A System Theoretic Approach to Design Safety into Medical Device

By

Qingyang Song

Bachelor of Engineering, Measuring and Control Technology and Instruments
Harbin Engineering University, 2003

Submitted to the System Design and Management Program in Partial Fulfillment of the requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2012

Signature of Author: .....
Qingyang Song
System Design and Management
May 10, 2012

Certified by: .....
Dr. Qi D Van Eikema Hommes
Research Scientist of Engineering Systems Division
Thesis Supervisor

Accepted by: .....
Patrick Hale
Director of System Design and Management Fellows Program
Senior Lecture, Engineering System Division

A System Theoretic Approach to Design Safety into Medical Device System

By

Qingyang Song

Submitted to the System Design and Management Program on May 11, 2012 in Partial Fulfillment of the requirements for the Degree of Master of Science in Engineering and Management

Abstract

The goal of this thesis is to investigate and demonstrate the application of a systems approach to medical device safety in China. Professor Leveson has developed an accident modeling framework called STAMP (Systems Theoretic Accident Modeling and Processes.) Traditional accident models typically focus on component failure; in contrast, STAMP includes interactions between components as well as social, economic, and legal factors.

In this thesis, the accident of the artificial heart at a level II hospital in China was used as a test case to study whether Causal Analysis based on STAMP (CAST) is used to outline the interactions between the different medical device system components, identify the safety control structure in place, and understand how this control structure failed to prevent artificial heart accident in a Chinese hospital.

The analysis suggested that further changes might be necessary to protect the Chinese public and so, based on the results of the CAST, a new set of systemic recommendations was proposed.

Thesis Supervisor: Dr. **Qi D Van Eikema Hommes**

Title: Research Scientist of Engineering Systems Division

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Abstract 2
Acknowledgments 4
List of Abbreviations 6
List of Figures 7
1 Introduction 8
2 Background Information on China Medical Devices and Artificial Heart Accident 9
2.1 Growing China Market 9
2.2 Artificial Heart Event 11
3 Literature Review 12
3.1 Failure Mode and Effects Analysis (FMEA) 12
3.2 Fault Tree Analysis (FTA) 14
3.3 Event Tree Analysis (ETA) 16
3.4 Cause-Consequence Analysis (CCA) 18
3.5 Hazard and Operability Analysis (HAZOP) 19
3.6 Summary 21
4 Introduction to System Safety Engineering 22
4.1 System Safety Definition in this thesis 22
4.2 STAMP Framework 23
4.3 CAST introduction 25
5 Case Study by Using System Safety Engineering Approach 27
5.1 Event Chains of Artificial Heart 27
5.2 System and Hazards Analysis 28
5.3 System Safety Constraints and Requirements 29
5.4 Safety Control Structure 29
5.5 Physical Process Failure and Dysfunctional Interactions 33
5.6 Analysis of the Hierarchical Safety Control System Controllers 34
5.6.1 Hospitals and Patients Loop 35
5.6.2 Medical Device Company and Hospital Loop 41
5.6.3 The SFDA, Medical Device Company and Hospital Loop 46
5.6.4 Ministry of Health and Hospital Loop 51
5.6.5 The State Council and the MOH Loop 55
5.7 Summary of Causes of the Accident Based on CAST 58
6 Recommendations 59
7 Conclusion 63
REFERENCES 65

Acknowledgments

I would like to thank my thesis supervisor, Dr. Qi Hommes for her support and advice, without which this thesis could not have been completed possible.

I would like to thank Pat Hale and Chris Bates. I would not be able to begin, continue, and complete my graduate school without the encouragement and support from them.

Finally, I would like to thank my wife Han, without her lover and support through the year, I would not be where I am now.

List of Abbreviations

CAST	Causal Analysis based on STAMP
CCA	Cause-Consequence Analysis
ETA	Event Tree Analysis
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Analysis
MOH	Ministry of Health
	Simple Chinese: 卫生部
MOHRSS	Ministry of Human Resource and Social Security
	Simple Chinese: 全国人力资源与社会保障部
NPC	National People's Congress
	Simple Chinese: 全国人民代表大会
SFDA	State Food and Drug Administration
	Simple Chinese: 国家食品药品监督管理局
STAMP	Systems Theoretic Accident Model and Process

List of Figures

Figure 1- Current Consumption and Forecast for Medical Equipment 10
Figure 2-Ten steps for an FMEA 13
Figure 3-An example of FMEA 14
Figure 4-Example fault tree structure 15
Figure 5-Event Tree Analysis example 17
Figure 6-An example of CCA 19
Figure 7-An example of HAZOP 21
Figure 8-General Socio-Technical Safety Control Structure 24
Figure 9-Communications channels between control levels 25
Figure 10-Accidents can occur when the controller's process model does not match the system being controlled and the controller issues unsafe commands 25
Figure 11-Social System Safety Control Structure 31
Figure 12-Classification of control flaws leading to hazards 33

1 Introduction

In a systems approach to safety, the focus is on eliminating or mitigating hazards through appropriate system design and operations. Rather than focusing on adverse events after they occur, emphasis is instead placed on system modeling and analysis and building safety into the system design. While a systems approach to safety does include investigating accidents (adverse events) when they occur, hazard analysis is used to investigate an accident or adverse event before it happens. The results of the modeling and analysis are used to proactively identify causal factors and take steps to eliminate or control them. Such modeling and analysis must include identifying the unintended consequences of system designs [7].

With the development of technology, medical device system is becoming more complex; relationship between human and automation are also becoming more complex. These changes are leading to more system errors. As a result, traditional systems engineering approaches that focus on an individual component failure as the root cause of accidents or issues may not be applicable anymore.

Because of the complexity of healthcare systems, standard systems engineering approaches that focus on individual component failure as the cause of accidents or losses are not easily applicable. A new approach to system safety engineering is therefore necessary. Here safety is treated instead as a dynamic control problem that considers the entire socio-technical system under which it operates. This new model of accident causality, called STAMP (System-Theoretical Accident Model and Process), is capable of handling much more complex systems than traditional safety engineering methods based on simpler, more limited assumptions about causality.

This thesis intends to demonstrate the practicality of this new approach to modeling and designing improved medical device safety which entails determining whether it is possible to model and analyze the organizational and social dynamics behind a major failure of the system. An artificial heart product was chosen as the example not only

because of the severity of the problems but also because this case included a large number of the factors involved in such losses.

This thesis contains 6 Chapter. Section 1 is a rapid introduction. Chapter 2 introduces the background of medical devices in China and an artificial heart product accident. Chapter 3 presents some safety design tools that are popularly used in medical device design. Chapter 4 provides a background of System Safety Engineering and a new model called System-Theoretical Accident Model and Process (STAMP). Chapter 5 constitutes the STAMP analysis. It represents the core of the STAMP analysis with an analysis of the safety control structure and a detailed analysis of the different components in the system. Chapter 6 outlines a new set of policy recommendations

2 Background Information on China Medical Devices and Artificial Heart Accident

2.1 Growing China Market

Because of its recent economic growth and social development, China is already the third largest medical device market in the world, after the United States and Japan. Within 5 to 7 years, China will surpass Japan and become the second largest medical device market in the world. It's projected to grow from USD 10 billion in 2007 to USD 15.5 billion in 2012. Medical devices and medical drugs are the two major means of health care. The ratio of sales of medical devices and drugs in developed countries is about 1:1, while in China it is only 1:10 [8]. Figure 1 shows the fast growth of the China medical device market.

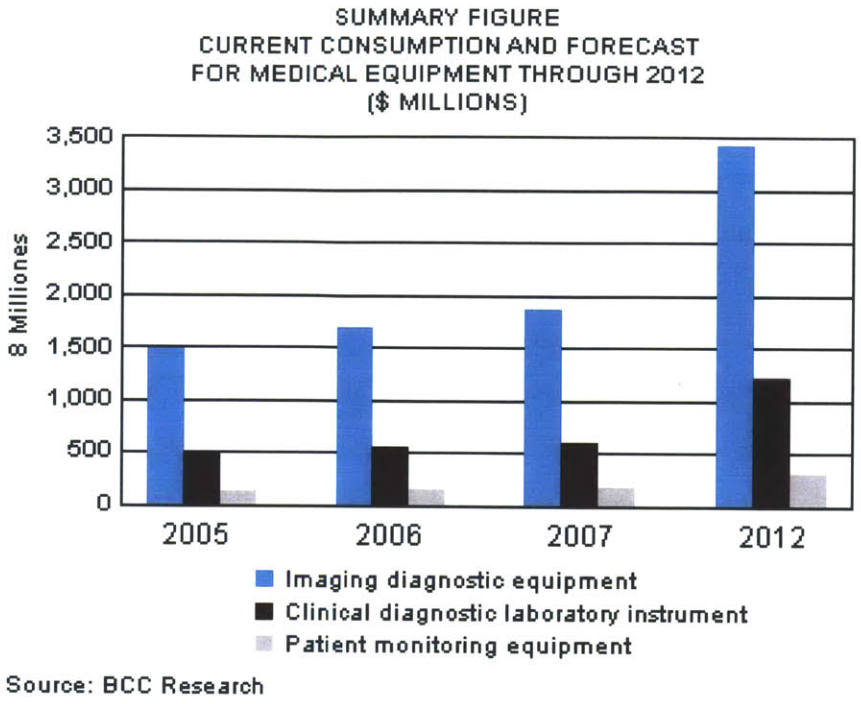

Figure 1- Current Consumption and Forecast for Medical Equipment

Before year 2002, more than 80 percent of China's 700 million rural residents lack health insurance [8]. In addition to, only a small number of citizens can afford standard Western medical care. Ongoing medical reforms are designed to expand the number of the insured. Up until 2011, the basic health insurance has covered more than 12.8 billion Chinese. Meanwhile, the new Healthcare Reform Plan is expected to result in a growing demand for new hospitals and CDCs. More than 400 new hospitals are expected to be built annually in the coming years, and even more are expected to be built, rebuilt, or expand at the country level in the next ten years [8]. Township health centers will also receive more attention to upgrade their facilities and devices.

With its growing and aging population, demands on China's health care system have ballooned in recent years. Growing prosperity and changing dietary habits mean that more and more Chinese are confronted with the same health issues that plague patients in developed nations. Chinese traditional medicine cannot deliver technology to afford diagnosis and treatment. Increasingly, patients are seeking out advanced medical techniques to treat these illnesses and there is a heavy reliance on Western technology for treatments. Therefore, during 2004 - 2007, the annual growth rate of China's medical device was 23%, and the imports rose from USD 3.1 billion to USD

4.3 billion with annual increase of 12%. Over 80% of high-tech medical equipment relies on imports [8].

The major buyers of the medical equipment are hospitals, urban and rural health centers, and Centers of Disease Control (CDCs). Averages of 322 new hospitals were built each year during 1990 - 2007. This number is expected to go up to 400 annually in the next 10 years. About 30% of total investment in these new hospitals is used for purchasing of medical device [8]. The key customers of imported equipment are large hospitals, the vast majority of which are state-run.

While there are more than 20,000 hospitals in China, only the most advanced ones (less than 1,000 Level III and possibly some of the 5,000 Level II) are able to afford foreign technology, they are also wary of the "made in China" label and continue to demand foreign brands when considering treatment. Foreign companies, especially large medical device manufacturers from Japan, Germany, and the USA, still have a comparative advantage in terms of technology and presently control more than half of the high-end device market. Chinese consumers also trust Western medical device brands over domestic ones and are willing to pay 20% more for them because they believe them to be more reliable and less likely to malfunction [8].

2.2 Artificial Heart Event

However, along with the increasing medical device market, the number of adverse events is increasing too. The artificial heart was a typical high-technical product that should be applied to heart disease area. This thesis intended to analyze a real case in China, but the real names of the product, hospital, and all stakeholders are not presented in this thesis.

In April 2004, a teenager was undergoing a surgery to install an artificial heart product by a foreign doctor A at a level II hospital in China. A local doctor B provided the treatment plan and made decision to suggest the teenager to take heart surgery. 15 months later, this hospital announced the teenager was dead because of *Systemic organ failure death* in July 2005. And according the public information from this

hospital, the same artificial heart product had been installed to total 9 patients from 2001. The investigation found that 7 of them had died within 15 months.

