table 3.14.

The STPA approach adopts a top-down fashion, i.e., from accident to causes to identify Defects. The innominate approach starts from deviations, i.e., deviate from goals (obstacle goal) to two directions. The upper direction is to analyze the accident or loss the deviation brings about. The lower direction is to identify the causes that result in the deviation. The innominate approach is similar to HAZOP [50].

There are similarities in preparations. The safety control structure is equivalent to item sketches, and safety requirements are similar to the goal model. However, the way to build the safety control structure and item sketches are different. The goal model is structured and layered, while safety requirements have decomposition relations. The STPA provides four taxonomies to look for UCAs, while in the innominate approach one has to design guide words and are used to look for obstacle goals.

The tailored STPA has one main step that encompasses two sub-steps to identify Defects and their related requirements and scenarios. THe innominate approach three steps in the identification. Moreover, it need two sets of guide words. one set is to elicit goal variations, and another set is to derive UCAs. The latter set can be the same as the taxonomies provided in the STPA approach. The tailored STPA is able to identify Defects, i.e., ICAs and UCAs, while the innominate approach can only identify UCAs.

The techniques are effective and practical for identifying and analyze hazards. The innominate approach needs more improvement to identify Defects. The results of the analysis are prodigious. The LGLD approach of documentation can straightforwardly represent the relationships among the

Table 3.14: A comparison of STPA and the innominate approach.

	Tailored STPA	**Innominate Approach**
Foundation	Systems Theory	No explicit statement
Phase of System Development	Concept phase	Concept phase
Preparation	Interested accident(s), system level hazards; safety requirement, safety control structure	Item sketch, goal model (including its verification), guide words
Application Area	Socio-technical systems	Software-intensive embedded systems
Complexity of Steps	One main step to elicit ICAs and UCAs, and related requirements and scenarios	Apply guide words to generates goal variations; hazard identification; apply guide words to control actions
Output Defects	Defects	UCAs
Results Documentation	LGLD approach	Not explicitly given

analytical results.

3.5.2 Effectiveness of the Tailored STPA

In the step of establishing system engineering of STPA, accidents and system hazards are provided mostly depend on the interest of an organization or the government [125]. For example, in this paper, the Accident is defined as physical harm of occupants due to heatstroke as illustrated in Table 3.9. It can be others besides due to heatstroke, e.g., severe cold. The concrete accidents are different due to the variety of environments, e.g., workplaces and the home environment. It is also determined by budget, the severity of occurrence, and frequency of occurrence [125].

In step one of STPA, originally, the taxonomies are 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 System. For example, the Performers System stopped working is achieved by the control action "set OFF" as shown in Figure 3.19. 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 for comfort to one for uncomfortable, then to hazardous. When a state for uncomfortable is detected, precautionary measures are adopted to pre-

vent the physical process from transferring into a state of hazardous. Precautionary measures refer to control actions that achieved by reconfigurations. Thus, the taxonomies are also applicable to the precautionary measures. For example, the control action "set OFF" in Figure 3.19 can both be the original control action and the precautionary measure. So does the control action "set to X $^{\circ}C$" as shown in Figure 3.20.

The purpose of adopting the hazard analysis technique is to identify Defects, to select appropriate precautionary and reaction measures for adjusting home environment anomalies to maintain a normal performance. By checking the comparison presented in Section 3.4.2, I found the tailored STPA can satisfy this purpose, while the original STPA cannot. First, ICAs under operation scenarios and reliability requirements of the ICAs can be identified by the tailored STPA. This is due to Service Failure, and the system-level reliability requirement are 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 both be identified by 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 3.14, which are identified in step three of STPA.

As discussed in Section 3.4.2, the STPA takes advantage of tables and lists to document the analytical results (see the results shown in Tables 3.12 and 3.13). I proposed the LGLD approach to document the analytical results. The advantage by comparing with tables and lists is that it can represent the relations among the results in a straightforward way. For example, in Figures 3.19 and 3.20, the relations among control actions, ICAs, precautionary measures, and UCAs are clear. Also, 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 by using tables and lists like the ones presented in Section 3.4.2. 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 identify UCAs under related operation scenarios, and safety requirements.

3.6 Conclusion

I found the tailored STPA can effectively identify Defects by comparing it with the innominate approach. In order to identify the Defects, i.e., ICAs and UCAs that result in abnormal system behaviors, the hazard analysis technique STPA is tailored and applied to the smart home system for indoor temperature adjustment. After comparing with the results derived by adopting the original STPA, I found that the tailored STPA is an efficient tool to assist in identifying the Defects. The analytical results of applying STPA used to adopt tables and lists for documentation, in which the relations among the results are not straight-forward and unclear. I then proposed the LGLD approach, which its advantages are demonstrated by the comparison of results.

4
Home Safety Architecture

The detection and prediction of physical process anomalies, i.e., Service Failure and Hazard that are introduced in Chapter ref ch2: title, should base on a safety problem architecture. To this end, this chapter introduces an event-based home safety probelm detection/prediction under the Cyber-Physical Systems (CPS) home safety architecture. The CPS home safety architecture is taken as the architecture foundation for safety problem detection/prediction. The event-based detection/prediction approach is realized based on this home safety architecture. Moreover, reactions to safety problems are also expected to base on this architecture. To demonstrate how the architecture can support safety problem reaction, a redundancy approach is proposed to retain the reliability of various indoor environment adjustment services, e.g., indoor temperature adjustment service.

The contributions of this chapter are as follows [227]:

- A CPS home safety architecture has been proposed for the detection/prediction of safety problems. It is also excepted to support safety problem reactions.
- An event-based home safety problem detection/prediction is proposed based on the architecture.
- Two examples are used to demonstrate the feasibility of detecting/predicting safety problems based on the proposed architecture.
- A theoretical mechanism for service redundancy for reaction is proposed.

4.1 Architecture Design

Safety problems that may happen in the home environment are varied. I classified three big types, i.e., home appliances safety, indoor environment safety, and interaction safety between occupants and home appliances [226]. Home safety problems are to result in undesired consequences, e.g., casualty

or home property loss, or both. So it is necessary to propose an effective method in order to detect/predict and react to the home safety problems. Proposed systems in literature, e.g., [55, 89, 111] in some way solved the problem partially. Some aspects left unsolved. First, smart home systems have a variety of functions, which interact with other systems inside and outside the home. For example, services that smart home systems can provide are home theatre, HVAC system, etc. as introduced in Section 1.1.1. They control multiple home appliances and share information. Thus, the system that enables the detection/prediction and reaction should not be separated from other systems. Second, safety problem detection/prediction service and reaction service to anomalies should be deployed in geographically different locations for easy management and cost-saving. Third, the ability to deal with safety problems that could occur in multiple homes is also required. These motivated the proposal of the home safety architecture.

Researches related to the CPS are pervasive in recent years. By integrating the event-based method into the CPS is also emerging [199]. The interactions between physical and cyber worlds are thought to be ruled by events. [200] proposed a CPS architecture that claimed to be the first event model that integrates characteristics of CPS for analysis in the time and space domain. There are some applications of CPS systems like [53, 55]. Events in conventional event-based methods have the same importance. However, it is not always true when coming to the events of the physical world. They should have different importance, e.g., eating may be more important than others when you are starving. Moreover, the occurrent of an event may due to the occurrence of some other events. Thus, we propose a layered FSM (Finite State Machine) approach that takes raw data and the predefined events with importance as inputs and outputs. After an (undesired) event is detected or predicted, the proposed architecture can also support to the reaction to the event. The reactions are various services that are designed and published by service providers. The Next Generation IP Network Promotion Forum* has proposed a service intermediary model for gathering, manageing, and distributing services. The proposed home safety architecture is based on the CPS and service intermediary model.

We proposed the CPS home safety architecture that enables both event-based and service-based methods for the detection and reaction of safety problems. Layered FSMs that composite events in the event-based method. It takes different events and raw data as input and output. Different events represent individual safety problems or safety levels of a home. Details of the service-based method are left to future work. Examples of heatstroke and carbon monoxide poisoning are used to demonstrate the proposed layered FSMs, in which the results prove the effectiveness of our proposal in supporting to detect safety problems.

4.1.1 Cyber-Physical Systems

CPS is considered the integration of the computation, communication, and control with physical processes. The term was coined by the U.S. National Science Foundation in 2006 [69]. It is a time-sensitive, spatially-distributed, and multi-scale networked embedded system, which connects the phys-

*Next Generation IP Network Promotion Forum, [visited in 2012] http://ngnforum.nict.go.jp/

ical world with the cyber world by actuators and sensors [61]. [57] summarised some characteristics of the CPS from the viewpoint of networking. They are network complexity; resource (like bandwidth, throughputs, energy efficiency, and rate through) limitations; hybrid traffic and enormous data including sensor data and various data contents; unreliability due to sensor measurement, software error, and unexpected events occurs in the physical world; complexities of modeling, design, analysis, implementation, and verification for the CPS. The state-of-the-art modeling of the CPS is by hybrid automata, which can model the discrete states of cyber systems and the continuous states of variations in physical processes [121].

There are many applications of CPSs. For example, aircraft manufacturing, smart electric grid, smart transportation, smart home/building, smart medical technologies, air traffic management, etc. To enable the integration of control, computation, and communication for quick deployment and design of CPSs, design, and architecture are essential for infrastructure [235]. For example, interfaces between the power network and cyber systems, between independent machines (smart devices and appliances), and between humans and machines. Furthermore, accurate controls on the physical processes by effectively assigning computing capabilities for a specific purpose are of importance. Therefore, architectures and its related techniques are needed to ensure integrity, availability of data, confidentiality, and also accurate controls.

[116] proposed a CPS architecture for industry 4.0-based manufacturing systems. The architecture is a 5-level CPS structure, i.e., the 5C architecture, for providing a step-by-step guideline to develop and deploy a CPS for various applications. This 5C architecture is outlined in Figure 4.1. [99] extended this architecture by adding 3C facets, i.e., coalition, customer, and content, into the 5C architecture. The 3C facets emphasize more on horizontal integration by comparing it with the vertical integration of the 5C architecture. One application of the 5C architecture and its derivatives can be used to develop systems like predictive production systems [117].

Authors of [200] discussed that events related to the interactions between the physical and cyber world in time and space domain are important. They explored the temporal and spatial properties of events and developed a layered Spatio-temporal event model for CPSs. Figure 4.1 illustrates a simplified architecture and events that processed in each part of the architecture.

The Internet of Things (IoT) could be considered as the backbone of CPSs [61]. The IoT is defined as the earth-wide infrastructure for the information society. It enables services by interconnecting things ground on existing and evolving communication technologies and interoperable information [3]. Things can be physical things or virtual things. They can be identified and integrated into communication networks. The IoT makes full use of things to provide various services to a variety of applications. Architectures of the IoT are varied due to the diversity of applications. For example, [171] surveyed IoT architectures, and they can be domain-specific, e.g., in domains of RFID (Radio-Frequency IDentification), Service Oriented Architecture, Supply Chain Management, Wireless Sensor Network, and Industry, Health Care, Smart Society, Cloud Service and Management, and Social Computing Security.

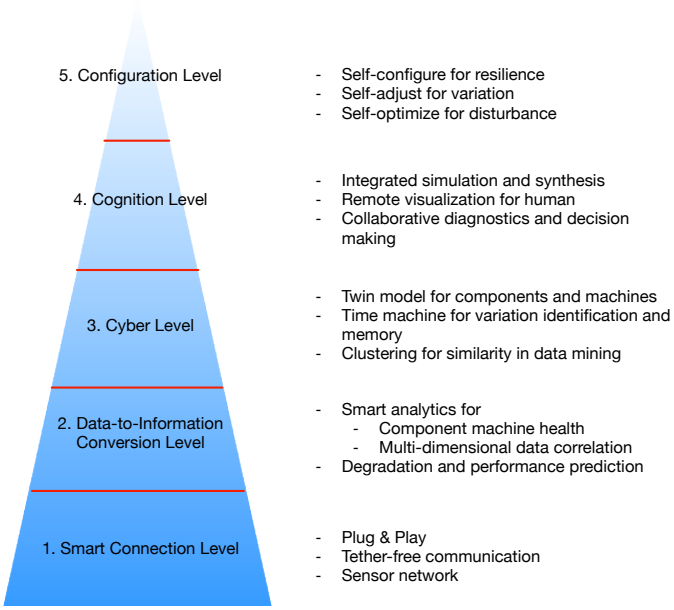


Figure 4.1: The 5C CPS architecture.

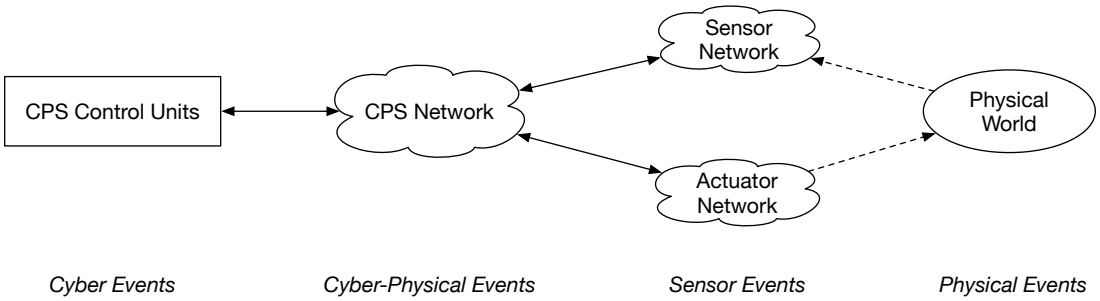


Figure 4.2: A simplified arhictecutre with events that processed in each part of the architecture.

4.1.2 Service Intermediary Model

Various home appliances are interconnected through smart home networks to produce integrated services [43, 148]. For example, the indoor temperature adjustment for thermal comfort is a service example of such services. So, many various service providers provide various services. Be aware that the service here is different from the definition in Chapter 2. With mainly considering service aggregation, management, and distribution, the Next Generation IP Network Promotion Form proposed the Service Intermediary Model (SIM) as illustrated in Figure 4.3. Others mean there can be other functions to be implemented in the SIM model.

Service aggregation aggregates various services from service providers through different forms. This

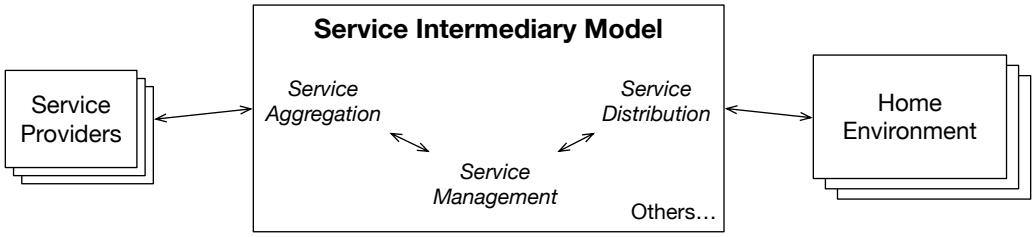


Figure 4.3: The service intermediary model.

is due to the services are devised and provided by different service providers, which have different service contents. Different forms mean the publish, update, and revoke can be diverse and up to user preference. To popularize this architecture, it is better to standardize the process. After services being published to the SIM, they need to be further managed. For example, backup them in case of data loss due to hardware failures; assembling advanced services based on the existing one(s) on the request of users from the home environment side. For example, a home theater service may need curtain control service, illumination service, stereo set control service, etc. Service distribution is responsible for service subscription from the home environment and service distribution in response to the subscription. There can be other functions to be added besides these three.

4.1.3 Home Safety Architecture

We propose the CPS home safety architecture to support the detection/prediction and reaction to detected/predicted safety problems in real-time. To this end, we employed the concept of the Service Intermediary Model and the concept of CPS. An event-based method is proposed for safety problem detection/prediction, and a service-based method is supposed to react to detected safety problems.

There are some assumptions to elaborate on the CPS home safety architecture. First, home networks enabled all home appliances to interconnection. Data about the home environment are collected by various sensors and reaction to anomalies through actuators. Second, sufficient computing and storage capability of devices in the home gateway and the service intermediary. Third, home networks also connect the related computing devices and databases in the form of wired and/or wireless.

Architecture Elaboration

Figure 4.4 illustrates the CPS home safety architecture. The architecture is divided into four main parts: Service Provider, Service Intermediary, Home Gateway, and Home Environment.

The Home Environment is where occupants live permanently, which equipped with various home appliances connecting to the home network to satisfy the requirements of occupants. This is the place where safety problems could occur. It also deploys with a variety of sensors and actuators, and thus sensed data can be collected and then transmitted through the Home Gateway. Moreover, control commands are also executed in the Home Gateway.

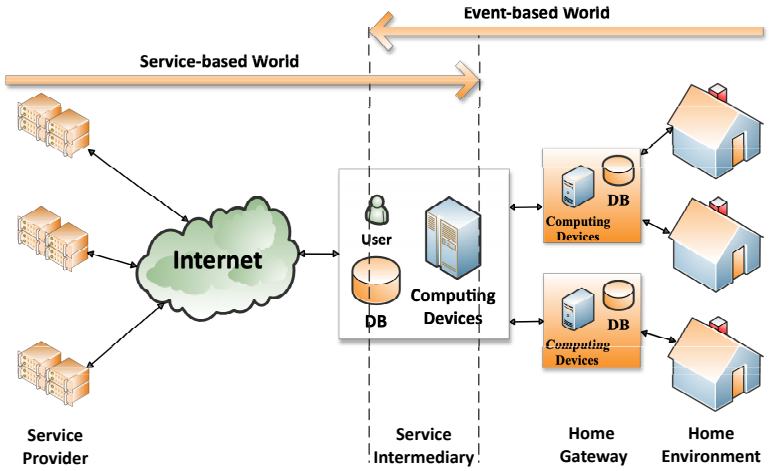


Figure 4.4: The CPS home safety architecture.

The Home Gateway that can be taken as a gateway connects the home network to the outside networks. It has the fundamental function of transforming different network protocols between the home network and the network outside the home. Moreover, it has the distinct function of capable to execute services to issue commands to actuators to adjust the indoor environment. It subscribes services from the Service Intermediary if the local database (DB) does not store them. The Home Gateway observes the home environment and generates corresponding events to decide which service needs to be chosen to execute. Also, these events will be passed to the Service Intermediary for mastering the whole situation. Two databases (DBs), i.e., a logging DB and a DB for managing the prescribed services are in the Home Gateway.

The Service Intermediary has two main functions. One is to aggregate services from different service providers and manage them locally. Another is to react to the service subscription. Safety levels of various home environments are also evaluated here. Then appropriate relevant services can be subscribed if not stored in the local BD of the Home Gateway for reactions. The Service Intermediary can also assemble advanced services. Similar to the Home Gateway, two DBs are also located here. A logging DB that stores detected events, and a cloud service DB that manages services gathered from Service Providers.

The Service Provider devises, publishes, updates, and revokes concrete services to the Service Intermediary.

Component Description

This section elaborates on the proposed architecture by introducing its constituent components that are illustrated in Figure 4.5. The Home Environment has home users, i.e., occupants, home devices, i.e., computing and appliance, and the indoor space. It also deploys various sensors, which send sensed data to the Elementary Event Generator. The first level of layered FSMs that will be discussed in

Section 4.2 corresponds to the Elementary Event Generator. Then, elementary events are passed to the Semantic Event Generator in the Home Gateway for further process.

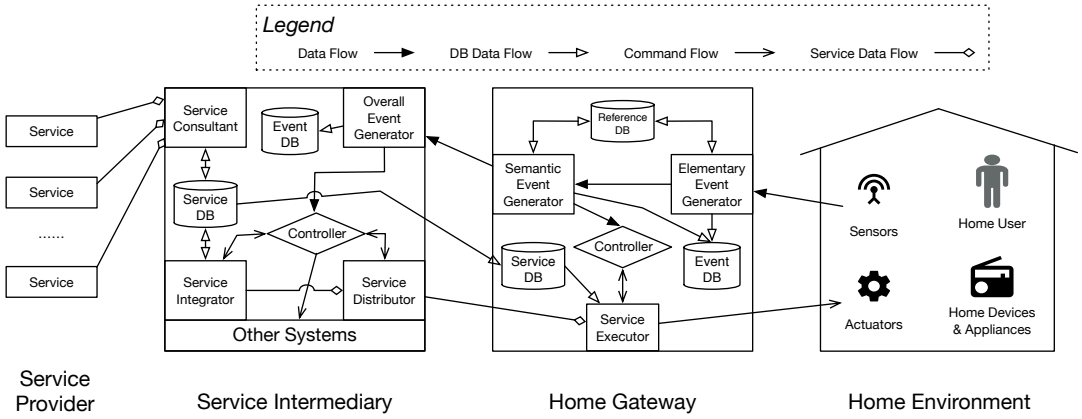


Figure 4.5: System components description.

As illustrated in the Home Gateway of Figure 4.5, One black arrow goes from the Semantic Event Generator to the Controller. The Controller takes over to execute services to control home appliances, etc. when disconnection between Home Gateway and Service Intermediary has occurred. Another black arrow connects to the Entire Event Generator that resides in the Service Intermediary. The semantic events are passed to the Service Intermediary. The second level of the layered FSMs corresponds to the Semantic Event Generator.

The safety level of a home is evaluated in the Overall Event Generator of Service Intermediary. Then, the results are passed to the Controller of Service Intermediary. The Controller notifies the Service Integrator to assemble the required services. And the Service Distributor distributes assembled services to the Service Executor of Home Gateway. Finally, control commands are issued to control actuators to retain home safety.

4.2 Event-based Method

Event has been defined as the occurrence of a particular set of circumstances [5, 154]. It can be one or more occurrence with one or several causes. Event models can be classified along several dimensions [199] as follows:

- Punctual (e.g., to send and receive a message) vs. durative (e.g., attending a lecture)
- Single vs. stream (e.g., object tracking)
- Change vs. action/observation

Generally, there are two distinct contexts, in which to use the term event. The first is about the physical world occurrences. The second relates to those occurrences in the cyber world. We defined four types of events in this section, that are, elementary event, semantic event, overall event, and service event. Service event is about the services provided by Service Providers, which will not be detailed here.

1. Elementary Event: it is generated by the abnormal variation of raw data. For example, indoor temperature varies greater than a preset value. It indicates the occurrence of Service Failures that introduced in Chapter 2.

2. Semantic Event: it is generated based on multiple Elementary events, which represents an individual safety problem. For example, events of temperature and/or humidity anomalies generate the event of heatstroke. It means the occurrence of the Accident that introduced in Chapter 2.

3. Overall Event: it means the safety level of a home. We define three levels, i.e., green denotes safety situations; yellow represents multiple safety problems that have occurred, which result in property loss; and red means the occurrence of safety problems that result in casualty, or casualty and property loss.

4. Service Event: events related to services, e.g., service subscription.

For detecting/predicting the defined events based on the architecture discussed in Section 4.1.3, a layered FSMs method that is illustrated in Figure 4.6 will be detailed.

Raw data are collected from sensors deployed in the Home Environment. Elementary Events are generated from raw data anomalies, e.g., abnormally high temperatures. A Semantic Event denotes the occurrence of an individual safety problem. Overall Event indicates the safety level of a home, which is generated by evaluating Semantic Events of a home.

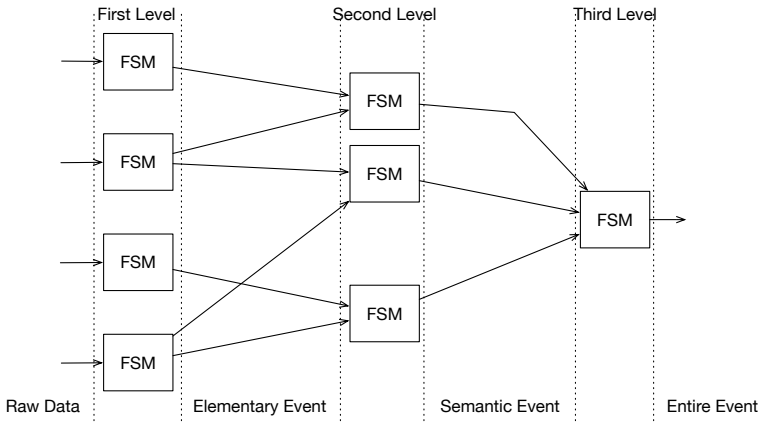


Figure 4.6: Layered FSMs method.

4.2.1 Event Sets

Event sets include the defined events as illustrated in Formula 4.1.

$$E = \{EL, EM, EN, ES\} \tag{4.1}$$

where EL denotes the finite set of Elementary Events; EM represents the finite set of Semantic Events; EN means the finite set of Overall Events, and ES is the finite set of Service Events.

General notation of every individual event that belongs to its corresponding event set is represented as follows.

$$el_{ID} \in EL, em_{ID} \in EM, en_{ID} \in EN, es_{ID} \in ES$$

4.2.2 Individual Event

An individual event has several properties that characterize an event. Except for the Service Event, the general representation of Elementary Event, Semantic Event, and Overall Event is shown in Formula 4.2.

$$e = \{e_{type}, t, l, s\} \tag{4.2}$$

where e_{type} means the event type that indicates the category of the event; t represents the time to generate the event; l denotes the location where the event has occurred. The location is denoted as $[h, r]$, where h means house ID, and r denotes room ID; s represents the event significance.

Assume that lower-level events have different importance in contributing to higher-level events. Every lower level event has the significance that represented by a value. Higher-level event significance is generated by relatively lower level event significances. Each individual event significance satisfies $s \in [0, 1]$. The sum of the significances of lower-level events satisfies $\sum s \leq 1$. The generation of a higher-level event is when the sum of the significances is greater than a threshold value. The threshold value of significance can be determined by rich experienced engineers who know safety problems well.

4.2.3 Relationships of Event Types

This section discusses the relationships of event types. Semantic Event type and Elementary Event type satisfy the relationship as represented in Formula 4.3.

$$em = \{\bigwedge_{i=1}^{N} el_i | N \in Integer, el_i \in EL\} \tag{4.3}$$

Multiple semantic events may happen in one or more rooms. Thus Semantic Event type and Overall Event type satisfy the relationship as shown by Formula 4.4.

$$en = \{ \bigwedge_{i=1}^{room\_num} \left(\bigwedge_{j=1}^{event\_num} em_j, l_i \right) | em_j \in EM, l_i \in [h, r] \} \tag{4.4}$$

4.2.4 Definition of FSMs

As discussed that the layered FSM method has three levels. Raw data and the defined events are inputs and outputs to the layered FSMs. Every FSM has different content with the same FSM definition. The FSM is defined as a five-tuples, which is shown as bellow.

$$M = (Q, \Sigma, \Gamma, \delta, q_0) \tag{4.5}$$

where M means a FSM; Q denotes a finite set of states; Σ represents a finite set of inputs; Γ means a finite set of outputs; δ is the transition function that is represented by $\delta : \Sigma \times Q \rightarrow \Gamma \times Q$. And q_0 is the initial state. The values of each tuple defined in the FSM are different for the FSMs in the layered FSM method.

Let us see the FSMs of the first level, $Q = \{normal, abnormal\}$, Σ represents the raw data, Γ denotes a subset of the Elementary Event set, and $q_0 = normal$.

For FSMs of the second level,

$$Q = \{safe, transforming, unsafe\}$$

where Σ means a subset of Elementary Event set, Γ denotes a subset of Semantic Event set, and $q_0 = safe$.

For FSMs of the third level, $Q = \{green, yellow, red\}$, where *green* represents the home is normal, *yellow* means property loss, and *red* denotes casualty or casualty and property loss. Σ means a subset of Semantic Event set, Γ is a subset of Overall Event set, and $q_0 = green$.

Significances are adopted to evaluate transition functions. A transition has occurred if the sum significance of the same level events is greater or equal to a threshold value.

4.2.5 Simulation Cases

This section discusses two simulation cases to verify the feasibility of detecting/predicting safety problems by the layered FSM based on the proposed CPS home safety architecture. One example is to detect/predict heatstroke that occurred indoors. Another example is to detect/predict carbon monoxide poisoning. The aim of the experiment is three-folds. First, to demonstrate how to use the defined events to represent what has happened. Second, to evaluate whether the layered FSMs method is efficient in detecting/predicting safety problems. Third, the proposed CPS home safety architecture can well support detection/prediction. Figure 4.7 shows the layered FSMs that model the two simulation cases.

Heat Stroke

The planet undergoes a lot of weather anomalies, as discussed in Section 1.1.2. In Japan, air conditioning units are working intermittently in hot and cold weather due to energy saving. Moreover, climate anomalies occur regularly. More attention should be paid to heatstroke since it can cause health problems or death to old people and young babies who are not sensitive to climate change.

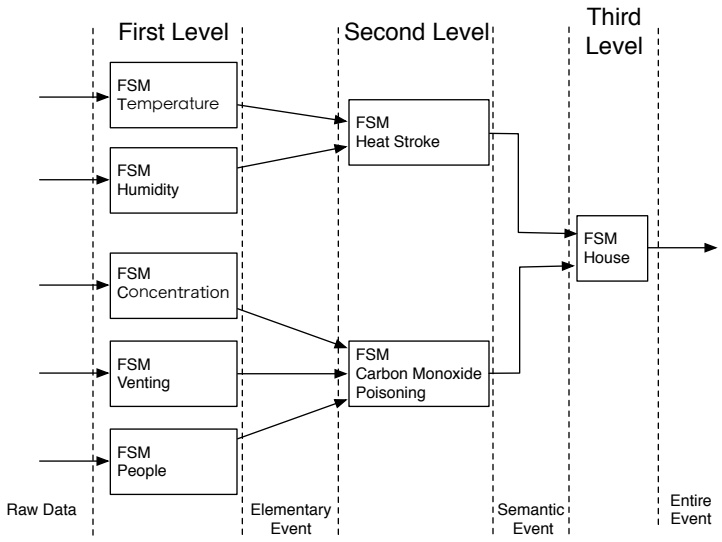


Figure 4.7: Layered FSMs that illustrate the simulation cases.

The indoor temperature and humidity are two important factors that affect the cooling effect in hot weather [78]. The relationship between them is inversely proportional, e.g., temperature increases while humidity will decrease. Generally speaking, people feel uncomfortable if the temperature and humidity are greater than threshold values, respectively. And these threshold temperature is 34°C and humidity is 35% [151].

The variations of indoor temperature and humidity are illustrated in Figure 4.8. On the left dashed line 1, the value of humidity is smaller than the threshold, which indicates the current state of the FSM of humidity is *normal*, and the output event is also *normal*. On the right side of dashed line 1, the humidity enters the state of *abnormal*. On the left side of the dashed line 2, the temperature is smaller than the threshold value, in which the current state of the FSM of temperature is *normal*, and the output event is also *normal*. The temperature data on the right of the dashed line 2 represents the FSM entered the abnormal state, and the output event is *abnormal*.

We assume that the significance of *abnormal* event for temperature is 0.6, and the significance of *abnormal* event for humidity is 0.4. We prescribe the threshold significance is 0.7. In this situation, on the right side of dashed line 2 denotes the high possibility for heatstroke to occur. Then, the output event is the Semantic Event. These output events can be because of detected evidence or predicted results.

Carbon Monoxide poisoning

Another safety problem that could occur indoor is carbon monoxide poisoning. Carbon monoxide is an odorless and colorless gas that can cause sudden illnesses or death. Normally, it could occur in the kitchen due to gas leakage or not full burnt materials. The carbon monoxide poisoning is dependent

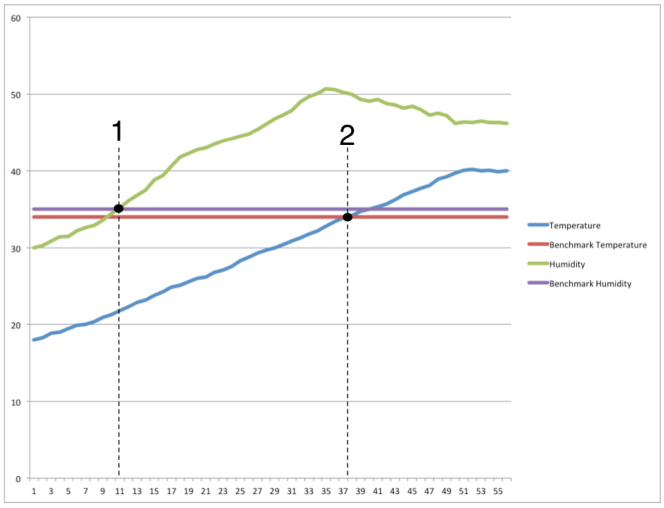


Figure 4.8: Data of temperature and humidity that contribute to heat stroke.

upon the concentration of carbon monoxide, venting condition, and people on the scene. Figure 4.9 illustrates how the data relate to the three factors could result in the occurrence of carbon monoxide poisoning. The venting system is not working if the value indicating the venting condition is smaller than 0. There are people on the scene if the value in the figure that indicating people are greater than 0. Elementary Event *abnormal* can be generated. For example, if the value of carbon monoxide concentration is greater than the benchmark, which indicates an Elementary Event of *abnormal*.

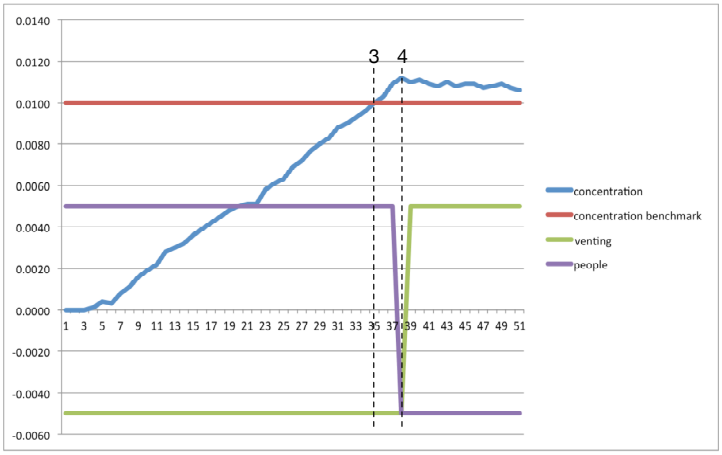


Figure 4.9: Related data that contribute to carbon monoxide poisoning.

It is assumed that the venting condition, the significance of carbon monoxide concentration, and the existence of people are 0.3, 0.4, and 0.3, respectively. The threshold significance is 0.7. So the data

between dashed lines 3 and 4 correspond to the *unsafe* state of the FSM, which means a Semantic Event, i.e., the occurrence of carbon monoxide poisoning.

Based on the simulation results as illustrated in Figures 4.8 and 4.9, the house is in state *red* between the simulation time [35, 37], the Semantic Event of carbon monoxide poisoning contributes to the production of the Overall Event. Semantic Events of carbon monoxide poisoning and heat stroke contributes to the production of Overall Event between simulation time [37, 38]. The Semantic Event that denotes the heatstroke contributes to the generation of the Overall Event after the simulation time 38. In summary, the simulation results verified the simulation goals.

4.3 Safety Problem Forecasting

Forecasting of safety problems in this dissertation refers to that the forecasting concerning the indoor climate, e.g., indoor temperature forecasting or events related to indoor safety problems, as discussed in Chapter 6. Safety problems are about the Hazards introduced in chapter 2. Various techniques can be used for forecasting. For example, artificial neural networks [13, 71], and machine learning [134] can be used for indoor temperature prediction. One significant advantage of the forecasting is energy-saving [13, 71]. In the viewpoint of this work, the forecasting can save time for precautionary reaction and remedial reaction. As discussed in Chapter 2, if a Service Failure is detected, then prepare the precaution reaction, but a Service Failure may always result in a hazardous situation. Therefore, forecasting is necessary.

The forecasting can be performed in the Home Gateway, as it gathers information about the indoor environment, e.g., indoor temperature, indoor humidity, and outdoor temperature around the house. And the raw data is used to generate elementary events. Then the forecasting is to generate semantic events. If something undesired is forecasted, look up or subscribe to the corresponding service in the local service DB. Therefore, the proposed CPS home safety architecture can be used to forecast the concerned safety problems.

