CAST Analysis on Medical Diagnostic Device

Vincent Balgos

MIT System Design & Management Alumni (2010)

Thesis: “A Systems Theoretic Application to Design for the Safety of Medical Devices”

Agenda

- Current Healthcare trends and Thesis question
- U.S. Regulatory Environment & Current Risk techniques
- Case System and Accident
- Control Structure
- CAST Analysis
- FMECA gap Analysis
- Conclusions

Current Trend

- US spends most in the world on healthcare
  - $2.5 Trillion (~17% of US GDP)
- US ranks 37th in overall quality of healthcare
  - 2000 World Health Organization report
- Approximately 98,000 annual US deaths due to medical errors; increasing injuries and accidents due to medical devices
- Safety is one of main elements for improving healthcare system

Thesis Question

"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?"

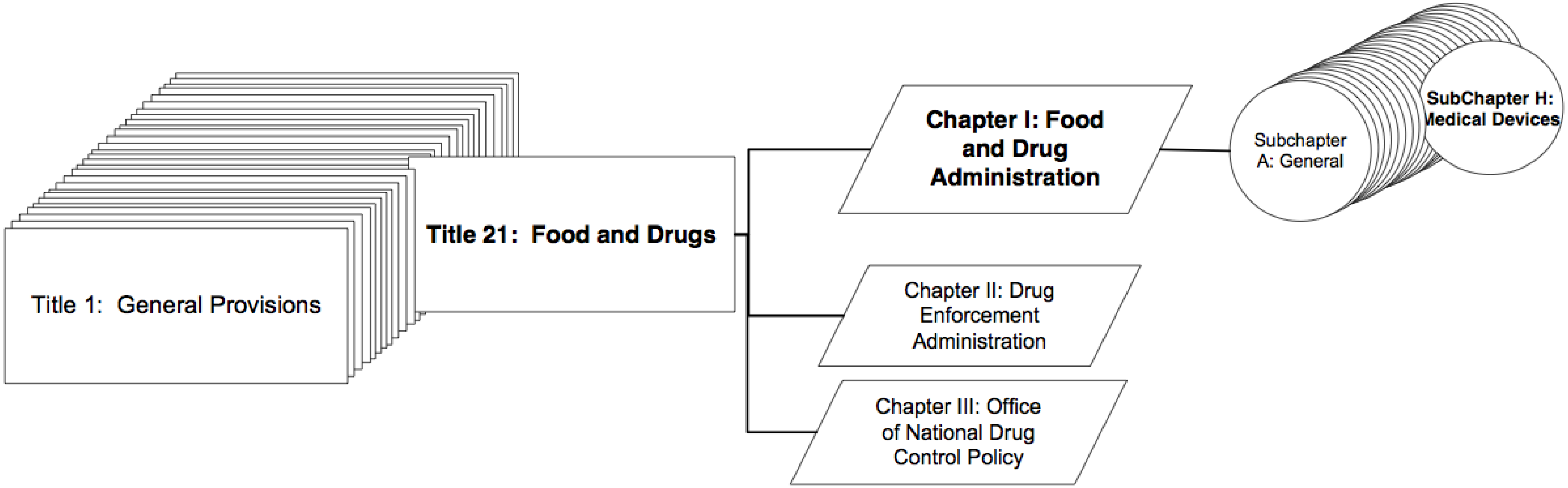
MITsdm
system design
and management

US Regulatory Environment

US Food and Drug Administration (FDA) responsibility:

- 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.***
- Annually regulate over $1 trillion worth of products