In June 2007, the State Food and Drug Administration had confirmed that there was no record in their product catalog, which meant the artificial heart was not legal in China. And the surgeon, who installed artificial heart to most of patient, was a foreign doctor from a Europe. The regulation has defined that the foreign doctors must get approval from the Ministry of Health before they provide health service in China. The local health bureau had confirmed they did not issue a license for the doctor B. That meant the doctor was not legal to provide diagnosis and treatment service in China.

According to investigation hold by former SFDA officer, the main contributor to the artificial heart event was the hospital. However, a few questions can be asked. Why could unregistered medical device product be used in the hospital? Why could an illegal doctor take surgeries in the hospital?

The research question that this thesis intends to answer is:
Can Causal Analysis based on STAMP (CAST) provide more insights to the causes of these medical device accidents?

3 Literature Review

To investigate and analyze the cause of an accident and prevent further losses, and assess the risk associated with using the systems and products, researchers have developed many methods through the system design (model) for states or conditions that could lead to system hazards. According to my past experience, there are some methods used widely in the medical device product design process in China, such as FMEA, FTA, ETA, and CCA.

3.1 Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) was developed in the 1950s, and applied to medical device industry since the 1970s. FMEA is a procedure in product development and operations management for analysis of potential failure modes within a system for classification by the severity and likelihood of the failures. Failure modes are any errors or defects in a process, design, or item, especially those that affect the customer, and can be potential or actual. Effects analysis refers to studying the consequences of those failures [10].

FMEA activity can help a team to identify potential failure modes based on past experience with similar products or processes, enabling the team to design those failures out of the system with the minimum effort and resource expenditure, thereby reducing development time and costs [10]. It is widely used in manufacturing industries in various phases of the product life cycle. A general FMEA has 10 steps as figure 2 below. A basic FMEA by Robin is shown below in Figure 3.

Step 1	Review the process or product.
Step 2	Brainstorm potential failure modes.
Step 3	List potential effects of each failure mode.
Step 4	Assign a severity ranking for each effect.
Step 5	Assign an occurrence ranking for each failure mode.
Step 6	Assign a detection ranking for each failure mode and/or effect.
Step 7	Calculate the risk priority number for each effect.
Step 8	Prioritize the failure modes for action.
Step 9	Take action to eliminate or reduce the high-risk failure modes.
Step 10	Calculate the resulting RPN as the failure modes are reduced or eliminated.

Figure 2-Ten steps for an FMEA

Failure Mode and Effects Analysis Worksheet

Process or Product: _____ FMEA Number: _____
FMEA Team: _____ FMEA Date (Original): _____
Team Leader: _____ (Revised): _____
Page: 1 of 1

	FMEA Process											Action Results					
Line	Component and Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) of Failure	Occurrence	Current Controls, Prevention	Current Controls, Detection	Detection	RPN	Recommended Action	Responsibility and Target Completion Date	Action Taken	Severity	Occurrence	Detection	RPN
1																	
2																	
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	

Figure 3-An example of FMEA

Since the effectiveness of FMEA is dependent on the members of the committee which examines product failures, it is limited by their experience of previous failures. FMEA is only part of a larger system of quality control. Used as a bottom up tool, FMEA may only identify major failure modes in a system. It is not able to discover complex failure modes involving multiple failures within a subsystem, or to report expected failure intervals of particular failure modes up to the upper level subsystem or system.

3.2 Fault Tree Analysis (FTA)

Fault tree analysis (FTA) was developed originally in 1961 for Minuteman based on converging chains-of-events accident model. FTA is a top down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean Logic to show specific combinations of identified basic events sufficient to cause the undesired top event (hazard) on a complex system [11]. This analysis method is mainly used in the field of safety engineering and reliability engineering to determine the probability

of a safety accident or a particular system level (functional) failure. Its graphical format can help in understanding system and relationship between events.

The analyst begins with an incident or undesirable event that is to be avoided and identifies the immediate causes of that event. Each of the immediate causes (called fault events) is further examined in the same manner until the analyst has identified the basic causes of each fault event or reaches the boundary established for the analysis [11]. The resulting fault tree model displays the logical relationships between basic events and the selected Top event. Figure 3 shows an example of FTA.

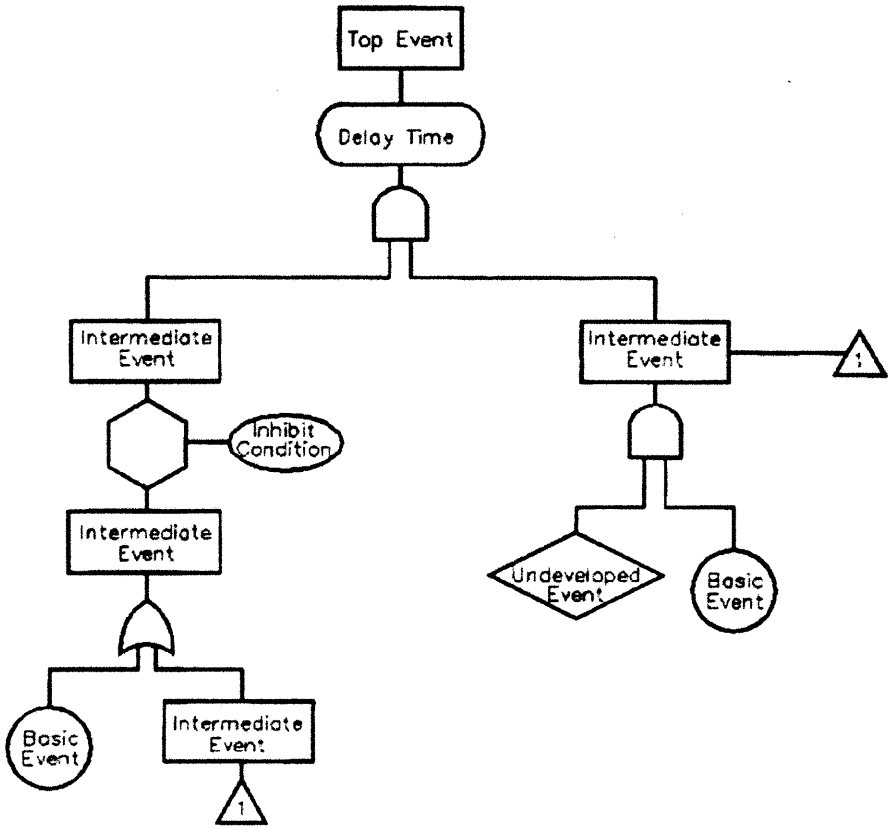

Figure 4-Example fault tree structure

Compared with failure mode and effects analysis (FMEA), which is an inductive, bottom-up analysis method aimed at analyzing the effects of single component or function failures on equipment or subsystems. FTA is very good at showing how resistant a system is to single or multiple initiating faults. But it is not good at finding all possible initiating faults. FMEA is good at exhaustively cataloging initiating faults,

and identifying their local effects. It is not good at examining multiple failures or their effects at a system level. FTA considers external events, FMEA does not [12].

As mentioned previously, complex system fail due to both component random failures and undesirable components interactions. Merely focus on component reliability does not ensure safety [20] Building safer systems requires going beyond the usual focus on components failure and reliability to focus on system hazards and eliminating or reducing their occurrence. This fact has important implications to analyzing and designing for safety. Bottom-up reliability engineering analysis techniques, such as FMEA, are not appropriate for safety analysis. Even top-down techniques, such as FTA, if they focus on component failure, are not adequate [19].

3.3 Event Tree Analysis (ETA)

An event tree analysis (ETA) is an inductive procedure that shows all possible outcomes resulting from an accidental (initiating) event, taking into account whether installed safety barriers are functioning or not, and additional events and factors [12]. By studying all relevant accidental events (that have been identified by a preliminary hazard analysis, a HAZOP, or some other technique), the ETA can be used to identify all potential accident scenarios and sequences in a complex system. Design and procedural weaknesses can be identified, and probabilities of the various outcomes from an accidental event can be determined.

The results of the ETA are event sequences; that is, sets of failures or errors that lead to an incident. An Event Tree Analysis is well suited for analyzing complex processes that have several layers of safety systems or emergency procedures in place to respond to specific initiating events. Figure 4 is an example for ETA.

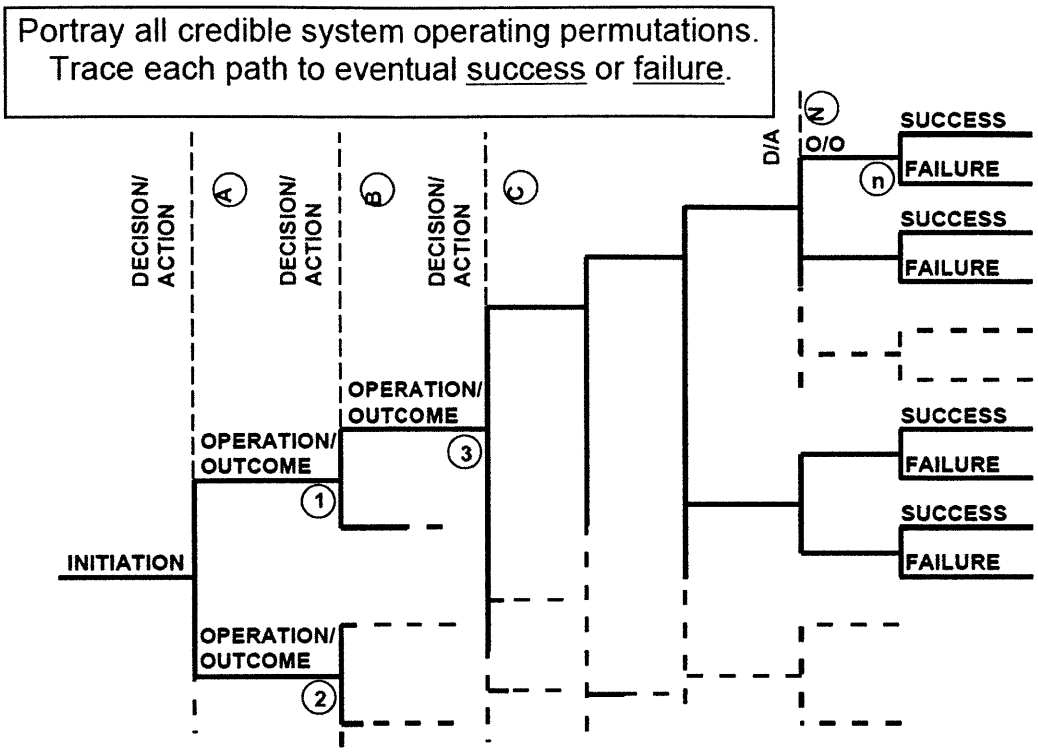

Figure 5-Event Tree Analysis example

The results of an Event Tree Analysis are the event tree models and the safety system successes or failures that lead to each defined outcome. Event sequences depicted in an event tree represent logical AND combinations of events; thus, these sequences can be put into the form of a fault tree model for further qualitative analysis. Analysts use these results to identify design and procedural weaknesses, and normally provide recommendations for reducing the likelihood and/or consequences of the analyzed potential incidents. The ETA can visualize event chains following an accidental event and barriers and sequence of activation; it's better at identifying and simplifying event scenarios; it's useful for evaluating the need for new or improved procedures and safety functions.

The problem is that there is no standard for the graphical representation of the event tree, and only one initiating event can be studied in each analysis. If the events are out of order and not independent of each other, the ETA cannot work. It's difficult to analyze and represent interactions among those events. And because of the simplicity,

it's easy to overlook subtle system dependencies, and not well suited for handling common cause failures in the quantitative analyses [19].

3.4 Cause-Consequence Analysis (CCA)

A Cause-Consequence Analysis (CCA) is a generalization of the most widely spread safety analysis techniques: FMEA and FTA. Generally, CCA can be applicable to the physical systems, with or without human operators. A major strength of a Cause-Consequence Analysis is its use as a communication tool. The cause consequence diagram displays the relationships between the incident outcomes (consequences) and their basic causes [12]. This technique is most commonly used when the failure logic of the analyzed incidents is rather simple, since the graphical form, which combines both fault trees and event trees on the same diagram, can become quite detailed.

CCA utilizes a visual logic tree structure known as a cause-consequence diagram. The purpose of CCA is to determine whether the initiating event will develop into a serious mishap, or if the event is sufficiently controlled by the safety systems and procedures implemented in the system design. With the probabilities of the various events in the CCA diagram, the probabilities of the various consequences can be calculated, thus establishing the risk level of the system. Figure 5 below shows a typical CCA.

