A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices

by

Vincent H. Balgos

B.S. Chemical Engineering
B.S. Chemistry
University of Missouri – Columbia, 2002

SUBMITTED TO THE SYSTEM DESIGN AND MANAGEMENT PROGRAM IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT

AT THE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

FEBRUARY 2012

@ 2012 Vincent H. Balgos. All rights reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created

Signature of Author: ____

Vincent H. Balgos
System Design and Management
January 20, 2012

Certified by: ____

Dr. Qi D. Van Eikema Hommes
Thesis Supervisor
Research Scientist, Engineering Systems Division

Accepted by: ____

Patrick Hale
Director, System Design and Management Program

THIS PAGE INTENTIONALLY LEFT BLANK

A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices

by

Vincent H. Balgos

Submitted to the System Design and Management Program on January 20, 2012 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management

ABSTRACT

In today's environment, medical technology is rapidly advancing to deliver tremendous value to physicians, nurses, and medical staff in order to support them to ultimately serve a common goal: provide safe and effective medical care for patients. However, these complex medical systems are contributing to the increasing number of healthcare accidents each year. These accidents present unnecessary risk and injury to the very population these systems are designed to help. Thus the current safety engineering techniques that are widely practiced by the healthcare industry during medical system development are inadequate in preventing these tragic accidents. Therefore, there is a need for a new approach to design safety into medical systems.

This thesis demonstrated that a holistic approach to safety design using the Systems Theoretic Accident Model and Process (STAMP) and Causal Analysis based on STAMP (CAST) was more effective than the traditional, linear chain-of-events model of Failure Mode Effects and Criticality Analysis (FMECA). The CAST technique was applied to a medical case accident involving a complex diagnostic analyzer system. The results of the CAST analysis were then compared to the original FMECA hazards. By treating safety as a control problem, the CAST analysis was capable of identifying an array of hazards beyond what was detected by the current regulatory approved technique. From these hazards, new safety design requirements and recommendations were generated for the case system that could have prevented the case accident. These safety design requirements can also be utilized in new medical diagnostic system development efforts to prevent future medical accidents, and protect the patient from unnecessary harm.

Thesis Advisor: Qi Van Eikema Hommes
Title: Research Scientist of Engineering Systems Division

DEDICATION

This thesis is dedicated to the countless lives and families that have been affected by medical accidents every year.

ACKNOWLEDGEMENTS

"If I have seen further it is only by standing on the shoulders of giants."

-Isaac Newton

Firstly, I would like to thank my thesis advisor, Professor Qi Hommes, for unwavering guidance and wisdom throughout this academic endeavor. This thesis could not have been completed as comprehensively and to the high scholarly degree without her support. I am also grateful for the personal growth and insight gained far beyond the scope of this thesis, and the opportunity to explore new realms of systems thinking.

Furthermore, I would not be able to begin, continue, and complete my graduate school experience without the love and support of my family and friends. My mom, dad, brother, and sister-in-law were influential in achieving this personal goal. Thank you for the steadfast support over the years.

Finally, I would like to thank the SDM community, particularly Pat Hale for his invaluable guidance into the world of MIT and System Design and Management program, and to my friends and colleagues within the program and university. Your contributions made the experience invaluable, and thank you for being great traveling partners on this tremendous journey.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

510(k)	PreMarket Notification
CAST	Causal Analysis based on STAMP
CE	Conformité Européenne
CFR	U.S. Code of Federal Regulations
CLIA 88	Clinical Laboratory Improvement Amendments of 1988
EC	Electrochemistry
ESC	EC Sensor Controller
FC	Fluidic Controller
FDA	U.S. Food and Drug Administration Agency
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FTA	Fault Tree Analysis
GMC	General Master Controller
GMP	Good Manufacturing Practices
GUI	Graphical User Interface
HACCP	Hazard Analysis and Critical Control Points
HAZOP	Hazard and Operability Study
H#	Hazard number #
HFE	Human Factors Engineering
ISO	International Organization for Standards
IVD	In-Vitro Diagnostics
MAUDE	FDA's Manufacturing and User Facility Device Experience
OIVD	Office of In-Vitro Diagnostics Device Evaluation and Safety
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PMA	PreMarket Approval
POC	Point of Care
SC#	Safety Constraint number #
SOC	System and Oximetry Controller
SE	Substantial Equivalence
SR#	Safety Requirement number #
STAMP	Systems Theoretic Accident Model and Process
UE	Usability Engineering

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1. Introduction and Motivation

"Learning without thought is labor lost. Thought without learning is perilous"

-Confucius

The United States is home to some of the world's most innovative breakthroughs such as the Human Genome Project [1], Hepatitis C treatment [2], and the management of several orphan diseases [3]. The U.S. spends the most for its healthcare, amounting to about $2.5 ***trillion*** a year, which is roughly 17% of the U.S. Gross Domestic Product (GDP) [4]. However, there is drastic contradiction between innovative technology and high spending, and the overall safety and effectiveness of the care provided to patients.   A 2000 report from the World Health Organization (WHO) ranked the U.S. as 37th in the world in overall quality of healthcare system performance [5]. Most of developed European, Asian, Middle Eastern, and South American countries are ranked higher for overall safety and effectiveness. The U.S. is listed just above Cuba, whose GDP is 0.08% of that of the U.S. The contrast is stark and illustrates that it is possible to attain safe and effective health care that does not directly result from high spending and technology.

Further studies have shown that almost 30% of the medical services provided in the U.S. are ineffective, and there are approximately 98,000 American deaths a year due to medical errors in hospitals [6]. The number of deaths due to preventable adverse events exceeds motor vehicle accidents, breast cancer, and AIDS related deaths [6]. "Crossing the Quality Chasm", a 2001 report by the Institute of Medicine (IOM), indicates safety as one of the six main elements for improving the healthcare system [4]. Safety is a rich, multi-dimensional issue in the healthcare industry. This thesis project chose to focus on safety assurance during the design phase of the medical system product development process.

The motivation to improve the overall the system safety emerged from one of the author's professional experiential accounts of the dramatic consequences of the lack of system safety. On an international visit to a large hospital for an accident investigation, several medical diagnostics systems failed prematurely promoting potentially hazardous conditions for the patients. One specific situation was prior to the start of an invasive operation of a patient, the primary diagnostic system failed and became unavailable for diagnostic usage.   A secondary diagnostic system was available since general hospital protocol requires a backup unit for emergency situations, and the patient underwent the scheduled operation. However, during the operation, the secondary system failed for the same issue and the medical staff was left to complete the procedure without any accurate diagnostics of the patient's blood status. This provided a hazardous environment where accidents could occur, and the patient safety was at risk. Fortunately, the surgery outcome was successful and the patient was unharmed. However, the medical staff on duty discussed the hazardous incident with the author and colleague with great fervor and emotion.

While the discussion was entirely in the native foreign language, the transcended disappointment and frustration of the system was not lost in translation and that experienced resounded deeply with the author.

Since that incident, there has been a professional and academic motivation for the author to improve the overall safety of medical systems, and strive to fulfill the personal goal of: "Change the world. One Patient at a Time." Adapting a new systems thinking approach in safety design in complex systems developed by Professor Nancy Leveson of MIT [7], achieving that goal maybe one step closer. Motivated by these existing challenges, this thesis has chosen to focus on how to improve the safety of medical diagnostic systems during the product development phase.

Safety is a critical parameter in complex systems that affect the end value delivery to the user. Regulatory bodies such as the U.S. Food and Drug Administration (FDA), and the Conformité Européenne (CE) establish medical device and diagnostic regulations for safety. These include several medical industry standard safety and risk management techniques such as Failure Mode Effects and Criticality Analysis (FMECA) that uses a reductionist chain-of-events analysis approach during the design phase to address potential safety issues [8]. While these techniques are sufficient in meeting current safety guidelines, they predominantly focus on a linear, reliability approach for addressing safety, and are inadequate for today's non-linear complex systems. This absence of a systems thinking approach may have contributed to the recent rise in medical device recalls [9].

This thesis applies a systems thinking methodology called Causal Analysis based on STAMP (CAST) to an accident on a complex medical product [7]. Systems Theoretic Accident Model and Process (STAMP) is a new systems methodology that approaches safety as a control problem, rather than a reliability issue. A gap analysis is performed on the CAST results with the standard FMECA findings from the original case system manufacturer to investigate common findings, variations, and discrepancies.

The research question that this thesis intends to answer is:

"Is the Systems Theoretic Accident Model and Process (STAMP) approach more effective in designing safety into the medical diagnostic systems than the current industry standard practices?"

The rest of this thesis is organized in the following fashion. In Chapter 2, the literature review discusses the history, and current safety regulations for medical diagnostic systems development. Furthermore, several acceptable industry standard practices for risk management are presented and their strengths and weaknesses of each method are discussed. In addition, the new systems safety methodologies of STAMP and CAST are presented. Chapter 3 discusses the case study company, the case study system, and an accident that is used for the case study. In Chapter 4, the CAST analysis is performed on the case accident. Chapter 5 discusses the potential hazards uncovered from the CAST application, and the new system safety design requirements and recommendations. A gap analysis between CAST and the FMECA methodologies is also performed in Chapter 5. In Chapter 6, a conclusion will offer a summary of the thesis, and provide an answer to the focused research question while offering future suggestions, insights, and departing statements.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2. Literature Review

"We can't solve problems by using the same kind of thinking we used when we created them."

-Albert Einstein

Product development is a complex and complicated process requiring substantial resources including money, time, and human activity. From the designer's 3D CAD model, to the factory floor ramping up production to the final product installation at a field site, a holistic view of the product lifecycle must be taken in order to balance the needs of various stakeholders. As products become more complex and develop into systems, emergent properties arise such as the end value-delivery function. But there are several others such as performance, quality, and safety that also need to be considered during the initial development phase.

In regards to developing new medical technology systems, satisfying the numerous complex federal regulations is an additional enormous effort that is needed for product market introduction. The United States Food and Drug Administration (FDA) is the agency in charge for medical technology safety and effectiveness regulations that protect the public health. A brief overview is provided next on the origin of the agency and the emergence of safety regulations.

2.1 The History of U.S. Drug and Medical Device Regulation and the Birth of the Food and Drug Administration (FDA)

The United States Food and Drug Administration (FDA) is the oldest consumer protection agency formed in 1906 [10]. It is a direct descendant and evolution of earlier regulatory agencies such as Division of Chemistry (1862), Bureau of Chemistry (1901), and Food, Drug and Insecticide Administration (1927). The birth of FDA guardianship and the origins of drug and medical product regulation began, unfortunately, with a massive medical accident.

In the 19th century, individual states regulated food and drug qualities for the public welfare, with significant variation from state to state. With the assistance of Harvey Washington Wiley (Chief Chemist of Division of Chemistry), who helped unified groups to prohibit adulteration and misbranding of food and drugs, the 1906 Pure Food and Drugs Act (aka Wiley Act) was approved by President Roosevelt [10]. In this Act, the Division of Chemistry then to become the Bureau of Chemistry was charged to prohibit interstate transport of unlawful food and drugs without regulation of product labeling, especially on drugs. For foods, law prohibited addition of ingredients that substitute for food, conceal damage, pose health hazard, or constitute a filthy or decomposed substance.

While a first national step in food and drug safety, the 1906 Act was limited in power but was replaced by a more comprehensive law in the 1938 Food, Drug, and Cosmetic Act. This Act was prompted by a mass-poisoning incident. In 1937, a Tennessee drug company marketed Elixir Sulfanilamide, a sweet raspberry tasting liquid form of the popular antibiotic sulfanilamide [11]. The company used diethelyene glycol, to transform the normal powder drug into liquid form to meet market needs. Little did the company know that diethelyene glycol is a deadly poison, and normally used in antifreeze. At that time, there were no required toxicities testing, scientific literature review, or animal experiments, and selling potentially toxic drugs was technically legal. In this case, product safety conflicted with another constraint- the desire for quick market placement. The company quickly sent shipments of 240 gallons of the toxic elixir across the U.S. [11].

After a few unusual deaths, investigations linked the deaths to Elixir Sulfanilamide. Once its toxic effect was discovered, the FDA (evolved from the Bureau of Chemistry), through gallant efforts, recovered most of it. However, 6 gallons that could not be retrieved due to human consumption, lethally poisoned over 100 people, mainly children.

After the incident, Dr. Samual Evans Massengill, the firm's owner, famously said [11]:

> *"My chemists and I deeply regret the fatal results, but there was no error in the manufacture of the product. We have been supplying a legitimate professional demand and not once could have foreseen the unlooked-for results. I do not feel that there was any responsibility on our part."*
>
> *- S.Massengill, Owner*

This brought massive public outcry, and Massengill eventually pleaded guilty to adulteration and misbranding and paid the largest fine at the time for violation of the 1906 Act [10].

The FDA was able to react on the massive disaster due to a misbranding technicality. At the time, marketing a product as an Elixir implied an alcoholic solution. Since Elixir Sulfanilamide contained no alcohol, the FDA was able to impose legal authority and recover the lethal substance from the general public. This labeling technicality allowed the FDA to prevent countless more poisonings. The FDA Commissioner at the time Walter Campbell, indicated that this incident shows how essential it is to public welfare that the distribution of highly potent drugs should be controlled by an adequate Federal Food and Drug law

> *"These unfortunate occurrences may be expected to continue because new and relatively untried drug preparations are being manufactured almost daily at the whim of the individual manufacturer, and the damage to public health cannot accurately be estimated. The only remedy for such a situation is the enactment by Congress of an adequate and comprehensive national Food and*

> *Drugs Act which will require that all medicines placed upon the market shall be safe to use under the directions for use. ...”*
>
> *-W. Campbell, FDA Commissioner*

Quickly after this accident, the 1938 Food, Drug, and Cosmetic Act was approved and gave US authority to oversee the safety of food, drugs and cosmetics [10]. Further incidents gave the FDA power to access and verify practices of company production processes and quality control records.

In another massive medical accident, the sedative Thalidomide produced thousands of birth defects in Europe in the 1960’s [10]. While this drug was not approved in the U.S, the incident led the initiative for the FDA to regulate efficacy as well as safety for U.S. bound drugs. In addition, further amendments transferred power from the Federal Trade Commission to the FDA for the regulation of prescription drug advertising and established good manufacturing practices guidelines for the drug industry. In addition, the 1962 Drug Amendment had laws preventing medical quackery, or fraudulent medical practices.

In the early 1970’s, there was another massive healthcare tragedy involving a medical device. The Dalkon Shield, an intrauterine device, caused uterus bacterial infection, which induced pelvic inflammatory disease in U.S. women [10][12]. This caused thousands of pregnancy complications like ectopic pregnancies, infertility, birth deformations, and septic spontaneous abortions, let alone the severe lingering mental injury [13]. The manufacturers of the Dalkon Shield knew there were safety concerns of the product and questionable clinical data, but like the Elixir Sulfanilamide case, the desire for market introduction conflicted and overrode any safe product development constraint [14]. The subsequent 1976 Medical Device Amendment required testing and FDA approval of medical devices and established three classes of medical devices, each requiring a different regulation level for safety and effectiveness [10]. Like previous medical regulation, it was catalyzed by massive accidents effecting thousands of patients.

In summary, the history of the FDA and the evolution of its regulation of medical products have followed a consistent pattern. The agency and its control expanded in reaction to catastrophic accidents that have lead to unnecessary injuries and deaths. These accidents were the results of the innovative scientific and technological solutions and the needs for business profitability. Today, the modern medical technology continues to evolve. Therefore, the FDA regulation for safety will require continued improvements.

2.2 Current FDA Conditions

In today's regulatory structure, the FDA is under the Health and Human Services Department that is responsible for establishing safety regulations to protect the U.S. population. According to the official FDA website [15], the agency's responsibilities include:

- Protecting the public health by assuring that foods are safe, wholesome, sanitary, and properly labeled; human and veterinary drugs, and vaccines and other biological products and medical devices intended for human use are safe and effective
- Protecting the public from electronic product radiation
- Assuring cosmetics and dietary supplements are safe and properly labeled
- Regulating tobacco products
- Advancing the public health by helping to speed product innovations
- Helping the public get the accurate science-based information they need to use medicines, devices, and foods to improve their health.

Therefore, the FDA is the regulatory body that establishes the safety requirements for medical device and diagnostic systems. According to the FDA website, over $1 trillion worth of products are annually regulated [16]. This broad and deep list of regulation responsibilities requires significant human resource, political and legal support, investment of time and coordination to enforce. As seen in the organizational chart in Figure 1, the agency 's responsibilities cover areas including food, tobacco, and medical products [17]. The current FDA Commissioner is Margaret Hamburg, MD as of May 2009.

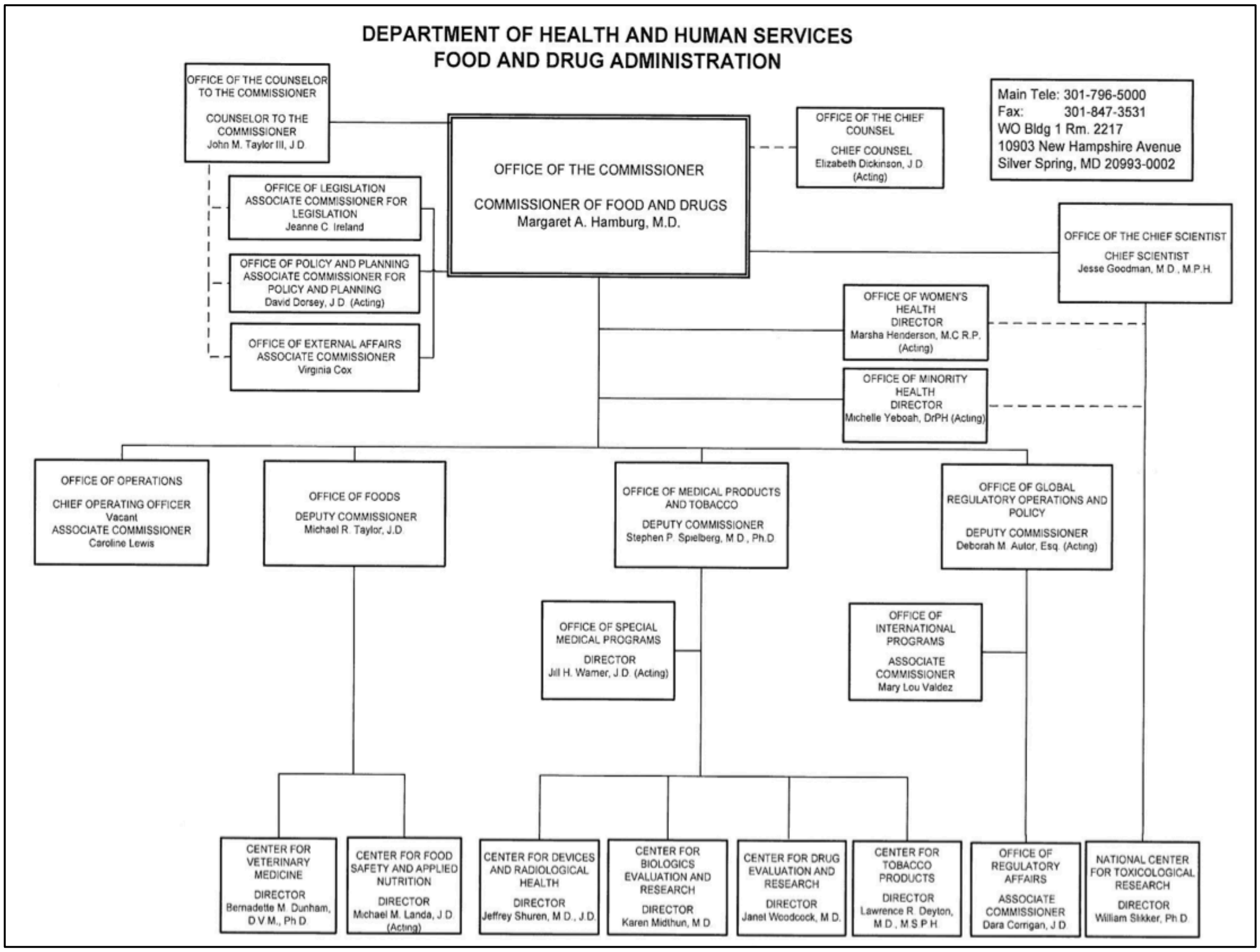
DEPARTMENT OF HEALTH AND HUMAN SERVICES
FOOD AND DRUG ADMINISTRATION
OFFICE OF THE COUNSELOR TO THE COMMISSIONER
COUNSELOR TO THE COMMISSIONER
John M. Taylor III, J.D
OFFICE OF THE COMMISSIONER
COMMISSIONER OF FOOD AND DRUGS
Margaret A. Hamburg, M.D.
OFFICE OF THE CHIEF COUNSEL
CHIEF COUNSEL
Elizabeth Dickinson, J.D (Acting)
Main Tele: 301-796-5000
Fax: 301-847-3531
WO Bldg 1 Rm. 2217
10903 New Hampshire Avenue
Silver Spring, MD 20993-0002
OFFICE OF LEGISLATION
ASSOCIATE COMMISSIONER FOR LEGISLATION
Jeanne C. Ireland
OFFICE OF POLICY AND PLANNING
ASSOCIATE COMMISSIONER FOR POLICY AND PLANNING
David Dorsey, J.D. (Acting)
OFFICE OF EXTERNAL AFFAIRS
ASSOCIATE COMMISSIONER
Virginia Cox
OFFICE OF THE CHIEF SCIENTIST
CHIEF SCIENTIST
Jesse Goodman, M.D., M.P.H.
OFFICE OF WOMEN'S HEALTH
DIRECTOR
Marsha Henderson, M.C R.P. (Acting)
OFFICE OF MINORITY HEALTH
DIRECTOR
Michelle Yeboah, DrPH (Acting)
OFFICE OF OPERATIONS
CHIEF OPERATING OFFICER
Vacant
ASSOCIATE COMMISSIONER
Caroline Lewis
OFFICE OF FOODS
DEPUTY COMMISSIONER
Michael R. Taylor, J.D.
OFFICE OF MEDICAL PRODUCTS AND TOBACCO
DEPUTY COMMISSIONER
Stephen P. Spielberg, M.D., Ph.D
OFFICE OF GLOBAL REGULATORY OPERATIONS AND POLICY
DEPUTY COMMISSIONER
Deborah M. Autor, Esq. (Acting)
OFFICE OF SPECIAL MEDICAL PROGRAMS
DIRECTOR
Jill H. Warner, J.D. (Acting)
OFFICE OF INTERNATIONAL PROGRAMS
ASSOCIATE COMMISSIONER
Mary Lou Valdez
CENTER FOR VETERINARY MEDICINE
DIRECTOR
Bernadette M. Dunham, D.V.M., Ph.D
CENTER FOR FOOD SAFETY AND APPLIED NUTRITION
DIRECTOR
Michael M. Landa, J.D. (Acting)
CENTER FOR DEVICES AND RADIOLOGICAL HEALTH
DIRECTOR
Jeffrey Shuren, M.D., J.D.
CENTER FOR BIOLOGICS EVALUATION AND RESEARCH
DIRECTOR
Karen Midthun, M.D.
CENTER FOR DRUG EVALUATION AND RESEARCH
DIRECTOR
Janet Woodcock, M.D.
CENTER FOR TOBACCO PRODUCTS
DIRECTOR
Lawrence R. Deyton, M.D., M.S.P.H.
OFFICE OF REGULATORY AFFAIRS
ASSOCIATE COMMISSIONER
Dara Corrigan, J.D.
NATIONAL CENTER FOR TOXICOLOGICAL RESEARCH
DIRECTOR
William Slikker, Ph.D.

Figure 1. U.S. Food and Drug Administration Organization Chart [17]

As seen in Figure 1, under the overarching drug area, responsible areas expand to include four large areas of tobacco, biologics, drug, and medical and radiological devices. For the purpose of this thesis, the regulatory body for medical *diagnostics* is established under the Center for Devices and Radiological Health which is comprised of seven smaller offices (as seen in Figure 2). The Office of In-Vitro Diagnostic Device Evaluation and Safety (OIVD) is the regulatory area that regulates the safety and performance of the case study system in this thesis. The current Director is Jeffery E Shuren, M.D., J.D as of January 2010.

