A Safety Model for Highly Networked Home Environment

By Zhengguo Yang

A thesis submitted to
School of Information Science,
Japan Advanced Institute of Science and Technology,
in partial fulfillment of the requirements
for the degree of
Master of Information Science
Graduate Program in Information Science

Written under the direction of
Professor Yasuo Tan(JAIST)
Associate Professor Yikui Zhang(TU)

March,2012

A Safety Model for Highly Networked Home Environment

By Zhengguo Yang (0910215)

A thesis submitted to
School of Information Science,
Japan Advanced Institute of Science and Technology,
in partial fulfillment of the requirements
for the degree of
Master of Information Science
Graduate Program in Information Science

Written under the direction of
Professor Yasuo Tan(JAIST)
Associate Professor Yikui Zhang(TU)

and approved by
Professor Yasuo Tan(JAIST)
Professor Yoichi Shinoda(JAIST)
Associate Professor Azman Osman Lim(JAIST)
Professor Jiawan Zhang(TU)
Associate Professor Yikui Zhang(TU)

February,2012 (Submitted)

Contents

Chapter 1

Introduction

1.1 Research Scope

As the development of intelligent home devices, more and more home devices are networked that forms the home network system. For one thing, based on this home network system, techniques about home information (of home environment, home devices and home users, etc.) gathering, remote control and home device intelligent are highly developed. These bring people with very convenience and comfortable normal home lives. For another, this home network together with intelligent home devices and legacy home appliances make the whole home environment more complexity than ever. So the consequence of this is the increasing probability of the occurrence of safety problems during the work of home devices, during the interaction between home user and home devices within the home environment.

This research is mainly focus on how to detect these safety problems and make response to them based on the highly networked home environment. Figure 1.1 shows networked home devices with the internal network connecting with the external network. In area "A", the home user, home devices and the environment between them are the places where safety problems would happen. The home information is collected for example by different kind of sensors and then send them to the external network through the home gateway and, make an analysis there in order to detect safety problems, then send commands through home gateway to the home network.

In order to detect and make response to safety problems, firstly, an abstraction of the domestic environment is made, which is called domestic environment model. Then the concept of dependability is applied to the model. Based on that, we proposed a Finite State Machine for the domestic environment model. Next, some rules for fault tolerance, error avoidance and failure handling are used to ensure the domestic safe and make response to safety problems. The detailed explanation about these is discussed through out this document.

1.2 Target of the Research

The target of our research is to detect safety problems and emergency situations within the domestic environment, and then made some rules, by which to make respond to these safety problems and emergency situations in order to reduce property loss and keep residents safe. Our research is based on the Service Intermediary Model and our proposed system is deployed in such a model. For another, we assume all home appliances are highly networked, which means the integration of networked home appliances, data collecting devices, communication media, data storage, processing device/equipment and necessary software that are used for collection, transmission, storage, and manipulation of information. In order to achieve our target, we first took the whole domestic environment as a system and abstract a model from that. After that, the concept of dependability was applied to such a model. And then based on that we proposed a finite state machine to represent how does safety problems happen, and by using which way to detect and eliminate safety problems.

As we all know, home appliances provide their functions as service to other home appliances and/or home user. Home users and home appliances will in turn have reactions on these services. And also home users will initiatively use home appliances. During all these interactions, safety problems and emergency situations would happen. So a Domestic Environment Model (DEM) for the domestic environment was proposed based on these interactions. And the model for the domestic environment is the basis for our research. Because all the possible safety problems and emergency situations were supposed to be happen in the DEM.

We applied the concept of dependability to the DEM, which is a concept for the computer system in the past. The attributes of the dependability of the DEM were given. And the threats to the dependability of the DEM were analyzed. Based on these analyses, means of fault tolerance, error avoidance and failure handling were proposed in order to obtain dependability.

As for the fault tolerance part, we applied the concept of fault tree analysis to analyze some cases of domestic fire and proposed some rules for that. For the error avoidance and failure handling, based on the analysis of the dependability of the DEM, some rules are made and a finite state machine (FSM) for the DEM was proposed. It is important to use the FSM and make it clear about the relationship among different kinds of safety problems and emergency situations. Based on the FSM, the proposed system is possible to detect abnormal states and make predictions to the next state. The proposed rules for error avoidance and failure handling could be applied to the reaction of abnormal states.

Figure 1.2 shows the thought of our research, by which to achieve our target. It starts from the Real Domestic Environment, an abstraction is made to set up the Domestic Environment Model. The dependability concept is applied to the DEM. Then we made the third abstraction based on the dependability analysis that is the FSM. Based on these abstractions, our proposed system reacts to the real domestic environment and makes it safe.

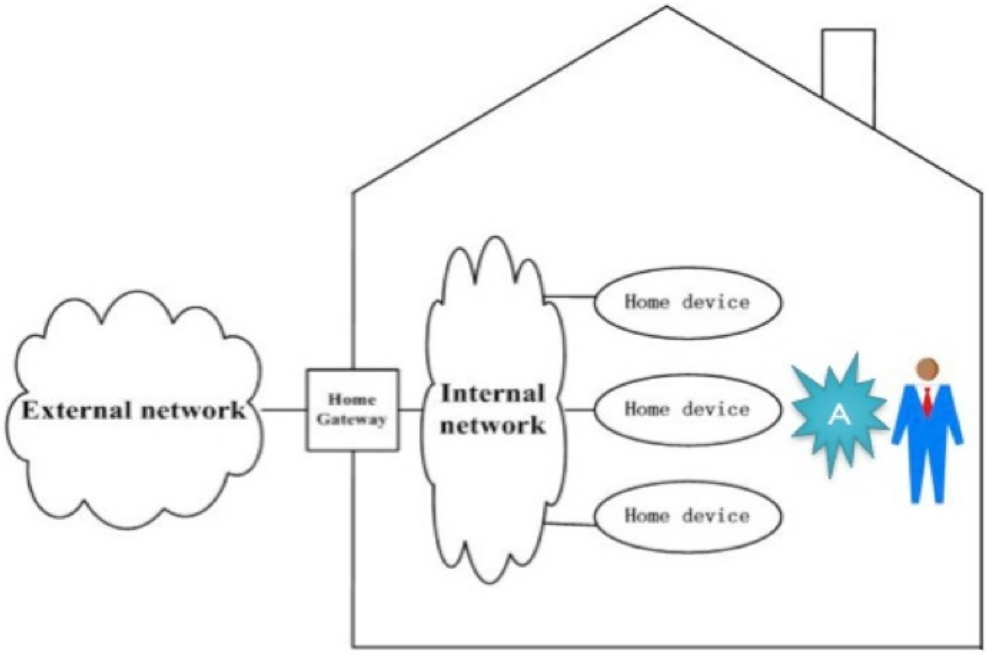

Figure 1.1: the home network connecting with external network

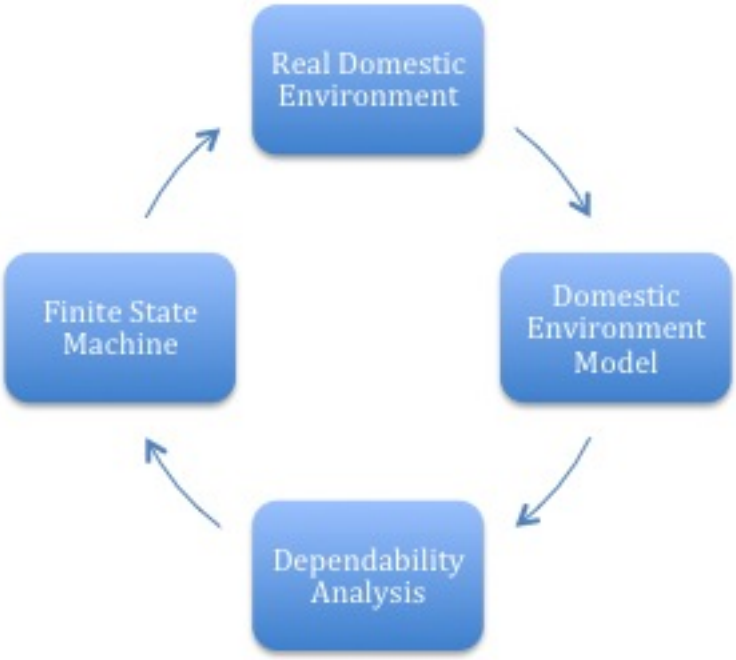

Figure 1.2: Overall thought of our research

1.3 Structure of This Document

The structure of this document is organized as follows:

In chapter 2, some related works are briefly given. They are mainly for gas leakage detection, fall detection and fire detection. Their advantages and disadvantages will also be given compare to our proposed system. Then we give an explanation on the safety problems of the domestic environment.

In chapter 3, a detailed explanation of the Domestic Environment Model will be presented. And what interactions would be happen in the DEM will also present.

In chapter 4, how the concept of dependability is applied to the DEM? What are the threats to the dependability of the DEM? What are the attributes of the dependability? And what are the means by which the dependability can be obtained? All these questions will be answered in this chapter.

In chapter 5, we analyzed some cases of domestic fires by using the concept of fault tree analysis. Based on these analyses, some rules are proposed in order for fault tolerance.

In chapter 6, The FSM of the DEM is going to be presented. We defined the states of the DEM, inputs and how transition happens from one state to another. Then rules for error avoidance and failure handling are given.

In chapter 7, our simulation work is done in this part. The simulation is done based on two cases: overload current and a fire caused by clothes dryer. The results show that the proposed system can detect abnormal states of the DEM.

In chapter 8, some conclusions and future work is going to be given.

Chapter 2

Research Background

Before move on, I would like to introduce some related works. They might have the following categories, which are for home abnormal event detection, fall detection, fire detection and gas detection. So in this chapter, we first introduce related works with respect to home safety. Then a classification of domestic safety problems is given. And this classification is mainly about the safety of home appliance, safety of indoor environment and safety of interaction between home user and home appliance. The following research is based on this classification.

2.1 Related Works

As the development of intelligent home network, more comfortable houses with high automation, which provided by home network, are come out. Many kinds of services are provided to home users fast and precisely in order to satisfy different kinds of need of home users. But in the other hand, this will also increase the complexity of domestic environment. Because, for one thing, even though many intelligent home appliances are introduced into the domestic environment, but some legacy home appliances are really hard to get rid of. These intelligent home appliance and legacy home appliances together will increase the complexity of home environment. For another, to the intelligent home appliances, it requires home users with higher knowledge to operate them. As we all know, they always need new, fresh knowledge to be operated. So to the home user's point of view, the home environment becomes complexity.

As for the increase complexity of domestic environment, indoor safety problems have a high probability to happen, which may cause property loss and danger home user's lives or even cause death. Big safety problem like fire, always have huge damage. [35] gives an estimation on U.S. fire by U.S. Fire Administration. Through the year of 2006 to the year of 2010, the number of fire happened in residential building is about 375900 in average, the number of deaths caused by residential fire is about 2588 in average, the number of injuries caused by residential fire is about 13010 in average and dollar loss is about 7372960000 in average. Now we can see how terrible the domestic environment can bring to us.

In the past, people make research in order to avoid these domestic safety problems. And indeed, some technologies are successfully applied to real domestic environment. For example, fire detection, gas detection and fall detection. Now lets get into them one by one.

Domestic fire is the most focused safety problem since people realized that it is so dangerous and they have to get rid of it. In the past, or event now, there always exist in any region or area, the fire department. This can be the original approach to fight with fire. Firemen wait for people to report a fire and then they can do their job. As the development of detection techniques, people use many different kinds of ways for detection. For example, Ali Rafiee and his workmates use wavelet analysis and disorder characteristics for fire and smoke detection [9]. A multilevel data fusion approach for early fire detection has done by Odysseas Sekkas and his workmates [8]. And in [10], Quanmin GUO and his workmates explained their fire detection model based on Fuzzy Neural Network.

Another safety problem focused by researchers is gas leakage or dangerous gas made by other materials like not fully burned honeycomb briquet. There are several ways in detecting the gas. The first one is to directly detect the gas concentration in domestic environment. As in [11], the proposed system will check whether the gas concentration is exceeding a certain pre-determined threshold. The second way is indirectly measure the gas concentration, [12] uses a variation of the induced electrical conductivity. Once the gas is absorbed, this electrical conductivity is determined by the free electrons and holes concentration in the solid.

A third concentration is fall detection. This is not for object falls, but for elderly and patient falls. It is said falls are the second leading cause of unintentional-injury death for people of all ages. When a fall was detected, a medical care would come earlier than that was not detected. And it will have a higher probability in saving people's lives. [5] divides the methods of fall detection into three approaches based on what sensors and how sensors are used. They are wearable device like [6], ambience device [4] and camera-based. And each approach will be divided into two or three classes according to the used principles. But some are beyond this classification, which means for fall detections we are not supposed to rely on machines. Education, awareness, exercises, etc. is also important in fall prevention [7].

Although the approaches introduced above solved their corresponding problem, to the more and more automation and complexity domestic environment, they still have shortcomings.

First, they only concern about one safety problem. In a high automation and complexity domestic environment, there are many different kinds of safety problems. For home safety, all domestic safety problems should to be considered.

Second, they didn't concern the relationship between one domestic safety problem and other domestic safety problems. How does one safety problem will affect (be affected by) others in causing safety problems?

Third, they are not concern problems like: how does one domestic safety problem forms. From some inefficient actions up to the form of a domestic safety problem, there exist a

path.

Fourth, after a safety problem was detected, just inform some department is not enough. Other actions should be done.

So a new approach, for safety problem detection and reaction to these safety problems, which should cover all domestic safety problems, is needed.

2.2 Safety Problems of the Domestic Environment

Before detection and reaction to domestic safety problems. We have to make it clear that what kinds of domestic safety problems are. [1] [3] gives a classification of domestic safety problems. They are local safety, global safety and environment safety. The local safety is defined by the safety instructions of individual networked appliances. The global safety happens when using multiple appliances simultaneously. And the environment safety is the residential constraints and rules in home and surrounding environments. But when multiple home appliances working together, sometimes even they do not have co-operation relationship, they can also affecting home appliances nearby. And for another, this classification didn't take home user into consideration.

Because of that, in my research I classified the domestic safety problems in the viewpoint of safety. And the classification also has three categories, which is shown in table 2.1 bellow. They are safety of home appliance, safety of indoor environment and safety of interaction between user and home appliance. Safety of home appliance means the safety problems that with respect to individual home appliance and this caused by not following its specification. For the safety of indoor environment, it is not only include the indoor environment, but also when multiple home appliances work together, the affection of other home appliances is also taken as the environment. And when home user is actively and/or inactively use or affect home appliances' safety is going to taken as the safety of interaction between user and home appliance. And for each sub-category, a brief explanation is descripted in table 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10 and 2.11.

Table 2.1: the classification of safety problems and its sub-categories

Big Category of Safety Problem	Sub-category of Safety Problem
Safety of home appliance	Unsteady energy supply
	Poor maintenance
	Abnormal internal-environment of appliances
	Electrical malfunction
	Electrical leakage
Safety of indoor environment	Abnormal indoor atmosphere
	Fire hazard
	Mechanical hazard
Safety of interaction between user and home appliance	Misuse of material
	Heat hazard

Table 2.2: Explanation of unsteady energy supply

Safety Problem	Cause	Preventive measure	Solution	Results
Unsteady energy supply	Power fluctuation	Electrical circuit check	Threshold	Out of work, harm users health, cause death
	Improper ventilation	Closeness check	Threshold	Harm users health, cause death
	Overload electrical circuit	Avoid using multiple large power appliances simultaneously	Threshold	Out of work

Table 2.3: Explanation of poor maintenance

Safety Problem	Cause	Preventive measure	Solution	Results
Poor maintenance	Component aging	Change at a fixed period	Maintenance	Out of work
	Component damage	Check frequently	Maintenance	Out of work
	Lack of maintenance	Maintenance frequently	Maintenance	Out of work
	Failure to clean	Clean after use	Maintenance	Out of work

Table 2.4: Explanation of abnormal internal-environment of appliances

Safety Problem	Cause	Preventive measure	Solution	Results
Abnormal internal-environment of appliances	Working temperature	Detection of abnormal change of temperature	Threshold	Out of work
	Working humidity	Detection of abnormal change of humidity	Threshold	Harm users health, cause death, out of work
	Static discharge	Use earth wire and other protection measures	Maintenance	Out of work, harm users health

Table 2.5: Explanation of electrical malfunction

Safety Problem	Cause	Preventive measure	Solution	Results
Electrical malfunction	Short circuit arc	Install protection device	Threshold	Out of work, harm users health, cause death
	Overload wiring	Avoid using multiple appliances plugging in one electrical outlet	Threshold	Out of work
	Electrical spark	Install protection device	Threshold	Harm users health, cause death, out of work
	Electrical failure	Check frequently	Maintenance	Out of work

Table 2.6: Explanation of electrical leakage

Safety Problem	Cause	Preventive measure	Solution	Results
Electrical leakage	Frayed electrical cord	Install electrical leakage protector	Maintenance	Out of work, harm users health, cause death
	Broken electrical outlet	Install electrical leakage protector	Maintenance	Harm users health, cause death, out of work
	Wet working environment	Avoid to contact with water and install electrical leakage protector	Threshold	Harm users health, cause death
	Improper insulation	Use authenticated appliance and install then professionally	Maintenance	Harm users health, cause death, out of work

Table 2.7: Explanation of abnormal indoor atmosphere

Safety Problem	Cause	Preventive measure	Solution	Results
Abnormal indoor atmosphere	Indoor temperature	Detection of abnormal change of temperature	Threshold	Out of work, harm users health
	Indoor humidity	Detection of abnormal change temperature	Threshold	Harm users health, cause death, out of work
	Dangerous gas	Good ventilation	Threshold	Harm users health, cause death
	Big smoke	Good ventilation	Threshold	Harm users health, cause death

Table 2.8: Explanation of fire hazard

Safety Problem	Cause	Preventive measure	Solution	Results
Fire hazard	Unattended cooking	Detection and education	Users position	Out of work, harm users health, cause death
	Combustibles nearby	Detection and education	Material detection	
	Smoking and children playing	Detection and education	Fire detection	
	Short circuit arc	Detection	Fire detection	
	Overload wiring	Detection	Fire detection	
	Electrical spark	Detection	Fire detection	
	Electrical failure	Detection	Fire detection	
	Smoldered trash or rubbish	Detection	Fire detection	
	Not work with plug in	Detection and education	Fire detection	

Table 2.9: Explanation of mechanical hazard

Safety Problem	Cause	Preventive measure	Solution	Results
Mechanical hazard	Fallen object	Education and do some protection	Fall detection	Out of work, harm users health, cause death
	Slips and falls	Additional equipment should be use in case of hurt	Fall detection	Harm users health, cause death, out of work

Table 2.10: Explanation of misuse material

Safety Problem	Cause	Preventive measure	Solution	Results
Misuse material	Cook with improper material	Education	Material detection	Out of work, harm users health, cause death
	Work with improper material	Education	Material detection	Harm users health, cause death, out of work

Table 2.11: Explanation of heat hazard

Safety Problem	Cause	Preventive measure	Solution	Results
Heat hazard	Burn	Wear protection clothes and gloves	Threshold	Harm users health, cause death
	Scalds	Wear protection clothes and gloves	Threshold	Harm users health, cause death

Chapter 3

Overview of Proposed System

In this section we will discuss how our proposed system is going to be deployed and how the real domestic environment was abstracted as a domestic environment model. First, a service model called Service Intermediary Model (SIM) will be introduced. Our proposed system will be deployed based on this model.

A service is provided by Service Providers (SP) to the Home Network System (HNS) in order to satisfy home user's specific need. The service may varying different kinds of functionality, for example, providing high speed calculation, smart in design making and regulation of energy consumption, etc. Our system is designed in order to provide services for safety problems detection and reactions to these safety problems. Now let us get into the first part, an introduction to the service intermediary model.

3.1 The Service Intermediary Model (SIM)

There are several conventional service models summarized in [13]. The method for service providing to home users in the HNS is to supply the user with specific, proprietary hardware that integrates tightly with the provided services. And also their disadvantages were discussed in [13]. We are not focus on that part, because it is beyond this documents research scope.

Although we may see the introduction from other materials, what we introducing here is mainly based on that of [13]. There are three main parts in the service intermediary model, which can be seen in figure 3.1.

The Service Provider (SP): This may be some companies that providing specific service in order to achieving some targets to the HNS.

The Home Gateway (HGW): It acts as a gateway of the HNS to the outside. It may gather information of home environment and requires services from outside. And execute services on its hardware, and then send commands to devices in the HNS.

The Service Intermediary (SI): the SI acts as a software bridge between the SP and the HGW. It registers service from different SPs and manages the prescribed services. Once HGW require services from SI and the SI access to the services of various SPs.

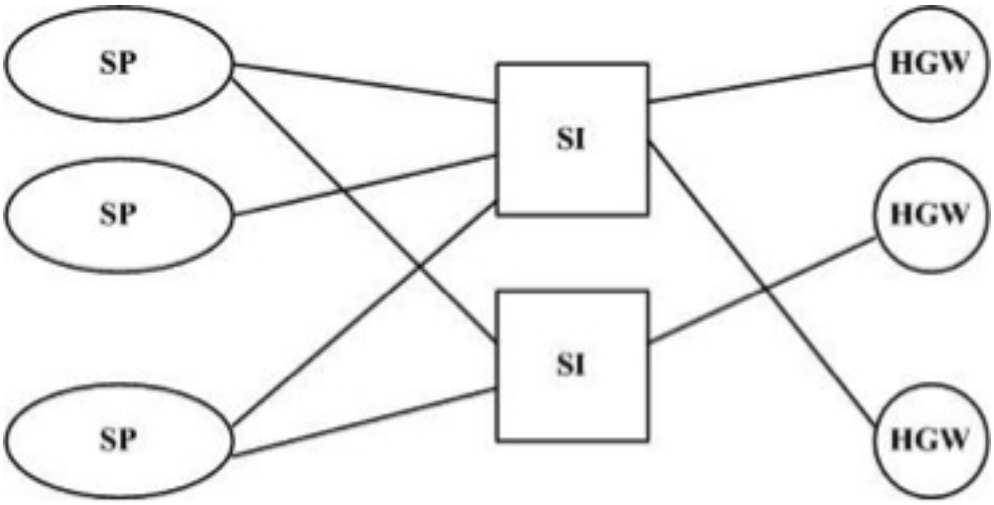

Figure 3.1: the service Intermediary Model

3.2 The System Deployment in the SIM

As discussed in section 2.2, our research is focus on the safety problems of domestic environment. Figure 3.2 shows the place where the safety problem would happen. These are home devices, home users and the environment among them. Sensors are deployed in the home environment to detect designate things. For example, a sensor used to detect temperature of the home environment, and another may used to detect the humidity. So obviously, sensors that deployed in the home environment, are used to collect information, which after analyze, something abnormal would be found.