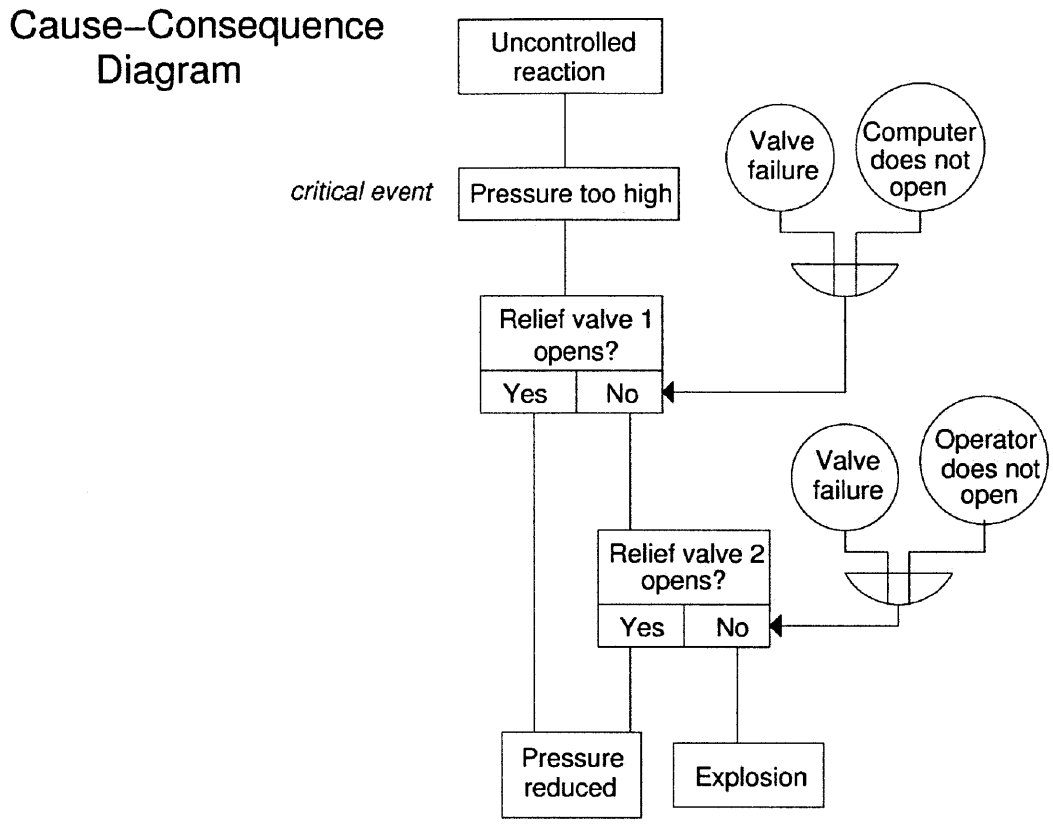

Figure 6-An example of CCA

The CCA technique is a method of risk assessment that provides a means of graphically displaying interrelationships between consequences and their caus. Safety design features that are intended to arrest accident sequences are accounted in the CCA. But CCA was based on converging chain-of-events model again, it can analyze for only a single event, multiple CCA will be required to evaluate the consequence of multiple initiating events [20]. Additionally, the analysis process requires an analyst with some training and practical experience, otherwise the diagrams can become unwieldy.

3.5 Hazard and Operability Analysis (HAZOP)

A hazard and operability analysis (HAZOP) is a technique for identifying and analyzing hazards and operational concerns of a system. It is very organized,

structured, and methodical process for carrying out a hazard identification analysis of a system, from the concept phase through decommissioning [12].

The HAZOP technique was initially developed in the early 1970s by Imperial Chemical Industries Ltd. to analyze chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems. It is a qualitative technique based on guide-words and is carried out by a multi-disciplinary team (HAZOP team) during a set of meetings.

HAZOP can be defined as the application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities to assess the hazard potential that arise from deviation in design specifications and the consequential effects on the facilities as a whole.

This technique is usually performed using a set of guidewords: NO/NOT, MORE OR/LESS OF, AS WELL AS, PART OF REVERSE, AND OTHER THAN. From these guidewords, scenarios that may result in a hazard or an operational problem is identified. Consider the possible flow problems in a process line, the guide word MORE OF will correspond to high flow rate, while that for LESS THAN, low flow rate.

The consequences of the hazard and measures to reduce the frequency with which the hazard will occur are then discussed. This technique had gained wide acceptance in the process industries as an effective tool for safety and operability improvements. Figure 6 gives an HAZOP example.

Guide Word	*Deviation*	*Possible Causes*	*Possible Consequences*
NONE	No flow	1. Pump failure 2. Pump suction filter blocked 3. Pump isolation valve closed.	1. Overheating in heat exchanger. 2. Loss of feed to reactor.

Figure 7-An example of HAZOP

The HAZOP study should preferably be carried out as early in the design phase as possible - to have influence on the design. As a compromise, the HAZOP is usually carried out as a final check when the detailed design has been completed. A HAZOP study may also be conducted on an existing facility to identify modifications that should be implemented to reduce risk and operability problems.

As a systematic examination, HAZOP is easy to learn and perform. The analysis doesn't require considerable technical expertise for technique application. HAZOP analysis can also provide rigor for focusing on system elements and hazards. But it focuses on single event rather than combinations of possible events. And the guide words may lead the analysis to overlook some hazards not related to a guide word [20]. Additionally, HAZOP analysis requires experienced team leader and members, because the analysis may divert to endless discussions of details that wastes too much time.

3.6 Summary

All models are abstractions; they simplify the thing being modeled by abstracting away what are assumed to irrelevant details and focusing on the features of the phenomenon that are judged to be the most relevant. Selecting some factors as relevant and others as irrelevant is, in most cases, arbitrary and entirely the choice of the modeler. That choice, however, is critical in determining the usefulness and

accuracy of the model in predicting future events. Accidents models impose patterns on accidents and cause is ascribed to an accident, the countermeasures taken to prevent future accidents, and the evaluation of the risk in operating a system, the power and features of the accident model used will greatly affect our ability to identify and control hazards and thus prevent accidents [20].

4 Introduction to System Safety Engineering

4.1 System Safety Definition in this thesis

This section is an introduction to system safety engineering. First the vocabulary required to understand this paper is defined followed by a description of the model used for the analysis. The following definitions are adapted from professor Leveson's book.

Safety vocabulary

Safety: Safety is defined as the absence of loss due to an undesirable event (accident).
Accidents: An accident is defined as "an undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, etc.)".

Incidents: Incidents are defined as events not leading to an unacceptable loss but that could have under other circumstances ("near-miss").

Hazards: Hazards are defined as "a system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss)".

Safety Control Structure: The control structure is the web of individuals and organizations (government agencies, companies, individuals ...) whose purpose is to

enforce safety related constraints. This control structure is typically embedded in an adaptive socio-technical system.

Controllers: The controllers are all the agents that are part of the control structure and who "control" the safety of the system through their actions.

STAMP: As discussed in the introduction, STAMP (System-Theoretical Accident Model and Process) is a model of accident causality based on systems theory and systems thinking and is capable of handling complex systems problems. In STAMP, safety is treated as an emergent property that results from the enforcement (through system design and operation) of safety related constraints on the behavior of the system components. Accidents or losses result from unsafe interactions among humans, machines or physical devices, and the environment. Losses are the result of complex processes, including indirect and feedback relationships, rather than simply chains of directly-related failure events (the typical model used to understand causality).

4.2 STAMP Framework

Three basic constructs underlie STAMP accident model: safety constraints, hierarchical safety control structures, and process models.

The most basic concept in STAMP is constraint. In order to provide the level of system safety demanded by society today, we firstly need to identify the system constraints to enforce and then to design effective control to enforce them.

The hierarchical safety control structure is the core of the STAMP accident causality model [20]. This model includes two basic hierarchical control structures, one illustrating the system development process (on the left) while the other represents the system operations (on the right), with interaction between them. Communication may be needed between the two structures. Figure 7 shows a generic example of a hierarchical safety control structure.

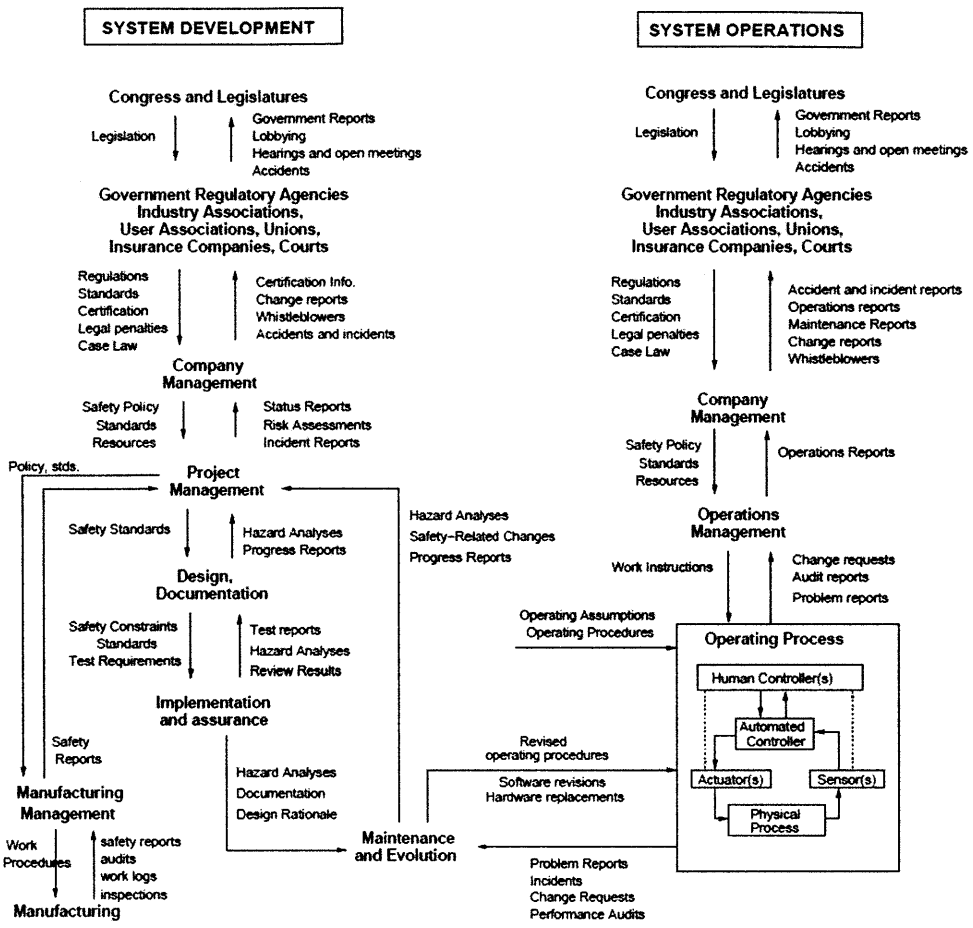

Figure 8-General Socio-Technical Safety Control Structure

Between hierarchical level of each safety control structure effective communication channel are needed. There is a downward channel and an upward feedback channel: The downward provide the information necessary to impose safety constraints on the level below, and the channels represent the ability of one controller to assert its authority and influence over another controller; the feedback channels updates the controller's model of the process it is controlling and shows that how effectively the constraints are being satisfied. Every controller contains a model of the state of the process it is controlling and assumptions about how the controlled process behaves. For human controllers, this is referred to as a mental model [20]. The communications channels between control levels like figure 9.

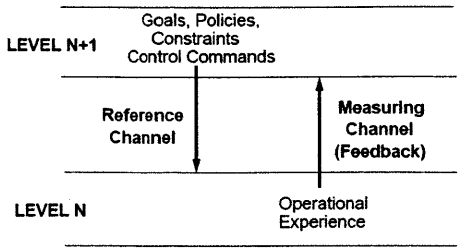

Figure 9-Communications channels between control levels

The third concept in STAMP is process model, which is an important part of control theory. Any controller needs a model of the process being controlled to control it effectively. Process model can help to understand why accidents happened and design safer systems. Components interaction accidents can usually be explained in terms of incorrect process model. Figure 10 shows a general process model.