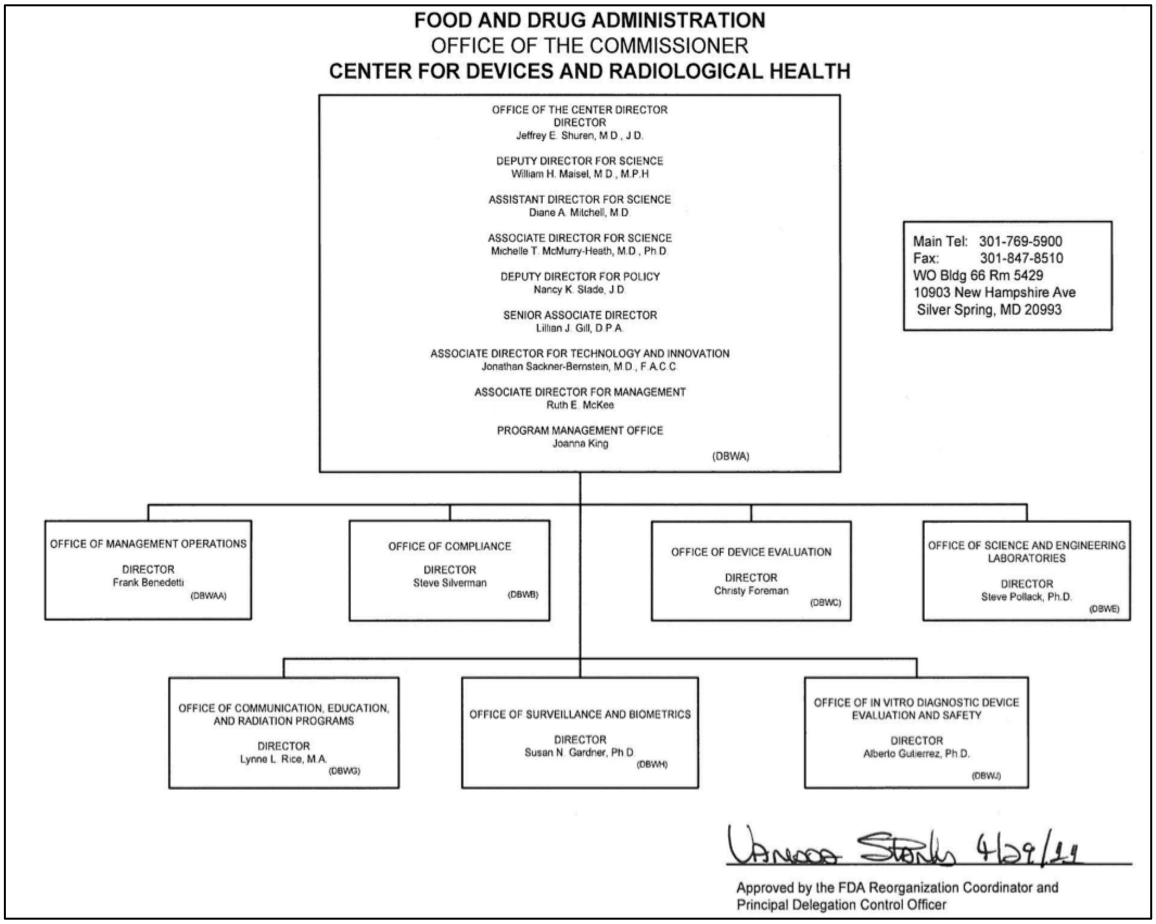
FOOD AND DRUG ADMINISTRATION
OFFICE OF THE COMMISSIONER
CENTER FOR DEVICES AND RADIOLOGICAL HEALTH
OFFICE OF THE CENTER DIRECTOR
DIRECTOR
Jeffrey E. Shuren, M.D., J.D.
DEPUTY DIRECTOR FOR SCIENCE
William H. Maisel, M.D., M.P.H
ASSISTANT DIRECTOR FOR SCIENCE
Diane A. Mitchell, M.D.
ASSOCIATE DIRECTOR FOR SCIENCE
Michelle T. McMurry-Heath, M.D., Ph.D.
DEPUTY DIRECTOR FOR POLICY
Nancy K. Slade, J.D.
SENIOR ASSOCIATE DIRECTOR
Lillian J. Gill, D.P.A.
ASSOCIATE DIRECTOR FOR TECHNOLOGY AND INNOVATION
Jonathan Sackner-Bernstein, M.D., F.A.C.C.
ASSOCIATE DIRECTOR FOR MANAGEMENT
Ruth E. McKee
PROGRAM MANAGEMENT OFFICE
Joanna King
(DBWA)
Main Tel: 301-769-5900
Fax: 301-847-8510
WO Bldg 66 Rm 5429
10903 New Hampshire Ave
Silver Spring, MD 20993
OFFICE OF MANAGEMENT OPERATIONS
DIRECTOR
Frank Benedetti
(DBWAA)
OFFICE OF COMPLIANCE
DIRECTOR
Steve Silverman
(DBWB)
OFFICE OF DEVICE EVALUATION
DIRECTOR
Christy Foreman
(DBWC)
OFFICE OF SCIENCE AND ENGINEERING LABORATORIES
DIRECTOR
Steve Pollack, Ph.D.
(DBWE)
OFFICE OF COMMUNICATION, EDUCATION, AND RADIATION PROGRAMS
DIRECTOR
Lynne L. Rice, M.A.
(DBWG)
OFFICE OF SURVEILLANCE AND BIOMETRICS
DIRECTOR
Susan N. Gardner, Ph.D
(DBWH)
OFFICE OF IN VITRO DIAGNOSTIC DEVICE EVALUATION AND SAFETY
DIRECTOR
Alberto Gutierrez, Ph.D.
(DBWJ)
Vanessa Starks 4/29/11
Approved by the FDA Reorganization Coordinator and
Principal Delegation Control Officer

Figure 2. FDA Center for Devices and Radiological Health Organization Chart [17]

2.3 U.S. FDA Regulations

The U.S. Code of Federal Regulations (CFR) is the codification of general and permanent rules published annually by the departments and agencies of the U.S. Federal Government [18]. These administrative laws, categorized amongst 50 titles, cover the broad areas of Federal Regulation and provide safety statutes for various agencies. The titles are further categorized into Chapters, SubChapters, and Parts. This is illustrated in Figure 3 and Table 1 below. Regulation is supervised and monitored by administrative governmental bodies such as the Federal Aviation Administration, Federal Transit Authority, and Food and Drug Administration.

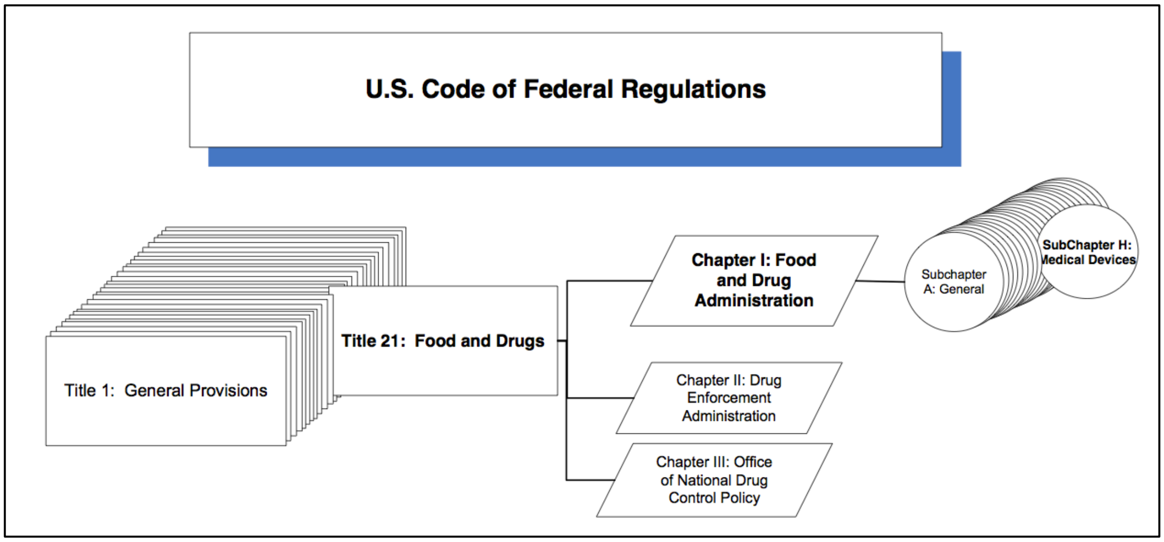
U.S. Code of Federal Regulations
Title 1: General Provisions
Title 21: Food and Drugs
Chapter I: Food and Drug Administration
Chapter II: Drug Enforcement Administration
Chapter III: Office of National Drug Control Policy
Subchapter A: General
SubChapter H: Medical Devices

Figure 3. U.S. Code of Federal Regulations

As Figure 3 displays, Medical Devices regulations are categorized beneath several layers of the overarching CFR. Under SubChapter H: Medical Devices, the laws can be further decomposed into 33 distinct parts, ranging from Labeling requirements (Part 801) to Quality System Regulation (Part 820). This information is tabulated in Table 1 below. Every individual part can be further decomposed to subparts, but was omitted for brevity. For this thesis, referencing regulations will follow the general nomenclature of #Title CFR Part (subpart). For example for Quality System Regulation subpart "g", it will be written as 21 CFR 820(g).

Table 1. Parts for SubChapter H: Medical Devices

SubChapter H: Medical Devices Parts	
Part 800 - GENERAL	Part 866 - IMMUNOLOGY AND MICROBIOLOGY DEVICES
Part 801 - LABELING	Part 868 - ANESTHESIOLOGY DEVICES
Part 803 - MEDICAL DEVICE REPORTING	Part 870 - CARDIOVASCULAR DEVICES
Part 806 - MEDICAL DEVICES; REPORTS OF CORRECTIONS AND REMOVALS	Part 872 - DENTAL DEVICES
Part 807 - ESTABLISHMENT REGISTRATION AND DEVICE LISTING FOR MANUFACTURERS AND INITIAL IMPORTERS OF DEVICES	Part 874 - EAR, NOSE, AND THROAT DEVICES
Part 808 - EXEMPTIONS FROM FEDERAL PREEMPTION OF STATE AND LOCAL MEDICAL DEVICE REQUIREMENTS	Part 876 - GASTROENTEROLOGY-UROLOGY DEVICES
Part 809 - IN VITRO DIAGNOSTIC PRODUCTS FOR HUMAN USE	Part 878 - GENERAL AND PLASTIC SURGERY DEVICES
Part 810 - MEDICAL DEVICE RECALL AUTHORITY	Part 880 - GENERAL HOSPITAL AND PERSONAL USE DEVICES
Part 812 - INVESTIGATIONAL DEVICE EXEMPTIONS	Part 882 - NEUROLOGICAL DEVICES
Part 814 - PREMARKET APPROVAL OF MEDICAL DEVICES	Part 884 - OBSTETRICAL AND GYNECOLOGICAL DEVICES
Part 820 - QUALITY SYSTEM REGULATION	Part 886 - OPHTHALMIC DEVICES
Part 821 - MEDICAL DEVICE TRACKING REQUIREMENTS	Part 888 - ORTHOPEDIC DEVICES
Part 822 - POSTMARKET SURVEILLANCE	Part 890 - PHYSICAL MEDICINE DEVICES
Part 860 - MEDICAL DEVICE CLASSIFICATION PROCEDURES	Part 892 - RADIOLOGY DEVICES
Part 861 - PROCEDURES FOR PERFORMANCE STANDARDS DEVELOPMENT	Part 895 - BANNED DEVICES

Part 862 - CLINICAL CHEMISTRY AND CLINICAL TOXICOLOGY DEVICES	Part 898 - PERFORMANCE STANDARD FOR ELECTRODE LEAD WIRES AND PATIENT CABLES
Part 864 - HEMATOLOGY AND PATHOLOGY DEVICES	

As Table 1 displays there are various categories of medical device laws. While all regulation statues are critical, the highlighted parts relates to new medical product approval process (Part 807), and the safety designed into the system (Part 820). These parts play a significant role in this thesis and will be further discussed.

In order to establish the appropriate FDA regulatory requirements for U.S. market release, new In-Vitro Diagnostic (IVD) product is classified into one of three categories as mandated in the 1976 Medical Device Amendments Act under 21 CFR 860 [19]. The classification is dependent of the product's complexity and risks to the patient. The higher the risk, the more stringent regulation is enforced on the device. These categories are:

- Class I - General Controls:
    - The least regulated medical products that have minimal potential harm for the user/patient. These products are normally simpler in design, and may follow General Controls. General Controls are basic regulations to ensure safety and effectiveness, which include Good Manufacturing Practices (GMP), labeling regulations, and enterprise registration, with some exemptions [19].
    - Examples include bandages, gloves, and surgical instruments

- Class II - General and Special Controls:
    - Medical products that pose more safety risks that are not entirely covered in General Controls require additional Special Controls. Special Controls are existing methods to assure safety and effectiveness of a new device and include mandatory performance requirements, special labeling, and post-market surveillance. A premarket notification 510(k) is normally required under 21 CFR 807, but there are some exemptions [19].
    - Examples are powered wheelchairs, infusion pump, and infectious disease genotyping assays.

- Class III General Controls and Premarket Approval:
    - This class requires the highest and most stringent safety regulations due to the high risk to patient safety, and requires premarket notification 510(k) and/or premarket approval (PMA) under 21 CFR 814. PMA includes a scientific review since there is normally insufficient predicate or equivalent data to assure safety and effectiveness [19].
    - Examples are invasive pacemaker, breast implants, and automated external defibrillators.

There are many exemptions and overlaps of the various classes and is dependent on the inherent risk of medical device. Figure 4 illustrates some of these interactions, and offers an overall view of the FDA medical device classification and their pertinent regulations.

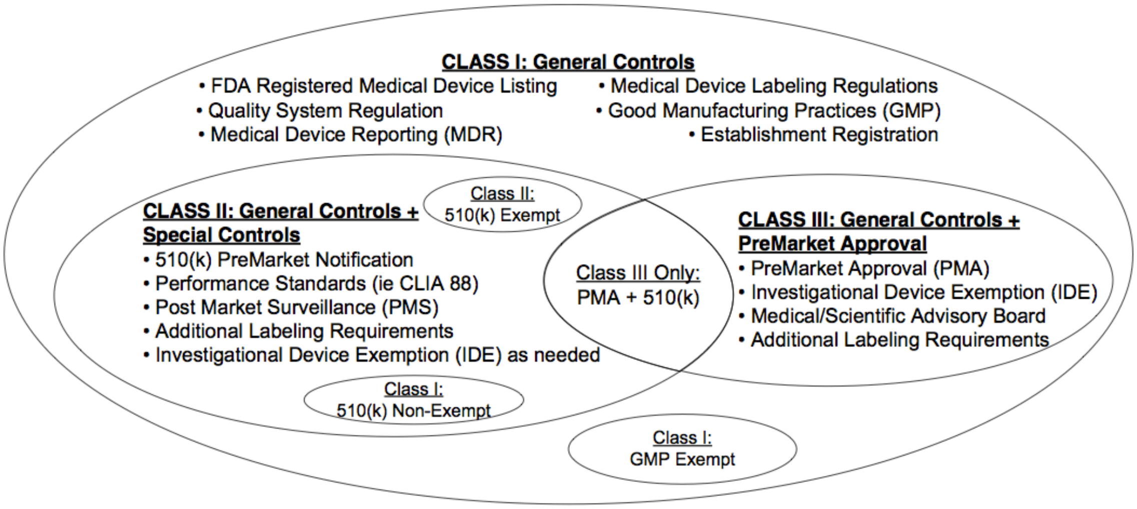
CLASS I: General Controls
• FDA Registered Medical Device Listing
• Quality System Regulation
• Medical Device Reporting (MDR)
• Medical Device Labeling Regulations
• Good Manufacturing Practices (GMP)
• Establishment Registration
CLASS II: General Controls + Special Controls
• 510(k) PreMarket Notification
• Performance Standards (ie CLIA 88)
• Post Market Surveillance (PMS)
• Additional Labeling Requirements
• Investigational Device Exemption (IDE) as needed
Class II: 510(k) Exempt
Class III Only: PMA + 510(k)
CLASS III: General Controls + PreMarket Approval
• PreMarket Approval (PMA)
• Investigational Device Exemption (IDE)
• Medical/Scientific Advisory Board
• Additional Labeling Requirements
Class I: 510(k) Non-Exempt
Class I: GMP Exempt

Figure 4. FDA Medical Device Classification

**Common cases are shown. Some exceptions may apply*

As Figure 4 shows, Class I General Controls include basic regulation guidelines such as registry listing, GMP and labeling requirements. Class II and Class III devices must also abide by these regulations, with some modification. For Class II, the majority of new products must submit a 510(k) PreMarket Notification (21 CFR 807) to the FDA that adds additional rigorous testing criteria, in supplement to the general controls [19]. Performance against acceptable standards is conducted. There are some Class II devices that are exempt from 510(k) regulation. Some Class I devices may also be required to comply with the 510(k) regulation. Class III is for medical products that sustain or support human life, have significant importance in preventing human harm or present potential unreasonable risk of injury or does not have a substantial approved equivalent [19]. This is the most stringent regulation and requires a PMA. This includes extensive clinical trials, scientific review boards, and Investigational Device Exemption [20]. In addition, there are class III devices that will need to also comply with the 510(k) regulation.

The system studied in this thesis is a Class II medical diagnostic device. Compliance with 510(k) is required for U.S. market approval. More details of the device certification process will be discussed in Chapter 3.

Since the Class II devices also need to meet performance standards, the 1988 Clinical Laboratory Improvement Amendment (CLIA 88) establishes the analytical acceptable quality standards for clinical laboratory testing [21]. These standards include the accuracy, reliability, and timeliness of results, and sets acceptable targets for total allowable error for specific assays and tests. As a part of 510(k) submission, new diagnostic product must show equivalent or better analytical results when compared to CLIA 88 targets to be considered for U.S. market approval. This provides a level of quality analytical performance and safety regulation since these are the end value deliverable to the user. Some other quality clinical laboratory standards include German RiliBAK, but for the case study system, the CLIA 88 quality standards were used for analytical verification in supplement to the 510(k) submission.

In addition to the quality analytical performance, FDA stipulates that for Class II or III medical products, manufacturers must establish and maintain procedures to control the design of the medical product [22]. As part of the Design Control, a risk management plan of the medical diagnostic system must be conducted to comply with regulatory guidelines. This is specified in Section G: Design Validation 820.30(g) (see Table 1) of the FDA Design Control Guide for Medical Device Manufacturing [23], and it states that:

"Design validation shall include software and risk analysis, where appropriate".
21 CFR 820.30(g) Revised as of April 1, 2011.

This statement indicates that a risk analysis of the system is required, but leaves it up to the manufacturers to determine how the risk analysis should be performed. Based on the author's professional experience in medical system development, the current practice is to comply with the Conformité Européenne (CE) Mark process of risk analysis that is established in the International Organization for Standards (ISO) 14917. CE Mark is the European regulation equivalent of the U.S. FDA, and all new medical products must approved for safety requirements for European market introduction [24]. Therefore with the understanding that if a new medical product is approved for CE Marking, the FDA will generally accept this risk analysis for a 510(k) submission. In a recent June 22, 2011 FDA Draft on Applying Human Factors (HFE) and Usability Engineering (UE) to Optimize Medical Device Design, risk management processes consistent with ISO 14971 is essential for a successful HFE/UE analysis [25], and supports the author's professional experience and current industry practice.

For CE Mark approval, recommended risk analysis techniques are documented under ISO 14971: *Medical devices – Application of risk management to medical devices* [8]. The document states that the intent of the risk analysis is to analyze every step for the chain of events, which may require several risk analysis techniques to be used concurrently as some have complementary features. These techniques are:

- Preliminary Hazard Analysis (PHA)
- Fault Tree Analysis (FTA)
- Failure Mode and Effects Analysis (FMEA)

- Failure Mode, Effects, and Criticality Analysis (FMECA)
- Hazard and Operability Study (HAZOP)
- Hazard Analysis and Critical Control Points (HACCP)

2.4 Current Industry Risk Management Analysis Techniques

A brief overview and critique of each risk technique is presented next.

2.4.1 Preliminary Hazard Analysis (PHA)

The preliminary hazard analysis (PHA) is an inductive, or top down, hazard analysis method that evaluates a design at an early stage. PHA is performed to identify hazards, associated causal factors, effects, level of risk, and potential mitigations measures based upon preliminary design information [26]. The only basic information needed for PHA is the system design that includes the functional flow diagram, reliability block diagram, critical components list, and the preliminary hazard list (PHL). The basic process is to review this information of system hardware, software, functions, energy source, and material and chemical compatibility and identify new hazards with a linear, chain of events approach.

A worksheet can be constructed to document PHA process and results, and below is an example used in military systems [26].

Preliminary Hazard Analysis					**System:** **Subsystem/Function:**			**Analyst:** **Date:**	
No.	**Hazard**	**Causes**	**Effects**	**Mode**	**IMRI***	**Recommended Action**	**FMRI****	**Comments**	**Status**

**Initial Mishap Risk Index (IMRI): Initial accident risk significance with probability and severity estimates before mitigation is implemented.*
**Final Mishap Risk Index (FMRI) = Final accident risk significance with probability and severity estimates after mitigation is implemented.*

Figure 5. Preliminary Hazard Analysis Worksheet Example

As Figure 5 illustrates, for every hazard, a cause, effect, and recommended mitigation is generated. The IMRI (defined above) qualitatively measures the initial significance of the risk with a severity and probability determined. The FMRI (defined above) then re-measures the risk after the recommended mitigation is implemented. The process is continued until all items in the PHL have been covered.

The strength of PHA is its ability for early design stage analysis, and identify previously unrecognized hazards early in the system development. The development team can then establish guidelines, specifications, and criteria to be followed in system requirements and/ or design based off these initial findings [27]. The intent is to find hazards early so can alter design with minimal resource and cost impact.

One clear disadvantage is with the minimal design information, only a limited hazard analysis can be produced. Without lower level data (such as sub-system components, functionality), a comprehensive hazard analysis cannot be achieved. Another observation is that this linear methodology applies a reductionist view where a single failure is used to cause the accident. The worksheet is even structured to promote the chain of events model. As stated by Leveson, accidents can be caused by multiple failures, and therefore PHA may not identify all hazards [27]. Additionally, the worksheet above does not provide guidance on how to find the causes. It is merely a documentation step that records the results of the exercise of the system analyst.

2.4.2 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is an analytical and graphical methodology that allows an accident or undesired state of the system to be deductively decomposed to all credible ways that the undesired event can occur [28]. This International Electrotechnical Commission (IEC) standard 61025 is a reliability analysis that can include the context of the system environment, operation, human interaction, and many other factors. There are two applications of FTA with the most common being a proactive FTA used during system development [26]. The alternative is after an accident occurs, a reactive FTA may be performed to illustrate the leading corresponding events. While the both approaches use the same methodology, only the reactive version can use the evidence and data from the accident itself.

As Leveson summarizes, there are four basics components of FTA: 1) System Definition, 2) Fault Tree construction, 3) Qualitative Analysis and 4) Quantitative Analysis [27]. Defining the system and the related events, conditions, and their interconnections is first needed to establish key nodes of the fault tree. Once this has been completed, a fault tree can be generated using the system definition. The resulting fault tree then depicts the logical interactions that lead to the accident, which is established at the beginning top node. A basic example of an FTA was generated in Figure 6 using the standards from the National Regulatory Commission Fault Tree Handbook with the undesired event connected to the subsequent interactions.

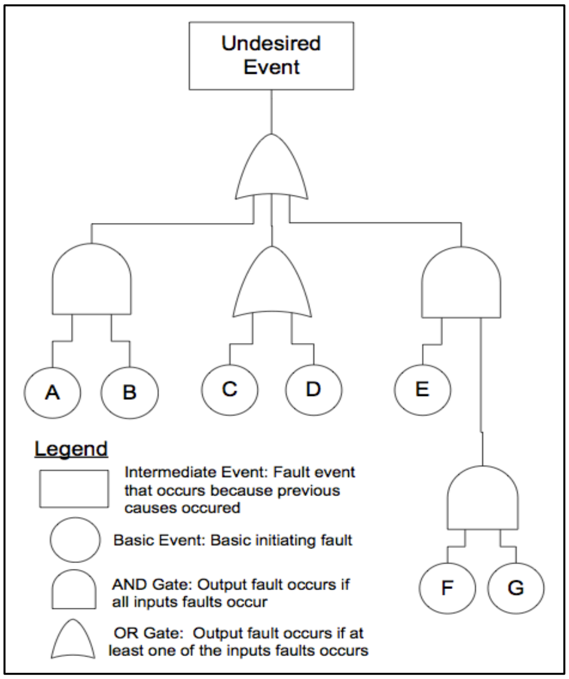
Undesired Event
A
B
C
D
E
F
G
Legend
Intermediate Event: Fault event that occurs because previous causes occured
Basic Event: Basic initiating fault
AND Gate: Output fault occurs if all inputs faults occur
OR Gate: Output fault occurs if at least one of the inputs faults occurs

Figure 6. Fault Tree Analysis Example

As seen in the Figure 6 example, there are several conditions that were needed to result in an undesired event. Starting at the top of the fault tree, there are three conditions that could lead to this undesired, and due to the OR gate, only one was necessary to cause the accident. With the leftmost AND gate, both Event A and B had to occur in order to potential cause the fault. In the center OR Gate, either Event C or D needed to happen to produce the undesired result. For the rightmost AND gate, all three events (E, F, G) had to present itself to catalyze the higher system failure. This is a basic example, and there are more complex and conditional elements to the FTA available in literature for a more detailed and accurate analysis.

After completion of the fault tree, both a qualitative and quantitative analysis can be performed. The qualitative analysis requires defining "cut set" which is a set of events that caused the final undesirable event [26]. This is similar to what was previously discussed above. The goal is to determine the minimal cut sets that are the critical path to accident [27]. Once this has completed, the probabilities for each cut sets can be aggregately calculate to determine the final probability of the fault event, assuming all preceding events are statistically independent [28].

Thus, some advantages that FTA provides are that all events leading up to an accident, and their interrelationships are illustrated in a graphical model for qualitative cause and effect assessment. Using event probabilities, a quantitative analysis of the probability of the accident can then be determined and used to predict reliability failure rates such as mean time between failures (MBTF). This in turn can be used for risk and design assessment, root cause analysis, and a decision making tool.

One disadvantage associated to FTA quantitative analysis is that it takes a reliability engineering approach. The calculation of top-level event failure probability is based on the lower leaf nodes' random failure probability. Complex systems fail due to both component random failures and undesirable component interactions. Merely focusing on component reliability does not ensure safety [7], and accidents can still occur. The Mars Polar Lander system that failed its landing on the Mars surface in 1999 is a clear example that highly reliable systems are unsafe [27]. Furthermore, it may be difficult to analyze the timing model with FTA, as specific sequence of events can lead to hazards. Therefore, the structure of FTA is limited in analyzing and identifying all hazards.

2.4.3 Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA), another IEC standard (60812), is an inductive or bottom up risk analysis approach that can be performed on a detailed system design. The intent is to identify all individual potential failure modes of the system, subsystems, assemblies, or components and its subsequent effect on system performance and reliability [29]. Functional-type FMEA can also be used to abstractly analyze failure modes based on the functional adverse states [26]. This can be applied to non-hardware areas, such as software and analyzed at the software functional level.