U.S. Code of Federal Regulations



Title 1: General Provisions

Title 21: Food and Drugs

Chapter I: Food and Drug Administration

Subchapter A: General

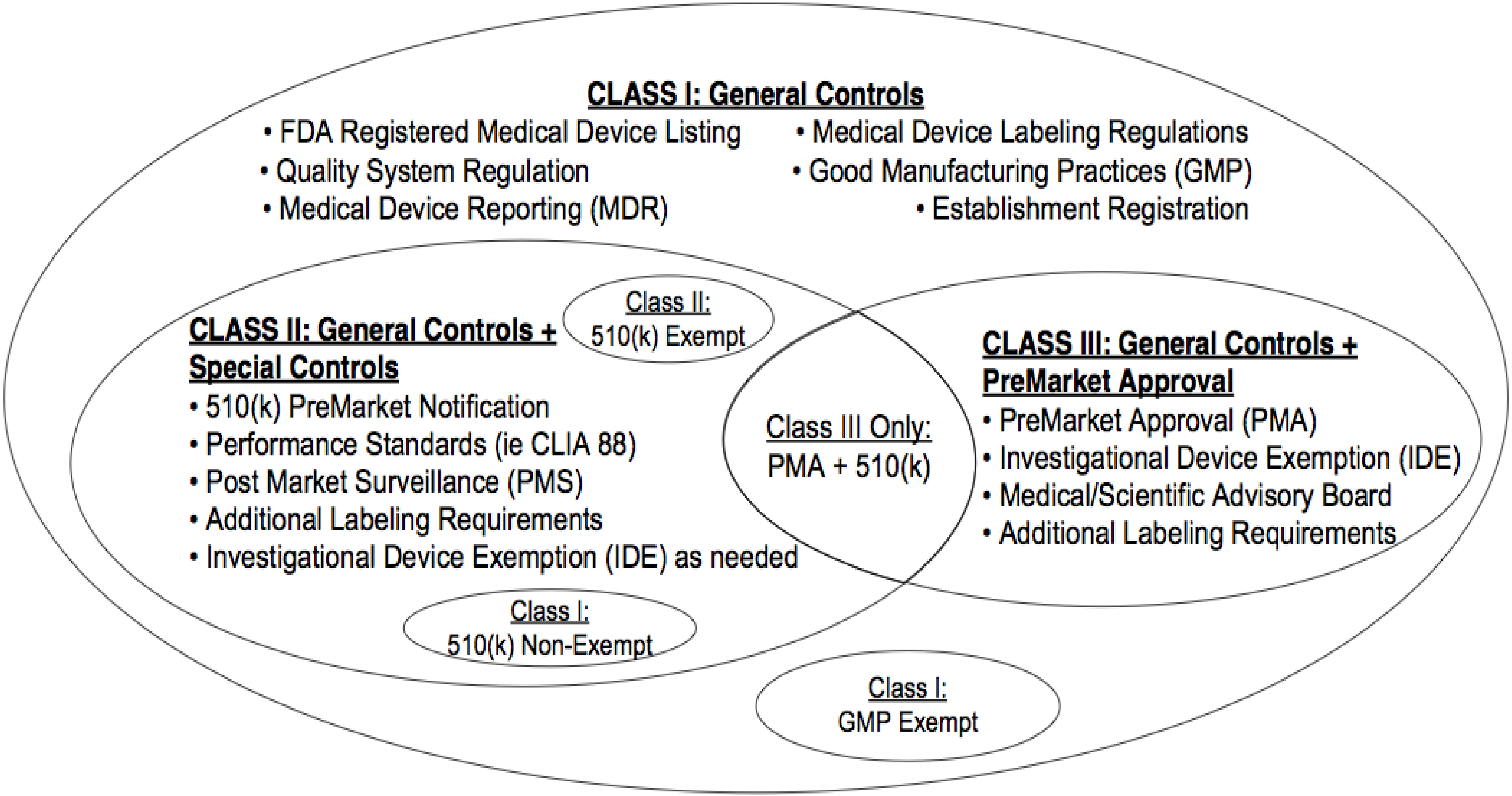
SubChapter H: Medical Devices

Chapter II: Drug Enforcement Administration

Chapter III: Office of National Drug Control Policy

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	

US Medical Device Classes



CLASS I: General Controls

- FDA Registered Medical Device Listing
- Medical Device Labeling Regulations
- Quality System Regulation
- Good Manufacturing Practices (GMP)
- Medical Device Reporting (MDR)
- 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

Current Risk Management

"Design validation shall include software and risk analysis, where appropriate"