The HGW here act as an information collector. It collects data from sensors and after packs them; the HGW will send them to SI, which our proposed system is deployed there. The system use these collected data and may require some services from outside SPs to make a final result about what the situation is. And then some commands are sent out to some departments and/or home users and/or let the HGW to control home devices in order to control the overall situation. The detailed technologies will be introduced in the following chapters.

3.3 Domestic Environment Model (DEM)

The concept of dependable computing is applied to a computer system, which addressing the trustworthiness of the delivered services. In my research, the dependability is introduced by trying to address the safety problem of domestic environment. The safety problems are happened by accompanying with some services delivery. And of course, the services here are quite different from that in computer systems. So what the services are? What are these services belong to? These questions will be answered in this section.

As described in the last section, we are focus on the safety of home appliances, safety of indoor environment and safety of the interaction between home user and home appliance. So, we need to set up a model for the domestic environment for the convenience of showing these safeties and also for the convenience of applying dependability.

3.3.1 The Interactions

Things like home appliances/devices, etc. within a house are designed to achieve some targets for serving home users by interacting with other things. In fact, we call them service providing, which will be introduced in chapter 4. During these services providing, safety problems have a probability to happen at the place where interactions happen. According to their functions of home appliances, we give a classification of home appliances that shown in table 3.1 and a detailed classification based on this table will be introduced in next section. Each type of home appliances may have similar ways of interaction with others.

Figure 3.3 roughly shows interactions of home appliances and interactions between home appliances and home users. They might be a mutual action or influence of a thing on other things within a domestic environment. It happens when using some interfaces of other things as input or serving other things as output or affecting by other thing's service. So the interactions here may have three fashions:

- Providing service to others: for example, power supply supplies electricity to home appliances; air-conditioner providing service to control domestic environment temperature.
- Receiving service from others: this happen to some things that passively receive service or being affected by other things. For example, multiple home appliance use hot water from a water heater, these home appliances may have conflicts when working at the same time. Another example is the indoor temperature would passively affected by room heater or air-conditioner.
- A mutual interaction which providing and receiving happens at the same time: This may happens when home user use a home appliance, for example, a home user may control air-conditioner by using remote controller and the air-conditioner will change the indoor temperature in order to affecting home user's feeling.

During these interactions, it has a probability for a safety problem to happen. A safety problem is an event that may cause property loss, casualty of home user or out of work of home appliances.

Table 3.1: classified home appliances

Categories of home appliances	Examples
Cooking appliance	Rice cooker, water heater, induction cooker, electric oven, microwave oven, toaster, gas range, hotplate and coffee maker
Temperature-control appliance	Air-conditioner, electric fan, electric blanket, electric heater, refrigerator, fan heater, electric hair dryer, fireplace, room heater
Cleaning appliance	Washing machine, dust collector, clothes dryer, dishwasher and electric iron
Entertainment appliance	TV set, electronic music instrument, radio, projector, recorder, audio/video recorder, cd/dvd player, video game consoles, home cinema
Others	Printer, kitchen ventilator, clocks, electric cord, electric outlet, tableware, humidifier, dehumidifier, indoor lights and receptacle

3.3.2 Abstraction of Domestic Environment

The abstraction of domestic environment is based on the interactions described above. Figure 3.4 shows the abstracted structure of the Domestic Environment Model (DEM). In the last section, we call home appliances and home devices things. Here we use another term for them - entity.

Definition of entity: it is a thing within the DEM, which has a specific function specified by its design and operation specification. An entity can be a system, e.g. a home appliance of air-conditioner, etc., a component/sub-system of a system, e.g. a faucet of a water supply system; an electrical wire of a power supply system, etc.

Definition of block: a block is a collection of entities when they satisfy one or more of the following conditions:

- They provide services to satisfy a specific need of home user, e.g. home appliances used for cooking;
- They belong to the same type of things, which for example a specific home appliance;
- They can be taken as components of a block, e.g. a pipe of gas supply system block.

Based on the terms of entity and block, let us see how the DEM is constructed. The DEM consists of three parts: the home architecture, which is the bottom layer; the infrastructure, which is the middle layer and home appliances, which is the top layer. They are constructed in such a sequence because of two reasons.

- When building a house, the architecture is the first thing to consider and then the infrastructure, the last thing is to introduce all kinds of home appliances.
- The second consideration is on the service providing. The architecture provides the fundamental need of other things of a house; the infrastructure provides resources to make sure that home appliances and home users can run normally. And home appliances are mainly used to achieve some targets of home users need.

As shown in figure 3.4, there is another part out of the DEM called The People. It includes home user, technologies and intruder. The Peoples activities will affect the domestic environment and the DEM will provide services to The People.

- Home user: It is the residents that lived in a house.
- Technologist: Persons who have expertise and work for a department in order to provide service like after-sale service, repairmen of a product, etc.
- Intruder: Persons who break into a house with malicious purpose.

So The People here actively interact with the DEM with malicious purpose, or usage purpose or repair purpose.

As we can see from figure 3.4, there are three layers of the DEM, the bottom layer, the middle layer and the top layer.

The bottom layer is the home architecture, which is a construction of the domestic environment. It mainly includes the interior part of a house that interact with internal entities. The entities included in the bottom layer are interior wall, floor, interior stair, ceiling, door and frames of window.

The middle layer is the infrastructure of a house that provide fundamental functionality to the normal working of upper layer appliances and living space to home user. The blocks that included in the middle layer are

- Electrical Power Supply,
- Water Supply/Drainage,
- Family Communication,
- Gas Supply,
- Living Space.

Table 3.2: an explanation of blocks of the middle layer

Block	Explanation	Included Entities
Electrical Power Supply	The electrical power system that provide electricity to domestic environment	Electrical Wire, Voltmeter, Switches, Electrical outlet, etc.
Water Supply/Drainage	The water supply and drainage system, which provide drinking water to domestic environment and drain waste water out of domestic environment	Water supply pipes, Drainage Pipes, Faucet, etc.
Family Communication	The telephone and computer network within a domestic environment	Telephone line, Internet line, Router, etc.
Gas Supply	The gas supply system that provide gas for cooking or/and warming purpose	Gas transmission pipeline, Gas can, Gas valve, etc.
Living Space	The space that home user lived in with all kinds of home appliances	The living space within domestic environment

Table 3.2 gives a detail explanation of the above five blocks.

The top layer consists of all kinds of home appliances that can provide different kinds of services to satisfy home user's need. It includes blocks of

- indoor air control appliance,
- cooking appliance,
- cooking related appliance,
- illumination appliance,
- cleaning appliance,
- communication and entertainment appliance,
- furniture and others,

which table 3.3 gives a detailed explanation of that.

Table 3.3: an explanation of blocks of the middle layer

Block	Explanation	Included Entities
Indoor Air Control Appliance	Appliances that used to control indoor temperature, humidity, etc.	Air-conditioner, Electrical fan, Electrical heater, Fan heater, Room heater, Kitchen ventilator, Humidifier, Dehumidifier, Range hood, etc.
Cooking Appliance	Appliances that used for cooking	Rice cooker, Water heater, Induction cooker, Electric oven, Microwave oven, Toaster, Hotplate, Coffee maker, etc.
Cooking Related Appliance	Appliances that used to process, store food in order to assist cooking	Gas range, Disinfector, Refrigerator, Food mixer, etc.
Illumination Appliance	Appliances used for illumination	All kinds of lamps and lanterns used indoor
Cleaning Appliance	Appliances used for cleaning	Dish washer, Washing machine, Dust collector, Cloth dryer, etc.
Communication and Entertainment Appliance	Appliances used for communication and entertainment	Telephone, Computer, TV set, Radio, Projector, A/V Recorder, Video game console, Home cinema, etc.
Furniture	Movable articles that are suitable for living	Table, Chair, Bed, Tableware, Cups, etc.
Others	Entities that not included in above blocks	Clock, Electrical blanket, Shaver, Hair dryer, ect.

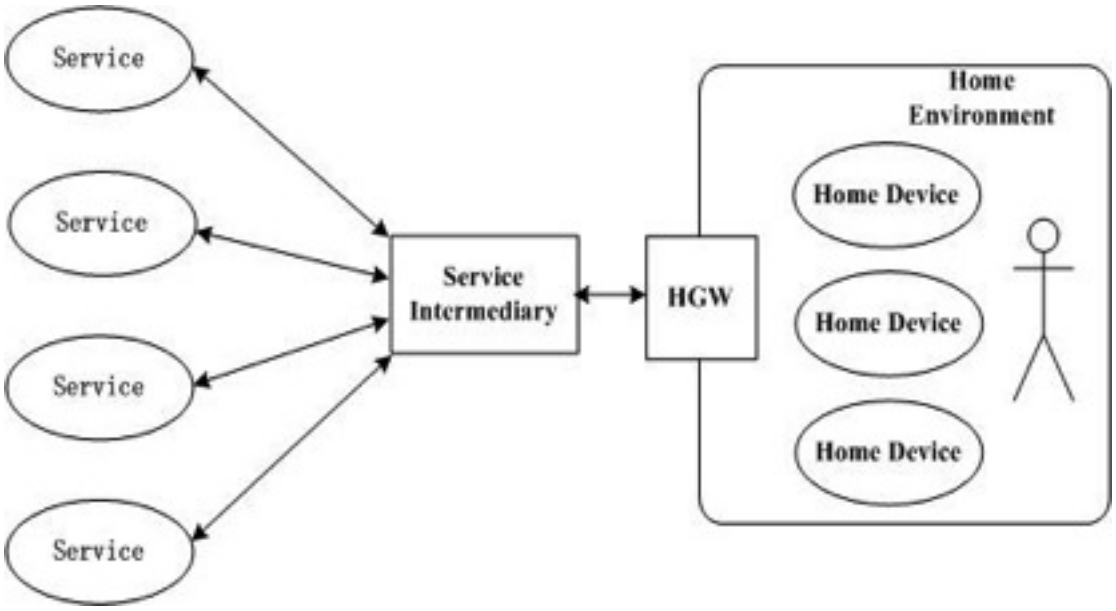

Figure 3.2: the overall topology

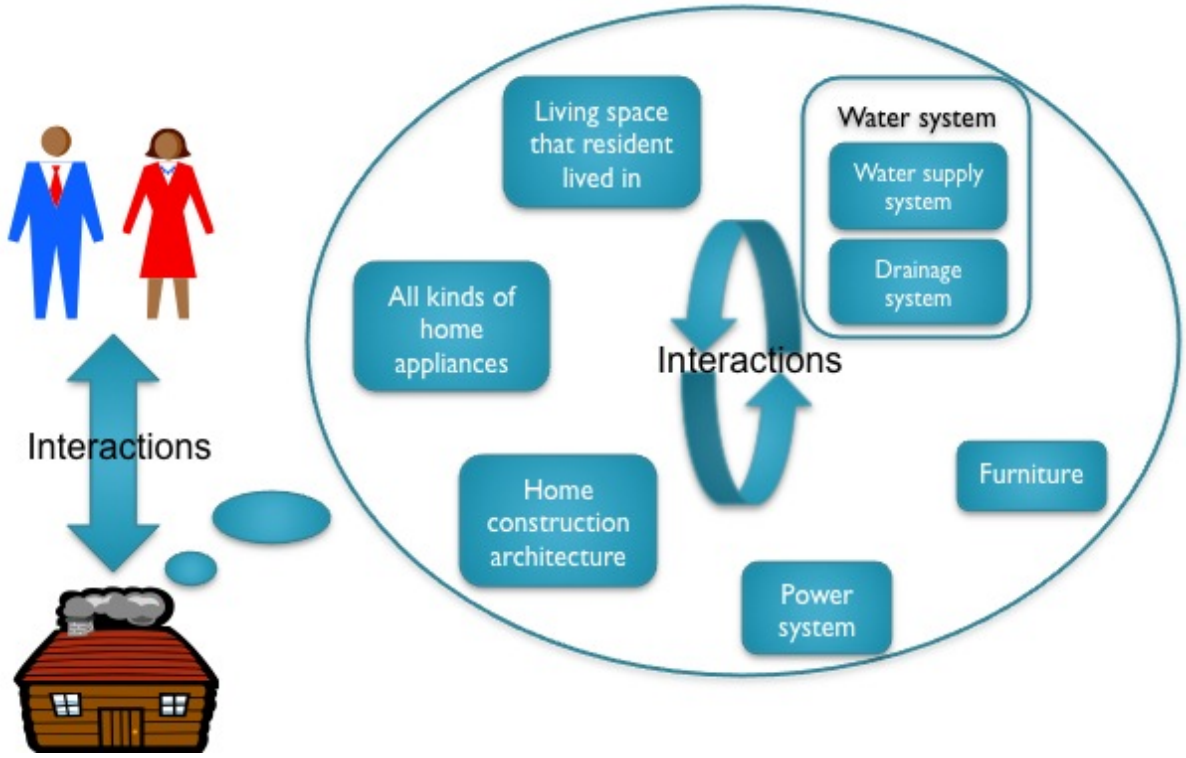

Figure 3.3: rough descriptions of interactions of domestic environment

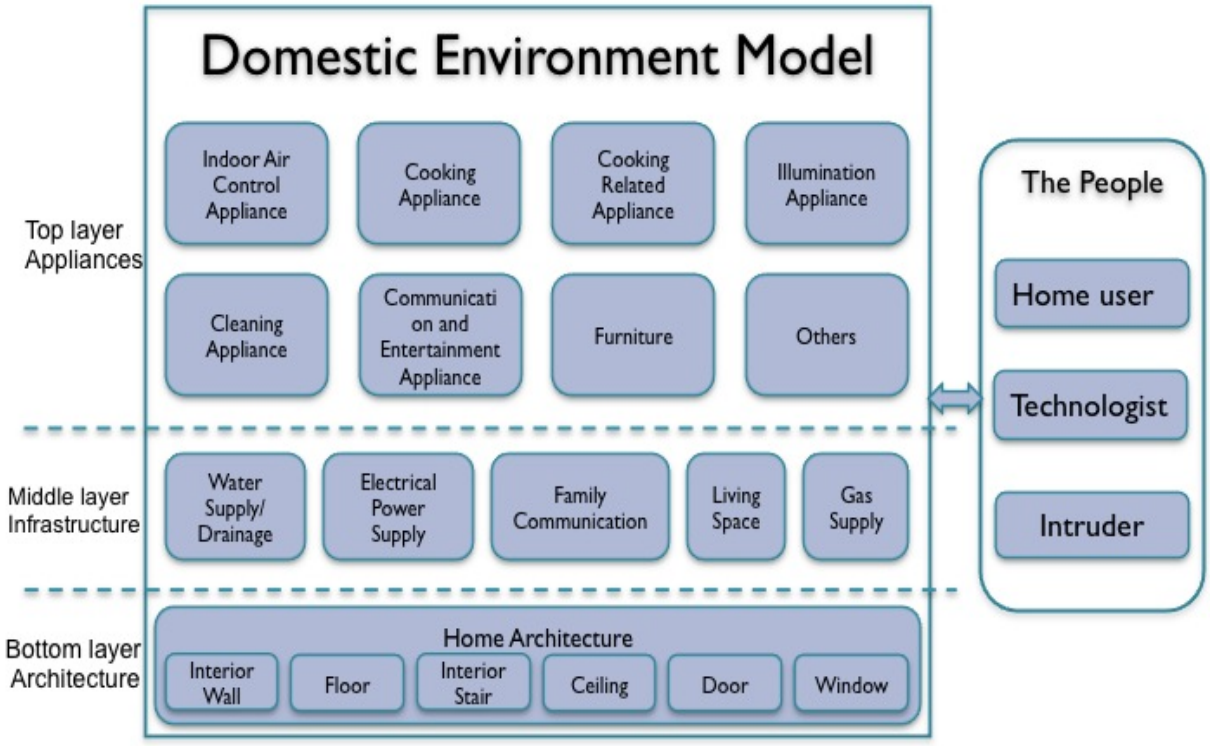

Figure 3.4: the Domestic Environment Model and The People

Chapter 4

Dependability of Domestic Environment Model

The concept of dependability was first employed to improve the reliability of the unreliable components of electronic computers. As developed for centuries, for one thing it has developed more mature than ever, for another its application varies from software to hardware of computing systems. In our research, we apply this to the DEM. And use this concept for the analysis of dependability of the DEM and uses means of fault tolerance, error avoidance and failure handling to obtain the dependability of the domestic environment.

In this chapter we first give a brief introduction of the concept of dependability. Then give the definition and detailed explanation of how the concept was applied to the DEM model.

4.1 Original Concept of Dependability

The origin and integration of the concept of dependability was introduced in [17]. The concept of dependability computing first appeared in the 1830's in the context of Babbages Calculating Engine. At the same time, J. von Neumann, E.F. Moore and C.E. Shannon and their successors used multiple redundant components to build the reliable logic structures. After that W.H. Pierce unified the theories of making redundancy. Then more and more things like error detection, fault diagnosis, etc. were added. From 1970, the information of the IEEE-CS TC on Fault-Tolerant Computing in 1970 and of IFIP WG 10.4 Dependable computing and Fault Tolerance in 1980 accelerated the emergence of a consistent set of concepts and terminology.

The following introduction on the concept of dependability is based on [14], [15], [16], [17]. Be attention that the concept of dependability is quite different from the concept of secure computing. The concept of secure computing and their differences can be found on some of the cited references by this document and other materials, which if the readers of this document are interested in, you can find them by yourself.

The concept of **dependability** consist of three parts:

- the threats to,
- the attributes of, and
- the means by which dependability is attained

which we can see from figure 4.1.

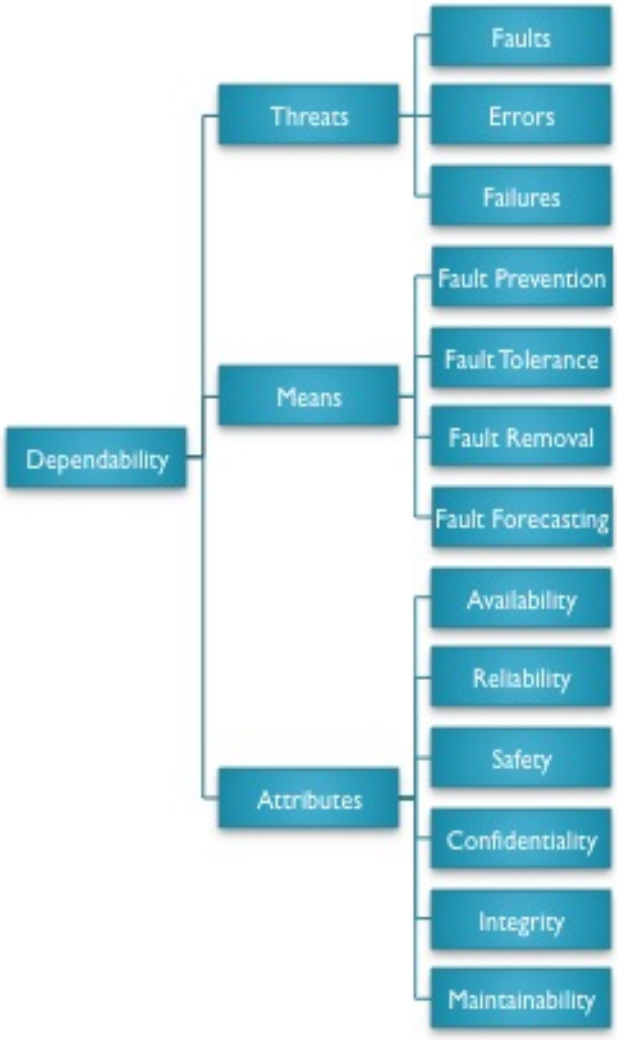

Figure 4.1: the dependability tree

Before move on, there are some other concepts should be introduced.

- The **service** delivered by a system is its behavior as it is perceived by its users; a **user** is a physical entity or a person that interacts with the former at the service interface.
- The **function** of a system is what the system is intended for, and is described by the system specification.

- **Correct service** is the service that implements the system function.

As we can see from figure 4.1, the threats including faults, errors and failures. A failure is an event that occurs when the delivered service deviates from the correct service. An error is a part of the system state that may cause a subsequent failure. When an error reaches the service interface and alters the service, we say a failure occurs. A fault is the adjudged or hypothesized cause of an error.

The attributes of dependability are used to describe its properties, which can be differentiating from other concepts like security. It encompasses the following attributes:

- availability: readiness for correct service;
- reliability: continuity of correct service;
- safety: absence of catastrophic consequences on the users and the environment;
- confidentiality: absence of unauthorized disclosure of information;
- integrity: absence of improper system state alterations;
- maintainability: the ability to undergo repairs and modifications.

The above attributes may be emphasized to a greater or lesser extent depending on the application.

The means include four techniques: fault prevention, fault tolerance, fault removal and fault forecasting. Fault prevention is attained by quality control techniques employed during the design and manufacturing of hardware and software. Fault tolerance generally implemented by error detection and subsequent system recovery and it is intended to preserve the delivery of correct service in the presence of active faults. Fault removal consists of three steps during the development phase: verification, diagnosis and correction. During the operational life of a system, the fault removal is corrective or preventive maintenance. And for the fault forecasting, it is performed when evaluation of a system behavior with respect to fault occurrence or activation.