4.4 Safety Problem Prevention

If a safety problem is detected or forecasted, corresponding services are needed for reactions. One way of prevention can be redundancy of services, e.g., redundancy of indoor temperature adjustment service. Because it can ensure the reliability of these services.

The reliability is defined as the continuity of correct service [25]. Reliability $R(t)$ of a system at time t is the probability that the system operates without a failure in the interval $[0, t]$, given that the system was performing correctly at time 0 [56]. Because a service relates to the controller and the Performers of the Performers System. There are two types of redundancy, controller redundancy, and Performer redundancy as illustrated in Figure 4.10. Controller redundancy is executed when Performer works well. It can either be reconfiguration or issue the same command to the same appliance by a spare controller. Performer redundancy is executed when the working Performer cannot perform its functions. It switches to an alternative Performer that provides the same function.

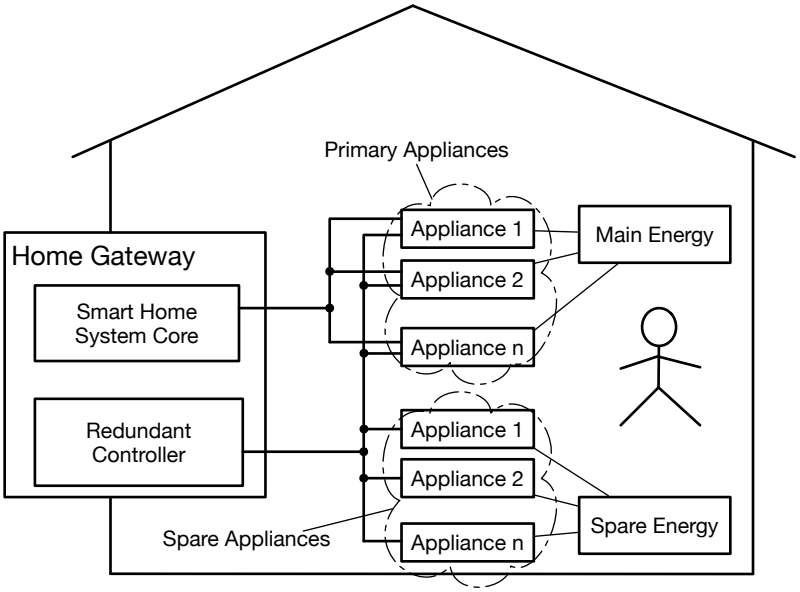


Figure 4.10: Different forms of redundancies.

The service redundancy model consists of four main parts: error detection, infection identification, error recovery, and redundancy management. The components and their connections of the proposed redundancy model are shown in Figure 4.11.

Error detection has three main functions:

1. It represents the context information based on home environment status and appliance working status;

2. Under context information to detect errors according to predefined rules;

3. It generates proper error events for further processing

This component provides a list of current working Performers from the redundancy management component. Then, error events are passed to the infection identification component.

The infection identification component identifies corrupted Performers based on the received error events and the list of working Performers. And it maps the errors to corresponding Performers and packs the mapping and related information. It receives error events from the error detection component and a list of current working Performers from the redundancy management component. After identification, it passes the processed information to the error recovery component.

For the error recovery component, it receives the processed information from the infection identification component, then queries the corresponding redundancy plan from the redundancy management component. Next, the redundancy plan is executed to issue commands to the spare Performers

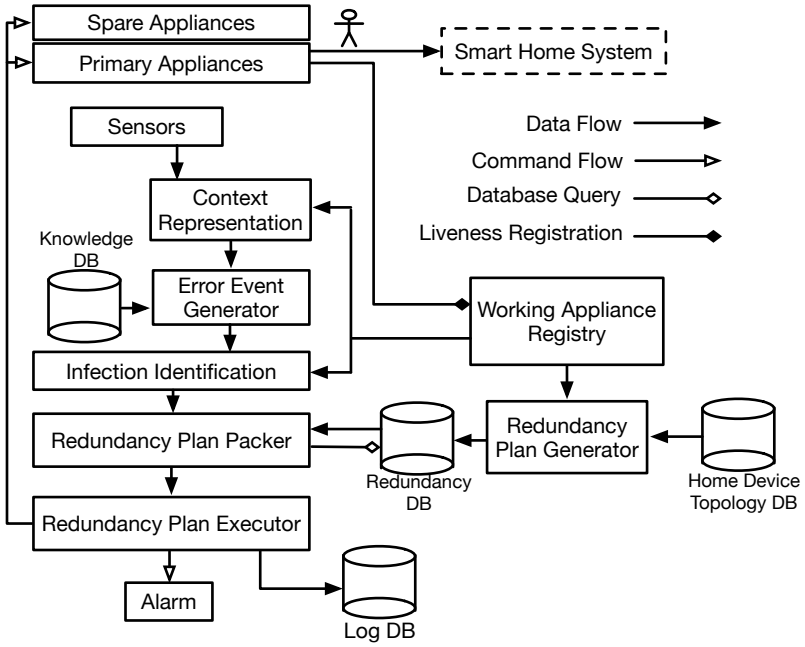


Figure 4.11: The components of the proposed redundancy model.

or reconfiguration to the working Performer. Or, it connects to proper devices, e.g., smartphones, or systems for warning. Last, it logs the corresponding events into a database.

The redundancy management component maintains a list of working Performers. Since each Performer will register itself to this component and update their working status. The redundancy plans are made based on the available resources (controllers, Performers, and energy sources), and are stored into a database for query by the error recovery component. These plans should be updated regularly. The redundancy management also provides a list of current working Performers to the error detection and the infection identification Component.

The important factor for redundancy is that the redundant component is independent of the primary component. The redundancy system is a completely different system from other systems in the Home Gateway. The working of the spare Performers and their energy supply should be independent of the primary Performers. Also, the reconfiguration commands and energy supplies should be independent to ensure reliability.

4.5 Conclusion

This chapter discussed the proposed CPS home safety architecture that supports event-based detection/prediction and service-based reaction for safety problems. We discussed the event-based method for safety problem detection/prediction in detail. The service-based method is left for future work. The event-based method includes a layered FSMs with raw data and events, i.e., elementary event, se-

mantic event, and overall event as inputs and outputs. Finally, we employed two simulation cases to verify the feasibility of the proposed architecture and the event-based detection/prediction approach. Last, safety problem forecasting and prevention are roughly discussed.

5
Safety Problem Detection

This chapter introduces the way to detect physical process anomalies, i.e., Service Failures and Hazards, as introduced in chapter 2. Conformance testing was adopted to check whether indoor temperature data conforms to requirements that are modeled by hybrid automata. If the conformance check failed, which indicates a Service Failure or Hazard has occurred. The detection approach can be implemented based on the CPS home safety architecture that was discussed in Chapter 4. I summarize the contributions of this chapter as follows [229, 230, 232]:

- An example of home appliances control was devised with the purpose to elicit the modeling of required variations of indoor temperature.
- Based on the control example, I adopted hybrid automata to model required variations of indoor temperature with considering thermal indices, heat transfers, and knowledge related to the health. The introduction of hybrid automata enabled the detection of thermal problems at different timepieces of test duration.
- A multiple-conformance approach has been proposed, which encompasses five conformance rules for detecting eight thermal problems. The multiple-conformance approach takes the hybrid-automata-modeled requirement as the specification. And its implementation is the temperature data.
- I checked the conformance of temperature data against the requirements that are modeled by hybrid automation and evaluated its performance by comparing it with the conventional approach.

List of Variables

C	Convective heat flow (W/m^2)
H	Relative humidity (%rh)
L	Thermal load of a human body
M	Metabolic rate (met)
R	Radiative heat flow (W/m^2)
T	Operative temperature or the required indoor temperature (°C)
Tol	Tolerance time
TPD	Time to increase or decrease 1 °C
V	Air velocity (m/s)
W	External work (w/m^2)
f_{cl}	Clothing area factor
h_c	Convective heat transfer coefficient
H_i	Humidity of indoors (%rh)
H_o	Humidity of outdoors (%rh)
h_r	Radiative heat transfer coefficient
I_{cl}	Clothing insulation (clo)
P_a	Water vapor pressure (Pa)
T_a	Air temperature (°C)
T_{cl}	Clothing surface temperature (°C)
T_g	Globe thermometer temperature (°C)
T_{ini}	Initial temperature (°C)
T_i	Operative temperature of indoors (°C)
T_i^t	Desired indoor temperature level (°C)
T_{or}	Radiant temperature of outdoors (°C)
T_o	Operative temperature of outdoors (°C)
T_{rd}	real data of indoor temperature (°C)
T_r	Mean radiant temperature (°C)
T_{sk}	Mean skin temperature (°C)
T_w	Natural wet-bulb temperature (°C)
V_i	Air velocity of indoors (m/s)

5.1 Introduction

Occupants stay indoors for most of their time [110]. The productivity and health of people are affected by the indoor environment [67, 68, 186]. Especially, health problems may occur due to abnormal changes in indoor temperature. For instance, it can result in heat illnesses or death to older people

in hot weather [218, 221]. It also has a negative effect on sleep and circadian rhythm which causes cardiac autonomic response during sleep in cold weathers [145, 156]. So, it needs to check the indoor temperature to detect thermal problems.

Conventionally, various thermal indices [1, 19, 37] were adopted to detect different thermal problems. From the point of view of engineering, they are not flexible in detecting multiple thermal problems by a single method that includes only one index. Moreover, it is also not flexible to deal with new thermal problems since new detection methods are needed to be designed. Thus, I propose a method for comprehensively checking the indoor temperature to detect thermal problems. Therefore, let us check whether indoor temperature conforms to the requirement of no thermal problems by conformance testing [10]. Conformance testing is to check the validity of implementation against its specification. More precisely, It checks whether outputs of specification and implementation are conformant with the same inputs [10, 142]. So, it is necessary to first design required variations of indoor temperature [229, 232]. Then, I extend upon a conventional conformance approach [10] to fulfill the needs.

Hybrid automata are used to model the required changes in indoor temperature. First, hybrid automata are to model systems with discrete and continuous components. Discrete states of systems can be modeled by discrete components of hybrid automata. And transitions between states are the discrete dynamics. Second, indoor temperature changes continuously, while different pieces of it correspond to discrete thermal sensations. Therefore, hybrid automata can be applied to model the required changes in indoor temperature.

As far as I know, this is the first try to adopt hybrid automata [82] to model required changes in indoor temperature. In literature, systems for temperature control are either narrowly considered thermal discomfort without heat or cold exposure [100], or are in the form of examples [82]. The contents of discrete components in these applications are the discrete control states, which are different from our case.

There are two problems to conquer in order to model by hybrid automata. First, it needs to split the changes in indoor temperature so that each piece can correspond to a distinct thermal sensation. To this end, let us split the indoor temperature by resorting to heat stress indices [37], the PMV-PPD index [19], and cold stress indices [1]. Each piece of temperature also corresponds a state of hybrid automata. Second, it needs to prescribe curves of the required changes in indoor temperature, which are derived from an indoor temperature adjustment example that will not cause thermal problems. In other words, the required changes in indoor temperature is derived from heat exchanges between indoor that is adjusted with considering the example and outdoor.

For the conformance check, let us extend the (τ, ε)-closeness method [10, 142]. The (τ, ε)-closeness method checks on the whole test duration to see if time lag and value difference are smaller than τ and ε, respectively. But, there are limitations to detect thermal problems at a time interval of test duration. For example, unbearable hot can only occur when the temperature is high. Moreover, temperature data satisfies its requirements with respect to the (τ, ε)-closeness when values of τ and ε are properly given. There are some thermal problems cannot be detected, e.g., undesired temperature fluctuation. Second, the (τ, ε)-closeness method rejects some situations that accepted by our cases. For instance, in the situation that indoor temperature is required to reach the preset level quickly. So, the time

lag between temperature data and its requirement may be greater than τ. Therefore, I substitutes the (τ, ε)-closeness with multiple conformance relations to detect thermal problems at different time intervals of test duration. This inspired us to propose the multiple-conformance approach [230, 232].

To model the required changes in indoor temperature by hybrid automata, which guarantees the detection at various time intervals of test duration. This is possible since the test duration can be divided by considering discrete transitions between states. Every state of hybrid automata handles the concerned thermal problems by devising corresponding conformance relations. Generally, the conformance relations are different from the (τ, ε)-closeness method. Section 5.2.2 discusses the conformance problems so as to design the conformance rules.

I checked temperature data that were collected from a testbed smart house against the hybrid-automata-modeled requirement with considering the proposed multiple-conformance approach. I used Matlab to conduct the experiment. The experimental results illustrate that thermal problems can be comprehensively detected at different time intervals of test duration. This demonstrates the capability of hybrid automata in modeling the required changes in indoor temperature, and the reasonableness of the proposed multiple-conformance approach. I also applied confusion matrix and its related terms to evaluate our proposal, which the results demonstrate a better performance of the proposal than the (τ, ε)-closeness approach.

5.1.1 Indoor Climate Monitoring

The indoor climate is a collective designation of the environmental factors, e.g., temperature, humidity, heat, light, noise, smoke and particles, and chemicals that can affect occupants. Researches related to indoor climate monitoring refer to observing and predicting indoor climate anomalies to select appropriate reactions to maintain good performance of indoor climate adjustment. This chapter focuses on the observation of temperature changes in the smart home environment to detect thermal problems.

Smart home systems that for indoor environment adjustment usually is based on the observation of the environment. [184] proposed a system which can observe indoor climate properties, e.g., temperature dynamically. [176] presented a domotic framework which is to enhance the interaction among human beings, smart devices, and environments based on a sensing and actuator network.

Commonly, indoor temperature adjustment only for thermal comfort. A field study in naturally ventilated office buildings to evaluate thermal comfort by the subjective judgment of occupants [168]. Traditional on/off controllers are to adjust the indoor temperature to the preset level. Roberto2008 took advantage of PMV-index [19] to adjust the indoor temperature to pursue accurate adjustment. It calculates PMV-index with respect to physical and personal factors. One can understand this as temperature adjustment based on a dynamic preset level. Some other work also considered energy saving during the adjustment, e.g, [41] adopted linguistic variables of fuzzy logic to represent temperature intervals that correspond to distinct thermal sensations to help in adjusting the indoor temperature. It is claimed they can save energy up to 40%.

5.1.2 Hybrid Automata

Hybrid automation is taken as a model and specification language for hybrid systems. For each state of the hybrid automation, its behaviors are governed by a set of differential equations. It can be taken as a generalized finite-state machine for modeling hybrid systems. Hybrid systems are dynamical with continuous and discrete behaviors, i.e., flows are represented by differential equations, and jumps are described by state machines. The formal definition of it is presented in Definition 13, which is referenced from Henzinger's work [82].

Definition 13 (Hybrid Automata)**.** *A hybrid automation HA includes the five components:*

- ***Variables***
  - *A finite set* $X = \{x_1, \cdots, x_n\}$ *of real-numbered variables,* n *is the dimension of HA*
  - $\dot{X} = \{\dot{x}_1, \cdots, \dot{x}_n\}$ *represents first derivatives during continuous change*
  - $X' = \{x_1', \cdots, x_n'\}$ *represents values at the conclusion of discrete change*
- ***Control graph***
  - *A finite directed multigraph* (V, E)*, where* V *and* E *are called* control modes *and* control switches *respectively*
- ***Vertex labeling functions***
  - *Initial(*init*), invariant(*inv*) and flow conditions(*flow*) are functions that assign a predicate to each control mode* $v \in V$
  - *The free variables of* $init(v)$*,* $inv(v)$ *and* $flow(v)$ *are from* X*,* X *and* $X \cup \dot{X}$ *respectively*
- ***Jump conditions***
  - *An edge labeling function* jump *assigns a predicate to each control switch* $e \in E$
  - *Each jump condition* $jump(e)$ *is a predicate whose free variables are from* $X \cup X'$
- ***Events***
  - *A finite set* Σ *of events, and an edge labeling function event:* $E \to \Sigma$ *that assigns each control switch an event.*

Hybrid automata are adopted to model systems that have continuous and discrete components. Different operating modes of nonlinear hybrid systems are modeled by hybrid automata [26]. For example, a liquid heating system with discretely controlled valves and the continuous changing liquid level. [180] presented to model compression systems with continuous dynamics of physical processes, e.g. mass flow, and the discrete dynamics of control functions. Some work related to hybrid automata verification. For example, [207] proposed an algorithm to verify of hybrid systems. [59] presented to link the specification of supervisory controllers to the verification of embedded systems with hybrid dynamics.

5.1.3 Conformance Testing

Conformance testing is to check if the properties satisfied an implementation is equivalent to that by the specification [10]. It has many applications. For example, model reduction [41, 135, 177], model elicitation, and implementation equivalence with its specification [10, 142]. Practically, it checks the closeness or equivalence of output trajectories of two models.

The closeness check has different content for different kinds of systems. For systems that are modeled by timed automata [36, 83], the only time in trajectories is considered. Timed automata are the extension of finite-state automata with real-valued variables that measure delays between actions. [83] proposed quantitative similarity functions that measure the closeness of two timed transition systems as a real. [36] presented a construction that enables the implementation of timed automata. Two timed automata modeled systems are close if the timings of events of their traces have the same sequence. Values in trajectory closeness are considered for some hybrid automata. For example, [135, 177] proposed for model reduction of hybrid systems. The closeness checks the value differences at any time point in trajectories. For cyber-physical systems (CPS) that modeled by hybrid automata [10, 142], the closeness checks both time and value in trajectories. [10] presented to check the closeness in time and value for CPS systems. Then, [142] proposed a process for sound conformance testing based on the proposal of [10].

5.2 Safety Problem Detection

This section introduces the details of the detection of Service Failures and Hazards. The modeling of the required changes in indoor temperature is going to be introduced first, then come with the discussion of conformance problems. Thereafter, let us discuss the multiple-conformance approach, then an experiment will be conducted to verify the reasonableness of the proposed multi-conformance approach and the hybrid-automata-modeled requirement. Finally, a performance evaluation of the proposal also to be conducted by adopting the confusion matrix and its related terms.

5.2.1 Modeling the Requirement

Let us assume indoor temperature adjustment takes advantage of a window, an air-conditioner, and a curtain for thermal comfort and without resulting in thermal discomfort.

Indoor Temperature and Thermal Sensation

The indoor temperature here denotes operative temperature that is the uniform temperature of an imaginary black enclosure in which people would exchange the same amount of heat by radiation and convection as in the actual nonuniform environment [19]. One can derive the operative temperature from air temperature and radiant temperature with Formula 5.1 [19]. $V > 1.0$ is not considered due to it is usually bellow 0.3 m/s for over 85% of the measurements [27].

$$T = \begin{cases} 0.5T_a + 0.5T_r, V < 0.2 \\ 0.6T_a + 0.4T_r, 0.2 \leq V < 0.6 \\ 0.7T_a + 0.3T_r, 0.6 < V \leq 1.0 \end{cases} \tag{5.1}$$

Value-added integrated services are provided by home appliances that connect to the home networks [43, 148]. Indoor temperature adjustment service is an example of the integrated service, which is for thermal comfort with energy-saving. This causes a mixed way of adjustment, e.g., it can use the air-conditioner, window, curtain, or any combination of them. Moreover, if one makes use of the outdoor climate or air-conditioner to adjust a not well-insulated room, it may cause unpleasant thermal sensation due to abnormal changes in temperature. For instance, undesired temperature fluctuation [29, 115] brings about uncomfortableness and constantly being cooler or warmer than expected as a result of temperature stabilized at a level that deviated far from expectation. Also, one exposure to undesirable temperatures longer than a tolerable time [1, 237], or to severe temperature levels may cause health problems. The tolerance time is the maximum tolerable exposure time the body keep heating or cooling under the conditions of cold or heat exposure.

Let us divide the indoor temperature into five situations by considering thermal sensations. Neutral denotes indoor temperature causes a pleasant thermal sensation. Hot means high indoor temperature results in heat exposure, while Cold means low indoor temperature leads to cold exposure. Warm represents relatively high indoor temperature, while Cool represents relatively low indoor temperature. But both will not result in health problems.

Let us consider thermal problems that could happen in each situation are shown in Table 5.1. Indoor temperature is usually set to a level Neutral for thermal comfort. Undesired temperature fluctuation or the temperature is *Just-Noticeable Difference* [115] deviated from the preset level will lead to uncomfortable. It will cause undesired duration if the exposure time is longer than the tolerance time for situations of Cool and Warm. Very low or very high temperatures or they last longer than expected will cause health problems. Very low or very high is when the indoor temperature is lower or higher than the requirement. Also, the thermal problems in Table 5.1 correspond to the Service Failure and Hazard that discussed in Chapter 2.

Indoor Temperature and Energy Conservation

There are some assumptions to discuss energy conservation for indoor temperature adjustment. First, there is a target temperature level within the Neutral situation for thermal comfort. Second, the indoor

Table 5.1: Thermal problems correspond to the situations.

Situation	Thermal Problem	Service Failure or Hazard
Cold	Unbearable cold or undesired duration	*Hazard*
Cool	Undesired duration	*Service Failure*
Neutral	Undesired fluctuation or constantly cooler/warmer than expectation	
Warm	Undesired duration	
Hot	Unbearable hot or undesired duration	*Hazard*

temperature should be adjusted to the target preset level less than the tolerable time. Third, the indoor temperature adjustment service should make full use of the outdoor climate.

Indoor temperature adjustment service chooses home appliance(s) to work spend the least energy consumption. For instance, the highest priority is to open a curtain and window to use the outdoor climate for indoor temperature adjustment. Then, the medium priority is to turn on the Fan mode of the air-conditioner (compressor does not work). The least priority is to choose the Heat/Cool mode of the air-conditioner (compressor works).

An Example of Indoor Temperature Adjustment Service

Let us assume the considered home appliances have working states, as shown in Table 5.2. Heat exchange through walls, opening/closing doors, and window gaps are heat noise sources.

The working states of concerned home appliances are affected by environmental factors, as illustrated in Table 5.3. This depends on the functions home appliances can provide. For example, the indoor temperature is the factor that can affect the working of an air-conditioner. The reason is that the Cool mode of air-conditioner works when the indoor temperature is high, and the Heat mode of air-conditioner works when the indoor temperature is low. Empirically, the curtain has two functions, i.e., introducing radiant heat, as stated in Table 5.2 and illumination. Illumination depends on indoor activities of occupants and has nothing to do with indoor temperature adjustment. So, illumination in the control scenario introduced in this chapter is not considered. But the indoor temperature adjustment service has a higher priority here if a conflict has occurred when using these two functions. Auxiliary ways to resolve this conflict are recommended. For instance, if introducing radiant heat is needed while illumination is not needed, an eye mask is recommended for occupants who may sleep. And if people want to close the curtain to prevent introducing radiant while illumination is needed, illumination devices like light bulbs are recommended.

Let us consider three outdoor climate situations, i.e., *hot*, *neutral*, and *cold*. For the *hot* situation, people do not use the Heat mode of the air-conditioner. The window is closed to insulate the indoor against the outdoor when outdoor humidity and/or air temperature is high. So, the window and curtain need to be closed to use the Dry mode of the air-conditioner. For the *neutral* situation, people

Table 5.2: Working states of home appliances.

Home Appliance	**Working State**	**Note**
Air-conditioner	Cool	Adjust temperature and fan speed to cool the room; it corresponds to the Cool mode or cooling phase of Auto mode
	Heat	Adjust temperature and fan speed to warm the room; it corresponds to the Heat mode or heating phase of Auto mode
	Dry	Gently cooling while dehumidifying the room (by removing moisture from indoor air)
	Fan	Ventilate the room; it is helpful to refresh the stale air in the room
	OFF	The air-conditioner is turned off
Window	Open	Adjust the indoor temperature by introducing cool but not humid air; it can be fully open or half open but not close
	Close	A fully closed status
Curtain	Open	Adjust the indoor temperature by introducing radiant heat; it can be fully open or half open but not close
	Close	A fully closed status

Table 5.3: Factors that affect the appliance working states.

Home Appliance / **Factors**	Air-conditioner	Window	Curtain
Indoor temperature	✓	✓	✓
Indoor humidity	✓		
Indoor air velocity	✓		
Outdoor temperature	✓	✓	
Outdoor humidity		✓	
Outdoor air velocity	✓	✓	
Outdoor radiant temperature			✓

choose dehumidify rather than temperature adjustment due to high humidity and temperature greatly affect thermal sensations. Thus, people usually use the window and curtain to save energy consumption. For the *cold* situation, people use the Heat mode of air-conditioner and curtain quite often. The window should be closed. Usually, people use desiccant and not the Dry mode of the air-conditioner when indoor humidity is high. Since the Dry mode of air-conditioner has a cooling effect. Our adjustment example that is modeled by automata is shown in Figure 5.1. Table 5.4 explains the states. The transitions between states depend on the values of climate properties, e.g., temperature.

T_i^l denotes the desired level of indoor temperature, which can be prescribed manually or the indoor temperature adjustment service. $[TC_l, TC_h]$ means the temperature interval that brings about thermal

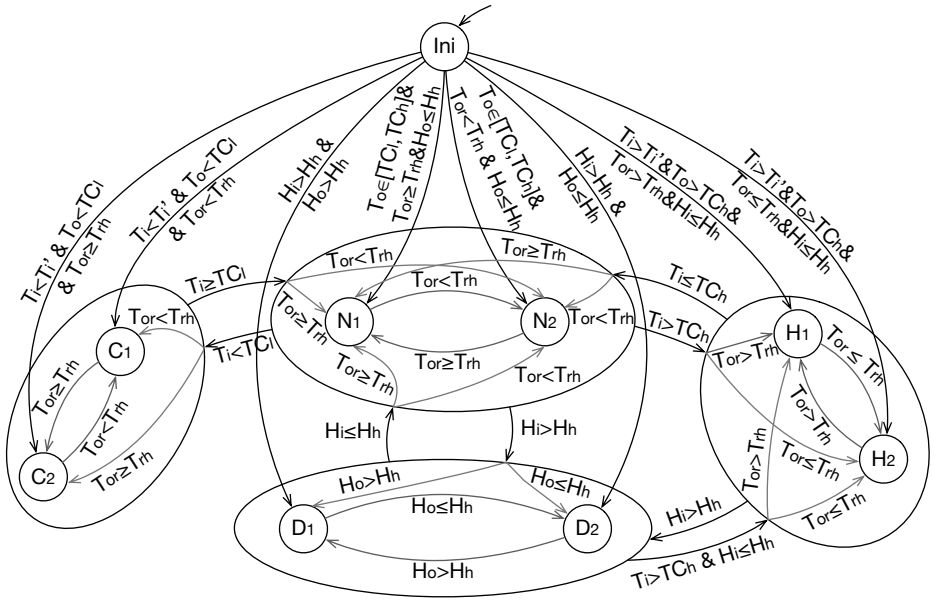


Figure 5.1: Automata of the indoor temperature adjustment example.

Table 5.4: State explanations.

State Name	State Description
Ini	Air-conditioner(*OFF*); Window(*Close*); Curtain(*Close*)
C_1	Air-conditioner(*Heat*); Window(*Close*); Curtain(*Close*)
C_2	Air-conditioner(*Heat*); Window(*Close*); Curtain(*Open*)
H_1	Air-conditioner(*Cool*); Window(*Close*); Curtain(*Close*)
H_2	Air-conditioner(*Cool*); Window(*Close*); Curtain(*Open*)
N_1	Air-conditioner(*OFF*); Window(*Open*); Curtain(*Open*)
N_2	Air-conditioner(*OFF*); Window(*Open*); Curtain(*Close*)
D_1	Air-conditioner(*Dry*); Window(*Close*); Curtain(*Close*)
D_2	Air-conditioner(*Fan*); Window(*Open*); Curtain(*Open*)
(C_1,C_2)	A combination of states C_1 and C_2 for heating the room
(H_1,H_2)	A combination of states H_1 and H_2 for cooling the room
(N_1,N_2)	A combination of states N_1 and N_2 for utilizing outdoor climate
(D_1,D_2)	A combination of states D_1 and D_2 for dehumidifying the room

comfort. The detail is illustrated in Table 5.5. If the indoor temperature is greater than TC_h, one needs to cool the room down. If the indoor temperature is smaller than TC_l, one need to warm the room up. $[H_l, H_h]$ represents an interval for neutral humidity. If the humidity is greater than H_h, one need dehumidification. If the humidity is lower than H_l, one need humidification. $[T_{rl}, T_{rh}]$ represents

the interval for outdoor neutral radiant temperature. Sufficient solar radiation is when the outdoor radiant temperature is greater than T_{rh}, or insufficient solar radiation when it is smaller than T_{rl}.

Table 5.5: Thermal effects of various temperature intervals.

Temperature Interval	**Thermal Effects**
$[HT, +\infty)$	It has a high possibility to cause health problems due to heat exposure.
$[WM_l, WM_h]$	It will cause unpleasant thermal sensation with no health problems and $WM_h = HT$.
$[TC_l, TC_h]$	Pleasant thermal sensation and $TC_h = WM_l$.
$[CL_l, CL_h]$	It will cause unpleasant thermal sensation with no health problems and $CL_h = TC_l$.
$(-\infty, CD]$	It has a high possibility to cause health problems due to cold exposure and $CD = CL_l$.

For transitions between composite state except (D_1,D_2), the radiant temperature is the key parameter to determine which component state to transit to. For example, it transits to C_2 of (C_1,C_2) from (N_1,N_2) when the radiant temperature is greater than T_{rh}. Since sufficient radiant heat has been introduced so that one can open the curtain. Or, it goes to C_1. This is because of insufficient radiation and hoping to save energy. It goes to D_2 of (D_1,D_2) when outdoor humidity is smaller than H_h. Or, it will go to D_1 of (D_1,D_2). The reasons behind this are twofold. The first is to save energy. Because the Fan mode of air-conditioner consumes less energy than the Dry mode. The second is that outdoor humidity is low. So, one can open the window.

The Requirements

The required changes in indoor temperature come from the adjustment example to assist in detecting the problems, as illustrated in Table 5.1. The adjustment example depends on the weather conditions to control various home appliances. For consistency, the states of the required changes in indoor temperature come from considering the corresponding weather conditions. The control actions of home appliances in the adjustment example can be taken as events in designing hybrid automation. By knowing the control actions, it is further can be used in reacting to detected thermal problems. More importantly, the curves of the required changes in indoor temperature are derived from the heat exchanges between indoors that adjusted by working home appliances and outdoors. The required changes in indoor temperature are modeled by hybrid automation, which is to simulate temperature changes in a house. Let us use the definition of hybrid automata that introduced in Section 5.1.2.

The modeling of the required changes in indoor temperature by hybrid automation, as illustrated in Figure 5.2. The states comes from the situations, as discussed in Section 5.2.1 with the initial state *Ini*. The modeling is by using hybrid automata, which ensures the detection at different time intervals of test duration. Assume that no arrows from Neutral to Cool (Warm), then to Cold (Hot) to prevent unacceptable transition loops. This has some reasons. First, the required changes in indoor temperature are taken as the specification in the conformance check. Second, if the transitions go to the reverse

directions, it may due to either indoor temperature adjustment service failure, or no need for the indoor temperature adjustment service and thus indoor temperature reversely transits autonomously through heat exchange. The former case is apparently cannot be prescribed as the requirement. The latter case maybe because of no people in the room, and thus there is no need to consider this situation. T_i belongs to an interval is the invariant condition and $T_i \in X$. For example, indoor temperature belongs to that, as illustrated in Table 5.5. The flow condition $\dot{T}_i = \mathit{flow}()$ means the rate of change of the required changes in indoor temperature and $\dot{T}_i \in \dot{X}$. Different states of hybrid automation have different content. The event set Σ includes control actions of working home appliances from the control example, as discussed in Section 5.2.1. For example, one can label the event *turn on the Cool mode of air-conditioner* to the edge between Hot and Warm. The events are taken as output events, e.g., the event *turn on the Cool mode of air-conditioner* occurs when transit to Warm from Hot. The events are implicitly depicted in Figure 5.2 due to the indoor temperature adjustment service selects appropriate home appliances to work based on the automation introduced in the last section. The desired temperature level $T_i^{'}$ satisfies $T_i^{'} \in X^{'}$. It can be manually set.

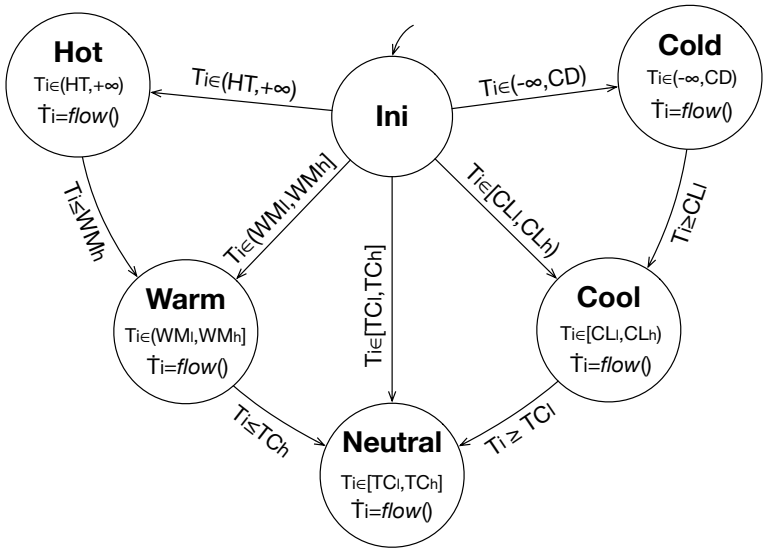


Figure 5.2: Hybrid-automata-represented requirement.

Invariant conditions can be derived from cold stress indices [1], PMV-PPD index [19], and heat stress indices [37]. They are proved techniques to evaluate thermal sensations and have a complex relationship with personal and environmental factors. By fixing personal factors and environmental factors other than the temperature, one can derive the intervals of invariant conditions.

Use PMV-PPD Index to Calculate $[TC_l, TC_h]$

PMV [19] means the predicted mean vote, which is an index that predicts the mean value of the votes of a large crowd on the thermal sensation scale shown in Table 5.6. It has relations with environmental factors, e.g., air/radiant temperature, wind speed, and humidity, and personal factors, e.g., metabolic rate and clothing insulation. PPD [19] denotes the predicted percentage of dissatisfied, which is also an index that quantitively predicts the percentage of people who feel thermal discomfort. It derives from PMV. One specifies other factors other than the temperature to determine the boundaries of $[TC_l, TC_h]$. One can calculate PMV and PPD through Formulas 5.2 and 5.6.

$$PMV = (0.028 + 0.303e^{-2.0934M}) \times L \tag{5.2}$$

where,

$$\begin{aligned} L = {} & M - W - 3.05 \times 10^{-3}[5733 - 6.99(M - W) - Pa] \\ & -0.42(M - W - 58.15) - 1.7 \times 10^{-5} M(5867 - Pa) \\ & -1.4 \times 10^{-3} M(34 - T_a) - f_{cl} h_c (T_{cl} - T_a) \\ & -3.96 \times 10^{-8} f_{cl}[(T_{cl} + 273)^4 - (T_r + 273)^4] \end{aligned} \tag{5.3}$$

$$f_{cl} = \begin{cases} 1 + 0.2I_{cl}, I_{cl} \leq 0.5 \\ 1.05 + 99.975I_{cl}, I_{cl} > 0.5 \end{cases} \tag{5.4}$$

$$h_c = min(2.38(T_{cl} - T_a)^{0.25}, 12.1\sqrt{V}) \tag{5.5}$$

Table 5.6: ASHRAE thermal sensation scale.

+3	hot
+2	warm
+1	slightly warm
0	neutral
-1	slightly cool
-2	cool
-3	cold

$$PPD = 100 - 95e^{-(0.03353PMV^4 + 0.2179PMV^2)} \tag{5.6}$$

[19] recommended that $-0.5 < PMV < 0.5$ and $PPD < 10$ for general comfort. For example, Indoor temperature interval for thermal comfort is $[25, 27.73]$°C with $V_i = 0.15, I_{cl} = 0.5, H_i = 45$, and $M = 1$ by using the tool [209].