- *21 CFR 820.30(g) Revised as of April 1, 2011.*

- ISO 14971: 5 Recommended Risk Analysis
  - Preliminary Hazard Analysis (PHA)
  - Fault Tree Analysis (FTA)
  - Failure Mode and Effects Analysis (FMEA)
  - Hazard and Operability Study (HAZOP)
  - Hazard Analysis and Critical Control Points (HACCP)

Case System

- Case system is point of care (POC) blood diagnostic analyzer for blood gas, metabolites, and other constituents
  - Key Performance Features
    - Precise and accurate blood diagnostic results
    - Fast turn-around-time (TAT) for results
    - High uptime and reliability
- Case company was dutiful in performing all required regulatory requirements
  - FDA supported Substantial Equivalence → US Market
  - CE Mark approved → EU Market

Case Accident

- FDA recall issued for case system
  - Specific reportable assay that reported erroneously low levels to medical staff that resulted in adverse event

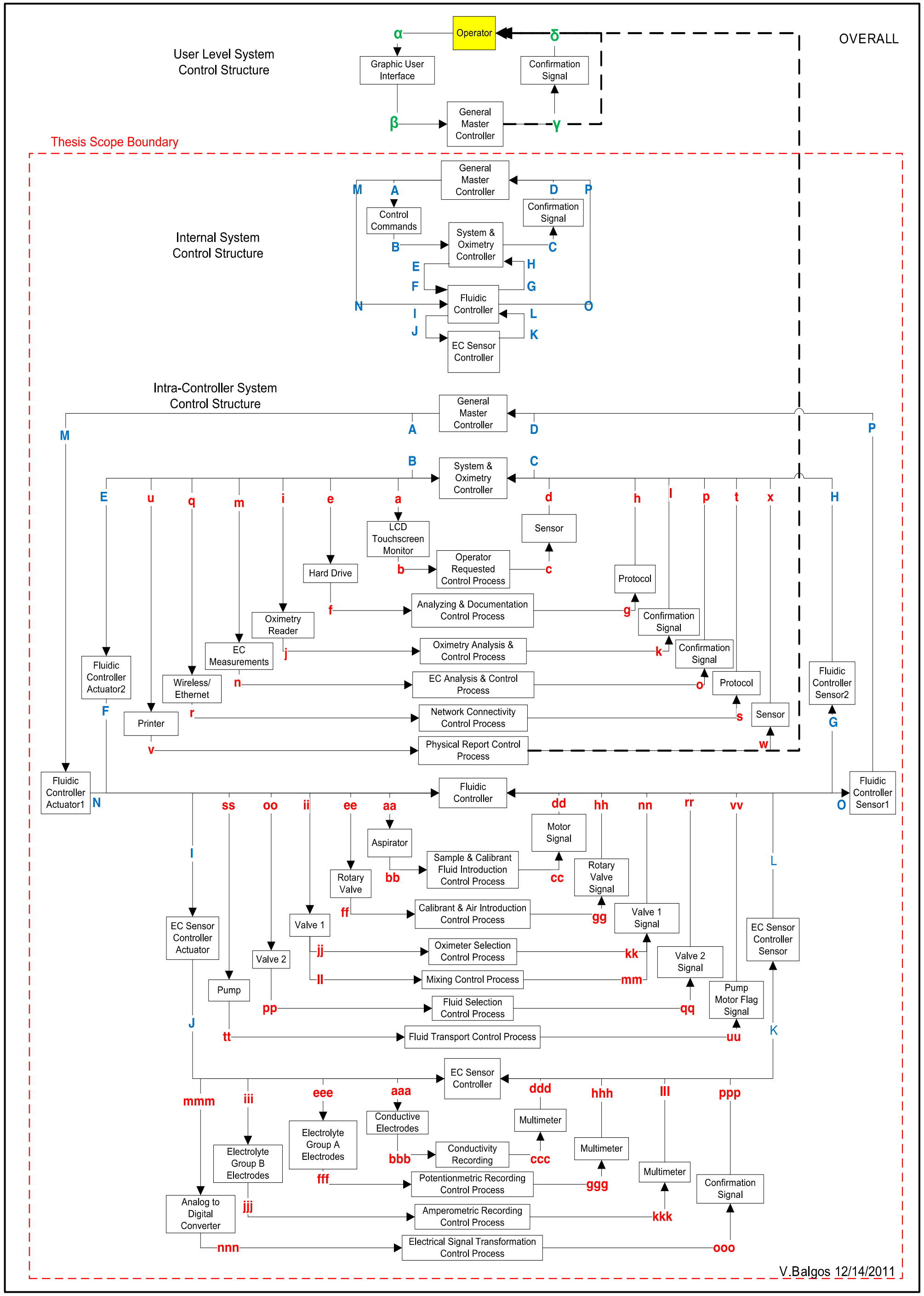
- Example of adverse event
  - Medical staff uses the case system to diagnose the patient.
  - Medical staff performed standard medical procedure on patient based off suspected low result.
  - Patient reacted adversely, and may result in seizure, cardiac arrhythmia, or death.
  - Subsequent testing of the same patient sample on an external reference system verified normal electrolyte levels.