The FMEA process is normally performed during the development phase when there is sufficient information of the design so findings can influence its development for product and process improvements in the early stages [30]. Similar to FTA, FMEA has the capability to include reliability rates for every failure mode to provide a quantitative analysis [26]. Failure Mode Effects and Criticality Analysis (FMECA) is a richer alternative to FMEA, by also incorporating a critical analysis (CA) by defining the criticality and detectability of the failure mode [26].

Some basic definitions necessary for clarification:

- Failure: Unintended operation, function or behavior of a specific item [26]
- Failure Mode: The manner the failure occurs [29]
- Failure Effect: Consequences a failure mode has on system functionality, operation, or status [26]
- Risk Priority Number (RPN): Risk ranking index for reliability and is mathematically defined as [26]:

$$RPN = Severity \times Probability\ of\ Occurrence \times Detection\ Ranking$$

The overall methodology to FMEA is to analyze every component (hardware, software) or functional single failure mode, and determine the effect on the higher system's reliability [26]. This is where detailed information like design specifications, software code, and schematics play a major factor since analysts can identify, and evaluate in depth all conceivable single points of failure. The output of this analysis is identified failure modes, system effects, and quantitative forecast on hazards and risks forecasts. The effort to produce a comprehensive FMEA may be substantial based on the product's complexity.

Similar to PHA, a worksheet is generally utilized to provide the analysis structure, consistency and documentation [26]. A basic FMEA example by Ericson is shown below in Figure 7 below.

Failure Mode and Effects Analysis						
Component	Failure Mode	Failure Rate	Causal Factors Effect	Immediate Effect	System Effect	RPN

Figure 7. Failure Mode and Effects Analysis Example Worksheet

As Figure 7 shows, it captures the failure mode, its consequences (immediate and system effect), the frequency, and the calculated RPN value. The RPN is a quantitative analysis of the risk of the identified hazard in terms of severity and probability [26]. As mentioned earlier, there are adaptions to FMEA such as FMECA. From various literature research and supported by past professional experience, the usage of FMECA is industry standard practices in analyzing risks in new medical product developments. In Figure 8, an example of a system safety FMEA worksheet is provided below.

Failure Mode and Effects Analysis										
System:			**SubSystem:**				**State:**			
Item	**Failure Mode**	**Failure Rate**	**Causal Factors**	**Immediate Effect**	**System Effect**	**Detection Method**	**Current Controls**	**Hazard**	**Risk**	**Mitigation Action**

Figure 8. FMEA of Systems Safety Example Worksheet

While FMEA is useful in the design development phase (also known as dFMEA), it is also applicable in the manufacturing and assembling process and is referred to as Process FMEA or pFMEA [8]. pFMEA similarly analyzes the how the process methods affect the operation of the system as do the design [26]. From professional experiences, this is a common tool used in Six Sigma process, and generally occurs in the Analyze phase of the DMAIC (Define, Measure, Analyze, Improve, Control) approach.

A major observation is that FMEA only analyzes a single point of failure and not multiple failure combinations [27]. As mentioned earlier by Leveson, hazards can be the result of many failures and events other than failure mode. Furthermore, FMEA assumes systems fail due to component failure, but accidents can still occur while all components did not fail performing the designed intentions (i.e. Mars Polar Lander incident) [27]. Similarly to FTA technique, the reliability aspect of this methodology may be limited in discovering hazards in a system. As medical technology evolves and becomes more complex and integrated with other systems, the application of FMEA/FMECA may not identify some of the system interaction hazards.

2.4.4 Hazard and Operability Study (HAZOP)

Hazard and Operability Study (HAZOP) is a risk methodology that assumes accidents are caused by deviations from design or operating intentions [8]. This IEC 61882 method provides a structured technique for identifying and analyzing hazards and operation concerns of a system [27]. This analysis can be used at various levels from system to components, and from the abstracted conceptual design phase to the actual detailed design phase.

The methodology requires the selection of the expert HAZOP team leader and multidisciplinary team that uses key or guide words and compares it to a list of system parameters [26]. This can be illustrated as:

Guide Word + Parameter = Deviation

Parameters can be the design features or intents between various components such as temperature, vibration, or software data flow. Some Guide Words, provided by Leveson, are captured below along with an example using fluid flow as a parameter.

Table 2. HAZOP Guide Words

Guide Words	Meaning	Example
No, Not, None	Intended result does not happen.	No fluid flow.
More	Increase in design intent occurs.	Increase in fluid flow.
Less	Decrease in design intent occurs.	Decrease in fluid flow.
As Well As	An additional activity occurs with original design intent.	Fluid flow plus Pressure.
Part of	Only some of design intent is achieved.	Partial fluid flow.
Reverse	The opposite design intent occurs.	Reverse fluid flow.
Other than	Design intent not achieved, and subsequent results are different than expected.	Fluid flow in unexpected areas.

The team then brainstorms possible deviations from the design intent and subsequent hazards using this basic process. There are possible combinations of the Guide Word and Parameter that are meaningless, and should be discarded. For documentation, a constructed worksheet with the parameter, guideword, and identified hazard and risk is generally used, and an example is provided below from Ericson in Figure 9 below. These generated results can then be used to implement mitigation recommendations for each identified hazard.

HAZOP Analysis										
No	Item	Function	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Mitigation	Comments

Figure 9. Hazard and Operability Analysis (HAZOP) Worksheet Example

Similar to FMEA, an observation made was that this risk analysis performs only single failure events. Multiple failure events are not analyzed, and this maybe a constraint for HAZOP utilization in complex systems. This linear causal chain of events is limited in identifying all hazards in the system.

2.4.5 Hazard Analysis and Critical Control Points (HACCP)

Hazard Analysis and Critical Control Points (HACCP) is the universally accepted safety assurance method used primarily in the food industry [43]. It is a systematic approach to the identification, assessment, and control of hazards during the process and preparation of food. Food safety is addressed through the analysis and control of biological, chemical, and physical hazards from raw material production, procurement and handling, to manufacturing, distribution and consumption of the finished product [31]. This preventative method is designed to integrate food safety control in to the development process, and has shown more effective than end product testing.

The HACCP methodology follows seven basic principles [31]

- Principle 1: Conduct a hazard analysis
    - Identify significant hazards that are likely to cause injury or illness.
    - Generation and analysis of entire process flow diagram including raw materials, process steps, storage, distribution, and final preparation by the consumer are considered

- Principle 2: Determine critical control points (CCP)
    - Identify control points that can be applied to prevent or mitigate the safety hazard at any step along the process flow diagram.
    - Example is cooking time and temperature of raw meat

- Principle 3: Establish critical limits
    - To distinguish between safe and unsafe conditions, critical limits need to be established throughout the process to control biological, chemical, and

or physical parameters in order to prevent, or mitigate potential safety hazards.

- Principle 4: Establish monitoring procedures
    - To verify effectiveness of critical control points, monitor procedures are established throughout the process for each CCP.
    - Monitoring examples could be real time observations, and or quick measurements.

- Principle 5: Establish corrective actions
    - For any deviation from the critical limits, a corrective action needs to be developed and implemented.
    - Documentation of all deviations and subsequent corrective action is required.

- Principle 6: Establish verification procedures
    - Evaluating the effectiveness of the overall HACCP is required to verify its scientific soundness, and determine hazards are effectively controlled.
    - Performed by an independent authority or third party.

- Principle 7: Establish record-keeping and documentation procedures
    - Documentation of the HACCP plan, critical limits, corrective actions, and verification procedures is required.
    - This can be captured in a specialized worksheet as depicted in Figure 10 below

Hazard Analysis and Critical Control Points						
CCP	Hazards	Critical Limits	Monitoring	Corrective Actions	Verification	Records

Figure 10. HACCP Worksheet Example

As mentioned earlier, HACCP is predominantly used in the food industry to prevent contaminated food to reach the population for consumption. During the thesis literature review, there are a few examples of applications of HACCP outside of the food industry, but those found are applied to the pharmaceutical industries in the preparation of drug preparation [32][33]. According to a 2003 WHO report, HACCP was mentioned as a complementary, but not a replacement technique for Good Manufacturing Practices (GMP). It is uncertain at this time, its applicability and effectiveness in medical diagnostic system safety due HACCP limitation to biological, chemical, and physical analysis constraints. Another observation is that this method is focused on the processes of the system only. This may be an additional constraint of the technique that limits the effectiveness of identifying hazards in the design stage.

2.4.6 Current Industry Risk Management and Analysis Summary

In summary, there are several techniques available for medical diagnostic risk analysis as indicated by ISO 14971. While somewhat effective and government approved, the FMEA, and HAZOP methods take a reductionist perspective on safety. This approach assumes system accident is the result of a linear chain of events from a singular independent random component failure. These methods cannot identify hazards when the system safety is compromised without any component failure.

Furthermore, FMEA and FTA assume that safety is a reliability issue, but reliability is focused on failures and failure rate reduction [27]. Increasing reliability does not necessarily increase safety. Safety is an emergent property of systems and is defined as an absence of accidents. While there are overlaps of safety and reliability, accidents can happen without any components ever failing. Conversely, components can fail without resulting in an accident [27].

Therefore, there is a need for a new approach to safety design in complex systems. Leveson developed a new approach based on System Theoretical Accident Model and Process (STAMP). The following section will describe this methodology in detail.

2.5 Systems Theoretic Accident Model and Process (STAMP)

The Systems Theoretic Accident Model and Process (STAMP) is a systems approach to safety. The STAMP model treats safety as a controls problem and views systems as dynamic rather than static entities [7]. It examines the hierarchical control structure, and monitors how the contextual control structures interact to maintain a safe state and/or the migration to unsafe states. Unlike the previous risk analysis techniques, STAMP is applicable to complex socio-technological systems. The technique has the capability of analyzing not only the technical risks, but risks associated to organizational, social, and environmental factors. This incorporates the "systems thinking" mindset in risk analysis.

As mentioned previously, safety is an emergent property of systems from the interactions of the system components. These components necessitate control, which can be achieved by applying constraints. Therefore safety is a control problem, not simply a reliability issue. The inadequate control or misapplication of safety related constraints in the design, development, and system can leads to accidents [7]. Accidents are defined as undesired and unintentional events that lead to human injury, loss, or death and can happen without failed components and/or by the interaction of other entities (human, external systems, environment). The STAMP approach uses these concepts to improve safety and prevent accidents.

STAMP contains three basic fundamentals [7]:

- Safety Constraints
- Safety Control Structure
- Process Model

Safety constraints are derived from the defined system hazards and provide boundaries to what is a "safe" and "unsafe" state for the system. The constraints are established from higher levels of the system, and if successfully designed and maintained, the system maintains a safe state. If these constraints are violated, or not properly enforced, the system then migrates to an unsafe state. Jens Rasmussen stated that systems tend to migrate to unsafe state in competitive and environmental pressure [7]. These constraints help maintain a safe state. From these constraints, requirements can be generated to prevent the system from entering an unsafe state.

The safety control structure is a hierarchical structure of control loops within the system [7]. The hierarchy provides control from the highest level down to lower level loops and components. Figure 11 below is a standard control loop defined by Leveson.

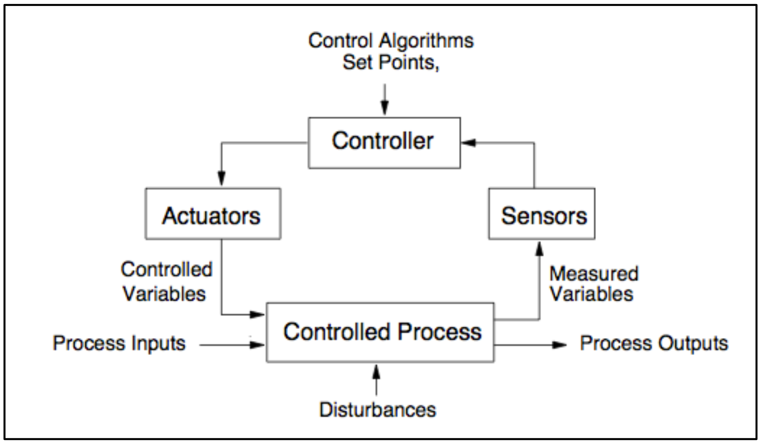

Figure 11. System Control Loop

The four elements (Controller, Actuators, Controlled Process, Sensors) provide the basic feedback loop. In this scheme, the Controller receives set points and has control algorithms. Once a command is received from an external entity (i.e. from the user, master controller), the controller runs the control algorithm, and may send a command signal to the actuator to change the state of the controlled process. The Actuator then sends controlled variables to the controlled process so the desired function is carried out. The verification of the system state is then monitored by the Sensors element via measured variables, and this information is sent back to the original controller. The controller then compares the system state with the desired states, and determines the next control action.

Process model is the logic in the controller on how the controlled process works. Whether it is the human user's mental images of the system, or the logical algorithm embedded in the microprocessor, the process models illustrate representations for system variables, its effect on the current state, and the ways to change the state. The process model provides a reference for the controller to figure out how to change the system state by using the system variables. Accidents may happen if the process model does not accurately represent the actual system.

To change a system's state, a control action has to be initiated. A controller can move the system to an unsafe state if it issues one of the following:

- Incorrect control commands
- Control actions not provided
- Incorrect timing of control action execution
- Control action prematurely terminates

With these above concepts, STAMP allows a clear understanding of accidents by understanding which safety constraints were broken. It also illustrates the causes for the inadequate control violations that could ultimately lead to improvements or recommendations for future safety analysis [7]. Misalignment of process models and the actual system process is also a contributor to accidents. With STAMP defined, an application of STAMP in accident analysis called Causal Analysis based on STAMP (CAST) is discussed next.

CAST is a retrospective accident analysis methodology that uses a system approach to investigate accidents by analyzing the control structure dynamics [7]. By evaluating the system constraints and its inadequacies, CAST can illustrate the hierarchical cascade effects that a constraint violation has on the system. Since the safety is an emergent property of the system, this analysis methodology can improve the understanding of the causes of accidents.

The CAST methodology follows these steps [7]:

1. Define the system and hazards in the accident.
2. Identify system safety constraints and associated safety requirements.
3. Define system control structure.
4. Estimate the events leading up to the accident.
5. Analyze loss at the physical system level.
6. By ascending and descending throughout the system control, determine the how and why each successive higher level allowed the inadequate control to continue to be erroneous.
7. Evaluate overall coordination and communication contributors to the accident.
8. Determine dynamic changes in the system and the safety control structure relating to the loss and any weakening of the safety over time.

9. Generate Recommendations.

CAST's unique approach to accident investigation deters blame, and instead investigates why accidents happen due to the existing control structure around the issue. Rather than fixing symptoms of the system, it focuses on the real cause(s) of the problem such as inadequate control. The CAST method will be applied to the case study.

In summary, STAMP and CAST methodology provides a system-thinking approach to safety and risk analysis. By treating safety as a control issue rather than a reliability problem, and its use of control structures, safety constraints, and process models, it has been able to identify many more hazards than standard industry practices previously described. Previous applications of CAST and STAMP to case accidents have further exemplified this claim in various industries including food [34], pharmaceuticals [35], and aviation [36].

2.6 Summary of the Hazard Analysis Methods

As this chapter discusses, there are several available methods that assess risk in complex processes. There are several similar attributes that are common such as a linear chain of events model in the FMEA and PHA techniques. In addition, there are some critical differences such as analyzing safety as a control problem rather than a reliability issue. An overall comparison chart of all the risk methodologies and their attributes was generated, see Table 3 below, to highlight the similarities, and differences.

Table 3. Risk Analysis Comparison Table

	Methodology Discussed in This Chapter					
Attributes	PHA	FTA	FMEA	HAZOP	HACCP	CAST
Single Failure Event	Yes	Yes	Yes	Yes		Yes
Multiple Failure Event (>1)		Yes				Yes
System Approach Model (Organization-Environment-Technical)						Yes
Able to address system interaction accidents						Yes
Applicable in Design Phase	Yes	Yes	Yes	Yes		Yes
Applicable in Operations Phase		Yes	Yes	Yes	Yes	Yes
Applied with limited system info	Yes					Yes
Ease of Application	Yes					Yes

As Table 3 displays, STAMP and the CAST approach offers several unique attributes to find complex hazards when compared to the standard practices. With this holistic approach, the practices can identify a multitude of hazards that normally elude the other single fault or linear chain of events approaches. With more hazards discovered, more mitigation can be designed and implemented into products to make it safer for the end user.

2.7 Conclusion

In conclusion, the previous sections have described the history of the U.S. medical device regulation and the FDA's role in maintaining the safety in numerous classes of medical technology. The numerous historical mass medical accidents have resulted in countless human injuries and death. With these tragedies, new and improved safety regulations for drug and medical devices were developed to prevent these accidents. However, with the growing complexity of the medical instruments and the increased use of software in today's environment, the current regulations are no longer sufficient in maintaining safety. The case study in this thesis will illustrate this point.

Chapter 3 provides an overview of the medical diagnostic system, and the case accident. Chapter 4 applies the CAST steps discussed in this section to the accident. The results will be analyzed in details, and compared to an industry standard risk technique, FMECA, to verify which approach is safer.

During writing of this thesis, it is noted that safety and effective FDA regulations are in flux. There is a growing concern on whether the current 510(k) approval process (as described above) achieves the goal of safety and effectiveness for application to the U.S. population. This is due to a recent rise in medical adverse events [37]. In the June 2011, the FDA made changes to the medical device approval process with a particular focus on updating safety regulations. However, in an IOM review of these changes, they recommended that it is not as safe and effective is it should be [38]. In a July 20, 2011 IOM letter to FDA Director Jeffrey Shuren, the IOM concluded

"…the 510(k) process generally is not intended to evaluate the safety and effectiveness of medical devices and, furthermore, cannot be transformed into a premarket evaluation of safety and effectiveness."

D.Challoner, MD
Chair, Committee on the Public-Health Effectiveness
of the FDA 510(k) Clearance Process

Therefore, uncertainty remains in the future of medical device and diagnostic regulation. But it is clear that a new methodology of evaluating safety and effectiveness in medical technology is needed. A systems thinking model and approach may fulfill that unmet need.

For the purpose of this thesis, the FDA regulations that will be referenced will be those documented above prior to the 2011 changes since the medical diagnostic case study was approved with the previous regulation statutes.

CHAPTER 3. Case Study Overview

"A man's errors are his portals of discovery"

-James Joyce

For confidentiality purposes, all specific information of the case study system, company, and accident will be generalized for this thesis discussion. A case study will be performed on a medical diagnostic system that analyzes a variety of constituents in patient blood samples. The medical diagnostic system will be referred to as the "case system" for this thesis discussion. The case system was developed by a medical diagnostic company, and will be referred to as the "case company" for this thesis discussion. The case study accident is an FDA recall notice for the case system on a specific sensor, which will be defined as "case sensor". The severity of the recall is global with the potential for human injury, and death.

3.1 Company Overview

The case company has developed several medical diagnostics systems for over the years with successful global market placement.

3.2 Case System Overview

The case system is a blood diagnostic analyzer developed by the case company that measures blood gas, electrolytes, and oximetry within human whole blood. The system is marketed in point-of-care (POC) market that allows "bedside" diagnosis in medical facilities. Its small footprint provides flexible mobility to allow usage in the many areas, including but not limited to areas in the emergency room, intensive care department, operating room and even in the central laboratory. The case system has been well received in the global market and continues to increase its foothold in the POC market including the U.S., Canada, and European Union. By providing valuable total solutions to a variety of clinical diagnostic needs, the case company gained the position as an innovative leader in critical care diagnosis.

The case system is a consumable cartridge-based system that allows a single whole blood sample to be analyzed and simultaneously produce various analytical results. This capability provides a competitive advantage over most current products. In addition, its data quality system provides the user a virtually maintenance free automatic quality control system.

The case system can be decomposed into two essential subsystems:

1. The instrument subsystem where the user interface, data processor, analytical modules, fluidic pumps, and network connectivity reside.

2. A consumable, disposable multi-use cartridge subsystem which handles the physical blood analyzing, chemical reagent deposition, and waste management functionalities.

The design intent of the case system was that the user would be able to install the instrument anywhere in the medical facility needing only a power outlet and a network connection. Once the instrument is setup, a multi-use cartridge is then installed, containing all necessary reagents, calibrations, and medical waste containment providing extended continual usage. After the cartridge life has expired, the user simply replaces the cartridge with a new one, and disposes the used cartridge as medical waste, which contains all the used blood samples, chemical reagents, and calibrations solutions.

The case system is operated in the following scenario. The users, usually a medical technician, nurse, or physician, may either transport the analyzer to the patient or bring the patient's blood sample to the analyzer. The freshly drawn blood is typically contained in a capillary tube, arterial syringe, or a closed tube container. The user selects the desired test assays, initiates the sampling procedure and introduces the sample to the analyzer. After sample aspiration by the analyzer, the user removes the sample container, and results are obtained within a desirable, user need driven timeframe. After the test results are provided, the case system automatically prepares itself for the next sample by performing necessary washes, calibrations, and checks. The average turn-around time for sample is therefore minimal, providing the user value of immediate diagnosis of the patient's health.

The case system also provides the user the unique ability to track test results, instrument status, and monitors other users. The case system software allows each system to connect with other systems via the hospital information system. This allows for test results to sync with the hospital network and provide remote viewing of patient results virtually anywhere in the hospital. This data networking enables the user with extended flexibility and mobility in their heavy work schedules.

As mentioned in the Chapter 2, the case system is a Class II product requiring a 510(k) under 21 CFR 807 for U.S. market release. A 510(k) requires demonstration of substantial equivalency (SE) to other legally released U.S. marketed device [39]. Substantial equivalency means that the new device is at least as safe and effective as predicates in the market. A device is SE to a predicate if one of the two following conditions apply [39]:

- New device has same intended use as predicate and has same technological characteristics as the predicate.
- New device has same intended use as predicate but has different technological characteristic. New device must then show that it does raise new concerns with safety and effectiveness and demonstrate that it is at least as safe and effective as the legally marketed device.

A device may not be marketed in the U.S. until the medical company receives a letter from the FDA declaring the device is substantially equivalent [39]. In addition to the General Controls of GMP, FDA registry, and labeling requirements, analytical performance was compared against acceptable quality standards for clinical laboratory tests (CLIA 88) in several internal and external studies. The case system was also tested for analytical equivalency against 510(k) approved predicate devices for every analyte parameter. Furthermore, a risk analysis was conducted on the case system as mandated by 21 CFR 820.30(g). A FMECA risk analysis was performed on the system, and covered a variety of areas. The resulting work documented potential hazards and associated mitigation efforts.

The 510(k) was submitted to the FDA and after review, the FDA found the case system submission complete and supports a SE decision. This indicates that the case system is at least as safe and effective as equivalent diagnostic analyzers released to the market, and is acceptable for U.S. market introduction [39]. The FDA sent the case company a letter stating substantial equivalence of the case system, and the case system was subsequently released to the U.S. market later that year.

3.3 Case Study Accident

The case company issued an FDA recall notice for a specific reportable electrolyte capability in the case system. In the recall filing documentation found on the FDA Medical & Radiation Emitting Device Recall website, the reported reason for the recall was that low electrolyte results on patient blood samples were being reported to medical staff. Secondary analysis of the same patient sample on an external reference instrument indicated the low electrolyte results was erroneous and was outside the CLIA 88 standard 493.931 for total allowable error.

The recall was initiated by numerous earlier medical adverse event reports, also documented by the FDA in the Manufacturing and User Facility Device Experience (MAUDE) database. The following is an example from an actual medical accident documented in MAUDE concerning the low electrolyte blood result, including the medical staff reactive actions, and the undesired consequence.

1. Medical staff uses the case system to diagnose the patient status.
2. Medical staff suspected an issue with the low blood electrolyte result.
3. Medical staff notified case company of suspected result.
4. Medical staff performed standard medical procedure on patient based off suspected low result.
5. Patient reacted adversely, and may result in seizure, cardiac arrhythmia, or death.
6. Subsequent testing of the same patient sample on an external reference system verified normal electrolyte levels.

As regulated by the FDA, the case company issued a recall for the electrolyte sensor on the case system and sent an "Urgent Field Safety Notification" letter to all users. In the letter it describes the problem and instructions on how to disable the electrolyte from all cartridges to eliminate the potential hazard.

The case company invested significant time, money, and enterprise resources to address the recall issue. The author had direct involvement in these activities. After intense investigation and activities, the recall issue has been addressed with mitigations emplaced. During the writing of this thesis, the FDA is reviewing the recall submission.

As stated earlier, the case system underwent FDA approved risk analysis using the FMECA methodology finding numerous hazards, and implementing the derived mitigations. However, as the recall illustrated, despite the engineers' best effort, some hazards were not identified by standard practices and that led to said medical accidents. Therefore the application of the linear, reductionist technique of the FMECA to a non-linear complex medical device system was inadequate. A new approach that employs systems-thinking model is needed.

Next, Chapter 4 discusses the application of a systems approach to this accident using the CAST technique. The intent is to investigate whether the STAMP model could have discovered the hazard that led to the recall. If the specific hazard were found using this technique, there could have been mitigations in the design phase to prevent this accident from ever occurring in the current case system. Furthermore, additional hazards may be identified using CAST that was not found with FMECA. Therefore, knowledge gained from this CAST analysis may be used for future medical diagnostic product development efforts. By applying a systems model to risk analysis, it may improve the overall safety of the medical diagnostic system.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 4. Case Accident CAST Analysis

"Harmony makes small things grow, lack of it makes great things decay."

-Sallust

As discussed previous chapters, a CAST analysis will be applied to the case system following the CAST steps outlined in Chapter 2

4.1 Context, Roles, and Responsibilities

The context of the case study system is that medical diagnostic system adds high value to the overall medical treatment of the patient in this environment. The patient is nominally in an unstable, critical condition, and the overseeing physician orders medical diagnostic monitoring to observe any changes in the patient's health status (i.e. specifically blood condition). It is also important to note that the time in receiving these patient results is critical, and could be a factor in the patient outcome. The case systems are continuously utilized throughout the patient's stay in the hospital or until doctor's orders changed. Therefore, the system must have high performance accuracy, uptime reliability, quick time to results and utmost, the safety in test results and alarms that have direct influence in the patient's health.