Use Heat Stress Indices to Calculate $[HT, +\infty)$

Heat stress is that people are exposed to the net heat load contributed from metabolic heat, clothing, and environmental factors, which causes increased heat storage in the body [37]. One of the widely used indices is wet bulb globe temperature (WBGT) in $^{\circ}C$ to assess heat stress. One can calculate the WBGT of indoors from Formula 5.7.

$$WBGT = 0.7T_w + 0.3T_g \tag{5.7}$$

where,

$$\begin{aligned} T_w =& T_a \arctan\left[0.151977(H + 8.313659)^{0.5}\right] \\ &+ \arctan\left(T_a + H\right) - \arctan\left(H - 1.676331\right) \\ &+ 3.91838 \times 10^{-3} H^{1.5} \arctan\left(2.3101 \times 10^{-2} H\right) - 4.686035 \end{aligned}$$

from [189] and T_g can be derived from

$$\begin{aligned} &13.46V^{0.6}T_g + 5.3865 \times 10^{-8}(T_g + 273.15)^4 \\ =&13.46V^{0.6}T_a + 5.3865 \times 10^{-8}(T_r + 273.15)^4 \end{aligned}$$

from [107].

By substituting T_w and T_g into Formula 5.7, WBGT can be represented as a function of variables T_a and T_r. Then $WBGT = g(T_a, T_r)$.

The NIOSH [37] recommended heat stress alert limits for unacclimatized people, which this recommendation is the Recommended Alert Limit (RAL), and is derived from Formula 5.8. More specifically, the combinations of environmental and metabolic heat should be smaller than the RALs.

$$RAL = 59.9 - 14.1 \log_{10}(58.15M) \tag{5.8}$$

where RAL is the recommend WBGT in $^{\circ}C$. Thus, one can calculate the boundaries of $[HT, +\infty)$ under the condition when the WBGT values are smaller than RAL under specific conditions.

If Formula 5.1 is represented as $T = h(T_a, T_r)$, we have $WM = \{max\{h(T_a, T_r)\} | g(T_a, T_r) < RAL\}$. The reasons to take the maximum value of $h(T_a, T_r)$ have twofold. First, WM satisfies $WBGT < RAL$. Second, WM is the boundary between state Hot and Warm of the hybrid automation. If choose the minimum value of $h(T_a, T_r)$, these exist values even greater than WM still do not have a high possibility to cause heat illnesses.

Use Cold Stress Indices to Calculate $(-\infty, CD]$

Cold stress 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 and sometimes heat debt [1]. IREQ [1] is one of the cold stress indices that represent the required clothing insulation for preserving body heat balance at defined levels of physiological strain. It can be used to measure the cold stress with the effects of air temperature, relative humidity, air velocity, and mean radiant temperature for defined levels of metabolic rate. This index is to derive the required clothing insulation under a specific condition.

Formula 5.9 shows the way of calculating the IREQ. There is an increased risk of hypothermia if inadequate insulation of clothing ensemble is provided that causes progressive exposure. If clothing ensemble, i.e., IREQ is known, then the temperature boundary CD of $(-\infty, CD]$ can be calculated when other environmental factors and personal factors are fixed.

$$IREQ = \frac{T_{sk} - T_{cl}}{R + C} \tag{5.9}$$

where $R = f_{cl} \cdot h_r \cdot (T_{cl} - T_r)$ and $C = f_{cl} \cdot h_c \cdot (T_{cl} - T_a)$.

After substituting R and C into Formua 5.9, IREQ can be written as a function of variables T_a and T_r, i.e., $IREQ = p(T_a, T_r)$. I use the notation of T that was used in the previous subsection, i.e., $T = h(T_a, T_r)$. Thus, CD can be derived by $CD = \{min\{h(T_a, T_r)\} | IREQ = p(T_a, T_r)\}$. There are two reasons for choosing the minimum value of $h(T_a, T_r)$. First, CD has to satisfy $IREQ = p(T_a, T_r)$. Second, CD is the boundary of state Cool and Cold of the hybrid automation. If choose the maximum value of $h(T_a, T_r)$, there exist values even smaller than CD still do not have a high possibility to cause illnesses relate to cold exposure.

Flow Conditions

With the expectation of detecting undesired duration, except the Neutral state, flow conditions derive from to achieve the desired level less than a prescribed time that is smaller than the tolerance time [1, 237]. This is due to the indoor temperature adjustment service need sufficient time to adjust the indoor temperature to a safe level. The prescribed time can be calculated concerning working home appliances and unwanted heat noises. The required indoor temperature changes monotonously and should not cause thermal problems, as shown in Table 5.1. Thus, flow conditions in Formula 5.10 are defined as proportional to the time.

$$\dot{T}_i = flow() = {}^{\partial T}/_{\partial t} = 2at \tag{5.10}$$

where t means time and a represents the coefficient. Next, Let us discuss the way to determine a.

Assume requirement changes in indoor temperature follow $T_i(t) = T_{ini} + at^2$. It is required to achieve the desired temperature level $T_i^{'}$ in t_r time unit. Then we have $T_i(t) = T_{ini} + at_r^2 = T_i^{'}$, and after transformation we have $t_r = \sqrt{|{}^{(T_i^{'} - T_{ini})}/_{a}|}$. With considering working home appliance and heat noises, the average time to increase or decrease 1°C is assumed to be TPD time unit (TPD is short for Time Per Degree). Therefore, we have $t_r = |T_i^{'} - T_{ini}| \times TPD$. Then we get $t_r = \sqrt{|{}^{(T_i^{'} - T_{ini})}/_{a}|} = |T_i^{'} - T_{ini}| \times TPD$. After transformation, we finally get $a = {}^{\pm 1}/_{|T_i^{'} - T_{ini}| \times TPD^2}$.

For a room, *TPD* is the time working home appliances to dissipate or introduce the amount of heat to decrease or increase by 1°C. We can derived it from Formula 5.11.

$$TPD = \frac{Q_r}{Q_p - Q_n} = \frac{\rho v c}{W \times COP - \partial(Q_{win} + Q_{wall})/\partial t} \tag{5.11}$$

where the explanations of the parameters are as follows:

- $Q_r(J)$ is the sensible heat [190] that required to decrease or increase by 1°C for a fully insulated room, and $Q_r = \rho v c \Delta T$, where
  - ρ: air density (kg/m^3)
  - v: air volume of a room (m^3)
  - c: specific heat capacity of air ($J/(kg°C)$)
  - ΔT: temperature difference (°C) and is 1 here
- $Q_p(J/s)$ means the heat producing rate of an appliance, e.g., an air-conditioning unit. We can derive it from $Q_p = W_h \times COP$ with
  - *COP* represents the coefficient of performance. The *COP* of a home appliance is the ratio of cooling or heating provided to work required [220]
  - $W_h(J/s)$ is the work consumed by a home appliance
- $Q_n(J/s)$ denotes the heat of noises that can be derived from the thermal model in [152]. For example, by considering the heat noises from walls and a window, we get $Q_n = \partial(Q_{win} + Q_{wall})/\partial t$, where
  - Q_{win} represents the heat exchange through window at time t and $Q_{win}(t) = C_{heat} \cdot A_{win} \cdot T_{diff}(t)$, where C_{heat} is the heat transmission coefficient, A_{win} means the area of the window, and $T_{diff}(t)$ means the temperature difference between outdoor and indoor at time t.
  - Q_{wall} represents the heat exchange through walls and

    $$Q_{wall} = A_{wall} \cdot (\sum_{j=0} Y_j T_o(t - j\delta_T) - \sum_{j=0} Z_j T_i(t - j\delta_T))$$

    where A_{wall} means the surface area of walls; Y_j and Z_j are response factors; $T_o(t - j\delta_T)$ and $T_i(t - j\delta_T)$ are surface temperatures of the wall at time $t - j\delta_T$; δ_T is time interval.

Thus, the flow condition shown in Formula 5.10 is transformed into Formula 5.12 (positive when $T_{ini} < T_i'$, negative otherwise).

$$\dot{T}_i = \frac{\pm 2t}{|T_i' - T_{ini}| \times (\frac{\rho v c}{W \times COP - \partial(Q_{win} + Q_{wall})/\partial t})^2} \tag{5.12}$$

For the detection of undesired fluctuation and constantly being cooler or warmer than expected at the Neutral state, required changes in indoor temperature should be stable at the desired temperature level. Thus, the flow condition for the Neutral state uses a negative exponential function. So,

$$\dot{T}_i = \pm 2|T_{ini} - T_i'|t_1^2 t^{-3}$$

where t_1 denotes the first non-zero time stamp to sample data, and positive when $T_{ini} > T_i'$, negative otherwise. It can be calculated to get $\dot{T}_i$ by Formulas 5.13 to 5.16. Formula 5.13 means temperature change at the *Neutral* state; Formula 5.14 is for the calculation of the initial temperature based on Formula 5.13; then one can get the coefficient c by transforming Formula 5.14 into Formula 5.15. After substituting c into Formula 5.13 and derivative for time, we have $\dot{T}_i$ as shown in Formula 5.16.

$$T_i = \frac{c}{t^2} + T_i' \tag{5.13}$$

$$\frac{c}{t_1^2} + T_i' = T_{ini} \tag{5.14}$$

$$c = (T_{ini} - T_i') \times t_1^2 \tag{5.15}$$

$$\dot{T}_i = {}^{\partial T_i}/_{\partial t} = \pm 2|T_{ini} - T_i'|t_1^2 t^{-3} \tag{5.16}$$

For demonstration, consider the case where temperature intervals illustrated in Table 5.5 are instantiated by the first row of Table 5.7, then the second row when conditions changed after some time, e.g., the metabolic rate changed due to occupant's activity, which results in thermal discomfort to the temperature used to be comforting. They are used by invariant conditions of the hybrid automation. As occupants in Cold and Hot states are easier to cause health problems than in Cool and Warm states, so it requires that temperature changes are faster to reach a safe level in Cold and Hot states than in Cool and Warm. Also by considering the discussion in this subsection, I choose $|a| = 8$ for states Hot and Cold, and $|a| = 4$ for states Warm and Cool for demonstration. Then feed the initial temperature of 0°C to the hybrid automation. The output of the hybrid automation that represents the required changes in indoor temperature and the corresponding states are illustrated in Figure 5.3.

Table 5.7: Examples of temperature intervals.

Cold	**Cool**	**Neutral**	**Warm**	**Hot**
$(-\infty, 10]$	$[10, 20]$	$[20, 30]$	$[30, 40]$	$[40, +\infty]$
$(-\infty, 0)$	$[0, 10]$	$[10, 20]$	$[20, 30]$	$[30, +\infty]$

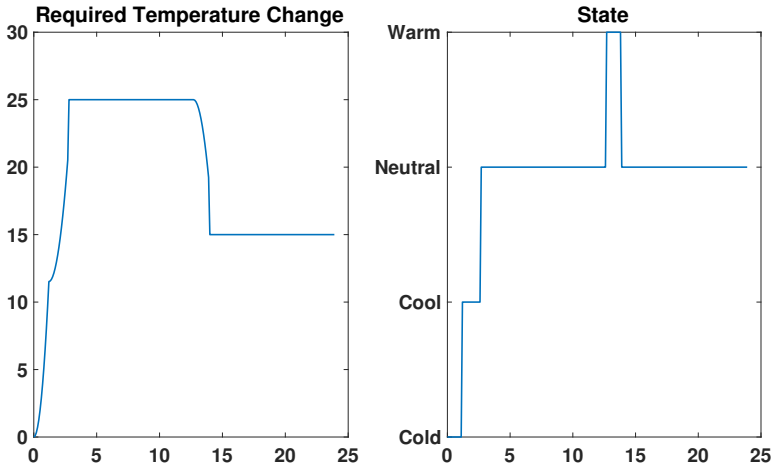


Figure 5.3: Requirement of temperature change and its corresponding states.

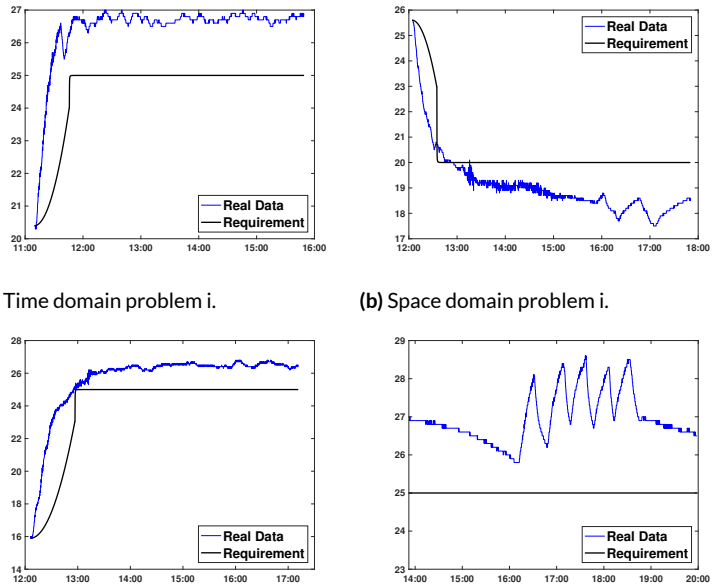
5.2.2 Conformance Problems

Given two output trajectories y_1 (specification) and y_2 (implementation) of two hybrid automata, the (τ, ε)-closeness [10] defines the conformance of y_1 and y_2 in time and space domain. If, at any time in the test duration, the value difference between y_1 and y_2 is smaller than ε, the time-lag is smaller than τ. Then, it says y_1 and y_2 are (τ, ε)-closeness. Let us also discuss the conformance between temperature data and its requirements in space and time domains. However, our discussion has two differences. First, I split the test duration into different intervals. Every conformance problem is discussed in one of the time intervals. Second, all conformance problems are discussed in this section cannot be directly solved by the (τ, ε)-closeness approach. The notations of τ and ε are used in this section to compare with the (τ, ε)-closeness method. They will be revised when introducing the proposed multiple-conformance approach.

Time Domain

(i) People can tolerate unpleasant thermal sensations for a limited time period [1, 237] (say t time unit). Assume a variable d is to represent the duration when indoor temperature results in unpleasant thermal sensations. Thus d satisfies $d \leq t$. If d is assigned a value t_0 as the requirement, which represents the indoor temperature has to be adjusted to the preset level for thermal comfort in at most t_0 time unit. Then, let us define τ as $t - t_0$. Generally, it is expected that the smaller the value of d, the more favorite it will be to occupants. Therefore, it is possible that $t_0 - d \geq \tau$, which is accepted by our conformance requirement but rejected by the (τ, ε)-closeness approach.

- For temperature data and its requirements in Figure 5.4a, it is expected that the tem-



(a) Time domain problem i.

(b) Space domain problem i.

(c) Space domain problem ii.

(d) Space domain problem iii.

Figure 5.4: Real data for demonstrating the problems.

perature to reach the desired temperature level ($25°C$) in at most about 33 min ($t_0 = 33\ min$). Temperature data reached the desired level in 13 min ($d = 13\ min$). If $\tau = 5$, we got $t_0 - d = 33 - 13 = 20 > \tau$.

Space Domain

Assume temperature data and its requirements are represented by T_{rd} and T, respectively. In our case, problems in space domain are not just about the value difference between temperature data and its requirements, but a tailored value difference and the temperature fluctuations. Problem (i) and (ii) related to relaxing the lower and higher bounds of (τ, ε)-closeness metric. In (τ, ε)-closeness, the combination of τ and ε creates an envelope for deviations from the specification that are still considered acceptable. In this work, since reaching the desired temperature level from a hot or a cold condition as fast as possible (even faster than prescribed by the specification) is good, implementation is still considered a valid one if the difference with respect to the specification is outside this envelope. Therefore, the envelope becomes a lower or higher bound in these situations. Let us discuss conformance problems (i) and (ii) before the preset level is reached, and (iii) and (iv) after reaching the preset level.

(i) For heat exposures, the changes in indoor temperature are expected to achieve a preset level and not raise to higher levels. Or, this may cause health problems without giving sufficient time to adjust the indoor temperature to the preset level. Moreover, quickly reaching the preset level

is favored. Thus, if ε is given appropriately, we could have $T - T_{rd} \geq \varepsilon$. This violates the requirement of $|T - T_{rd}| \leq \varepsilon$ in the (τ, ε)-closeness approach. But we accept this situation.

- Assume $\varepsilon = 1.5°C$, let us check temperature data and its requirements at 12:30 in Figure 5.4b. We get $T = 23.8°C$ and $T_{rd} = 21°C$, then $T - T_{rd} = 23.8 - 21 = 2.8 > \varepsilon$.

(ii) For cold exposures, the changes in indoor temperature are desired to reach a preset level without reaching to lower levels. Or, this may cause health problems as a result of cold exposure without giving sufficient time for the indoor temperature to reach the preset level. Furthermore, quickly reach the preset temperature level is favored. Thus, if ε is appropriately given, one can obtain $T_{rd} - T \geq \varepsilon$. We accept this situation but not for the (τ, ε)-closeness approach.

- In Figure 5.4c, let us check the temperature data at 12:30. We get $T = 17.5°C$ and $T_{rd} = 22.5°C$. Assume $\varepsilon = 2°C$, then $T_{rd} - T = 22.5 - 17.5 = 5 > \varepsilon$.

(iii) Let us discuss the unexpected temperature fluctuation problem after reaching the preset temperature level. Temperature fluctuation affects thermal sensations if the amplitude of temperature fluctuation is greater than the *Just-Noticeable Difference* [29, 115] value. This cannot be reflected by the (τ, ε)-closeness approach.

- The amplitude of temperature fluctuation, as illustrated in Figure 5.4d, should not exceed the requirement. We reject this situation in our conformance requirements. It is thus required to consider this situation in our case.

(iv) The last conformance problem we consider is the value difference in temperature variation. It will result in constantly warmer or cooler than expected. For instance, in Figure 5.4a, after achieving the preset level, i.e., $25°C$, indoor temperature stabled at about $26.8°C$ ($1.8°C$ greater than the preset level), which results in constantly warmer than expected. Our proposal to overcome this problem takes advantage of the value difference conformance of the (τ, ε)-closeness approach with some extra constraints. The detail of the proposal refers to Section 5.2.3.

The multiple-conformance approach is proposed by considering the conformance problems discussed in this section.

5.2.3 Service Filure/Hazard Detection

Let us discuss the multiple-conformance between temperature data and its requirements. It includes five conformance relations to guarantee a comprehensive detection of the problems, as shown in Table 5.1, for the states but not the initial state of the hybrid automation. The corresponding relations between thermal problems, conformance definitions, conformance problems and states of the hybrid automata are shown in Table 5.8. To use these conformance definitions, a mapping function from discrete states to conformance definitions, i.e., each state is attached with one or more conformance

rules, is provided. The detail will be discussed right after introducing the conformance definitions in Section 5.2.3. The differences between our proposal and the (τ, ε)-closeness method are that I substitute the (τ, ε)-closeness with multiple conformance relations that each of them is to detect the thermal problem(s) at different time intervals of test duration.

Table 5.8: Corresponding relationships.

Conformance Problem	**Thermal Problem**	**State of Hybrid Automation**	**Conformance Definition**
Time Domain Problem (i)	Undesired duration	*Cold*, *Cool*, *Hot*, *Warm*	State Duration Conformance
Space Domain Problem (i)	Unbearable hot	*Hot*	Upper Bound Conformance
Space Domain Problem (ii)	Unbearable cold	*Cold*	Lower Bound Conformance
Space Domain Problem (iii)	Undesired fluctuation	*Neutral*	Fluctuation Conformance
Space Domain Problem (iv)	Constantly cooler/warmer than expectation	*Neutral*	Value Difference Conformance

Preliminaries

In this section, let us introduce some concepts that relate to hybrid automata and temperature data.

Definition 14 (Hybrid Time Domain [10, 142])**.** *A hybrid time domain $E \subset \mathbb{R}^+ \times \mathbb{N}$ is defined as $E = \bigcup_{j=0}^{J-1} [t_j, t_{j+1}] \times \{j\}$, where $0 = t_0 \leq t_1 \leq t_2 \leq \cdots \leq t_J$. The set of all hybrid time domains are denoted by $\mathbb{T}$.*

j represents discrete evolutions, i.e., jumps, and $[t_j, t_{j+1}]$ represents continuous evolutions. Straightforwardly, the hybrid time domain is a split of the continuous-time domain into pieces. The time a hybrid system run once is the test duration $\mathcal{T} \leq t_J$

Let us assume some notations. A set of real-valued variables Var. A valuation of Var is a function $Var \mapsto \mathbb{R}$, which assigns a real number to each variable $var \in Var$. The set of all valuations of Var is represented by $Val(Var)$ [142].

Definition 15 (Trajectory [10, 142])**.** *Take a hybrid time-domain E and a set of variables Var. A trajectory over E is a function $\varphi : E \mapsto Val(Var)$, where for every $j, t \mapsto \varphi(t, j)$ is absolutely continuous in t over the interval $I_j = \{t | (t, j) \in E\}$.*

A trajectory is continuous valuations of a set of variables over the hybrid time domain.

Definition 16 (A sequence of sampling time). *A sequence of sampling time over a test duration $\mathcal{T}$ is a sequence $ST : st_1 \quad st_2 \quad \cdots \quad st_N$, where $0 = st_1 < st_2 < \cdots < st_N \leq \mathcal{T}$, $st_i \in \mathbb{R}_0^+$, $i \in [1, N]$; two adjacent sampling time points are denoted as $st_i \sim st_{i+1}$*

A sequence of sampling time is a series of time points, at which temperature data are sampled.

Definition 17 (Sampled temperature data). *The sampled temperature data is a function $T_{rd} : ST \mapsto \mathbb{R}$*

Definition 18 (Temperature level achievement). *Given a trajectory φ, $t^{'} > 0$, real data $T_{rd}(t^{'})$ and $\beta > 0$, a function $\psi : \mathbb{R}_0^+ \mapsto \varphi$ represents a required indoor temperature change. $T_{rd}(t^{'}) \cong_{(\beta)} \psi$ hold if one of the following hold*

1. $|T_{rd}(t^{'}) - \psi| \leq \beta$
2. $T_{rd}(t^{'}) > \psi \wedge \exists t_m \in ST, t_m \sim t^{'}, T_{rd}(t_m) < \psi$
3. $T_{rd}(t^{'}) < \psi \wedge \exists t_m \in ST, t_m \sim t^{'}, T_{rd}(t_m) > \psi$

This definition indicates at what conditions real data reached a prescribed temperature level. β represents a small number that indicates the difference between temperature data and its requirement is acceptably small at a certain sampling point. Predicate 1 represents two cases. First, the value of sampled point equals to the desired level, i.e., $T_{rd}(t^{'}) = \psi(t^{'})$. Second, the sampled points are not at the desired level. However, there exists a sampled point $t^{'}$ at the first point in the sampling sequence whose value is acceptably close to the desired level. In this situation, we say the desired level is reached at $t^{'}$, i.e., $|T_{rd}(t^{'}) - \psi| \leq \beta$. Predicate 2 means that a sampled point exceeded the desired level, while its adjacent following sampled point is bellow than the desired level. The desired level is reached somewhere in between these two sampled points. Predicate 3 means a reverse case to that represented by the predicate 2. If comparing β in Predicate 2 and 3 with ε in the (τ, ε)-closeness approach in the situation that two sampled points is beyond the envelope that created by τ and ε. There must an intersection with the required level by connecting the two sampled points. Therefore, the desired level has achieved by using β and not achieved by using ε.

Conformance Definitions

Let us formally discuss the conformance relations of the proposal in this section.

State Duration Conformance

It takes time to reach a preset temperature level by the indoor temperature adjustment service, which should not greater than the tolerance time. Thus, it is expected that the time to reach the desired temperature level should not greater than the prescribed time.

The time indoor temperature in Hot, Warm, Cold and Cool states is expected to last no more than the requirement plus τ_0 time unit. τ_0 substitutes τ of time domain problem (i) of Section 5.2.2.

Different states have different values of τ_0. $\tau_0 = t - t_0$, where t and t_0 are the same as in the time domain problem (i) of Section 5.2.2.

Let us first define the state duration of a state of hybrid automata. It is the time the state lasted.

Definition 19 (State Duration). *State duration is a function* $\Delta : E \mapsto \mathbb{R}^+$. $\Delta(t,j) = t_{j+1} - t_j$, *where* $t_j = min\{t|(t,n) \in E \wedge n = j\}$, $t_{j+1} = max\{t|(t,n) \in E \wedge n = j\}$

j means the jth jump to the current state in a *run*. It transited to the current state at t_j and leave it at t_{j+1}.

Definition 20 (State Duration Conformance). *Given* $i \geq 0$, *a trajectory* $\varphi(t,i)$, $t \in [t_i, t_{i+1}]$, $e_i \in E$, *a function* $\psi : \mathbb{R}_0^+ \mapsto \varphi$, *real data* $T_{rd}(t)$, $t \in [0, \mathcal{T}]$, $\beta > 0$ *and* $\tau_0 > 0$. T_{rd} *is said to be state-duration conform with* φ, *if* $\exists t_a, t_b, 0 \leq t_a < t_b \leq \mathcal{T} \wedge T_{rd}(t_a) \cong_{(\beta)} \psi(t_i) \wedge T_{rd}(t_b) \cong_{(\beta)} \psi(t_{i+1}) \wedge (t_b - t_a) - \Delta(e_i) < \tau_0$. *It is denoted by* $SD(i, \beta, \tau_0)$.

i means the ith jump to a state (e.g., Cold or Cool or Warm or Hot) in a *run*. The trajectory $\varphi(t,i)$ represents the required changes in indoor temperature. ψ is a function that maps from non-negative real number to φ. It first calculated the time to reach the desired temperature level. It started at when entering the state through jump i, which satisfies $T_{rd}(t_a) \cong_{(\beta)} \psi(t_i)$. It ended at the time to reach the desired level, which $T_{rd}(t_b) \cong_{(\beta)} \psi(t_{i+1})$ hold. τ_0 is the permitted error that a state can last at most τ_0 greater than it requirement.

It is known that τ_0 can be calculated through the tolerance time and its requirement. The tolerance time can be calculated from [1, 237]. The required time is derived by multiplying the temperature difference between the initial temperature and the desired level with the average time to decrease or increase by $1°C$, i.e., the value of *TPD*. Then we have $\tau_0 = Tol - |T_i' - T_{ini}| \times TPD$.

For the example in the time domain problem (i) of Section 5.2.2, it is assumed that $TPD = 2$ and $Tol = 14.2$, then we get $\tau_0 = 14.2 - (25 - 20.4) \times 2 = 5$. $\varphi(t,i)$ is the requirement with $t \in [11:12, 11:45]$ ($\Delta = 33$). Temperature data $T_{rd}(t)$, $t \in [11:12, 11:25]$ ($T_{rd}(11:12) = \psi(11:12) = 20.4°C$, and $T_{rd}(11:25) = \psi(11:45) = 25°C$), so, $t_b - t_a = 11:25 - 11:12 = 13$. Finally, we have $(t_b - t_a) - \Delta = 13 - 33 = -20 < \tau_0 = 5$. By using our proposed approach, temperature data conform to the requirement when $t \in [11:12, 11:45]$.

Lower Bound Conformance

Cold exposure as a result of low temperature may cause health problems. So, people expect indoor temperature not to be unacceptably low, and it should approach higher levels of temperature.

Indoor temperature in the Cold state is expected to be $\underline{\varepsilon}$ lower than the requirement with respect to the value domain problem (ii) of section 5.2.2. I substitute ε with $\underline{\varepsilon}$ in the value domain problem (ii) of Section 5.2.2 for differentiation. $\underline{\varepsilon}$ is the lower bound permitted error for changes in temperature in the *Cold* state.

Definition 21 (Lower Bound Conformance). *Given* $i \geq 0$, *a trajectory* $\varphi(t,i)$, $t \in [t_i, t_{i+1}]$, *real data* T_{rd}, $t \in [0, \mathcal{T}]$ *and* $\underline{\varepsilon} > 0$. T_{rd} *is said to be lower bound conformance with* φ, *if* $\varphi(t,i) - T_{rd}(t) < \underline{\varepsilon}$ *hold. It is denoted by* $LB(\underline{\varepsilon}, i)$

i means the ith jump to a state (e.g., Cold) in a *run*. The trajectory $\varphi(t, i)$ means the required changes in indoor temperature. $\varphi(t, i) - T_{rd}(t) < \underline{\varepsilon}$ guarantees that indoor temperature is at most $\underline{\varepsilon}$ lower than its requirement.

$\underline{\varepsilon}$ can be calculated by Formula 5.17. T_{ic} denotes the lower limit of indoor temperature, which is derived from cold stress indices. T_{sl} represents the annual statistic's lowest indoor temperature. $T_{sl} \leq T_{ic}$ means the working home appliances have an inefficient capability, which should not be taken as the requirement.

$$\underline{\varepsilon} = T_{sl} - T_{ic}, T_{sl} > T_{ic} \tag{5.17}$$

Let us consider the value domain problem (ii) of Section 5.2.2. Assume $\underline{\varepsilon} = 2$, then $\varphi(12 : 30, i) - T_{rd}(12 : 30) = 17.5 - 22.5 = -5 < \underline{\varepsilon}$. It is accepted by using the proposed lower bound conformance.

Upper Bound Conformance

Heat exposure because of hot weather may cause health problems. The high indoor temperature should approach lower levels without abruptly increase to higher levels than expected.

Indoor temperature in the Hot state should be no more than $\overline{\varepsilon}$ greater than its requirement for the value domain problem (i) of Section 5.2.2. $\overline{\varepsilon}$ substitutes ε in the value domain problem (i) of Section 5.2.2 for differentiation. $\overline{\varepsilon}$ is taken as the upper bound permitted error for changes in indoor temperature in the Hot state.

Definition 22 (Upper Bound Conformance)**.** *Given $i \geq 0$, a trajectory $\varphi(t, i)$, $t \in [t_i, t_{i+1}]$, real data T_{rd}, $t \in [0, \mathcal{T}]$ and $\overline{\varepsilon} > 0$. T_{rd} is said to be upper bound conformance with φ, if $T_{rd}(t) - \varphi(t, i) < \overline{\varepsilon}$ hold. It is denoted by UB$(\overline{\varepsilon}, i)$*

i means the ith discrete transition to a state (e.g., Hot) in a *run*. The trajectory $\varphi(t, i)$ represents the required changes in indoor temperature. $T_{rd}(t) - \varphi(t, i) < \overline{\varepsilon}$ guarantees that the indoor temperature is at most $\overline{\varepsilon}$ greater than the requirement.

Similar to $\underline{\varepsilon}$, $\overline{\varepsilon}$ can be calculated by Formula 5.18.

$$\overline{\varepsilon} = T_{ih} - T_{sh}, T_{ih} > T_{sh} \tag{5.18}$$

T_{ih} means the upper limit of indoor temperature. It can be derived from heat stress indices. T_{sh} represents the highest annual statistic indoor temperature. $T_{ih} \leq T_{sh}$ means home appliances have an inefficient capability, which cannot be taken as the requirement.

Assume $\overline{\varepsilon} = 1.5$, let us check the example in value domain problem (i) of Section 5.2.2. We have $T_{rd}(12 : 30) - \varphi(12 : 30, i) = 21 - 23.8 = -2.8 < \overline{\varepsilon}$. Thus, temperature data are accepted by the upper bound conformance.

Fluctuation Conformance

The amplitude of temperature fluctuation is greater than the value of JND [29, 115], which will result in thermal discomfort. Thus, it is required the amplitude should be a constraint.

The fluctuation conformance prescribes the amplitude of temperature fluctuation in the Neutral state less than α plus the requirement in considering the value domain problem (iii) of Section 5.2.2. α denotes the permitted error for temperature fluctuation to exceed the requirement. The amplitude is the maximum difference between a series of sampled temperature data and their average.

Definition 23 (Amplitude of Fluctuation)**.** *Given a function $f(x)$, $x \in [0, n], n \in \mathbb{N}$. The amplitude of $f(x)$ is $Amp(f(x)) = \begin{cases} max(|f(x) - \frac{1}{n}\int_0^n f(x)dx|) \\ max(|f(x) - \frac{1}{n}\sum_0^n f(x)|) \end{cases}$*

$f(x)$ is a piecewise function. It considers situations when $f(x)$ is a continuous or discrete function.

Definition 24 (Fluctuation Conformance)**.** *Given $i \geq 0$, a trajectory $\varphi(t, i)$, $t \in [t_i, t_{i+1}]$, real data $T_{rd}(t)$, $t \in [0, \mathcal{T}]$ and $\alpha \geq 0$. T_{rd} is said to be fluctuation conformance with φ, if $|Amp(T_{rd}(t) - Amp(\varphi(t, i))| < \alpha$ hold. It is denoted by $FC(i, \alpha)$.*

i means the ith discrete transition to a state (e.g., Neutral) in a *run*. The trajectory $\varphi(t, i)$ represents the required changes in indoor temperature. α denotes the difference between the JND value and the required amplitude of temperature fluctuation. The JND [29] is about human reactions to physical stimuli. Assume S is the magnitude of a measurable stimulus, and ΔS is the discrepancy required for discrimination, then $c = \frac{\Delta S}{S}$ is a constant, where ΔS is the JND. The JND value for $(23 - 27°C)$ is about $[0.09, 0.80]°C$ for warm or cool sensation [115].

Consider the example of value domain problem (iii) of Section 5.2.2, assume $\alpha = 0.5$ we get

$$Amp(T_{rd}) - Amp(\varphi) = 2.8 - 0.1 = 2.7 > \alpha = 0.5.$$

This means that temperature data are not conformed to its requirement. So, one can detect unacceptable fluctuation.

Value Difference Conformance

To solve the value domain problem (iv) of Section 5.2.2, there are two differences of our proposal with the value difference of the (τ, ε)-closeness approach. First, the pass of the fluctuation conformance is the premise to check the problem of value difference. Second, let us discuss the value difference conformance at the Neutral state.

The value differences between temperature data and the preset level exceeded the *JND* value will cause different thermal sensation than expected. Informally, the value difference conformance is the maximum departure of indoor temperature from the preset level should not be ε greater or smaller than the requirement.

Definition 25 (Value Difference Conformance). *Given $i \geq 0$, a trajectory $\varphi(t,i)$, $t \in [t_i, t_{i+1}]$, real data $T_{rd}(t)$, $t \in [0, \mathcal{T}]$ and $\alpha \geq 0$ and $\varepsilon \geq 0$. T_{rd} is said to be the value difference conformance with φ, if $FC(i,\alpha) \wedge |T_{rd}(t) - \varphi(t,i)| \leq \varepsilon$ hold. It is denoted by $VD(i,\alpha,\varepsilon)$.*

i means the ith discrete transition to a state (e.g., Neutral) in a *run*. The trajectory φ denotes the required changes in indoor temperature. ε represents the permitted error of temperature deviation at the Neutral state, It can be derived from $[NL, NH]$ and α with considering the following cases. The reason is that to achieve thermal comfort, $T_i' + \alpha \leq NH$ and $T_i' - \alpha \geq NL$ have to be satisfied.

- When the initial temperature is bellow the desired temperature level.
  - If desired level plus α is smaller than TC_h, $\varepsilon = \alpha$.
  - if desired level plus α is greater than TC_h, $\varepsilon = TC_h - T_i'$.
- When the initial temperature is above the desired level.
  - if desired level minus α is greater than TC_l, $\varepsilon = \alpha$.
  - if desired level minus α is smaller than TC_l, $\varepsilon = T_i' - TC_l$.

Use of the Conformance Definitions

If any of the conformance relations discussed is rejected, which means the corresponding thermal problem, as shown in Table 5.1 has occurred. For a *run* of hybrid automata, temperature data are accepted if all the conformance relations that assigned to the states of the *run* are all accepted.