CAST Hazard Definition

Hazards	Safety Constraints	Safety Requirements
H1: The system reports erroneous patients results to the user.	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: The system reports the patient results too late.	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.
H2: The system is unavailable for intended use due to premature failure or cartridge rejection.	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.

Safety Control Structure

- Technical System
- Start with User loop
- Decompose into 3 lower controlled process
- Each loop was further developed


OVERALL
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
b
c
Operator Requested Control Process
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
Motor Signal
Aspirator
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
EC Sensor Controller Actuator
Valve 1
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 Electrodes
Multimeter
Electrolyte Group A Electrodes
Electrolyte Group B Electrodes
bbb
Conductivity Recording
ccc
Multimeter
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

Safety Control Structure

- 20+ Control Loops
- Used highlight to emphasize which control loops are use for specific process

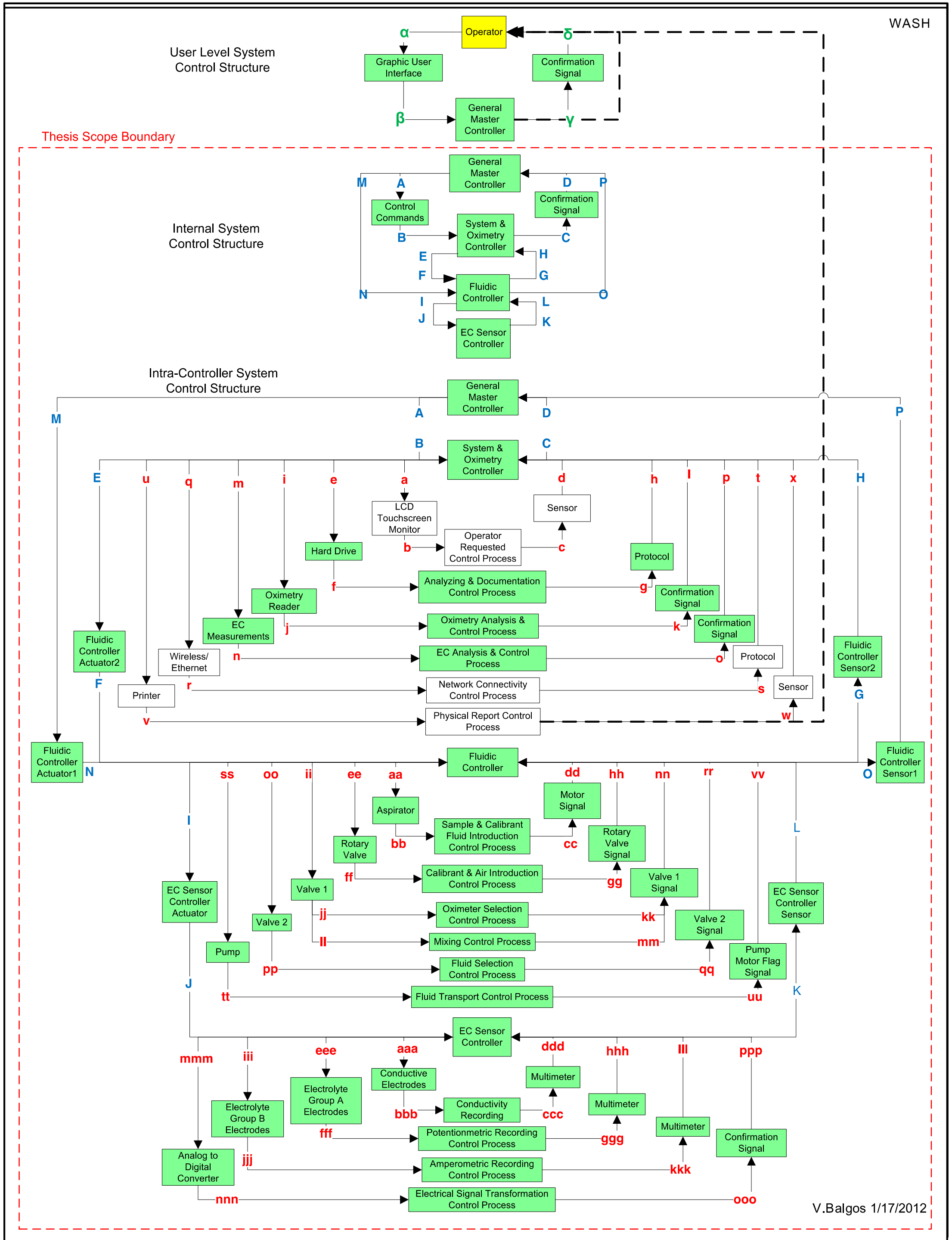
Sample Preparation

Sample Aspiration

EC Sample

Oximetry & Report

Wash & Calibration



WASH

User Level System Control Structure

Operator

Graphic User Interface

Confirmation Signal

General Master Controller

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

Oximetry Reader

Confirmation Signal

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

Motor Signal

Aspirator

Sample & Calibrant Fluid Introduction Control Process

Rotary Valve

Rotary Valve Signal

Calibrant & Air Introduction Control Process

Valve 1

Valve 1 Signal

EC Sensor Controller Actuator

Oximeter Selection Control Process

Valve 2

Valve 2 Signal

EC Sensor Controller Sensor

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

Electrolyte Group B Electrodes

Conductivity Recording

Multimeter

Potentiometric Recording Control Process

Multimeter

Confirmation Signal

Analog to Digital Converter