4.2 The Definition of the Dependability of Domestic Environment

After the introduction of original concept of dependability, let us get into our definition of dependability for the DEM. Before move on let me give some preliminary knowledge.

- The **function** of an entity is what the entity is intended to do. It is described in its product design and operation specification.
- The **behavior** of an entity is what the entity does to implement its function and is described by a sequence of states.

As discussed in last chapter, entities are interacting with each other according to the services they provide. The **service** here should be the provider's (to be introduced later) functional behaviors that can be perceived by its users and is represented by a sequence of external states (the effect caused by its functional behavior) of the provider. And if the delivered service implements the provider's function with no safety problem happening, then we call it **correct service**.

Another concept is the provider/user that represent entities' roles when interaction happens. As discussed, each entity provides services to other entities that interact with it, and also can receive services from other entities.

- **Provider**: it's the entity that provides services to other entities at its service interface where service delivery happens.
- **User**: it's another entity that receives services from its provider(s) at its user interface.

The provider/user concept is a relative concept, which is explained in figure 4.2.

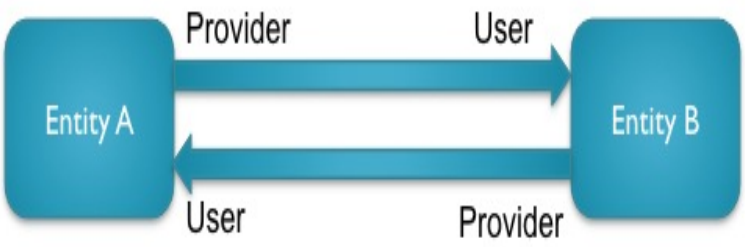

Figure 4.2: the relationship between provider and user

Assume entity A and B, when entity A provide service to entity B, we say, entity A is the provider, entity B is the user. When entity B provide service to entity A, we say, entity B is the provider and entity A is the user.

The definition of dependability in computing system is the ability to deliver service that can justifiably be trusted [17]. We use this definition for the DEM, and use a criterion

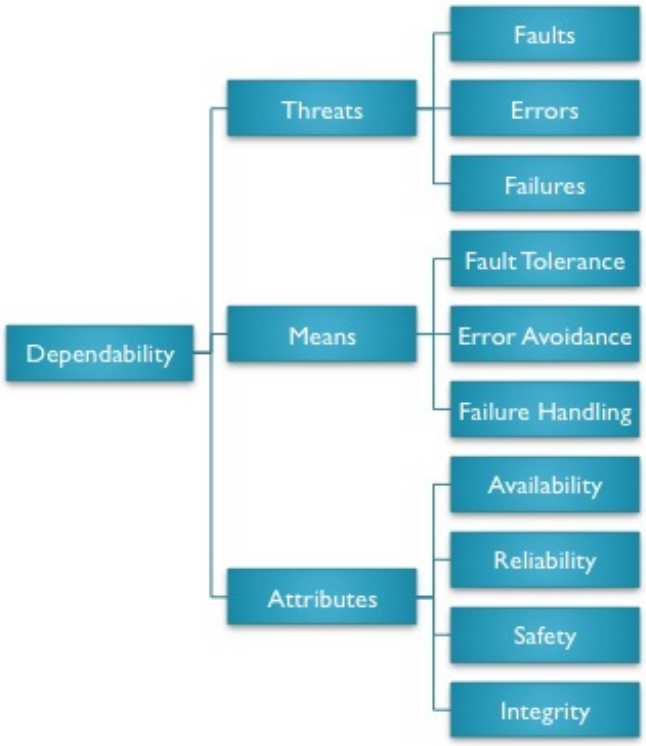

Figure 4.3: the dependability for the DEM

for deciding whether a service is dependable. The criterion is the ability of the DEM to avoid service failures that are emergency situations to the domestic environment and home users. The dependability for the DEM is still consists of three part, but with different content for the DEM.

- The **threats** to the DEM,
- The **attributes** of the DEM, and
- The **means** by which dependability is attained

As shown in figure 4.3:

4.2.1 The Threats to Dependability

Providers provide service to its users, but the provided services not always correct. When services are incorrect, we call that service failure. A **service failure** is an event that an entity's behavior generates a safety problem by not following its function. A service failure happens either because it does not comply with its function; or because it complies with some malicious purpose. But service failures are not always happened in the same way. The forms that the deviations from correct service are called **service failure modes**.

The service failure modes characterize incorrect services according to the following three items.

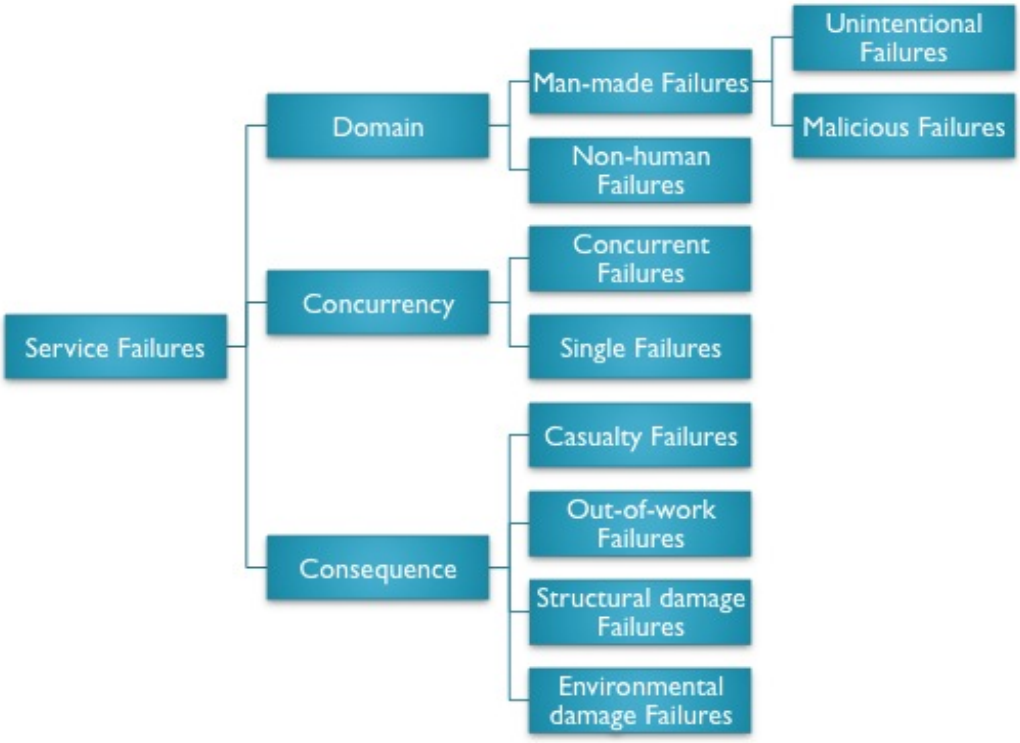

Figure 4.4: classifications of service failures

- The failure domain,
- The concurrent failures, and
- The consequence of failures to domestic environment and home user.

And this is described in figure 4.4.

The domain was defined according to that whether human take part into the service failure. For the man-made failure, some failures are caused by unintentional activities and some others may be caused by malicious purposes.

Most of the cases, it is understandable for one service failure to cause other failures. When more than one failure (no matter they have relationships or not) happens at the same time, it is called concurrent failures. While only one failure happens, we call that single failure.

After a service failure has happened, the consequence varies of different kind. It may cause casualty, out-of-work, structural damage and environmental damage.

As described, failures are caused by errors when they enter the service interface and alter the service. So what are errors of the DEM? An **error** is a part of the entity states, which represent an abnormal changing. As we all know, a failure's happen is the accumulation of something. When the accumulation exceeds lets say a threshold value, a failure happen. And errors may cause subsequent failures when reaches the entities service interface and change the entitys behavior. We classify errors according to the accidents

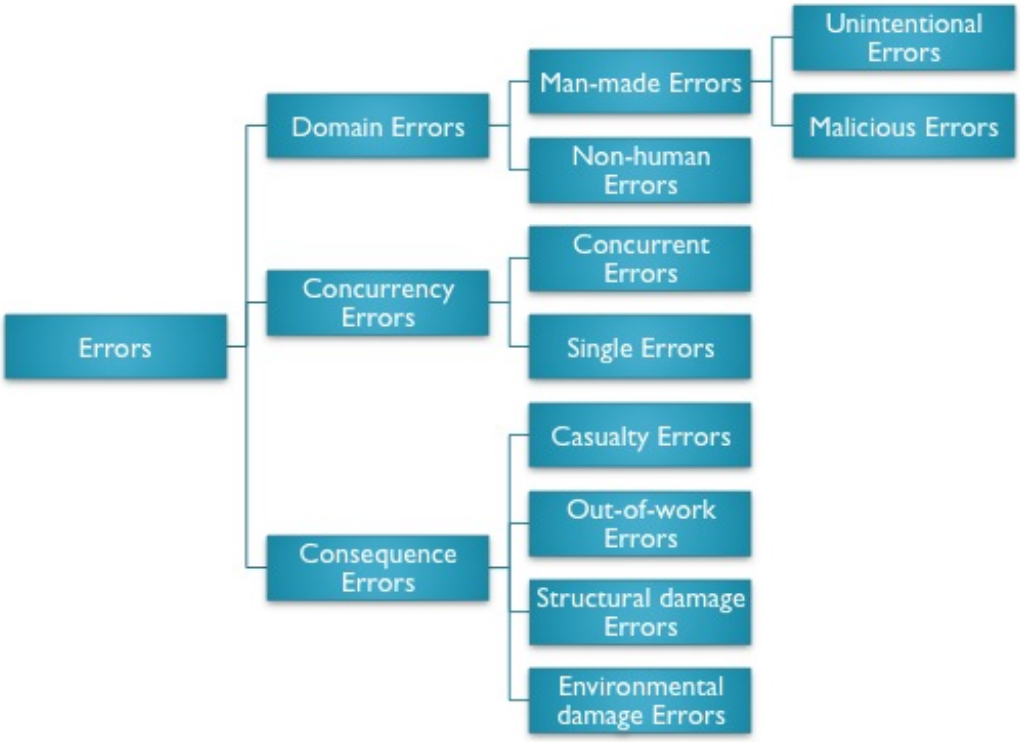

Figure 4.5: the classification of errors

that they cause and are shown in figure 4.5. Because errors are classified according to the failures that they cause, the explanation of these errors are easy to understand.

The last threat to dependability is **fault**, and we define it as the reasons that can generate an error and it can be internal or external fault of an error. When a fault occurs from internal of an entity, it is called internal fault. When a fault occurs because of external reasons, it is called external fault. Sometimes a fault cannot be detected until it active. A fault is active when it causes an error and the classification of faults is shown in figure 4.6.

The faults can be classified according to four different approaches: the scope, intent, boundaries and persistence. For the scope, some faults are related to electricity and some are with respect to of physics. The intent here is mainly of human's intention. Some are with malicious and some are without. The Boundary classification has already introduced. And the last one is persistence, to some faults they may really hard to eliminate or maybe repeatedly occurrence or may happens for a short limited of times, that the classification of permanent and transient.

The relationship of threats is shown in figure 4.7. A fault is the cause of an error within an entity. An error may cause other errors within an entity. When an error reaches the service interface and alters the entitys services, which may cause a failure. The failure of an entity may affect other entities and generate external faults to other entities.

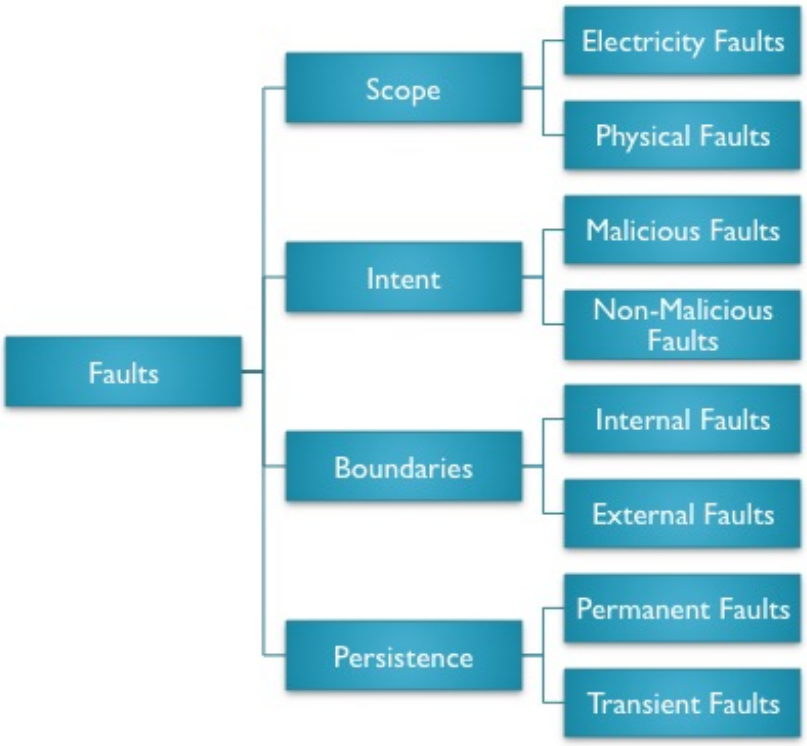

Figure 4.6: the classification of faults

4.2.2 The Attributes of Dependability

As for the DEM, we hope every home appliances are ready for use without losing their function. If not, lets say an inactive fault exists, or errors happen when operating. This may generate failures and cause safety problem and/or emergency situations. If an entity is working, the intent situation is that the entity successfully accomplishes a task without causing safety problems and/or emergency situations. In other word, we want an entity to provide continuous correct services. And in all of its working states, there is no other factors or reasons that alter its states. After working, there is no catastrophic consequence either on home user or on the domestic environment.

So the attributes of dependability of the DEM are availability, reliability, safety and integrity.

- **Availability**: readiness for correct service;
- **Reliability**: continuity of correct service;
- **Safety**: absence of catastrophic consequence on home users and the domestic environment;
- **Integrity**: absence of improper system state alterations.

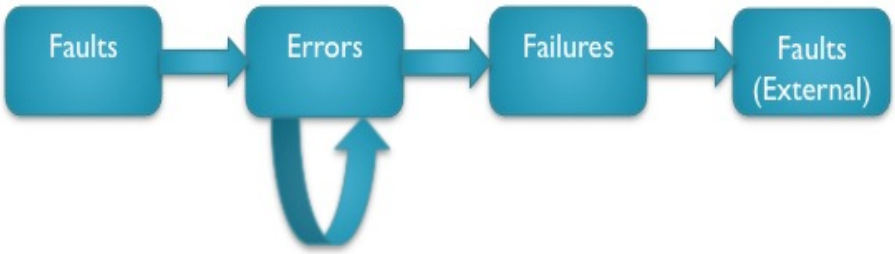

Figure 4.7: the relationships of the threats

4.2.3 The Means to Obtain Dependability

In order to ensure these attributes and obtain dependability of the DEM, the means of fault tolerance, error handling and failure handling are proposed.

For the fault tolerance, first we analyzed event of fires that happened within the DEM environment by using the concept of fault tree analysis (FTA). By doing this, we can find out the basic events (the reasons) why a safety problem is happened. Based on these basic events, we can propose the right approach for fault tolerance.

For error avoidance and failure handling, we are using the concept of finite state machine to setup a model for the DEM. In the model, we defined the states of the DEM and make it clear of their transition relationship. When something abnormal is detected, adjusting measure will be used for error avoidance to keep the DEM safe and failure treatment for failure handling to reduce the damage to the DEM and harm home users.

The more detailed description will be introduced in chapter 5 and chapter 6.

Chapter 5

Fault Tolerance for the DEM

In this chapter we are going to discuss fault tolerance for the DEM. Originally, fault tolerance is intended to preserve the delivery of correct service in the presence of active faults. It may uses two techniques, one is error detection and another is subsequent system recovery. For the error detection, it can use the finite state machine that is going to introduce next chapter. For subsequent system recovery, redundancy technologies always used for computing systems. But for the DEM, it is a very complexity system. For each safety problem, we have to know what are the original reasons. Based on these reasons we propose our ways for fault tolerance.

The rest of this chapter is organized as follows; we first introduce the concept of fault tree analysis. After that we are going to analysis some case of fire hazard based on the concept of fault tree analysis in order to get the original reasons for the fire hazard. Based on that several rules are going to be proposed for fault tolerance of the DEM.

There are some step in the FTA and some ground rules for analysis.

5.1 The Concept of Fault Tree Analysis

The concept of fault tree analysis (FTA) introduced in this section is based on [18] [19]. And also the concept of FTA is used in other research areas [20] [21]. Here we use it for the analysis of some cases of fire hazard. The definition is given in [18]: FTA can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety or reliability standpoint), and the system is then analyzed in the contest of its environment and operation to find all realistic ways in which the undesired event (top event) can occur. In other words, FTA is trying to find out certain specified causes lead to one specified TOP event of interest.

1. System Definition
   System design and component operation: for this part, it has already done in section 3.3.

   The analysis of TOP event: The TOP events in my research are these situations bellow:

- Any event that can cause casualty of home user;
- Any event that can cause home property loss.

Examples are like: Fire Hazard, Mechanical hazard, Electrical malfunction, Out of work of home appliances, etc.

2. Fault Tree Construction
Fault Tree Symbols: Primary event symbols, Gate symbols and Transfer symbols. The description for each event should include what and when. What is happening and when does that happen?

Boundary Conditions:

- The physical boundaries of analysis: all the included entities in my research.
- Interfaces to the system (such as power source or water supply), if not, their state (inputs to a contributor) need to be defined.
- External stresses: in my research, they are activities caused mainly by The People - home user, technologist and intruder.

Ground Rules: The FTA is deductive, top-down fashion approach, which has several rules for construction of fault tree.

Ground Rule 1: Write the statements that are entered in the event boxes as fault; state precisely what the fault is and the conditions under which it occurs. Do not mix successes with faults.
Rule 1 consists two parts: what and when. "what" describes the relevant failed state of the component; "when" describes the condition under which the failed state occurring.

Ground Rule 2: If the answer to the question "Is this fault a component failure?" is "Yes", classify the event as a "state of component fault". If the answer is "No", classify the event as a "state of system fault".
As a general rule, when energy originates from a point outside the component, the event may be classified as "state of system".

No Miracles Rule: If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.

Complete-the-Gate Rule: All inputs to a particular gate should be completely defined before further analysis of any one of them is undertaken.

No Gate-to-Gate Rule: Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates.
Another statement for fault tree contribution can also be taken as a rule. That is think small - the necessary and sufficient immediate events that result in the top event.

Depth to which a fault should be constructed: The general principal is that the fault tree should developed to the necessary depth to identify functional dependencies and to a depth that is consistent with the data available and the objectives of the analysis.

3. Fault Tree Evaluation
   In this part, there are two types of ways for evaluation. One is qualitative evaluation, and another is quantitative evaluation.
   The qualitative evaluation has two techniques Binary Decision Diagram and Minimal Cut Set. They are trying to find out which are the main basic reasons for a TOP event. And the quantitative evaluation is an approach trying to find out who has the bigger probability in contributes the TOP event.

5.2 Cases Analysis by Using FTA

In this section, we are going to analyze some cases of fires happened in domestic environment by the approach of FTA, and trying to get the basic event for the top event. These cases are based on [22] [23] [24] [25] [26] [27] [28].

5.2.1 Case 1: air-conditioner fire

The fire that caused by air-conditioner would be due to two reasons, one is power supply and another is the air-conditioner itself. As mentioned in last section, the reasons of design and manufacturing, which contribute to the fire is not going to be analyzed. Because designers and manufacturers are supposed to take responsible for that. And figure 5.1 shows the FTA of analyzed result. And two basic events here are contributing to the air-conditioner fire: the fire caused by electric wire overheats and short circuit.

5.2.2 Case 2: Clothes dryer fire

For the clothes dryer fire, it seems more complexity than air-conditioner fire. There three big reasons for that, one is the clothes dryer itself, another is its venting system and the last one is the energy supply. And the analyzed result by using FTA is shown in figure 5.2. From the picture we know, the basic events are drying clothes of flammable material, component aging of dryer, the time and/or temperature of heating of clothes is beyond the required, improper use of material of duct between the vent and the clothes dryer, the dryers vent is too long and contain sharp turns and bends (compromised vent), failure to clean of lint inside duct, improper connection of plug and outlet to the dryer and gas leakage.