Therefore, let us first assign conformance relations to the corresponding states of hybrid automation.

Definition 26 (Conformance Assignment). *Given a set of states $v = \{v_1, \cdots v_n\}$ of a hybrid automation and a set of conformance definitions $c = \{c_1, \cdots c_5\}$. Conformance assignment is a function $C : v \to 2^c$, where 2^c is the power set of c*

E.g. $C(v_i) = \{c_p, \cdots c_q\}$.

Next, let us evaluate if temperature data corresponding to the state of hybrid automata is accepted or not with respect to the assigned conformance relation(s).

Before that, let us introduce the formal definition of solution pair [21]. A hybrid automation HA is denoted by $HA = (Loc, X, (l_0, v_0), \to, inv, flow)$, where *Loc* denotes the finite set of locations; X is the set of continuous variables; l_0 and x_0 represent the initial location and valuation of X respectively; $\to$ means a set of jumps; *inv* denotes invariation conditions; *flow* represents the flow conditions. Assume g is the guard function, and r is the reset function.

Definition 27 (Solution [21]). *A solution to a hybrid automation HA is a function $s : E \mapsto Loc \times Val(V)$, where*

- $s(0,0) = (l_0, x_0)$;
- *for each* $(t,j) \in dom(s)$: x *satisfies* $inv(l)$ *and* $flow(l)$, *where* $(l,x) = s(t,j)$ *is the pair of location and valuation at time (t,j);*
- *for each* $(t_j,j) \in dom(s)$ *with* $j > 0$; *there exists* $l \xrightarrow{g,r} l'$ *such that* x *satisfies* g *and* (x,x') *satisfies* r, *where* $(l,x) = s(t_j,j-1)$ *and* $(l',x') = s(t_j,j)$ *are the pairs of location and valuation at times* $(t_j,j-1)$ *and* (t_j,j), *respectively.*

Definition 28 (Trajectory Restriction [21]). *The restriction of a trajectory* $\varphi : E \to Val(X)$ *to* $X' \subset X$ *is a trajectory* $E \to Val(X')$, *denotes by* $\varphi \downarrow X'$, *for which* $\varphi \downarrow X'(t,j) = \varphi(t,j) \downarrow X'$, $\forall (t,j) \in dom(\varphi)$.

Definition 29 (Solution Pair [21]). *Let* u *and* y *be two trajectories of types* $E \to Val(X_I)$ *and* $E \to Val(X_O)$, *respectively;* (u,y) *is a solution pair to a hybrid automation HA if*

- *dom(u)=dom(y);*
- *there exists a trajectory* φ *for HA such that* $dom(\varphi) = dom(u)$, $u = \varphi \downarrow X_I$ *and* $y = \varphi \downarrow X_O$.

Definition 30 (Multiple Conformance Relation). *Consider a trajectory* y *of a hybrid automation HA, and a trajectory RD that mapping hybrid time domain to temperature data* T_{rd}, *i.e.,* $\varphi : E \mapsto T_{rd}$. *Given a test duration* $\mathcal{T} \in \mathbb{R}^+$, *a maximum number of jumps* $J \in \mathbb{N}$, *and* $\beta, \tau_0, \underline{\varepsilon}, \overline{\varepsilon} > 0$, $\alpha, \varepsilon \geq 0$. T_{rd} *conforms to* y *iff:*

- *For all solution pairs (u,RD) of temperature data, there exists a solution pair (u,y) of HA;*
- *For each piece of temperature data* $RD(t,j)$, *there exists a state* v_j *of HA such that* $RD(t,j)$ *conforms to* $y(t,j)$ *w.r.t.* $C(v_j)$ *hold;*

We denote it by $T_{rd} \dddot{\approx}_{(\beta,\tau_0,\underline{\varepsilon},\overline{\varepsilon},\alpha,\varepsilon)} HA$.

Definition 31 (State Conformance Evaluation). *Given a state* v *of hybrid automata, state conformance evaluation is a function* $Eva : C(v) \mapsto \{accept, reject\}$.

The State Conformance Evaluation is defined by Algorithm 2. With the same input for generating the real data and the output of hybrid automation, it checks the conformance of real data with the output of hybrid automation by considering the conformance rules. The *accept* means all conformance rules attached to a state of hybrid automation are hold concerning the trajectory of the state and real data, while *reject* means at least one of the conformance rules rejected.

Definition 32 (State Conformance). *Given a state* v *of a hybrid automation. State conformance* $SC(v)$ *is defined as follows:*

Algorithm 2: State conformance evaluation: given a state of hybrid automation, its trajectory, and corresponding real data, it determines the conformance rules it concerns will *accept* or *reject* the real data.

Input: A state v of a hybrid automation HA; its trajectory $\varphi(t,i)$; real data $T_{rd}(t)$ $(t \in [t_i, t_{i+1}])$

Output: accept or reject

```
p ← φ(t,i)    /* trajectory for the state of the hybrid automation */
q ← φ : E ↦ T_rd                          // trajectory for the real data
u ← φ                                  /* u represents input trajectory and
 dom(u)=dom(x)=dom(y)[21] */
(u,p);                                                  // solution pair
(u,q);                                                  // solution pair
for each c ∈ C(v) do
    if q conforms to p w.r.t. c hold then
        continue;
    else
        return reject;
    end
end
return accept;
```

- $\forall c \in C(v), Eva(c) = accept.$

The *run* conformance is defined based on the state conformance.

Definition 33 (Run Conformance)**.** *Given a* run $r : (v_0, e_0) \to (v_1, e_1) \to \cdots \to (v_n, e_n)$ *of a hybrid automation,* $(v_i, e_i), i \in [0, n]$ *belongs to the* control graph*.* Run *conformance* $RC(r)$ *is defined as follows*

- *For all* v_i *in* r*,* $SC(v_i)$ *hold.*

5.2.4 Experiment

The purposes of the experiment are twofold. The first is to verify the reasonableness of using the hybrid-automata-modeled requirement and the multiple-conformance approach to check the indoor temperature for comprehensively detecting thermal problems shown in Table 5.1. For comparison, the (τ, ε)-closeness is also applied to check temperature data. The second is to evaluate the performance of the multiple-conformance approach and the hybrid-automata-modeled requirement in detecting thermal problems by comparing that with by using the (τ, ε)-closeness approach.

Reasonableness Verification

I use Matlab to verify the reasonableness. The Matlab code includes four main parts, that is, read temperature data, requirement generation, and conformance check by using the proposal and the (τ, ε)-closeness. I collected temperature data from the western style room 1 of iHouse, as shown in Figure 5.5. The iHouse is a testbed house for smart home services located at Ishikawa prefecture, Japan. There is an app that is taken as the controller of home appliances, i.e., an air-conditioner, a window, and a curtain. The control commands are issued remotely from our lab, as illustrated in Figure 5.5. Temperature data are first stored locally, then acquired later from the lab. The requirement generation is to generate output trajectories of hybrid automation. It fed the first sampled temperature data as initial temperature to the hybrid automation. The conformance check by the proposal based on the conformance relations is discussed in Section 5.2.3. And the conformance check by the (τ, ε)-closeness is based on the introduction from [10, 142]. Matlab pseudo-codes are illustrated in Algorithms 3, 4, and 5. For Algorithms 4, it works in the while loop $while(state! = null)$, and the *break* statement is omitted for each *case* statement.

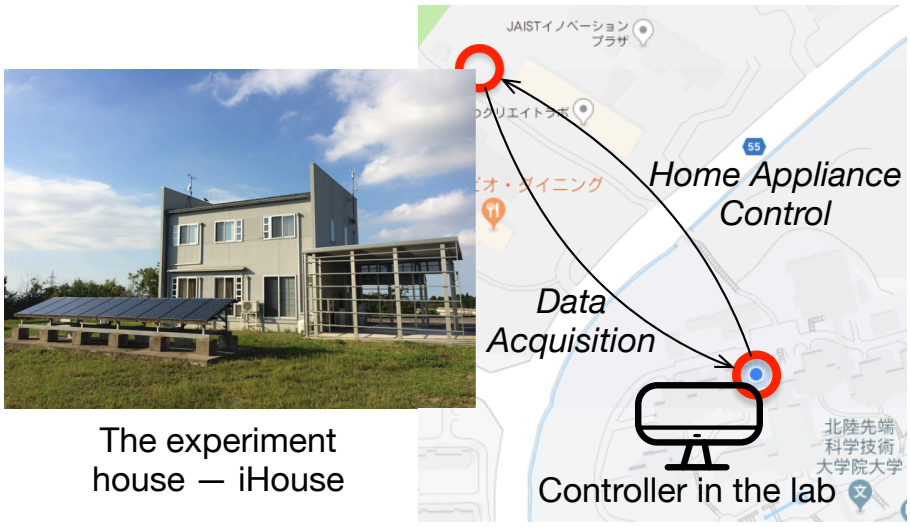


Figure 5.5: Temperature data collection.

Some of the results are illustrated in Figure 5.6. Every column of this figure includes the upper one for the conformance check of temperature data, and the lower one the states of the requirement. For demonstration, indoor temperature belongs to the intervals illustrated in Table 5.9 are invariant conditions of hybrid automata. Every row is adopted by the hybrid automation to produce the requirement in the corresponding column of Figure 5.6. For example, hybrid automation uses the second row to produce the requirement used in Figure 5.6b. The conformance check by the proposal shares the same set of parameter values, as shown in the Conformance Parameters row of Table 5.9. Text messages in Figures5.6a, 5.6b, and 5.6c are printed by the conformance check of the proposal. The parameter values of the (τ, ε)-closeness satisfy $\tau = 10min$ and $\varepsilon = 2°C$. Temperature data that are depicted by

Algorithm 3: Check the conformance of temperature data with its requirements by using the proposal and the (τ, ε)-closeness.

```
1  rdata ← load(realData,startTime,endTime)
2  time ← extractTime(rdata)
3  temp ← extractTemp(rdata)
4  require ← init(temp(1))
5  state ← discreteState(temp)
6  for i=1 to length(state) do
7  |  if state(i) == Cold then
8  |  |  require.append(flow(Cold))
9  |  else if state(i) == Cool then
10 |  |  require.append(flow(Cool))
11 |  else if state(i) == Neutral then
12 |  |  require.append(flow(Neutral))
13 |  else if state(i) == Warm then
14 |  |  require.append(flow(Warm))
15 |  else if state(i) == Hot then
16 |  |  require.append(flow(Hot))
17 |  end
18 end
19 To be continued in Algorithm 4 ...
```

red circles in Figures 5.6a, 5.6b, and 5.6c means the rejection of value difference of the (τ, ε)-closeness. Let us discuss the time lag problem in the next paragraph.

The conformance check rejected the Value Difference Conformance at the Neutral state, as shown in Figure 5.6a. This implies our proposal has detected the constantly warmer than expected. The (τ, ε)-closeness rejected temperature data correspond to the Cool state, which was accepted by our proposal. The check rejected the Fluctuation Conformance at the Neutral state, as illustrated in Figure 5.6b. This indicates the detection of the undesired fluctuation by the proposal. However, one cannot identify the fluctuation problem from that some data were rejected by the (τ, ε)-closeness. Moreover, the time lag between temperature data and its requirement is about 17 min. The (τ, ε)-closeness rejected this situation, but not for our proposal. This is because based on the proposed State Duration Conformance, the time lag is -17, and $-17 < 15$. There are multiple rejections, as illustrated in Figure 5.6c. Both the Upper Bound Conformance that detects the unbearable hot, and the State Duration Conformance that detects the undesired duration at the Hot state were rejected. The State Duration Conformance that detects the undesired duration at the Warm state was rejected. The Value Difference Conformance was not checked due to the Fluctuation Conformance has rejected at the Neutral state. Some data were rejected by the (τ, ε)-closeness, but one cannot tell what problems

Algorithm 4: continues Algorithm 3, and is continued in 5.

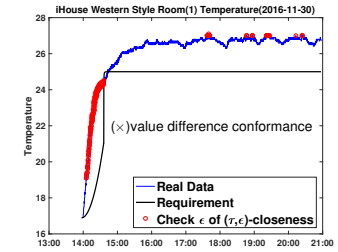
```
switch state do
    case Cold do
        if SD(i, β, τ0) == reject then
            text("(×)state duration(Cold)")
        end
        if LB(ε̲, i) == reject then
            text("(×)lower bound(Cold)"
        end
    case Cool do
        if SD(i, β, τ0) == reject then
            text("(×)state duration(Cool)")
        end
    case Neutral do
        if FC(i, α) == reject then
            text("(×)fluctuation conformance")
        else if VD(i, α, ε) == reject then
            text("(×)value difference conformance")
        end
    case Warm do
        if SD(i, β, τ0) == reject then
            text("(×)state duration(Warm)")
        end
    case Hot do
        if SD(i, β, τ0) == reject then
            text("(×)state duration(Hot)")
        end
        if UB(ε̄, i) == reject then
            text("(×)upper bound(Hot)")
        end
    end
    otherwise do
        error : not a state
    end
end
```

Algorithm 5: continues Algorithm 3 and 4.

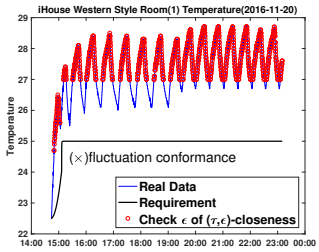
```
if τε_closeness(time, temp, require) == reject then
    plot(rejected data as red circles)
end
```

Table 5.9: Temperature intervals of invariant conditions and conformance parameters.

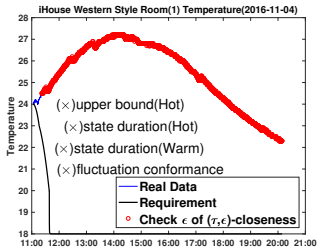
	Cold	Cool	Neutral	Warm	Hot
Intervals	$(-\infty, 5]$	$[5, 21]$	$[21, 26]$	$[26, 32]$	$[32, +\infty)$
	$(-\infty, 10]$	$[10, 24]$	$[24, 27]$	$[27, 32]$	$[32, +\infty)$
	$(-\infty, 6]$	$[6, 16]$	$[16, 20]$	$[20, 23]$	$[23, +\infty)$
Conformance Parameters	$\tau_0 = 10min$ $\underline{\varepsilon} = 0.2°C$	$\tau_0 = 15min$	$\alpha = 2°C$ $\varepsilon = 2°C$	$\tau_0 = 15min$	$\tau_0 = 10min$ $\overline{\varepsilon} = 0.2°C$



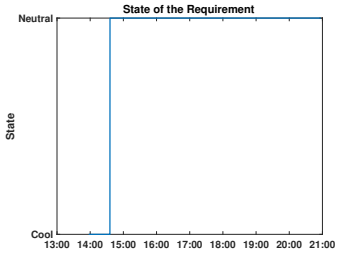
(a) Value sifference violation.



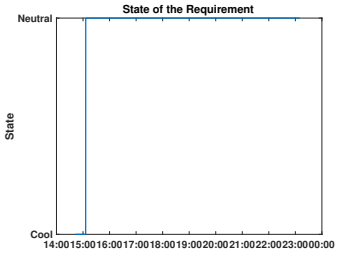
(b) Fluctuation violation.



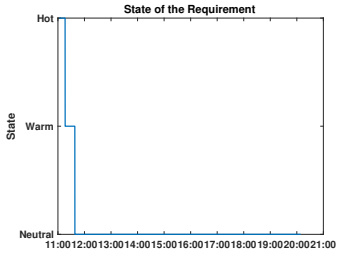
(c) Conformance violation.



(d) State of requirement.



(e) State of requirement.



(f) State of requirement.

Figure 5.6: Results of the conformance check.

are there.

Performance Evaluation

This section introduces the evaluation of the performance of the proposed multiple-conformance approach and the hybrid-automata-modeled requirement in detecting thermal problems by comparing with the (τ, ε)-closeness approach. As detected results may be incorrect, e.g., the occurrence of a thermal problem is regarded as not occurring, or vice versa or a thermal problem is concluded as another one. The evaluation is based on the confusion matrix.

A confusion matrix is a table to describe the performance of a classifier on a set of test data for which the true values are known. The table looks like the one shown in Table 5.10. The columns denote the predicted class, and the rows represent the true class. In Table 5.10, there are two classes, i.e., *Yes* and *No*. Each cell shows the number of corresponding results. For example, if $TN = 2$ which means two samples are correctly classified into the *No* class, and if $FP = 3$ that denotes three samples are incorrectly classified into the *Yes* class.

Table 5.10: Confusion matrix.

		Predicted Class	
		No	**Yes**
True Class	**No**	TN (True Negative)	FP (False Positive)
	Yes	FN (False Negative)	TP (True Positive)

There are some terminologies, as shown in Table 5.11, that is calculated based on the confusion matrix to evaluate the performance of a classifier. The confusion matrix and its related terms can be automatically generated by the Matlab function *confusionchart*. The layout of the output graph is shown in Figure 5.7. The yellow part represents the percentages of correctly and incorrectly classified observations for each true class and predicted class. They correspond to the the terms in Table 5.11.

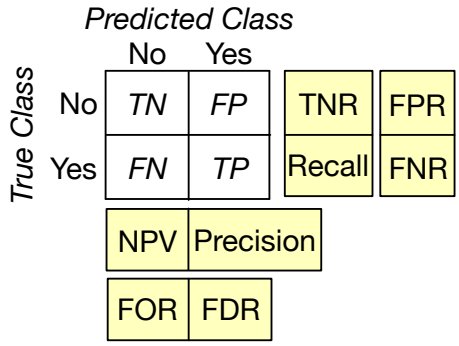


Figure 5.7: Layout of the output graph generated by the Matlab function *confusionchart*.

To adopt the confusion matrix, it is required to prepare a set of sample data for a specific thermal problem. Whether the sample data can cause a thermal problem or not is known, that is the true class.

Table 5.11: Terminologies related to confusion matrix.

Term	Formula
True Positive Rate (TPR) or Recall	$Recall = \frac{TP}{TP+FN}$
True Negative Rate (TNR)	$TNR = \frac{TN}{TN+FP}$
Positive Predictive Value (PPV) or Precision	$Precision = \frac{TP}{TP+FP}$
Negative Predictive Value (NPV)	$NPV = \frac{TN}{TN+FN}$
False Negative Rate (FNR)	$FNR = \frac{FN}{FN+TP}$
False Positive Rate (FPR)	$FPR = \frac{FP}{FP+TN}$
False Discovery Rate (FDR)	$FDR = \frac{FP}{FP+TP}$
False Omission Rate (FOR)	$FOR = \frac{FN}{FN+TN}$
Accuracy	$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$
F Score or F Measure is the harmonic mean of precision and sensitivity	$F = \frac{2\times Recall\times Precision}{Recall+Precision} = \frac{2\times TP}{2\times TP+FP+FN}$

Then, let us check the set of sample data by using the proposal and the (τ, ε)-closeness approach to detect the thermal problems, respectively. When adopting the (τ, ε)-closeness approach, it focuses on each state of hybrid automata for the checking. The detected results are the predicted class. Finally, let us feed the true class and predicted class to the Matlab function *confusionchart* to construct the confusion matrix and to calculate its related terms.

As discussed in Section 5.2.1, there are different thermal problems considered in different situations. They are numbered in Table 5.12 for better reference. Each of the thermal problems corresponds to one type of raw data that is shown in Figure 5.8. For example, thermal problem 1 corresponds to the data type 1. It is necessary to point out that data ① and ② in Figure 5.8 will not cause thermal problems. However, they are taken as problems by the (τ, ε)-closeness approach.

Table 5.12: Thermal problems with numbering.

No.	Thermal Problem
1	Unbearable hot (Hot)
2	Undesired duration (Hot)
3	Undesired duration (Warm)
4	Undesired fluctuation (Neutral)
5	Constantly cooler/warmer than expectation (Neutral)
6	Undesired duration (Cool)
7	Undesired duration (Cold)
8	Unbearable cold (Cold)

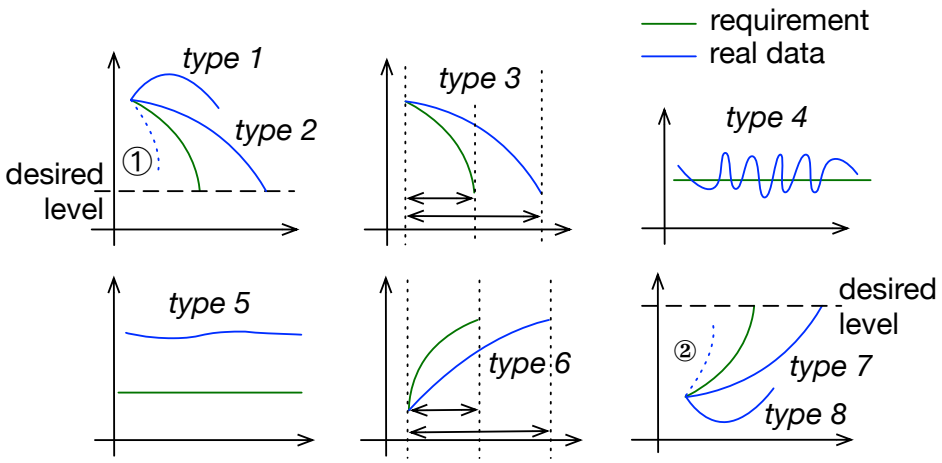


Figure 5.8: A classification of data type.

The classified data types are shown in Figure 5.8 are considered in the problem domain, i.e., temperature changes affect thermal sensations. It is assumed that each type of data is either trustable or processed by technologies related to sensor data error detection and prediction [72, 225] (These techniques are irrelevant to the work of this research). This is because the data may be corrupted or lost due to errors in sensors, data transmission, storage, and process.

There are two data sources. One is acquired from the iHouse that was introduced in the last subsection. The system to acquire real data from the iHouse was implemented by other technicians. Temperature data acquired by using the system is assumed to be trustable. Under weather conditions during a limited period, the acquired data cannot cover all concerned thermal problems. Therefore, some other data are made based on the facts discussed in Section 5.2.3. For example, a thermal problem occurred when the amplitude of temperature exceeded a given JND value. The data are made based on four Matlab functions that the author wrote, i.e., *increase*(), *decrease*(), *stable*(), and *fluctuation*(). Figure 5.9 shows the output data to illustrate how these functions work. The data between $[0, 195]$ were generated by the function *decrease*(); the data between $[195, 468]$ were generated by the function *increase*(); the data between $[468, 1453]$ were generated by the function *stable*(); and the rest were generated by the function *fluctuation*().

The resulting confusion matrix tables that produced by the Matlab function *confusionchart* for the thermal problems in Table 5.12 are shown in the Figures 5.10, 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, and 5.17. There are two classes in the confusion matrix tables, i.e., *Yes* and *No*. *Yes* denotes there exist the corresponding thermal problem. *No* means there does not exist the corresponding thermal problem. There is another class denoted as *Irrelevance*, which means the detecting result is irrelevant to the *Yes* and *No*. In other words, the related approach cannot be used for detecting the corresponding thermal problem.

The two confusion matrix terms, i.e., accuracy and F-Measure, are not produced by the Matlab

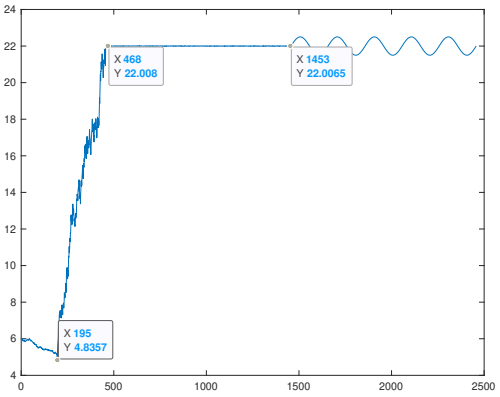
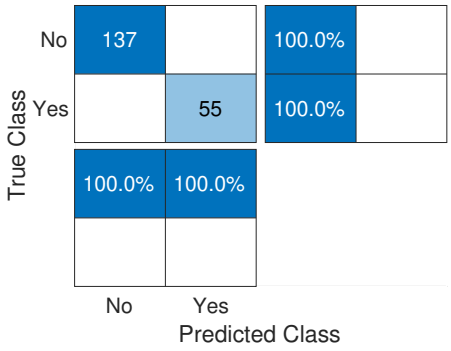
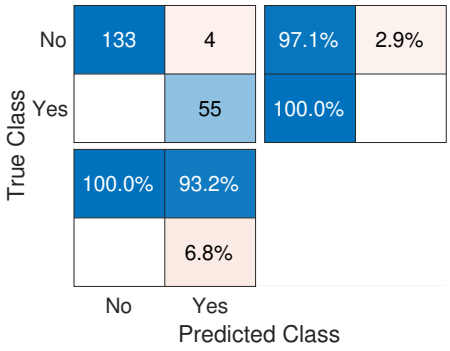


Figure 5.9: Example output of faked data.



(a) Confusion matrix for the proposal.



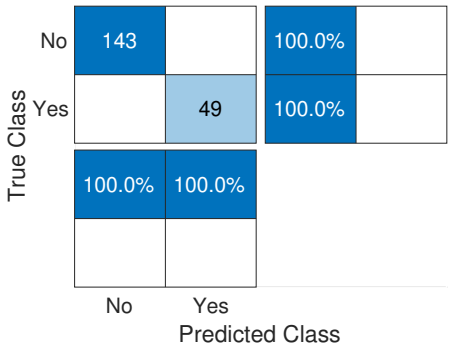
(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.10: Confusion matrix based on the detection of thermal problem 1.

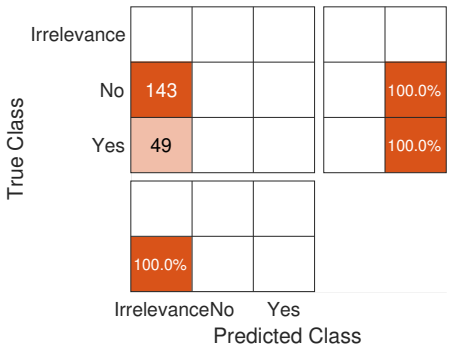
function *confusionchart*. Their results are calculated based on the formulas introduced in Table 5.11 and the resulting confusion matrix tables shown in Table 5.13.

5.2.5 Discussion

Required changes in indoor temperature in Figure 5.6a, 5.6b, and 5.6c are produced based on the scenario similar to that generated the requirement in Figure 5.3. It is expected the indoor temperature to be adjusted to the desired level, e.g. 20°C in Figure 5.6a should less than the tolerable time. Then, it stabilizes at the desired level. Moreover, it should not result in the undesired fluctuation or constantly cooler/warmer than expected after reaching the desired level. If initially in the hot weather, e.g. Figure 5.6c, it requires to reach the desired level within the tolerable time, also will not cause the unbearable hot. Required changes in indoor temperature, as shown in Figures 5.6a, 5.6b, and 5.6c,

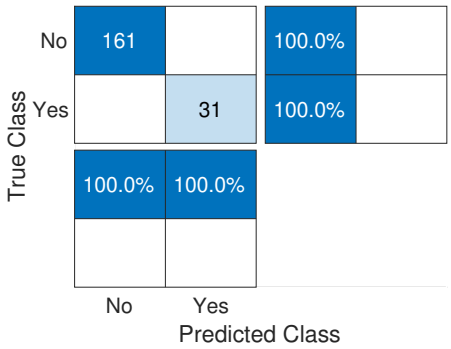


(a) Confusion matrix for the proposal.

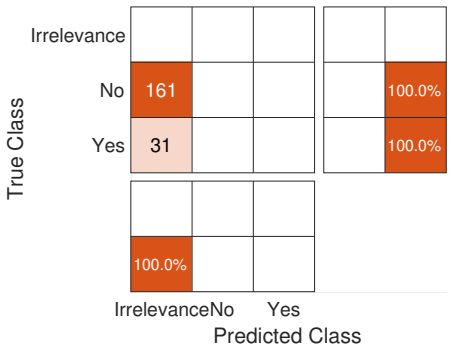


(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.11: Confusion matrix based on the detection of thermal problem 2.

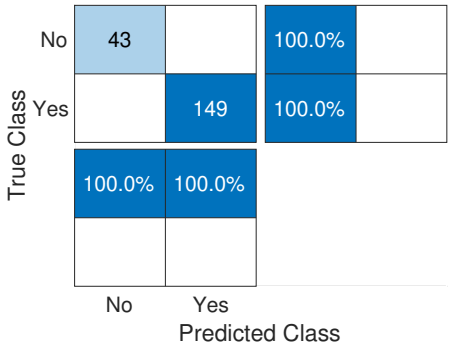


(a) Confusion matrix for the proposal.



(b) Confusion matrix for the (τ, ε)-closeness.

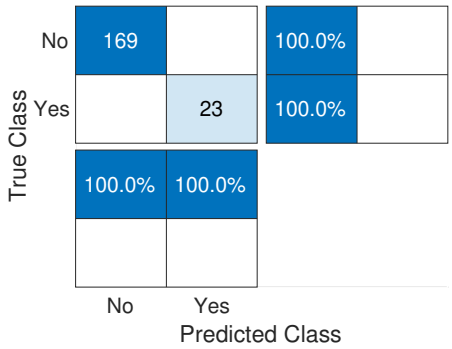
Figure 5.12: Confusion matrix based on the detection of thermal problem 3.



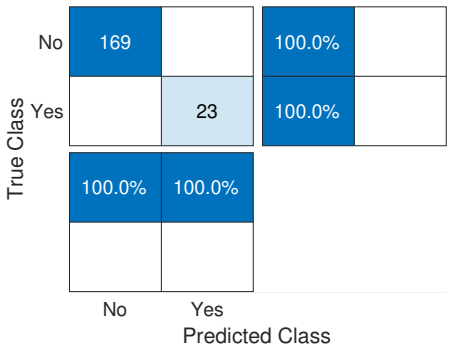
(a) Confusion matrix for the proposal.

(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.13: Confusion matrix based on the detection of thermal problem 4.

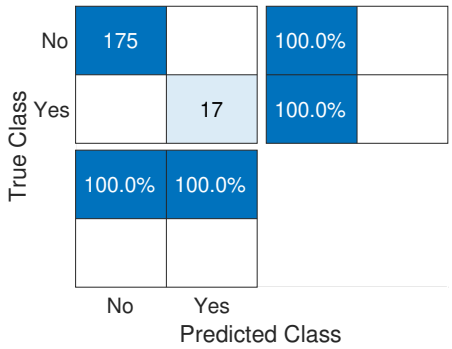


(a) Confusion matrix for the proposal.

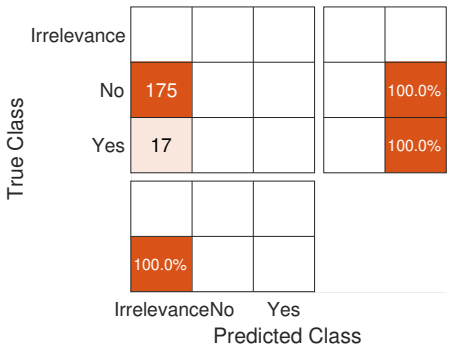


(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.14: Confusion matrix based on the detection of thermal problem 5.

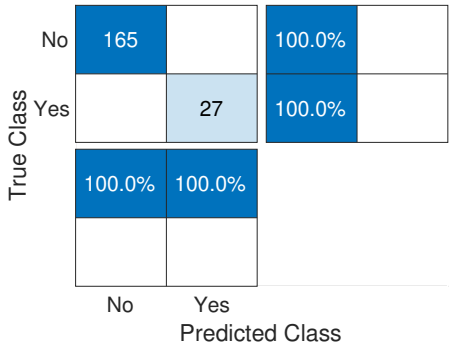


(a) Confusion matrix for the proposal.

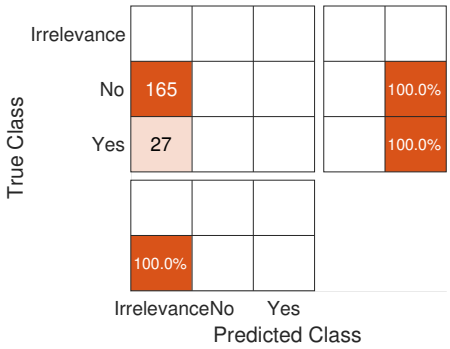


(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.15: Confusion matrix based on the detection of thermal problem 6.

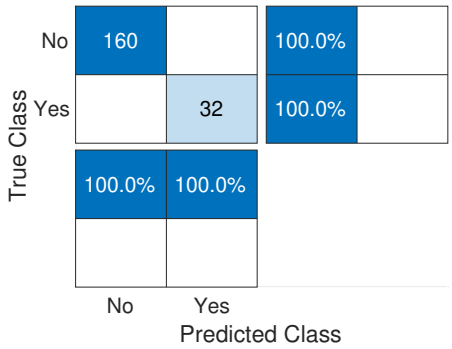


(a) Confusion matrix for the proposal.

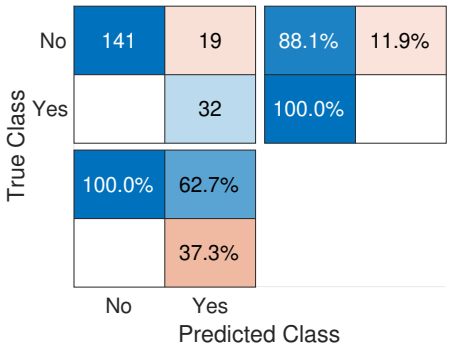


(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.16: Confusion matrix based on the detection of thermal problem 7.



(a) Confusion matrix for the proposal.



(b) Confusion matrix for the (τ, ε)-closeness.

Figure 5.17: Confusion matrix based on the detection of thermal problem 8.

Table 5.13: The calculation of accuracy and F-Measure based on the confusion matrix tables.

	Thermal Problem Detection by Using the Proposal		**Thermal Problem Detection by Using the (τ, ε)-closeness**	
No. of Thermal Problem	Accuracy	F-Measure	Accuracy	F-Measure
1	1	1	47/48	55/57
2	1	1	0	0
3	1	1	0	0
4	1	1	0	0
5	1	1	1	1
6	1	1	0	0
7	1	1	0	0
8	1	1	173/192	64/83

meet the requirement of these facts. These validate the modeling of the required changes in indoor temperature.

The modeling of required changes in indoor temperature by hybrid automata theoretically validates the proposal, which is equivalent to employing human feelings. The temperature intervals of invariant conditions of hybrid automata were calculated from the PMV-PPD index, heat indices, and cold indices that are proven techniques to evaluate various thermal sensations. The required changes in temperature for every time interval is calculated from heat exchange between outdoor and indoor. The discussed thermal problems are based on the facts about, for instance, the *Just-Noticeable Difference* [115], the tolerance time [1, 237], etc.

Hybrid automata can be used to represent the required changes in indoor temperature. Various thermal sensations correspond to the states of hybrid automata. For instance, the Cold state is shown in Table 5.9 corresponds to the invariant condition $T_i \in (-\infty, 5]$, which related to the cold sensation. Carefully design of the flow condition of a state (in Section 5.2.1) can avert the discussed thermal

problems. For example, the time the change in indoor temperature at the Cold state should reach the Cool state less than the tolerance time so that undesired duration will not occur.

I adopted hybrid automata to model the required changes in indoor temperature. This guarantees the detection at various time intervals of test duration. The time partition is realized through discrete transitions between states. For example, the test duration was split by the jump from Cool to Neutral in Figure 5.6b (i.e., 14:42-15:06 and 15:06-23:10); the test duration was split by jumps from Hot to Warm, then to Neutral in Figure 5.6c (i.e., 11:02-11:16, 11:16-11:38, and 11:38-20:08). Therefore, concerned thermal problems are possible to be detected at different intervals of test duration. However, the (τ, ε)-closeness approach checks the conformance on the test duration. This restricted detection at different time intervals.