There are several stakeholders that interact directly or indirectly with the system and have significant roles and responsibilities. These are defined in Table 4 below.

Table 4. Case Study Stakeholder and Responsibilities

Stakeholder	Responsibilities
Patient	The passive indirect value stakeholder of the diagnostic system, and source of the system's input values.
Nurses/Lab technicians	The common direct primary users of the system, whose responsibility is to perform, report, and react to system output.
Physicians	Direct value stakeholders that adjust overarching patient medical decisions based off system output. Also infrequent users of the case system.
Case Company	The developers and manufacturers of the system.
Regulatory Bodies	Overseeing regulatory body (FDA, CE) that defines and enforce safety regulations for medical diagnostics systems.

As the table above describes, the common primary user of the case system is the attending nurse or lab technician monitoring a patient's blood condition. The nurse's primary objective is the treatment, safety, and recovery of their patients. The diagnostic system should effectively warn the nurses and lab technicians of dangerous patient health conditions. The other two important stakeholders in the hospital context are the physicians who prescribe the overall medical treatment plan, and the patient who is being monitored. The next important stakeholder within the value web is the case company who designs and manufactures the case systems. Additionally, the regulatory bodies are also important stakeholders who oversee healthcare safety by establishing rules and standards for healthcare products.

4.2 System and Hazard Identification

As discussed in Chapter 2, an initial step in CAST analysis is to define the system and hazard in the accident.

System:

The case system is the medical diagnostic analyzer of patient blood constituents.

Hazard:

The definition of hazard is defined below [7]:

> *Hazard: State of system conditions when interact with other condition in environment of system, lead to accidents.*

The hazards relevant to the documented accidents of the case system are listed in Table 5 below. While there may be other hazards in the system, only those listed in Table 5 will only be discussed in this thesis.

Table 5. Case System Hazards

Hazard (H)	
H1:	The system reports erroneous patients results to the user.
H2:	The system reports the patient results too late.
H3:	The system is unavailable for intended use due to premature failure or cartridge rejection.

The H1 hazard of reporting of erroneous patient results is clinically significant and can lead to medical accidents. As discussed in Chapter 3, the erroneous low electrolyte reported result led to hazardous medical intervention. This resulted in an adverse event, which is an undesirable experience associated with the use of the medical product [40]. This accident and similar ones eventually led to the case accident of the case system.

H2 is the hazard where the system reports the correct patient results but untimely, or too late for usage. Such delay may have medical consequences. Since the design intent of the case system is for Point of Care (POC) environments, there is a need for a quick turn around time (TAT) starting from inputting the patient sample to receiving the final results. This is a significant need of the user due to the time sensitivity of the patient's health and subsequent medical treatment. Therefore, a hazard is present in having an undesired TAT for patient results.

H3 is the hazardous incident that the author experienced in Chapter 1, where the whole diagnostic system is unavailable due to premature system failures. Normal mitigations require a new cartridge installation and calibrations, which require unnecessary resources and money, but more importantly extends the time to when the next available patient sample can be analyzed. Similar to H2, time is a sensitive factor and may provide a hazardous situation for:

1. the medical staff because the patient's status is unknown and there is low confidence in the correct course of medical intervention.

2. the patient because there is a timely need for blood diagnostics. When this information is unavailable, the correct subsequent medical intervention is delayed.

4.3 System Safety Constraints and Safety Requirements

The next step in the CAST analysis, after hazards have been established, is to define safety constraints imposed by the hierarchical system of controls. Furthermore for each constraint, associated safety requirements must be established to set criteria to ensure the safety constraints (SC) are not violated. The safety requirements (SR) are listed below in Table 6.

Table 6. Case Study Safety Constraints and Requirements

Hazard	Safety Constraints (SC)	Safety Requirements (SR)
H1	SC1: Accurate patient results must be reported to the medical staff.	SR1: The system shall report accurate patient results within an acceptable total allowable error as defined by CLIA 88.
H2	SC2: Patient results must be reported to the medical staff in a useable timeframe.	SR2: The system shall have a patient result report turn-around-time of X.
H3	SC3: The system should be available for intended use as designed.	SR3: The system shall have a minimal cartridge uptime of X% during its use life.

The SC1 constraint for H1 indicates the analytical accuracy of the reportable patient results. As noted later in this section, a misdiagnosis of a patient result that is reported to the medical staff can lead to unnecessary and extremely dangerous medical consequences. Undesired results can leave the patient severely injured or deceased. The SR1 addresses this constraint by strictly adhering to the CLIA 88 accuracy guidelines for total allowable error for each analytical parameter. The violation of this requirement was described in Chapter 3.

Patient results need to be reported at a usable timeframe. The delay of a reported patient result leaves the medical staff and patient in a potentially hazardous state (H2) since the patient maybe under a critical situation (i.e. surgery), and require immediate intervention. Any unnecessary delay to the needed medical treatment could cause injury or death to the patient. The ensuing requirements address this concern by necessitating that all patient samples are reported with an X turn-around-time.

H3 prevents patient diagnosis to be performed because the system is totally unavailable due to premature system shutdown. The shutdown may be due to physical, software, or sensor related issues. The inaccessibility of this diagnostic system creates a significant hazardous situation, as the patient status is unknown. Without correct blood diagnostics, the medical staff is literally "blind" to the patient's status, and is unable to make a confident or correct medical decision. SR3 can be designed into the system from the system level down to the component, so that cartridge life up time can be maximized and hazardous conditions thwarted.

For the purpose of the case study, the hazard that will be analyzed is H1. The system reports erroneous patients results to the medical staff is the hazard that led to the medical casualty, and subsequent case accident. Furthermore, while not specifically analyzed, H2 is plays an important factor into the case accident that will be later discussed.

4.4 System Control Structure

As described in Chapter 2, a safety control structure is needed to investigate the accident to show the hierarchical relationship of control throughout the system. While CAST is applicable at the organization, environmental, and technical level, in this case, the physical system is the first control structure that needs to be investigated to understand the factors leading to the accident [7]. Therefore the boundary of the CAST analysis and thesis will be the technical system. Organizational and environmental factors may be discussed, but are not in the scope of this thesis. The control structure of the technical case system has been generated to the author's knowledge and interpretation of the case system and is located in Figure 12 below. The hyphenated red line denotes the scope of this thesis.

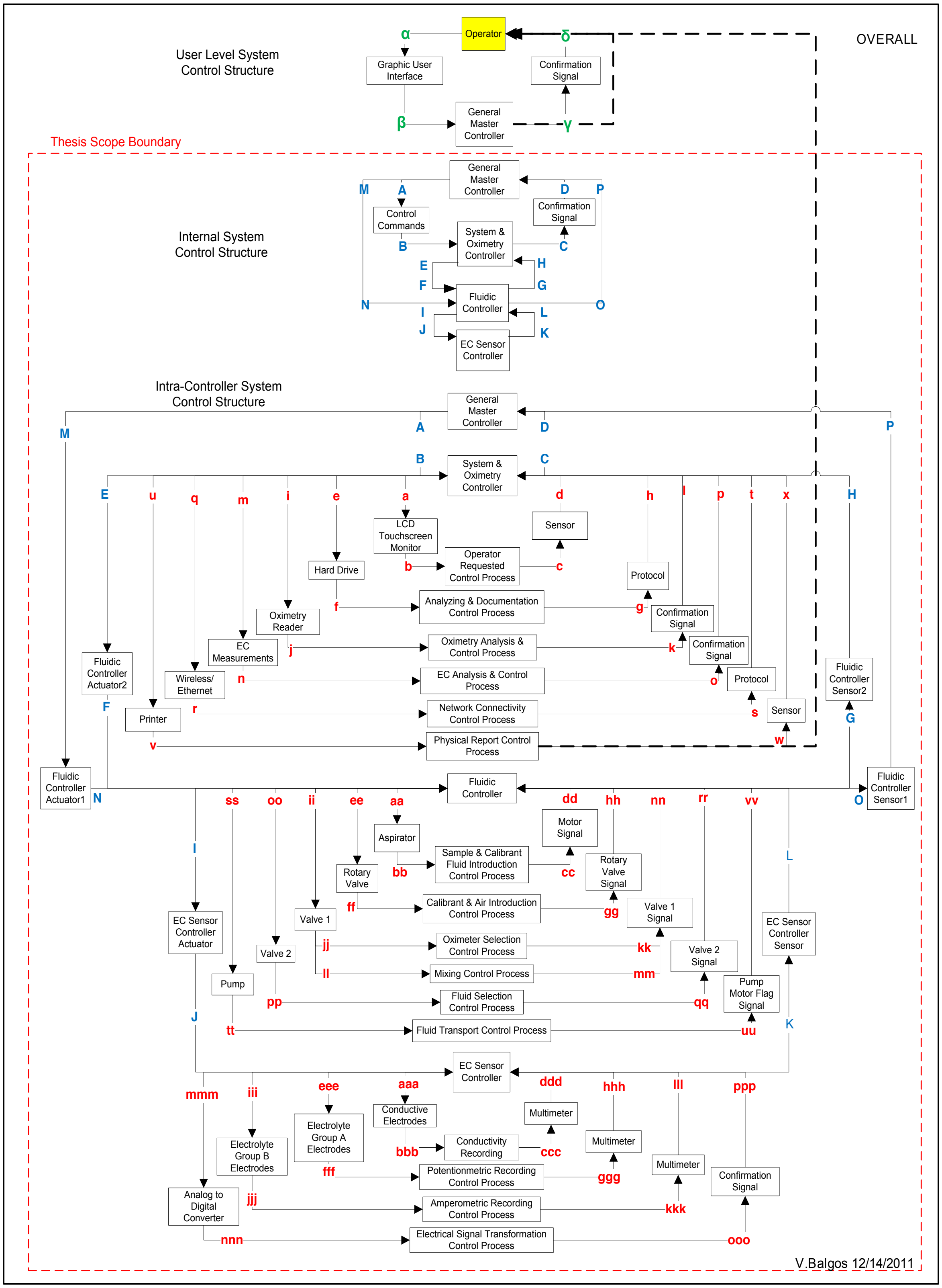
User Level System Control Structure
OVERALL
Operator
α
δ
Graphic User Interface
Confirmation Signal
β
General Master Controller
γ
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
M
A
D
P
Control Commands
Confirmation Signal
B
System & Oximetry Controller
C
E
H
F
G
Fluidic Controller
N
O
I
L
J
K
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
M
A
D
P
B
C
System & Oximetry Controller
E
u
q
m
i
e
a
d
h
l
p
t
x
H
LCD Touchscreen Monitor
Sensor
Hard Drive
b
Operator Requested Control Process
c
Protocol
f
Analyzing & Documentation Control Process
g
Confirmation Signal
Oximetry Reader
Oximetry Analysis & Control Process
k
Confirmation Signal
EC Measurements
j
Fluidic Controller Actuator2
Wireless/ Ethernet
n
EC Analysis & Control Process
o
Protocol
Fluidic Controller Sensor2
F
Printer
r
Network Connectivity Control Process
s
Sensor
G
v
Physical Report Control Process
w
Fluidic Controller Actuator1
N
Fluidic Controller
Fluidic Controller Sensor1
O
ss
oo
ii
ee
aa
dd
hh
nn
rr
vv
Aspirator
Motor Signal
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve
bb
cc
Rotary Valve Signal
I
L
ff
Calibrant & Air Introduction Control Process
gg
Valve 1
Valve 1 Signal
EC Sensor Controller Actuator
EC Sensor Controller Sensor
jj
Oximeter Selection Control Process
kk
Valve 2
Valve 2 Signal
ll
Mixing Control Process
mm
Pump
Pump Motor Flag Signal
pp
Fluid Selection Control Process
qq
J
K
tt
Fluid Transport Control Process
uu
EC Sensor Controller
mmm
iii
eee
aaa
ddd
hhh
lll
ppp
Conductive Electrodes
Multimeter
Electrolyte Group A Electrodes
bbb
Conductivity Recording
ccc
Multimeter
Electrolyte Group B Electrodes
fff
Potentionmetric Recording Control Process
ggg
Multimeter
Confirmation Signal
Analog to Digital Converter
jjj
Amperometric Recording Control Process
kkk
nnn
Electrical Signal Transformation Control Process
ooo
V.Balgos 12/14/2011

Figure 12. Case System Control Structure

As Figure 12 shows, the case study control structure is complex, containing many elements within multiple layers. It is noted that there are more elements to the control structure, but the shown elements are the critical factors for this thesis discussion. The basic control loop elements described in Chapter 2 are present, and the relationships between all elements are explicitly shown and enumerated. For the purpose of the thesis discussion, the control loops will be referred by a case sensitive 4-part naming convention. For example, the Fluidic Controller – Pump – Fluid Transport Control Process – Pump Motor Flag Signal loop, will be referred to as control loop "ss-tt-uu-vv". Similarly, each relationship between two elements will be defined as a single link (i.e. "tt" for the Pump to Fluid Transport Control Process). This nomenclature will be utilized throughout this thesis.

The creation of the technical control structure began at the highest level with the user. The single straightforward but influential control loop α-β-γ-δ predominately dictates the value delivery of the system. The Greek alphabet nomenclature was used to distinguish the origin of the control structure, and highest chain of command. After establishing the control structure origin, the controlled process element was evaluated further and functionally decomposed. Based on the author's knowledge of the system architecture, the decomposition resulted in three separate controlled processes. The nomenclature of capitalized modern English Alphabet was used to distinguish the subordinate hierarchical level, and a commonality between the three levels since they work together to produce the higher level value. Finally, each of the three controlled process was further detailed with more specific controlled processes. This is denoted by usage of lower case modern English Alphabet, and the number of letter replicates helped dictate and group the detailed controlled process. For example, all single letter (i.e. a) denotes subjection to a different controller than a triple letter loop (i.e. aaa). This facilitated the understanding and management of the numerous loops and elements in the control structure.

As mentioned earlier, the User Control Structure is the highest-level view of the system hierarchy. Essentially, it captures how the users (nurse and lab technicians) interact with the case system. The graphical user interface (GUI) allows the user to request function such as sample process, input patient information, review patient data, configures system settings and performs additional calibrations. The GUI is the actuator that sends commands to the Controlled Process, in this case the General Master Controller (GMC), for desired functions. Verifications of the requested processes are fed back to the user in the form of visual and auditory information.

Decomposing the General Master Controller in the User Level System Control Structure, the next layer of the control structure shows more details about the internal controls. At this layer, the GMC serves as the Controller, and acts as the "master" for three lower lever controlled processes: System & Oximetry Control (SOC), Fluidic Control (FC), and the EC Sensor Control (ESC). The SOC maintains the overall system, Oximetry and EC analytical data processing. The FC oversees the fluidic system and maintains the pump, valves, and mechanical aspirator. The analog ESC monitors and records the EC sensor data from patient samples, and system calibrants. Each of the three controllers has dedicated actuator and sensor elements and are control commands and confirmation signals, respectively.

Finally, to add details to the above three controllers, a more detailed control diagram for the technical system was generated to capture the Intra-Controller system. In this view, the direct controls of the actual components (mechanics, electrical, software) are exhibited. As illustrated, the SOC, FC, and ESC work together concurrently and successively. The emergent function of these interactions is the system end value, the safe analysis and reporting of the patient sample result. In addition, almost 20 control loops also maintain other system functionalities such as calibrations, washing, and networking capabilities.

4.5 Control Structure under Normal Intended Usage:

Most of the control loops work together in tandem or concurrently throughout Figure 13 to Figure 17. These control loops may work in series, parallel, or independent from one another. For ease of discussion, the normal process will be divided into five basic steps: Sample Preparation, Aspiration, EC Sample Process, Oximetry & Patient Reporting, and Wash & Calibration Cycle. In addition, each control loop element that is used in the each step will be highlighted to illustrate the process flow and interaction between the various loops.

For normal typical patient blood analysis, the user initiates the sample process with a single selection on the GUI. This initiates the sample preparation process and the control structure initiates several control actions. These enabled control loops are highlighted in Figure 13 below.

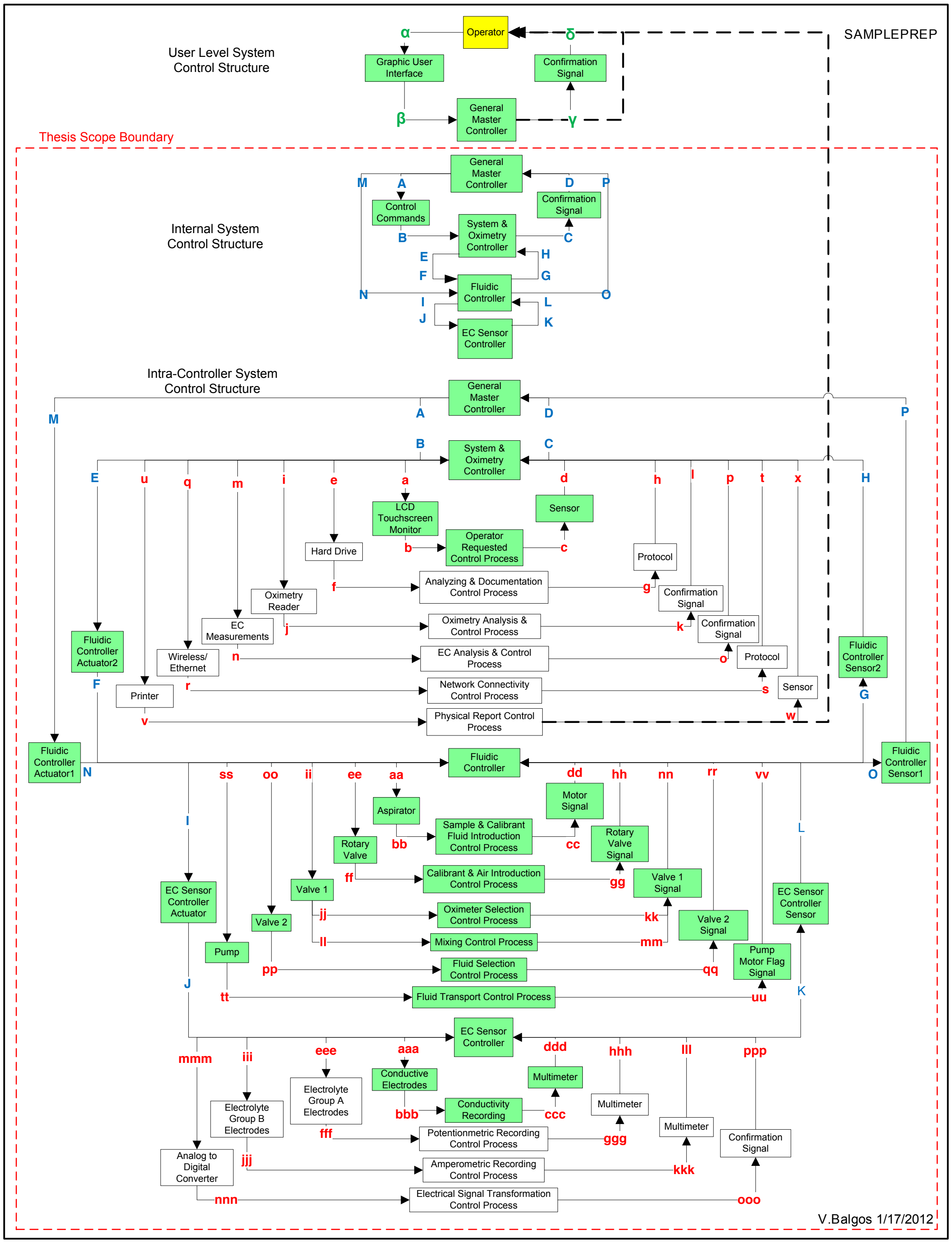
SAMPLEPREP
User Level System Control Structure
Operator
α
δ
Graphic User Interface
Confirmation Signal
β
γ
General Master Controller
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
M
A
D
P
Control Commands
Confirmation Signal
B
C
System & Oximetry Controller
E
H
F
G
N
O
Fluidic Controller
I
L
J
K
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
M
A
D
P
B
C
System & Oximetry Controller
E
u
q
m
i
e
a
d
h
l
p
t
x
H
LCD Touchscreen Monitor
Sensor
Hard Drive
b
Operator Requested Control Process
c
Protocol
Oximetry Reader
f
Analyzing & Documentation Control Process
g
Confirmation Signal
EC Measurements
j
Oximetry Analysis & Control Process
k
Confirmation Signal
Fluidic Controller Actuator2
Wireless/ Ethernet
n
EC Analysis & Control Process
o
Protocol
Fluidic Controller Sensor2
F
Printer
r
Network Connectivity Control Process
s
Sensor
G
v
Physical Report Control Process
w
Fluidic Controller Actuator1
N
Fluidic Controller
Fluidic Controller Sensor1
O
ss
oo
ii
ee
aa
dd
hh
nn
rr
vv
Aspirator
Motor Signal
I
Rotary Valve
bb
Sample & Calibrant Fluid Introduction Control Process
cc
Rotary Valve Signal
L
ff
Calibrant & Air Introduction Control Process
gg
Valve 1 Signal
EC Sensor Controller Actuator
Valve 1
Valve 2
jj
Oximeter Selection Control Process
kk
Valve 2 Signal
EC Sensor Controller Sensor
ll
Mixing Control Process
mm
Pump
pp
Fluid Selection Control Process
qq
Pump Motor Flag Signal
J
tt
Fluid Transport Control Process
uu
K
EC Sensor Controller
mmm
iii
eee
aaa
ddd
hhh
lll
ppp
Conductive Electrodes
Multimeter
Electrolyte Group B Electrodes
Electrolyte Group A Electrodes
bbb
Conductivity Recording
ccc
Multimeter
Multimeter
fff
Potentiometric Recording Control Process
ggg
Confirmation Signal
Analog to Digital Converter
jjj
Amperometric Recording Control Process
kkk
nnn
Electrical Signal Transformation Control Process
ooo
V.Balgos 1/17/2012

Figure 13. Sample Preparation in Control Structure

As Figure 13 shows, the user initiates the GMC which in turns enables the three lower controllers, SOC, FC, and ESC. In the SOC structure, control loop a-b-c-d enables the GUI application to notify the system when the user is ready to aspirate sample. The FC enables all its lower control loops (aa to vv) to prepare the system for blood sample. This includes the following:

Control Loop	Controlled Function
aa-bb-cc-dd	Patient sample introduction into system
ee-ff-gg-hh	Introduction of pre-sample air segment and calibrant solution
ii-jj-kk-nn	Selection of the Oximetry process
ii-ll-mm-nn	Mixing Process disabled
oo-pp-qq-rr	Selection of EC process
ss-tt-uu-vv	Fluid transport mechanism

The ESC has only the control loop aaa-bbb-ccc-ddd enabled for detection and positioning of the sample.

Once the system is ready to accept a blood sample, the user then presents the blood sample to the system, and initiates the sample aspiration process by selecting the LCD Touchscreen. This enables control loop ss-tt-uu-vv to draw the necessary volume of sample into the system, while control loop aaa-bbb-ccc-ddd is actively monitoring and position the sample in the correct EC area. This is highlighted in Figure 14 below.