5.2.3 Case 3: Mattress and bedding fires

We classified mattress and bedding fires into two types with respect to whether human take part into the activity. The detailed explanation can be seen in figure 5.3. And the basic events for mattress and bedding fires can be playing with cigarettes, lighters, matches or candles, flammable material nearby, smoking while lying on bed, flammable materials of mattress and beddings and arson

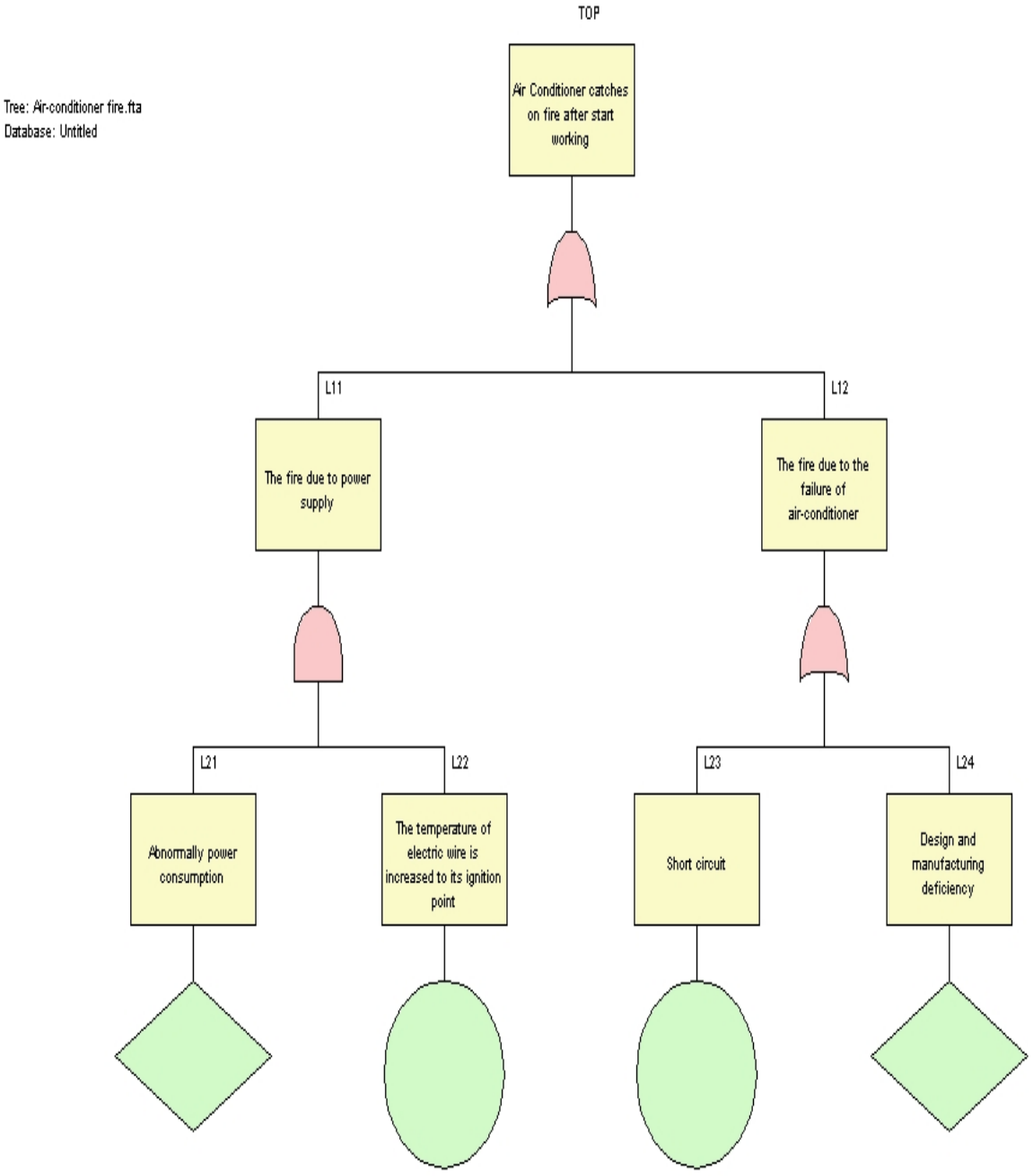

Figure 5.1: the analysis of the air-conditioner fire by using FTA

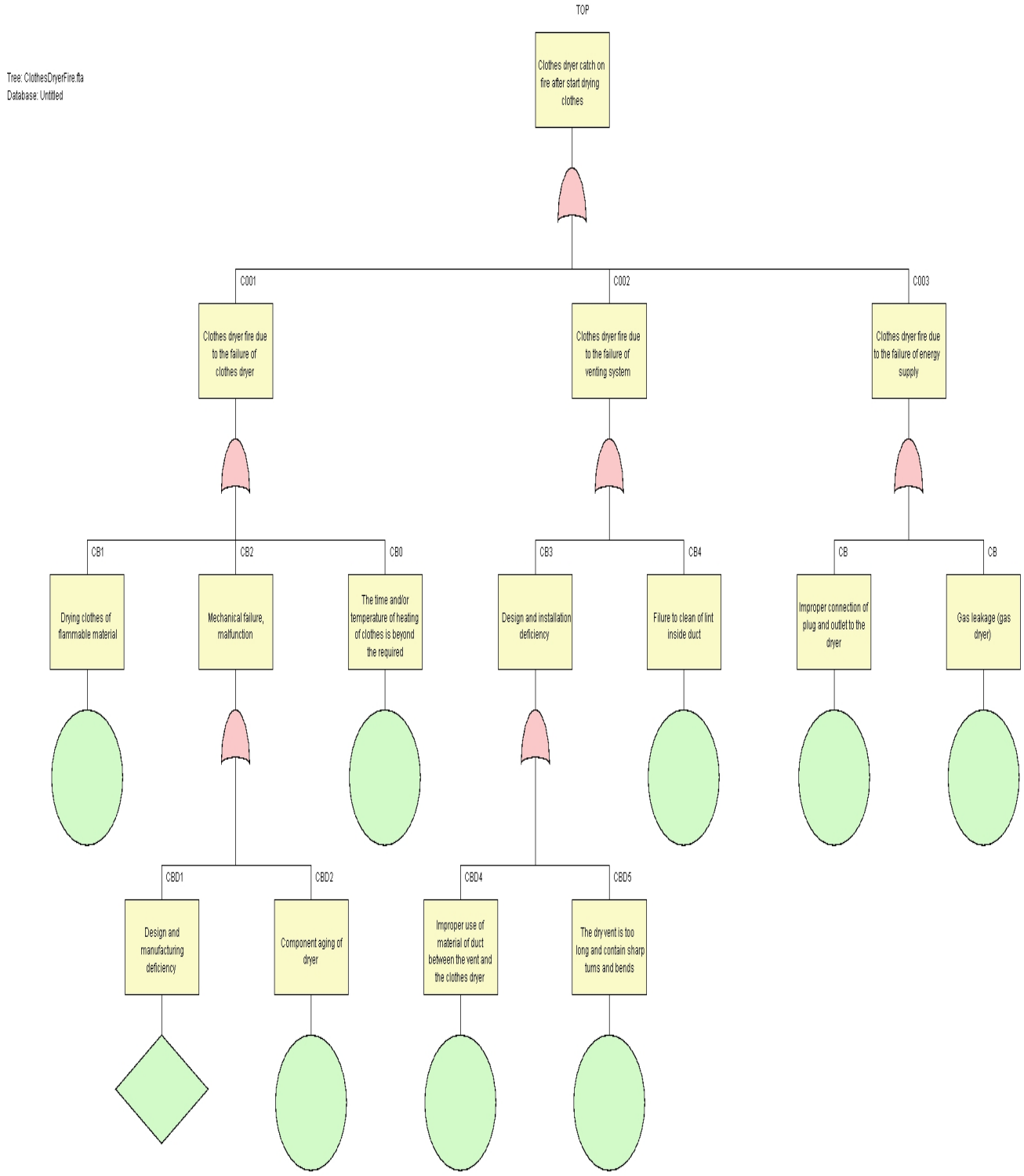

Figure 5.2: the analysis of clothes dryer fire by using FTA

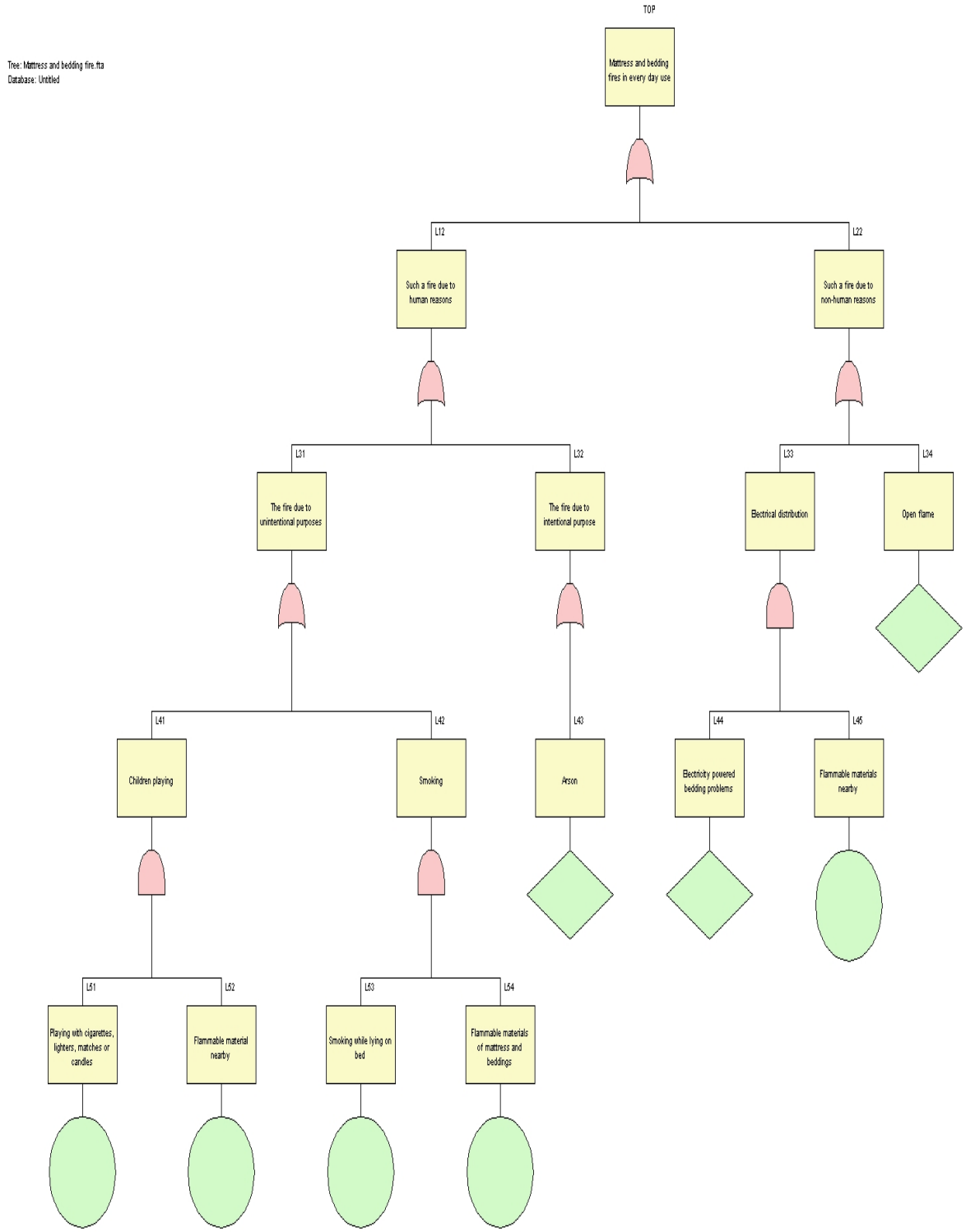

Figure 5.3: the analysis of mattress and bedding fire by using FTA

5.2.4 Case 4: Portable heater fires

A portable heater is flexible to put anywhere you want to keep warm. That increases the probability to catch a fire. We analyze it according to three big categories: one is a portable heater itself, another is the power supply and the last is human activities. And because of the character of portable, the human activities take more probability than the other two categories. Figure 5.4 shows the FTA of the analysis of portable heater. The basic reasons are unsteady power supply, unspecified short circuit arc, too close to combustibles and equipment unattended.

5.2.5 Case 5: Residential building electrical fire

This supposed to be the fire caused by the overall power supply system. This maybe because of two reasons, one is failure of the electric wire and another should be appliances like outlet, etc., which attached to the electric wire. And the analyzed result is shown in figure 5.5. From the picture we know the basic events would be unspecified short-circuit arc ignite flammable material nearby, short-circuit arc from defective, worn insulation, which ignite flammable material nearby, arc from faulty contact, broken conductor, which ignite flammable material nearby and overloading that create enough heat to ignite flammable material nearby.

5.2.6 Case 6: Structure cooking fire

Cooking is the leading cause of fires and fire injuries in structures. And cooking with unattended is the leading factor that contributes to cooking fire. According to the analysis, cooking fire is mainly due the careless of human being. Figure 5.6 shows the detailed analysis. The basic events are unattended equipment, misuse of material or product and having the heat source too close to combustibles and abandoned or discarded materials or products.

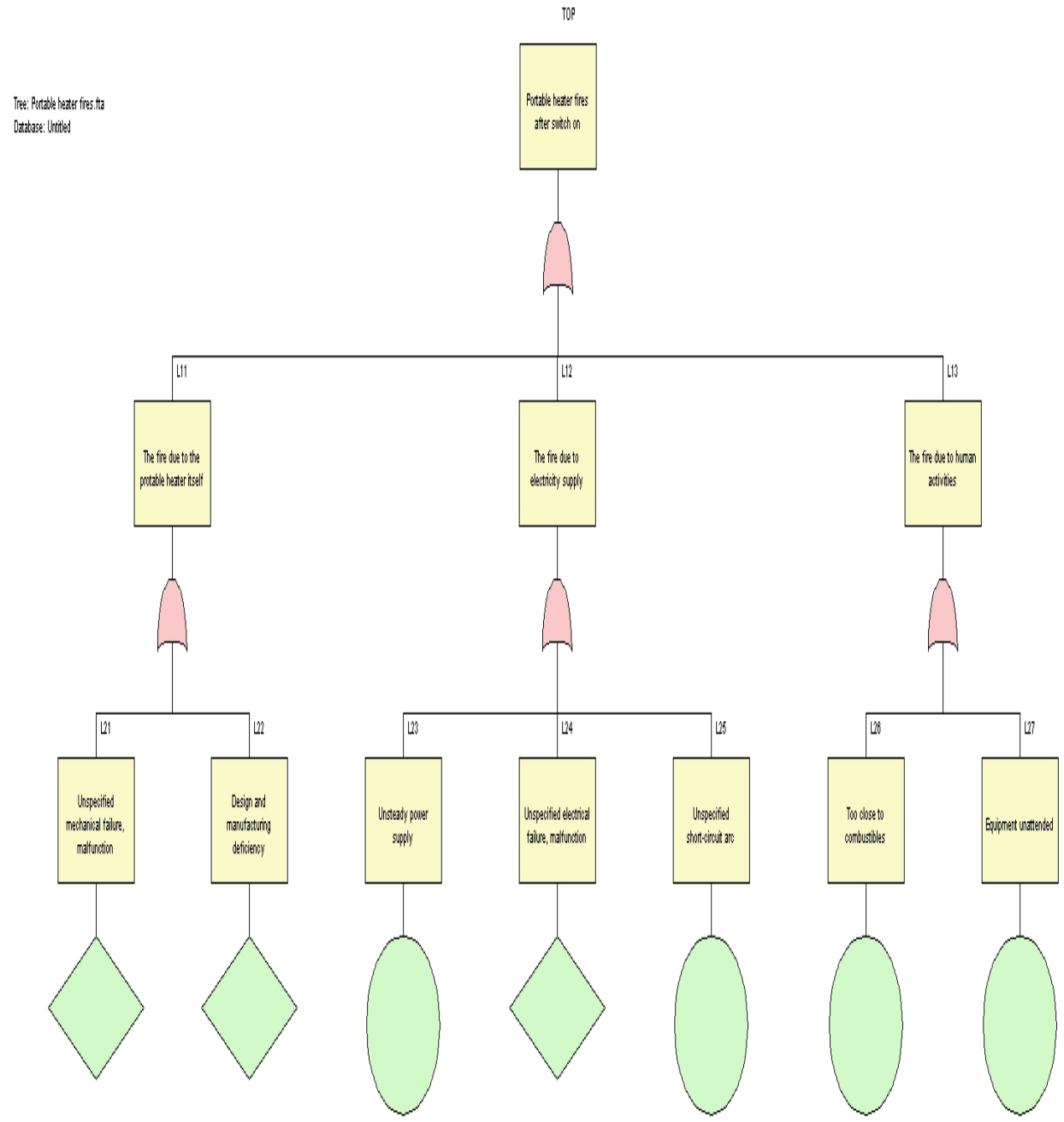

Figure 5.4: the analysis of portable heater fire by using FTA

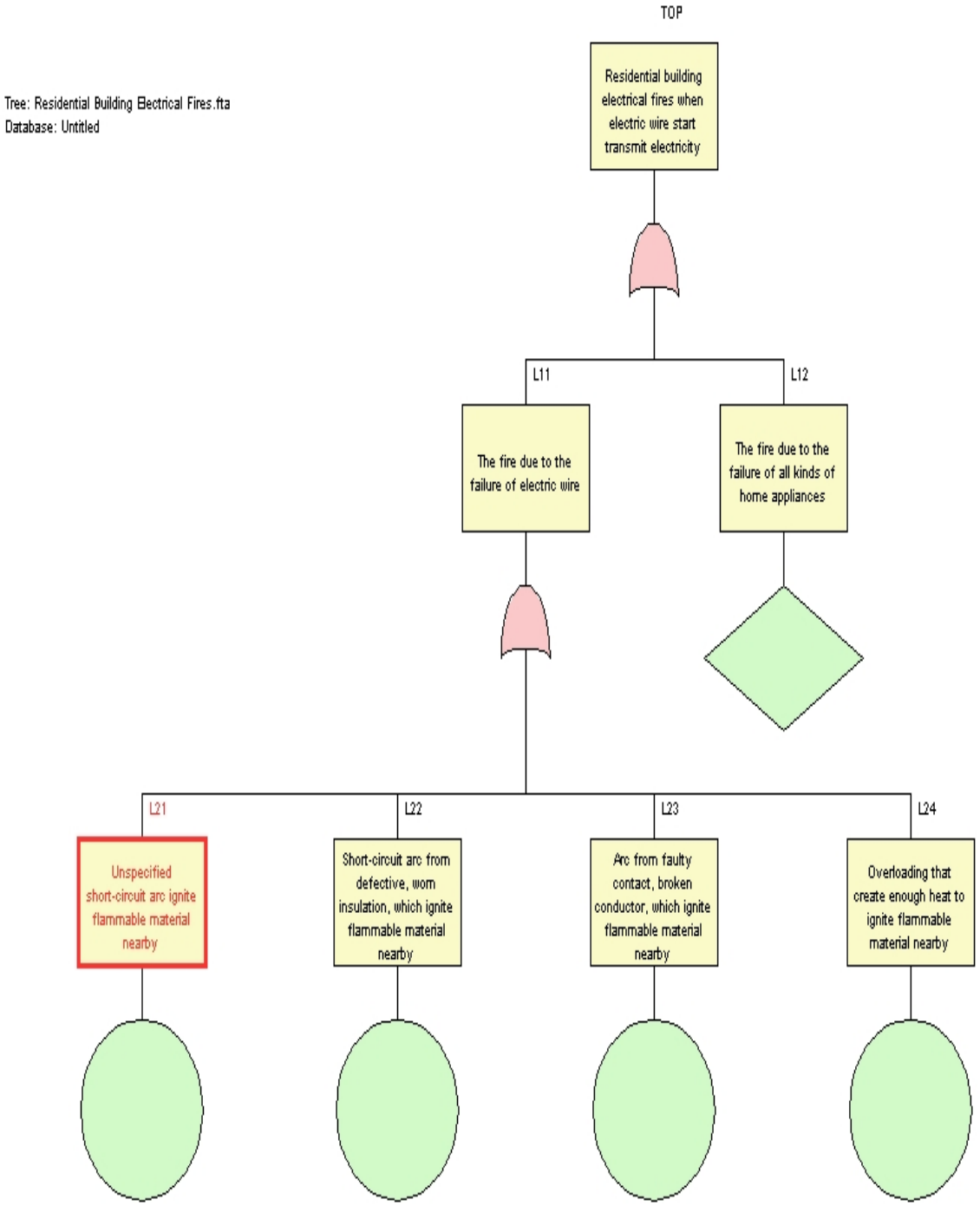

Figure 5.5: the analysis of residential building electrical fires by using FTA

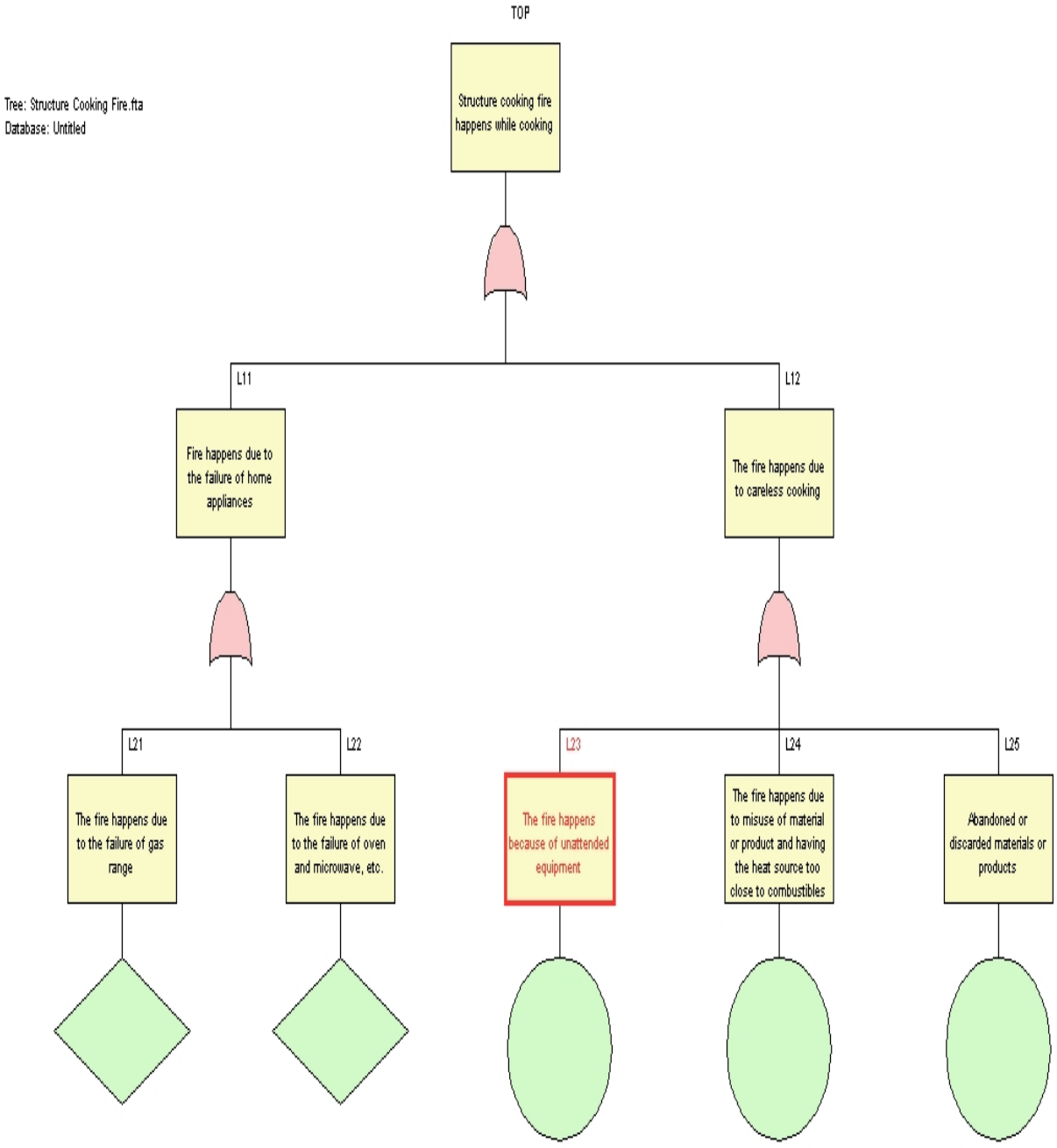

Figure 5.6: the analysis of structure cooking fire by using FTA

5.3 Fault Tolerance Approach Based on the Analysis

Based on the cases above, we classify the basic events into several categories, which is shown in table 5.1. The human activity is the activity that would generate fire hazard inside the domestic environment. And other categories of overloading, short circuit, component aging, improper installation and flammable material, are easy to understand.