Amperometric Recording Control Process

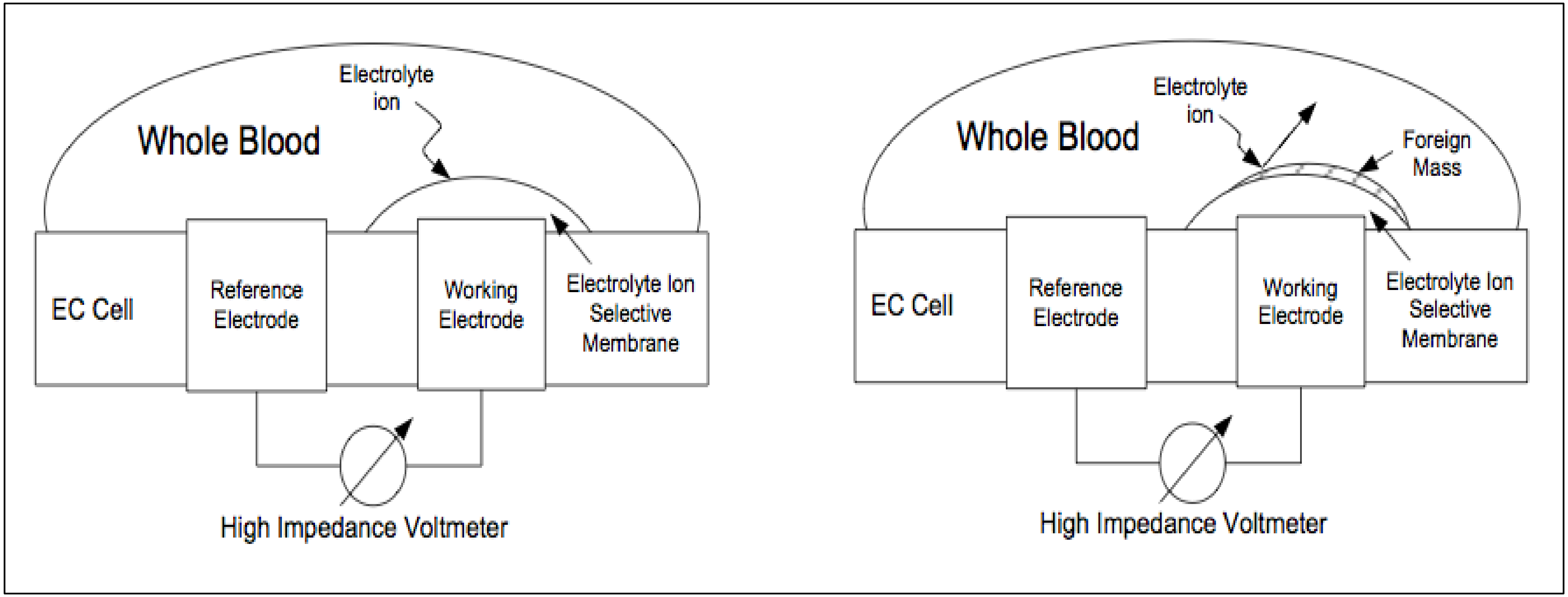
Electrical Signal Transformation Control Process

V.Balgos 1/17/2012

Proximal Chain of Events

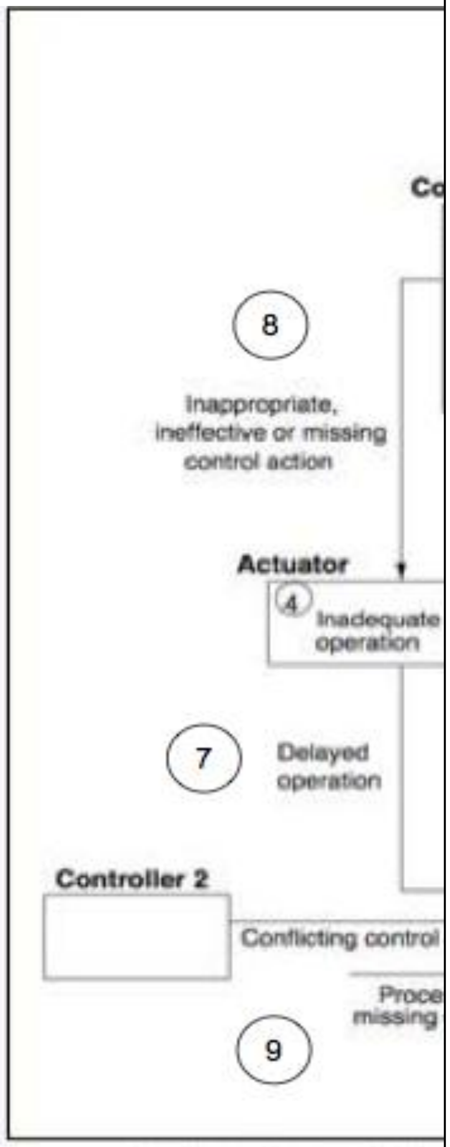
1. Patient is prescribed by physician(s) to be observed by diagnostic testing. Medical staff performs testing on the patient.
2. The case system performs patient sample analysis and reports an erroneous low electrolyte result, indicating a potential threatening *hypo*-electrolytic condition. There is no immediate error message.
3. Medical staff quickly reacts to low electrolyte result with medical intervention to increase the believed low level to normal levels.
4. Since the patient actually has normal level, the sudden increase in electrolytes raises the level beyond normal and induces a *hyper*-electrolytic condition. Patient then may undergo cardiac arrhythmia, epileptic seizure and/or death.
5. Post accident investigation confirmed that the case system reported erroneously low electrolyte results when compared to a laboratory reference system.