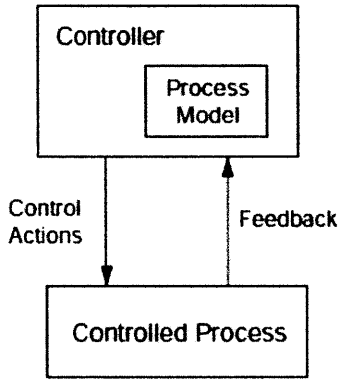

Figure 10-Accidents can occur when the controller's process model does not match the system being controlled and the controller issues unsafe commands

4.3 CAST introduction

Most of accidents reports are written from the perspective of an even-based model. They almost always clearly describe the events and usually one or several of these events are chosen as "root cause(s)." The analysis often stopped at here, the "root cause(s)" always was described as human operator error. Opportunity to learn important lessons is lost. An approach to accidents analysis, based on STAMP, called CAST (Causal Analysis based on STAMP), is used in following analysis. It provides

the ability to examine the entire social-technical system design to identify the weakness in the existing safety control structure. One goal of CAST is to get away from assigning blame and instead to shift the focus to why the accidents occurred and how to prevent similar losses in the future [20].

The STAMP based risk analysis process used in this thesis can be defined in following steps [20]:

1) Identify the system and hazards.
2) Identify system safety constraints and system requirements.
3) Model the safety control structure, discover the main controller, and map the feedback and control channels.
4) Estimate the proximate events leading up to the accident.
5) Analyze the losses at the physical system level.
6) Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to inadequate control at the current level.
7) Examine overall coordination and communication contributors to the loss.
8) Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure overtime.
9) Generate recommendations.

In general, the description of the role of each component in the control structure includes the following:

1) Safety requirements and constraints
2) Controls
3) Context:
   - Roles and responsibilities
   - Environmental and behavior-sharping factors
4) Dysfunctional interaction, failures, and flawed decisions leading to erroneous control actions
5) Reasons for the flawed control actions and dysfunctional interactions

- Control algorithm flaws
- Incorrect process or interface models
- Inadequate coordination or communication among multiple controllers
- Reference channel flaws
- Feedback flaws

The next section mainly focuses on the artificial heart event analysis.

5 Case Study by Using System Safety Engineering Approach

5.1 Event Chains of Artificial Heart

The direct events leading to the death are:

1) A foreign doctor A brought the artificial heart to a Chinese hospital X.
2) A teenage boy moved into hospital X at April 2004, because of primary cardiomyopathy and heart failure.
3) A doctor B worked at hospital X diagnosed the teenager and said he might die within 1 day.
4) The Doctor B suggested taking a surgery to install the artificial heart.
5) The parents of the teenager trusted the doctor and agreed to take surgery.
6) The foreign doctor A and local doctor B were in charge of the surgery at April 2004.
7) The surgery that installed artificial heart seemed successful.
8) The teenager felt uncomfortable, the hospital X provide additional two surgeries to treat the teenager between April 2004 and July 2005. Both of them failed recover the teenager.
9) The doctor B at hospital X suggested taking cardiac transplantation surgery.
10) This cardiac transplantation surgery failed.
11) The teenager died at July 30 2005.

The information above can be found on Chinese media. People blamed the doctor A and B. It seems to be an operator issue. The following content intends to analyze this case again, to see whether deep insight can be found from a social level system.

5.2 System and Hazards Analysis

In this case, ***the system is social technical system for medical device.***

A clear definition of what is considered accidents and incidents is key to any STAMP analysis since preventing or mitigating them is the ultimate goal of the analysis. In this thesis, accident is identified for medical device:

A1: Patients are injured or killed when accepting artificial heart transplant.

According to the investigation report, 9 patients were installed this type artificial heart from 2001 to 2004. 7 patients had died with 2 years since they installed the artificial heart. But the hospital stated that the successful rate of this surgery was 90%.

In the healthcare field, as in most other domains, it is impossible to reach a totally "safe" state. The goal then is to reduce hazards, which are the events and states that can lead to an accident. In medical device "safe" can be interpreted as having an acceptable risk/benefit profile for a device with respect to a specific population.

For medical device products, the system-level hazards can be defined as following:

H1: The artificial heart is not approved for safe use by the SFDA.
H2: The doctor is not qualified to make the surgery.

The effects of this hazard can be magnified in the case of popular medical devices which a large part of the population is treated with. However, there may be other hazards in the system, this thesis only intends to focus these two hazards.

5.3 System Safety Constraints and Requirements

From this hazard, a set of system constraints and requirements can be derived. In system engineering, the requirements may not be totally achievable in any practical design. For one thing, they may be conflicting among themselves or with other system (non-safety) constraints. The goal is to design a system (or to evaluate and improve an existing system) that satisfies the requirements as much as possible today and to continually improve the design over time using feedback and new scientific and engineering advances. Tradeoffs that must be made in the design process are carefully evaluated and revisited when necessary.

Some constraints and requirements emerged from the hazards outlined above. The constraint and requirements are deemed necessary to ensure patient safety during the development and subsequent diagnosis and treatment of medical devices.

H1: The artificial heart is not approved for safe use by the SFDA.
SC1: The artificial heart must be safe for clinical usage.
SR1: The artificial heart must get approval from the SFDA.

H2: The doctor is not qualified to make the surgery.
SC2: The diagnosis and treatment service must be provided by qualified doctor who has license from Ministry of Health.
SR2: The doctor must follow the rules in China.

The main risks in this system are H1 and H2. SC1 and SC2 can provide general constraints to artificial heart, and the detailed constraints can be extended in further study. This thesis discusses the accident from social level, so the technical discussion can be done in further study.

5.4 Safety Control Structure

Now that the accident, the hazards and the requirements have been defined, it is important to study the system itself, identify the different controllers who have a role to play regarding safety and specify how they interact with each other. The first step in studying the system is to identify the ***hierarchical safety control structure*** relevant for this system.

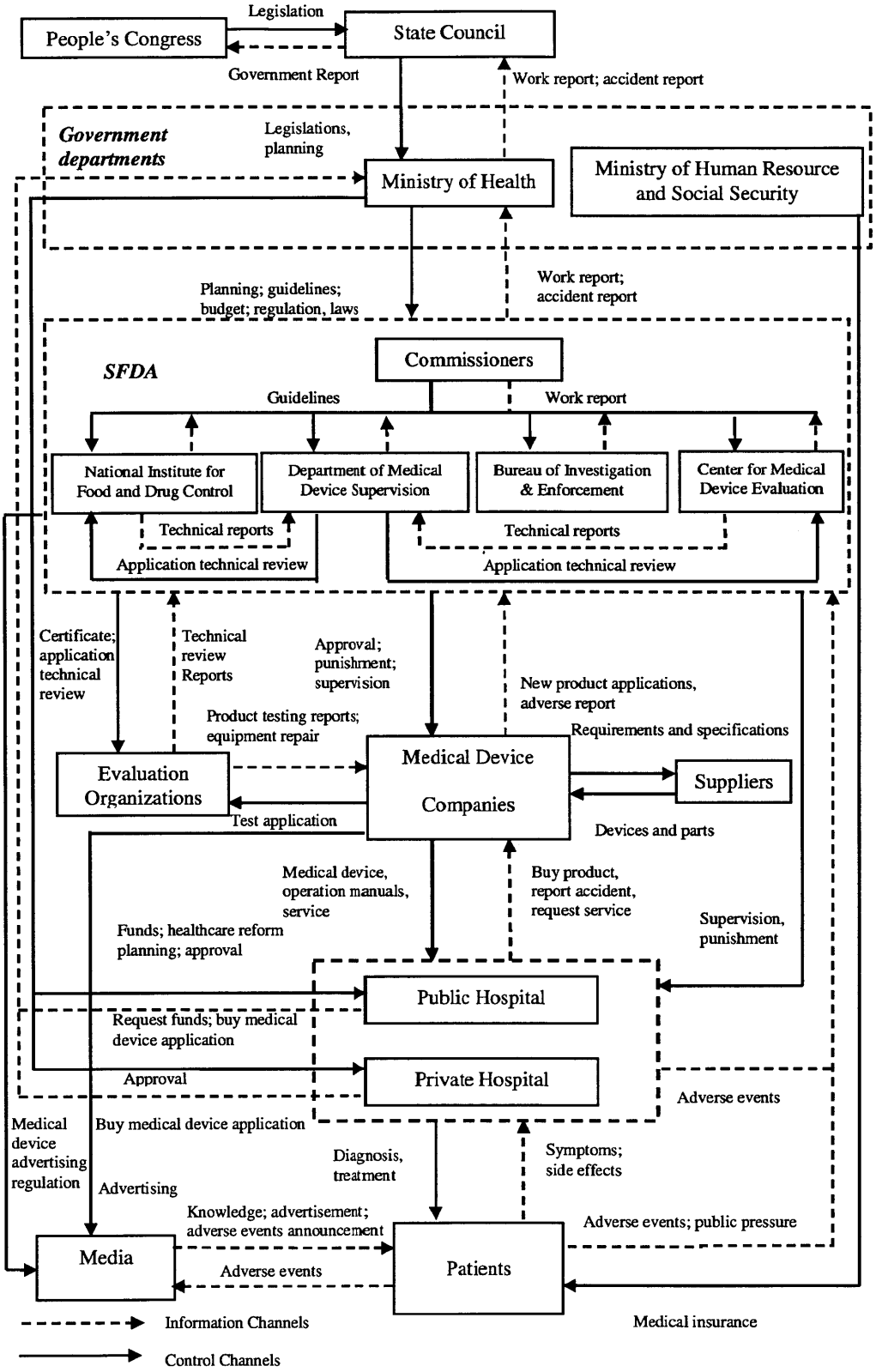

Figure 11-Social System Safety Control Structure

This control structure shows that the medical device safety is enforced by a very complex and interconnected system. Three main controllers (the SFDA, Medical device companies, Healthcare Providers) compose the core of the system and a variety of smaller controllers play a peripheral role in medical device safety (State Council, evaluation organization, media, etc.)

Those controllers are interrelated and their interactions are of two types: control and information. The control allows one controller to impose safety requirements on another. For example, healthcare providers control patient's access to medical device through diagnosis and treatment. The information serves as feedback mechanism: patients can report the side effects when they are taking the treatment.

In this safety control structure, each of the safety requirements is enforced by at least one controller. But, if each of the controllers relies on the others to monitor the medical device safety, issues can go unmonitored. In addition, the assignment of responsibilities does not mean that they are effectively carried out.

Once the responsibilities for each of the controllers has been identified, the controllers can be analyzed independently to see whether the context they work in allows them to properly fulfill their safety responsibilities and if they have the resources and information they need to enforce the safety constraints they have been assigned.

Controller operation has three primary parts: control inputs, control algorithms, and process model [20]. Inadequate, ineffective, or missing control actions can lead to system failures. Figure below from professor Leveson's book established several classifications of control loop deficiencies that could lead hazards.