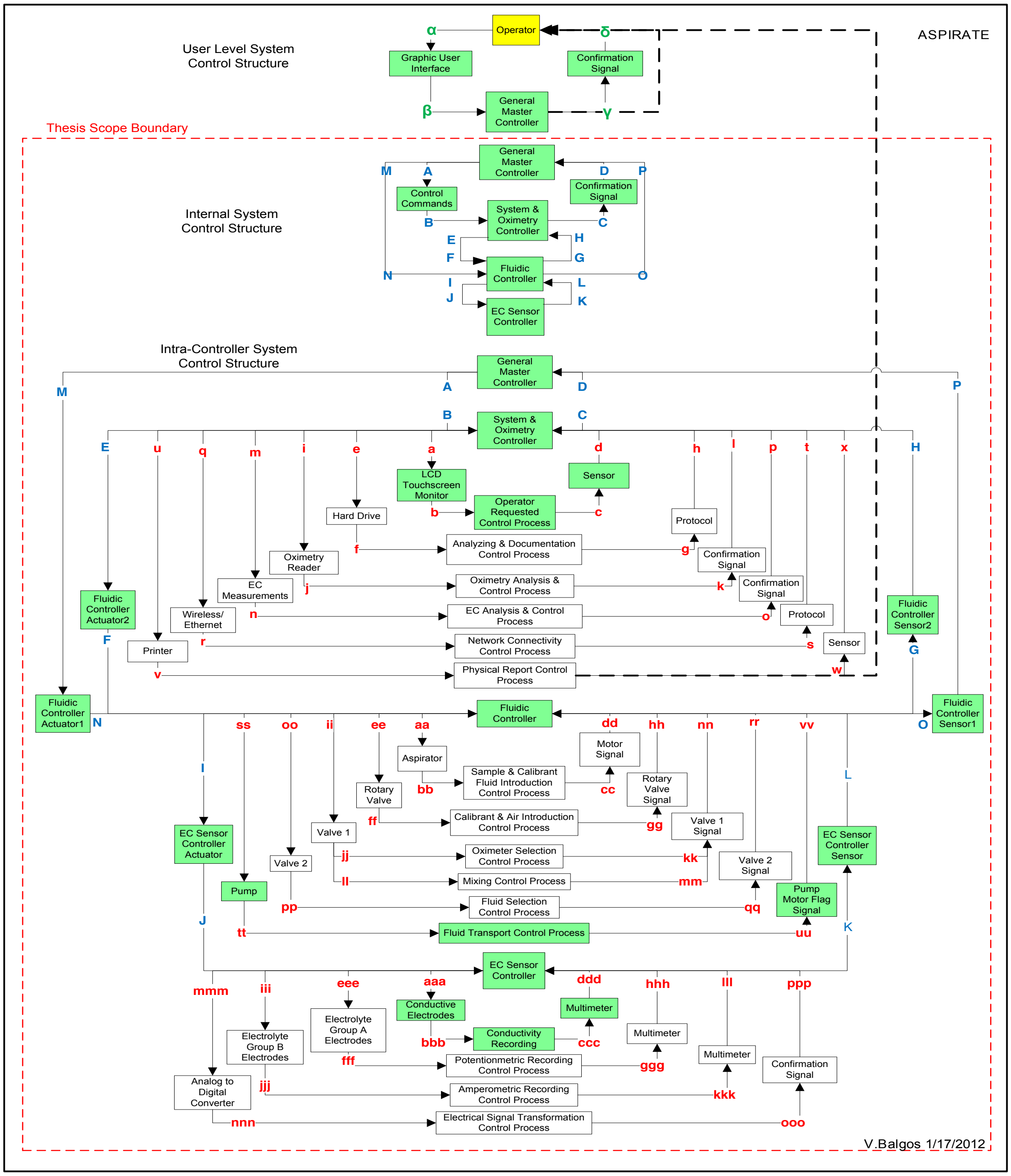
ASPIRATE
User Level System Control Structure
Operator
α
δ
Graphic User Interface
Confirmation Signal
β
General Master Controller
γ
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
M
A
D
P
Control Commands
Confirmation Signal
B
System & Oximetry Controller
C
E
H
F
G
Fluidic Controller
N
O
I
L
J
K
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
M
A
D
P
B
C
System & Oximetry Controller
E
u
q
m
i
e
a
d
h
l
p
t
x
H
LCD Touchscreen Monitor
Sensor
Hard Drive
b
Operator Requested Control Process
c
Protocol
Oximetry Reader
f
Analyzing & Documentation Control Process
g
Confirmation Signal
EC Measurements
j
Oximetry Analysis & Control Process
k
Confirmation Signal
Fluidic Controller Actuator2
Wireless/ Ethernet
n
EC Analysis & Control Process
o
Protocol
Fluidic Controller Sensor2
F
Printer
r
Network Connectivity Control Process
s
Sensor
G
v
Physical Report Control Process
w
Fluidic Controller Actuator1
N
Fluidic Controller
O
Fluidic Controller Sensor1
ss
oo
ii
ee
aa
dd
hh
nn
rr
vv
Aspirator
Motor Signal
I
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve
bb
cc
Rotary Valve Signal
L
ff
Calibrant & Air Introduction Control Process
gg
Valve 1
Valve 1 Signal
EC Sensor Controller Actuator
EC Sensor Controller Sensor
jj
Oximeter Selection Control Process
kk
Valve 2
Valve 2 Signal
ll
Mixing Control Process
mm
Pump
Pump Motor Flag Signal
pp
Fluid Selection Control Process
qq
J
K
tt
Fluid Transport Control Process
uu
EC Sensor Controller
mmm
iii
eee
aaa
ddd
hhh
lll
ppp
Conductive Electrodes
Multimeter
Electrolyte Group A Electrodes
Electrolyte Group B Electrodes
bbb
Conductivity Recording
ccc
Multimeter
Multimeter
fff
Potentiometric Recording Control Process
ggg
Confirmation Signal
Analog to Digital Converter
jjj
Amperometric Recording Control Process
kkk
nnn
Electrical Signal Transformation Control Process
ooo
V.Balgos 1/17/2012

Figure 14. Sample Aspiration in Control Structure

After the blood sample is within the system, EC blood measurements are taken in ESC loops aaa through ppp in Figure 15 below. The EC measurement values (electrical currents and voltages) are then sent to the FC whom then relays the data to the SOC. In m-n-o-p control loop, digital readings are analyzed with proprietary software algorithms. The SOC then transforms them into useful clinical diagnostic results. This EC data is stored in the e-f-g-h loop, and the sample is then ready for the next step, oximetry processing.

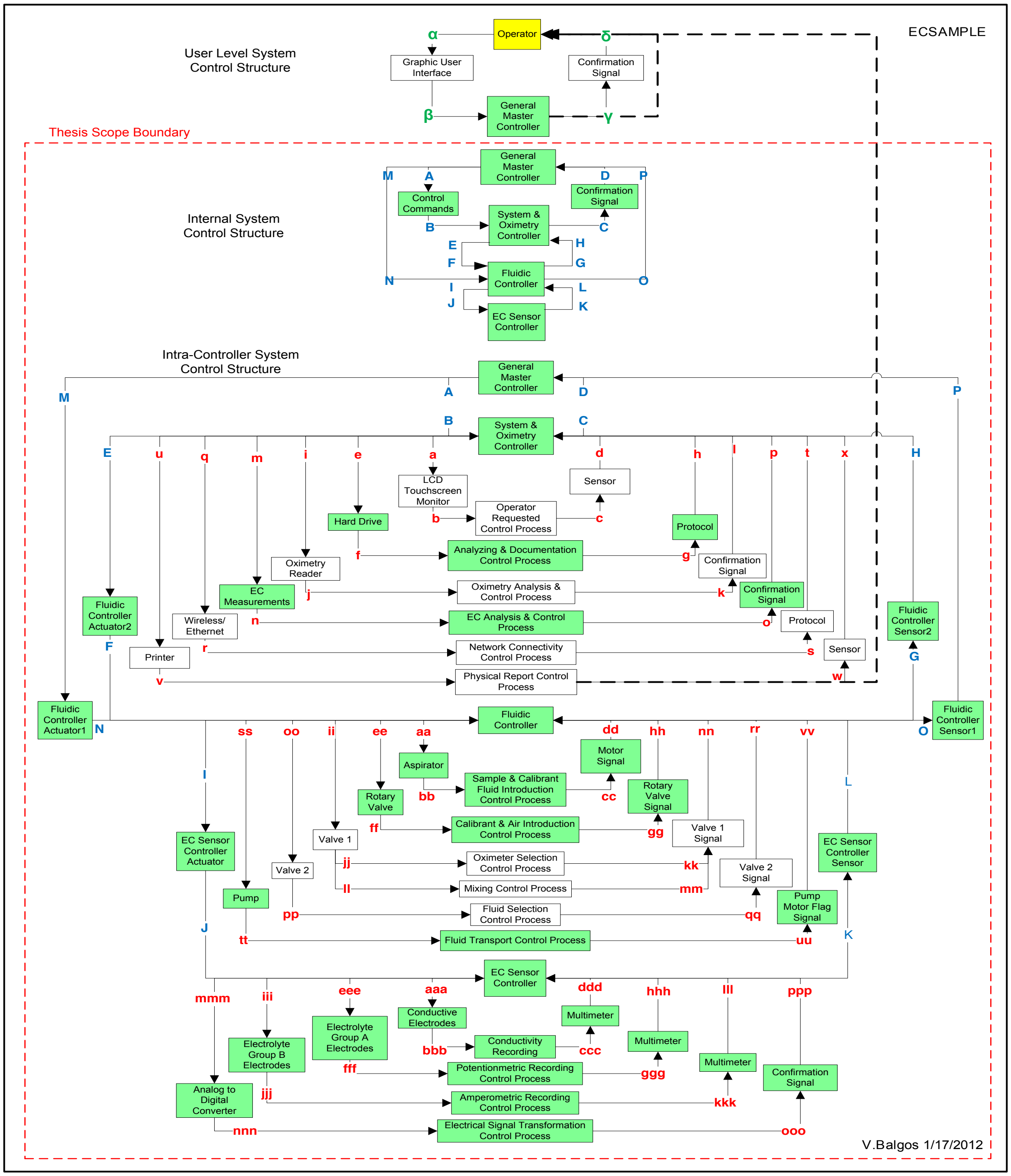
ECSAMPLE
User Level System Control Structure
Operator
α
δ
Graphic User Interface
Confirmation Signal
β
General Master Controller
γ
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
M
A
D
P
Control Commands
Confirmation Signal
B
System & Oximetry Controller
C
E
H
F
G
Fluidic Controller
N
I
L
O
J
K
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
M
A
D
P
B
C
System & Oximetry Controller
E
u
q
m
i
e
a
d
h
l
p
t
x
H
LCD Touchscreen Monitor
Sensor
Operator Requested Control Process
b
c
Hard Drive
Protocol
f
g
Analyzing & Documentation Control Process
Oximetry Reader
Confirmation Signal
EC Measurements
j
k
Oximetry Analysis & Control Process
Confirmation Signal
Fluidic Controller Actuator2
Wireless/ Ethernet
n
o
EC Analysis & Control Process
Protocol
Fluidic Controller Sensor2
F
Printer
r
Network Connectivity Control Process
s
Sensor
G
v
Physical Report Control Process
w
Fluidic Controller Actuator1
N
Fluidic Controller
O
Fluidic Controller Sensor1
ss
oo
ii
ee
aa
dd
hh
nn
rr
vv
Aspirator
Motor Signal
I
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve
bb
cc
Rotary Valve Signal
L
ff
Calibrant & Air Introduction Control Process
gg
Valve 1
Valve 1 Signal
EC Sensor Controller Actuator
jj
Oximeter Selection Control Process
kk
EC Sensor Controller Sensor
Valve 2
Valve 2 Signal
ll
Mixing Control Process
mm
Pump
Pump Motor Flag Signal
pp
Fluid Selection Control Process
qq
J
tt
Fluid Transport Control Process
uu
K
EC Sensor Controller
mmm
iii
eee
aaa
ddd
hhh
lll
ppp
Electrolyte Group A Electrodes
Conductive Electrodes
Multimeter
Electrolyte Group B Electrodes
Multimeter
bbb
Conductivity Recording
ccc
Multimeter
fff
Potentionmetric Recording Control Process
ggg
Confirmation Signal
Analog to Digital Converter
jjj
Amperometric Recording Control Process
kkk
nnn
Electrical Signal Transformation Control Process
ooo
V.Balgos 1/17/2012

Figure 15. EC Sample Process in Control Structure

After the EC samples are processed, the FC transports the sample to the oximeter measurement area via the ii-jj/ll-kk/mm-nn, oo-pp-qq-rr, and ss-tt-uu-vv loops. Once the fluid is in the measurement area, the oximetry reader processes the optical readings of the blood sample in loop i-j-k-l into useful diagnostic results. The oximetry data is stored in the e-f-g-h loop, and the now completed diagnostic results are reported up the hierarchical control structure to the user (α-β-γ-δ loop). It is important to note that at this time, that the patient results need to be reported immediately for the TAT requirement compliance. The results are displayed on the GUI of the system whereby the user can explicitly see the results. In addition, an electronic version of the data is sent to the HIS (if available) via control loop q-r-s-t, and a paper copy is produced in loop u-v-w-x for physical documentation. The direct value delivery to the end user is designated in Figure 15 and Figure 16 as hyphenated lines.

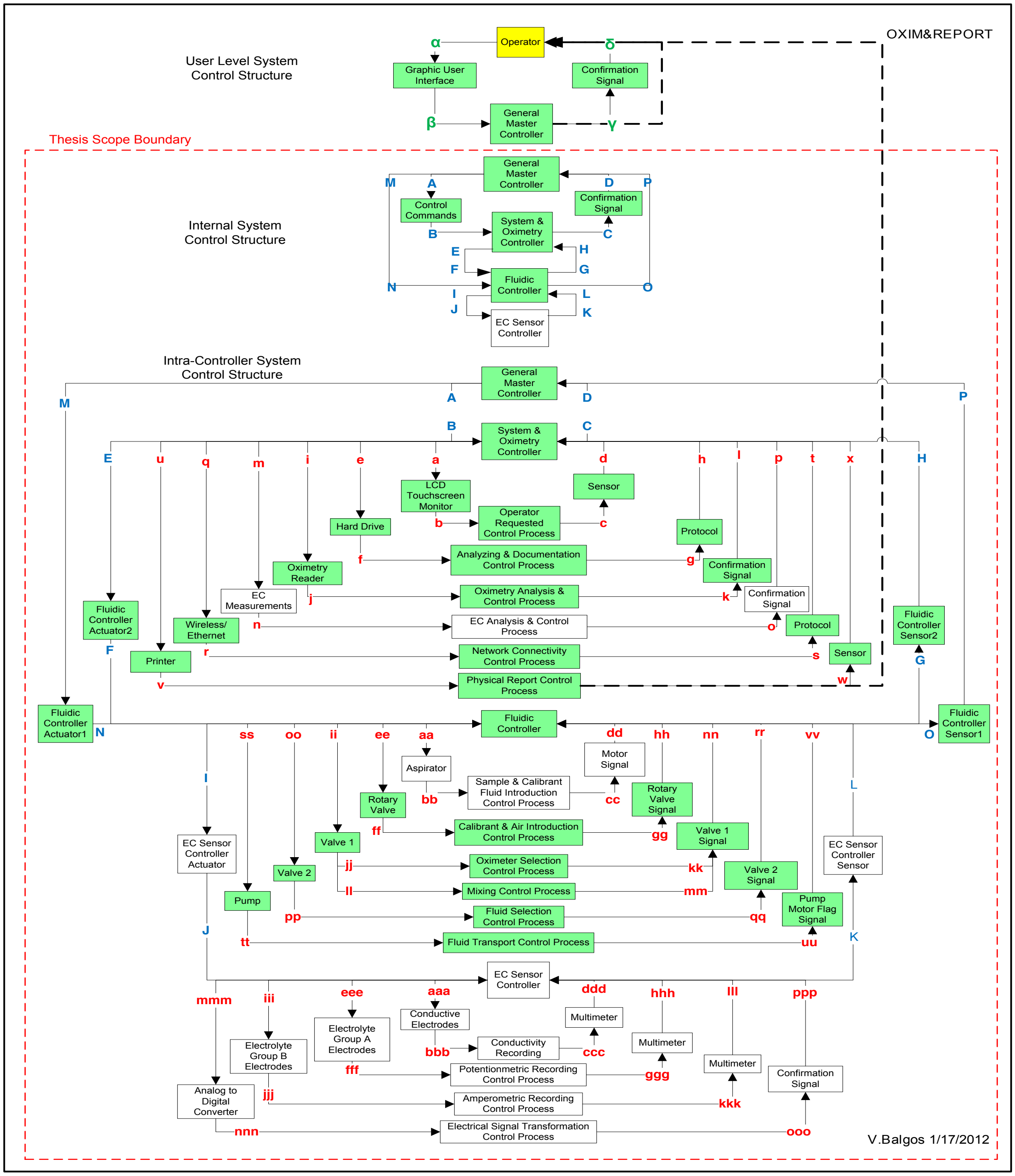
OXIM&REPORT
User Level System
Control Structure
Operator
Graphic User Interface
Confirmation Signal
General Master Controller
α
β
γ
δ
Thesis Scope Boundary
Internal System
Control Structure
General Master Controller
Control Commands
Confirmation Signal
System & Oximetry Controller
Fluidic Controller
EC Sensor Controller
Intra-Controller System
Control Structure
General Master Controller
System & Oximetry Controller
LCD Touchscreen Monitor
Sensor
Operator Requested Control Process
Hard Drive
Protocol
Analyzing & Documentation Control Process
Confirmation Signal
Oximetry Reader
EC Measurements
Oximetry Analysis & Control Process
Confirmation Signal
Fluidic Controller Actuator2
Wireless/ Ethernet
EC Analysis & Control Process
Protocol
Fluidic Controller Sensor2
Printer
Network Connectivity Control Process
Sensor
Physical Report Control Process
Fluidic Controller Actuator1
Fluidic Controller
Fluidic Controller Sensor1
Aspirator
Motor Signal
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve
Rotary Valve Signal
Calibrant & Air Introduction Control Process
Valve 1 Signal
EC Sensor Controller Actuator
Valve 1
EC Sensor Controller Sensor
Oximeter Selection Control Process
Valve 2
Valve 2 Signal
Mixing Control Process
Pump
Fluid Selection Control Process
Pump Motor Flag Signal
Fluid Transport Control Process
EC Sensor Controller
Conductive Electrodes
Multimeter
Electrolyte Group A Electrodes
Multimeter
Electrolyte Group B Electrodes
Conductivity Recording
Multimeter
Potentionmetric Recording Control Process
Confirmation Signal
Analog to Digital Converter
Amperometric Recording Control Process
Electrical Signal Transformation Control Process
A B C D E F G H I J K L M N O P
a b c d e f g h i j k l m n o p q r s t u v w x
aa bb cc dd ee ff gg hh ii jj kk ll mm nn oo pp qq rr ss tt uu vv
aaa bbb ccc ddd eee fff ggg hhh iii jjj kkk lll mmm nnn ooo ppp
V.Balgos 1/17/2012

Figure 16. Oximetry and Patient Result Reporting in Control Structure

Once the patient results have been reported, the system undergoes a wash & calibration cycle. The FC removes now unusable patient blood sample from the system and sends it to the waste containment module (not shown). The FC also flushes the entire system with proprietary solutions to remove any contaminants and carryover from the sample. After the flushing, the system performs a calibration on all sensors via loops aaa to lll (EC) and i-j-k-l (Oximetry) to ensure that the system was able to return to a normal, safe state. Once an acceptable calibration values are measured and verified by the SOC, the system is now ready for the next patient sample. This is illustrated in Figure 17 below. It is important to note, that if the sensors do not pass this calibration, a limited number of subsequent washing and calibrations are performed until sensor has recovered. If the sensor does not recover within a predetermined range, the original patient result is flagged with a message indicating questionable results and all future patient results for this sensor are disabled.

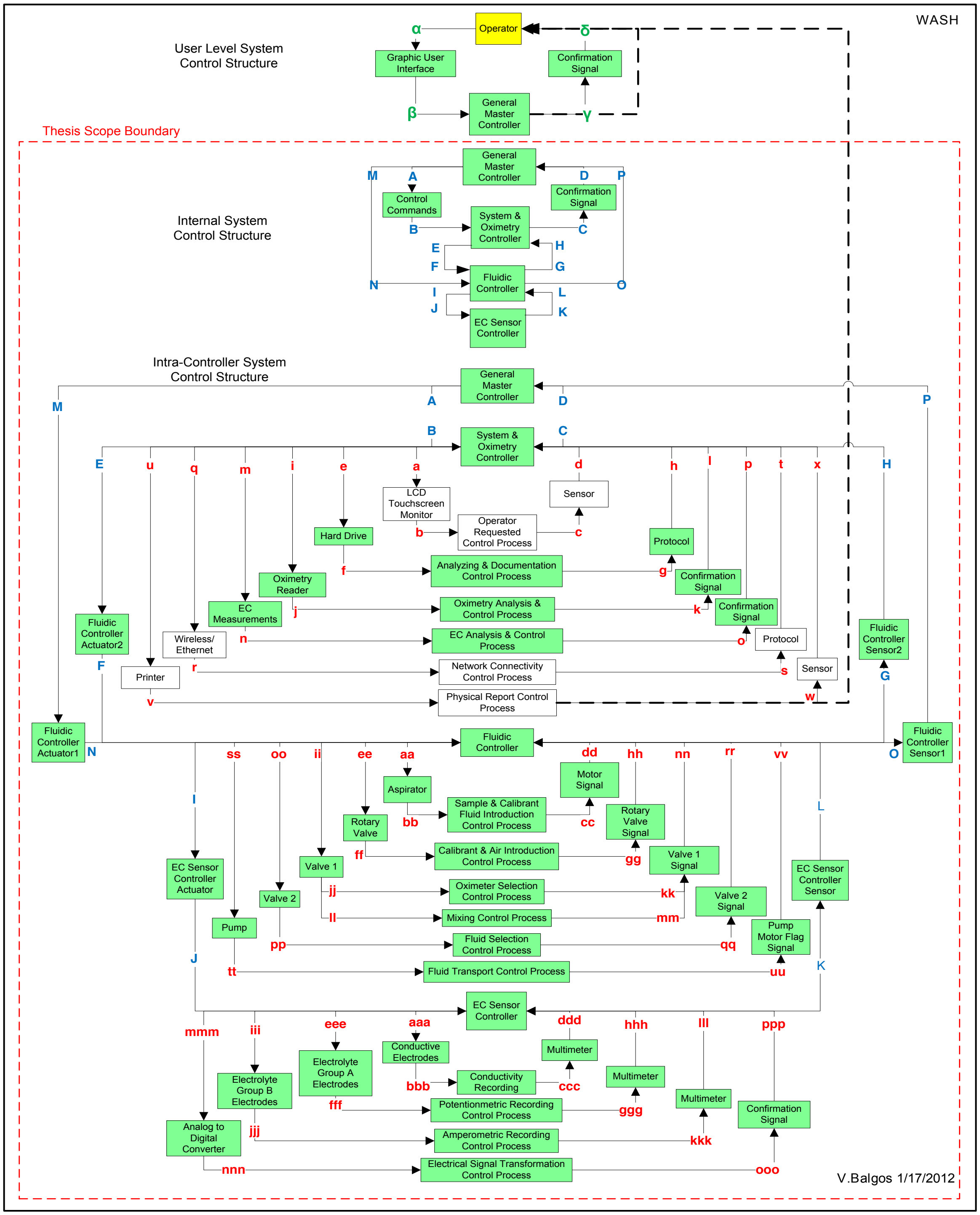
WASH
User Level System Control Structure
Operator
α
δ
Graphic User Interface
Confirmation Signal
β
γ
General Master Controller
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
M
A
D
P
Control Commands
Confirmation Signal
B
C
System & Oximetry Controller
E
H
F
G
Fluidic Controller
N
O
I
L
J
K
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
M
A
D
P
B
C
System & Oximetry Controller
E
u
q
m
i
e
a
d
h
l
p
t
x
H
LCD Touchscreen Monitor
Sensor
Operator Requested Control Process
b
c
Hard Drive
Protocol
f
Analyzing & Documentation Control Process
g
Oximetry Reader
Confirmation Signal
EC Measurements
j
Oximetry Analysis & Control Process
k
Confirmation Signal
Fluidic Controller Actuator2
Wireless/ Ethernet
n
EC Analysis & Control Process
o
Protocol
Fluidic Controller Sensor2
F
Printer
r
Network Connectivity Control Process
s
Sensor
G
v
Physical Report Control Process
w
Fluidic Controller Actuator1
N
Fluidic Controller
Fluidic Controller Sensor1
O
ss
oo
ii
ee
aa
dd
hh
nn
rr
vv
Aspirator
Motor Signal
I
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve Signal
L
Rotary Valve
bb
cc
ff
Calibrant & Air Introduction Control Process
gg
Valve 1 Signal
Valve 1
EC Sensor Controller Actuator
EC Sensor Controller Sensor
jj
Oximeter Selection Control Process
kk
Valve 2
Valve 2 Signal
ll
Mixing Control Process
mm
Pump
Pump Motor Flag Signal
pp
Fluid Selection Control Process
qq
J
K
tt
Fluid Transport Control Process
uu
EC Sensor Controller
mmm
iii
eee
aaa
ddd
hhh
lll
ppp
Conductive Electrodes
Multimeter
Electrolyte Group A Electrodes
Electrolyte Group B Electrodes
bbb
Conductivity Recording
ccc
Multimeter
fff
Potentionmetric Recording Control Process
ggg
Multimeter
Confirmation Signal
Analog to Digital Converter
jjj
Amperometric Recording Control Process
kkk
nnn
Electrical Signal Transformation Control Process
ooo
V.Balgos 1/17/2012

Figure 17. Wash & Calibration Cycle in Control Structure

For the purpose and scope of this thesis, the Internal and Intra-Controller system will be the focus, and is depicted in Figure 12 to Figure 17 as the red boundary line. The highest level control structure, User Level, was needed to understand the complete relationship and linkage to the final medical staff user(s).

4.6 Proximal Chain of Events

Due to Health Insurance Portability and Accountability Act (HIPAA) and other confidentiality factors, specific information of the medical accidents could not be obtained or published. Therefore, a general outline of the accident was generated based on the limited data found on the FDA MAUDE database, informal deductions, and professional experience with the case system.

1. Patient is prescribed by physician(s) to be continuously observed by routine BMP (Basic Metabolic Panel) diagnostic testing for precaution due to several reasons (i.e. during operation, post operation recovery, observation).

   BMP usually evaluates the electrolyte levels in a patients blood supply:
   Variations of BMP exist, but the case sensor is a standard routine assay across clinical practices.

2. Medical staff (Nurse, lab technicians) performs the regular BMP testing as prescribed on the patient.

3. The case system appears to function normally (i.e. no system warnings) during patient sample analysis and reports an erroneous low electrolyte result, indicating a potential threatening *hypo*-electrolytic condition. There is no immediate error message attached to the patient result.

4. Medical staff quickly reacts to low electrolyte patient result by with medical intervention with potentially administering aqueous electrolyte solution intravenously to the patient to increase the believed low electrolyte level to normal levels.

5. Since the patient actually had normal electrolyte levels, the sudden increase in electrolyte raises the level beyond normal range and induces a *hyper*-electrolytic condition. The patient then may undergo cardiac arrhythmia, muscular fibrillation, epileptic seizure and/or death.

6. Post accident investigation confirmed that the case system reported erroneously low electrolyte results when compared to a laboratory reference diagnostic system.

It is presumed all erroneously low electrolyte medical adverse events occurred in clinical hospital environments, with some in critical patient areas such as intensive care areas or in the operation area. The hospital environment is extremely dynamic with peaks and valleys of activities. The number of patients usually remains relatively constant, but the level of medical staff peaks during the daytime and decline during the night shifts. Therefore, while intended use of the case study system remains constant, the medical staff on duty responsibilities changes accordingly to schedule.

4.7 Analysis of Loss at the Physical System Level

It was found that a foreign material was an immediate cause that leads to erroneously diagnosing the low levels of a specific electrolyte in the blood. A foreign mass was present on the surface of the specific electrolyte membrane in study, and physically covered it. In normal working electrodes, the ion selective membrane of an electrochemical cell attracts the specific electrolyte ion in a patient blood sample (see left side of Figure 18). By measuring the potential difference between the reference and working electrode, the value recorded can be related to the specific activity of the targeted electrolyte ion in blood. This is the eventual clinical result that is reported to the user.

In the case of the accident, the foreign mass prevented the transport of the blood ions into the sensor, and thus affects the potentiometric measurement (see right side of Figure 18). By blocking the correct ion transport flow into the sensor, an erroneous low result will be reported in the presence of normal electrolyte level in the blood.