Our proposal can comprehensively detect the thermal problems that range from uncomfortable to serious, as shown in Table 5.1, at different intervals of test duration. For instance, in Figure5.6c, unbearable hot and undesired duration was detected at the Hot state, undesired duration was detected at the Warm state, and undesired fluctuation was detected at the Neutral state. The problem of constantly warmer than the expected level at the Neutral state is shown in Figure 5.6a. Figure 5.6b shows the undesired fluctuation at the Neutral state. The problems are shown in Table 5.1 but not illustrated in Figure 5.6 can also be detected by using our proposal. The (τ, ε)-closeness method is only able to detect the problem of whether an excess of an allowable error could happen in the time and space domain. For example, in Figure 5.6b, one cannot figure out the thermal problems by just showing that unacceptable temperature in comparison with the requirement, and the time lag is about 17min has occurred.

For the reasons for the concerned thermal problems, I summarize them as unexpected heat exchange between outdoor and indoor, or other indoor heat sources. Intuitively, these are heat noises to changes in indoor temperature. For instance, the reason to constantly warmer than the expectation that shown in Figure 5.6a could be excessive heat accumulation due to the air-conditioner keep heating the well-insulated room. The reason for the undesired fluctuation that showed in Figure 5.6b could be the usage of the energy-saving mode of the air-conditioner in the not well-insulated room. By working at this working mode, the air-conditioner heats intermittently. The reason for the unbearable hot, as shown in Figure 5.6c, could be the usage of the heating mode of the air-conditioner for the well-insulated room in hot weather. To summary, I classify the causes into two types, i.e., ambient noise and performer noise. The former means insulation of a room while home appliances are working properly, which results in unexpected dissipation or the introduction of heat outdoor. The latter refers to improperly working of home appliances (intentionally or unintentionally), which introduces or dissipates excess heat than expected for the well-insulated room.

Hybrid automata are flexible and intuitive to model the required changes in indoor temperature. States of hybrid automata can represent various thermal sensations concerning different indoor temperature intervals. Moreover, by devising the corresponding conformance relations used in every state to detect the concerned thermal problems. The hybrid-automata-modeled requirements together with the multiple-conformance approach can be used to validate the indoor temperature adjustment service. Multiple specifications of home appliances could make it difficult to validate if operations of home appliances comply with their specifications dynamically. This is due to that the selection of

home appliances to work depends on the dynamic weather conditions. So, it is possible to adopt the proposal to see if the indoor temperature adjust service is appropriate or not, while do not care which home appliances are selected to work. One disadvantage if the *monitor* dynamically observes changes in indoor temperature could be that there may exist a time lag between the time a problem occurs and the time the problem is detected. For example, to detected the unexpected temperature fluctuation, the *monitor* may take time to detect it.

One can easily expand and tailor the multiple-conformance approach. For instance, one could add new conformance rules if other temperature anomalies arise. Furthermore, one can also adopt hybrid automata to model other expected phenomena which have discrete and continuous characteristics. For example, the change in humidity. Then, different conformance rules can be devised and used at different states of hybrid automata to detect concerned problems. one could also expand to use our proposal at other indoor places, e.g., an office, or maybe outdoors that have similar considerations.

The proposed multiple-conformance approach and the hybrid-automata-modeled requirement have better performance in detecting the thermal problems by comparing with the conventional (τ, ε)-closeness approach. The proposal got all 1s in accuracy and F-Measure (Table 5.13) due to it focuses only on the problem domain, i.e., changes in temperature cause thermal problems. Both the proposed and conventional approaches can detect thermal problem 1. However, the proposed approach has better performance due to the values of F-Measure and accuracy are all 1s, and 55/57 and 47/48 respectively for the conventional approach. This is because the conventional approach takes both the data *type 1* and ① as the thermal problem 1. However, data ① cannot cause thermal problem 1. That is why there are 4 false-positive results as shown in Figure 5.10b.

The conventional approach cannot detect thermal problem 2, 3, 4, 6, and 7. According the confusion matrix tables shown in Figures 5.11b, 5.12b, 5.13b, 5.15b, and 5.16b, all the results are concluded as a different result (*Irrelevance*) rather than whether a thermal problem is happening or not. The reason is that the (τ, ε)-closeness approach cannot be used in detecting the thermal problems.

Both the proposed and the conventional approach have a perfect performance in detecting thermal problem 5. Because the values of F-Measure and accuracy are all 1s. But, the (τ, ε)-closeness can only be used when the test duration is part or all of the lifetime of the *Neutral* state of hybrid automata.

Both the proposed and the conventional approach can detect thermal problem 8. However, the proposed approach has better performance due to the values of F-Measure and accuracy are all 1s, and 64/83 and 173/192 respectively for the conventional approach. The reason is that the (τ, ε)-closeness approach takes data *type 8* and ② as the thermal problem 8. But data ② will not thermal problem 8. That's why there are 19 false-positive results as shown in Figure 5.17b.

5.3 Conclusion

In this chapter, I proposed to comprehensively detect thermal problems by proposing the multiple-conformance approach with hybrid-automata-modeled requirements. The modeling derived from the example of indoor temperature adjustment service that is represented by automation. It enabled the detection of thermal problems at different time intervals of test duration. The multiple-conformance

approach extended the (τ, ε)-closeness approach [10], which guaranteed the detection of eight thermal problems. It includes five conformance rules that enhanced its ability to detect thermal problems that range from uncomfortable to serious.

I demonstrated the practical effectiveness of our proposal by checking temperature data to detect thermal problems through an experiment. Experimental results prove that thermal problems can be comprehensively detected at different time intervals of test duration. I also adopted the confusion matrix and its related terms to demonstrate the performance of our proposal, in which the results show a higher performance of the proposed method than the (τ, ε)-closeness approach.

6
Safety Problem Prediction

This chapter discusses the prediction of safety problems. As an example, we introduce the detection of heat shock during a bath in Japan. The number of bathroom death due to heat shock has been greater than that in traffic accidents since 2011 in Japan. Countermeasures to heat shock are usually tips and recommendations for people to follow, which may be inefficient for the elderly. It is reasonable to devise a prediction system that can predict and react to heat shock. Conventionally, the prediction of heat-related illnesses is based on thermal-regulation models, which are impractical if only some evidence is observed. In this paper, I employ Bayesian networks to predict heat shock during a bath in smart homes to conquer this problem. To this end, I proposed a procedure to construct the structure of the Bayesian network, and the concept of degree of influence together with the probability scale method to elicit conditional probabilities to construct the Bayesian network. We validate the network by analyzing the sensitivity. Two study cases are conducted to verify the feasibility of the network. I evaluate the advantage of the network in predicting heat shock based on partially observed evidence by comparing it with the thermal-regulation approach.

I summary the contributions of this paper [233]:

- The structure of the prediction system in IoT-based smart homes is proposed.
- I constructed a BN model for predicting heat shock.
- I proposed a procedure to construct the DAG graph based on surveyed knowledge.
- I extended the probability scale method with the degree of influence to mimic experts' behaviors in eliciting conditional probabilities.

6.1 Introduction

According to the vital statistics of the Ministry of Health, Labour and Welfare of Japan*, the number of bathroom death due to heat shock has been greater than that of traffic accidents since 2011. Most of the former are over 65 years old. To prevent heat shock casualty, several countermeasures were concluded from field experiments, for example, set up appropriate bathroom temperature [105, 206], avoid high bathwater temperature [210], thermal insulation of the bathroom [109], and warm up the bathroom [104, 210]. These countermeasures are represented by tips and recommendations which can easily be used to educate people. However, this may be inefficient for the elderly due to the degradation of their physical and mental abilities.

To effectively and timely select appropriate countermeasures, a system that can predict heat shock is necessary. This is enabled by the IoT (Internet of Things)-based smart home systems [22]. The core of such a system is the prediction technology. Conventionally, the prediction of heat-related illnesses, e.g., heatstroke resorts to the modeling of thermal-regulation of the human body. The model presented in [14] evaluates physiological parameters to predict vascular response in a hot environment. A new active-system model was developed in [65] based on regression analysis of physiological responses of unacclimatized subjects. Some other models predict in the temporal dimension, e.g., the system in [224] predicted the thermal environment based on meteorological data, then predicted the heatstroke by the core body temperature prediction system that takes the predicted thermal environment data as inputs. However, the predictions require all input parameters of the model instantiated. Otherwise, it cannot make the prediction.

In the case of predicting heat shock, it is required to know the prediction result before the bather immersing in the bathtub, which means evidence relates to the bath are not observed. One advantage of this is that the prediction system can have sufficient time to react to heat shock. To achieve this, I adopt Bayesian networks (BNs) [32, 86, 162]. BNs are probabilistic graphical models that express causal relationships of a set of variables, based on which and observed evidence to infer uncertain knowledge. There are two reasons to adopt BNs. First, they provide a way of documenting knowledge, i.e., causal relationships of variables and conditional probabilities in a given domain. This documentation ability enables the representation of knowledge about the occurrence of heat shock. Second, BNs can readily process incomplete data set [81]. The inference of BNs can be based on the observed evidence of partial variables. This thus overcomes the problem the prediction based on thermal-regulation models brought about.

Generally, there are three ways to construct a BN, that is, manual construction that depends on the prior expert knowledge, automatic learning that learns from databases, and a hybrid approach that combines the above two [88, 90]. Two constraints make the manual construction the only option for the time being. First, A database with related parameters of the occurrence of heat shock is not available. Second, moral issues restrict us to collect heat shock data through field experiments. However, here comes with another awkward situation, that is, none of us are experts in medicine. To conquer this problem for building the BN for predicting heat shock, I surveyed 32 papers including journals,

*https://www.mhlw.go.jp/english/

conference papers, thesis, and interview articles. Moreover, tons of online materials that aimed to educate people about heat shock are also consulted.

The BN encompasses the directed acyclic graph (DAG) and conditional probabilities. To devise the BN for predicting heat shock, I proposed a procedure to construct the DAG graph and extended a probability elicitation method. The former is based on the surveyed knowledge, which conventionally depends on interviewing related experts [216]. The latter extends the probability scale method [172, 215] with the degree of influence to elicit conditional probabilities. The probability scale method is a direct method that provides a verbal and/or numerical probability scale to experts for eliciting probabilities. Since we are not experts in medicine, the concept of degree of influence is proposed to mimic experts' behavior in eliciting probabilities. The constructed BN was validated by sensitivity analysis. Two experiment cases were conducted to verify the feasibility of the BN in predicting heat shock. A comparison was made between the BN approach and the thermal-regulation approach to demonstrate the advantage of the former in predicting heat shock based on partially observed evidence. Moreover, the BN for predicting heat shock also supports the realization of the prediction system in IoT-based smart homes.

The rest of this chapter is organized as follows. Section 6.2 introduces the prediction system in IoT-based smart homes and the knowledge of heat shock during bath. I construct the BN and then analyze the sensitivity in Section 6.3. Two cases are studied in Section 6.4 with discussions. I finally conclude this paper in Section 6.5 and point out future work.

6.2 Preliminaries

Let us introduce the prediction system in IoT-based smart homes, the relationship of the BN model with the prediction system, and knowledge about heat shock during bathing in this section.

6.2.1 Prediction System

The functionality of the prediction system based on Bayesian networks perform can be taken as a service. The system may be built upon the system architecture shown in Figure 6.1 which I discussed in detail in Chapter 4 [227]. The system can inform related parties in response to a predicted verdict, I thus explicitly illustrate the corresponding architecture components connected by gray arrows.

I briefly introduce every architecture component as follows.

- Home: the living place that equipped with various sensors and actuators.
- Home Gateway: the gateway between the home network and the outside networks. It can execute services, e.g., executable apps to collect data from sensors and issue commands to actuators.
- Service Intermediary: it aggreates services from service providers and distributes them in response to acquisitions from the home gateway.
- Service Provider: it publishes services.

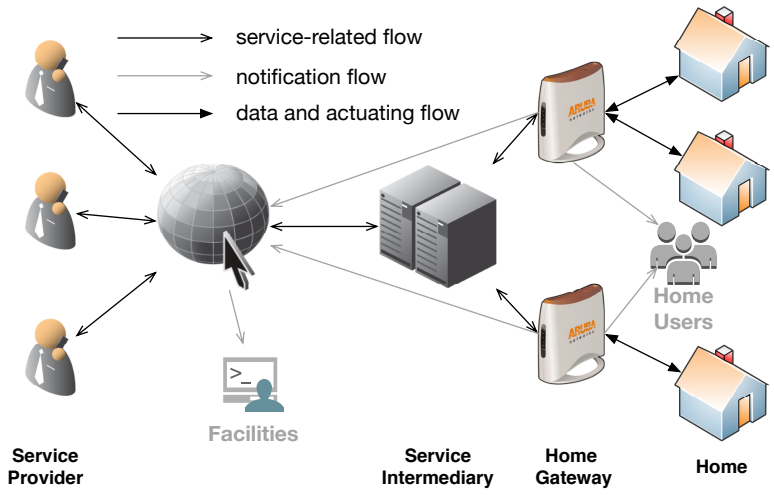


Figure 6.1: The system architecture that supports to build the prediction system.

- Home Users: inhabitants who carry portable terminal, e.g., smart phone that can receive notification.
- Facilities: in the case of heat shock prediction, it can be an emergency center, hospital, etc., which can deal with the heat shock event.

The prediction system gathers various sensor data taken as inputs to the BN to predict heat shock. If the heat shock is likely to occur, the system issues a command to actuators or informs occupants to avert it. System components are depicted in Figure 6.2.

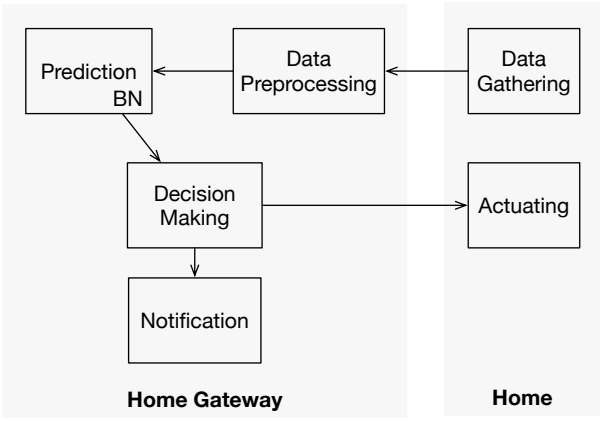


Figure 6.2: System components of the prediction system.

Each component has designated functions.

- Data Gathering: It collects five types of data.
    1. Physical data, e.g., room temperature and bathwater temperature;
    2. Physiological data, e.g., blood pressure variation and heart rate;
    3. Living habits data, e.g., bath frequency and favor of hot bathwater;
    4. Meteorological data when taking a bath, e.g., season and time of day;
    5. Installation data, e.g., window and heater.
- Data Preprocessing: It checks collected data based on rules to generate evidence. For example, if the room temperature bellow 17 °C means cold (rule), then it checks if the room temperature satisfies this rule to generate corresponding evidence, that is cold or not.
- Prediction: The constructed BN works here, which predict the likelihood of heat shock occurrence with evidence as input.
- Decision Making: It decides a response strategy to the predicted result. For example, it issues a command to adjust bathwater temperature, or inform related parties, e.g., home users through the Notification component.
- Actuating: It relates to actuating to change variables of the BN in the real environment so that the probability of heat shock occurrence will decrease.
- Notification: It can inform or warn related parties, e.g., home users and hospitals, about the predicted heat shock.

6.2.2 Heat Shock During Bath

Heat shock is a heat-related illness that resulted from a sudden extreme temperature change that is usually over 10°C. This brief introduction is based on a survey of 32 publications and tons of online materials with the keyword heat shock and its Japanese translation.

Bathroom death due to heat shock in Japan mostly happens in winter. Although the pathology of heat shock is still unclear [44], there are still physiological and environmental factors that can be taken as indicators of heat shock occurrence. Japanese people are fond of a hot bath. The dressing room and bathroom usually have no air-conditioning unit, and thus are cold in winter (usually bellow 17°C). When people undressed and immersed in a cold environment, the systolic blood pressure and heart rate increase. Then, people quickly go into the bathtub and immerse themselves in the hot bathwater to keep warm. At this time, the systolic blood pressure decreases, and the heart rate may maintain a high level. After the bath, they go into the cold environment again, and the systolic blood pressure increases again, and the heart rate decreases.

People may drown in the bathwater since the blood pressure variation can cause unconsciousness. Moreover, other diseases like arrhythmia, cardiovascular diseases, cerebral hemorrhage, and myocardial infarction, etc. may be caused during the bathing process. The aging population and people who

drink before bath are the most sensitive groups to heat shock, and take a large proportion of bathroom death due to heat shock.

6.3 Bayesian Network Construction

This section discusses the construction of BN for predicting heat shock. A brief introduction of Bayesian networks will be given first. Then, the building of the BN, including structure construction and probability elicitation, will be discussed in detail. Last, I analyze the sensitivity of the constructed BN.

6.3.1 A Brief Introduction of Bayesian Networks

BNs [32, 86, 162] are probabilistic graphical model which represent joint probability distributions of a set of variables in a given domain. Formally, a BN is defined as a two-tuple

$$BN = (\mathbb{G}, P) \tag{6.1}$$

where $\mathbb{G}$ is the directed acyclic graph (DAG), and P is the joint probability distribution that can be represented by conditional probability table. $\mathbb{G}$ satisfies $\mathbb{G} = (\mathbb{V}, \mathbb{E})$, where $\mathbb{V}$ is a set of nodes that denote variables, and $\mathbb{E}$ is a set of directed edges that connect the nodes, and $\mathbb{E} \subseteq \mathbb{V} \times \mathbb{V}$. The joint probability distribution factorize into conditional probabilities and marginal probabilities. Let us use upper case letters to represent variables and lower case letters to denote values of variables. So, the joint probability of variable $V_1, V_2, ..., V_n$ can be represented as

$$P(V_1, V_2, ..., V_n) = \prod P(V_i|\pi(V_i)) \tag{6.2}$$

where $\pi(V_i)$ denotes the parent nodes of V_i, and $V_i \in \mathbb{V}$. $P(V_i = v_i|\pi(V_i))$ defines the conditional probability table.

Given a target variable $V \in \mathbb{V}$, I want to predict the probability that V is in some state $V = v$. The prediction is achieved when the probability of the target node is updated once some other nodes in the BN have observed evidence. This process can be achieved by Bayes theorem, i.e.,

$$P(A|B) = \frac{P(B|A)P(A)}{P(AB)} \tag{6.3}$$

where A and B are nodes in the BN. Luckily, many tools can help people to do this tedious work. I adopt GeNie modeler[†] in this work to assist in constructing the BN for predicting heat shock.

Figure 6.3 illustrates the constructed Bayesian network for predicting heat shock. Let us give a detail discussion on the construction of it in the following two sections.

[†]It is available free of charge for academic research and teaching use from BayesFusion, LLC, http://www.bayesfusion.com

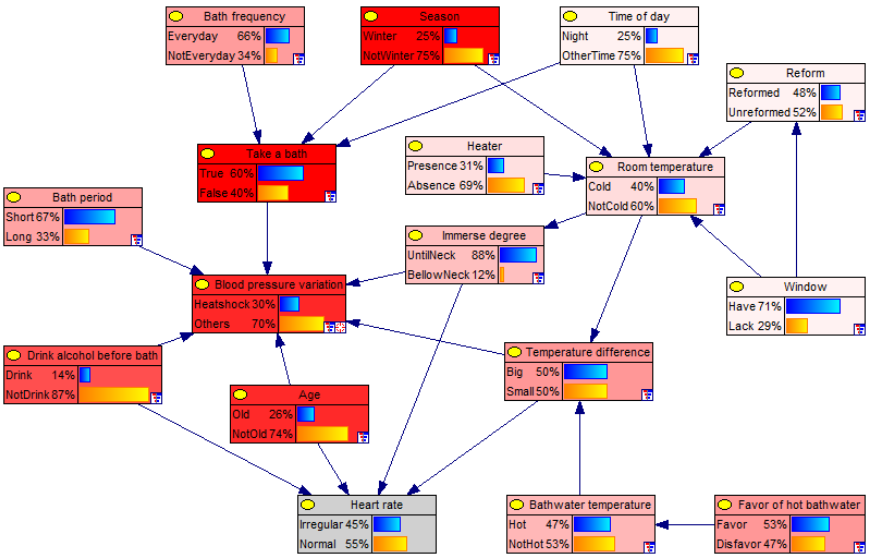


Figure 6.3: A Bayesian network for heat shock prediction, which the red-colored nodes are sensitive to the occurrence of heat shock.

6.3.2 Structure Construction

This section introduces the way of constructing the DAG graph, which is based on the surveyed knowledge of heat shock. To this end, I propose a construction procedure that is shown in Figure 6.4.

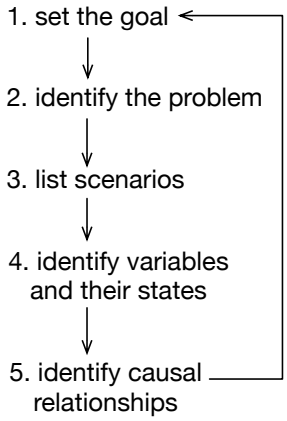


Figure 6.4: The procedure for constructing the DAG graph.

The use of BNs can have various purposes, e.g., knowledge identification [91] and prediction [113]. It is thus necessary to set the goal of adopting BNs in step one. I employ BNs for prediction. Then

in step two, let us identify what to predict, i.e., prediction of heat shock during bath. It can predict the likely an occupant go to take a bath and the probability of heat shock if the occupant did go to take a bath. The constructed BN also has to support real-time prediction in the prediction system introduced in Section 6.2.1. In step three, I list possible scenarios related to heat shock. To do this, let us first summarize the key findings of the surveyed articles. Then I enumerate scenarios of heat shock occurrence concerning these findings. The scenarios are in two dimensions, i.e., temporal and spatial. The temporal dimension is with the process of bathing, which is undressing, bathing, and redressing. The spatial dimension is at a specific event time point, e.g., bathing or undressing. Next, let us identify variables and their states in step four based on the results of step three. Heat shock as a heat-related illness cannot be directly observed. Let us identify observable variables that represent the symptoms of heat shock and environmental factors. So their data can be collected through sensors. Blood pressure variation is an optimal symptom to indicate heat shock, and its fluctuation should within ± 10 mmHg [105]. I also use the heart rate as a supplemental symptom to heat shock. Step five is to connect the variables concerning their causal relationships. These causal relationships can be derived from the identified scenarios in step three. This construction procedure is a repetitive process until all relevant scenarios are reasonably represented by the DAG graph. The determination of reasonable representation depends on the competence and insight of the people who construct the BN. The variables with their states and connections are illustrated in Figure 6.3. Some states of variables may be incomprehensible by the names, and I explain them in Table 6.1.

6.3.3 Probability Elicitation

The conventional way of eliciting probability through manual construction is the probability scale method [172, 215]. It is a direct method, where domain experts are asked to mark their degree of belief on the probability scale to elicit probability. This method relies heavily on experts, which are extravagant resources to the authors. Therefore, let us first give a brief introduction of the method, then introduce the concept of degree of influence to mimic experts' behavior in eliciting probabilities.

The probability scale method encompasses two essentials, i.e., the probability scale and experts. The expertise and rich experience are focused characters for the latter. The probability scale is a horizontal or vertical line with numerical and/or verbal anchors. Figure 6.5 illustrates an example of a probability scale with five numerical anchors. The verbal anchors like frequent, rare, or other descriptive text on the probability scale are to assist experts who have difficulty in understanding mathematical notations of conditional probability. Since the authors are familiar with these mathematical notations, the probability scale with numerical anchors was adopted.

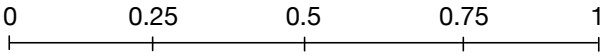


Figure 6.5: An example of probability scale with numerical anchors.

Degree of influence describes the strength of condition influences on the occurrence of an event.

Table 6.1: State explanation of some incomprehensible variables of the BN.

Variable	State	Explanation
Bath period	Short	The bath period is less than 10 min
	Long	The bath period is more than 10 min
Age	Old	The one who is over 65 years old
	NotOld	The one who is less than 65 years old
Blood pressure variation	Heatshock	An indication of heat shock, and the blood pressure is changed beyond 10 mmHg
	Others	Other situations rather than the Heatshock
Room temperature	Cold	The temperature of dressing room and bathroom is bellow 17 °C that is the minimum tolerable temperature
	NotCold	The temperature is above 17 °C
Reform	Reformed	The window is reformed for heat insulation
	Unreformed	The window is not reformed
Temperature difference	Big	The difference between room temperature and bathwater temperature is 10 °C and above
	Small	The temperature difference is smaller than 10 °C
Bathwater temperature	Hot	Bathwater temperature is 41 °C and above
	NotHot	Bathwater temperature is less than 41 °C
Heart rate	Irregular	The heart is irregularly beat due to heat shock, e.g., bradycardia and palpitation
	Other	Other situations

For a conditional probability

$$P(X = x|\pi(X)) \tag{6.4}$$

the state of $\pi(X)$ affects the probability of $X = x$. The degree of influence is to represent this probability. Given the probability, as shown in Equation 6.4, let us follow the recursive procedure bellow with considering the probability scale and degree of influence to elicit the probability.

1. Find the least or most likely, i.e., find a state of $\pi(X)$ in its state space, under which $X = x$ is the least or most likely to occur. This is the first step, since finding the least or most probability is easier.

2. Mark the probability on the probability scale either approach 0 or 1.

3. For the rest states of $\pi(X)$, the influence on the probability of $X = x$ becomes weaker or

stronger by comparing with the previously identified state. Choose the state of $\pi(X)$ that has a one-step weaker or stronger influence by comparing it with the state in the previous step. $\pi(X)$ may have one or more variables with multiple states, the one-step weaker or stronger influence means only change a state of a variable at a time. The determination of weaker or stronger depends on expertise.

4. Mark the probability on the probability scale, and go to step three until all states of $\pi(X)$ are enumerated.

To better understand the procedure, I give the following example. For the node *Blood pressure variation* in Figure 6.3, the conditional probability

$$\begin{aligned} P(&\textit{Blood pressure variation} = \textit{Heatshock} | \textit{Take a bath} = \textit{true}, \textit{Age} = \textit{Old}, \\ &\textit{Temperature difference} = \textit{Big}, \textit{Bath period} = \textit{Long}, \\ &\textit{Immerse degree} = \textit{UntilNeck}, \textit{Drink alochol before bath} = \textit{Drink}) = 0.98 \end{aligned}$$

is the most likely that *Blood pressure variation* = *Heatshock*. So, the conditional probability condition on the one-step weaker condition can be

$$\begin{aligned} P(&\textit{Blood pressure variation} = \textit{Heatshock} | \textit{Take a bath} = \textit{true}, \textit{Age} = \textit{Old}, \\ &\textit{Temperature difference} = \textit{Big}, \textit{Bath period} = \textit{Long}, \\ &\textit{Immerse degree} = \textit{UntilNeck}, \text{Drink alochol before bath=NotDrink}) = 0.83 \end{aligned}$$

Only the state of variable *Drink alcohol before bath* changed from *Drink* to *NotDrink*, which weakened the influence on the probability of heat shock occurrence. It is expected that the degree of influence can also conquer expert bias [172] to some degree by comparing with solely experts' belief in eliciting conditional probabilities.

6.3.4 Sensitivity Analysis

Sensitivity analysis [47] of a BN is to study the effects of conditional probabilities of the network on a target probability. I employ it to validate the constructed BN by checking the variables that affect blood pressure variation. It checks the degree of variation of the target probability with varying other probabilities of the network. The GeNie modeler supports sensitivity analysis. Nodes in red represent the corresponding variables that are sensitive to the target node. It varies up to 10% (default setting of the GeNie modeler) of the current probability values to check the sensitivity.

Let us set the node *Blood pressure variation* as the target node, in which the result is shown in Figure 6.3. It is easy to understand that *Take a bath* with its parent nodes, i.e., *Bath frequency*, *Season*, and *Time of day* have an effect on the occurrence of heat shock during bath. Without taking a bath, bathroom death due to heat shock will not occur. *Bath period*, *Age*, *Batwater temperature*, and *Room temperature* are sensitive to heat shock occurrence, which are findings in [197]. *Drink alcohol before bath* has been found as a factor that affects the occurrence of heat shock in [194]. Others like *Immerse*

degree, *Temperature difference* have also been found factors that affect heat shock occurrence. These findings in the literature validated the constructed BN.

In the viewpoint of engineering to enable the prediction system introduced in Section 6.2.1, the Actuating component can control those controllable variables that are sensitive to the occurrence of heat shock to achieve an efficient and effective result. This is due to a small variation of these variables will have a great impact on the likelihood of heat shock occurrence. One deficiency might be that according to the definition of heat shock *Temperature difference* should be very sensitive to the *Blood pressure variation*. However, the BN in Figure 6.3 does not show that intensity. As the *Temperature difference* is colored in light red.

6.4 Case Study and Discussion

This section will introduce two study cases to verify the feasibility of the constructed BN. I also compare the prediction results with the prediction by using the thermal-regulation approach. The two cases refer to that bathroom death due to heat shock will occur (case one) and will not occur (case two). For timely inform people or take actions to prevent the occurrence of heat shock, let us make a prediction before immersing the bather in the bathtub. This indicates the evidence related to bath, i.e., *Bath period*, *Immerse degree*, *Bathwater temperature*, and *Temperature difference* are not observed. The results are shown in Figure 6.6 and 6.7.

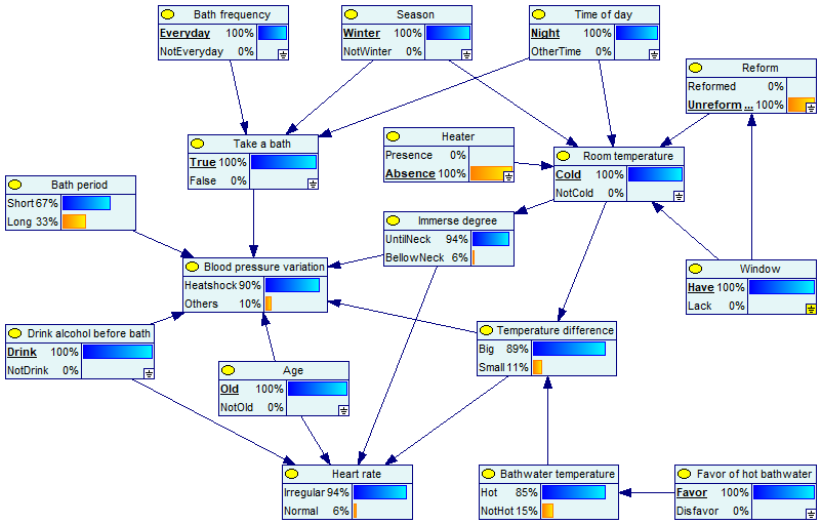


Figure 6.6: The prediction result of case one.

As for the result illustrated in Figure 6.6, the probability of heat shock is 90%. This is supported by the probability of *Heart rate* in *Irregular* state is 94%. It is thus, can be concluded that the occurrence of heat shock is predicted correctly. The prediction result shown in Figure 6.7 illustrates the probability of heat shock occurrence is 37% and the probability of *Hear rate* in *Irregular* state is

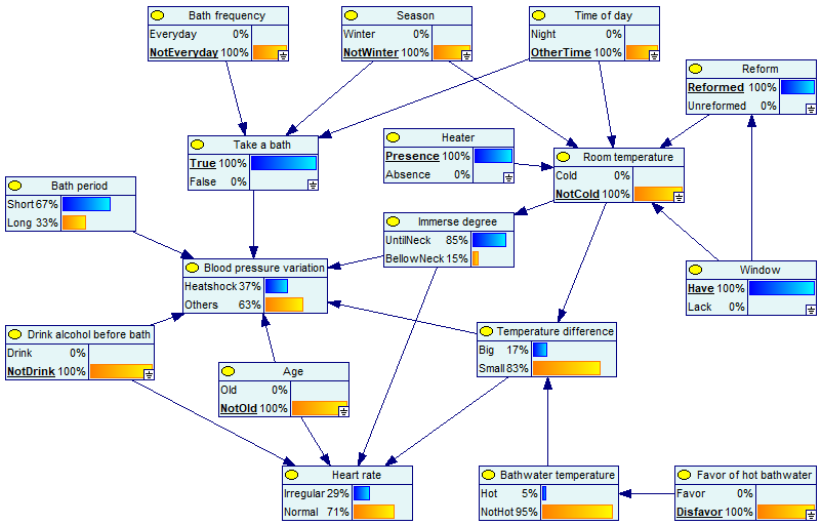


Figure 6.7: The prediction result of case two.

29%. The constructed BN thus correctly predicted that the heat shock would not occur. These illustrate the methods, that is, the proposed procedure in constructing the DAG graph and the probability elicitation method in constructing the BN are effective.

The nodes (variables) in the constructed BN are observable so that their values can be collected through various sensors in the Data Gathering component of the prediction system discussed in Section 6.2.1. Sensors here can be anything that collects data. For example, temperature sensors, and databases that keep updating living habits data can be this kind of sensors.

It is expected to compare the results of case one and case two with the prediction by using a thermal-regulation model specifically for heat shock. However, such a thermal-regulation model does not exist for the time being. Since thermal-regulation models for heat-related illnesses are represented by formulas [14, 65, 224], it is reasonable to assume that such a model can be represented as in Equation 6.5.

$$TR_{heatshock} = f(living\ habit, physiology, bath, physical, etc.) \tag{6.5}$$

where *living habit* denotes parameters relate to daily life, e.g., bath frequency, *physiology* represents physiological parameters, e.g., heart rate, *bath* means bath related parameters, e.g., immerse degree, *physical* are physical parameters, e.g., room temperature, and there may be other parameters that are omitted here.

Based on the conditions in case one and case two, the evidence related to *bath* was not observed, it is, therefore, cannot directly predict heat shock by using Equation 6.5. So the BN approach has an advantage in predicting heat shock with only observe some evidence. It is a better approach to implement the prediction system by comparing it with the thermal-regulation approach.

6.5 Conclusion

A BN model for predicting the occurrence of heat shock during a bath was proposed. The DAG graph of the BN was constructed by following a proposed procedure based on the surveyed knowledge of heat shock. The conditional probabilities were elicited by the probability scale method and the proposed concept of degree of influence. Then, I analyzed the sensitivity to validate the constructed BN. Two simulation cases were conducted to verify the feasibility of using the constructed BN in predicting heat shock. Finally, a comparison was made with an envisioned thermal-regulation model for heat shock, in which the results demonstrated that the BN approach has advantages in predicting heat shock with partially observed evidence. It is thus an optimal option for implementing the prediction system.

7 Conclusion and Future Work

The goal of my Ph.D. project concerns home environment safety. It mainly dealt with home safety problem detection and prediction. Home safety problems happen in the home environment between home users and various home appliances. The causes of home safety problems are due to abnormal behaviors of smart home systems under severe outdoor climate, e.g., heatwaves. Smart home systems failed to adjust the indoor climate to a safe level, and thus caused morbidities or even casualties. I divide my work into four main parts. The first is to understand indoor safety problem formation that connects the physical world and the cyber world, comprehensively. Then I proposed a hazard analysis technique, i.e., tailored STPA to identify Defects. The second is that I proposed a home safety architecture to support safety problem detection/prediction and reactions. In this dissertation, I left the work related to precautionary and reaction measures to the future. The third is physical process anomaly detection. To this end, I adopted conformance testing and hybrid automata to check indoor temperature change to detect anomalies that will cause thermal discomfort as well as health problems. Last, I adopted Bayesian networks to predict heat shock during baths for the elderly.

I summary the work has been done and figure out possible future work as in the follows:

1. In Chapter 2, I first proposed the concept of Performers System, based on which I defined terms like Service. Then terms related to Service are defined to comprehensively illustrate safety problem formation that connects the physical world and the cyber world.

   The accident model is to describe accident formation concerning the Behavior of the Performers System with physical processes. Other forms of indoor accident formation may be different from the proposed one. When coming to a new safety problem, it is expected to propose a new model or alter existing ones.