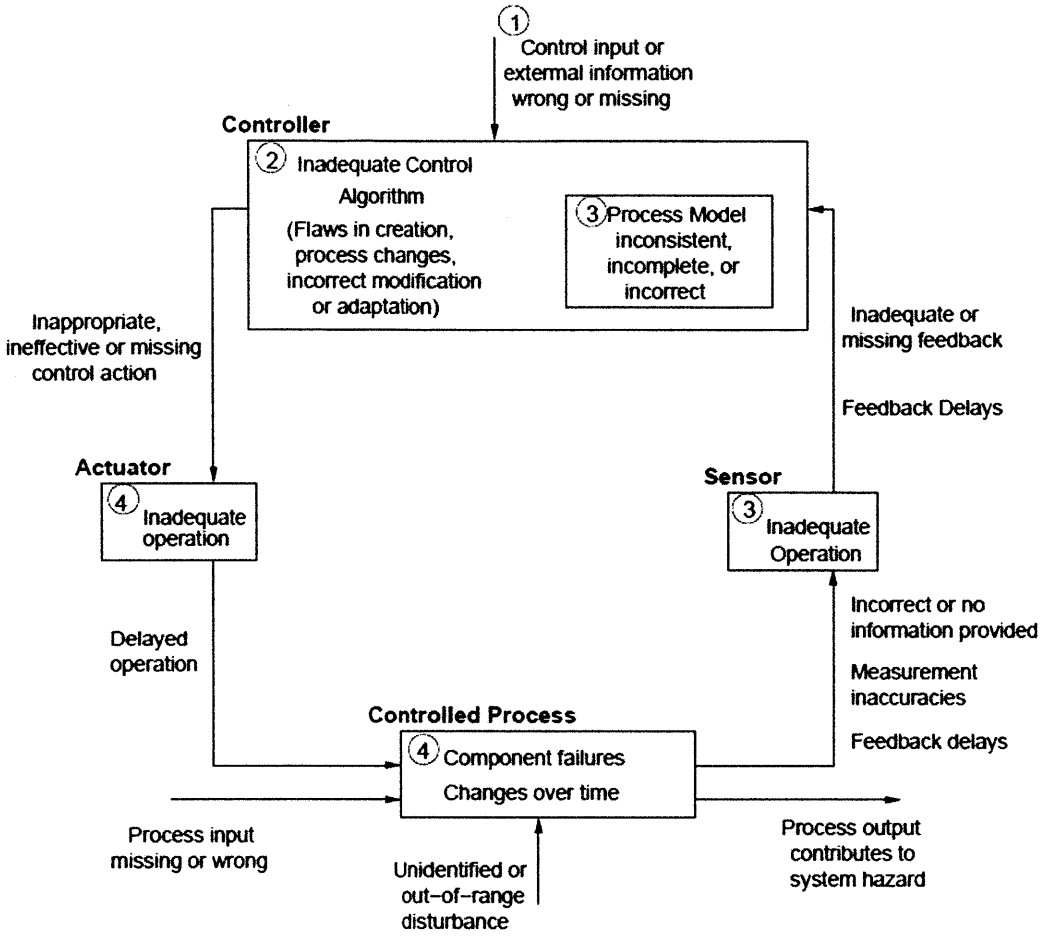

Figure 12-Classification of control flaws leading to hazards

5.5 Physical Process Failure and Dysfunctional Interactions

From the event chains, the artificial heart case seems a normal death of a failed surgery. Every surgery has risk, in particularly the heart relating surgery. However, the investigation hold by former SFDA officer found some abnormal activities:

1) China Customers mentioned that the foreign doctor A brought the artificial heart into China, but he didn't report this item to them when he got through customers.
2) The hospital X said the Success rate of surgery was 90%.

3) The doctor B might provide inadequate diagnosis and treatment suggestions to teenager's parents, because another teenager had same situation but didn't take artificial heart surgery was alive.
4) The foreign doctor A was not legal to be a doctor in China because he didn't get approval from local Health Bureau.
5) The doctor B might provide inadequate treatment to teenager after artificial heart surgery.
6) After the death of the teenager. His parents claimed that the hospital X could waive part of fees around hundreds of thousands of RMB if they could sign a special contract that required them couldn't report the details of treatment to governments, media, and judiciary. But hospital X denied they have done this.
7) The SFDA mentioned they didn't issue a certificate to the artificial heart.
8) The hospital X claimed that the artificial heart used on teenager was imported at 1998. The regulation for medical device was established at 2000. Therefore, the artificial heart didn't violate the regulation.
9) The hospital X didn't have permission to take pediatric surgery and pediatric cardiothoracic surgery.
10) The hospital X claimed that they had gotten permission at 2004 from Shanghai Health Bureau. So the surgery for teenager was legal. But the date they got permission was later than the date of surgery.
11) Investigation found the hospital X had installed this kind of artificial heart to total 9 patients since 2001. 7 of them had died within 2 years.

As a common investigation, it stopped here and gave very good root causes why this accident occurred. Examining the higher levels of control is necessary to obtain the information to prevent future occurrences.

5.6 Analysis of the Hierarchical Safety Control System Controllers

The safety control structure gives a big picture to show the interactions between each controller. In this section, not all control loops are analyzed. The analysis intends to start from the control loops directly relating to the artificial heart accident from bottom to up. The higher level control loops require investigating politics and culture

background which was too complex in China. Additional studies can be taken in future.

5.6.1 Hospitals and Patients Loop

The hospitals directly control the patients, including that provide diagnosis and treatment service. The patients can only give feedback information and pay service fees to the hospitals. The responsibilities of hospitals and patients are first described, followed by the context in which their decision and actions took place. Then the inadequate control actions are outlined and the factors that led to them are described. Finally, the dysfunctional interactions and reason why the inadequate control happened at this level of the control structure are analyzed.

Hospital

General Information:

A hospital is a healthcare institution that provides diagnosis and treatment for patients by specialized staff and equipment. In China, the healthcare providers include public hospital, private hospital, urban and rural health center, and CDC. The public hospitals are first choice of most of Chinese.

The public hospitals are usually funded by the government, and the private hospitals often funded by themselves. But all healthcare providers should get approval from the Ministry of Health firstly. Historically, the public hospitals provide traditional Chinese Medicine to patients, and operate few traditional Chinese medical devices. Today, more than more hospitals are offering Western Medicine, and have largely professional physicians, surgeons, nurses, and high-technical medical devices.

Roles and responsibilities:

The hospitals should follow Chinese regulations

First of all, the hospital should follow Chinese regulations for health. The legal hospitals must get approval from the Ministry of Health (MOH), every section that provides diagnosis and treatment service in the hospital should have registered at the MOH. The hospital cannot provide service they do not registers. For example, the

hospital could not take heart surgery if it does not have a record at the MOH, even if the hospital has heart disease professionals.

The hospital is expected to provide safe healthcare service to patient.

The patient needs safety when accepting diagnosis and treatment. Medical devices are used in these processes. Generally, a medical device is imposed on human body directly. Firstly, the hospital should buy legal medical device product that has a legal certificate from the SFDA [1]. For some special medical devices, the hospital needs to submit application to the MOH to get approval.

Secondly, the hospital is expected to recruit qualified professionals. The doctors should be professional and have a legal license from the MOH. It's the doctor's responsibility to make treatment decisions based on the best interests of their patients, that they will weigh the risks of treatment and non-treatment.

Finally, hospitals are expected to monitor the long term health of their patients and report potential adverse events or negative interactions to the medical device manufacturers.

Context in Which Decisions Were Made:

Health resource and funds pressure

The population was too large in China. Although the MOH had allocated a lot of funds and health resources to the hospitals, it's difficult to meet the increasing patient's needs. The distribution of resources might not reasonable in some areas. Most of level III hospitals in urban areas could get more resource than rural areas because of some special reasons. Additionally, the Chinese always believed that level III could provide better diagnosis and treatment service, even if the prices were much higher. Therefore, most of Chinese preferred to accept treatment at level III hospitals.

Actually, it's true that the level III hospitals could provide good healthcare service, but they were located at big cities and there are more patients than small counties. Many patients from rural areas will go to level III hospitals if they get some critical disease that the level I hospital can't handle. Their visiting increase the pressure of level III hospitals, so that hospitals have to require more and more funds and

resources from the MOH, then they can hire better doctors, buy better medical devices, and provide better healthcare service, to increasing patients. At the same time, their doctors were notoriously busy and their time was limited, so that they had to work intensively and overtime, which might result some risks. Rather, the level I hospitals could not get enough resource to develop.

The hospital trusted medical device company

As doctors, they mostly learnt about new products from the medical device companies themselves. Many medical devices were new to Chinese, so the doctors always trusted information from the manufacturers, in particular the western companies, they believed the western brands have better quality and effectiveness. Furthermore, the patients were too much to the doctors didn't have enough time on studies of new medical devices, so their operations might violate the right instruction.

The hospital tried to improve reputation and grade.

The hospital X was a level II hospital, and looking forward to upgrading to level III hospital. One criterion of promotion was the hospital had its strengths, for example, the artificial heart surgery had low successful rate in China, if the hospital could complete a couple of successful artificial heart surgeries, then its reputation could be increased a lot.

As a leader at hospital X, doctor B was responsible for the promotion of hospital, which could bring higher position, income and personal reputation. Certainly, the promotion meant more resource and funds to hospital. Doctor B had some foreign background at Europe and U.S. He had some connections with many western medical device research institutions and companies. So he could buy some new products from Europe. And as a Chinese professional, he knew the regulations and standards had some defects.

Patients

Roles and Responsibilities:

Patient should know effectiveness and side effect of diagnosis and treatment provided by hospital.

The patients are the ones most directly affected by the risks and benefits of the medical device: they benefited from the diagnosis and treatment provided by medical devices but might also have suffered from an adverse event related to the use of the medical device. Patients are expected to take care of their own health, which entails seeing a doctor when they feel ill and maintain a healthy lifestyle. In some cases, patient access to a medical device is limited and the medical device has to be provided by a doctor. They have right to know why should they take such treatments and what is the effectiveness and side effect. Once patients feel uncomfortable or abnormal when accepting treatment, they should report to the doctors immediately.

Context in Which Decisions Were Made:

Patient trusted hospital and did not care the side effect.

Because only a small part of Chinese had received college education, patients didn't have professional medical knowledge, so they always trusted what doctors said in some big hospitals, especially the high level hospitals. Generally, patients might follow everything the doctors suggested and not question the doctor, for example, took unnecessary diagnosis and treatment. In addition, the Chinese patient only focused on the effectiveness of the treatment, few of them might know to ask the side effect.

The medical insurance could afford not the expense of critical diseases.

Another Chinese characteristic was the large population. The medical insurance was provided by China government. However, China was a developing country, although the government had provided medical insurance to cover over 12.8 billion Chinese, the compensation was not enough to cover the treatment fees of some critical illness. Many patients could not afford huge service fees. They might accept the treatment plan if hospitals could waive some fees.

Dysfunctional Interaction at this level:

Communication between hospital and patients was completely dysfunctional. The hospital hid critical information that might be harmful to the patients and patients did not ask the effectiveness and side effect of the artificial heart surgery.

Flawed or Inadequate Decision and Control Actions:

Hospital

The hospital provided unnecessary diagnosis and treatment plan.

In a competitive environment, where doctors have to fight to keep their clientele, it is easy to imagine how doctors might cave under the pressure and provide an unnecessary treatment service.

Firstly, according to the investigation reports, for every patient, the doctor B provided exaggerated diagnosis result, and suggested an unnecessary treatment to them for purpose. Obviously, his treatment plans were contradictory with his diagnosis. But the patients did not have medical knowledge to know if they should take surgery to install an artificial heart. Patients had to follow doctor's suggestions.

The hospital conducted surgery that they did not get approval.

Secondly, doctor B didn't inform the patients that hospital X did not have approval to conducted pediatric surgery. The record in local health bureau showed the hospital got approval at July 21 2004. But the investigation showed total 9 surgeries were done between 2001 and 2004, all of them were taken before approval.

The hospital used illegal artificial heart

The SFDA had confirmed the artificial heart was a product had not a legal certificate from them. According to the investigation, the hospital could not explain how they got the artificial heart. The investigation showed the artificial heart that applied to the teenager was took by the foreign doctor A. And before this one, the hospital bought artificial heart from a Chinese medical device company which disappeared at 2001. The hospital did not tell the patients that the product was an illegal product, they just told the patients this artificial heart had been successful used in the Europe with a high successful rate.

The hospital allowed illegal foreign doctors to provide medical service.

Furthermore, the doctor B allowed the foreign doctor A to take surgery for patients. The surgery reports showed that the foreign doctor A was the primary surgeon. But according to the Chinese laws, foreign doctor can only provide medical services after they get permission from health bureau.

The hospital did not stop illegal activities.

In addition, the hospital X didn't stop the surgeries when they found some patients had died after took artificial heart surgeries. The hospital also didn't provide incentive to encourage its staff to report inadequate actions done by some doctors.

The hospital did not report accident.

Finally, the hospital X tried to pay money or compensation to some patients who had died after heart surgery. The deal was the families of patients could not report the surgeries to public and government.

Patients

Patients did not insist on their right.

The patients had rights to know the effectiveness and side effect of diagnosis and treatment provided by hospital. But few of them asked for the details, they just followed the suggestions from the doctors.

Reason for Flawed Control Action and Dysfunctional Interaction

Incorrect Metal Model:

The hospital X believed that artificial heart was safe, in particular the medical device company that manufactured the heart had mentioned the product had been applied widely and successfully in Europe. Like many Chinese hospitals, the hospital X believed that western brand had higher quality and effectiveness. And the doctors believed that expensive medical device was much better and safer than cheap medical device. Of course they could charge higher service fee and get more money, so the doctors recommended unnecessary but expensive diagnosis and treatment. The investigation found that the total healthcare service fee for this teenager was more than 600,000 RMB. Same as this teenager, other patients who had taken this surgery were charged a lot.