As we all know, the requirement for a fire to happen should be two things. The first is **enough heat**, and the second is **flammable material**. Then we can trace back to their sources, in other words, why and how the requirements satisfied. For the enough heat, according to table 5.1, overheating, short circuit, component aging and improper installation may have a probability to create enough heat for ignition. And flammable material is of course satisfied the other requirement. For human activity, it may vary of different kind. But the consequences of the activities may both satisfy the two requirements and cause a fire to happen. So our purpose is to eliminate at least one requirement, and based on that, we propose the rules of redundancy for fault tolerance.

For the enough heat, because it always related to physical hardware, so the best way for it is physical redundancy. For one thing, use the same component as redundancy. For the overheating, short circuit, component aging and component aging, it may use two of the same component working by turns. When the temperature of one of the same component is approaching to a specific value, lets say bellow the ignition point of nearby material, and then stop the working component and run the other same component (the redundant one) instead. The mechanism is shown in figure 5.7 bellow.

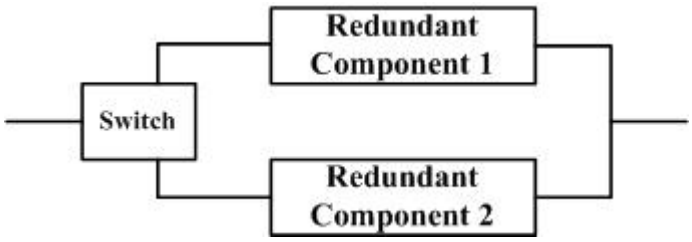

Figure 5.7: a redundant mechanism for enough heat

As shown in the figure, redundant component 1 and 2 are the same component with same function. The switch has the function to choose which component to use according to the working temperature. And for the component aging, the useful way is to check and replace frequently.

For flammable material, it is better to use non-flammable material instead. And for human activity, education and training is necessary. That may reduce the probability for a fire to occur.

Table 5.1: the classified basic events

Category	Basic Events
Overheating	1. Electric wire overheats 2. The time and/or temperature of heating of clothes is beyond the required 3. Overloading the create enough heat to ignite flammable material nearby
Short Circuit	1. Short circuit 2. Unsteady power supply 3. Unspecified short circuit arc 4. Unspecified short-circuit arc ignite flammable material nearby 5. Short-circuit arc from defective, worn insulation, which ignite flammable material nearby
Component aging	1. Component aging of dryer
Improper Installation	1. The dryers vent is too long and contain sharp turns and bends 2. Improper connection of plug and outlet to the dryer
Flammable Material	1. Drying clothes of flammable material 2. Gas leakage 3. Flammable material nearby 4. Flammable materials of mattress and beddings 5. Too close to combustibles 6. Having the heat source too close to combustibles
Human Activity	1. Failure to clean of lint inside duct 2. Playing with cigarettes, lighters, matches or candles 3. Smoking while lying on bed 4. Arson 5. Equipment unattended 6. Unattended equipment 7. Misuse of material or product 8. Abandoned or discarded materials or products

Chapter 6

Error Avoidance and Failure Handling for the DEM

In this chapter, we abstract another model based on the DEM and the analysis of the dependability of the DEM, and that is the finite state machine. We defined four states for the DEM, and the transition function of how transition happens from one state to another are also proposed. Finally, some rules for error avoidance and failure handling are going to be discussed at the end of this chapter.

6.1 Finite State Machine (FSM) of the DEM

Finite state machine is the widely used concept in text search and in software for industrial control [32]. And we use this concept for the analysis of the DEM and how the transition happens from normal state of the DEM to abnormal state. First, lets talk about the concept of finite state machine, which is based on [29] [30] [31].

A state machine is a model of a system with discrete dynamics. At each state, when accept some inputs it may transit to other state and produce some outputs. A finite state machine (FSM) is a state machine where the possible state is finite. And there are two types of state machines, one is Mealy machine and another is Moore machine. And the Moore machine is characterized by that of its output values are determined only by its current state; the Mealy machine is characterized by that of its output value is determined by its current state and the current inputs. In a word, they are different is the transition function. And in our research, we are using the model of Mealy machine.

As we all know, the DEM consists of many kinds of entities. And each entity has a state when in a specific stage. All these states together in a specific time are a state of the DEM. So when considering dependability of the DEM, it may transits from a normal state to an abnormal state; or from the abnormal state to normal state. Based on that we defined the FSM for the DEM in order to detect abnormal state and then use the error avoidance approach and failure-handling approach to handle them.

The FSM M defined here is a five-tuple, which the representation is shown bellow:

$$M = \{Q, \Sigma, \Gamma, \delta, q_0, F\}$$

Q: a finite set of states for the DEM;
Σ: a finite set of input of actions/behaviors that would cause transitions;
Γ: A finite set of output actions;
δ: Transition function $\delta : Q \times \Sigma \rightarrow Q \times \Gamma$
q_0: The initial state and it is a finite set of states of entities where $q_0 \subset Q$
F: a set of accepting states, which represent the happening of errors and failures and $F \subset Q$
Next, lets discuss each one of them.

6.1.1 The States of the FSM

The set of states Q of M is a four-tuple defined in the following representation:

$$Q = \{(a, b, c, d) | a \in A^*, b \in B^*, c \in C^*, d \in D^*\}$$

where A, B, C and D are four classes of states that defined in table 6.1, and for each entity, the state is always belong to one class of A, B, C and D, and $Z^*(Z \in \{A, B, C, D\})$means the power set of Z.

Table 6.1: Four classes of finite set of states of DEM

Class	Name	Description	Representation
A	Readiness State	It represents the readiness to work of all entities in a DEM	$\{a_0, a_1, \ldots, a_n\}$
B	Normal Working State	It represents the steady state (normal working state) of entities in a DEM	$\{b_0, b_1, \ldots, b_n\}$
C	Abnormal Changing State	It represents the errors that would happen in a DEM	$\{c_0, c_1, \ldots, c_m\}$
D	Emergency State	It represents the failures that would happen in a DEM	$\{d_0, d_1, \ldots, d_t\}$

Where 'n' in table 6.1 means the number of entities; 'm' means number of errors and 't' means the number of failures. Based on the representation of Q, we know that there are $2^4 = 16$ states in total of the DEM, but as we all know, there is always entities in the DEM ready for work. Then we define 8 states, which are described in table 6.2.

In table 6.2, '1' means there are some entities in such a state and '0' means there is no entity in such a state. Take P_2 for example, it means the DEM in the state of there are some entities ready for work, no entities normal working, some entities working in their abnormal changing states and no entities working in their emergency states. And table 6.3 gives the meaning for each state.

Table 6.2: Considered states of the DEM

State	a	b	c	d
P_0	1	0	0	0
P_1	1	0	0	1
P_2	1	0	1	0
P_3	1	0	1	1
P_4	1	1	0	0
P_5	1	1	0	1
P_6	1	1	1	0
P_7	1	1	1	1

Table 6.3: Explanations for each state

State	Description
P_0	A state with entities of ready to work, no working state, no occurring errors and no occurring failures
P_1	A state with entities of ready to work, no working entities, no occurring errors and have occurring failures
P_2	A state with entities of ready to work, no working entities, have occurring errors and no occurring failures
P_3	A state with entities of ready to work, no working entities, have occurring errors and occurring failures
P_4	A state with entities of ready to work, working entities, no occurring errors and no occurring failures
P_5	A state with entities of ready to work, working entities, no occurring errors and have occurring failures
P_6	A state with entities of ready to work, working entities, occurring errors and no occurring failures
P_7	A state with entities of ready to work, working entities, occurring errors and occurring failures

From the tables of 6.2 and 6.3, we know the eight states that include states of errors and failures of entities that representing one state of the DEM. And also it is better to make a priority of states of errors and/or failure. Because if a fire and an out-of-work of an appliance happen at the same time, of course the fire should have the higher priority to deal with. So it is necessary to make a refinement for these states.

First let's make the priority and then based on some criteria, we define the refined states. State priority:

- Highest: Emergency state
- High: Abnormal changing state

- Low: Normal working state
- Lowest: Readiness state

There are two criteria for state refinement:

1. Always ignore lower priority. When multiple states of different entities have different priorities, choose the higher one and make reaction to that.
2. When one state of the DEM transits to two or more other states under the same input, combine these states that have the same priority.

So the refined states are shown in table 6.4.

Table 6.4: refined states of the DEM

Refined State	State Description	Including Previous State
P1	It represents all entities in the DEM ready for work	P_0
P2	It represents the state of normal working of entities of the DEM	P_4
P3	It represents the state of errors of the DEM	P_2, P_6
P4	It represents the state of failures of the DEM	P_1, P_3, P_5, P_7

Table 6.5: Classes of inputs of the FSM

Class	Name	Description	Representation	Example
IA	Start working	Any actions that indicate start working	$\{a_0, a_1, \ldots, a_m\}$	Turn on, power on, etc.
IB	Stop working	Any actions that indicate stop working	$\{b_0, b_1, \ldots, b_n\}$	Turn off, power off, etc.
IC	Service Assisting	Any action that assists an entity to accomplish its target in providing correct services.	$\{c_0, c_1, \ldots, c_p\}$	action includes the execution of the function of entity and resource consuming
ID	Inefficient action	Its an action that is representing either an internal or external fault. It has a probability to generate an error.	$\{d_0, d_1, \ldots, d_q\}$	Operation at an improper time or not follow its function specification, etc.
IE	Service Alteration	It represents an error that reach the service interface of an entity and alter the entitys service	$\{e_0, e_1, \ldots, e_r\}$	A clothes dryer cannot dry clothes properly, etc.
IF	Adjusting Measures	They are measures that trying to eliminate the detected errors	$\{f_0, f_1, \ldots, f_s\}$	Selectively cut off power supply, etc.
IG	Failure Treatment	After a failure has happened, the treatment means actions that trying to control the failure and/or give warnings to home user and department	$\{g_0, g_1, \ldots, g_t\}$	Assume a fire has happened, warn people inside a house cut off electricity supply and inform fire department, etc.

6.1.2 The Inputs of the FSM

The inputs of the FSM described here are actions of all entities of the DEM. And the inputs mean the reasons that can trigger a transition of states from one to another of the DEM. There are seven classes of inputs in total, which is shown in table 6.5. When in simulation, these inputs are actually outputs of FSMs of different of entities. The inputs for these FSMs of different of entities vary from values like temperature, humidity, etc. to signals like that represents switch on. And that will be introduced in the next chapter.

6.1.3 The outputs of the FSM

The outputs of the FSM are the affection of various different of services of entities in the DEM. And there are four classes in total, which is shown in table 6.6.

Table 6.6: classes of the outputs of the DEM

Class	Name	Description	Representation	Example
OA	Task accomplishing	Its the action by using correct services to accomplish different tasks	$\{oa_1, oa_2, \ldots, oa_a\}$	Normally using the function of air-conditioner to control indoor temperature
OB	Abnormal changing	It represents an error is happening and it is the impact of the error	$\{ob_1, ob_2, \ldots, ob_b\}$	Increasing consumption of electricity, etc.
OC	Safety threatening	It represents a safety problem is happening and it is the impact of the safety problem	$\{oc_1, oc_2, \ldots, oc_c\}$	A fire is caused because of a clothes dryer lost its function
OD	Readiness obtaining	It represents a readiness state is obtained	$\{od_1, od_2, \ldots, od_d\}$	Every entities stop working and return to readiness state

6.1.4 Transition Function of the FSM

As introduced in previous sections, the outputs are determined by its current state and current inputs, which is called a Mealy machine. And we define the transition function like this:

$$\delta : Q \times \Sigma \to Q \times \Gamma$$

And the letter's meaning has already introduced in the beginning of section 6.1. And the transition table and state transition diagram are shown in table 6.7 and figure 6.1, respectively.

In each entry of the following table, its means "next state/output", and "-" means the state will not react to the corresponding input. The top row means "input" and the left column means "state".

Table 6.7: transition table the FSM for the DEM

	IA	IB	IC	ID	IE	IF	IG
P1	P2/OA	-	-	-	-	-	-
P2	-	P1/OD	P2/OA	P3/OB	-	-	-
P3	-	-	-	P3/OB	P4/OC	P2/OA	-
P4	-	-	-	-	-	-	P1/OD

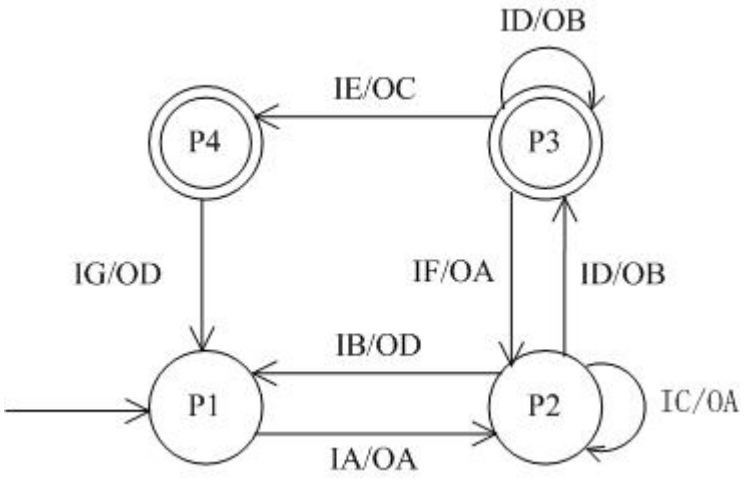

Figure 6.1: the state transition diagram of the FSM for the DEM

6.2 Error Avoidance

As discussed in section 4.2.1, an error is a part of the entity states, which represent an abnormal changing. Error Avoidance is intended to preserve the delivery of correct service in the presence of errors. It includes two parts. One is **error detection**, and another is **adjusting measures**.

Error detection is obviously aimed to detect errors. It is intended to use the FSM defined in the last section for error detection. And errors may be represented by different signals generated by the system when errors has detected.

For the adjusting measures, it is taken as a kind of system recovery that transforms a system state that contains errors to a system state with no errors. Based on the abnormal changing of the definition of error, the adjusting measures have three different forms:

1. **Redundancy**, this is similar to that of defined in section 5.3. It aims to eliminate errors before it causes failures by switching to the redundant component. The redundant component must be sensitive to a specific variable, e.g. temperature or humidity, etc. For example, when the temperature of the component of an entity is too high, then switch to the redundant component and cool down the hotter one.

2. **Branch**. This aims to eliminate errors by break down the value of abnormal increase into pieces and each piece is under normal state. For example, when the current of main electric wire is going to beyond the rated current, it may uses sub-lines for the share of overall load.

3. **Assisting**. A third way for error elimination is assisting. It uses extra devices for the adjusting of abnormal changing. For example, use fan to vent smoke within the DEM; use some cooling system to cool down an entity to keep it from too hot.

function has the trend to be broken, but still can work for a limited time. And for the detailed techniques of the proposed rules, some may already exist, some may be developed in future research. In next section, we will talk about how to deal with failures.

6.3 Failure Handling

A failure is actually a safety problem according to the definition in section 4.2.1. Failure handling aims to eliminate failure as soon as the failure is detected. And also aimes to reduce property loss and try to avoid casualty. Failure handling has two steps, the first is **failure detection**, and the second is **failure treatment**. For the failure detection, it supposes to use the same way as in error avoidance.

According to the classification of failure according to the consequence discussed in section 4.2.1 and the classification of safety problems discussed in section 2.2.

Failure treatment has three different forms:

1. Inform home user and/or department. When a failure happens, the first thing is to inform home user and/or department. And send them the detail situation of failure, and then both home user and department knows what to do next. For example, when a fire has happened, the home user and fire department will be informed. If there are home users inside the house, then they know where the fire start, and choose which rout to escape. If these are no home users inside the house, then they know the situation of their house. For the fire department, if they know the situation of the fire, so they can evaluate the fire and send firefighters to put out the fire. And the departments may include fire department, after-sale department and medical department.

2. Cut off resource supply. The resource supply for the DEM always is electricity supply, gas supply and water supply. If a failure happens to an entity, in order not to let it last for a longer time, it is better to cut its resource supply off. For example, when gas leakage happens, if we do not cut off gas supply, the gas density would increase and bring even catastrophic consequence of safety problem.

3. Open the appropriate safety equipment. To some specific failures, there exist different kinds of equipment for home user use or automatically eliminate failures. For example, in order to put out a fire, a extinguisher may be used; when a failure of gas leakage happens, the venting system of the DEM may running, etc.

It may covers almost all situations that come out. As the development of automation and intelligence of the DEM, there would be new forms of failures happens. And new rules of the detailed techniques for these failures required to be developed in future research.

Chapter 7

Simulation Cases and Results

In this chapter, we are going to do the simulation based on the FSM that defined in section 6.1. As we all know, the abnormal states are error states and failure states. What are the inputs to the FSM will generate these abnormal states? And how the FSM work? What results would be get from the simulation. In this chapter two example cases are given to illustrate these questions. The objectives of the simulation are, first to verify the state transitions from initial state to abnormal state under specific input sequences. Second, to detect abnormal states according to the characteristics.

We first introduce how the simulation environment is built and then use two cases (an error and a failure) for simulation. At last a conclusion is made based on the simulation.

7.1 Simulation Environment

The environment includes the physical home topology of the DEM and the simulation environment. Because home topologies are different from house to house, here the simulating home topology can be taken as an example. For the simulation environment, I use C language to implement the FSM based on the physical environment.

7.1.1 Domestic Environment for Simulation

Because our simulation is based on two cases, one is overload current and another is a fire caused by clothes dryer. So the home topology for the simulation is based on these two cases and also connects all common resources to the domestic environment. This home topology can be used not only for the current simulation, but also for the simulation of future research.

The resources to the domestic environment are electricity supply, water supply and gas supply. These are the basic supplies to a domestic environment that satisfy home users basic need. Of course, there are other resources like telephone line, Internet connection, etc., for telecommunication and entertainment. But these are not going to appear in the this simulation.

The domestic environment used for simulation has a main electricity wire, which connecting to the outside power line. It has three sub-lines, line 1, line 2 and line 3, connecting to three different rooms of the domestic environment, the living room, the kitchen and the laundry area. There is a fuse connects the main electric wire and these three sub-lines. And this fuse is different from traditional ones; it attaches a sensor, which can send the data of consumed current for each line to the home gateway.

Each room has one or more home appliances that powered by electricity. As we all know, for each home appliance, it may works in different modes. And in each mode, the consumed current is also different. The domestic environment like temperature, humidity, etc. and also some other commands will have affection on the selection of mode for each home appliance. For example, the indoor temperature will affect on the working mode of the air-conditioner. And the detailed explanation will be discussed in section 7.2.

For the clothes dryer, together with its venting system is used for the simulation of clothes dryer fire. Based on [22], we make some signals that represent different constraints of inputs to the FSM, and that would cause clothes dryer fire to happen. The FSMs for the clothes dryer and the main electric wire that used for simulation will be discussed in section 7.2 and section 7.3. And the home topology used for simulation is shown in figure 7.1 bellow. Notice that the service intermediary and service providers are not shown in the figure and the home gateway is supposed to connecting the service intermediary and it in turn connecting to different service providers that already introduced in section 3.1.