2. In Chapter 3, for identifying the causes in the cyber world that cause indoor climate anomalies, I tailored the hazard analysis technique STPA to also identify ICAs that cause Service Failures. For representing the relations of analytical results clearly and straightforwardly, I proposed an

LGLD approach. I also practiced applying an innominate approach for hazard identification, which is based on the goal-based requirement engineering, guide words, and item sketch.

System safety aims to make systems and single products work safely. Integrated services might involve various independent Performers that behave unpredictably. Therefore, how to ensure their functional safety can be future work. This can be divided into three problems. The first is product safety, e.g., electric/electronic product safety. Second, single system safety. Third, system cooperation safety. Different integrated services may involve more than one system and may have conflict functions. Therefore, they are supposed to no only work to comply with their safety designs but also cooperate safely.

3. In Chapter 4, a CPS home safety architecture was proposed that can support the detection/prediction, and reaction to safety problems.

   Collaboration with other systems is not considered yet. For example, detecting or predicting results may have conflicts with other systems' normal functioning. The other systems are various, and this may involve in different projects. Reaction services relate to the research area of cybernetics that is a different research area by comparing it with the current research topics. I thus left this to the future.

4. In Chapter 5, I proposed a multiple-conformance approach that takes the hybrid-automata-modeled requirement as the specification. It can detect safety problems of Service Failure and Hazard.

   Science benefits lives through the way of making it real, i.e., implementing it. So, the future work for this part could be to implement a system that can detect for example indoor temperature anomalies.

5. In Chapter 6, I adopted Bayesian networks to predict heat shock during a bath. To this end, I proposed a procedure to construct the DAG graph of Bayesian networks with concerning the surveyed knowledge of heat shock. I also proposed a method to elicit conditional probabilities. This method is based on the probability scale method and the proposed concept of degree of influence.

   It is expected to introduce doctors in medicine to help in eliciting probabilities to increase the accuracy of the constructed Bayesian network. I would also like to implement a system based on the constructed Bayesian network to predict heat shock in real time.

A

Services and Functions of Home Appliances

Table A.1: Functions of home appliances in different rooms (to be continued in Table A.2 and A.3)

Areas	Category	Appliances	Functions	Service
Entrance Hall	Security	Electric Door	Lock/unlock the door including remote controls; checking the status of the door; open and close automatically	Access control by authenticating the "keys"; open and close the door
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment
Living Room	Entertainment	TV	Receives contents from remote or local resources then display contents onto the display and plays sound simultaneously	Plays video information; volume control
		Projector	Projects contents onto a projection screen	Plays video information
		Speaker	It converts an electrical audio signal into sound	Volume control
		Stereo	It converts an electrical audio signal into a corresponding sound with high quality	Volume control
	Ventilation	Air Purifier	It removes contaminants from the air. E.g., airborne pollutants, odors, volatile organic compounds and microorganisms that cause disease	Purify contaminants from the air
		Dehumidifier	It reduces the level of humidity in the air, eliminates musty odor	It reduces humidity level; eliminates musty odor
		Electric Window	Open and close including remote control; check the status of a window	Air-interchange between indoor and outdoor
		Air Conditioner	Cooling, heating, dehumidification	Temperature control; airflow control; dehumidification
		Electric Fan	Indoor airflow and airflow rate control	Adjust room air circulation; cool down
		Humidifier	It increases indoor humidity	It increases humidity level
		Space Heater	It warms a small space	Warm up
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment
		Electric Curtain	Open and close including remote control; check the status of a curtain	Luminance adjustment
		Window Shade	Open and close including remote control; check the status of a shade	Luminance adjustment
	Cleaning	Vacuum cleaner	Suck up dust and dirt from a surface like floor	Clean a surface like floor
	Security	Surveillance camera	It transmits live video and audio information to remote place	It provides indoor view for remote monitoring

Table A.2: Functions of home appliances in different rooms (continues Table A.1 and to be continued in Table A.3)

Areas	Category	Appliances	Functions	Service
Kitchen	Storage	Refrigerator	It maintains a cool or cold temperature for food storage	Temperature control for food storage
		Freezer	It maintains a cold temperature for food storage	Temperature control for food storage
	Ingredient Processing	Blender	Mix food	Mix food
	Heating	Cooktop	Direct heat for cooking	Temperature control for cooking
		Electric Range	Direct heat for cooking by conventing electric into heat	Temperature control for cooking
		Microwave Oven	It heats food	Temperature control for heating food
		Electric Kettle	It boils water by using electrical energy	Temperature control for boiling water
		Coffee Maker	It brews coffee with modes like regular or strong brew; keep warm	Brew coffee; keep warm
		Slow Cooker	It maintains a relatively low temperature for simmering; keep warm	Temperature control for simmering food; keep warm
		Pressure Cooker	Cooking with the high pressure; reduced cooking time; keep warm	Temperature control with high pressure for cooking; keep warm
		Rice Cooker	It boils or steams rice; keep warm	Temperature control for boiling or steaming rice; keep warm
		Water Boiler	It boils water; maintains water at a constant temperature	Temperature control for boiling water; keep warm
		Toaster	It makes bread	Temperature control for toasting bread
		Steamer	It cooks or prepares various foods with steam heat	Temperature control with steam for heating food
	Cleaning	Dishwasher	It cleans dishes and eating utensils by spraying hot water	It cleans dishes and eating utensils by spraying hot water
		Garbage Disposal	It shreds food waste into pieces	It shreds food waste into pieces
	Ventilation	Range Hood	It removes airborne grease, combustion products, fumes, smoke, odors, heat, and steam from the air by evacuation of the air and filtration	Indoor air cleaning by exhausting air
		Electric Window	Open and close including remote control; check the status of a window	Air-interchange between indoor and outdoor
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment
		Window shade	Open and close including remote control; check the status of a shade	Luminance adjustment
Wash Room	Laundry	Washing Machine	It washes clothes with predefined programs for different laundry types	Wash; spin-dry
		Cloth Dryer	It removes moisture from a load of clothing shortly after they are washed in a washing machine	Temperature control; humidity control
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment
	Ventilation	Electric Fan	Indoor airflow and airflow rate control	Adjust room air circulation; cool down; ventilation
		Electric Window	Open and close including remote control; check the status of a window	Air-interchange between indoor and outdoor

Table A.3: Functions of home appliances in different rooms (continues Table A.2)

Areas	Category	Appliances	Functions	Service
Bedroom	Entertainment	TV	It receives content from remote or local resources, then displays contents onto the display and plays sound	Plays video and audio information
	Ventilation	Air-conditioner	Cooling, heating, dehumidification	Temperature control; airflow control; dehumidification
		Air Purifier	It removes contaminants from the air E.e., airborne pollutants, odors, volatile organic compounds, and microorganisms that cause disease	Improve air quality by removes contaminants
		Dehumidifier	It reduces the level of humidity in the air; eliminates musty odor	Dehumidification; eliminates musty odor
		Humidifier	It increases indoor humidity	Increases humidity level
		Space Heater	Warm a small space	Warm up
		Electric Window	Open and close including remote control; check the status of a window	Air-interchange between indoor and outdoor
	Lighting	Electric Curtain	Open and close including remote control; check the status of a curtain	Luminance adjustment
		Lamp	Ambient lighting; dimming	Luminance adjustment
	Cleaning	Vacuum Cleaner	Suck up dust and dirt from a surface like floor	Clean a surface like floor
Toilet	Ventilation	Ventilator	Exchange of air with outdoor; air circulation	Improve air quality by exhausting air; circulation of air
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment
Wash Room	Laundry	Washing Machine	It washes clothes with predefined programs for different laundry types	Wash; spin-dry
		Cloth Dryer	It removes moisture from a load of clothing shortly after they are washed in a washing machine	Temperature control; humidity control
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment
	Ventilation	Electric Fan	Indoor airflow and airflow rate control	Adjust room air circulation; cool down; ventilation
		Electric Window	Open and close including remote control; check the status of a window	Air-interchange between indoor and outdoor
Bathroom	Heating	Water Heater	It transforms energy resources to heat water for bath	Temperature control for heating water
	Ventilation	Ventilator	Exchange air with outdoor; air circulation	Temperature control for heating water
		Bathroom Heater	It warms the bathroom to a comfortable level for bath especially in winter	Warm indoor temperature
	Lighting	Light Fixture	Ambient lighting; dimming	Luminance adjustment

Table A.4: Services related to the functions of home appliances

Categories	Appliances	Services	Service Details
Security	Electric Door	Access control	Authenticates the "keys"
		Automatic control of the door	Open the door
			Close the door
	Surveillance Camera	Provide indoor view for remote monitoring	Image display
			Volume up
			Volume down
			Maintains a volume level
Lighting	Light Fixture	Luminance Adjustment	Maintains a certain brightness
	Electric Curtain		Increases brightness
	Window Shade		Decreases brightness
	Lamp		
Entertainment	TV	Plays video contents	Image display
		Volume Control	Volume up
			Volume down
			Maintains a volume level
	Projector	Plays video information	Image display
	Speaker	Volume Control	Volume up
	Stereo		Volume down
			Maintains a volume level
Ventilation	Air Purifier	Air Purification	Removes airborne pollutants
			Reduces odors
			Absorbs volatile airborne pollutants
			Kills microorganisms that cause disease
	Dehumidifier	Humidity Regulation	Reduces humidity level
		Air Purification	Eliminates musty odor
	Electric Window	Air Circulation	Increases airflow rate
		Temperature control	Cool down
	Air Conditioner	Temperature control	Warm up
			Cool down
			Maintains a certain temperature
		Air Circulation	Increases airflow rate
			Decreases airflow rate
		Humidity Regulation	Reduces humidity level
	Electric Fan	Air circulation	Increases airflow rate
			Decreases airflow rate
			Change airflow direction
		Temperature control	Cool down
	Humidifier	Humidity Regulation	Increases humidity level
	Space Heater	Temperature control	Warm up
	Range Hood	Air Purification	Exhausts heat, steam, odors, fumes, etc.
			Filtrates airborne grease, smoke, combustion products
		Humidity Regulation	Reduces humidity level
	Ventilator	Air Purification	Exhausts heat, steam, odors, fumes, etc.
		Air Circulation	Increases airflow rate
		Humidity Regulation	Reduces humidity level
	Bathroom Heater	Temperature control	Warm up
Cleaning	Vacuum Cleaner	Cleans a surface like floor	Suck up dust and dirt
	Dishwasher	Cleans dishes and eating utensils by spraying hot water	Washing-up
	Garbage Disposal	Shreds food waste into pieces	Shreds food waste into pieces
Storage	Refrigerator	Temperature control	Maintains a certain temperature
	Freezer		Cool down
Heating	Cooktop	Temperature control	Heat up
	Electric Range		
	Microwave Oven		
	Electric Kettle		
	Coffee Maker	Brews coffee	Brews coffee
		Temperature control	Maintains a certain temperature
	Slow Cooker	Temperature control	Heat up
	Pressure Cooker		
	Rice Cooker		Maintains a certain temperature
	Water Boiler		
	Toaster	Temperature control	Heat up
	Steamer		
	Water Heater		
Laundry	Washing Machine	Wash	Washes clothes
		Spin-dry	Spin-dry
	Clothes Dryer	Temperature control	Heat up
		Humidity Regulation	Reduces humidity level

B

The Relationships of the Various Terms

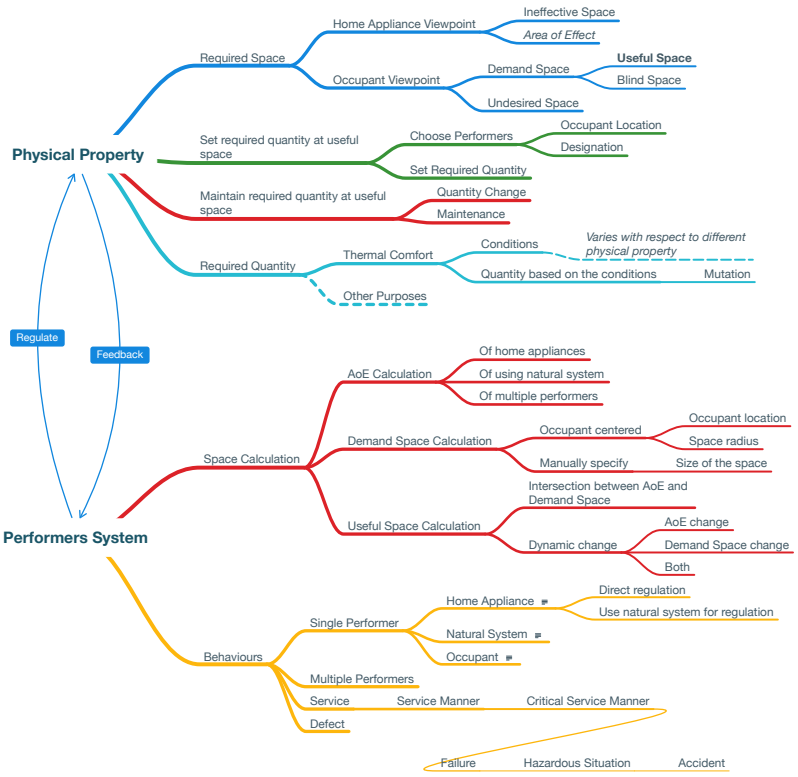
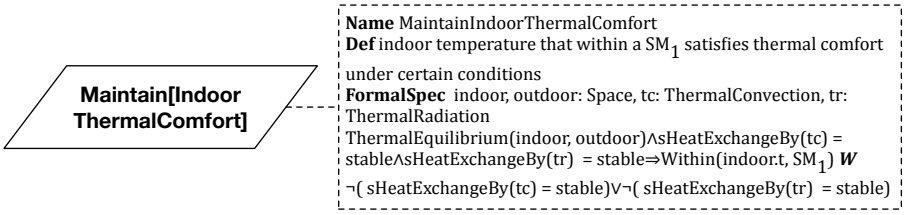


Figure B.1: The relationships of the various terms.

C

The Annotations of the Goals in the Goal Models Shown in Figure 3.6 and 3.7

1. Indoor thermal comfort is maintained in the situation that indoor temperature is smaller than outdoor temperature. For example, heatwaves and very hot summer.

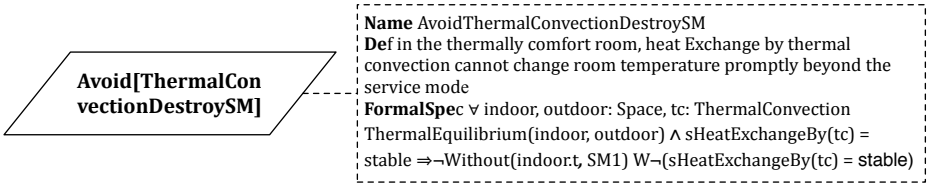


   (a) Object: Space, ThermalConvection, ThermalRadiation

   (b) Function: *Within*(*Room.InTemp*, *Room.SMinTemp*): Whether the InTemp is within the SMinTemp.
   sHeatExchangeBy(*HeatTransfer*): the state of heat Exchange by ways of heat transfer (HeatTransfer).
   HeatTransfer can be instance of *ThermalConvection*, *ThermalRadiation* and other heat transfer mechanisms.
   ThermalEquilibrium(*obj*1, *obj*2) denotes limited heat exchange between *obj*1 and *obj*2 that cannot change their system states. In other words, the temperature of *obj*1 and *obj*2 are stabilized in a predefined range

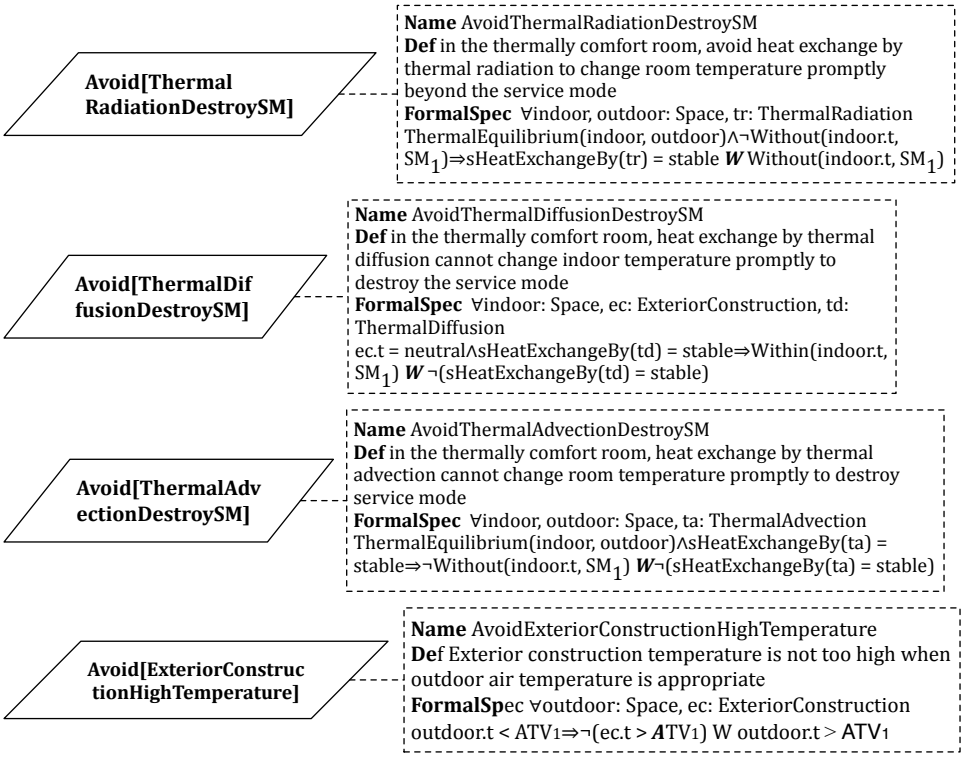
   (c) Note: Thermal neutrality is maintained when heat generated by human metabolism is allowed to dissipate, thus maintain thermal equilibrium with the surroundings. (From Wikipedia [thermal comfort])

(d) SM1 means a service mode



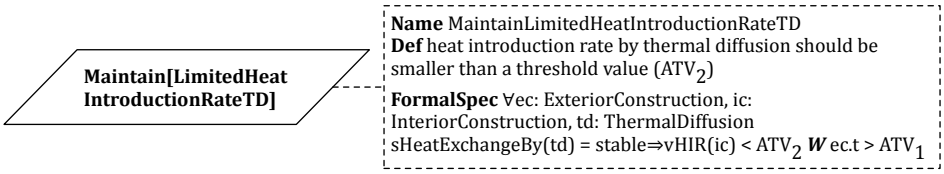
(a) Note:

$$HeatExchangeBy(ThermalConvection) \Leftrightarrow HeatExchangeBy(ThermalDiffusion) \wedge HeatExchangeBy(ThermalAdvection)$$



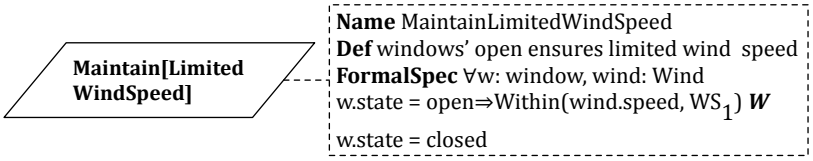
(a) outdoor.t represents outdoor temperature

(b) ATV stands for a threshold value

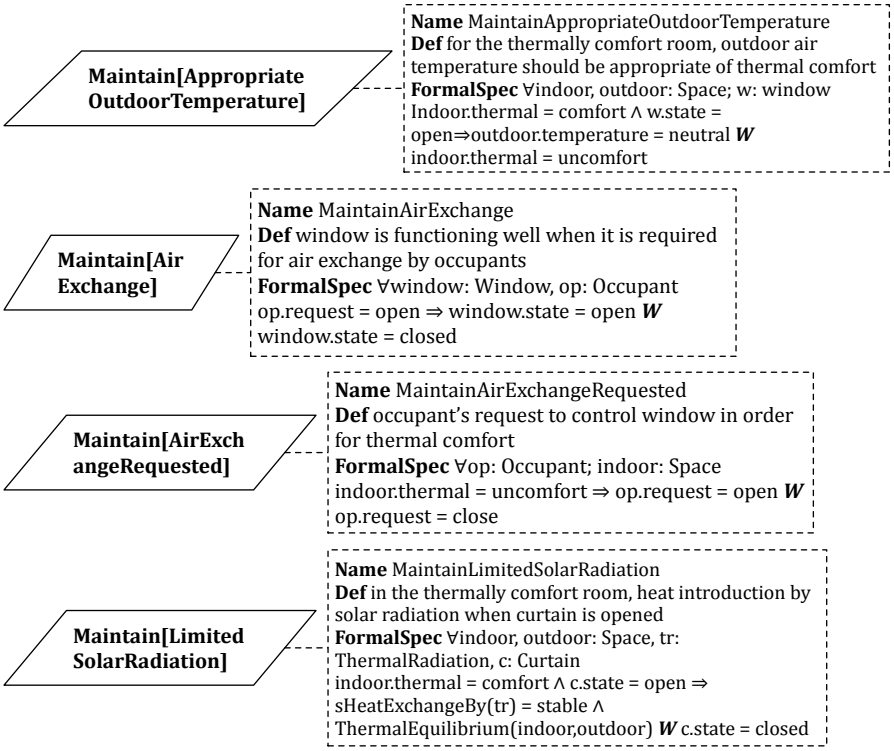


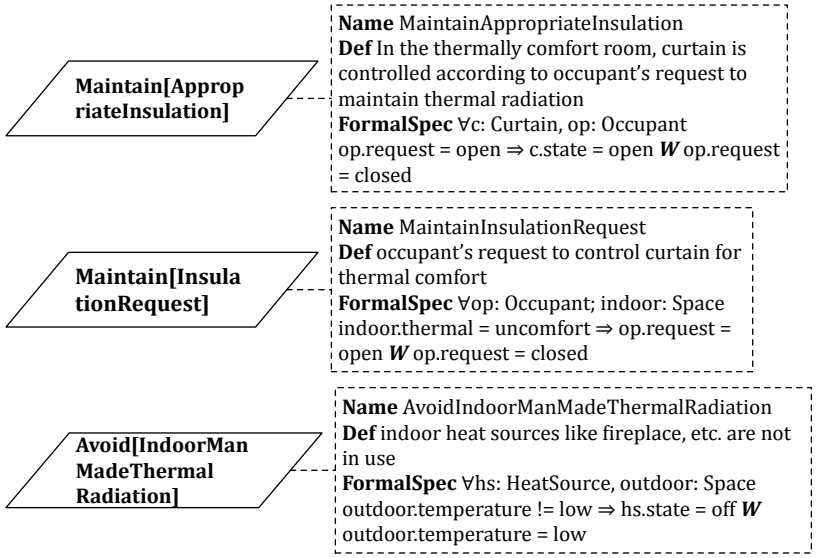
(a) Function: $vHIR(ic)$ means the value of Heat Introduction Rate through interior construction

(b) The focus is on how much heat can be gained by the indoor environment, that is why use introduction rate instead of exchange rate

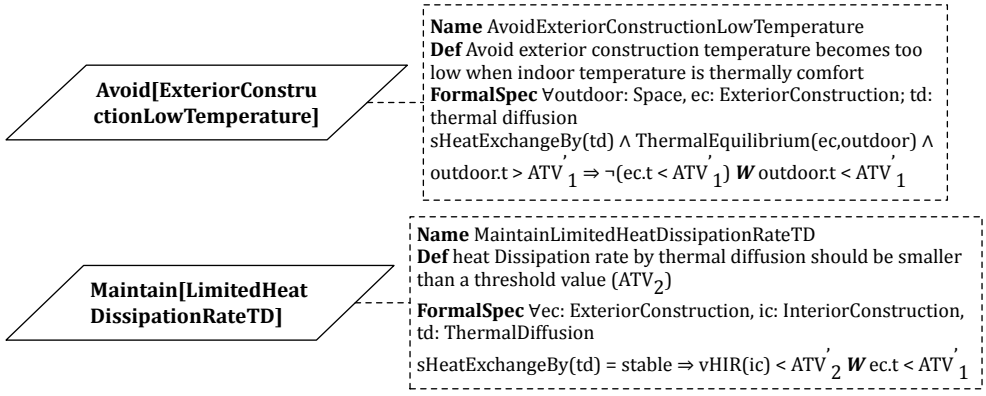


(a) WS_1 means an interval of appropriate value of wind speed

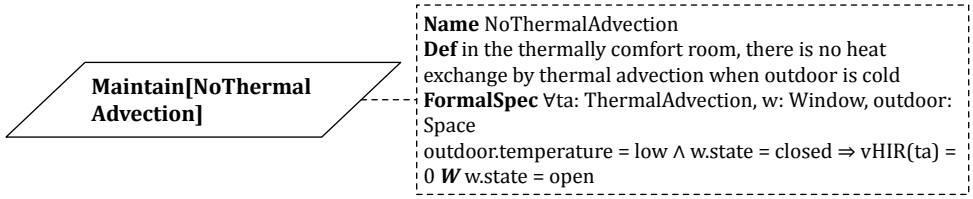


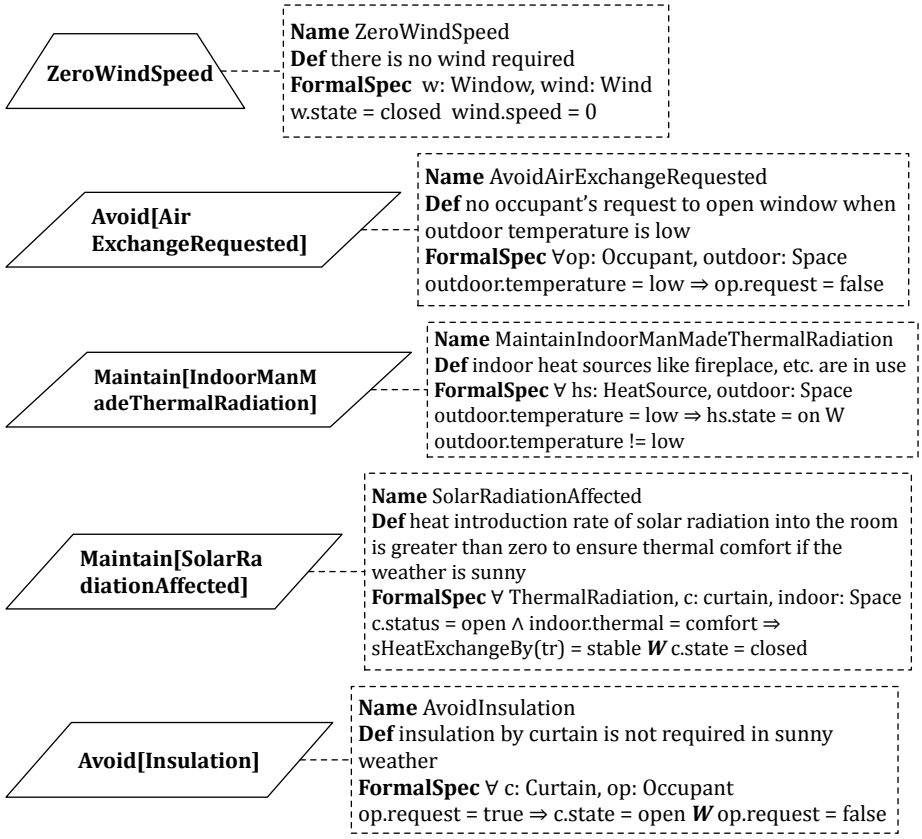


2. Indoor thermal comfort is maintained in the situation that indoor temperature is greater than outdoor temperature. E.g. in cold winter. Some goals listed in the goal model are the same as listed above that are not depicted bellow.



(a) Heat Dissipation Rate equals Heat Introduction Rate in value, except opposite heat transfer direction




ZeroWindSpeed
Name ZeroWindSpeed
Def there is no wind required
FormalSpec w: Window, wind: Wind
w.state = closed wind.speed = 0
Avoid[Air ExchangeRequested]
Name AvoidAirExchangeRequested
Def no occupant's request to open window when outdoor temperature is low
FormalSpec ∀op: Occupant, outdoor: Space
outdoor.temperature = low ⇒ op.request = false
Maintain[IndoorManMadeThermalRadiation]
Name MaintainIndoorManMadeThermalRadiation
Def indoor heat sources like fireplace, etc. are in use
FormalSpec ∀ hs: HeatSource, outdoor: Space
outdoor.temperature = low ⇒ hs.state = on W
outdoor.temperature != low
Maintain[SolarRadiationAffected]
Name SolarRadiationAffected
Def heat introduction rate of solar radiation into the room is greater than zero to ensure thermal comfort if the weather is sunny
FormalSpec ∀ ThermalRadiation, c: curtain, indoor: Space
c.status = open ∧ indoor.thermal = comfort ⇒
sHeatExchangeBy(tr) = stable W c.state = closed
Avoid[Insulation]
Name AvoidInsulation
Def insulation by curtain is not required in sunny weather
FormalSpec ∀ c: Curtain, op: Occupant
op.request = true ⇒ c.state = open W op.request = false