The hospitals also typically believed that information provided by manufacturer was accurate. However, the manufacturer always described their products better than they are. Additionally, the hospitals believed that patients might go to another hospital if they did not provide expensive and high technical treatment plan. Chinese patients always require expensive treatment because they believed that was much better than cheap one

Finally, the hospital always believed that patients did not understand their treatment. They believed that patients trusted everything they did was good to them. Even if they did something wrong. And the patient could not know the diagnosis and treatment was not necessary. The hospital told the patients that every surgery had risk. So the patients died, the hospital explained that was a normal failure.

Patients

The Chinese patients believed that the higher level hospitals could provide better treatment service. Also they believed higher price of the service, the better effectiveness of the service. The patients also believed what the doctors provided were right for their health. Few of them might question the doctors what they were doing, and why did they do that.

5.6.2 Medical Device Company and Hospital Loop

General Information:

A medical device company is in charge of the medical device research & development, manufacturing, sales and service. Currently, the medical device company in China can be defined two types: domestic medical device company and foreign medical device company. The main providers in mainland are foreign companies, in particularly the western companies, like GE, Philips, and Siemens. Western companies provide more than 70% high technical medical device products. The Chinese healthcare providers, especially public hospitals, trust western brands more than domestic brands. They believed western companies can deliver better technology.

Role and Responsibilities:

The safety requirements and constraints imposed on medical device company extend from the pre-approval phase, where the company is expected to be researching new medical device, to post-approval requirements such as conducting more studies to look for long-term side effects. Those safety responsibilities are organized in four

major sections believed to cover the major safety requirements imposed on medical device company.

Ensure that patients are protected from avoidable risks

Manufacturers are expected to provide safe and effective medical device. Patients are exposed to medical device when they accepting diagnosis and treatment. Firstly, the medical device company should meet regulation requirements provided by the State Council, the MOH, the SFDA and other governmental departments. The company should have strict internal quality and safety control process to ensure that the product is safe and effective as its description. And because some risks may be difficult to find in house, the company should provide long-term safety monitoring system to ensure the safety of the patients and avoid their exposure to unnecessary and preventable risk after the product is used on patients.

Additionally, the company is expected to provide operation manuals and training to medical device operators. According to the statistics from SFDA report at year 2010, the risk is mainly from operation issue. Therefore, it's important to ensure that the operator is working on right way, which should reduce a lot adverse events. It's medical device company's responsibility to edit properly operation manuals and provide training to operators. Furthermore, the company should learn operator's behaviors and design product to prevent unsafe operation, because some operators may not follow operation manuals and result patient injury.

Monitor medical device for safety

After medical devices are on the market, the companies are expected to keep on monitoring their products for long term side effects. After a medical device has been approved, it is the responsibility of the medical device companies to run the studies in a timely manner and report to the SFDA annually on the progress of their post-marketing commitment. For example, the company should do a post-marketing study to gather more information about whether the product is safety, efficacy or optimal use, and decide whether the product needs to a design change to prevent hazards.

Furthermore, the medical device company should encourage customers and its employees to report adverse events, the company should try to investigate that hazard

and conduct new studies to solve trouble, even if it is expensive for the firm. Similarly, if new risks are discovered during studies run by the companies, it is expected that they should share this information with the SFDA, even if the results are negative. The disclosure of negative results goes against the company's business interest but it would be considered unethical for a company to conceal health risks associated with a medical device. Therefore, the company must recall or remove a dangerous product from market to protect the patients.

Give accurate and up-to-date product information to SFDA and customers

As mentioned above, the medical device company should provide all available information about the safety of the product to the SFDA, so that SFDA can decide whether issue the registration certificate, and check the product in the market regularly. Secondly, the information must be reliable and traceable. Unlike the SFDA, customers do not have techniques and resources to assess if the product is safe or not. They have to trust and follow information the company provides.

Develop the products to eliminate potential hazards

Medical device companies are constantly innovating, finding treatments for new diseases or improving on the existing treatments to limit their side effects.

Context in Which Decisions Were Made

The medical device company was profit-oriented

The company has a fiduciary duty to shareholders to provide a return on their investment and stakeholders demand a high return. Furthermore, medical device company executives are partly paid in stock options and therefore have strong incentives to return a high profit. As mentioned in Chapter 2, the China medical device market is extremely competitive now, especially for the domestic companies, because according to the survey [8], Chinese consumers would like to trust large western medical device brands over domestic ones and are willing to pay 20% more for them. The reason is that Chinese consumers believe the large western medical device companies have a comparative advantage in terms of technology and service. They believe them to be more reliable and less likely to malfunction. As a result, many domestic companies cannot get satisfied return.

The medical device company delivered unsafe products when regulations system was developing in China

And as mentioned previously, the regulation system in China has few defects and needs optimization. However, because of complex and special situation in China, it's difficulty to build a perfect regulation and supervision system in a short term. Thus, a few domestic and many small western medical device companies developed some products that may be dangerous for patients. These products will not be recalled or removed unless accident happened, because they did not violate the current regulations. Even if the products violated the regulations, the SFDA might not find the illegal activities. So the companies can get better profit return.

As a result, both domestic and western medical device companies have no incentive to do extra safety testing. The goal of running business is profit, extra testing activities always cost more money and human resource, and the product will be delayed to release to customers. Similarly, they have no incentives to publish negative internal studies, which may reduce the profit, and band's reputation.

Dysfunctional Interaction at this level:

In this case, the investigation report did not provide clear description about the deal between medical device company and hospital. The Europe medical device company refused to answer any question from China. So the author has to analyze the inadequate control actions based on known information.

Flawed or Inadequate Decision and Control Actions:

The medical device company exported product to a Chinese hospital without SFDA license. The goal was to do illegal clinical test in China, because the clinical test was complex, expensive and long time in the Europe.

For profit-oriented company, time is money. As discussed earlier in the previous section, medical device companies need to make a profit and generate revenues for their stakeholders. Their activities were motivated by marketing goals. The company always speeded up the product design and development process to enter market earlier. So it did not run some necessary tests and studies that might find its product to be dangerous. Such tests and studies are costly and risky, especially for some developed market, it costs a lot of money to do tests, for example, the clinical test.

The artificial heart is a product that requires clinical test in China if the foreign product wants to enter China market [3]. And the registration process is much longer than standard in China, for example, the longest registration process should be 90 days [1], but it always needs more time, some product needs 18 months. It may be too long to the medical device company, so that the company may lose market and profit. And if the product cannot get approval, the company has to re-design the product until it meets the SFDA's requirements, and re-apply for registration, which may take more time and resource.

Therefore, a few small companies decided to manufacture and sell medical device products without applying SFDA registration certificate. Actually, the hospitals should not buy the medical devices without official certificate, but these unqualified products were sold at very low prices or sold with bribe activities. Some small public hospitals and private hospitals might buy these unsafe products to cut the expenses.

Therefore, the Europe medical device company that manufactured artificial heart entered China market by an illegal way. The investigation found that someone started up a medical device in China firstly. Then the domestic company imported artificial heart from Europe to China. But the domestic company did not apply registration for this artificial heart; this local company counterfeited a registration license for sale. And in China, few consumers might check if the license was legal with the SFDA, because it's hard to check the license. After the hospital in this case bought some artificial heart, the company disappeared.

The foreign medical device company refused to answer any question.

After accident happened, the medical device company didn't respond for this accident. They only said: "Please ask that hospital X." A lot of information was lost so that the investigation could not find more inadequate actions. For example, did the company know the product may cause death?

Reason for Flawed Control Action and Dysfunctional Interaction

Incorrect Metal Model:

Although no evidence can verify the medical device company intended to deliver illegal product to China. They claimed they did not know and please asked for the hospital X. But investigation report found that the doctor A provided at least one artificial heart to the hospital X. The doctor A was an employee of this medical device company.

Obviously, same as the hospital, the company also believed if they did not report the negative results to Chinese public and government, none might know the artificial product was unsafe. And their reputation would not be decreased. In addition, medical device company believed that the regulation system and supervision system in China was not so good to discover their activities. Therefore, they could deny everything, just like they did.

5.6.3 The SFDA, Medical Device Company and Hospital Loop

In Chinese medical device system, the SFDA is responsible for administration and supervision for medical devices. In this accident, the SFDA was supposed to monitor the medical device market, and remove unsafe product from the market.

State Food and Drug Administration (SFDA)

General information:

The State Food and Drug Administration (SFDA) (Chinese: 国家食品药品监督管理局) is founded in 2003 on the basis of the State Drug Administration. The State Food and Drug Administration is under the Ministry of Health, which is in charge of comprehensive supervision on the safety management of food, health food, cosmetics and medical device, and is the competent authority of drug regulation in mainland China. The sections within the FDA responsible for medical device are **Department of Medical Devices Supervision**, **Bureau of Investigation & Enforcement, National Institute for Food and Drug Control and Center for Medical Device Evaluation**. This thesis puts them together for analysis [4].

Role and Responsibilities:

Follow regulations and guidelines from the State Council and the MOH

Firstly, SFDA is expected to follow regulations provided by the State Council and the MOH, and draws up detailed regulations and standards to administrate and supervise medical device. It's SFDA's responsibility to set requirements for all new medical device applications and define the approval process for new medical device. The regulation for registration was established in 2004 and every medical device since has been the subject before commercialization. The SFDA provides guidance documents for different types of new medical device applications on its website.

Provide administration and supervision system to prevent potential hazards.

Once an application has been submitted to the SFDA, it is SFDA's responsibility to critically examine the applicant's claim that a medical device is safe for intended use and to impartially evaluate the new medical device for safety and efficacy and approve it for sale if deemed appropriate. The SFDA does not run the clinical trials but sets the standards for the evidence required for a medical device's approval, monitors the research and reviews the results from the company's data. If SFDA considers that the medical device is effective and its health benefits outweigh the risks, the medical device is approved.

The SFDA is responsible for overseeing the promotion of medical device and ensures that promotional materials are not misleading or false. The SFDA has to review all the material submitted by medical device companies and identify potential violations such as advertisements minimizing the risks of a medical device and overstating a medical device's safety and effectiveness.

The SFDA is in charge of post-marketing surveillance to identify adverse events that were not detected during the initial approval process. The SFDA also collects notices of adverse events in China mainland market and analyzes this event to publish new regulation and standards to prevent potential hazards.

Remove unsafe products from China market

The SFDA has the power, and the responsibility, to remove a medical device from the market if it discovers new information about the safety and effectiveness profile of the medical device that may put the public at risk. At the same time, the SFDA needs to publish the medical device that has high risk on its website for notification to public.

Context in Which Decisions Were Made:

The authority of administration and supervision shifted many time between different governmental departments so that the authority is complex

Because of historical and special reason, a few departments have been involved into medical device administration and supervision. These departments have published some regulations, laws and standards for medical device. After the SFDA was established, it should be the only legal department that was in charge of medical device. However, regulations, laws and standards enacted by pervious governmental departments are still effective, and some of them conflict with and have higher power than current regulations and standards established by the SFDA. Therefore, medical device companies find that they are not sure which regulation they should follow when they want to apply for product registration. For example, some cardiac pacemaker products should be registered and get license from the SFDA, but the General Administration of Quality Supervision, Inspection and Quarantine of P.R.C has defined that if these products could not get a CCC certificate, they could not be sold in China market even if the products had gotten approval at the SFDA.

Number and ability of employees was not good enough to provide thorough supervision

According to the statistics, there were only 250 employees that had medical device background in SFDA [16]. But there were over 13,600 types of medical device companies and over 100,000 hospitals by end of year 2007. Obviously, the professional staffs were not enough to take regular inspection to monitor so many medical device products in the market. It still needs time to train enough qualified professionals. Although the SFDA has defined many regulations and policies that constraint illegal products and activities, it could not find all violations in a so complex market.

Trusted information from the medical device company

As mentioned previously, clinical trials and other tests are done by the medical device company manufacturing the medical device, there is no independent external group that tests the medical device and the only information available to the SFDA at the time of approval is the information from testing departments and medical device

company. But no one can ensure that the technical testing work was quality enough. The SFDA has to make decision whether provide license for the registration application based on some unreliable technical review and evaluation. And because of limited personnel and resource, more and more registration applications were submitted, the review process was always much longer than standard. And no extra safety study after medical device was approved although it's required in the rules.