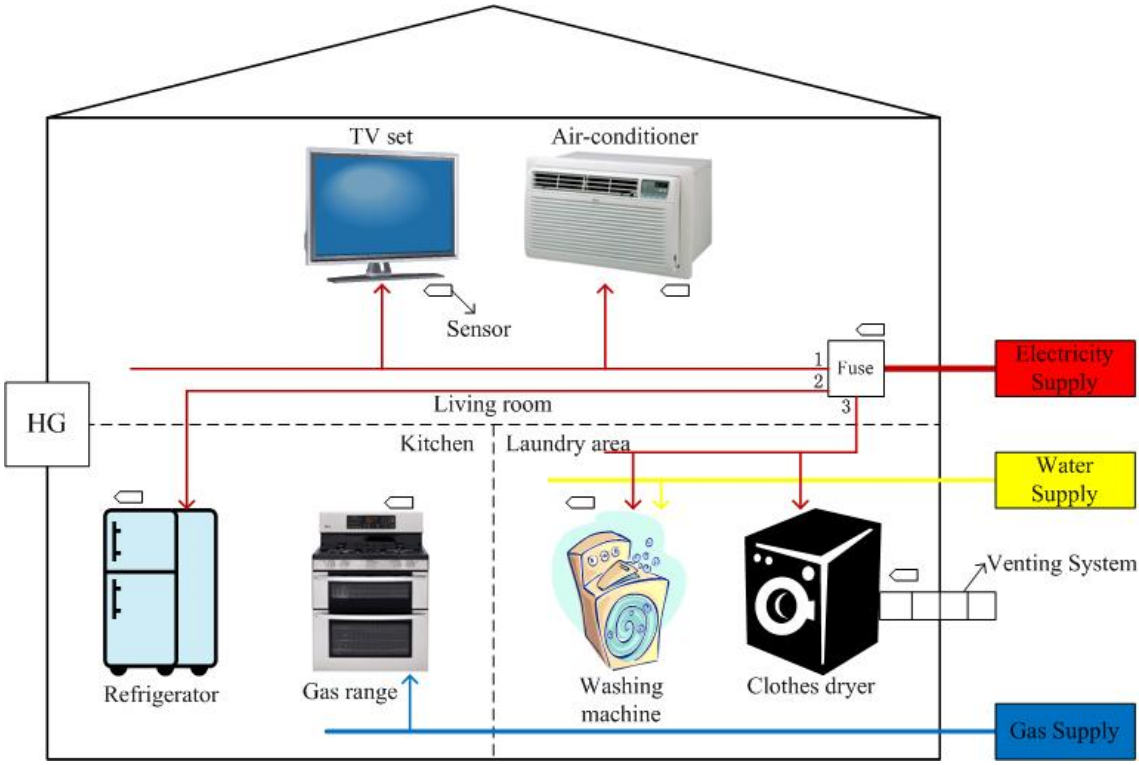

Figure 7.1: home topology for simulation

7.1.2 Simulation Tools

In order to simulate the two cases descripted in section 7.2 and 7.3 within the environment of depicted in figure 7.1. We are going to implement two simulators based on FSMs of all home appliances depicted in figure 7.1. One is text-based user interface simulator and another is graphic user interface simulator. The text-based simulator is the simulator that implement all the FSMs of related home appliances and all the simulated results come from this simulator. For case 1, all home appliances that powered by electricity contribute to the current of the main electric wire; each home appliance works in different state that consumes different values of current. So when part or all of these home appliances work may have a probability to generate the overload current of the main electric wire. For case two, we give different input signals sequence to the FSM for clothes dryer, which may generate the clothes dryer fire. The outputs of text-based simulator are two text files. One is for overload current and all consumed currents of home appliances, total consumed current and the occurrence of overload current happens are stored. Another is for the clothes dryer fire and all possible input signals, output state and the occurrence of a fire are stored.

For the graphic user interface simulator, it dynamically graphically shows the simulation results that come from the text-based simulator. It reads the output text files of text-based simulator as its inputs and stores them into memory. When press "start simulation" button, it reads the data and shows the simulation graphically to users.

The programming environments for the two simulators are as follows:

Model Name: MacBook Pro
Model Identifier: MacBookPro6,2
Processor Name: Intel Core i7
Processor Speed: 2.8 GHz
Memory: 4 GB 1067 MHz DDR3
OS Version: Mac OS X 10.6.8
IDE: Eclipse IDE for C/C++ Developers(test-based simulator)
Qt Creator(graphic user interface simulator)
IDE Version: Helios Service Release 2(text-based simulator)
Qt Creator 2.4.0(Based on Qt 4.7.4(64bit))(graphic user interface simulator)
Build id: 20110301-1815(text-based simulator)
Build on Nov 28 2011 at 10:21:33(graphic user interface simulator)

The source files of the text-based simulator consist of four files shown in figure 7.2 and the declaration for all FSMs of home appliance are implemented in the file of home_appliances.h and its realization is in the file of home_appliance.c. The possible inputs for each FSM are implemented in the file inputs.h and the main.c is for the main function.

The whole implementation of the text-based simulator is based on multithread, which each thread runs one single FSM for a home appliance. The main function maintenance the simulation time and create all the necessary threads. The relationship of the main thread and all the created threads together with required resources are shown in figure 7.3 and the detail implementation can be found in the source files.

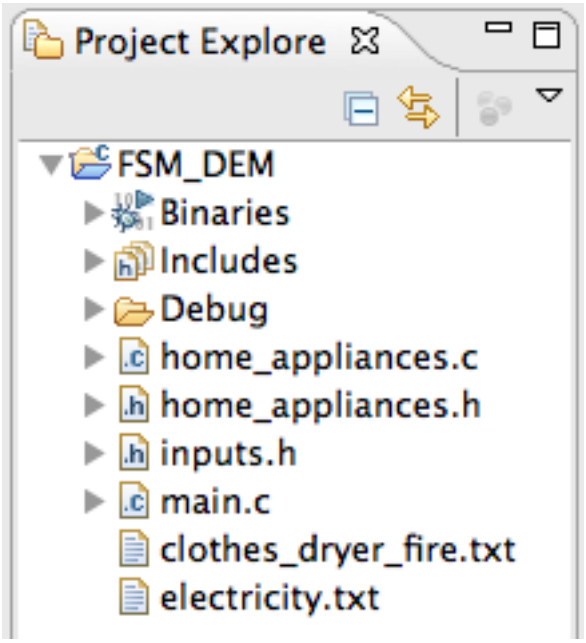

Figure 7.2: source files for the implementation of text-based simulator

The source files of the graphic user interface simulator are shown in figure 7.4. The files of ewire.h and ewire.cpp are used to draw electric wires and change its color when the corresponding home appliance start working. The files of widget.h and widget.cpp are used to implement the main window of the GUI and also read text files that are output of the text-based simulator. The file main.cpp is the main function. There are two resource files, one is events.qrc and another is HomeTopology.qrc. The file events.qrc includes three pictures, thunder.png, fire.png and overheat.png. When the picture thunder.png is shown, it means overload current of main electric wire has happened. When the picture overheat.png is shown, it means the clothes dryer is in the state of overheat. And when the picture fire.png is shown, it means a clothes dryer fire has happened. The file HomeTopology.qrc includes only one picture, HomeTopologyforGUI.jpg. It is shows the overall topology of the simulated DEM.

The picture 7.5 shows the graphic user interface. After GUI simulator has read the input file that is the output of the text-based simulator. The push button can be pushed. For electric wires 1, 2 and 3. When its attached home appliances start working, its color changes to red. When overload current happens, the picture of thunder.png will be shown in area 4. When the clothes dryer in overheating state, the picture of overheat.png will be shown in area 5 and when fire.png is shown that means the clothes dryer fire has happened. And the attached numbers shows consumed current of the corresponding home appliance.

There are two classes that are implemented in order to realize the GUI simulator. The classes are Window and EWire. The class EWire used to draw electric wire 1, 2 and 3, and also the main electric wire that is shown in figure 7.5. Another function is to change the color of electric wires when necessary. The class Window's function is for the

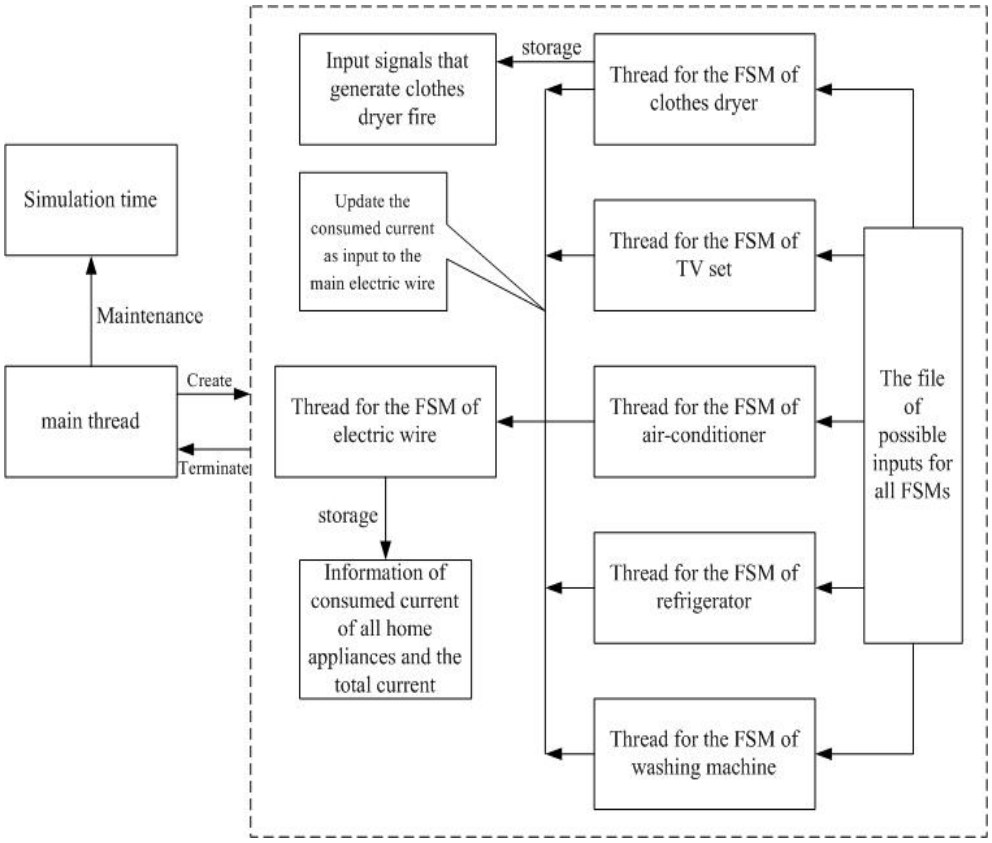

Figure 7.3: relationships of all threads and required resources for the text-based simulator

main GUI window of the simulator and necessary widgets. Another important function of class Window is to load input data and show the necessary information of simulated data visually. All the two classes are derived from the class QWidget. In the implementation of class Window, there is an instance of class EWire for drawing electric wires and the relationship of these classes are shown in figure 7.6.

For the working mechanism of the GUI simulator, we use a state diagram of figure 7.7 to illustrate it. The first step initialization is to display necessary widgets and pictures for the main window of the GUI simulator. After that load the input data that is the output of the text-based simulator. Then push the "start simulation" button to start the simulation and set a timer of 1 second. So it will update the data to the window every 1 second. When time out satisfied, the simulator will read data from memory(It was implemented by using QList). Here it has two branches, one for overload current and another is for clothes dryer fire. If the consumed current is not zero, its corresponding electric wire color will be changed to red. And if the overall consumed current is greater than the rated current, a picture of overload current will be shown. For the clothes dryer fire, if the clothes dryer is in the overheating state, a specific picture will be shown. If it is in the fire state, a picture of fire will be shown to give the information of fire to user.

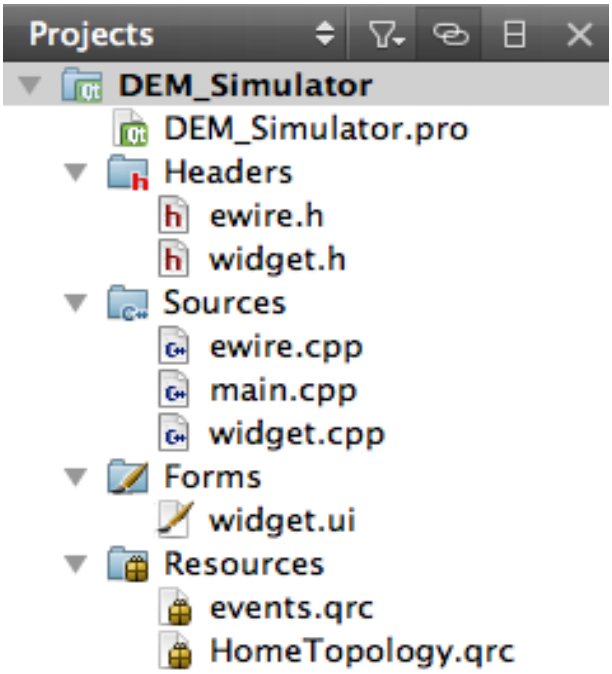

Figure 7.4: source files for the implementation of graphic user interface simulator

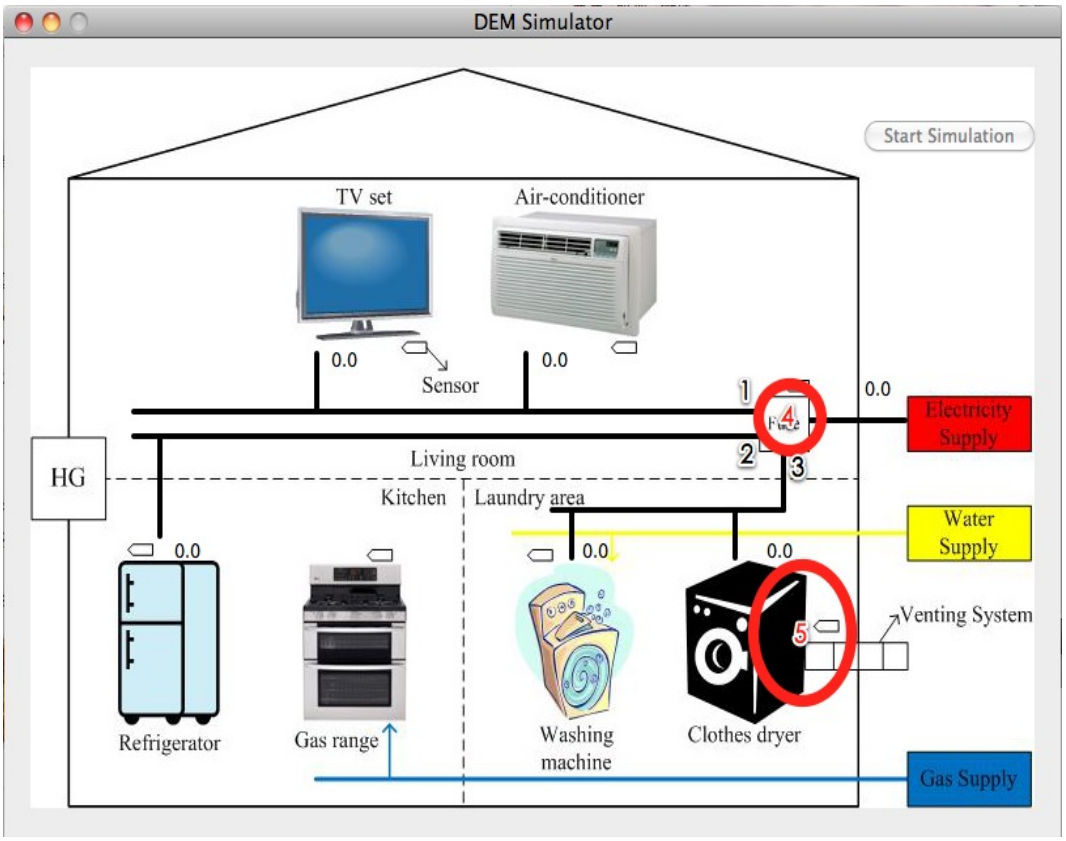

Figure 7.5: the GUI of the graphic user interface simulator

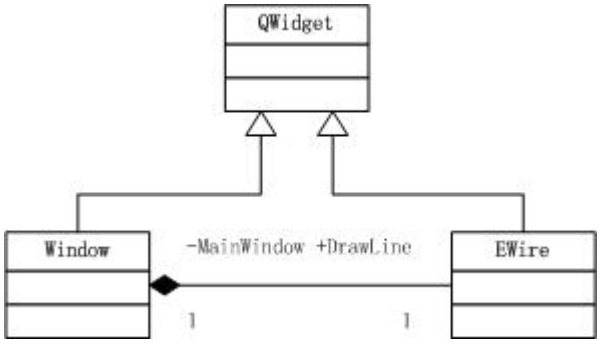

Figure 7.6: the relationship of classes

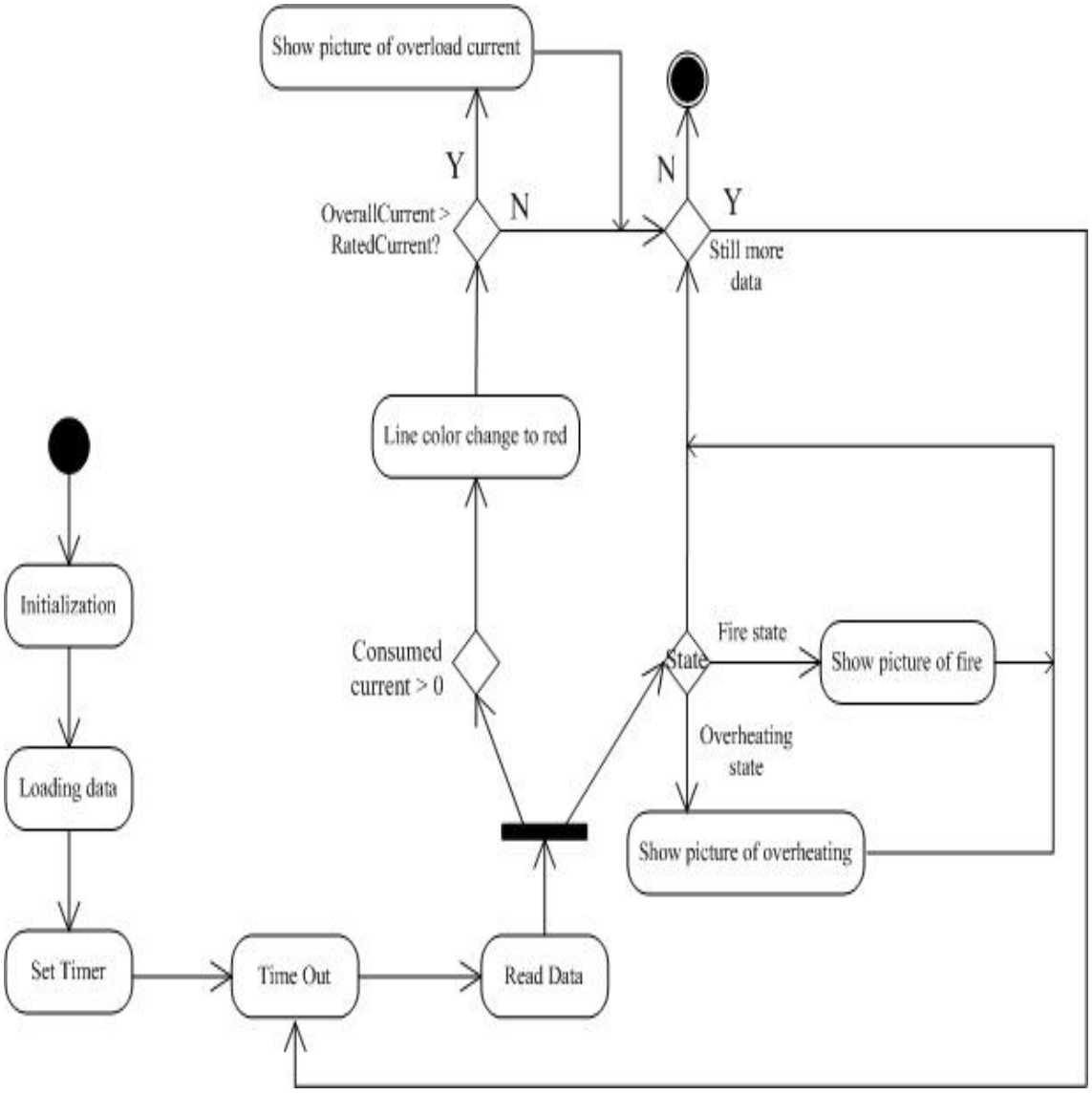

Figure 7.7: state diagram of the GUI simulator

7.2 Case 1: Overload Current

In this case of experiment, we are going to simulate the overload current of the main electric wire. Home appliances that powered by electricity contribute the current transmitted by the main electric wire. Each home appliance has different modes, working, not working. If it is in working mode, it also has some different working modes. And in different mode, the consumed current is also different. Another thing need to be concerned is that, to a home appliance, how it transits from one working mode to another. We were planning to use FSMs to illustrate every home appliances involved. There are five different home appliances in our simulation environment as shown in figure 7.1. And lets introduce the FSMs of them one by one.

Before move on, one thing needs to be mentioned. As defined in section 6.1, the DEM has four states: readiness state, normal working state, abnormal changing state and emergency state. And for the main electric wire, it also has these four states that contribute to the state of the DEM. But for each home appliance when analyze the overload current, they may have different states that output different values of current. Now lets define the FSM for air-conditioner first.

A FSM for the air-conditioner is defined like this:

$$M_{ac} = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is a finite set of states. And it includes states of readiness, cooling and heating states and initial state q_0 is readiness state.

Σ is a finite set of input to the FSM. There are two input variables, switch and Tcd. "switch" is a Boolean variable and its means a switch that control power on/off, '1' means power on and '0' means power off. And Tcd means the environmental temperature values to the air-conditioner. Here we choose two values for Tcd and Tcd = {25, 17}.

Γ is a finite set of output to the FSM. And output variables are I_{ac} and cmd_warmup. I_{ac} means the consumed current of the air-conditioner and the output values for I_{ac} are {0, 3, 7}. And unit is ampere. '0' means output current is 0 ampere when switch = 0; '3' means the consumed current when the air-conditioner working in cooling down mode; '7' means the consumed current when the air-conditioner working in warming up mode. The output variable cmd_warmup is a Boolean variable the control of temperature. If cmd_warmup = 1 means warming up, if cmd_warmup = 0 means cooling down.

δ is the transition function. And we show this by a transition function in table 7.1. In the table, the top row means input variables in the sequence of (switch, Tcd); the most left hand side column means "state"; and the outputs in the table are in the form of (next state/(cmd_warmup, I_{ac})).

The working mode of the air-conditioner is affected by the environmental temperature. And the environmental temperature is another FSM. The input for this FSM is cmd_warmup and the output for this FSM is Tac. This FSM together with the FSM of the air-conditioner is shown in figure 7.8 bellow.