D

The NuSMV Code for Verifying Goal Refinement

```
/-- This file contains the description of the FSM of the goal
    model of indoor temperature. And it is used for the
    verification of the goal model refinement.
For the modeling of indoor temperature, an input language of
    NuSMV is used, which is a symbolic model checker originated
    from the reengineering, reimplementation and extension of
    CMU SMV, the original BDD-based model checker developed at
    CMU.
For goal refinement verification, the refutation principle in
    logic is used. E.g. a goal G is refined into subgoals G1, G2
    , ... , Gn, then determine whether the temporal logic
    formula G1 ∧ G2 ∧ ... ∧ Gn ∧ Dom ∧ ¬G is satisfiable. If a solution
     satisfying this formula is found, we have found a history
    counterexample showing that the refinement is NOT complete.
    And this is represented by using Linear Temporal Logic (LTL)
    . --/

/--
--- autor: Yang Zhengguo
--- date : Tue Nov 24 15:58:12 JST 2015
--- place: Tan Lab, JAIST
--/
```

```
MODULE outdoor_air_temperature  -- state of outdoor air
   temperature
VAR
        temperature : { high,     -- temperature is high
                        neutral, -- temperature is just right
                           for thermal comfort
                        low};     -- temperature is low
ASSIGN
        init(temperature) := neutral;-- initial outdoor
           temperature, if not applicable, change it
        next(temperature) := case
                        temperature = high       : neutral;
                        temperature = neutral    : {high, low};
                        temperature = low        : neutral;
                    esac;

MODULE exterior_construction(ot) -- ot :
   outdoor_air_temperature
VAR
        ec : {  high,            -- the temperature of exterior
           construction
                neutral,         -- the temperature under
                   thermal equilibrium
                low};            -- low temperature
ASSIGN
        init(ec) := neutral;
        next(ec) := case
                        ec = high & next(ot.temperature) =
                           neutral       : neutral;
                        ec = neutral & next(ot.temperature) =
                           low           : low;
                        ec = neutral & next(ot.temperature) =
                           high          : high;
                        ec = low & next(ot.temperature) =
                           neutral          : neutral;
                        TRUE : ec;
                    esac;

MODULE interior_construction  -- the wall, affecting the state
   of heat exchange rate
VAR
```

```
        rate : { fast,          -- heat exchange rate is fast
                 blance,        -- heat exchange rate maintains
                     heat equilibrium, but may not thermal
                    comfort
                 slow};         -- heat exchange rate is slow
ASSIGN
        init(rate) := blance;

MODULE thermal_diffusion(p_ic, p_ec) -- p_ic:
   interior_construction; p_ec: exterior_construction
VAR
        diffusion : {maintain, breaking};
ASSIGN
        init(diffusion) := maintain;
        next(diffusion) := case
                                diffusion = maintain &
                                !(next(p_ec.ec) = neutral &
                                   next(p_ic.rate) = blance) :
                                   breaking;
                                diffusion = breaking &
                                next(p_ec.ec) = neutral & next(
                                   p_ic.rate) = blance :
                                   maintain;
                               TRUE : diffusion;
                           esac;

MODULE air_exchange_request -- whether air exchange is required
    by occupants
VAR
        request : boolean; -- TRUE: require air exchange
ASSIGN
        init(request) := TRUE;

MODULE window(req)  -- the status of window, which affects air
   exchange
VAR
        o: boolean; -- TRUE: the window is opened
ASSIGN
        init(o) := TRUE;
        next(o) := case
```

```
                        o = TRUE & next(req.request = FALSE) :
                            FALSE;
                        o = FALSE & next(req.request = TRUE) :
                            TRUE;
                        TRUE : o;
                        esac;

MODULE wind_speed(ww) -- ww: window; wind speed through window
VAR
        wspeed : { neutral,     -- wind speed is greater than o
            and is just right
                   weak};       -- wind speed is weak and maybe
                       o
ASSIGN
        init(wspeed) := neutral;
        next(wspeed) := case
                         wspeed = neutral & next(ww.o) = FALSE
                             : weak;
                         wspeed = weak & next(ww.o) = TRUE :
                             neutral;
                         TRUE : wspeed;
                        esac;

MODULE thermal_advection(out_temp, winds) -- out_temp:
   outdoor_air_temperature; winds: wind_speed
VAR
        advection : {maintain, breaking};
ASSIGN
        init(advection) := maintain;
        next(advection) := case
                                advection = maintain &
                                !(next(out_temp.temperature) =
                                    neutral & next(winds.wspeed)
                                     = neutral) : breaking;
                                advection = breaking &
                                (next(out_temp.temperature) =
                                    neutral & next(winds.wspeed)
                                     = neutral) : maintain;
                                TRUE : advection;
                                esac;
```

```
MODULE thermal_convection(diff, adve) -- diff:
    thermal_diffusion; adve: thermal_advection
VAR
        convection : {maintain, breaking};
ASSIGN
        init(convection) := maintain;
        next(convection) := case
                                convection = maintain &
                                !(next(diff.diffusion) =
                                    maintain & next(adve.
                                    advection) = maintain) :
                                    breaking;
                                convection = breaking &
                                (next(diff.diffusion) =
                                    maintain & next(adve.
                                    advection) = maintain) :
                                    maintain;
                               TRUE : convection;
                               esac;
MODULE insulation_request -- the request of insulation through
    curtain
VAR
        req : boolean;
ASSIGN
        init(req) := TRUE;

MODULE curtain(request) -- request : insulation_request; status
     of curtain
VAR
        status : {open, close};
ASSIGN
        init(status) := open;
        next(status) := case
                                status = open & next(request.
                                    req) = FALSE : close;
                                status = close & next(request.
                                    req) = TRUE : open;
                               TRUE : status;
                        esac;
```

```
MODULE solar_radiation(c) -- c : curtain; solar radiation that
    affects indoor temperature
VAR
        srad : boolean; -- Solar RADiation, if TRUE, there is
            solar radiation introduced
ASSIGN
        init(srad) := TRUE;
        next(srad) := case
                        srad = TRUE & next(c.status) = close :
                            FALSE;
                        srad = FALSE & next(c.status) = open :
                            TRUE;
                        TRUE : srad;
                        esac;

MODULE man_made_radiation(out) -- out : outdoor_air_temperature
    ; indoor heat sources, e.g. fireplace
VAR
        status : {on, off};
ASSIGN
        init(status) := off;
        next(status) := case
                                status = off & next(out.
                                    temperature) = low : on;
                                status = on & next(out.
                                    temperature) = high : off;
                                TRUE : status;
                        esac;

MODULE thermal_radiation(s,m) -- s : solar_radiation; m :
    man_made_radiation
VAR
        radiation : {maintain, breaking};
ASSIGN
        init(radiation) := maintain;
        next(radiation) := case
                                radiation = breaking &
                                (next(m.status) = on & next(s.
                                    srad) = FALSE) : maintain;
                                radiation = maintain &
```

```
                                !(next(m.status) = on & next(s.
                                    srad) = FALSE) : breaking;
                                TRUE : radiation;
                            esac;

MODULE indoor_temperature(cc,r) -- cc : thermal_convection; r :
    thermal_radiation
VAR
        thermal : {comfort, uncomfort};
ASSIGN
        init(thermal) := comfort;
        next(thermal) := case
                                thermal = uncomfort &
                                (next(r.radiation) = maintain &
                                    next(cc.convection) =
                                    maintain) : comfort;
                                thermal = comfort &
                                !(next(r.radiation) = maintain
                                    & next(cc.convection) =
                                    maintain) : uncomfort;
                                TRUE : thermal;
                        esac;

MODULE main
VAR
        indoor : indoor_temperature(cc,r);
        cc    : thermal_convection(diff, adve);
        diff : thermal_diffusion(p_ic, p_ec);
        p_ic : interior_construction;
        p_ec : exterior_construction(ot);
        ot    : outdoor_air_temperature;
        adve      : thermal_advection(out_temp, winds);
        out_temp : outdoor_air_temperature;
        winds     : wind_speed(ww);
        ww        : window(req);
        req       : air_exchange_request;

        r : thermal_radiation(s,m);
        s : solar_radiation(c);
        c : curtain(request);
        request : insulation_request;
```

```
        m : man_made_radiation(out);
        out : outdoor_air_temperature;

/-- indoor temperature < outdoor temperature --/

-- 1. Avoid[ExteriorConstructionHighTemperature] ∧ Maintain[
   LimitedHeatIntroductionRateTD] ∧ ¬Avoid[
   ThermalDiffusionDestroySM] : to show the goal refinement is
   complete when the result is false.
LTLSPEC G (((ot.temperature = neutral -> p_ec.ec = neutral U !(
   ot.temperature = neutral)) | ot.temperature = neutral ->
   p_ec.ec = neutral) & ((diff.diffusion = maintain -> p_ic.
   rate = blance U !(p_ec.ec = neutral)) | diff.diffusion =
   maintain -> p_ic.rate = blance)) & ((p_ec.ec = neutral &
   diff.diffusion = maintain -> indoor.thermal = comfort U diff
   .diffusion = breaking) | p_ec.ec = neutral & diff.diffusion
   = maintain -> indoor.thermal = comfort)


-- 2. Maintain[AirExchange] ∧ Maintain[AirExchangeRequested] ∧
   Maintain[LimitedWindSpeed] : to show  the goal refinement
   is complete when the result is false.
LTLSPEC G (((req.request = TRUE -> ww.o = TRUE U req.request =
   FALSE) | (req.request = TRUE -> ww.o = TRUE)) & ((indoor.
   thermal = comfort -> req.request = TRUE U req.request =
   FALSE) | (indoor.thermal = comfort -> req.request = TRUE)))
   & F !((ww.o = TRUE -> winds.wspeed = neutral U ww.o = FALSE)
    | ww.o = TRUE -> winds.wspeed = neutral)


-- 3. Maintain[LimitedWindSpeed] ∧ Maintain[
   AppropriateOutdoorTemperature] ∧ ¬Avoid[
   ThermalAdvectionDestroySM]
LTLSPEC G(((ww.o = TRUE -> winds.wspeed = neutral U ww.o =
   FALSE) | (ww.o = TRUE -> winds.wspeed = neutral)) & ((indoor
   .thermal = comfort & ww.o = TRUE -> ot.temperature = neutral
    U indoor.thermal = uncomfort) | (indoor.thermal = comfort &
    ww.o = TRUE -> ot.temperature = neutral))) & F !((adve.
   advection = maintain -> indoor.thermal = comfort U adve.
   advection = breaking) | (adve.advection = maintain -> indoor
   .thermal = comfort))
```

```
-- 4. Maintain[AppropriateInsulation] ∧ Maintain[
   InsulationRequest] ∧ ¬Maintain[LimitedSolarRadiation]
LTLSPEC G (((request.req = TRUE -> c.status = open U request.
   req = FALSE) | (request.req = TRUE -> c.status = open)) & ((
   indoor.thermal = uncomfort -> request.req = TRUE U request.
   req = FALSE) | (indoor.thermal = uncomfort -> request.req =
   TRUE))) & F !((indoor.thermal = comfort & c.status = open ->
    r.radiation = maintain U c.status = close) | (indoor.
   thermal = comfort & c.status = open -> r.radiation =
   maintain))


-- 5. Maintain[LimitedSolarRadiation] ∧ Maintain[
   IndoorManMadeThermalRadiation] ∧ ¬Avoid[
   ThermalRadiationDestroySM]
LTLSPEC G (((indoor.thermal = comfort & c.status = open -> r.
   radiation = maintain U c.status = close) | (indoor.thermal =
    comfort & c.status = open -> r.radiation = maintain)) &
   ((!(out.temperature = low) -> m.status = off U out.
   temperature = low) | (!(out.temperature = low) -> m.status =
    off))) & F !((r.radiation = maintain -> indoor.thermal =
   comfort U r.radiation = breaking) | (r.radiation = maintain
   -> indoor.thermal = comfort))


/-- indoor temperature > outdoor temperature --/

-- 6. Maintain[LimitedHeatDissipationRateTD] ∧ Avoid[
   ExteriorConstructionLowTemperature] ∧ ¬Avoid[
   ThermalDiffusionDestroySM]
LTLSPEC G (((diff.diffusion = maintain -> p_ic.rate = blance U
   p_ec.ec = low) | (diff.diffusion = maintain -> p_ic.rate =
   blance)) & ((diff.diffusion = maintain & ot.temperature =
   neutral -> !(p_ec.ec = low) U ot.temperature = low) | (diff.
   diffusion = maintain & ot.temperature = neutral -> !(p_ec.ec
    = low)))) & F !((p_ec.ec = neutral & diff.diffusion =
   maintain -> indoor.thermal = comfort U diff.diffusion =
   breaking) | (p_ec.ec = neutral & diff.diffusion = maintain
   -> indoor.thermal = comfort))
```

```
-- 7. ZeroWindSpeed ∧ Avoid[AirExchangeRequested] ∧ ¬Maintain[
   NoThermalAdvection]
LTLSPEC G ((ww.o = FALSE -> winds.wspeed = weak) & (out_temp.
   temperature = low -> req.request = FALSE)) & F !((out_temp.
   temperature = low & ww.o = FALSE -> adve.advection =
   maintain U ww.o = TRUE) | (out_temp.temperature = low & ww.o
    = FALSE -> adve.advection = maintain))


-- 8. Avoid[Insulation] ∧ Maintain[InsulationRequest] ∧
   ¬Maintain[SolarRadiationAffected]
LTLSPEC G (((request.req = TRUE -> c.status = open U request.
   req = FALSE) | request.req = TRUE -> c.status = open) & ((
   indoor.thermal = uncomfort -> request.req = TRUE U request.
   req = FALSE) | indoor.thermal = uncomfort -> request.req =
   TRUE)) & F !((c.status = open & indoor.thermal = comfort ->
   r.radiation = maintain U c.status = close) | c.status = open
    & indoor.thermal = comfort -> r.radiation = maintain)


-- 9. Maintain[IndoorManMadeThermalRadiation] ∧ Maintain[
   SolarRadiationAffected] ∧ ¬Avoid[ThermalRadiationDestroySM]
LTLSPEC G(((out.temperature = low -> m.status = on U !(out.
   temperature = low)) | (out.temperature = low -> m.status =
   on)) & ((c.status = open & indoor.thermal = comfort -> r.
   radiation = maintain U c.status = close) | (c.status = open
   & indoor.thermal = comfort -> r.radiation = maintain))) & F
   !((indoor.thermal = comfort -> r.radiation = maintain U
   indoor.thermal = uncomfort) | (indoor.thermal = comfort -> r
   .radiation = maintain))
```

Publications

Journal

1. Zhengguo Yang, Toshiaki Aoki, and Yasuo Tan. Multiple-conformance to hybrid-automata-modeled requirements for detecting indoor temperature anomalies. 2020. To be submitted*

2. Zhengguo Yang, Yuto Lim, and Yasuo Tan. An accident model with considering physical processes for indoor environment safety. *Applied Sciences*, 9(22):4732, nov 2019. doi: 10.3390/app9224732. URL https://doi.org/10.3390/app9224732

Conference Paper

1. Zhengguo Yang, Yuto Lim, and Yasuo Tan. Event-based home safety problem detection under the cps home safety architecture. In *2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE)*, pages 491–495, October 2013

2. Zhengguo Yang, Yuto Lim, and Yasuo Tan. A risk model for indoor environment safety. In *2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, pages 1–5, October 2017

3. Zhengguo Yang, Toshiaki Aoki, and Yasuo Tan. Modeling the required indoor temperature change by hybrid automata for detecting thermal problems. In *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pages 135–144, Dec 2018. doi: 10.1109/PRDC.2018.00024

4. Zhengguo Yang, Toshiaki Aoki, and Yasuo Tan. Multiple conformance to hybrid automata for checking smart house temperature change. In *2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, pages 1–10, Oct 2018. doi: 10.1109/DISTRA.2018.8601005

5. Zhengguo Yang, Yuto Lim, and Yasuo Tan. Prediction of heat-shock during bath by Bayesian networks. To be submitted, 2020†

*This journal paper has been finished writing.

†This conference paper may be extended and submitted to a journal in the future.

References

[1] ISO/TC 159. Ergonomics of the thermal environment. Standard ISO 11079:2007, International Organization for Standardization, 2007.

[2] ISO/TC 199. Safety of machinery – Risk assessment – part 1: principles. Standard ISO 14121-1, International Organization for Standardization, 2007.

[3] ITU-T Study Group 20. Overview of the internet of things. Standard ITU-T Y.4000/Y.2060, International Telecommunication Union, 2012.

[4] ICAO 2009. *Safety Management Manual (SMM).* ICAO Doc 9859: Second edition. Inernational Civil Aviation Organization, 2009. ISBN 978-92-9231-295-4.

[5] ISO/TC 262. Risk Management – Principles and guidelines. Standard AS NZS ISO 31000, International Organization for Standardization, 2009.

[6] ISO/TC 262. Risk management – Risk assessment techniques. Standard ISO/IEC 31010, International Organization for Standardization, 2009.

[7] IEC SyC AAL WG 7. Cooperative multiple systems in connected home environments – functional safety of electrical/electronic safety-related systems – AAL aspects – part 2: Concpet phase. Standard (ACD) IEC WD 63168-2:2019, International Electrotechnical Commission, 2019.

[8] IEC SyC AAL WG 7. Cooperative multiple systems in connected home environments – functional safety of electrical/electronic safety-related systems – AAL aspects – part 3: Product development. Standard (ACD) IEC WD 63168-3:2019, International Electrotechnical Commission, 2019.

[9] IEC SyC AAL WG 7. Cooperative multiple systems in connected home environments – functional safety of electrical/electronic safety-related systems – AAL aspects – part 4: Production, operation, modification and supporting processes. Standard (ACD) IEC WD 63168-4:2019, International Electrotechnical Commission, 2019.

[10] H.Y. Abbas. *Test-based falsification and conformance testing for cyber-physical systems*. PhD thesis, Arizona State University, May 2015. Doctoral Dissertation Electrical Engineering 2015.

[11] Anthony P. Acfield and Robert A. Weaver. Integrating safety management through the bowtie concept a move away from the safety case focus. In *Proceedings of the Australian System Safety Conference - Volume 145*, ASSC '12, pages 3–12, Darlinghurst, Australia, Australia, 2012. Australian Computer Society, Inc. ISBN 978-1-921770-15-9.

[12] C. E. Adams. Home area network technologies. *BT Technology Journal*, 20(2):53–72, Apr 2002. ISSN 1573-1995. doi: 10.1023/A:1015640322106.

[13] Zakia Afroz, GM Shafiullah, Tania Urmee, and Gary Higgins. Prediction of indoor temperature in an institutional building. *Energy Procedia*, 142:1860 – 1866, 2017. ISSN 1876-6102. doi: https://doi.org/10.1016/j.egypro.2017.12.576. Proceedings of the 9th International Conference on Applied Energy.

[14] Yogender Aggarwal, Bhuwan Mohan Karan, Barda Nand Das, and Rakesh Kumar Sinha. Prediction of heat-illness symptoms with the prediction of human vascular response in hot environment under resting condition. *Journal of Medical Systems*, 32(2):167–176, Apr 2008. ISSN 1573-689X. doi: 10.1007/s10916-007-9119-3.

[15] Marco Aiello and Schahram Dustdar. Are our homes ready for services? a domotic infrastructure based on the web service stack. *Pervasive and Mobile Computing*, 4(4):506 – 525, 2008. ISSN 1574-1192. doi: https://doi.org/10.1016/j.pmcj.2008.01.002.

[16] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, and M.L.M. Kiah. A review of smart home applications based on internet of things. *Journal of Network and Computer Applications*, 97:48 – 65, 2017. ISSN 1084-8045. doi: https://doi.org/10.1016/j.jnca.2017.08.017.

[17] Craig K. Allison, Kirsten M. Revell, Rod Sears, and Neville A. Stanton. Systems theoretic accident model and process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Safety Science*, 98:159 – 166, 2017. ISSN 0925-7535. doi: https://doi.org/10.1016/j.ssci.2017.06.011.

[18] G. Brooke Anderson, Michelle L. Bell, and Roger D. Peng. Methods to calculate the heat index as an exposure metric in environmental health research. *Environmental Health Perspectives*, 121(10):1111–1119, October 2013. doi: 10.1289/ehp.1206273.

[19] ANSI/ASHRAE. Thermal environmental conditions for human occupancy. Standard ANSI/ASHRAE Standard 55-2010, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., 2010.

[20] Fatma Keskin Arabul, Ahmet Yigit Arabul, Celal Fadil Kumru, and Ali Rifat Boynuegri. Providing energy management of a fuel cellâbatteryâwind turbineâsolar panel hybrid off grid smart home system. *International Journal of Hydrogen Energy*, 42(43):26906 – 26913, 2017. ISSN 0360-3199. doi: https://doi.org/10.1016/j.ijhydene.2017.02.204.

[21] Hugo Araujo, Gustavo Carvalho, Morteza Mohaqeqi, Mohammad Reza Mousavi, and Augusto Sampaio. Sound conformance testing for cyber-physical systems: Theory and implementation. *Science of Computer Programming, Special Issue on TASE 2016*, 162:35 – 54, 2018. ISSN 0167-6423. doi: 10.1016/j.scico.2017.07.002.

[22] Jatin Arora, Gagandeep, and Ravinder Kumar. Iot-based smart home systems. In H. S. Saini, Rishi Sayal, A. Govardhan, and Rajkumar Buyya, editors, *Innovations in Computer Science and Engineering*, pages 531–538, Singapore, 2019. Springer Singapore. ISBN 978-981-10-8201-6.

[23] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010. ISSN 1389-1286. doi: https://doi.org/10.1016/j.comnet.2010.05.010.

[24] A. Avižienis, J.C. Laprie, B. Randell, and University of Newcastle upon Tyne. Computing Science. *Fundamental Concepts of Dependability*. Technical report series. University of Newcastle upon Tyne, Computing Science, 2001.

[25] A. Avizienis, J. . Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1 (1):11–33, Jan 2004. ISSN 1545-5971. doi: 10.1109/TDSC.2004.2.

[26] O. Azzabi, C. B. Njima, and H. Messaoud. Modeling a system with hybrid automata and multi —models. In *2017 International Conference on Control, Automation and Diagnosis (ICCAD)*, pages 087–091, Jan 2017. doi: 10.1109/CADIAG.2017.8075636.

[27] Peter E.J Baldwin and Andrew D Maynard. A survey of wind speeds in indoor workplaces. *The Annals of Occupational Hygiene*, 42(5):303 – 313, 1998. ISSN 0003-4878. doi: https://doi.org/10.1016/S0003-4878(98)00031-3.

[28] Barnana Baruah and Subhasish Dhal. A two-factor authentication scheme against fdm attack in ifttt based smart home system. *Computers & Security*, 77:21 – 35, 2018. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2018.03.004.

[29] Edward Batschelet. *Introduction to mathematics for life scientists*, pages 157–162. Springer study edition. Springer-Verlag Berlin Heidelberg, 3 edition, 1979. ISBN 9783642618697 (online), 9783540096481 (print). doi: 10.1007/978-3-642-61869-7.

[30] Patricia Baudier, Chantal Ammi, and Matthieu Deboeuf-Rouchon. Smart home: Highly-educated students' acceptance. *Technological Forecasting and Social Change*, 2018. ISSN 0040-1625. doi: https://doi.org/10.1016/j.techfore.2018.06.043.

[31] Fabien Belmonte, Walter Schön, Laurent Heurley, and Robert Capel. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision. *Reliability Engineering & System Safety*, 96(2):237 – 249, 2011. ISSN 0951-8320. doi: https://doi.org/10.1016/j.ress.2010.09.006.

[32] Irad Ben-Gal. *Bayesian Networks*. American Cancer Society, 2008. ISBN 9780470061572. doi: 10.1002/9780470061572.eqr089. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470061572.eqr089.

[33] Frédéric Bergeron, Kevin Bouchard, Sébastien Gaboury, and Sylvain Giroux. Tracking objects within a smart home. *Expert Systems with Applications*, 113:428 – 442, 2018. ISSN 0957-4174. doi: https://doi.org/10.1016/j.eswa.2018.07.009.

[34] Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei. Design of an internet of things-based smart home system. In *2011 2nd International Conference on Intelligent Control and Information Processing*, volume 2, pages 921–924, July 2011. doi: 10.1109/ICICIP.2011.6008384.

[35] Torbjørn Bjerga, Terje Aven, and Enrico Zio. Uncertainty treatment in risk analysis of complex systems: The cases of stamp and fram. *Reliability Engineering & System Safety*, 156:203 – 209, 2016. ISSN 0951-8320. doi: https://doi.org/10.1016/j.ress.2016.08.004.

[36] Patricia Bouyer, Kim G. Larsen, Nicolas Markey, Ocan Sankur, and Claus Thrane. Timed automata can always be made implementable. In *Proceedings of the 22nd International Conference on Concurrency Theory*, CONCUR'11, pages 76–91, Berlin, Heidelberg, 2011. Springer-Verlag. ISBN 978-3-642-23216-9.

[37] Jacklitsch Brenda, Williams W. Jon, Musolin Kristin, Coca Aitor, Kim Jung-Hyun, and Turner Nina. NIOSH criteria for a recommended standard: Occupational exposure to heat and hot environments. Recommendation, U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, NIOSH, 2016.

[38] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. Home automation in the wild: Challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, number 10 in CHI '11, pages 2115–2124, Vancouver, BC, Canada, 2011. ACM.

[39] Grahame M. Budd. Wet-bulb globe temperature (wbgt)—its history and its limitations. *Journal of Science and Medicine in Sport*, 11(1):20 – 32, 2008. ISSN 1440-2440. doi: https://doi.org/10.1016/j.jsams.2007.07.003. URL http://www.sciencedirect.com/science/article/pii/S1440244007001478.

[40] Aditi Bunker, Jan Wildenhain, Alina Vandenbergh, Nicholas Henschke, Joacim Rocklöv, Shakoor Hajat, and Rainer Sauerborn. Effects of air temperature on climate-sensitive mortality and morbidity outcomes in the elderly; a systematic review and meta-analysis of epidemiological evidence. *EBioMedicine*, 6:258 – 268, 2016. ISSN 2352-3964. doi: https://doi.org/10.1016/j.ebiom.2016.02.034.

[41] Athanasios C. Antoulas, Danny C. Sorensen, and Serkan Gugercin. A survey of model reduction methods for large-scale systems. *Contemporary Mathematics*, 280:193–219, Dec 2000.

[42] Huiyi Cao, Shigang Hu, Qingyang Wu, Zhijun Tang, Jin Li, and Xiaofeng Wu. Research and design of smart home system based on cloud computing. In Fatos Xhafa, Srikanta Patnaik, and Albert Y. Zomaya, editors, *Advances in Intelligent Systems and Interactive Applications*, pages 643–648, Cham, 2018. Springer International Publishing. ISBN 978-3-319-69096-4.

[43] S. Chemishkian. Building smart services for smart home. In *Proceedings 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525)*, pages 215–224, Jan 2002. doi: 10.1109/IWNA.2001.980856.

[44] Takashi Chiba, Misa Yamauchi, Naoki Nishida, Taeko Kaneko, Katsuaki Yoshizaki, and Naofumi Yoshioka. Risk factors of sudden death in the japanese hot bath in the senior population. *Forensic Science International*, 149(2):151 – 158, 2005. ISSN 0379-0738. doi: https://doi.org/10.1016/j.forsciint.2004.04.085. URL http://www.sciencedirect.com/science/article/pii/S0379073804003573.

[45] G. Chong, L. Zhihao, and Y. Yifeng. The research and implement of smart home system based on internet of things. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, pages 2944–2947, Sept 2011. doi: 10.1109/ICECC.2011.6066672.

[46] A F Colver, P J Hutchinson, and E C Judson. Promoting children's home safety. *BMJ*, 285 (6349):1177–1180, 1982. ISSN 0007-1447. doi: 10.1136/bmj.285.6349.1177.

[47] Veerle M. H. Coupé, Linda C. Van Der Gaag, and J. Dik F. Habbema. Sensitivity analysis: An aid for belief-network quantification. *The Knowledge Engineering Review*, 15(3):215–232, September 2000. ISSN 0269-8889. doi: 10.1017/S0269888900003027. URL https://doi.org/10.1017/S0269888900003027.

[48] Uesako Daisuke. 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, 2016.

[49] Enrico Denti. Novel pervasive scenarios for home management: the butlers architecture. *SpringerPlus*, 3(1):52, Jan 2014. ISSN 2193-1801. doi: 10.1186/2193-1801-3-52. URL https://doi.org/10.1186/2193-1801-3-52.

[50] TC 56 Dependability. Hazard and operability studies (hazop studies) - application guide. Standard IEC 61882:2016, International Electrotechnical Commission, 2016.

[51] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, 138:1 – 12, 2018. ISSN 1389-1286. doi: https://doi.org/10.1016/j.comnet.2018.03.024.

[52] Egarter Dominik, Monacchi Andrea, Khatib Tamer, and Wilfried Elmenreich. Integration of legacy appliances into home energy management systems. *ArXiv e-prints*, Jun. 2014. Provided by the SAO/NASA Astrophysics Data System.

[53] S. Don, Eunmi Choi, and Dugki Min. Event driven adaptive awareness system for medical cyber physical systems. In *4th International Conference on Awareness Science and Technology*, pages 238–242, Aug 2012. doi: 10.1109/iCAwST.2012.6469620.

[54] Ana-Maria Claudia Drăgulinescu, Andrei Drăgulinescu, Ioana Marcu, Simona Halunga, and Octavian Fratu. Smartgreeting: A new smart home system which enables context-aware services. In Octavian Fratu, Nicolae Militaru, and Simona Halunga, editors, *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, pages 158–164, Cham, 2018. Springer International Publishing. ISBN 978-3-319-92213-3.

[55] Lydie du Bousquet, Masahide Nakamura, Ben Yan, and Hiroshi Igaki. Using formal methods to increase confidence in a home network system implementation: a case study. *Innovations in Systems and Software Engineering*, 5(3):181–196, Sep 2009. ISSN 1614-5054. doi: 10.1007/s11334-009-0092-5.

[56] Elena Dubrova. *Fault-Tolerant Design*. Springer-Verlag New York, 2013. ISBN 978-1-4614-2113-9.

[57] Ioan Dumitrache, Ioan Stefan Sacala, Mihnea Alexandru Moisescu, and Simona Iuliana Caramihai. A conceptual framework for modeling and design of cyber-physical systems. *Studies in Informatics and Control*, 26(3), 2017. ISSN 1220-1766.

[58] ISO/TC 22/SC 32 Electrical, electronic components, and general system aspects. Road vehicles – functional safety – part 3: Concept phase. Standard ISO 26262-3:2011, International Organization for Standardization, 2011.

[59] SEBASTIAN ENGELL, SVEN LOHMANN, and OLAF STURSBERG. Verification of embedded supervisory controllers considering hybrid plant dynamics. *International Journal of Software Engineering and Knowledge Engineering*, 15(02):307–312, 2005. doi: 10.1142/S021819400500204X.

[60] Clifton A. Ericson II. *Hazard Analysis Techniques for System Safety*, chapter 3, pages 31–54. John Wiley and Sons, Inc., Hoboken, New Jersey, 2005. ISBN 9780471739425.

[61] Lukas Esterle and Radu Grosu. Cyber-physical systems: challenge of the 21st century. *e & i Elektrotechnik und Informationstechnik*, 133(7):299–303, Nov 2016. ISSN 1613-7620. doi: 10.1007/s00502-016-0426-6. URL https://doi.org/10.1007/s00502-016-0426-6.

[62] FAA and EUROCONTROL. Atm safety techniques and toolbox. Technical report, FAA and EUROCONTROL, EEC Technical / Scientific Reports, Oct. 2007.

[63] Xiaodong Fan, Bo Qiu, Yuanyuan Liu, Haijing Zhu, and Bochong Han. Energy visualization for smart home. *Energy Procedia*, 105:2545 – 2548, 2017. ISSN 1876-6102. doi: https://doi.org/10.1016/j.egypro.2017.03.732. the 8th International Conference on Applied Energy, ICAE2016, 8-11 October 2016, Beijing, China.

[64] Sebastian Feuerstack, Marco Blumendorf, Grzegorz Lehmann, and Sahin Albayrak. Seamless home services. In *Developing Ambient Intelligence*, pages 1–10, Paris, 2006. Springer Paris. ISBN 978-2-287-47610-5.

[65] D. Fiala, K. J. Lomas, and M. Stohrer. Computer prediction of human thermoregulatory and temperature responses to a wide range of environmental conditions. *International Journal of Biometeorology*, 45(3):143–159, Sep 2001. ISSN 1432-1254. doi: 10.1007/s004840100099.

[66] Anastacio Pinto Goncalves Filho, Gyuchan Thomas Jun, and Patrick Waterson. Four studies, two methods, one accident – an examination of the reliability and validity of accimap and stamp for accident analysis. *Safety Science*, 113:310 – 317, 2019. ISSN 0925-7535. doi: https://doi.org/10.1016/j.ssci.2018.12.002.

[67] William J. Fisk. Review of some effects of climate change on indoor environmental quality and health and associated no-regrets mitigation measures. *Building and Environment*, 86:70 – 80, 2015. ISSN 0360-1323. doi: https://doi.org/10.1016/j.buildenv.2014.12.024.

[68] William J. Fisk and Arthur H. Rosenfeld. Estimates of improved productivity and health from better indoor environments. *Indoor Air*, 7(3):158–172, 2004. doi: 10.1111/j.1600-0668.1997.t01-1-00002.x.

[69] U.S. National Science Foundation. Cyber-physical systems (cps), 2014. URL https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf12520. nsf12520.

[70] Roberto Z. Freire, Gustavo H.C. Oliveira, and Nathan Mendes. Predictive controllers for thermal comfort optimization and energy savings. *Energy and Buildings*, 40(7):1353 – 1365, 2008. ISSN 0378-7788. doi: https://doi.org/10.1016/j.enbuild.2007.12.007.

[71] F.Zamora-Martínez, P. Romeu, P. Botella-Rocamora, and J. Pardo. On-line learning of indoor temperature forecasting models towards energy efficiency. *Energy and Buildings*, 83:162 – 172, 2014. ISSN 0378-7788. doi: https://doi.org/10.1016/j.enbuild.2014.04.034. SCIENCE BEHIND AND BEYOND THE SOLAR DECATHLON EUROPE 2012.

[72] Jianliang Gao, Jianxin Wang, Ping Zhong, and Haodong Wang. On threshold-free error detection for industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 14 (5):2199–2209, May 2018. ISSN 1551-3203. doi: 10.1109/TII.2017.2785395.

[73] Ernesto Garcia Davis and Anna Calveras Augé. A presence-aware smart home system (pash). In José Bravo, Ramón Hervás, and Vladimir Villarreal, editors, *Ambient Assisted Living*, pages 159–166, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. ISBN 978-3-642-21303-8.

[74] Flavio G. Gaudio and Colin K. Grissom. Cooling methods in heat stroke. *The Journal of Emergency Medicine*, 50(4):607 – 616, 2016. ISSN 0736-4679. doi: https://doi.org/10.1016/j.jemermed.2015.09.014. URL http://www.sciencedirect.com/science/article/pii/S0736467915009440.

[75] Yunhua Gong and Yuntao Li. STAMP-based causal analysis of china-donghuang oil transportation pipeline leakage and explosion accident. *Journal of Loss Prevention in the Process Industries*, 56:402 – 413, 2018. ISSN 0950-4230. doi: https://doi.org/10.1016/j.jlp.2018.10.001.

[76] Steven Goodwin. *Smart Home Automation with Linux and Raspberry Pi*. Apress, Berkely, CA, USA, 2nd edition, 2013. ISBN 143025887X, 9781430258872. doi: 10.1007/978-1-4302-5888-9.

[77] Kirsten Gram-Hanssen and Sarah J. Darby. "home is where the smart is"? evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science*, 37:94 – 101, 2018. ISSN 2214-6296. doi: https://doi.org/10.1016/j.erss.2017.09.037.

[78] H. Grogan and P.M. Hopkins. Heat stroke: implications for critical care and anaesthesia. *British Journal of Anaesthesia*, 88(5):700 – 707, 2002. ISSN 0007-0912. doi: https://doi.org/10.1093/bja/88.5.700.

[79] ISO/TMBG Technical Management Board groups. Risk management – vocabulary. Standard ISO Guide 73, International Organization for Standardization, 2009.

[80] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, 78:398 – 428, 2018. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2018.07.011.

[81] David Heckerman. *A Tutorial on Learning with Bayesian Networks*, pages 33–82. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008. ISBN 978-3-540-85066-3. doi: 10.1007/978-3-540-85066-3_3. URL https://doi.org/10.1007/978-3-540-85066-3_3.

[82] T. A. Henzinger. The theory of hybrid automata. In *Proceedings 11th Annual IEEE Symposium on Logic in Computer Science*, pages 278–292, Jul 1996. doi: 10.1109/LICS.1996.561342.

[83] Thomas A. Henzinger, Rupak Majumdar, and Vinayak S. Prabhu. Quantifying similarities between timed systems. In Paul Pettersson and Wang Yi, editors, *Formal Modeling and Analysis of Timed Systems*, pages 226–241, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. ISBN 978-3-540-31616-9.

[84] Theis Solberg Hjorth and Rune Torbensen. Trusted domain: A security platform for home automation. *Computers & Security*, 31(8):940 – 955, 2012. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2012.07.003.

[85] Erik Hollnagel. *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. CRC Press, Boca Raton London New York, 1 edition, 2012. ISBN 9781409445517.

[86] Dawn E. Holmes and Lakhmi C. Jain. *Introduction to Bayesian Networks*, pages 1–5. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008. ISBN 978-3-540-85066-3. doi: 10.1007/978-3-540-85066-3_1.

[87] Qi Van Eikema Hommes. Applying stpa to automotive adaptive cruise control system, 2012.

[88] Michal Horný. Bayesian networks. Technical Report 5, Boston University, School of Public Health, Department of Health Policy & Management, Boston MA 02215, USA, Apr. 2014.

[89] Hui-Huang Hsu, Po-Kai Chen, and Chi-Yi Lin. Rfid-based danger prevention for home safety. In *2010 2nd International Symposium on Aware Computing*, pages 56–60, Nov 2010. doi: 10.1109/ISAC.2010.5670455.

[90] Lida Huang, Guoray Cai, Hongyong Yuan, and Jianguo Chen. A hybrid approach for identifying the structure of a bayesian network model. *Expert Systems with Applications*, 131:308 – 320, 2019. ISSN 0957-4174. doi: https://doi.org/10.1016/j.eswa.2019.04.060. URL http://www.sciencedirect.com/science/article/pii/S0957417419302969.

[91] Steven Hwang, Linda Ng Boyle, and Ashis G. Banerjee. Identifying characteristics that impact motor carrier safety using bayesian networks. *Accident Analysis & Prevention*, 128:40 – 45, 2019. ISSN 0001-4575. doi: https://doi.org/10.1016/j.aap.2019.03.004. URL http://www.sciencedirect.com/science/article/pii/S0001457519303987.

[92] Mohammad Noor Ibrahim, Saipunidzam Mahamad, Khairul Shafee Khalid, Eliza Mazmee Mazlan, and Redza Shafique Md. Ridzuan. Controlling electrical appliances using an open source technology. In Khaled Elleithy, editor, *Innovations and Advanced Techniques in Systems, Computing Sciences and Software Engineering*, pages 429–434, Dordrecht, 2008. Springer Netherlands. ISBN 978-1-4020-8735-6.

[93] Asif Iqbal, Farman Ullah, Hafeez Anwar, Kyung Sup Kwak, Muhammad Imran, Waseef Jamal, and Atta ur Rahman. Interoperable internet-of-things platform for smart home system using web-of-objects and cloud. *Sustainable Cities and Society*, 38:636 – 646, 2018. ISSN 2210-6707. doi: https://doi.org/10.1016/j.scs.2018.01.044.

[94] Masao Ito. Finding hazards and threats in concept phase. *SEC Journal*, 10(6):18 – 27, 2015. in Japanese.

[95] ITU-T. Overview of the Internet of Things. Recommendation, ITU-T Y.2060, Jun. 2012. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks. Next Generation Networks – Frameworks and functional architecture models.

[96] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56:719 – 733, 2016. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2015.09.003.

[97] Laprie Jean-Claude, editor. *Dependability: Basic Concepts and Terminology*. Springer-Verlag Wien, 1992. ISBN 978-3-7091-9172-9. doi: 10.1007/978-3-7091-9170-5.

[98] Son Ji-Yeon, Park Jun-Hee, Moon Kyeong-Deok, and Lee Young-Hee. Resource-aware smart home management system by constructing resource relation graph. *IEEE Transactions on Con-*

sumer Electronics, 57(3):1112–1119, August 2011. ISSN 0098-3063. doi: 10.1109/TCE.2011.6018863.

[99] Jehn-Ruey Jiang. An improved cyber-physical systems architecture for industry 4.0 smart factories. In *2017 International Conference on Applied System Innovation (ICASI)*, pages 918–920, May 2017. doi: 10.1109/ICASI.2017.7988589.

[100] M. Jiao, D. Y. Sen, Q. L. Lin, W. Gang, and W. Da Xin. Hybrid control of greenhouse temperature system based on crop temperature integration theory. In *2017 36th Chinese Control Conference (CCC)*, pages 2426–2431, Jul 2017. doi: 10.23919/ChiCC.2017.8027722.

[101] Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei. Smart home system based on iot technologies. In *2013 International Conference on Computational and Information Sciences*, pages 1789–1791, June 2013. doi: 10.1109/ICCIS.2013.468.

[102] Karen R. Josephson, Diana A. Fabacher, and Laurence Z. Rubenstein. Home safety and fall prevention. *Clinics in Geriatric Medicine*, 7(4):707 – 732, 1991. ISSN 0749-0690. doi: https://doi.org/10.1016/S0749-0690(18)30515-9. URL http://www.sciencedirect.com/science/article/pii/S0749069018305159. Geriatric Home Care.

[103] Mr.Rohit Kadam, Mr.Pranav Mahamuni, and Mr.Yash Parikh. Smart home system. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, 2(2):81 – 86, 2015. ISSN 2349-2163.

[104] Kiyoko Kanda, Jun Tsuchiya, Masako Seto, Tadakatsu Ohnaka, and Yutaka Tochihara. Thermal conditions in the bathroom in winter and summer, and physiological responses of the elderly during bathing. *Japanese Journal of Hygiene*, 50(2):595–603, 1995. doi: 10.1265/jjh.50.595.

[105] Kiyoko Kanda, Tadakatsu Ohnaka, Yutaka Tochihara, Kazuyo Tsuzuki, Yoshihiko Shodai, and Kenichi Nakamura. Effects of the thermal conditions of the dressing room and bathroom on physiological responses during bathing. *Applied Human Science*, 15(1):19–24, 1996. doi: 10.2114/jpa.15.19.