Therefore, medical device companies always deliver the most favorable results to SFDA to speed up the review process. This lack of transparency hinders the work of the SFDA and puts the public at risk by hiding potentially important safety information. Even if adverse event happened, the medical device companies always tried to hide it.

Dysfunctional Interaction at this level:

Communication between the SFDA, the medical device company and the hospital was obviously dysfunctional. The system constraints required the SFDA to remove the unsafe medical device. But the medical device company did not apply for registration and clinical test. The hospital did not tell the SFDA that they bought and used an illegal product on patient.

Flawed or Inadequate Decision and Control Actions:

The SFDA did not remove unsafe product from market.

The system required the SFDA should remove unsafe products before the products applied to human body. So it seems that the inadequate control action for the SFDA was they failed to find an unsafe product and remove it. But the real inadequate control action was the SFDA did not provide qualified administration and supervision system, a subsystem in medical device system, to find potential risks. The following discussion mainly focuses on the losses of the subsystem.

The SFDA didn't have enough professionals and could not provide effective regulations and supervisions to constraint illegal activities.

As mentioned above, the human resource issue was a big trouble that SFDA was facing. It was difficult to hire qualified professionals. Similar, it was hard to provide professional training to its staff, because the medical device products were innovating

too fast. As a result, sometimes the SFDA may approve medical device's registration based on an assumption that the materials medical device company submitted were correct.

Even though the SFDA had its technical center to evaluate medical device, the same problem was that the SFDA could not ensure the quality of evaluation. The unprofessional evaluation might fail to find potential defects. Secondly, it cannot review all submissions thoroughly because of the volume of materials it receives and that only a small portion of the required submissions of final promotional materials were examined for potential violations.

The state SFDA could not provide oversight on activities of its regional branches

Although there are many regulations to constraint the medical device, a few products are still trying to violate the regulations. The SFDA has required its branches to conduct additional monitoring and surveillance to detect violations that could not be identified through a review of submitted materials, but some provincial branches or rural branches did not follow the requirement. Therefore many companies counterfeited the SFDA license and sold unsafe products to consumers. The patients might be exposed to the potential risks.

The state SFDA did not provide uniform management for its branches

Finally, the internal management of the SFDA was disordered. The SFDA didn't provide a uniform standard and process for medical device registration. There were more than 700 branches in China could handle medical device registration and supervision. The problem was that the State SFDA only provided regulations, but did not provide a uniform work standard and process for its branches. And the employees in different level branches must have different capacity, which lead the different results on the effectiveness of supervision [17]. Similar, the state SFDA could not monitor the effectiveness of its 700 branches too, because of manpower pressure. Therefore many medical device companies could maximize its profits by not submitting registration application at a certain place and deliver unsafe products to Chinese consumers. Like those companies, some hospitals bought illegal products even if they knew the products were unsafe, because of some dirty trading. They thought the SFDA could not find their illegal activities.

Reason for Flawed Control Action and Dysfunctional Interaction

Incorrect Metal Model:

As a controller, the SFDA assumed regulations and supervision system was good to prevent losses. Secondly, the SFDA assumed medical device companies should follow the regulations and provide safe products to consumers. Thirdly, the SFDA believed all products that had passed their evaluation to enter China market were safe. Then, the SFDA assumed the hospitals should buy illegal products which had illegal licenses issued by the SFDA. Finally, the SFDA assumed the adverse event report channel was good.

5.6.4 Ministry of Health and Hospital Loop

Ministry of Health

General information:

The Ministry of Health (MOH; Chinese: 卫生部) of the Government of the People's Republic of China is established in 1949, and MOH is an executive agency of the state which plays the role of providing information, raising health awareness and education, ensuring the accessibility of health services, and monitoring the quality of health services provided to citizens and visitors in the mainland of the People's Republic of China [6].

The Ministry of Healthcare also provides experts to investigate poisoning cases, enforces food safety, ***medical device safety*** and hygiene inspections, and can order local health departments to conduct investigations into food and medical product quality violations. The Ministry of Health also oversees the State Food and Drug Administration (SFDA), an agency that has studied and identified unsafe foods, drugs and medical devices, and has helped local health authorities form policies and training programs to combat unsafe food and medical production and handling practices. It also cooperates and keeps in touch with other health ministries and departments, including those of the special administrative regions, and the World Health Organization (WHO).

MOH is a big organization that is in charge of many affairs, this section mainly focuses on its responsibilities that have relationship with hospitals and medical devices.

Role and Responsibilities:

Provide regulations, standards, and provisions for healthcare providers and medical devices.

MOH is expected to provide detailed regulations, standards and provisions to support the State Council's regulation, and oversee the effectiveness of the regulation system. Currently, the MOH was responsible for the administration and supervision for hospitals, and the SFDA, part of the MOH, drew up the regulation or provision for medical device, and supervised the China market.

The SFDA could publish regulation by itself, but the legal level was lower than the regulation published by the MOH. So many regulations were published by the MOH to improve the legal level. Certainly, the MOH has the power to approve or deny the inadequate regulations from the SFDA. It's the MOH's responsibility that ensured the regulations could protect people's health and lives.

Allocate health funds and resource according to health development plan

The MOH is expected to decide how to allocate and balance healthcare resources and funds among public hospitals, urban and rural health centers, and CDCs. In addition, the MOH has the power to define the regulations and policies about registration, scope, medical device purchasing, and service prices for government fund hospitals. The MOH also provided the license for medical professionals. A doctor could not provide medical service if he or she did not have license from the MOH. Finally, it's MOH's responsibility to oversee these hospitals and medical professional's activities. Once the MOH found that any activity of hospital violated current regulations and laws, the MOH could annul the hospital's qualification.

Context in Which Decisions Were Made:

The authority of administration and supervision of medical device shifted many time between different governmental departments so that the authority is complex now

As mentioned in previous part, during past 10 years, a special situation is that no single agency is responsible for all medical device safety regulations and enforcement in China, several government departments and ministries under the State Council wants to be involved into medical device area. These include the Ministry of Health, the State Administration for Industry and Commerce, the General Administration of Quality Supervision, Inspection, and Quarantine, the Ministry of Commerce, and the Ministry of Science and Technology. And there is no clear hierarchy of agencies at the local or national levels.

The MOH was supposed to oversee the all aspects of medical device safety regulations and unify safety controls since 2008. However, the other national agencies have continued to regulate and monitor some medical devices. This unclear division of duties has created conflict and confusion when citizens have sought to complain or a when major crisis needed to be resolved.

The MOH is responsible for drafting regulations, standards and policies, however, a few staffs and decision makers were not familiar with the hospitals and medical devices. The MOH could not build perfect regulation system to regulate and monitor hospitals and medical devices. Furthermore, the evergrowing people's healthcare requirement pushed the government to build more and more public hospitals, which required a lot of funds and healthcare resource. But the funds and resources were limited. The traditional way was that allocated more funds and resources to high level hospitals in urban area. For some small hospitals, it's hard to get enough resources to develop.

At the same time, more and more hospitals were building in China urban and rural areas, and it became more difficulty for the MOH to evaluate potential risks, and supervise the market.

Dysfunctional Interaction at this Loop:

The interaction between MOH and hospital was abnormal. It played a critical role in the accident. According to the investigation report, the hospital X did not report its illegal activities to the MOH. Same, the MOH did not provided oversight on the hospitals. Both control and feedback were missing.

Flawed or Inadequate Decision and Control Actions:

The MOH provided an ineffective oversight on activities of its local bureau.

The MOH has thousands of branches in all over China. The head of MOH flow down regulations, standards and policies to its regional health branches. And those branches report work performance to the head of MOH. Nevertheless, the transparency of some branches was not so good. They didn't follow the orders from the head. In this accident, the local bureau mentioned they did not know the illegal surgeries. They only pointed out that's illegal after accident happened.

But the head of MOH usually have to trust reports from these branches, it's difficult for the head of MOH to oversee so many branches' activities. The MOH could only know they were not following regulations, unless accident happened and was reported. For example, once a provincial health bureau received extra money from a hospital, and approved some requests without evaluation as required, the head of MOH could not know if none reported this bribe.

The MOH did not provide effective regulation system and oversight on hospital.

As discussion previously, it's MOH's responsibility to oversee the hospital. The MOH had power to shut down hospital if the hospital violated regulations. However, the regulation system might not be effective in this accident. Illegal artificial heart was used; illegal foreign doctor was involved in surgery; few patients died after surgery. The regulations did not let the hospital stop their illegal surgeries.

People were part of the system. Because of historical reason, there were few people that have professional medical background worked for the MOH. Especially in some regional health branches, the gap between professionals and freshmen was big. As a result, the staffs could not take responsibilities to find unsafe hospital, illegal professionals and unsafe products.

Reason for Flawed Control Action and Dysfunctional Interaction

Incorrect Metal Model:

As a controller, the MOH assumed the regulations were good enough to prevent potential losses; assumed supervision system can find all illegal hospitals; thought the hospital could take its responsibilities; assume the patients could protect themselves.

Coordination among Multiple Controllers:

In this accident, the MOH was the controller for the hospital, and the SFDA was responsible for the artificial heart. They should work together to monitor the usage of medical device in hospital. But in this event, there was no coordination between them.

Up until now, the directly controllers and control loops has been analyzed. Fully understanding the behavior at any level of the socio-technical control structure requires analysis of higher level of the control structure.

The Higher Levels of Control:

5.6.5 The State Council and the MOH Loop

State Council

General Information

The State Council's full name is **State Council of the People's Republic of China** (simplified Chinese: 国务院;), which is largely synonymous with the Central People's Government after 1954, is the highest executive organization of State power, as well as the highest organization of State administration. It is chaired by the Premier and includes the heads of each governmental department and agency. The premier and other members of the State Council is nominated by the president, reviewed by the NPC, and appointed and removed by the president [5].

In the politics of the People's Republic of China, the State Council directly oversees the various subordinate People's Governments in the provinces, and in practice maintains an interlocking membership with the top levels of the Communist Party of China creating a fused center of power. The State Council is responsible for carrying out the principles and policies of the Communist Party of China as well as the regulations and laws adopted by the NPC. Under the current Constitution, the State Council exercises the power of administrative legislation, the power to submit

proposals, the power of economic and budget management, and other powers granted by the NPC and its Standing Committee.

Role and Responsibilities:

Provide regulation and guidelines for medical device

It's the State Council's responsibility to provide regulations for medical device to protect people's health and safety. This regulation should give clear definition about administration, manufacturing, operation, and post-marketing. The State Council should also provide legislative guidelines for subordinate departments, so that those departments can publish provision for medical devices. At the same time, it is also expected to provide legislative oversight on the effectiveness of the subordinate departments, in particularly the MOH.

Ensure the MOH has enough funds

Furthermore, the State Council is expected to ensure that the MOH has enough funding to operate independently. There were more than 13,600 medical device companies and 100,000 healthcare providers in China, the MOH have to request a lot of resource to operate and ensure the public's health and safety. And it is expected to provide enough budgets for the MOH and MOHRSS. The MOH needs to allocate healthcare budget to over 13,850 public hospitals, 80,500 urban and rural health centers, and 3,585 Centers of Disease Control (CDCs) in China. Similarly, the MOHRSS needs a lot of budget to cover 13.7 billion Chinese basic medical insurance.

Oversee the medical device system

In addition, it is State Council's responsibility to oversee the effectiveness of regulations and activities of subordinate departments. It has the power to revise the inadequate medical device regulations, elect and annul the management of governmental departments, if they were not qualified to take responsibilities.

Context in Which Decisions Were Made

The State Council has part legislative power to define administrative regulations. It's State Council's responsibility to ensure that regulation could be effective. However, because of historical and special reasons, people who were in charge of regulations might not have medical device background, so they might miss some key rules. As a

result, the first version of regulation only included 6 chapters and 48 articles, was established within 7 days by the State Council. Some of its definitions and rules could not provide clear description for readers. For example, some Provincial Government and the SFDA met a lot of problems when followed this regulation. For instance, there was no clear definition about counterfeit and inferior medical device, and how to punish them.