Table 7.1: the transition table for air-conditioner

	(0, 0)	(1, 25)	(1, 17)
Readiness	Readiness/(0,0)	Cooling/(0,3)	Heating/(1,7)
Cooling	Readiness/(0,0)	Cooling/(0,3)	Heating/(1,7)
Heating	Readiness/(0,0)	Cooling/(0,3)	Heating/(1,7)

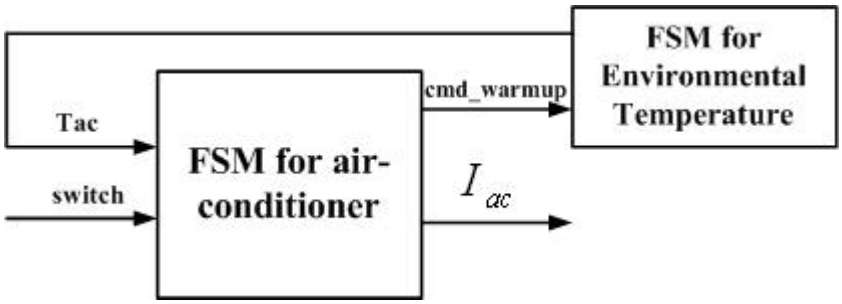

Figure 7.8: the FSMs for the environmental temperature and air-conditioner

Next lets discuss the FSM about a TV set. The FSM for TV set is also a five tuple. And the definition is like this:

$$M_{tv} = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is also the same meaning as in the FSM for air-conditioner, a finite set of state. And Q = {readiness, start-up, playing} and the initial state is readiness.

Σ is the finite set of input to the FSM. And the input variables are switch, start-up, playing and Ttv. "switch" is also the same meaning as in the FSM for air-conditioner; "start-up" is the signal from the remote controller and it is a Boolean variable, '1' means we have the signal as input to the FSM while '0' we dont have the signal for the FSM. "playing" is a signal that represent the normal working of the TV set. '1' means normal working of the TV set and '0' means not. So the inputs in the sequence of {switch, start-up, playing} are {000, 110, 101}. For the Ttv, it means the working temperature as input to the FSM for the TV set. We give it the values of Ttv = {30, 80}.

Γ is finite set of output to the M_{tv} and input variables are I_{tv} and is_increase. I_{tv} is the output current that the TV set consumed. The output currents are {0, 0.5, 2.5, 1.5}. '0' means the consumed current when switch is 0; '0.5' means the consumed current when the TV is normal working; '2.5' the consumed current when start-up = 1 and its in the mode of start-up; '1.5' means the extra consumed current under high working temperature. And is_increase is signal of Boolean value and meaning whether the working temperature heating up and '1' means heating up, '0' means not.

δ is the transition function and we show these transitions by a transition table of table 7.2. The input row is the sequence of ({switch,start-up,playing}, Ttv) and the outputs are in the form of next state/(I_{tv},is_increase).

Table 7.2: the transition table for TV set

	(000, 30)	(110, 30)	(101, 30)	(101,80)
Readiness	Readiness/(0,0)	Start-up/(2.5,0)	-	-
Start-up	Readiness/(0,0)	Start-up/(2.5,0)	Playing/(0.5,0)	-
Playing	Readiness/(0,0)	-	Playing/(0.5,1)	Playing/(0.5+1.5, 1)

We assume that the working temperature affects the consumed current of the TV set. And the working temperature is another FSM. It uses is increase as input and Ttv as output. The FSMs are shown in figure 7.9.

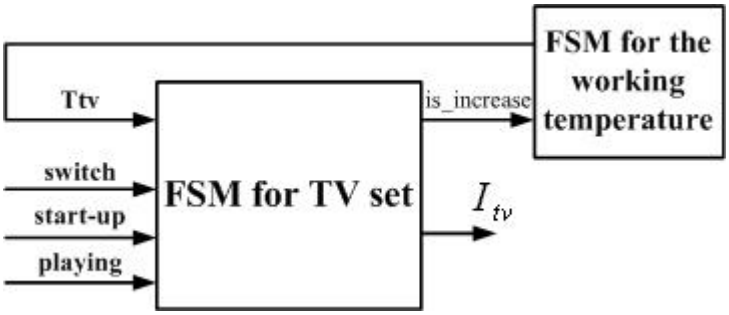

Figure 7.9: the FSMs for the TV set and its working temperature

The third FSM is that for a refrigerator. And the definition is shown below.

$$M_r = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is also the finite set of states and in this case it includes state of readiness, start-up, normal working (use nw to represent it), normal working with door open (use nwdo to represent it). The initial state is readiness.

Σ is the finite set of inputs for M_r. The input variables of Σ are switch, start-up and Tr. "switch" and "start-up" have the same meaning as in M_{tv}. Tr means the inside temperature of a refrigerator. The input values for the sequence of {switch, start-up} are {00,10,11}. The input values for Tr are {10, 2}.

Γ is the finite set of output for M_r. The output variables are (I_r, cmd_cooldown. The variable (I_r means the consumed current of the refrigerator and (I_r={0,0.65,4,0.8}(the unit is ampere). When switch = 0, then I_r=0; '0.65' is the consumed current for the normal working; '4' is the consumed current when the refrigerator is start-up; '0.8' is the extra consumed current when the inside temperature of a refrigerator is affected by outside environmental temperature. It means when open the door of a refrigerator and the inside temperature is increased and need to cool down. The cmd_cooldown is a Boolean value, which means whether need to cool down. '1' means need to cool down and '0' means not.

δ is the transition function and here we still use transition table to represent it. The transition table is shown in table 7.3 and the inputs have a sequence of (switch, start-up, Tr). The outputs are in the form of next state/(I_r, cmd_cooldown)

Table 7.3: the transition table for refrigerator

	(00, 10)	(10, 10)	(10,2)	(11, 10)
Readiness	Readiness/(0,0)	-	-	Start-up/(4,1)
Start-up	Readiness/(0,0)	nwdo/(0.65+0.8, 1)	nw/(0.65,0)	Start-up/(4,1)
Normal working (nw)	Readiness/(0,0)	nwdo/(0.65+0.8, 1)	nw/(0.65,0)	-
Normal working with door open (nwdo)	Readiness/(0,0)	nwdo/(0.65+0.8, 1)	nw/(0.65,0)	-

The working mode of a refrigerator is affected by the inside temperature. And the inside temperature is another FSM, its input is cmd_cooldown and output is Tr. Figure 7.10 shows the relationship of the two FSMs.

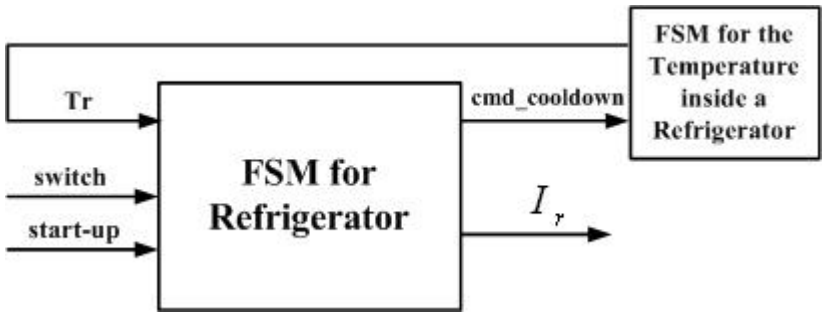

Figure 7.10: the FSMs for refrigerator and inside temperature of the refrigerator

The fourth FSM is for washing machine. Still, we use a five tuple to represent it and shown below.

$$M_{wm} = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is the finite set of states of the washing machine. It includes states of readiness, washing and dehydration. And the initial state is readiness state.

Σ is the finite set of inputs to the M_{wm}. And input variables = {switch, wash, dehydration, Twm}. "switch" is the same meaning as in previous FSMs; "wash" means the washing command from the control panel, and 1 means the command to wash clothes and 0 means not; "dehydration" means the dehydrating command from the control panel, and 1 means dehydrate clothes and 0 means not; "Twm" means the temperature of the water inside the washing machine. So the inputs for the sequence of {switch, wash, dehydration} are {000, 110, 101}, and the inputs for Twm are {10, 25}.

Γ is the finite set of output of the M_wm. The output variables are I_{wm} and is_heatup. The I_wm means the output current that the washing machine consumed and I_{wm}={0,1.1,

2.2,7.9} (unit is ampere). 0 means the consumed current when switch = 0; 1.1 means the consumed current of the washing machine under washing state; 2.2 is the consumed current of the washing machine under dehydrating state and; 7.9 means the extra consumed current when need to heat up the water inside the washing machine. For the is_heatup, it means whether the water inside the washing machine need to heat up, and 1 means need to heat up.

δ is the transition function and we still use transition table to represent it. Table 7.4 shows the transition relationship among current state, inputs and next state and outputs. The input row is in the form of ({switch,wash,dehydration}, Twm) and the outputs inside the table are in the form of next state/(I_{wm}, is_heatup).

Table 7.4: the transition table for the FSM of washing machine

	(000, 25)	(110, 25)	(110, 10)	(101, 25)
Readiness	Readiness/(0,0)	Washing/(1.1,0)	Washing/(1.1+7.9,1)	-
Washing	Readiness/(0,0)	Washing/(1.1,0)	Washing/(1.1+7.9,1)	Dehydration/(2.2,0)
Dehydration	Readiness/(0,0)	-	-	Dehydration/(2.2,0)

The M_{wm} is affected by the temperature of the water inside washing machine. And the water temperature is another FSM; the two FSMs relationship is shown in figure 7.11.

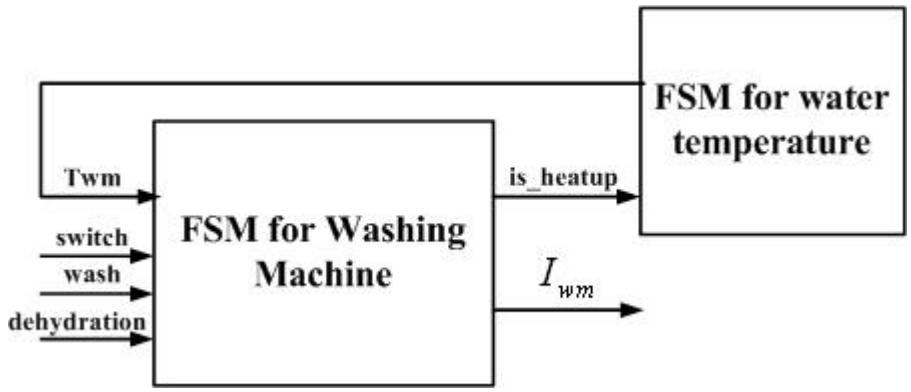

Figure 7.11: the FSMs for the washing machine and water temperature

The fifth FSM is for clothes dryer. This FSM is a little bit different from that of the previous four FSMs. There are two parts for this FSM, one part is concerning the current consumption and another is concerning the clothes dryer fire that will be introduced next section. So the representation of the FSM for clothes dryer is also have two forms. The representation of the FSM for the current consumption of clothes dryer is shown below.

$$M_{cd1} = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is the finite set of states of the clothes dryer. And it includes the states of readiness, cool down and very dry. The initial state is readiness state.

Σ is the finite set of inputs of the M_{cd1}.The input variables are switch, cool_down, very_dry and Tcd. "switch" has the same meaning as in previous FSMs. "cool_down" and "very_dry" are commands from the control panel of the clothes dryer. '1' mean do the actions of cool down and dry, and '0' means not. Input values in the sequence of {switch, cool_down, very_dry} are {000, 110, 101}, and the input values for Tcd are {30, 80} and it means the internal temperature of a clothes dryer.

Γ is the finite set of outputs of the M_{cd1}. Output variables are I_{cd} and is_heatup. And I_{cd} means the consumed current of the clothes dryer. The values for I_{cd} are {0, 3, 9} (the unit is ampere). '0' means the consumed current is 0 when switch = 0; '3' means the consumed current when in cool down state; '9' means the consumed current when in very dry state. The output is_heatup means whether to heat the inside temperature up. '1' means heat up and '0' means not.

δ is the transition function and we use transition table to represent it. And the table is shown in table 7.5. The input row is in the form of ({switch, cool_down, very_dry}, Tcd) and the outputs in the table are in the form of next state/(I_{cd}, is_heatup).

Table 7.5: the transition table for the FSM of clothes dryer

	(000, 30)	(110, 30)	(101, 80)
Readiness	Readiness/(0,0)	Cool down/(3,0)	Very dry/(9,1)
Cool down	Readiness/(0,0)	Cool down/(3,0)	Very dry/(9,1)
Very dry	Readiness/(0,0)	Cool down/(3,0)	Very dry/(9,1)

The working states of the clothes dryer are affected by internal temperature of the clothes dryer; the internal temperature is affected by the internal humidity. When the humidity is high, so it needs high temperature, otherwise, low temperature is needed. Part one of the figure 7.12 shows the relationship of these FSMs.

Based on the outputs of the five FSMs, we define the FSM for the electric wire. The representation of the FSM for the electric wire is shown below.

$$M_{ew} = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is the finite set of states and it includes states of readiness, transmission and overloading. The initial state is readiness state.

Σ is the finite set of inputs and input variables are $I_{tv}, I_{ac}, I_r, I_{wm}, I_{cd}$. They are outputs of FSMs of home appliances just introduced. And input values for each variable are shown below.

I_{tv} = {0,0.5,2.5,1.5}
I_{ac} = {0,3,7}
I_r = {0,0.65,4,0.8}

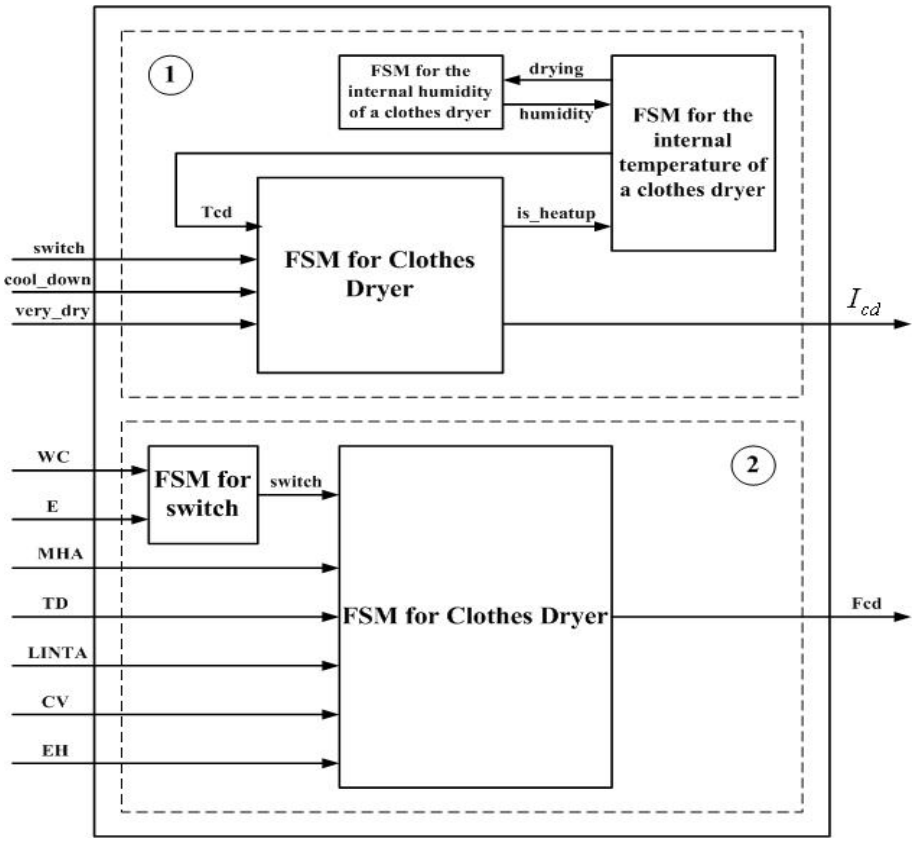

Figure 7.12: the FSM for the clothes dryer and its related FSMs

I_{wm} = {0,1.1 ,2.2,7.9}
I_{cd} = {0,3,9}
And the unit is ampere.

Γ is the finite set of outputs and output variable is is_overload. When is_overload is '1' means overload and when is '0' means not.

δ is the transition function and, use the sum of inputs compare with a threshold value to determine whether transit to the state of overload. So based on that, the transition table should be like in table 7.6. And the inputs are the sum of $I_{tv}, I_{ac}, I_r, I_{wm}, I_{cd}$, and they belong to three value intervals. The outputs are in the form of next state/is_overload. The rated current of the electric wire is I_{rated}.

Table 7.6: the transition table for the electric wire

	0	(0, I_{rated})	[I_{rated}, +∞)
Readiness	Readiness/0	Transmission/0	-
Transmission	Readiness/0	Transmission/0	Overloading/1
Overloading	-	-	-

Based on all FSMs introduced in this section, the M_{ew} is given in figure 7.13 and in this figure the FSM for clothes dryer is the part one of that in figure 7.12.

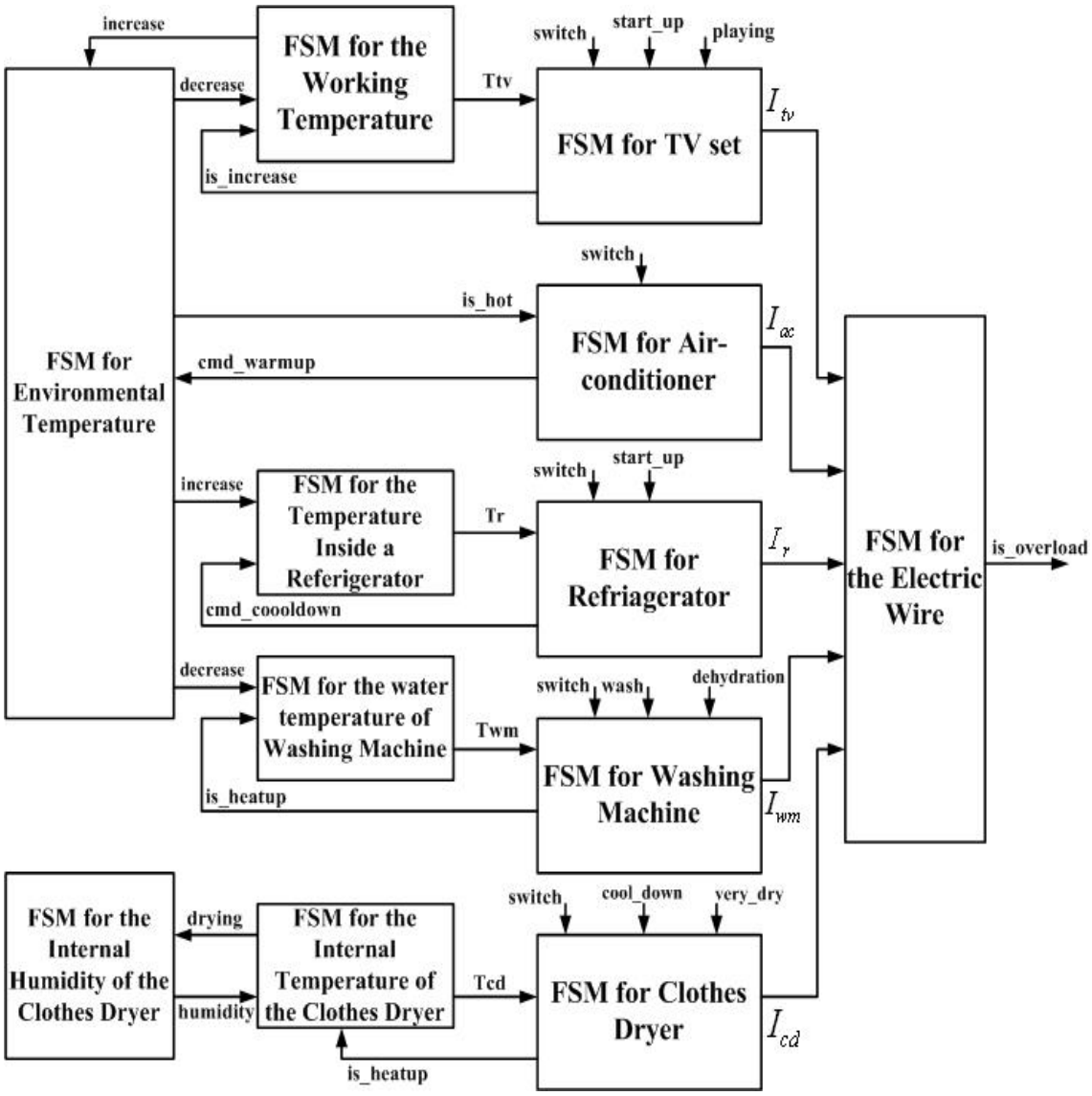

Figure 7.13: the FSM for the electric wire and its related FSMs

In the simulation for overload current, we set the simulation time to 60 seconds. Figure 7.14 shows the simulation result with respect to all input current of home appliances and the output result. From the figure 7.14, we can see the rated current is 20 ampere. The most top line means the total consumed current and the lower ones are the consumed current of all home appliances. In the vertical direction, the total current is contributed by the sum of consumed currents of home appliances. And for the total current, it has points above the horizontal line of 20 ampere. That means our system can detect the state of overload current.