[106] S. Karjalainen. Thermal comfort and gender: a literature review. *Indoor Air*, 22(2):96–109, 2011. doi: 10.1111/j.1600-0668.2011.00747.x.

[107] Mohammad Kazkaz and Milan Pavelek. Operative temperature and globe temperature. *Engineering Mechanics*, 20(3/4):319–325, 2013. ISSN 1805-4633.

[108] M. Killian, M. Zauner, and M. Kozek. Comprehensive smart home energy management system using mixed-integer quadratic-programming. *Applied Energy*, 222:662 – 672, 2018. ISSN 0306-2619. doi: https://doi.org/10.1016/j.apenergy.2018.03.179.

[109] Erina Kitamura, Yoshie Shibata, and Naoki Matsubara. A study on the prevention of heat shock from the viewpoint of residents. *Japanese Journal of Biometeorology*, 53(1):13–29, 2016. doi: 10.11227/seikisho.53.13. in Japanese.

[110] NEIL E KLEPEIS, WILLIAM C NELSON, WAYNE R OTT, JOHN P ROBINSON, ANDY M TSANG, PAUL SWITZER, JOSE V BEHAR, STEEN C HE, and WILLIAM H ENGELMANN. The national human activity pattern survey (nhaps): a resource for assessing exposure to environmental pollutants. *Journal of Exposure Science and Environmental Epidemiology*, 11(3), 7 2001. ISSN 1559-064X. doi: 10.1038/sj.jea.7500165.

[111] Pushpa Kumar, Nary Subramanian, and Kang Zhang. Savit: Technique for visualization of digital home safety. In *2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, pages 1120–1125, June 2009. doi: 10.1109/ICIS.2009.126.

[112] J. Kurnitski, T. Kalamees, J. Palonen, L. Eskola, and O. Seppänen. Potential effects of permeable and hygroscopic lightweight structures on thermal comfort and perceived iaq in a cold climate. *Indoor Air*, 17(1):37–49, 2006. doi: 10.1111/j.1600-0668.2006.00447.x.

[113] Boniphace Kutela and Hualiang Teng. Prediction of drivers and pedestrians' behaviors at signalized mid-block danish offset crosswalks using bayesian networks. *Journal of Safety Research*, 69:75 – 83, 2019. ISSN 0022-4375. doi: https://doi.org/10.1016/j.jsr.2019.02.008. URL http://www.sciencedirect.com/science/article/pii/S0022437518306595.

[114] H. Lee, L. Park, S. Park, T. Chung, and J. Moon. Interactive remote control of legacy home appliances through a virtually wired sensor network. *IEEE Transactions on Consumer Electronics*, 56(4):2241–2248, November 2010. ISSN 0098-3063. doi: 10.1109/TCE.2010.5681096.

[115] Hak Min Lee, Chang K Cho, Myung Hwan Yun, and Myun W Lee. Development of a temperature control procedure for a room air-conditioner using the concept of just noticeable difference (jnd) in thermal sensation. *International Journal of Industrial Ergonomics*, 22(3):207 – 216, 1998. ISSN 0169-8141. doi: https://doi.org/10.1016/S0169-8141(97)00009-7.

[116] Jay Lee, Behrad Bagheri, and Hung-An Kao. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3:18 – 23, 2015. ISSN 2213-8463. doi: https://doi.org/10.1016/j.mfglet.2014.12.001.

[117] Jay Lee, Chao Jin, and Behrad Bagheri. Cyber physical systems for predictive production systems. *Production Engineering*, 11(2):155–165, Apr 2017. ISSN 1863-7353. doi: 10.1007/s11740-017-0729-4.

[118] Seong Joon Lee, Ilseok Ko, and Min Wook Kil. A user interface for controlling information appliances in smart homes. In Ngoc Thanh Nguyen, Adam Grzech, Robert J. Howlett, and Lakhmi C. Jain, editors, *Agent and Multi-Agent Systems: Technologies and Applications*, pages 875–883, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-72830-6.

[119] Taek Lee, Jiyong Park, and Hoh Peter In. Effective appliance selection by complementary context feeding in smart home system. In Roman Obermaisser, Yunmook Nah, Peter Puschner, and Franz J. Rammig, editors, *Software Technologies for Embedded and Ubiquitous Systems*, pages 233–242, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-75664-4.

[120] Lisa R. Leon and Abderrezak Bouchama. *Heat Stroke*, pages 611–647. American Cancer Society, 2015. ISBN 9780470650714. doi: 10.1002/cphy.c140017. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/cphy.c140017.

[121] A. A. Letichevsky, O. O. Letychevskyi, V. G. Skobelev, and V. A. Volkov. Cyber-physical systems. *Cybernetics and Sys. Anal.*, 53(6):821–834, Nov 2017. ISSN 1060-0396. doi: 10.1007/s10559-017-9984-9.

[122] Nancy Leveson. *An STPA Primer*, 1 edition, June 2015.

[123] Nancy G. Leveson. *Safeware: System Safety and Computers*. ACM, New York, NY, USA, 1995. ISBN 0-201-11972-2.

[124] Nancy G. Leveson. *System Safety Engineering : Back To The Future*. Massachusetts Institute of Technology, 2006.

[125] Nancy G. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety*. Engineering systems. MIT Press, 2011. ISBN 9780262016629.

[126] Peter Lewycky. Notes toward an understanding of accident causes. *Journal of System Safety*, 23(2), 1987.

[127] Min Li, Wenbin Gu, Wei Chen, Yeshen He, Yannian Wu, and Yiying Zhang. Smart home: Architecture, technologies and systems. *Procedia Computer Science*, 131:393 – 400, 2018. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2018.04.219. Recent Advancement in Information and Communication Technology:.

[128] Yu Li, Yazhe Wang, and Yuan Zhang. Sechome: A secure large-scale smart home system using hierarchical identity based encryption. In Sihan Qing, Chris Mitchell, Liqun Chen, and Dongmei Liu, editors, *Information and Communications Security*, pages 339–351, Cham, 2018. Springer International Publishing. ISBN 978-3-319-89500-0.

[129] Yehui Liu. Study on smart home system based on internet of things technology. In Wenjiang Du, editor, *Informatics and Management Science IV*, pages 73–81, London, 2013. Springer London.

[130] Yuanyuan Liu, Bo Qiu, Xiaodong Fan, Haijing Zhu, and Bochong Han. Review of smart home energy management systems. *Energy Procedia*, 104:504 – 508, 2016. ISSN 1876-6102. doi: https://doi.org/10.1016/j.egypro.2016.12.085. Clean Energy for Clean City: CUE 2016–Applied Energy Symposium and Forum: Low-Carbon Cities and Urban Energy Systems.

[131] Gabriele Lobaccaro, Salvatore Carlucci, and Erica Löfström. A review of systems and technologies for smart homes and smart grids. *Energies*, 9(5), 2016. ISSN 1996-1073. doi: 10.3390/en9050348.

[132] Haneet Mahajan, Thomas Bradley, and Sudeep Pasricha. Application of stpa to a lane keeping assist system, 2017.

[133] Sioutis Marios. Area of effect and compromising techniques for the detection and resolution of environmental conflicts between services in the home network system. Master's thesis, Japan Advanced Institute of Science and Technology, Nomi, Ishikawa, March 2011.

[134] Fernando Mateo, Juan José Carrasco, Abderrahim Sellami, Mónica Millán-Giraldo, Manuel Domínguezc, and Emilio Soria-Olivas. Machine learning methods to forecast temperature in buildings. *Expert Systems with Applications*, 40(4):1061 – 1068, 2013. ISSN 0957-4174. doi: https://doi.org/10.1016/j.eswa.2012.08.030.

[135] E. Mazzi, A. S. Vincentelli, A. Balluchi, and A. Bicchi. Hybrid system reduction. In *2008 47th IEEE Conference on Decision and Control*, pages 227–232, Dec 2008. doi: 10.1109/CDC.2008.4739350.

[136] Daniel Meana-LloriÃ¡n, Cristian GonzÃ¡lez GarcÃa, B. Cristina Pelayo G-Bustelo, Juan Manuel Cueva Lovelle, and Nestor Garcia-Fernandez. Iofclime: The fuzzy logic and the internet of things to control indoor temperature regarding the outdoor ambient conditions. *Future Generation Computer Systems*, 76:275 – 284, 2017. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2016.11.020.

[137] Peter Mell and Tim Grance. The NIST Definition of Cloud Computing. Recommendation, National Institute of Standards and Technology, U.S. Department of Commerce, Sep. 2011.

[138] Xiangkun Meng, Guoming Chen, Jihao Shi, Gaogeng Zhu, and Yuan Zhu. STAMP-based analysis of deepwater well control safety. *Journal of Loss Prevention in the Process Industries*, 55: 41 – 52, 2018. ISSN 0950-4230. doi: https://doi.org/10.1016/j.jlp.2018.05.019.

[139] Sarah Mennicken and Elaine M. Huang. *Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[140] MIL-STD-882E. Department of defense standard practice: System safety. Standard, Department of Defense, USA, May 2012.

[141] Kohei Mitsui, Hiroshi Igaki, Masahide Nakamura, Ken-ichi Matsumoto, and Kentaro Takemura. Exploiting eye gaze information for operating services in home network system. In Hee Yong Youn, Minkoo Kim, and Hiroyuki Morikawa, editors, *Ubiquitous Computing Systems*, pages 13–27, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. ISBN 978-3-540-46289-7.

[142] M. Mohaqeqi and M. R. Mousavi. Sound test-suites for cyber-physical systems. In *2016 10th International Symposium on Theoretical Aspects of Software Engineering (TASE)*, pages 42–48, Jul 2016. doi: 10.1109/TASE.2016.33.

[143] Barbara A. Morrongiello and Sophie Kiriakou. Mothers' home-safety practices for preventing six types of childhood injuries: What do they do, and why? *Journal of Pediatric Psychology*, 29 (4):285–297, 2004. doi: 10.1093/jpepsy/jsh030.

[144] Haider Mshali, Tayeb Lemlouma, Maria Moloney, and Damien Magoni. A survey on health monitoring systems for health smart homes. *International Journal of Industrial Ergonomics*, 66:26 – 56, 2018. ISSN 0169-8141. doi: https://doi.org/10.1016/j.ergon.2018.02.002.

[145] A. Muzet, J. P. Libert, and V. Candas. Ambient temperature and human sleep. *Experientia*, 40(5):425–429, May 1984. ISSN 1420-9071. doi: 10.1007/BF01952376.

[146] Tatsuo Nakajima. Pervasive servers: A framework for creating a society of appliances. *Personal and Ubiquitous Computing*, 7(3):182–188, Jul 2003. ISSN 1617-4909. doi: 10.1007/s00779-003-0222-2.

[147] M. Nakamura, A. Tanaka, H. Igaki, H. Tamada, and K. Matsumoto. Adapting legacy home appliances to home network systems using web services. In *2006 IEEE International Conference on Web Services (ICWS'06)*, pages 849–858, Sept 2006. doi: 10.1109/ICWS.2006.23.

[148] Masahide Nakamura, Akihiro Tanaka, Hiroshi Igaki, Haruaki Tamada, and Ken ichi Matsumoto. Constructing home network systems and integrated services using legacy home appliances and web services. *International Journal of Web Services Research (IJWSR)*, 5(1):82 – 98, 2008.

[149] Masahide Nakamura, Akihiro Tanaka, Hiroshi Igaki, Haruaki Tamada, and Ken-ichi Matsumoto. Constructing home network systems and integrated services using legacy home appliances and web services. *International Journal of Web Services Research (IJWSR)*, 5(1):82–98, 2008. doi: 10.4018/jwsr.2008010105.

[150] Arun Kumar Nanda and C.K. Panigrahi. Review on smart home energy management. *International Journal of Ambient Energy*, 37(5):541–546, 2016. doi: https://doi.org/10.1080/01430750.2015.1004107.

[151] Maria Nedealcov and Zaharia Nedealcov. Evaluation of thermal comfort degree in canicular days - record for the republic of moldova's territory. *Present Environment and Sustainable Development*, 6:5 – 10, 2012.

[152] Hoaison Nguyen, Yoshiki Makino, Azman Osman Lim, Yasuo Tan, and Yoichi Shinoda. Building high-accuracy thermal simulation for evaluation of thermal comfort in real houses. In Jit

Biswas, Hisato Kobayashi, Lawrence Wong, Bessam Abdulrazak, and Mounir Mokhtari, editors, *Inclusive Society: Health and Wellbeing in the Community, and Care at Home*, pages 159–166, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-39470-6.

[153] Richard Nute. Hbse and risk assessment adventure on a tight-rope. In *2013 IEEE Symposium on Product Compliance Engineering (ISPCE)*, pages 1–5, Oct 2013. doi: 10.1109/ISPCE.2013.6664159.

[154] OB-007. Risk management. Standard AS/NZS 4360, Standards Australia/Standards New Zealand, 2004.

[155] Ministry of Defence. Safety Management Requirements for Defence Systems. Standard Defence Standard 00-56, Part 1 Issue 4: Requirement, UK Defence Standardization, Jun. 2007.

[156] Kazue Okamoto-Mizuno and Koh Mizuno. Effects of thermal environment on sleep and circadian rhythm. *Journal of Physiological Anthropology*, 31(1):14, May 2012. ISSN 1880-6805. doi: 10.1186/1880-6805-31-14.

[157] Min Ouyang, Liu Hong, Ming-Hui Yu, and Qi Fei. STAMP-based analysis on the railway accident and accident spreading: Taking the china–jiaoji railway accident for example. *Safety Science*, 48(5):544 – 555, 2010. ISSN 0925-7535. doi: https://doi.org/10.1016/j.ssci.2010.01.002.

[158] Etienne Pardo, David Espes, and Philippe Le-Parc. A framework for anomaly diagnosis in smart homes based on ontology. *Procedia Computer Science*, 83:545 – 552, 2016. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2016.04.255. The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016) / The 6th International Conference on Sustainable Energy Information Technology (SEIT-2016) / Affiliated Workshops.

[159] Etienne Pardo, David Espes, and Philippe Le-Parc. A framework for anomaly diagnosis in smart homes based on ontology. *Procedia Computer Science*, 83:545 – 552, 2016. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2016.04.255. The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016) / The 6th International Conference on Sustainable Energy Information Technology (SEIT-2016) / Affiliated Workshops.

[160] Jong Hyuk Park, Jungsuk Song, Byoung-Soo Koh, Deok-Gyu Lee, and Byoung-Ha Park. A hybrid intelligent multimedia service framework in next generation home network environment. In Marcin S. Szczuka, Daniel Howard, Dominik ŚlÈ©zak, Haeng-kon Kim, Tai-hoon Kim, Il-seok Ko, Geuk Lee, and Peter M. A. Sloot, editors, *Advances in Hybrid Information Technology*, pages 395–403, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-77368-9.

[161] Riccardo Patriarca, Giulio Di Gravio, and Francesco Costantino. A monte carlo evolution of the functional resonance analysis method (fram) to assess performance variability in complex

systems. *Safety Science*, 91:49 – 60, 2017. ISSN 0925-7535. doi: https://doi.org/10.1016/j.ssci.2016.07.016.

[162] Judea Pearl. The handbook of brain theory and neural networks. chapter Bayesian Networks, pages 149–153. MIT Press, Cambridge, MA, USA, 1998. ISBN 0-262-51102-9. URL http://dl.acm.org/citation.cfm?id=303568.303676.

[163] T. Perumal, A. R. Ramli, and C. Y. Leong. Design and implementation of soap-based residential management for smart home systems. *IEEE Transactions on Consumer Electronics*, 54(2): 453–459, May 2008. ISSN 0098-3063. doi: 10.1109/TCE.2008.4560114.

[164] Minh Pham, Yehenew Mengistu, Ha Do, and Weihua Sheng. Delivering home healthcare through a cloud-based smart home environment (coshe). *Future Generation Computer Systems*, 81:129 – 140, 2018. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2017.10.040.

[165] Sandor Plosz, Istvan Moldovan, Tuan Anh Trinh, and Andreas Foglar. Design and implementation of a practical smart home system based on dect technology. In Nikos Hatziargyriou, Aris Dimeas, Thomai Tomtsi, and Anke Weidlich, editors, *Energy-Efficient Computing and Networking*, pages 104–113, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. ISBN 978-3-642-19322-4.

[166] Ashlinn Quinn, James D. Tamerius, Matthew Perzanowski, Judith S. Jacobson, Inge Goldstein, Luis Acosta, and Jeffrey Shaman. Predicting indoor heat exposure risk during extreme heat events. *Science of The Total Environment*, 490:686 – 693, 2014. ISSN 0048-9697. doi: https://doi.org/10.1016/j.scitotenv.2014.05.039.

[167] Carsten R246cker, Maddy D. Janse, N. Portolan, and Norbert A. Streitz. User requirements for intelligent home environments: a scenario-driven approach and empirical cross-cultural study. In *sOc-EUSAI '05*, 2005.

[168] Iftikhar A Raja, J.Fergus Nicol, Kathryn J McCartney, and Michael A Humphreys. Thermal comfort: use of controls in naturally ventilated buildings. *Energy and Buildings*, 33(3):235 – 244, 2001. ISSN 0378-7788. doi: https://doi.org/10.1016/S0378-7788(00)00087-6.

[169] Jens Rasmussen. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-13(3):257–266, May 1983. ISSN 0018-9472. doi: 10.1109/TSMC.1983.6313160.

[170] Jens Rasmussen. Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2):183 – 213, 1997. ISSN 0925-7535. doi: https://doi.org/10.1016/S0925-7535(97)00052-0.

[171] P.P. Ray. A survey on internet of things architectures. *Journal of King Saud University - Computer and Information Sciences*, 30(3):291 – 319, 2018. ISSN 1319-1578. doi: https://doi.org/10.1016/j.jksuci.2016.10.003.

[172] Silja Renooij. Probability elicitation for belief networks: Issues to consider. *The Knowledge Engineering Review*, 16(3):255–269, September 2001. ISSN 0269-8889. doi: 10.1017/S0269888901000145. URL http://dx.doi.org/10.1017/S0269888901000145.

[173] Harper Richard, editor. *Inside the Smart House*. Springer-Verlag, Berlin, Heidelberg, 2003.

[174] Paul Salmon, Amy Williamson, Michael Lenné, Eve Mitsopoulos-Rubens, and Christina Rudin-Brown. Systems-based accident analysis in the led outdoor activity domain: Application and evaluation of a risk management framework. *Ergonomics*, 53:927–39, 08 2010. doi: 10.1080/00140139.2010.489966.

[175] Paul M. Salmon, Miranda Cornelissen, and Margaret J. Trotter. Systems-based accident analysis methods: A comparison of accimap, hfacs, and stamp. *Safety Science*, 50(4):1158 – 1170, 2012. ISSN 0925-7535. doi: https://doi.org/10.1016/j.ssci.2011.11.009.

[176] Amilcare Francesco Santamaria, Floriano De Rango, Domenico Falbo, and Domenico Barletta. Smarthome: a domotic framework based on smart sensing and actuator network to reduce energy wastes. *Proc.SPIE*, 9103:9103 – 9103, 2014. doi: 10.1117/12.2053328.

[177] Giordano Scarciotti and Alessandro Astolfi. Model reduction for hybrid systems with state-dependent jumps. *IFAC-PapersOnLine*, 49(18):850 – 855, 2016. ISSN 2405-8963. doi: https://doi.org/10.1016/j.ifacol.2016.10.272. 10th IFAC Symposium on Nonlinear Control Systems NOLCOS 2016.

[178] Alexandra Schieweck, Erik Uhde, Tunga Salthammer, Lea C. Salthammer, Lidia Morawska, Mandana Mazaheri, and Prashant Kumar. Smart homes and the control of indoor air quality. *Renewable and Sustainable Energy Reviews*, 94:705 – 718, 2018. ISSN 1364-0321. doi: https://doi.org/10.1016/j.rser.2018.05.057.

[179] Alexandra Schneider and Susanne Breitner. Temperature effects on health - current findings and future implications. *EBioMedicine*, 6:29 – 30, 2016. ISSN 2352-3964. doi: https://doi.org/10.1016/j.ebiom.2016.04.003.

[180] A. Schwung. Cyber-physical modeling of compression systems using hybrid automata. In *2015 IEEE International Conference on Automation Science and Engineering (CASE)*, pages 1125–1130, Aug 2015. doi: 10.1109/CoASE.2015.7294248.

[181] Hussain Shareef, Maytham S. Ahmed, Azah Mohamed, and Eslam Al Hassan. Review on home energy management system considering demand responses, smart technologies, and intelligent controllers. *IEEE Access*, 6:24498–24509, 2018. ISSN 2169-3536. doi: 10.1109/ACCESS.2018.2831917.

[182] Chen Shih-Yeh, Lu Yu-Sheng, Joel J. P. C. Lai Chin-Feng", editor="Rodrigues, Zhou Liang, Chen Min, and Kailas Aravind. A smart appliance management system with current clustering

algorithm in home network. In *Green Communications and Networking*, pages 13–24, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-33368-2.

[183] Jungwoo Shin, Yuri Park, and Daeho Lee. Who will be smart home users? an analysis of adoption and diffusion of smart homes. *Technological Forecasting and Social Change*, 134:246 – 253, 2018. ISSN 0040-1625. doi: https://doi.org/10.1016/j.techfore.2018.06.029.

[184] Z. Shiqi, W. Xiaohui, and C. Hongbing. Equipment control and environmental monitoring design of smart home. In *2018 Chinese Control And Decision Conference (CCDC)*, pages 513–517, Jun 2018. doi: 10.1109/CCDC.2018.8407186.

[185] Xuping Song, Shigong Wang, Yuling Hu, Man Yue, Tingting Zhang, Yu Liu, Jinhui Tian, and Kezheng Shang. Impact of ambient temperature on morbidity and mortality: An overview of reviews. *Science of The Total Environment*, 586:241 – 254, 2017. ISSN 0048-9697. doi: https://doi.org/10.1016/j.scitotenv.2017.01.212.

[186] John D. Spengler. Climate change, indoor environments, and health. *Indoor Air*, 22(2):89–95, 2012. doi: 10.1111/j.1600-0668.2012.00768.x.

[187] L. Spigel. *Domestic technologies and the modern home*, pages 383–398. Elsevier., 12 2012. ISBN 9780080471716. doi: 10.1016/B978-0-08-047163-1.00316-7.

[188] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454 – 1464, 2017. ISSN 0959-6526. doi: https://doi.org/10.1016/j.jclepro.2016.10.006.

[189] Roland Stull. Wet-bulb temperature from relative humidity and air temperature. *Journal of Applied Meteorology and Climatology*, 50(11):2267–2269, 2011. doi: 10.1175/JAMC-D-11-0143.1.

[190] Roland Stull. *Meteorology for Scientists and Engineers, 3rd Edition*, pages 53–56. University of British Columbia, 2011.

[191] Md Shakil Suleiman. Integration of legacy appliances into the smart home. Master's thesis, Dalhousie University, Halifax, Nova Scotia, Aug. 2015.

[192] Haibin Sun. *The Smart Home System Design Based on i.MX51 Platform*, pages 209–216. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012. ISBN 978-3-642-27708-5. doi: 10.1007/978-3-642-27708-5_28. URL https://doi.org/10.1007/978-3-642-27708-5_28.

[193] Dajiang Suo. A system theoretic analysis of the "7.23" yong-tai-wen railway accident, 2012.

[194] Masaru Suzuki, Takuro Shimbo, Toshiharu Ikaga, and Shingo Hori. Sudden death phenomenon while bathing in japan - mortality data. *Circulation Journal*, 81(8):1144–1149, 2017. doi: 10.1253/circj.CJ-16-1066.

[195] I Svedung and J Rasmussen. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. *Safety Science*, 40(5):397 – 417, 2002. ISSN 0925-7535. doi: https://doi.org/10.1016/S0925-7535(00)00036-9.

[196] Y. Tajika, T. Saito, K. Teramoto, N. Oosaka, and M. Isshiki. Networked home appliance system using bluetooth technology integrating appliance control/monitoring with internet service. *IEEE Transactions on Consumer Electronics*, 49(4):1043–1048, Nov 2003. ISSN 0098-3063. doi: 10.1109/TCE.2003.1261193.

[197] Yuji Takasaki, Tadakatsu Ohnaka, Yutaka Tochihara, Yumiko Nagai, Hiromitsu Ito, and Shiro Yoshitake. Environmental and behavioral conditions of bathing among elderly japanese. *Journal of Physiological Anthropology*, 26(2):235–240, 2007. doi: 10.2114/jpa2.26.235.

[198] Kato Takekazu, Cho Hyun Sang, Lee Dongwook, Toyomura Tetsuo, and Yamazaki Tatsuya. Appliance recognition from electric current signals for information-energy integrated network in home environments. In Mokhtari Mounir, Ismail Khalil, Bauchet Jérémy, Zhang Daqing, and Nugent Chris, editors, *Ambient Assistive Health and Wellness Management in the Heart of the City*, pages 150–157, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. ISBN 978-3-642-02868-7.

[199] Carolyn Talcott. Cyber-physical systems and events. In Martin Wirsing, Jean-Pierre Banâtre, Matthias Hölzl, and Axel Rauschmayer, editors, *Software-Intensive Systems and New Computing Paradigms*, pages 101–115. Springer-Verlag, Berlin, Heidelberg, 2008. ISBN 978-3-540-89436-0. doi: 10.1007/978-3-540-89437-7_6.

[200] Ying Tan, Mehmet C. Vuran, and Steve Goddard. Spatio-temporal event model for cyber-physical systems. In *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, pages 44–50, June 2009. doi: 10.1109/ICDCSW.2009.82.

[201] Ming Tao, Jinglong Zuo, Zhusong Liu, Aniello Castiglione, and Francesco Palmieri. Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes. *Future Generation Computer Systems*, 78:1040 – 1051, 2018. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2016.11.011.

[202] A. Tascikaraoglu, A.R. Boynuegri, and M. Uzunoglu. A demand side management strategy based on forecasting of residential renewable sources: A smart home system in turkey. *Energy and Buildings*, 80:309 – 320, 2014. ISSN 0378-7788. doi: https://doi.org/10.1016/j.enbuild.2014.05.042.

[203] Deborah A. Tertinger, Brandon F. Greene, and John R. Lutzker. Home safety: Development and validation of one component of an ecobehavioral treatment program for abused and neglected children. *Journal of Applied Behavior Analysis*, 17(2):159–174, 1984. doi: 10.1901/jaba.1984.17-159.

[204] Lanzisero Thomas. Applied safety science and engineering techniques: The asset safety management process. In *2012 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pages 1–6, May 2012. doi: 10.1109/LISAT.2012.6223105.

[205] Jin Tian, Juyi Wu, Qibo Yang, and Tingdi Zhao. Frama: A safety assessment approach based on functional resonance analysis method. *Safety Science*, 85:41 – 52, 2016. ISSN 0925-7535. doi: https://doi.org/10.1016/j.ssci.2016.01.002.

[206] Yutaka Tochihara, Nobuko Hashiguchi, Ikuko Yadoguchi, Yumi Kaji, and Shigeko Shoyama. Effects of room temperature on physiological and subjective responses to bathing in the elderly. *Journal of the Human-Environment System*, 15(1):13–19, 2012. doi: 10.1618/jhes.15.13.

[207] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, Jul 2003. ISSN 0018-9219.

[208] Guilherme Mussi Toschi, Leonardo Barreto Campos, and Carlos Eduardo Cugnasca. Home automation networks: A survey. *Computer Standards & Interfaces*, 50:42 – 54, 2017. ISSN 0920-5489. doi: https://doi.org/10.1016/j.csi.2016.08.008.

[209] Hoyt Tyler, Schiavon Stefano, Piccioli Alberto, Cheung Toby, Moon Dustin, , and Steinfeld Kyle. 2017 CBE Thermal Comfort Tool, 2018. URL http://comfort.cbe.berkeley.edu/. Center for the Built Environment, University of California Berkeley.

[210] Wataru Umishio, Toshiharu Ikaga, Kazuomi Kario, Yoshihisa Fujino, Tanji Hoshi, Shintaro Ando, Masaru Suzuki, Takesumi Yoshimura, Hiroshi Yoshino, Shuzo Murakami, and null null. Cross-sectional analysis of the relationship between home blood pressure and indoor temperature in winter. *Hypertension*, 74(4):756–766, 2019. doi: 10.1161/HYPERTENSIONAHA.119.12914.

[211] Peter Underwood and Patrick Waterson. A critical review of the stamp, fram and accimap systemic accident analysis models. *Advances in Human Aspects of Road and Rail Transportation*, pages 385 – 394, 07 2012.

[212] Peter Underwood and Patrick Waterson. Accident analysis models and methods: Guidance for safety professionals. *Loughborough: Loughborough University*, page 28, 2013.

[213] A. M. Vainio, M. Valtonen, and J. Vanhala. Learning and adaptive fuzzy control system for smart home. In *Developing Ambient Intelligence*, pages 28–47, Paris, 2006. Springer Paris. ISBN 978-2-287-47610-5.

[214] S. Valero, E. del Val, J. Alemany, and V. Botti. Enhancing smart-home environments using magentix2. *Journal of Applied Logic*, 24:32 – 44, 2017. ISSN 1570-8683. doi: https://doi.org/10.1016/j.jal.2016.11.022. SI:SOCO 2015.

[215] L. C. van der Gaag, Silja Renooij, Cilia L. M. Witteman, B. M. P. Aleman, and B. G. Taal. How to elicit many probabilities. In *Proceedings of the Fifteenth Conference on Uncertainty in Artificial Intelligence*, UAI'99, pages 647–654, San Francisco, CA, USA, 01 1999. Morgan Kaufmann Publishers Inc. ISBN 1-55860-614-9. URL http://dl.acm.org/citation.cfm?id=2073796.2073869.

[216] L.C. van der Gaag, S. Renooij, C.L.M. Witteman, B.M.P. Aleman, and B.G. Taal. Probabilities for a probabilistic network: a case study in oesophageal cancer. *Artificial Intelligence in Medicine*, 25(2):123 – 148, 2002. ISSN 0933-3657. doi: https://doi.org/10.1016/S0933-3657(02)00012-X. URL http://www.sciencedirect.com/science/article/pii/S093336570200012X.

[217] Axel van Lamsweerde. *Requirements Engineering*. A John Wiley and Sons, Ltd., Publication, 2009. ISBN 978-0-470-01270-3.

[218] J.A.F. van Loenhout, A. le Grand, F. Duijm, F. Greven, N.M. Vink, G. Hoek, and M. Zuurbier. The effect of high indoor temperatures on self-perceived health of elderly persons. *Environmental Research*, 146:27 – 34, 2016. ISSN 0013-9351. doi: https://doi.org/10.1016/j.envres.2015.12.012.

[219] J.A.F. van Loenhout, A. le Grand, F. Duijm, F. Greven, N.M. Vink, G. Hoek, and M. Zuurbier. The effect of high indoor temperatures on self-perceived health of elderly persons. *Environmental Research*, 146:27 – 34, 2016. ISSN 0013-9351. doi: https://doi.org/10.1016/j.envres.2015.12.012.

[220] G. Venkatarathnam. The coefficient of performance of an ideal air conditioner. *International Journal of Refrigeration*, 32(8):1929 – 1931, 2009. ISSN 0140-7007. doi: https://doi.org/10.1016/j.ijrefrig.2009.06.010.

[221] Jalonne L. White-Newsome, Brisa N. Sánchez, Olivier Jolliet, Zhenzhen Zhang, Edith A. Parker, J. Timothy Dvonch, and Marie S. O'Neill. Climate change and health: Indoor heat exposure in vulnerable populations. *Environmental Research*, 112:20 – 27, 2012. ISSN 0013-9351. doi: https://doi.org/10.1016/j.envres.2011.10.008.

[222] Wikipedia. *home*, 2018 (accessed Aug.). URL https://www.wikipedia.org/.

[223] David D. Woods, Erik Hollnagel, and Nancy Leveson. *Resilience Engineering: Concepts and precepts*. CRC Press, 1 edition, September 2006. ISBN 9780754649045.

[224] Nobuyoshi Yabuki, Takuya Onoue, Tomohiro Fukuda, and Shinji Yoshida. A heatstroke prediction and prevention system for outdoor construction workers. *Visualization in Engineering*, 1(1):11, Oct 2013. ISSN 2213-7459. doi: 10.1186/2213-7459-1-11.

[225] Chi Yang, Chang Liu, Xuyun Zhang, Surya Nepal, and Jinjun Chen. A time efficient approach for detecting errors in big sensor data on cloud. *IEEE Transactions on Parallel and Distributed Systems*, 26(2):329–339, Feb 2015. ISSN 1045-9219. doi: 10.1109/TPDS.2013.2295810.

[226] Zhengguo Yang. A safety model for highly networked home environment. Master's thesis, Japan Advanced Institute of Science and Technology, Nomi, Ishikawa, March 2012.

[227] Zhengguo Yang, Yuto Lim, and Yasuo Tan. Event-based home safety problem detection under the cps home safety architecture. In *2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE)*, pages 491–495, October 2013.

[228] Zhengguo Yang, Yuto Lim, and Yasuo Tan. A risk model for indoor environment safety. In *2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, pages 1–5, October 2017.

[229] Zhengguo Yang, Toshiaki Aoki, and Yasuo Tan. Modeling the required indoor temperature change by hybrid automata for detecting thermal problems. In *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pages 135–144, Dec 2018. doi: 10.1109/PRDC.2018.00024.

[230] Zhengguo Yang, Toshiaki Aoki, and Yasuo Tan. Multiple conformance to hybrid automata for checking smart house temperature change. In *2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, pages 1–10, Oct 2018. doi: 10.1109/DISTRA.2018.8601005.

[231] Zhengguo Yang, Yuto Lim, and Yasuo Tan. An accident model with considering physical processes for indoor environment safety. *Applied Sciences*, 9(22):4732, nov 2019. doi: 10.3390/app9224732. URL https://doi.org/10.3390/app9224732.

[232] Zhengguo Yang, Toshiaki Aoki, and Yasuo Tan. Multiple-conformance to hybrid-automata-modeled requirements for detecting indoor temperature anomalies. 2020. To be submitted.

[233] Zhengguo Yang, Yuto Lim, and Yasuo Tan. Prediction of heat-shock during bath by Bayesian networks. To be submitted, 2020.

[234] J. Yu, G. Cao, W. Cui, Q. Ouyang, and Y. Zhu. People who live in a cold climate: thermal adaptation differences based on availability of heating. *Indoor Air*, 23(4):303–310, 2013. doi: 10.1111/ina.12025.

[235] Xinghuo Yu and Yusheng Xue. Smart grids: A cyber–physical systems perspective. *Proceedings of the IEEE*, 104(5):1058–1070, May 2016. ISSN 0018-9219. doi: 10.1109/JPROC.2015.2503119.

[236] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, Feb 2014. ISSN 2327-4662. doi: 10.1109/JIOT.2014.2306328.

[237] Jing Zhao, Neng Zhu, and Shilei Lu. Productivity model in hot and humid environment based on heat tolerance time analysis. *Building and Environment*, 44(11):2202 – 2207, 2009. ISSN 0360-1323. doi: https://doi.org/10.1016/j.buildenv.2009.01.003. Special Issue for 2008 International Conference on Building Energy and Environment (COBEE).

[238] Bin Zhou, Wentao Li, Ka Wing Chan, Yijia Cao, Yonghong Kuang, Xi Liu, and Xiong Wang. Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renewable and Sustainable Energy Reviews*, 61:30 – 40, 2016. ISSN 1364-0321. doi: https://doi.org/10.1016/j.rser.2016.03.047.

[239] Daniel Oudin Åström, Forsberg Bertil, and Rocklöv Joacim. Heat wave impact on morbidity and mortality in the elderly population: A review of recent studies. *Maturitas*, 69(2):99 – 105, 2011. ISSN 0378-5122. doi: https://doi.org/10.1016/j.maturitas.2011.03.008.