Resource pressure was a common issue that many governmental departments were facing. The large population in China required a large amount of healthcare resource. Currently, over 100,000 public healthcare providers need to get funds from the MOH. However, China is a developing country, and government has to put funds to national defense, infrastructure, public affairs, education, agriculture and healthcare areas. The State Council had to balance the investment between them. Additionally, the MOH need to recruit enough professionals with medical device background to build regulation system for medical device and monitor the effectiveness of it.

Dysfunctional Interaction at this Loop:

The interaction in this loop was normal.

Flawed or Inadequate Decision and Control Actions:

The State Council provided a regulation that might be not good enough to prevent accident.

As mentioned earlier, the current regulation was only 6 chapters that missing some situation. The increasing adverse events have verified that the current regulation was unable to prevent many losses associated with medical devices. However, the regulation is still not revised now. The MOH and SFDA had to publish a lot of provisions and notifications to prevent similar problems after adverse events happened. It might be useful to prevent future accidents, but those provisions didn't have a high level legislative position. The State Council should revise the current regulation and make it better.

The State Council underfunded the MOH

Furthermore, the State Council underfunded the MOH. But it's not State Council's fault to underfund the MOH. The main reason was that China is a developing country,

and funds are insufficient, that is why State Council has to balance the funds between defense, agriculture, education, healthcare and others. However, this situation is improving. The State Council began to invest more money and resource to healthcare area from year 2006.

Reason for Flawed Control Action and Dysfunctional Interaction:

Incorrect Mental Models:

The State Council thought each component in the system can take responsibilities and assumed funds were enough for the MOH.

The safety control structure is a system for general medical device product. In this thesis, the artificial heart event related controller has been analyzed. The further study can be done to analyze other medical device products.

5.7 Summary of Causes of the Accident Based on CAST

Based on the above analysis, the main causes of this accident are summarized as following:

The hospital

The patient did not insist on their rights.

The hospital provided unnecessary diagnosis and treatment plan.

The hospital took surgery that they did not get permission.

The hospital allowed illegal foreign doctors to provide medical service.

The hospital did not stop illegal activities.

The hospital did not report accident but hided it.

The medical device company

The medical device company exported product to a Chinese hospital without permission. The goal was to do illegal clinical test in China. The clinical test was complex and expensive in the Europe.

The SFDA

The SFDA did not remove unsafe product from market.

The SFDA didn't have enough professionals and could not provide effective regulations and supervisions to constraint illegal activities.

The MOH

The MOH provided an ineffective oversight on activities of its local bureau.

The MOH did not provide effective regulation system and oversight on hospital.

The State Council

The State Council provided a regulation that might be not good enough to prevent accident.

The State Council underfunded the MOH

The investigation pointed out the hospital and unregistered artificial heart was root cause of several deaths. But in the discussion above, more causes are found. The context and the mental models when taking these actions help to explain the reasons for these unsafe actions. The CAST provides deep insight to the flawed behavior of the controllers of this system that contributed to the losses in the ***artificial heart*** event.

6 Recommendations

The goal of an accident analysis should not be just to address symptoms, to assign blame, or to determine which group or groups are more responsible than others. How to change or re-engineer the entire safety control structure in the most cost-effective and practical way to prevent similar accident processes in the future is more important than blaming certain persons [20].

A list of recommendations is resulted from the CAST analysis. The recommendations are given for each controller.

The State Council

1) The State Council should provide national economic and social development plan and national budget plan, which includes health development plan and budget.

2) The State Council should provide efficacious regulation and supervision system to make the governmental departments, healthcare providers and medical device companies cannot violate.
    a. The State Council should provide new regulations to system for administration and supervision of medical device.
    b. The State Council should provide clear official definition and explanation for every regulation.
    c. The State Council should give legislative power to the MOH.
    d. The State Council should provide health guidelines to the MOH.
    e. The State Council should reject and annul inadequate regulations, provisions, and decisions.
    f. The State Council should provide up-to-date regulations to fit for fast developing healthcare industry.
    g. The State Council should create oversight system to oversee the effectiveness of regulation system and activities of the MOH, the SFDA and other departments.
    h. The State Council should create transparency rules so that the MOH, the SFDA, hospitals, and medical device companies to disclose their works to prevent corruptions.
    i. The State Council should provide enough funds and resource to build this system.
    j. The State Council should create rules so that regulations system and oversight system can work well.
3) The State Council should provide funds to the MOH.
    a. Funds for operation.
    b. Funds for healthcare providers.

Ministry of Health

4) Same as the State Council, the MOH should be involved into regulation and supervision system building.
    a. The MOH should provide detailed regulations into regulation system of medical device.
    b. The MOH should provide standards for hospitals, healthcare service, and qualifications of healthcare professionals.

c. The MOH should create efficacious regulations for administration and supervision of hospitals, and healthcare professionals.
d. The MOH should oversee the effectiveness of regulations, policies, and standards.
e. The MOH should create rules for internal management, for example, the transparency between local health bureau and MOH; the qualification of staffs and positions.
f. The MOH should oversee the activities of regional branches, the SFDA, and the healthcare providers in China.
g. The MOH should recruit qualified staffs and provide adequate training.
h. The MOH should build adverse event reporting system and database for public and provide easy access to check the qualification of hospitals and medical devices.

5) The MOH should allocate healthcare resources and funds to national wide hospitals according healthcare development plan.
   a. The MOH should ensure the needs from hospitals are true and reasonable.
   b. The MOH should ensure the funds are allocated as planning.
   c. The MOH should ensure the funds can get to the hospital.
   d. The MOH should oversee the spending of the funds.

The SFDA

6) The SFDA should be involved into regulation and supervision system building.
   a. The SFDA should provide detailed and uniform provisions, policies, and standards for detailed medical device products.
   b. The SFDA should provide effective and uniform supervision to inspect unsafe products before they enter market.
   c. The SFDA should define the uniform qualifications for its positions and hire qualified staffs to fill those positions.
   d. The SFDA should ensure the regulations and supervision is implemented as required.
   e. The SFDA should build adverse event channel to incent consumers to report unsafe products.
   f. The SFDA should ensure the transparency between its branches and medical device companies.

7) The SFDA should build effective and uniform product review and evaluation processes and standards for medical device registration.
8) The SFDA should ensure its branches have funds to operate.

Medical Device Company

9) The medical device company should follow China regulations, provisions, and standards.
    a. The medical device company should take enough internal testing and clinical tries before products are delivered to market.
    b. The medical device company should provide accurate and correct product information to the SFDA and consumers.
    c. The medical device company should take actions once an adverse event is reported.
    d. The medical device company should expose negative events that may injure consumers.
    e. The medical device company should refuse inadequate request from consumers.

The Hospitals

10) The hospitals should follow regulations and standards.
    a. The hospitals should only provide healthcare service they register.
    b. The hospitals should hire qualified staffs as required.
    c. The hospitals should buy medical device that has registration at the SFDA.
    d. The hospitals should use medical device as product instruction.
    e. The hospitals should provide effectiveness and side effect information to the patients.
    f. The hospitals should refuse inadequate request from patients.
    g. The hospitals should report adverse event to the medical device company and the MOH.

The recommendations are generated from the application of the CAST analysis. These may be good and useful to generate the new system safety requirements and constraints to improve safety. But how to implement the recommendations in China is a new challenge. As mentioned above many times, China is a big country and has a

large number of population, the relationship between stakeholders is very complex. The safety control structure can only describe a general connection between them. Some deep connections can be studied.

Compare with the former SFDA officer's conclusion. These are systemic issues, beyond punishing a doctor or blaming on a product. If we do not change the systemic issues, then similar problem will occur again and again. People's lives are still at risk.

7 Conclusion

With the development of Chinese economics, Chinese consumers begin to concern healthcare safety. The traditional risk analysis tools such as FMEA, FTA and ETA can provide a linear analysis to the technical system. But they are not applicable to complex sociotechnical system when the hazards are resulted from policy and social behaviors.

Unlike the popular safety tools, CAST provided more findings in the analysis of a healthcare accident from a social-technical level. Along with the fast development of the medical device, creating a completely safe healthcare system is impossible but that does not mean that it is not important to learn from past mistakes and work to improve the existing system.

This thesis focused on understanding the healthcare system and how the artificial heart accident happened by first studying the system as a whole and outlining the control structure that dictates the way safety is enforced. The second step was to identify the main clusters of power (hospitals, patients, medical device company, the SFDA, the MOH, the State Council...) and map the way they interact with each other.

Third, the relating controller of the system and its control loops were studied individually to look for ways in which they violated their safety responsibilities and to try to understand what motivated the controllers by recreating the environment in which they operated at the time.

Based on the CAST analysis, some recommendations that target the controllers were given. However even those recommendations should not be expected to be enough to protect the public in the long term. The healthcare system will keep evolving and new medical devices for diagnosis and treatments will be innovated and bring new and unknown risks. It is important to keep in mind that the system is constantly evolving and that it is necessary to monitor each of the controllers adapts to new changes and how they affect the system as a whole. It is only by proactively monitoring the changes that future health safety problems can be prevented. Further studies can focus on more complex medical device like CT scanner and MRI.

REFERENCES

[1] State Council (2000, April 1, 2000). Regulations for the Supervision and Administration of Medical Devices. Retrieved from http://www.sfda.gov.cn/WS01/CL0784/16570.html

[2] SFDA (2004, Aug. 9, 2004). Measures for the Administration of Medical Device Registration. Retrieved from http://www.sfda.gov.cn/WS01/CL0053/25844.html.

[3] SFDA (2004, January 17, 2004). Provisions for Clinical Trials of Medical Devices. Retrieved from http://www.sfda.gov.cn/WS01/CL0053/24475.html.

[4] SFDA (2012). SFDA's organization, mission, and responsibilities. Retrieved from http://www.sfda.gov.cn.

[5] National People's Congress (2012). NPC responsibilities. Retrieved from http://www.npc.gov.cn/.

[6] Ministry of Health (2012). MOH's responsibilities. Retrieved from http://www.moh.gov.cn/.

[7] Couturier, M.M.J. (2010). A case study of Vioxxx using STAMP. Engineering System Division. Cambridge, MA, MIT.

[8] Elena Luk'yanenko (2009, 16 April 2009). Medical Equipment in China. PTL Group. Retrieved from http://www.ptl-group.com/index.php/blogs/business-china/blogger/listings/elena?start=10.

[9] Liu Y, Rao K (2006). Providing Health Insurance in Rural China: From Research to Policy. J Health Polit Policy Law 2006, 31:71-92.

[10] SFDA (2010). SFDA annual report. Retrieved from http://www.sfda.gov.cn.

[11] Robin E. McDermott, Raymond J. Mikulak, Michael R. Beauregard (2008). The Basics of FMEA. CRC Press.

[12] Center for Chemical Process Safety/AIChE. (2008). Guidelines for Hazard Evaluation Procedures.

[13] Long, Allen (2010, 16 January 2010). Beauty & the Beast – Use and Abuse of Fault Tree as a Tool, Retrieved from http://www.fault-tree.net.

[14] Clifton A. Ericson, II. (2005). Hazard Analysis Techniques for System Safety, John Wiley & Sons, Inc.

[15] Dr. W. Vesley, Dr. Joanne Dugan, J. Fragole, J. Minarik II, and J. Railsback (2002). Fault Tree Handbook with Aerospace Applications. NASA Office of Safety and Mission Assurance, Washington DC 20546, August 2002.

[16] Mi Huayang, Wang Lei (2007) 医疗器械监督管理中亟待解决的问题, Anhui Medical and Pharmaceutical Journal, 2007 Jul; 11(7).

[17] Yue Wei (2009). Medical Device Registration System Comparison between China and USA, Chinese Journal of medical Instrument, P52, 1671-7104 (2009) 01-051-08.

[18] Shi jingjie, Bai Xiumei, Yue Suxue, Wang Juan, Meng Fanling and Zhu Jun (2009). Analysis of the Primary Medical Device Regulatory Status and Countermeasures, China Pharmaceutical Affairs, 1002-7777 (2009) 11-1053-03.

[19] Leveson, Nancy. G (1995). Safeware: system safety and computers. Reading, Mass.:Addison-Wesley.

[20] Leveson, Nancy G. (2012). Engineering a safer world: System thinking applied to safety (Book draft). Retrieved from http://sunnyday.mit.edu/safer---world/index.html, to be published by MIT Press in 2012.