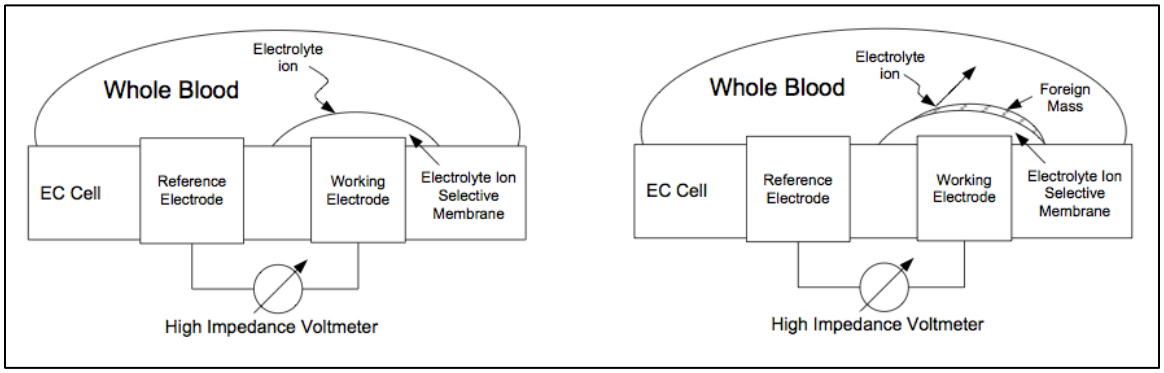

Figure 18. Electrochemical Potentiometric Cell

Efforts by the case company found that the removal of the foreign mass covering the membrane eliminates the erroneous low results of that particular sensor. It was also found that the sensor itself did not have failures and had the proper ion transfer capability. Therefore, the company then focused on activities to prevent the foreign mass from covering the sensor. The details of the foreign material will not be discussed further in this thesis, as it is not needed for the CAST analysis. While the immediate cause is a significant element, it does not really explain how such a fault was allowed to deviate in the product while the company's design and production engineers thought they were producing a high quality product able to control fault system variations. The rest of the chapter applies the STAMP model to illustrate that the cause of the accident was an absence of control of the case system, not merely a component failure.

4.8 CAST Analysis

The next step is to specifically investigate the control loops that may have initiated the recall. The objective is to look for violation of safety constraints that may have come from other control loops. From the main control structure located in Figure 12, there were seven identified control loops across all three identified control structure layers that may have been a factor in the erroneous patient result hazard. They are listed below:

Control Layer	Controlled Process	Control Loop
Intra	Potentiometric recording	eee-fff-ggg-hhh
Intra	Electrical Signal Transformation	mmm-nnn-ooo-ppp
Internal	ESC data transfer to FSC	I-J-K-L
Internal	FSC data transfer to SOC	E-F-G-H
Intra	EC and Analysis	m-n-o-p
Internal	SOC data transfer to GMC	A-B-C-D
User *	GMC data display to Operator	α-β-γ-δ

** Outside scope of thesis*

Three control loops of interest were found in the intra-controller layer, while others found in each of the higher layers (Internal and User Level). For the purpose of this thesis, only the first six located in list above will be further analyzed and discussed. The other one will not be discussed, and is outside the scope of this thesis. It will be assumed that all other loops were functioning correctly.

The identified control loops of interest will now be analyzed for factors that could contribute to a hazardous state. Leveson established several classifications of control loop deficiencies that could lead to hazards. This captured in Figure 19 below from Leveson [7] with the encircled numbers.

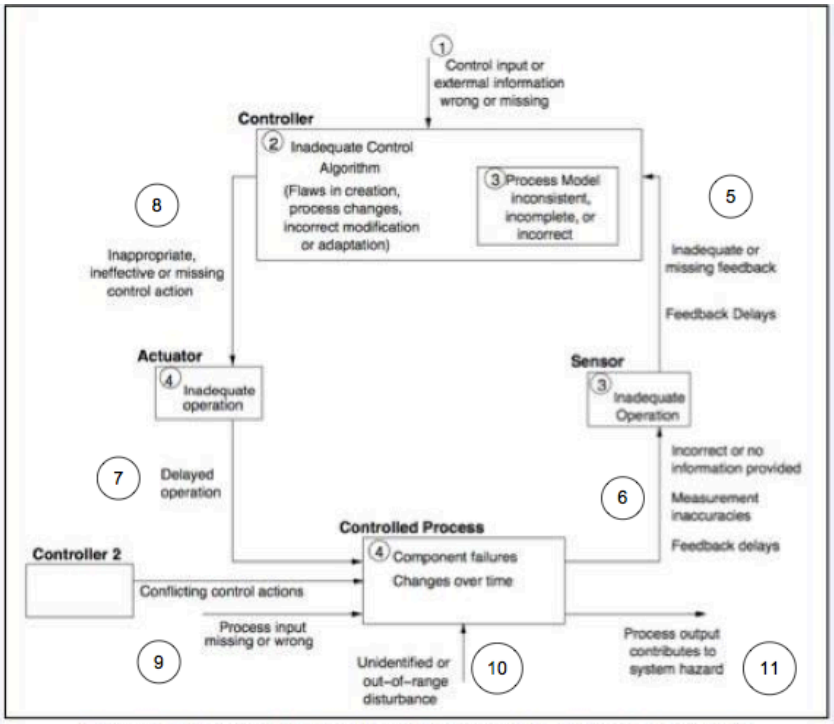
1
Control input or external information wrong or missing
Controller
2 Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
3 Process Model inconsistent, incomplete, or incorrect
8
Inappropriate, ineffective or missing control action
5
Inadequate or missing feedback
Feedback Delays
Actuator
4 Inadequate operation
Sensor
3 Inadequate Operation
7
Delayed operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
6
Controlled Process
4 Component failures
Changes over time
Controller 2
Conflicting control actions
Process input missing or wrong
9
Unidentified or out-of-range disturbance
10
Process output contributes to system hazard
11

Figure 19. General Control Deficiencies Leading to Hazards

Four significant encircled categories in the above figure are briefly described below:

1. Unsafe Inputs to the Controller:
   The delivery of unsafe information from an external system or user onto the controller that leads to hazardous state. The information may be missing, inadequate, or clearly wrong.

2. Unsafe Control Algorithms in Controller:
   The execution of inadequate or unsafe logical programs by the controller onto the control loop. Since humans develop the programs, they are susceptible to error, logical flaws, or inadequate design.

3. Incorrect Process Models on Controller and Sensor:
   Inaccurate model of the process by the Controller and Sensor that doesn't reflect the actual process. Failure examples include missing data, feedback controls, and response delays.

4. Inadequate Operation on the Actuator and Controlled Process:
   The inability to execute the control actions properly by the actuator and or controlled process. Common failures are transmission of control signals, component failure, or inadequate inputs from other entities in the system.

In addition to the above categories, there are several other considerations illustrated in Figure 19 that can also elucidate potential causes of hazards. By superimposing the elements of the control loop of interest in Figure 19, every element and linkage will be analyzed with the basic question "How could the 'guide words' lead to the specific hazard?" This would be performed along the control loop on all elements, and continue will all relevant control loops of the focused hazard.

Using this framework for the thesis CAST analysis, the intent is to identify the hazards that led to the case accident. The focus of the analysis will be for H1: Accurate patient results must be reported to the medical staff at all time, since this was the catalyst for the FDA recall. The identified hazards of the case accident will serve as the driver to the design requirements that will be generated in the next section. Furthermore, during the CAST analysis, additional hazards that could lead to other accidents will be documented for the purpose of comparing against the original set of hazards identified by the standard FMECA methodology.

To begin the analysis, the lowest control loop, eee-fff-ggg-hhh, will be discussed first since this is where the hazards initiated. The results from this loop analysis will later show how these failures move up to higher levels of the control structure. Further discussion will discuss why each higher layer failed to control the hazard. As a reminder control loop of eee-fff-ggg-hhh, it records the potentiometric readings directly off the patient sample, and is shown again at the bottom of Figure 20.

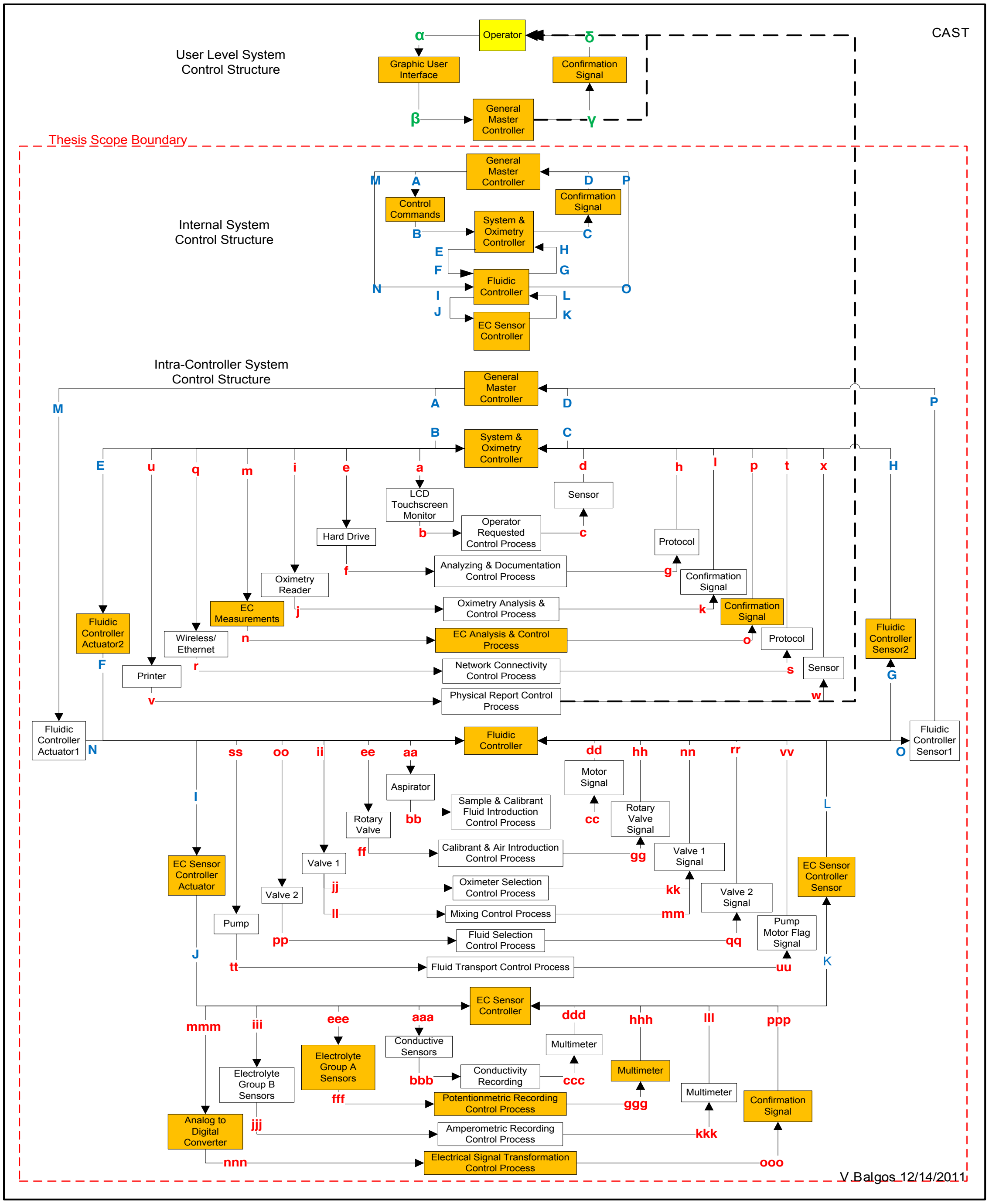
CAST
User Level System Control Structure
Operator
α
δ
Graphic User Interface
Confirmation Signal
β
General Master Controller
γ
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
M
A
D
P
Control Commands
Confirmation Signal
B
System & Oximetry Controller
C
E
H
F
G
N
Fluidic Controller
O
I
L
J
K
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
M
A
D
P
B
C
System & Oximetry Controller
E
u
q
m
i
e
a
d
h
l
p
t
x
H
LCD Touchscreen Monitor
Sensor
Hard Drive
Operator Requested Control Process
b
c
Protocol
Oximetry Reader
f
Analyzing & Documentation Control Process
g
Confirmation Signal
EC Measurements
j
Oximetry Analysis & Control Process
k
Confirmation Signal
Fluidic Controller Actuator2
Wireless/ Ethernet
n
EC Analysis & Control Process
o
Protocol
Fluidic Controller Sensor2
F
Printer
r
Network Connectivity Control Process
s
Sensor
G
v
Physical Report Control Process
w
Fluidic Controller Actuator1
N
Fluidic Controller
O
Fluidic Controller Sensor1
ss
oo
ii
ee
aa
dd
hh
nn
rr
vv
Aspirator
Motor Signal
I
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve
bb
cc
Rotary Valve Signal
L
ff
Calibrant & Air Introduction Control Process
gg
Valve 1 Signal
Valve 1
EC Sensor Controller Actuator
jj
Oximeter Selection Control Process
kk
Valve 2 Signal
EC Sensor Controller Sensor
Valve 2
ll
Mixing Control Process
mm
Pump
Pump Motor Flag Signal
pp
Fluid Selection Control Process
qq
J
tt
Fluid Transport Control Process
uu
K
EC Sensor Controller
mmm
iii
eee
aaa
ddd
hhh
lll
ppp
Conductive Sensors
Multimeter
Electrolyte Group A Sensors
Electrolyte Group B Sensors
Conductivity Recording
Multimeter
bbb
ccc
fff
Potentiometric Recording Control Process
ggg
Multimeter
Confirmation Signal
Analog to Digital Converter
jjj
Amperometric Recording Control Process
kkk
nnn
Electrical Signal Transformation Control Process
ooo
V Balgos 12/14/2011

Figure 20. Accident Related Loops in Control Structure

Based on the categories covered in Figure 19, the following control deficiencies were discovered for potential hazards and those were items that were relevant to the case accident are underlined. The hazards were identified for the first three control loops, and are identified in Table 7 below. The hazards for the last three control loops, E-F-G-H, m-n-o-p, and A-B-C-D, are separately located in Table 8.

Table 7. CAST Results Table for Control Loops

Note: Underlined items are relevant to case accident

Cat	Guide Words	Control Loops		
		eee-fff-ggg-hhh	mmm-nnn-ooo-ppp	I-J-K-L
1	Control Input or external information wrong or missing	• Input command missing to initiate EC process • Input command execution too early to initiate EC process • Input command execution too late to initiate EC process • Wrong input command to initiate EC process • Incorrect input command to initiate EC process	• Input command missing to initiate data conversion process • Input command execution too early to initiate data conversion process • Input command execution too late to initiate data conversion process • Noisy analog data input • Missing analog data input	• Inadequate digital data input • Missing digital data input • Input command missing to initiate data transfer process
2	Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation	• Inadequate algorithm for acquiring patient sample potentiometric measurements • Inadequate algorithm for potentiometric calibration comparison • Inadequate algorithm for patient sample potentiometric measurements	• Inadequate analog data conversion algorithms	• Inadequate control algorithm for upstream data transfer • Inadequate control algorithm for downstream data transfer •
3	Process Model incosistent, incomplete or incorrect Inadequate Operation	• CONTROLLER: Assume erroneous low potentiometric results from sensor is accurate result • CONTROLLER: Assume erroneous high potentiometric results from sensor is accurate result • SENSOR: Inadequate potentiometric result feedback • SENSOR: Assume erroneous low potentiometric results from controlled process is accurate result • SENSOR: Assume erroneous high potentiometric results from controlled process is accurate result	• CONTROLLER: Assume converted digitial data is correct result • SENSOR: Assume converted digitial data is correct result	• Incorrect data transfer confirmation logic on sensor + controller • Incomplete data transfer confirmation logic on sensor + controller • Data transfer logic is inconsistent
4	Component failures Changes over time	• ACTUATOR: Failure of attraction of electrolyte to membrane • ACTUATOR: Contaminants gather on ion selective membrane • ACTUATOR: Inadequate transfer of ion to membrane (physical, chemical, biological, electrical) • ACTUATOR: Insufficient initial amount of ion selective membrane for adequate ion transport for cartridge life • ACTUATOR: Physical damage of electrolyte sensor during the use life • ACTUATOR: Sensor membrane delamination off working electrode • CP: Electrical interference from other sensors causing inadequate potentiometric recordings • CP: Inadequate adaptation to ion selective membrane performance degradation over time • CP: Physical disconnection of electrical readings	• ACTUATOR: Delay in data conversion • CP: Missing values in conversion of analog to digital • CP: Erroneous output in conversion of analog to digital	• CP: Inadequate data transfer • CP: Incomplete data transfer • Physical electrical connection degrades over time • Physical micro controller degrades
5	Inadequate or missing feedback Feedback delays	• Missing volt reading feedback to ESC controller • Incorrect volts readings feedback to the ESC controller • Fragmented volt reading feedback to ESC controller • Delayed volt feedback to the ESC Controller • Unexpected volt feedback to the ESC Controller	• Inadequate converted data feedback signal to controller • Missing converted data feedback signal to controller • Delay in converted data feedback to controller	• Delayed feedback on data transfer • Missing data transfer feedback • Inadequate data transfer feedback
6	Incorrect or no info provided Measurement inaccuracies Feedback delays	• Missing voltage readings to multimeter • Incorrect voltage readings to multimeter • Fragmented voltage readings to multimeter • Delayed voltage readings to multimeter • Unexpected volt fee to multimeter	• Incomplete converted digital data feedback received to sensor • Missing converted digital data feedback signal to sensor • Delay in converted data feedback to to sensor	• Erroneous data transfer feedback signal to sensor • Missing data transfer signal to sensor • Delayed data transfer signal to sensor
7	Delayed Operation	• Delayed potentiometric recordings	• Delay in sending analog data tot controller	• Delay in data transfer upstream • Delay in data transfer downstream
8	Inappropirate, ineffective or missing control action	• Incorrect potentiometric reading range and timing control action command • Missing potentiometric control action command	• Missing analog data conversion execution signal action • Incomplete or inadquate analog data conversion execution signal action • Incorrect data transfer execution signal	• Missing analog data transfer execution signal action • Incomplete or inadquate analog data transfer execution signal action • Incorrect data transfer execution signal
9	Conflicting Control Actions Process input missing or wrong	• Electrical interference from exogenous factors • Incorrect Reference Electrode readings • Higher level control actions interference	• Competing data conversion execution signals • Noisy signals to controller process • Higher level control actions	• Competing data transfer execution signals • Noisy signals to controller process • Higher level control actions
10	Unidentified or out of range disturbance	• Foreign disturbances on potentiometric readings	•Electrical interferences in data conversion from exogenous factors	• Electrical interference for data transfer from exogenous factors
11	Process output contributes to system hazard	• Electrolyte consumption affects downstream sensors	• Converted data erroneosly migrates to other control loops.	• Erroneosly data transfers to other control loops.

Table 8. CAST Results Table for Control Loops Continued

Note: Underlined items are relevant to case accident

Cat	Guide Words	Control Loops		
		E-F-G-H	m-n-o-p	A-B-C-D
1	Control Input or external information wrong or missing	• Inadequate digital data input • Missing digital data input • Input command missing to initiate data transfer process	• Inadequate digital data input • Input command missing to initiate clinical conversion process • Input command execution too early • Input command execution too late	• Inadequate digital data input • Missing digital data input • Input command missing to initiate data transfer process
2	Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation	• Inadequate control algorithm for upstream data transfer • Inadequate control algorithm for downstream data transfer •	• Erroneous low result failed future case sensor calibration limits and delayed patient result error message • Erroneous high result failed future case sensor calibration limits and delayed patient result error message • Inadequate clinical result comparison to future calibration limit criteria.	• Inadequate control algorithm for upstream data transfer • Inadequate control algorithm for downstream data transfer •
3	Process Model incosistent, incomplete or incorrect Inadequate Operation	• Incorrect data transfer confirmation logic on sensor + controller • Incomplete data transfer confirmation logic on sensor + controller • Data transfer logic is inconsistent	• CONTROLLER: Assume erroneous low clinical results from sensor is accurate result • CONTROLLER: Assume erroneous high clinical results from sensor is accurate result • SENSOR: Inadequate clinical result feedback • SENSOR: Assume erroneous low clinical results from controlled process is accurate result • SENSOR: Assume erroneous high clinical results from controlled process is accurate result	• Incorrect data transfer confirmation logic on sensor + controller • Incomplete data transfer confirmation logic on sensor + controller • Data transfer logic is inconsistent
4	Component failures Changes over time	• CP: Inadequate data transfer • CP: Incomplete data transfer • Physical electrical connection degrades over time • Physical micro controller degrades	• ACTUATOR: Delay in clinical data conversion • CP: Inadequate conversion of digital to clinical results • CP: No conversion of digital data to clinical results	• CP: Inadequate data transfer • CP: Incomplete data transfer • Physical electrical connection degrades over time • Physical micro controller degrades •
5	Inadequate or missing feedback Feedback delays	• Delayed feedback on data transfer • Missing data transfer feedback • Inadequate data transfer feedback	• Delayed feedback on clinical conversion • Missing clinical conversion data • Inadequate clinical conversion data	• Delayed feedback on data transfer • Missing data transfer feedback • Inadequate data transfer feedback
6	Incorrect or no info provided Measurement inaccuracies Feedback delays	• Erroneous data transfer feedback signal to sensor • Missing data transfer signal to sensor • Delayed data transfer signal to sensor	• No clinical data feedback • Erroneous clinical data feedback • Delay in clinical data feedback	• Erroneous data transfer feedback signal to sensor • Missing data transfer signal to sensor • Delayed data transfer signal to sensor
7	Delayed Operation	• Delay in data transfer upstream • Delay in data transfer downstream	• Delay in clinical data conversion	• Delay in data transfer upstream • Delay in data transfer downstream
8	Inappropirate, ineffective or missing control action	• Missing analog data transfer execution signal action • Incomplete or inadquate analog data transfer execution signal action • Incorrect data transfer execution signal	• Missing digital data conversion execution action • Incomplete or inadquate digital data conversion execution action • Incorrect data conversion execution signal	• Missing analog data transfer execution signal action • Incomplete or inadquate analog data transfer execution signal action • Incorrect data transfer execution signal
9	Conflicting Control Actions Process input missing or wrong	• Competing data transfer execution signals • Noisy signals to controller process • Higher level control actions	• Electrical interference from exogenous factors • Higher level control actions	• Competing data transfer execution signals • Noisy signals to controller process • Higher level control actions
10	Unidentified or out of range disturbance	• Electrical interference for data transfer from exogenous factors	• Electrical interference for data conversion from exogenous factors	• Electrical interference for data transfer from exogenous factors
11	Process output contributes to system hazard	• Erroneosly data transfers to other control loops.	• Clinical Data is erroneously migrated to unknown location	• Erroneosly data transfers to other control loops.

As the above tables show, by going through each of the six control loop, and their elements, and analyzing areas of deficiencies, many potential hazards were identified. Over 175 hazards were generated through this analysis, and some were directly related to the case accident and primary contributor to patient injury. The following sections discuses the hazards found for each control loop.

For H1 and the case accident, there were nine hazards (underlined) that were identified that could have lead to patient injury. A contributing factor of the physical loss of the case accident was identified, as "inadequate transfer of ion to membrane" in the eee-fff-ggg-hhh control loops and can describe the physical blockage of the membrane. This finding may seem biased to discovery since this analysis occurred post accident. A discussion on hindsight bias will be covered in the next section that addresses this situation. Another potential hazard discovered is that the potentiometric results do not have any immediate checks to verify the validity of the data. This could lead to erroneous clinical data upstream, and may be a factor in the case accident.

From the above list, there are litanies of hazards easily identifiable in the next control loop, mmm-nnn-ooo-ppp, that focus on the conversion of the analog potentiometric values into digital values. While analog to digital converter is mature technology, there are several hazards that are identified such as errors in the data handling, gaps in the conversion process, and unsafe process models. These hazards may not be covered in the original FMECA analysis and will be a part of the gap analysis in the next section.

In the next loop, I-J-K-L, the digital data is now requested by the FC from the ESC that will eventually be sent to the SOC. During this control loop analysis, it is recognized that the software engineering knowledge is limited for the author. However, there were several hazards easily identified using the guidelines in Figure 19. It provided the structure necessary for a comprehensive hazard analysis. Some hazards identified were left nondescript such as inadequate data transfer. This may indicate missing, late, erroneous transfer processes which maybe an advantage to discover new conditions at which the control loop migrates to an unsafe state. Once the data is obtained by the FC, it is similarly transported to the SOC by control loop E-F-G-H. The same data transfer hazards were identified in Table 8.

In control loop, m-n-o-p, the transported digital data originally from the EC is now converted to usable, clinical data. The case study's proprietary software algorithm performs this conversion and analyzes the results for quality. This analysis is where the CLIA 88 standards serve as for quality guidelines, such as total allowable error. In addition, this same control loop is later used for sensor integrity check during the calibration in the subsequent wash cycle, which will later be discussed in detail as a significant factor to the case accident. Both these hazards, plus an additional one related to the case accident are underlined in Table 8.

In the last control loop for CAST, the GMC recalls the clinical data to report it upstream to the user immediately to satisfy SR2 TAT requirement. The control loop, A-B-C-D, is similar to the other control loops where data is transferred up the hierarchical structure. Therefore similar hazards were found for this control loop as were for the other data transfer control loops. It is noted that the adherence to the TAT requirement will play a significant role in the case accident and will be discussed in detail in the next chapter.

It is at this point where the control structure is assumed to perform as designed. The GMC reports the "quality controlled" analyzed patient result in useful clinical form to the user in control loop α-β-γ-δ within a desirable timeframe. After reporting the patient results to the user, the case system undergoes the normal design intended wash cycle and subsequent calibration as previously described in Figure 17 without issue.