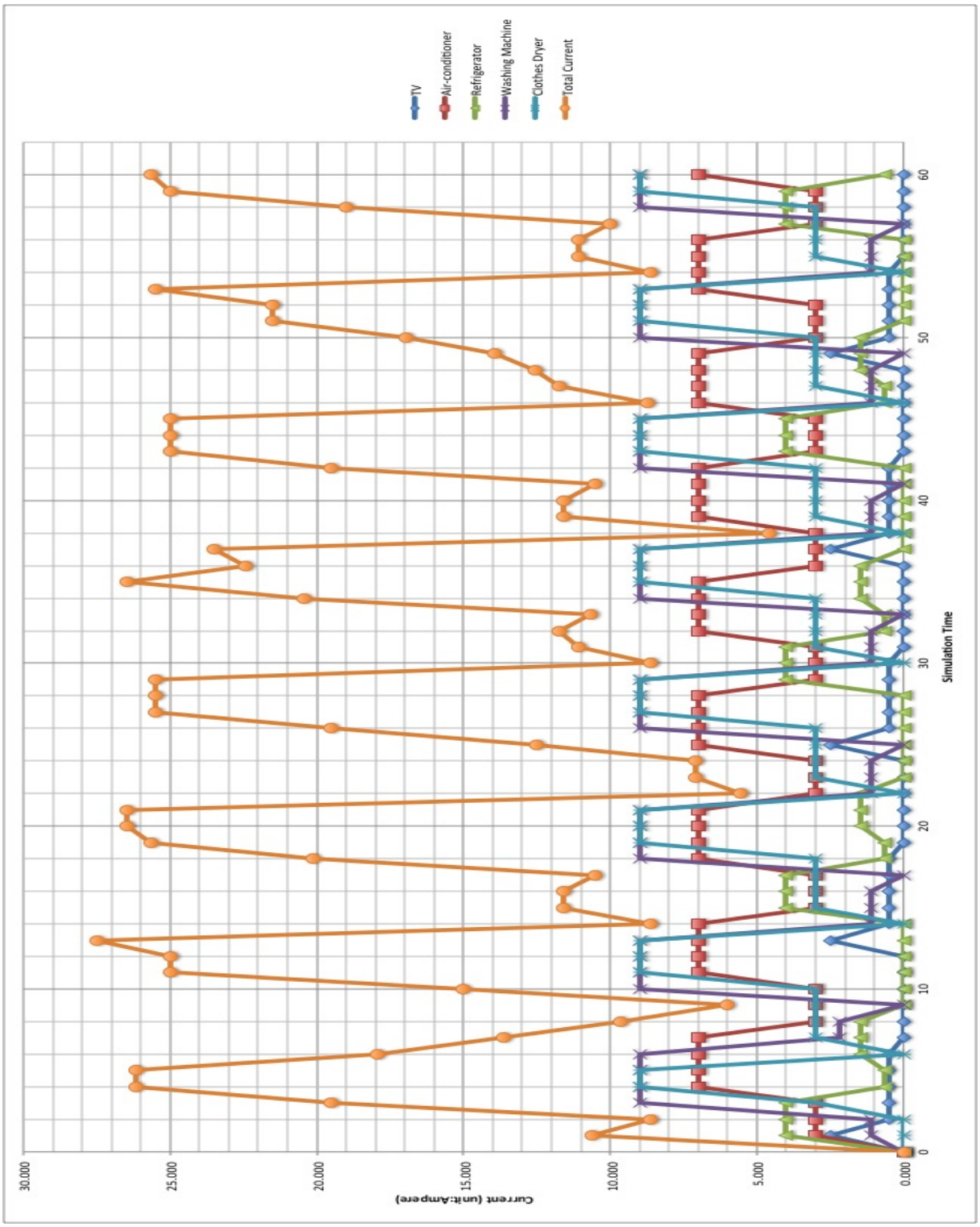

Figure 7.14: simulation result of the main electric wire

7.3 Case 2: A Fire Caused by Clothes Dryer

In this case of simulation, a clothes dryer fire is going to be simulated. Like that in section 7.2, a FSM for the clothes dryer is needed. The representation of the defined FSM for the clothes dryer is shown below.

$$M_{cd2} = \{Q, \Sigma, \Gamma, \delta, q_0\}$$

Q is the finite set of states and it includes states of readiness, normal working state, overheating and fire occurring, which use P1, P2, P3 and P4 to be represented. And the initial state is readiness.

Σ is the finite set of inputs and the input variables are WC, E, MHA, TD, LINTA, CV AND EH. They are representing signals that have a specific meaning, which the detailed explanation is shown in table 7.7.

Table 7.7: the detailed explanation of input variables

Signal	Explanation
WC	"wet clothes", it represents wet clothes put into the clothes dryer
E	"electricity", it represents normal power supply
MHA	"moving hot air", it represents the moving hot air in the dryer in order to make wet clothes dry
TD	"turning drum", it represents the drum is turning and together with the moving hot air to make clothes dry
LINTA	"lint accumulation", when working of the dryer, lint would accumulate both in the dryer and its venting system
CV	"compromised vent", improper installation of venting system with sharp turns and bends
EH	"enough heat", the temperature inside the drum is greater than and equal to the ignition point of nearby material

These signals are Boolean values and '1' means the corresponding signal works; '0' means not. We combine 'WC' and 'E' together as the "switch". So the input variables becomes {switch, MHA, TD, LINTA, CV, EH}. So the input values are {000000, 111000, 111100, 111101, 111010, 111110, 111111}.

Γ is the finite set of output and output variable is Fcd, which means whether a clothes dryer fire happens. '1' means a clothes dryer fire is happening and '0' means not happening.

δ is the transition function and is represented by the table 7.8 of transition table. And the FSM of M_{cd2} is shown in the part two of figure 7.12.

Table 7.8: the transition table for the electric wire

	000000	111000	111100	111101	111010	111011	111110	111111
P1	P1/0	P2/0	-	-	-	-	-	-
P2	P1/0	P2/0	P3/0	-	P3/0	-	P3/0	-
P3	P1/0	-	P3/0	P4/1	P3/0	P4/1	P3/0	P4/1
P4	-	-	-	P4/1	-	P4/1	-	P4/1

During this simulation, the program read input signals from an array that stores all possible input to the FSM. The simulation time is also set to 60 second and the result is shown in figure 7.15. In the figure, the state line above represent the states that the clothes dryer in. For other input signals, each box in the vertical direction means the corresponding signal exist. So in the vertical direction for a specific simulation time, the occurrence of state is contributed by all the signals represented by the colored boxes. In the figure of 7.15, state 0 means readiness state, state 3 means the normal working state, state 4 means the overheating state and the state 5 means a clothes dryer fire happen. For example in simulation time 6, the occurrence of fire occurring state is contributed by the signals of Switch, MHA, TD, CV and EH. According to the simulation result, the system can detect the state of clothes dryer fire.

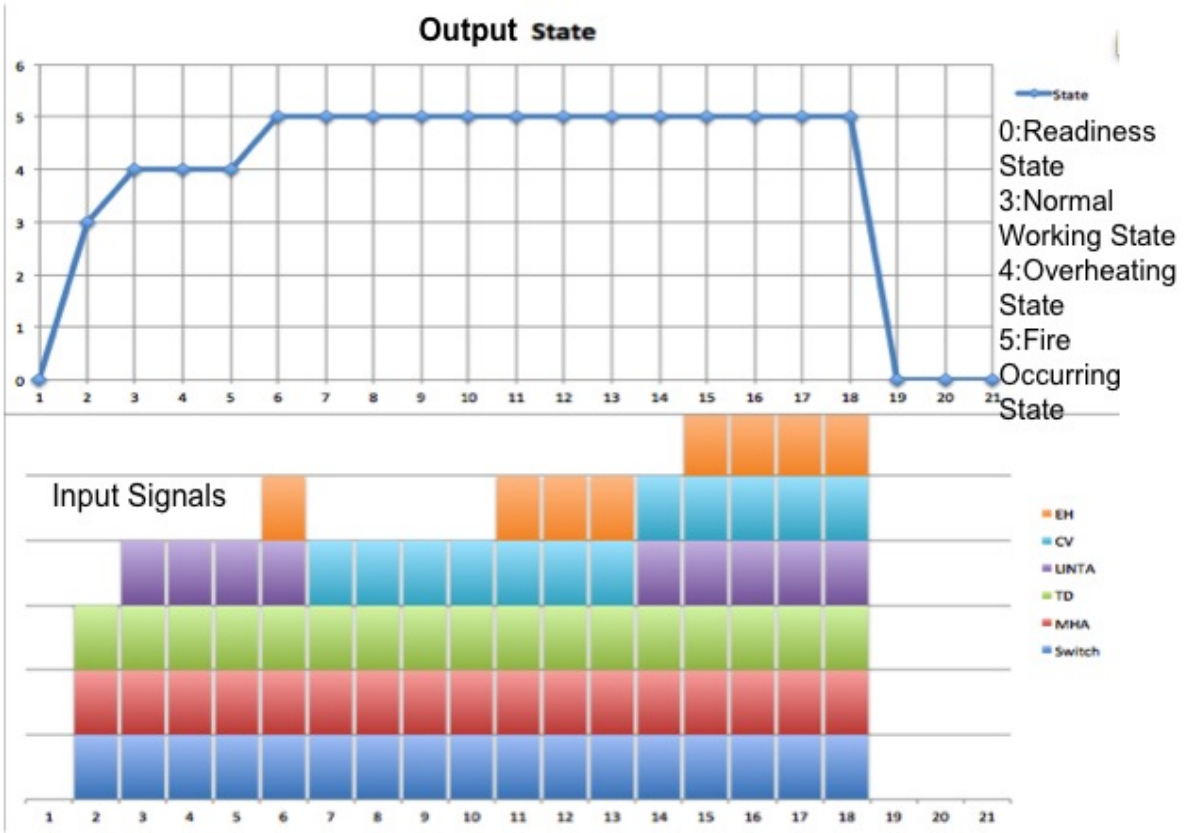

Figure 7.15: the simulation result of clothes dryer fire

7.4 Result Analysis

As discussed in this document, there are errors and failures in the DEM. And in our simulation experiment, there is one error and one failure in the DEM. So the logic that represents the overall safety situation should be given. In order to represent how the logic works, we assume there are two errors A and B, the output for error is Y1; and two failures C and D and, the output for failure is Y2. The truth table is shown in table 7.9 and table 7.10 below.

Table 7.9: the truth table for failures

A	B	Y1
0	0	0
1	0	1
0	1	1
1	1	1

Table 7.10: the truth table for errors

C	D	Y2
0	0	0
1	0	1
0	1	1
1	1	1

From the truth table, we can conclude the logic function:

$$Y1 = A + B, and\ Y2 = C + D$$

And figure 7.12 shows the logic relationship. When Y1 = 1 means there exist errors and when Y2 = 1 means there exist failures.

To our simulation, there is only one error and one failure. Assume B is the output of the FSM for electric wire and C is the output of the FSM for clothes dryer. And A=D=0, so we can get the overall logic for our simulation and shown that in figure 7.17.

Our simulation is actually based on a multilevel of FSMs. Each level of FSMs has different inputs and outputs. The lower level outputs is the inputs of the adjacent higher level. In our cases, there are two types of input, one is to represent value of variable like the current and another is to represent signals of actions and resources like MHA in the FSM for clothes dryer.

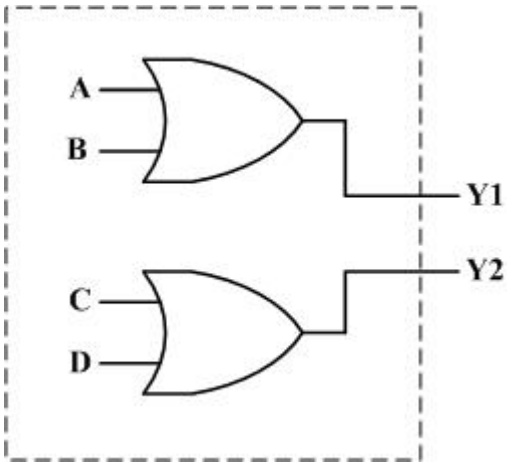

Figure 7.16: the overall logic for errors and failures

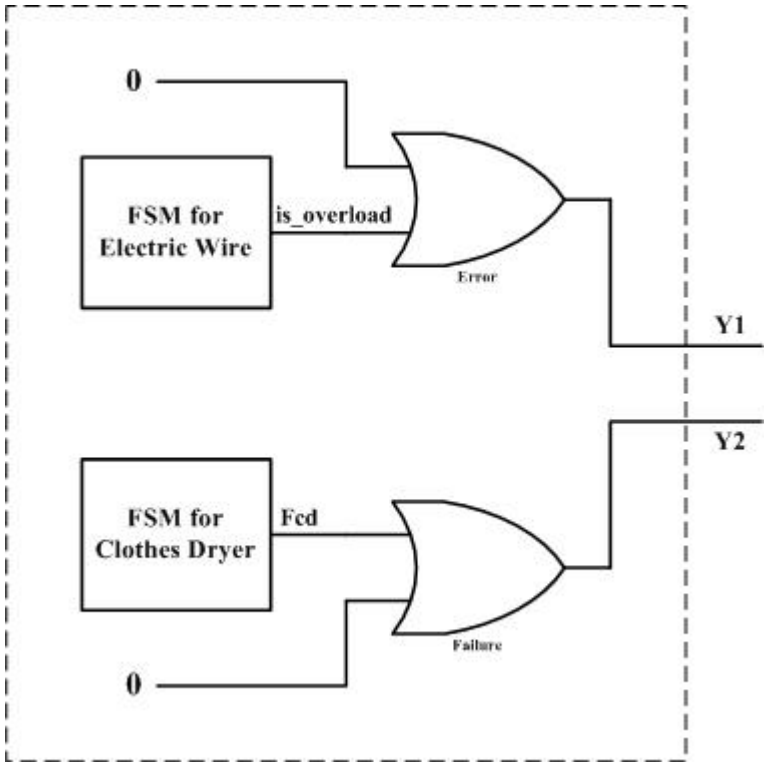

Figure 7.17: the overall logic for the simulation

According to the simulation results, our simulator can precisely detect abnormal state of errors and failures of the DEM. The overall state of the DEM is contributed by all other states of entities within the DEM. The occurrence of overall state of the DEM is generated by all inputs of entities within the DEM. So these input sequences are important to generate abnormal state.

Chapter 8

Conclusion and Future Work

In this chapter, a conclusion of this document is going to be made and a discussion of future research based on the current work is also to be presented.

8.1 Conclusion

In this research, a safety model for highly networked home environment was proposed.

At the beginning, we classified safety problems within the domestic environment: safety problems of home appliances, safety problems of interaction of home user and home appliances and safety problems of domestic environment. Next we applied the concept of dependability to the domestic environment. Before that, we abstracted a model of Domestic Environment Model from the real domestic environment. The DEM was abstracted based on the interaction of different kind of entities, which later called services when dependability was applied.

Based on the classified safety problems, we analyzed the threat to dependability of the DEM and also the attributes of dependability. For the means that in order to obtain dependability of the DEM, concepts of fault tolerance, error avoidance and failure handling are used. In implementation of these means, some rules are proposed.

As for the relationships of how safety problems are generated, we proposed a FSM for the DEM. And use transition function to be represented. The overall FSM is constructed by FSMs of entities, which means the FSM of overall DEM is the multilevel architecture. The inputs of lowest level of FSMs contribute the occurrence of safety problem (failures and errors) of the top level FSM.

Based on the analysis, a simulator was implemented and, according to the simulation results, safety problems of errors and failures can be precisely detected.

8.2 Future Work

Although our proposed system can detect safety problems within the DEM, but still have several shortcomings and also some other work need to be done in future work.

For the fault tolerance, only some limited rules were proposed. So more cases of safety problems need to be analyzing by using the concept of FTA and propose more rules for fault tolerance, so it can cover more situations. Also analyze the dependency relationship of safety problems, which means what factors that contribute to the accumulation of abnormal changings (errors) that generate failures. By using the same way, the means of error avoidance and failure handling can also be consummated.

Algorithms for error avoidance and failure handling in order for implementation and achieve the goal of automatically avoidance and handling are needed. Because in the current research, these are represented by some rules and that is not enough.

In the simulation, I wrote a simulator to simulate the DEM. The software simulation environment is quite different from the real physical environment. There are several factors may be left for simulation. The future simulation is supposed to put into real physical environment. So we can improve our system. For another, [33] [34] are giving another concept of test generation. It is can be used and applied to the FSM that we proposed. So it is can be automatically generate input sequences that cause safety problems.

Our research is focus on the service level, but not for the physical level. So in the future research, the overall system architecture of physical environment should also be considered. And for the communication of service level and physical level, another thing need to be considered is that the implementation of service API that control physical environment.

Bibliography

[1] Ben Yan, Masahide Nakamura, Lydie du Bousquet, and Ken-ichi Matsumoto, "Characterizing Safety of Integrated Services in Home Network System", ICOST 2007, LNCS 4541, pp. 130-140, 2007.

[2] Department of Health, Social Services and Public Safety UK, Home Accident Prevention, Strategy & Action Plan 2004-2009, November 2004

[3] Ben Yan, Masahide Nakamura, Lydie Du Bousquet and Ken-ichi Matsumoto, Validating Safety for the Integrated Services of the Home Network System Using JML, Journal of Information Processing Vol. 16 38-49 June 2008

[4] Majd Alwan, Prabhu Jude Rajendran, Steve Kell, David Mack, Siddharth Dalal, Matt Wolfe and Robin Felder, A Smart and Passive Floor-Vibration Based Fall Detector for Elderly, Information and Communication Technologis, 2006, ICTTA 06, 2nd

[5] Xinguo Yu, Approaches and Principles of Fall Detection for Elderly and Patient, e-health Networking, Applications and Services, 2008, HealthCom 2008. 10th Internaltional Conference, 2008, pp. 42-47

[6] Mitja Lu?trek and Bo?tjan Kalu?a, Fall Detection and Activity Recognition with Machine Learning, Slovene Society Informatika, Slovenia, 2009

[7] Nancye Peel, Margaret Steinberg and Gail Williams, Home safety assessment in the prevention of falls among older people, Australian and New Zealand Journal of Public Health 2000 Vol. 24. NO. 5

[8] Odysseas Sekkas, Stathes Hadjieftymiades, Evangelos Zervas, A Multi-level Data Fusion Approach for Early Fire Detection, 2010 International Conference on Intelligent Networking and Collaborative Systems

[9] Ali Rafiee, Reza Tavakoli, Reza Dianat, Sara Abbaspour and Mehregan Jamshidi, Fire and Smoke Detection Using Wavelet Analysis and Disorder Characteristics, Computer Research and Development (ICCRD), 2011 3rd

[10] Quanmin GUO, Junjie DAI and Jian WANG, Study on Fire Detection Model Based on Fuzzy Neural Network, Intelligent Systems and Application (ISA), 2010 2nd International Workshop

[11] Luay Fraiwan, Khaldon lweesy, Aya Bani-Salma and Nour Mani, A Wireless Home Safety Gas Leakage Detection System, Biomedical Engineering (MECBME), 2011 1st Middle East Conference

[12] Emil CORDOS, Ludovic FERENCZI, Sergiu CADAR, Simona COSTIUG, Gabriela PITL, Adrian ACIU, Adrian GHITA, Methane and Carbon Monoxide Gas Detection system based on semiconductor sensor, Automation, Quality and Testing, Robotics, 2006 IEEE International Conference

[13] Mariso Sioutis, "Area of effect and compromising techniques for the detection and resolution of environmental conflicts between services in the Home Network System", pp. 6-7,a master thesis of School of Information Science, JAIST, 2011

[14] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell and Carl Landwehr, Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, Vol. 1, NO. 1, January-March 2004

[15] J. C. Laprie, Dependability: Basic Concepts and Terminology, IFIP WG 10.4 Dependable Computing and Fault Tolerance

[16] Algirdas Avizienis, Jean-Claude Laprie, Dependable Computing: From Concepts to Design Diversity, Proceedings of the IEEE, vol. 74, Issue 5, 1986, pp. 629-638

[17] Algirdas Avizienis, Jean-Claude Laprie and Brian Randell, Fundamental Concept of Dependability

[18] Michael Stamatelators, William Vesely, Joanne Dugan, Joseph Fragola, Joseph Minarick III, Jan Railsback, Fault Tree Handbook with Aerospace Applications, Version 1.1, August, 2002, Chapter 3, 4 and 10

[19] Robert Beresh, Kinectrics, John Ciufo, Hydro One and George Anders, Kinectrics, Basic Fault Tree Analysis for use in Protection Reliability, Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2007, PSC

[20] C. V. Ramamoorthy, G.S. Ho and Y. W. Han, Fault tree analysis of computer systems, Proceedings of the June 13-16, 1977, national computer conference

[21] Edward J. Zampino, Application of Fault-Tree Analysis to Troubleshooting the NASA GRC Icing Research Tunnel, 2001 Proceedings Annual Reliability and Maintainability Symposium

[22] FEMA, Clothes Dryer Fires in Residential Buildings, Topical Fire Research Series Volume 7, Issue 1, January 2007

[23] FEMA, Heating Fires in Residential Buildings, Topical Fire Report Series, Volume 10, Issue 2, January 2010

[24] U.S. Fire Administration, Mattress and Bedding Fires in Residential Structures, Topical Fire Research Series, Volume 2, Issue 17, February 2002

[25] FEMA, Portable Heater Fires in Residential Buildings, Topical Fire Report Series, Volume 10, Issue 3, January 2010

[26] U.S. Fire Administration, Residential Air Conditioner Fires, Topical Fire Research Series, Volume 2, Issue 5, July 2001

[27] FEMA, Residential Building Electrical Fires, Topical Fire Report Series, Volume 8, Issue 2, March 2008

[28] U.S. Fire Administration/National Fire Data Center, Structure Cooking Fires, Topical Fire Research Series, Volume 5, Issue 6, August 2005

[29] Michael Sipser, "Introduction to the Theory of Computation, Second Edition",pp. 31-82

[30] John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman, "Introduction to Automata Theory, Languages, and Computation, 3rd Edition", pp.1-107

[31] Michael A. Arbib, A. J. Kfoury, Robert N. Moll, "A Basis for Theoretical Computer Science", Springer-Verlang, New York Heidelberg Berlin, pp.1-27,41-60,175-208

[32] Andrei Drumea, Camelia Popescu, Finite State Machine and their applications in software for industrial control, 27th Intl Spring Seminar on Electronics Technology

[33] Kwang-Ting Cheng, Jing-Yang Jou, Functional Test Generation for Finite State Machines, 1990 international Test Conference

[34] Irith Pomeranz and Sudhakar M. Reddy, Test Generation for Multiple State-Table Faults in Finite-State Machine, IEEE, Transactions on Computers, Vol. 46, NO. 7, July 1997

[35] http://www.usfa.fema.gov/statistics/estimates/index.shtm