In conclusion, the CAST methodology was applied to the case accident, and an extensive amount of hazards were identified. Of the over 175 hazards identified, nine were found to play a contributor to the case accident. In the next chapter, a further discussion on the CAST results will be conducted and generate safety design requirements and recommendations for the case system. These recommendations and requirements in the system design will manage the hazards identified in this section and fulfill the last section of the CAST analysis. Lastly, a gap analysis will be performed on case accident CAST results and the original FMECA results that were initially performed on the case system. This section will discuss any deficiencies, advantages, or variations between the two risk methodologies.

CHAPTER 5. CAST DISCUSSION

"A system is a network of interdependent components that work together to try to accomplish the aim of the system. A system must have an aim. Without an aim, there is no system. ...A system must be managed. The secret is cooperation between components toward the aim of the organization. We cannot afford the destructive effect of competition."

-William Edwards Deming

As discussed in the previous chapter, the CAST approach to system safety was applied to a case accident. Using the control structure, various contributors were identified that migrated the system to an unsafe state. The following section will explore the findings, generate improvement recommendations, and perform a gap analysis with the original risk assessment.

5.1 Evaluation of Control Structure Dynamics, Coordination and Conflicts

Based on the methodology described in Chapter 2, the CAST analysis was applied to a medical accident involving a medical diagnostic system in Chapter 4. There were nine items of deficiencies in the system control structure and they can be categorized into three distinct areas:

1. The EC sensor could not immediately detect the presence of a foreign material on the sensor surface.
2. Inadequate control of verifying abnormal potentiometric results at lower control level (Loop eee-fff-ggg-hhh).
3. Higher GMC constraint of reporting patient report before lower level control loop could verify sensor integrity.

While there were six control loops identified with the case accident, three control loops, eee-fff-ggg-hhh , m-n-o-p and A-B-C-D, were significant contributors. Not only did the individual loop contributed to the hazardous event but the combination of these hazards lead to a significant control conflict. The CAST analysis found minimal hazards in the other three control loops contributing to the case accident.

Control loop eee-fff-ggg-hhh failed to detect the presence of any foreign matter on the surface of the electrolytic sensors. An analysis of the original FMECA, later in this section, did not specifically identify the presence of foreign materials on the sensor surface as a potential hazard. Therefore, based on the requirements, the health of the sensor was acceptable and working correctly, although there was a superficial layer preventing adequate ion transfer from the blood to the membrane. Based on the author’s knowledge of the system and case accident, there is technology that engineers can use to detect the foreign mass. This hazard could have been mitigated with minimal efforts, if it were identified early on.

In addition, there are no lower level control algorithms to verify the potentiometric data for analytical accuracy and precision. This is left solely to the upper control loop, m-n-o-p to perform. Therefore there are no mitigations in the system design to accommodate this type of error at a lower control level. This is the first symptom of failed controlled actions that allowed a failure to continue to perpetuate in the overall system. A countermeasure to perform data verification at the lower level may be able to catch errors more quickly, adds an additional level of controlled action and improve the analytical accuracy of the result. However, it is unknown to the author whether this is achievable with the current system configuration and architecture.

While the previous deficiencies were shortcomings in the design, the last identified area, however, is the most significant factor in the case accident. It shows a potential conflict of design constraints that led to an accident without a component failure. The system performed as designed but a hazardous opportunity emerged due to inadequate control actions from various levels that lead to an unsafe system state.

As a reminder, the higher control loop, A-B-C-D, requires that the patient results are reported to the user as soon as they become available, in order to maintain the TAT constraint. Violation of this constraint can lead to patient injury. The reporting control action is therefore an overarching control action, and can supersede lower level constraints.

For the lower level control loop m-n-o-p, there is a constraint to ensure the patient result meets quality CLIA standards for accuracy and precision. This ensures that the measured patient result is within a certain total allowable error of the actual patient status. As described earlier, this is one of the main cruxes of the 510(k) approval process that verifies the system accurately and precisely measures the blood constituent levels within an acceptable range.

In addition, the lower control loop also verifies that the system sensors maintain physical and performance integrity. As indicated earlier, calibrations of the sensors are performed during the wash cycle after every patient sample. The intent of this process is to monitor any sensor deterioration that may have an effect on analytical results. The electrochemical sensor will degrade over the use life due to physical and chemical limitations in the design. Therefore the washing cycle helps sustain and maintain the life of the sensor. The case accident investigation found that it cannot effectively remove the foreign matter on the sensor surface with the current system configuration. The original design was to specifically wash and remove any leftover patient sample after analysis, and did not consider the need to address foreign material.

Once the wash and calibration cycle is performed, the sensor measurement is then compared to the previous calibration value, and must maintain an internal specified performance range determined by the case company. If the calibration has significant drifts or variation and fails the acceptance criteria, a warning message is only then attached to the original result indicating questionable results. This error flagging time delay provides a window of hazardous opportunity.

Figure 21 illustrates the timing sequence of patient reporting and sensor calibration that provided a hazardous condition. As stated earlier, the SR2 indicates that the case system must report the patient result within the TAT requirements of receiving a sample. Figure 21 shows this TAT requirement as X time for patient result to reach the user. The figure also shows the data reporting is before the subsequent calibration in the wash cycle.

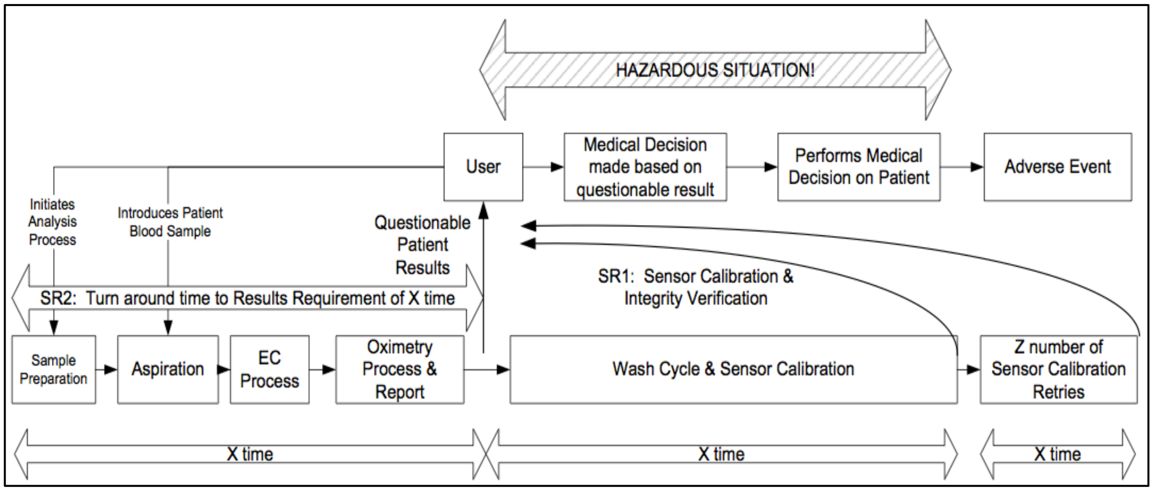
HAZARDOUS SITUATION!
User
Medical Decision made based on questionable result
Performs Medical Decision on Patient
Adverse Event
Initiates Analysis Process
Introduces Patient Blood Sample
Questionable Patient Results
SR1: Sensor Calibration & Integrity Verification
SR2: Turn around time to Results Requirement of X time
Sample Preparation
Aspiration
EC Process
Oximetry Process & Report
Wash Cycle & Sensor Calibration
Z number of Sensor Calibration Retries
X time
X time
X time

Figure 21. Case System Timing Cycles

For normal system performance after reporting a result, the time required for the Wash Cycle and Sensor calibration is the same X time. Therefore while TAT is X, verification of the sensor integrity is an additional X length of time if the sensor is normal. Any deviations will have an additional of Z subsequent calibration retries, and result in Z * X time delay.

Therefore there is a conflict in constraints in the hierarchical control structure. The higher control loop, A-B-C-D, require the patient results as soon as they become available. By adhering to this requirement, they may violate the m-n-o-p loop control calibration algorithm that lead to the above identified hazard: Higher GMC constraint of reporting patient report before lower level control loop could verify sensor verification. This is a clear violation of hierarchical control of the system, and a conflict of constraints. This supports Leveson's claim, the most common form of deficiency occurs when the process model is incomplete in terms of not defining appropriate behavior [13]. As it will be discussed later in this chapter, the process model of the controller failed to perform the correct controlled process in the context of the case accident. The patient reporting should have been delayed until the sensor could be verified for integrity in the presence of a foreign material.

If a patient result is reported, and the sensor fails the subsequent calibration, future patient results are mandatorily tagged for that specific sensor issues. Furthermore, only when the calibration cycle is complete will the warning message be attached to the original result, which is after the results are reported to the user. If all the successive calibration Z retries fails, and the sensor is disabled and cannot be used for further diagnosis. This lengthened time could provide a different type of hazard, similar to H3, to the user if the sensor was needed for another patient analysis. A question that arises then, is why not simply wait until the first wash calibration is completed to ensure sensor integrity?

The answer lies in the consideration of the other control loop, A-B-C-D, where the General Master Controller reports the patient results to the user. As mentioned earlier, time is a critical factor in healthcare and the TAT is a crucial requirement that must be maintained by the case system. Therefore, as soon as the patient results are ready, the system is designed to immediately send them to the medical staff regardless of the subsequent calibration outcome. The results are then used in a medical decision action on the patient. Since the intended use of the system is in critical areas of the hospital, the medical staff needs a fast TAT to react quickly emerging medical situations.

Designing the system to comply with the TAT parameter first rather than analytical verification is a competitive business decision. In the POC environment, competing diagnostic analyzers of the case system have, in general, similar analytical accuracy and performance. This is verified by the adherence to the federal regulated CLIA 88 requirements. Therefore, a significant marketing leverage is the TAT where the users historically prefer systems with a faster TAT. Consequently, having a fast TAT is crucial in maintaining a competitive edge in the market. Therefore the case system designers and engineers developed a system and default configuration to meet this market demand.

If the sensor calibration is suspect, the case system control structure assigns a warning message indicating a questionable patient data only after the calibration completes and fails the performance criteria. But this delay in syncing the sensor integrity check with the result may contribute to a hazardous situation. For example, if the patient was erroneously reported to have a low electrolytic level, the medical staff may need to quickly intervene by administering a high electrolytic solution to the patient. The medical staff may not see the patient results tagged with a warning message in time, or never see it at all. The patient may then experience a negative reaction to the erroneous medical treatment that could lead to injury or death.

In addition to patient harm, there are further potential consequences. After the system verifies sensor malfunction, it flags the questionable patient result. Without the knowledge of the case system and the time gap between sensor calibration after wash and flagging the data, an external investigator may then question why did the medical staff perform the harmful procedure based on suspicious data. This investigation on the adverse event may lead to false blame on the medical staff for administering the harmful procedure that lead to patient injury or death. Remedial actions may lead to more system training, reprimand or demotion, legal liability claims or even termination of the medical staff. These mitigations, however, do not solve the issue, and merely address the symptoms by focusing blame on the users. This is a common and reoccurring issue in accident analysis, where blame is falsely placed on the users and the real accident contributors are not understood and addressed [7].

In summary a hazardous situation occurred due to the conflicting constraints in the hierarchical control structure. By allowing patient results to be reported immediately by the higher control level, it may undermine the subsequent calibration sequence at the lower system level. The CAST results facilitated in understanding the complexity of the control structure, and the relationship between the numerous control loops. By analyzing the potential hazards at each level, the divergence in constraints within the structure was readily observed. These constraining linkages maybe describe one of the medical adverse events described in the FDA MAUDE database. But due to privacy laws, this cannot be confirmed.

A summary list of the analysis results and events is provided, but is not intended to suggest a linear chain of events. The intent is to show the numerous conditions that occurred before the accident and events may have happened sequentially, in parallel, or random. As described earlier there are several, dynamic situations that initiated the hazardous events.

- Foreign mass on sensors preventing adequate blood ion transfer.
- Obtain erroneously low potentiometric (analog) results.
- Erroneously low analog results converted to erroneously low digital results.
- Erroneously digital information sent to FC, then to SOC.
- SOC converts digital results to erroneously low clinical results.
- Erroneously low clinical result transferred upstream from SOC to GMC.
- GMC reports erroneously low clinical result to user (medical staff).
  - Adverse medical decision is made based off erroneous result.
  - Adverse medical procedure applied to patient.
  - Adverse reaction to the procedure by the patient.
- Wash & Calibration Cycle begins after sample report.
- Calibration drift error checks on the sensor fail acceptable performance criteria.
- After X time after reporting result, the result is then flagged with warning message.

By performing a CAST analysis on case accident, it elucidated several hazards that contributed to the case accident. Some of the hazards were due to inefficiencies in the lower control levels, and some are a direct incompatibility of competing constraints. With this knowledge of how these hazards happened, mitigations can be designed into the system to prevent future occurrences.

5.2 New Design Requirements and Recommendations

The next step in the CAST analysis is new system safety requirements can now be generated to prevent the identified CAST hazards. These requirements should control the hazards and prevent the system from migrating to an unsafe state. Based on the previous section, the following requirements were generated and are located in the table below.

Table 9. New Design Requirements based of CAST Analysis

#	General Hazard Identified by CAST	New System Design Requirement
1	The EC sensor could not detect the presence of a foreign material on the sensor surface.	The system shall be able to detect the presence of foreign material on the sensor surface with X% confidence level.
2	Inadequate control of verifying abnormal potentiometric results at lower level.	The system shall verify all potentiometric results for deviance at lower control levels in addition to the SOC.
3	Higher GMC constraint of reporting patient report before lower level control loop could verify sensor integrity.	The system shall allow the sensor integrity verification in the wash cycle to complete before patient results are reported to the user.

While there were nine hazards discovered during the CAST analysis that were related to the case accident, they were generalized into three categories as described in the previous section. The new system requirements were generated at this same high level with the potential to be further specified to the sub-system level. Some of the sub-system levels requirements and recommendations will be discussed in detail below.

The CAST analysis showed that the case system requires a new functionality to detect foreign substances on the electrolytic sensor. While it is preferred to design the system to prevent foreign matter from occurring on the sensor at all, mitigation can be incorporated immediately to detect its presence in case this type of hazard emerged. Therefore the new developed requirement state that “the case systems shall be able to detect the presence of foreign material on the sensor surface with X% confidence level”. This indicates a new functional check on the sensor for the lower level ESC controller. A further derived subsystem level requirement and or specification may establish the sensor performance criteria. For example, the sensor may need to perform within a targeted electrical signal range to signify the presence of a foreign substance on the superficial layer. Another subsystem level requirement may establish the frequency of the check, definition of various severity levels, and their subsequent actions such as error flagging, initiating system washes, or alert the user of a potential compromised sensor. This detection capability will now allow the system to manage any issues with the ion transport process. With the author's knowledge of the system and technology, this is a potential manageable design change that can be implemented into the current case system with minimal time and resources. For future development projects, this new safety requirement should still apply, but a focus on preventing the foreign matter introduction into the system needs to be considered.

The second design requirement calls for system capability of verifying the integrity of the sensor potentiometric results earlier in the sample process. It was found that the data verification was performed after initial acquisition and several data transfer transactions to a higher-level control level. By emplacing an earlier voltage check prior to clinical conversion, it maybe able to detect erroneous errors earlier and flag the patient result as "questionable". With the earlier requirement of detecting foreign substances on the sensor, acceptable potentiometric ranges may be established and used to verify the integrity of the current results. This would add additional layer of safety control to prevent an isolated failure from becoming a systemic issue. This requirement may be a complementary design change to the previous one, but may require a more effort and resources based on the current case system configuration.

The last new system requirement is needed to resolve the conflict and manage the various constraints across the case system control structure. Since the reporting of erroneous patient results is a pre-established high level system hazard (H1) before the CAST analysis, and a significant contributor of the medical accidents to patients, the new system design requirement shall enforce the system to mandatorily complete the sensor integrity verification in the wash cycle before reporting results to the user. This will ensure the accuracy and integrity of the clinical data that will be used for subsequent medical procedures.

After investigation of the case system by the author, there is already a design option in the case system configuration that allows the user to delay the patient result reporting until the sensor is calibrated and verified. However, the default system configuration is to report the patient results immediately to satisfy the market driven TAT requirement in derived by H2. The user has to take additional steps to enable the option to delay the patient result reporting until after the wash cycle. Based on the CAST findings and previous discussions, this is a counter-intuitive default system configuration setting that may lead to a hazard. Since it was shown that there is a window for hazardous opportunity to occur (see Figure 21), system safety could be improved by allowing the system to fully verify the sensor's performance post-analytical processes. Adherence to TAT requirements is critical, but should be secondary to the accurate and precise analytical diagnostic performance of the case system.

As mentioned earlier, competing analyzers have similar diagnostics performance as defined by regulation standards. Therefore, a primary differentiator is the TAT for patient results. The market demand has dictated that a faster time to result is desirable, and has significant impact on the case system's success, market penetration and overall profitability. The business and social pressures to meet the TAT takes priority, and is apparent in the default configuration of the case system. The engineers of the case company did not intentionally compromise analytical safety, but maintained marketability and competitive edge by meeting the user needs.

However there may be situations where TAT is a more frequent and significant safety concern than the analytical performance of the system. To further mitigate this dynamics in constraints, the ultimate case system configuration should be left for the specific end user (i.e. medical staff). The case company should still provide a default system configuration that allows the case system to complete sensor calibration and prevent the window of hazardous opportunity. A recommendation, but not a requirement, is to allow the user to opt out of the sensor integrity check, rather than having the user opt into the integrity check. This would enforce a conscientious acknowledgement of the user to make the critical safety trade off decision between sensor check and TAT. A clear warning on the consequences of selecting this configuration should be provided by the case system, and frequently communicated by the case company. This would alleviate the case company of potential liability issues and allow the user in the context of their specific environment to make the safety tradeoff. The new recommended default system configuration could have prevented some of the medical accidents that catalyzed the FDA recall. However, due to privacy concerns, this cannot be confirmed.

While overall safety should not ideally be a user-selected option, a safety tradeoff is necessary with the current case system design. The recommendation for the user to have the option of selecting out of the sensor integrity check may appear to reduce safety in terms of analytical integrity. But there is a safety tradeoff in the time delay of needed medical information and may at times be more significant. In a non-case accident example is the patient may have unknown cerebral hypoxia where there is a reduced oxygen supply to the brain and irreversible brain damage occurs within five minutes [41]. Time to patient diagnosis therefore plays a critical role in adverting patient injury. The administering of oxygen to this patient may be life saving if the patient does in fact have low oxygen levels, and a faster time to oxygenation is desired. If the case system erroneously reports low levels of oxygen in the patient, the administering of unnecessary oxygen to the patient for a certain time is generally harmless. Therefore, the delay in patient reporting can play a significant safety factor more so than analytical integrity. It is noted that oxygen toxicity is plausible, but the levels of administered oxygen is assumed to be at normal clinical levels. This condition dynamic is a tradeoff that the users may need to analyze during the configuration of the case system.

It is acknowledged that the current design is limited in providing complete safety in terms of TAT and sensor verification. This has been a difficult socio-technical issue to analyze in terms of priority and significance. The author notes that this issue may never be resolved with the current case system configuration. The total safety of the system needs be considered but potentially juxtaposes market competition, profitability, and overall success of the case system. It is recommended that this issue needs to be communicated, debated, and analyzed extensively amongst the executive and technical stakeholders for any new diagnostic system development.

Since time is an essential factor to the system performance and calibration, another subsequent design recommendation based on the CAST results is to reduce the time required for sensor calibration (i.e. X time in Figure 21). While there is a physical and chemical limitation due to the sensor membrane diffusion rate, there maybe alternative methods to improve upon wash calibration sequence that would reduce the overall time. This may be reducing the volume of electrolyte ion selective membrane, alternating surfactant components in the wash solution, or increasing the solution flow in the wash cycle. These recommendations may not be feasible with the current case system, but should be considered for future diagnostic analyzers.

Another safety design recommendation is to perform a quick sensor calibration immediately before the aspirating any blood sample. As mentioned earlier, with the current system design, sensor calibrations normally occur only in the wash cycle after sample. If no sample is programmed for greater than a pre-established time, the case systems proprietary control algorithms perform an automatic calibration sequence. However, between these scheduled events, a foreign substance could be over sensor membrane preventing correct ion transport process. Therefore, by performing a calibration immediately <u>prior</u> to all samples, any sensor performance deviations could be caught and potentially prevent erroneous results to be reported. If this scenario occurred, the system could adjust in several ways:

- Prevent the user from inputting sample that would be otherwise wasted on a questionable sensor.
- Accept the patient sample, but immediately flag the results as questionable until the wash calibration can verify sensor integrity.
- Accept the patient sample, but disable the deviated sensor from reporting any results and inform user of the compromised sensor.

As mentioned earlier, the presence of the foreign substance on the electrochemical sensor was a significant factor in the case accident. A recommendation for future system development is to design features that would prevent the foreign material from manifesting at all. This would prevent the situations such as the case accident from ever occurring, and ensure the safety of the analytical diagnosis of the patient. However, this may not be feasible with the current case system, and these types of efforts should be performed in new developing projects.

Furthermore, after observing the tremendous benefit from a CAST analysis from half of the loops in the control structure with a single hazard (H1), it is recommended to continue the CAST analysis on other system hazards on all control loops. This would discover more hazards from the systems, and lead to a more safety design requirements and mitigation features. With a fully complete CAST analysis on the entire control structure, a comprehensively safe system would be developed.

Finally, due to the scope and objective of this thesis, the CAST analysis was only performed on the technical system. CAST can be applied on a grander scale to discover factors to socio-technical hazards. Examples of this are controls in the production processes, feedback cycles between design and manufacturing departments, quality audit control loops, and interactions between executive management and technical bodies. This is applicable to a company's organization, between companies and regulatory bodies, and all the way up to government legislation. Leveson developed a general safety control structure in a regulated, safety critical industry that describes these connections and is illustrated in Figure 22 below. A complete CAST analysis on the entire socio-technical control structure will elucidate many more hazards. By understanding the control issues, requirements to maintain the system at a safe state will ultimately provide a safer, more effective medical product to the end user.

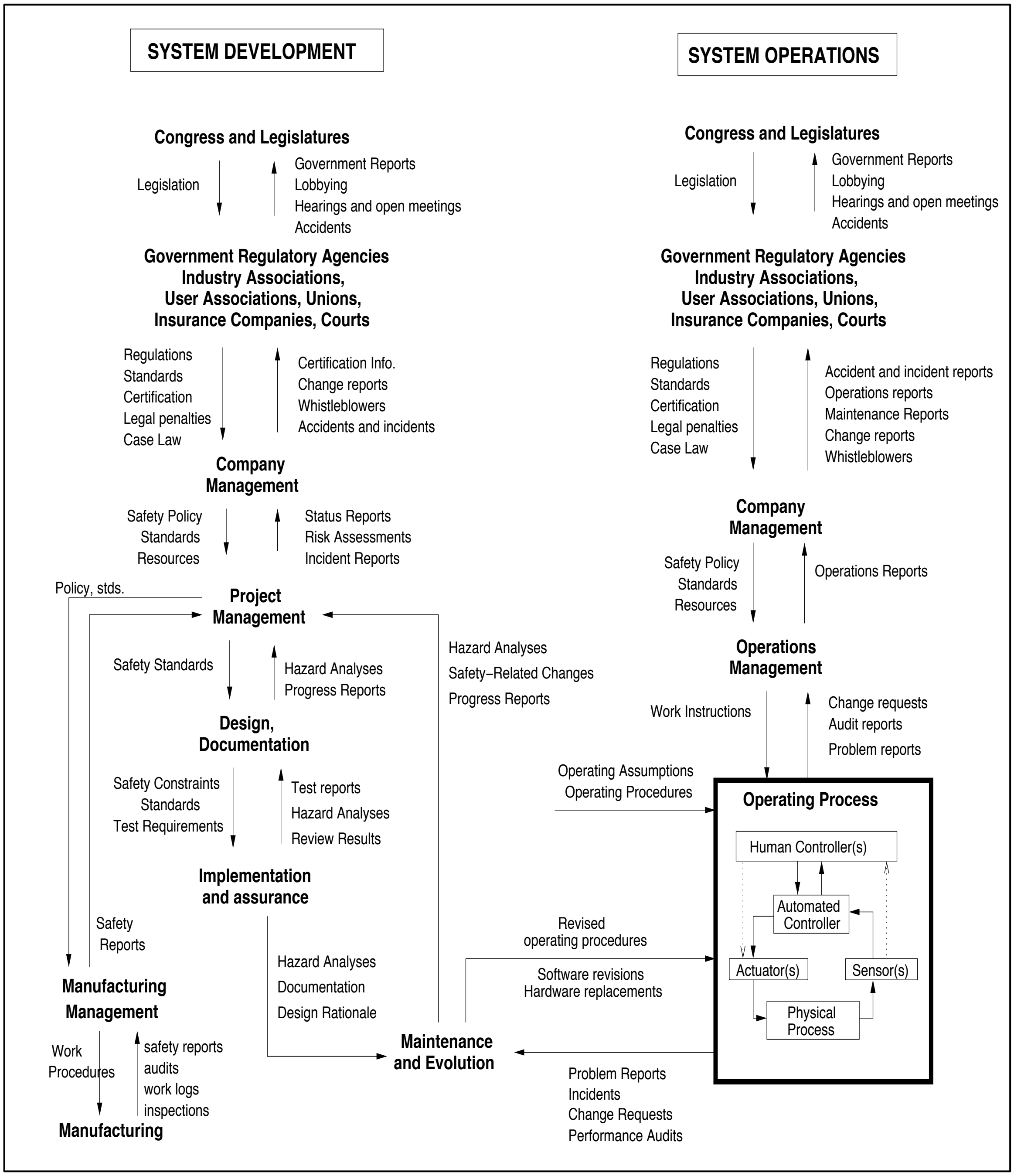

Figure 22. General Socio-Technical Control

In summary, after performing the CAST approach to system safety and identifying several new hazards, several new design requirements and recommendations were generated. Some may be applied to the current case system to mitigate issues as seen in the case accident while all can be applicable to developing or future diagnostic blood analyzers. These requirements and recommendations are listed below in no particular order.

1. Patient Result Reporting Time
    - Establish the case system settings so that the default configuration prohibits the reporting of patient results until after the sensor calibration in the wash cycle is complete. The tradeoff is it will increase the current TAT length two fold.
    - If shorter TAT is more critical, allow the user the ability to "opt out" of this configuration setting. This would force the user to acknowledge and accept the inherent risk with faster TAT.
2. Design control algorithms in the lower level controllers (specifically Control loop eee-fff-ggg-hhh) to verify the absence or presence of foreign material on the surface of all electrolytic membranes.
3. Initiate a sensor calibration immediately before the patient sample.
4. Decrease the overall Wash Cycle and Sensor Calibration time, thereby reducing the "window of hazardous opportunity".
5. As mentioned earlier, the control structure presented was limited to the thesis boundary. Therefore, perform CAST analysis with more resources and more information of the system.
6. Continue and complete a full CAST analysis on all control loops in the technical system.
7. Perform a full CAST on the socio-technical control structure.
8. For new system development, implement design to prevent the foreign mass from appearing on the electrochemical sensor.

These new design requirements were driven by the application of the CAST analysis. The past discussions have showed CAST can be used to design safety into the complex medical case system. The next question that emerges is how do the CAST results compared to the original risk analysis performed by the case company. A gap analysis on the CAST and industry standard FMECA methodology will be performed later in the chapter.

5.3 Hindsight Bias Discussion

As noted in the last chapter, the hazards for the medical accident were identified in the CAST analysis. It may seem it is a biased investigation since the CAST analysis was performed post accident with the author's knowledge of the case accident. However, the methodology of the CAST dispels hindsight bias that may occur.

Hindsight is the ability to look back on a sequence of events that lead to a known outcome [42]. This retrospective lens allows the analyst to understand the nature of the situation, the people involved, and the context at why specific decisions were made at that time. By focusing on the cause-consequence equivalence, this allows the analyst to focus only on a linear chain of events that lead to the undesired event. It assumes a "bad" process leads to a "bad" outcome. However, this simple cause-consequence is problematic as the chain of events leading to an accident is not unequivocally clear in complex worlds. Sometimes "bad" processes may not lead to a bad consequence. Sometimes "good" processes lead to undesired outcomes, like adhering to the TAT requirement. This powerful but biased perspective deters the ability to objectively understand the problem by converting ambiguous, complicated complexities into a simple, linear chain of events.

One of the strengths of the CAST analysis is that uses a systems approach to accident investigation. By utilizing a non-linear approach to understand why the control structure performed what it thought was the correct action, CAST helps to objectively understand all the factors in the events leading to the incident. By using this holistic tactic, it deters the linear hindsight bias, false blame on people, and elucidates the real flaws in the system.

With the case accident, it was the case systems programmed logic to avoid a hazardous condition by reporting patient results as fast as it could that undermined lower level controls such as sensor calibration sequences. This "good" process should have resulted in a "good" outcome, but it did not. By address the TAT requirement, the system developers did not intentionally compromise safety of analytical performance. The CAST analysis therefore provides the investigator or analyst (i.e. the author) an unbiased approach to risk analysis due to its rigid established structure of control loop examination as seen in Figure 19. With the unprejudiced guidewords, a non-partisan analysis of the accident can be performed, and hazards objectively identified.

5.4 Gap Analysis of CAST and FMECA

As mentioned in Chapter 3, the case company performed an extensive FMECA on the case system. This effort complied with the FDA's 510(k) submission, specifically regulation 21 CFR 820.30(g) on performing a risk assessment on the new medical system. It is a reminder to the reader that this FMECA technique is recommended in ISO 14971, and that the FDA approved risk assessment for the case system for U.S. market introduction. The case company complied with all current federal regulations to risk and hazard analysis.

The FMECA analysis was performed on all levels of the system, including most notably at the system level. The author reviewed the original FMEA analysis, and at the time of the risk analysis, less than 70 system level hazards were identified. For confidentiality reasons, the actual FMECA findings will not be displayed for the case system. However, the identified system level hazards were classified in the following categories:

- Electrical safety (14)
- Biohazard exposures (9)
- Chemical hazards (3)
- Noise (1)
- Storage conditions (3)
- Preventative maintenance (2)
- User operations (3)
- Packaging & labeling (3)

- Handling (3)
- Operating conditions (4)
- Calibration Processes (6)
- Sensor Performance (4)
- Transportation (3)
- System operation (1)
- Patient Error Handling (6)
- Data Process (4)

These original FMECA findings were generated over the life of the development cycle. Several members representing all disciplines of engineering, science, and business conducted the risk analysis. As indicated by FMECA structure and methodology, single failure events are only documented to understand its effect to the system and hazards that occur without failures cannot be discovered.

After careful review, there were only a few specific FMECA findings that were related to the case accident. They are generalized in Table 10 below.

Table 10. Identified FMECA Hazards of Case Accident

#	Failure Mode	Effects of Failure	Potential Causes	Severity	Frequency	Detectability	Current Design Controls
1	Sensor calibration drifting	Inaccurate Measurement	Working electrode membrane degradation	Hazardous	Moderate	Highly Frequent	Dynamic internal proprietary calibration program
2	Sensor do not calibrate after sample	Inaccurate Measurement	Slow response of sensor	Hazardous	Highly Frequent	Frequent	Dynamic internal proprietary calibration program
3	Failure pattern do not detect sensor malfunction	Inaccurate Measurement	Sensor calibration limits are not optimized	Hazardous	Frequent	Frequent	Historical analytical performance design
4	Incorrect Calibration Retry	Delayed patient results	Sensor malfunction	High	Moderate	N/A	Disable sensor after Z retries

As Table 10 indicates, there were only four identified FMECA items that have causal linkage to the case accident. While FMECA #1 did forecast a possible degradation of the working electrode membrane that affects the sensor calibration, it did not encapsulate the possibility of a physical blockage of the ion transfer as a potential hazard, which led to the case accident. The FMECA #1 specifically identified a condition when the membrane integrity itself degrades to the point where the ion transfer is ineffective in accurately diagnosing the patient's blood status. The cause could be physical deterioration, chemical corrosion of the sensor and or contaminants physically damaging the membrane. The FMECA result thus described a specific type of hazardous condition (i.e. component failure) that could occur at the lower level. Therefore, this type of analysis requires intimate knowledge of the technical system, such as an expert in sensor and electrochemistry for this particular FMECA item. As mentioned earlier, this was a limiting factor of this methodology.

The CAST analysis offers a systems level viewpoint of this hazard. As Table 7 shows for control loop eee-fff-ggg-hhh, the potential identified hazard is:

"Inadequate transfer of ion to membrane (physical, chemical, biological, electrical)"

By focusing on the broader function of the controlled process of the control loop (i.e. ion transfer), it compels the analyst to take a broader view on the causal analysis when determining inadequate conditions. Decoupling the controlled process (ion transfer) from the physical form of the actuator (i.e. electrochemical sensor membrane), allows the analyst to identify a multitude of hazards at the various elements in Figure 19. Hazards can include physical component failures of the sensor as previously found with FMECA, but also hazards without component failure, such as material deposits on the surface of the sensor. As mentioned earlier in the case accident investigation, the membrane was found to be in perfect physical working condition, but the ion transfer was inadequate. Therefore, a hazardous condition was present without a component failure. By focusing on what could adversely affect the ion transfer function, the analyst may define hazards that include physical blockage (i.e. foreign mass), chemical neutralization of the ion affinity, biological contaminants, and or electrical interference. By focusing on the function of the control loop on this particular element, CAST provided an implementation- neutral approach to identifying hazards, and did not require the specialized knowledge of the system (i.e. electrochemistry technology). This approach allowed more hazards to be discovered with fewer resources.

FMECA #2 identified a potential failure mode that the sensor does not calibrate after sample, and linked the cause to a slow response of the sensor. The FMECA item specifically focused again on the component (i.e. sensor), and failed to recognize the functionality issue: inadequate ion transfer in terms of time requirements. It assumed that the component failure identified in FMECA #1 – membrane degradation - was the cause of no calibration. It did not take into account that the sensor may be in perfect working condition, which was true in the case accident, but it was the controlled timing process of the ion transfer that was the issue. In addition, there may be other previous or exogenous factors that may have caused the sensor to not calibrate after sample. Finally since it was a single failure, isolated view, it assumed that all previous processes were correct.

The CAST results also identified a similar hazard in control loop m-n-o-p as a "delay in feedback to the (SOC) controller". Similar to the above CAST discussion, this analysis focused on the malfunction that causes the hazard, as oppose to the component failure. This opened up more possibilities and sets the mind frame for the analyst to determine possible system-level causes. While this certainly included a physically "slow sensor" as FMECA #2 indicated, the broader CAST analysis can further find more hazards such as inadequate wash cycle, inadequate component of calibration solution, and or a physical barrier on the sensor (i.e. foreign mass). This neutral approach again, guided the analyst to take a systems approach to investigate possible hazards.

In addition to "delay in feedback", another CAST finding was the "inadequate input" into the controller. This potential condition questioned the validity of the incoming data input (i.e. sensor calibration) and the analyst can investigate potential erroneous exogenous factors (such as electrical interference) or as in the case accident, upstream influences. If the sensor failed to detect the presence of a foreign substance, this failure is passed along to ensuing sequences as shown in Figure 12. Case System Control Structure. With the information to detect the foreign matter, it can be coupled to this hazard to verify any input as adequate or not. With these types of upstream and multiple hazards identified, system level mitigations can be implemented. The structure of the single fault, isolated view of the FMECA methodology prevented this type of analysis. With a systems approach CAST method, the case accident may have been averted.

A failure mode was identified in FMECA #3 if the case system could not detect a failure pattern during the sensor calibration sequence. The identified cause was the calibration limits were not optimized. The case accident still occurred since this analysis assumed the incoming data input was adequate, as was similarly found in FMECA #2. CAST also identified this hazard in control loop m-n-o-p as "erroneous low result failed future case sensor calibration limits and delayed patient result error message" (see Table 8). As previously mentioned, if a CAST approach were taken, the analyst could have questioned the validity of the incoming data and questioned whether an upstream failure was passed along to the current calibration process. The original FMECA focused only on optimizing the algorithmic limits, but failed to identify the importance of whether that calibration data was even good at the start of the process. It did not consider whether there were potential upstream errors, hence why the case accident still occurred with the FMECA #3 hazard identified.

The final FMECA #4 item relevant to the case accident was the number of calibration retries that occurs if the system detects a deviated sensor. The limited tries allows time for the sensor to return to a normal, safe state, but is also emplaces a constraint to allow the system to disable the errant sensor and continue to use the other stable sensors. This hazard was not a part of the CAST analysis since the Wash Cycle was assumed to work as intended. However, this hazard would have been identified if the CAST analysis were performed for the entire control structure for all hazards.

The case company was dutiful in risk analysis and completed a FMECA effort in accordance to FDA guidelines. Then why did the case accident still occur? As mentioned the structure of FMECA only analyzes a single fault, based on the linear chain of events scenario. The original FMECA analysis did identify sensor failures, but it focused more on the actuator (i.e. electrochemical sensor) rather than the controlled process (i.e. ion transfer). In addition, it assumed the incoming data input into the controller was “good” without question. By doing so, a much narrow, low-level analysis was performed, and therefore limited amounts of hazards defined. Furthermore, the FMECA methodology did not consider the implications of the business demands of TAT performance on the sensor verification process. This conflict of constraints cannot be identified by FMECA because there were no component failures. The design of the system failed to avert the case accident for this reason. In short, the reductionist view of FMECA has limitations in discovering more complex hazards.

For comparison, the author performed the CAST analysis of H1 and was able to identify over 175 individual system hazards, with nine directly related to the case accident. In addition, the 175 hazards found were only for the six identified control loop of almost 20 possible control loops. The CAST analysis produced significantly more system level hazards than the 70 found via the industry standard FMECA methodology in less than half of the identified loops in the control structure. The sheer voluminous findings indicate that the systems thinking model in the CAST methodology was more effective in discovering hazards.

Furthermore, in addition to the number of hazards, the type hazards identified were significant. This CAST analysis was able to identify single component factors (inability to detect foreign material on sensor) that were a critical factor in the case accident. Moreover, this non-reductionist approach allowed the analyst to consider upstream failures, and how it affected the downstream dynamics with the potential to migrate the system to an unsafe state. Therefore, this case accident and subsequent CAST analysis illustrated an example were there were inadequate system control of variables, and proves the fact that the loss of safety was a control issue.

Finally, the systems lens was able to identify additional hazards that did not include a component failure, a limitation of the FMECA practice. The control loop template in Figure 19 provided a guideline for easily recognizing system level hazards and conflicting constraints amongst the various control loops. Viewing safety as a control problem help elucidated many system level hazards. Therefore, the CAST application to risk analysis can provide a more rigid evaluation for a variety hazards that occur with and without failures.

In the last gap analysis comparison, as mentioned earlier, the FDA approved FMECA technique required significant amount of company resources to execute. From professional experience and knowledge of the case company, FMECA is a long, arduous process (from months to years) requiring representation from every discipline of engineering and business. In addition, during the FMECA process, there is less structured approach to identify hazards when compared to CAST. This was a considerable effort and cost for the case company, yet the initial findings failed to identify the significant contributor case accident of conflicting system control actions. In contrast, the CAST analysis was performed solely by the author with considerable less time and resource and was able to identify more than twice the number of hazards. The analysis was only performed on a half of the loops in the control structure. It is assumed that only more hazards will be identified when all loops of the control structured is analyzed, with additional resources, and focusing on other hazards beside H1.

As mentioned earlier, the case accident was a multifold issue that included a single component failure (inability to detect foreign mass on the sensor surface), and a scenario of competing control actions (TAT and sensor verification during the wash calibration conflict). The latter of the issue did not incur any failures of the system, but was an incompatibility of system controls that migrated the system to an unsafe state. While limitedly effective and regulatory approved, FMECA was unable to detect this type of hazard by its reductionist design. Its linear chain of events modeling was limited to only single fault analysis. The use of systems thinking model to hazard analysis, such as CAST, was be able to identify more hazards, including non-linear scenarios. The results from the CAST analysis of the case accident illustrated a superior method to recognize a multitude and disparate types of hazards more effectively than FMECA, with less time, cost, and resource invested.

In addition the safety tradeoff between TAT and sensor integrity was and still is a complicated challenge. The default system configuration to delay syncing the sensor calibration to the patient results poses a significant hazardous condition. However, the adherence to the TAT constraint is critical in certain context of the intended value delivery. In addition, the business aspect and increased profitability of a quicker TAT may have influenced and impacted the engineering design for system safety and priorities. This is a critical discussion that needs to be held amongst principal stakeholders for new diagnostic development.

Some of the design requirements and recommendations derived from the CAST analysis can be immediately implemented into the current case system. The default system configuration can be re-optimized to prevent a window of hazardous opportunity. If the user desires to address the other conflicting constraint of a fast TAT, that flexibility is present and available. Furthermore, these requirements and recommendations for improved safety can be used for future development of new diagnostic analyzers. With these hazards identified, the knowledge gained may be utilized to prevent tragic incidents such as the case accident.

CHAPTER 6. Conclusions

"The scientific man does not aim at an immediate result. He does not expect that his advanced ideas will be readily taken up. His work is like that of the planter — for the future. His duty is to lay the foundation for those who are to come, and point the way. He lives and labors and hopes."

-Nikola Tesla

This thesis has discussed the evolution in medical technology and specifically the need for safe and effective diagnostic systems. With innovation in technology, come increasing concerns of maintaining system safety. Traditional, linear risk analysis methodologies recommended by the regulatory bodies may not be capable of identifying complex hazards with multiple failures, or hazards that occur sans failures. A new, systems approach to safety is needed to adapt to the increasing complexities and emerging dynamics of this technology.

Based on the findings of the CAST analysis to a real life case accident involving a medical diagnostic analyzer, the systems approach was superior to the industry standard FMECA practice in identifying hazards. It was able to detect significant contributors to the case accident in form of failures (foreign material on the sensor), and non-failures (a conflict in controlling actions). From these identified hazards, new system safety requirements, such as establishing safer control settings, were generated to control the system from migrating to an unsafe state. This is the ultimate value that the CAST analysis can provide for the design and development of complex medical systems.

The CAST approach was able to distinguish more than twice the number of system level hazards with considerable less time and resources. Multiple failure hazards and hazards that occurred without component failures due to conflicting system control actions were confirmed. The CAST methodology was able to increase not only the quantity of hazards found, but identify complex and non-linear hazards. The current FMECA is incapable of producing these results based on its inherent design and structure.

In conclusion, the answer to the research question of this thesis confirms that the CAST and the STAMP approach was more effective in designing safety in medical diagnostic systems than the current industry standard practice of FMECA. The quantity and quality of hazards discovered with the CAST methodology are overall more productive in generating effective safety design requirements and recommendations in preventing medical accidents. A holistic approach in risk analysis can provide more value than the current linear techniques. With this systems methodology, the case accident could have been averted. Further expanding the CAST practice to other areas of medical technology development may prohibit future massive, disastrous medical accidents similar to those that gave birth to the FDA. Finally, the systems way will prevent history from repeating itself, and lead to new heights of safer and more effective medical care and innovation.

Finally, after this thesis experience, it further confirms to the author that the system thinking is a valuable mental model and can be applied to a variety of applications in addition to safety.   This is justified in the System Design and Management program, professional work experience, and in personal activities. Understanding the dynamics and interfaces of system components, one can design the system accordingly to produce value and benefit to many stakeholders. In other words, it enables the adage "Think globally, and act locally."

REFERENCES

[1] Human Genome Project Information. (2011). *Oak Ridge National Laboratory*. Retrieved from http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml

[2] U.S. Food and Drug Administration. (2011). *Approval of Incivek (telaprevir), a direct acting antiviral drug (DAA) to treat hepatitis C (HCV).* Retrieved from http://www.fda.gov/ForConsumers/ByAudience/ForPatientAdvocates/ucm256328.htm

[3] Genzyme Corporation. (n.d) *Fast Facts About Genzyme Corporation*. Retrieved from http://genzyme.com/corp/structure/fastfacts.asp

[4] Rouse, W. B., & Cortese, D. A. (2010). *Engineering the system of healthcare delivery*. Amsterdam: IOS Press.

[5] World Health Organization. (2000). *The World Health Report 2000 - Health systems: improving performance*. Retrieved from http://www.who.int/whr/2000/en/

[6] Kohn, L. T., Corrigan, J., & Donaldson, M. S. (2000). *To err is human building a safer health system*. Washington, D.C.: National Academy Press.

[7] Leveson, N. (2012). *Engineering a safer world: Systems thinking applied to safety.* (book draft). Retrieved from http://sunnyday.mit.edu/safer---world/index.html, to be published by MIT Press in 2012.

[8] Medical Devices – Application of Risk Management to Medical Devices. (2007). EN ISO 14971:2007. Brussels, Belgium : ISO.

[9] Nagreha, N., Parmar, M., (2011) *Study of Medical Device Recalls by FDA Over Last Four Years (2008-2011) - Applied Clinical Trials.* Applied Clinical Trials - Global Information & Resources to Develop, Execute and Manage Clinical Trials. Retrieved from http://appliedclinicaltrialsonline.findpharma.com/appliedclinicaltrials/Online+Extras/Study-of-Medical-Device-Recalls-by-FDA-Over-Last-F/ArticleStandard/Article/detail/740631

[10] U.S. Food and Drug Administration. (2011). *FDA History.* Retrieved from http://www.fda.gov/AboutFDA/WhatWeDo/History/Origin/ucm054819.htm

[11] Ballenstine, C. "Taste of Raspberries, Taste of Death. The 1937 Elixir Sulfanilamide Incident." *FDA Consumer Magazine.* (1981). Retrieved from http://www.fda.gov/AboutFDA/WhatWeDo/History/ProductRegulation/SulfanilamideDisaster/default.htm

[12] Kolata, G. (1987). THE SAD LEGACY OF THE DALKON SHIELD - New York Times. *The New York Times*. Retrieved from http://www.nytimes.com/1987/12/06/magazine/the-sad-legacy-of-the-dalkon-shield.html

[13] Brown & Szaller : The Dalkon Shield Saga. (n.d.). *Brown & Szaller : Accident Attorneys in Lakewood, Ohio*. Retrieved from http://lawandhelp.com/pages/publications/dalkonshield.html

[14] The Dalkon Shield story: a company rewarded for its faulty product - A.H. Robins Company Inc. lawsuit | Center for Medical Consumers | Find Articles. *Find Articles*. Retrieved from http://findarticles.com/p/articles/mi_m0815/is_n204_v21/ai_18349380/

[15] U.S. Food and Drug Administration. (n.d.). *FDA Basics for Industry.* Retrieved from http://www.fda.gov/ForIndustry/FDABasicsforIndustry/ucm234629.htm

[16] U.S. Food and Drug Administration. (n.d.). *Regulatory Information.* Retrieved from http://www.fda.gov/RegulatoryInformation/Legislation/default.htm

[17] U.S. Food and Drug Administration. (2010). *About the FDA Organization Charts.* Retrieved from http://www.fda.gov/AboutFDA/CentersOffices/OrganizationCharts/default.htm

[18] U.S. Government Printing Office Home Page. (n.d.) *U.S. Code of Federal Regulations (Annual Edition).* Retrieved from http://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR>

[19] U. S. Food and Drug Administration (n.d.). *Overview of IVD Regulation*. Retrieved from http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/IVDRegulatoryAssistance/ucm123682.htm#1

[20] U.S. Food and Drug Administration. (2010). *In Vitro Diagnostic (IVD) Device Studies - Frequently Asked Questions.* Retrieved from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM071230.pdf

[21] U.S. Food and Drug Administration. (2011). *Clinical Laboratory Improvements Amendments (CLIA).* Retrieved from http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/IVDRegulatoryAssistance/ucm124105.htm

[22] U.S. Food and Drug Administration. (2011). *Code of Federal Regulation Title 21.* Retrieved from http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1

[23] U.S. Food and Drug Administration. (1997). *Design Control Guidance For Medical Device Manufacturers*. Retrieved from http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm070627.htm

[24] EUROPA - European Commission. (n.d.) *CE marking - Enterprise and Industry.* Retrieved from http://ec.europa.eu/enterprise/policies/single-market-goods/cemarking/

[25] U.S. Food and Drug Administration. (2010). Draft Guidance for Industry and Food and Drug Administration Staff - Applying Human Factors and Usability Engineering to Optimize Medical Device Design. Retrieved from http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm259748.htm

[26] Ericson, C. A. (2005). *Hazard analysis techniques for system safety*. Hoboken, NJ: Wiley-Interscience.

[27] Leveson, N. (1995). *SafeWare: system safety and computers*. Reading, Mass.: Addison-Wesley.

[28] NRC: Fault Tree Handbook (NUREG-0492). (1981). *U.S. Nuclear Regulatory Commission*. Retrieved from http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/

[29] Dhillon, B. S. (2000). *Medical device reliability and associated areas*. Boca Raton: CRC Press.

[30] McDermott, R. E., & Mikulak, R. J. (2009). *The basics of FMEA, 2nd edition* (2nd ed.). New York: CRC Press :.

[31] U.S. Food and Drug Administration. (2011). *Hazard Analysis & Critical Control Points (HACCP).* Retrieved from http://www.fda.gov/food/foodsafety/hazardanalysiscriticalcontrolpointshaccp/default.htm

[32] Bonan, B., N. Martelli, M. Berhoune, M.L. Maestroni, L. Havard, and P. Patrice. (2008). "The application of hazard analysis and critical control points and risk management in the preparation of anti-cancer drugs." *International Journal for Quality in Health Care* 21.1 (2008): 44-50.

[33] World Health Organization. (2003). *WHO Expert Committee on Specifications for Pharmaceutical Preparations.* Retrieved from http://www.who.int/medicines/services/expertcommittees/pharmprep/en/index.html

[34] Helferich, J.D. (2011). A Systems Approach to Food Accident Analysis. System Design and Management. Cambridge, MA, MIT.

[35] Couturier, M.M.J. (2010). A case study of Vioxx using STAMP. Engineering Systems Division. Cambridge, MA, MIT.

[36] Stringfellow, M.V. (2010). Accident Analysis and Hazard Analysis for Human and Organizational Factors. Department of Aeronautics and Astronautics. Cambridge, MA. MIT.

[37] Geddes, L. A. (2002). *Medical device accidents and illustrative cases* (2nd ed.). Tucson, AZ: Lawyers & Judges Pub. Co.

[38] Medical Devices and the Public's Health: The FDA 510(k) Clearance Process at 35 Years - Institute of Medicine. (n.d.). *IOM Home - Institute of Medicine*. Retrieved from http://www.iom.edu/Reports/2011/Medical-Devices-and-the-Publics-Health-The-FDA-510k-Clearance-Process-at-35-Years.aspx

[39] U.S. Food and Drug Administration. (n.d.). *Premarket Notification (510k).* Retrieved from http://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketnotification510k/default.htm#se

[40] U.S. Food and Drug Administration. (n.d.). *What is a Serious Adverse Event?* Retrieved from http://www.fda.gov/safety/medwatch/howtoreport/ucm053087.htm

[41] Cerebral hypoxia - PubMed Health. (n.d.). *National Center for Biotechnology Information*. Retrieved from http://www.ncbi.nlm.nih.gov/pubmedhealth/PMH0002407/

[42] Dekker, S. (2006). *The field guide to understanding human error*. Aldershot, England: Ashgate.

[43] World Health Organization. (2007). *Hazard Analysis Critical Control Point System (HACCP).* Retrieved from http://www.who.int/foodsafety/fs_management/haccp/en/