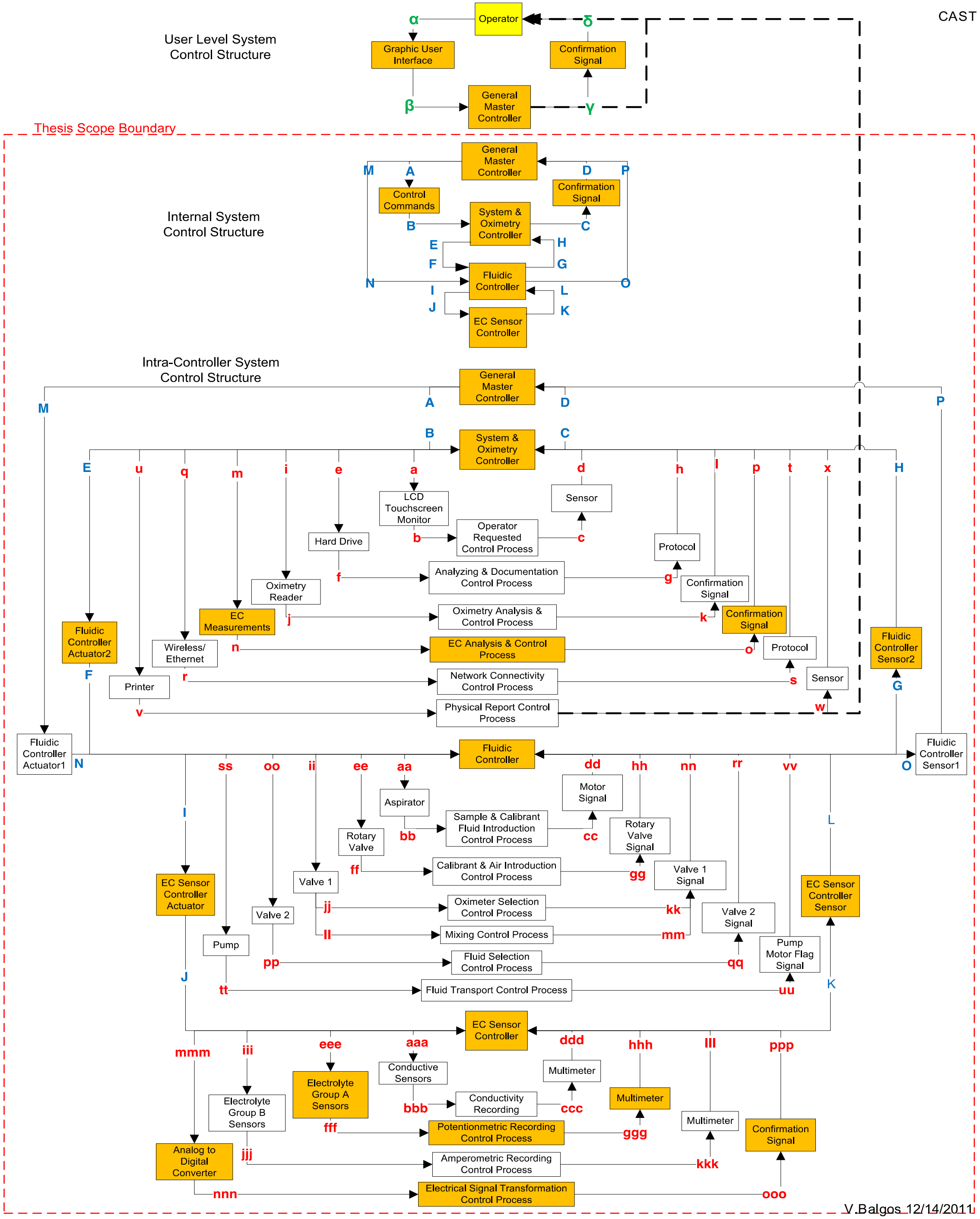
Analysis of Loss at Physical System



Significant finding, but does not explain how the fault migrated the system to an unsafe state.

CAST Analysis on H1

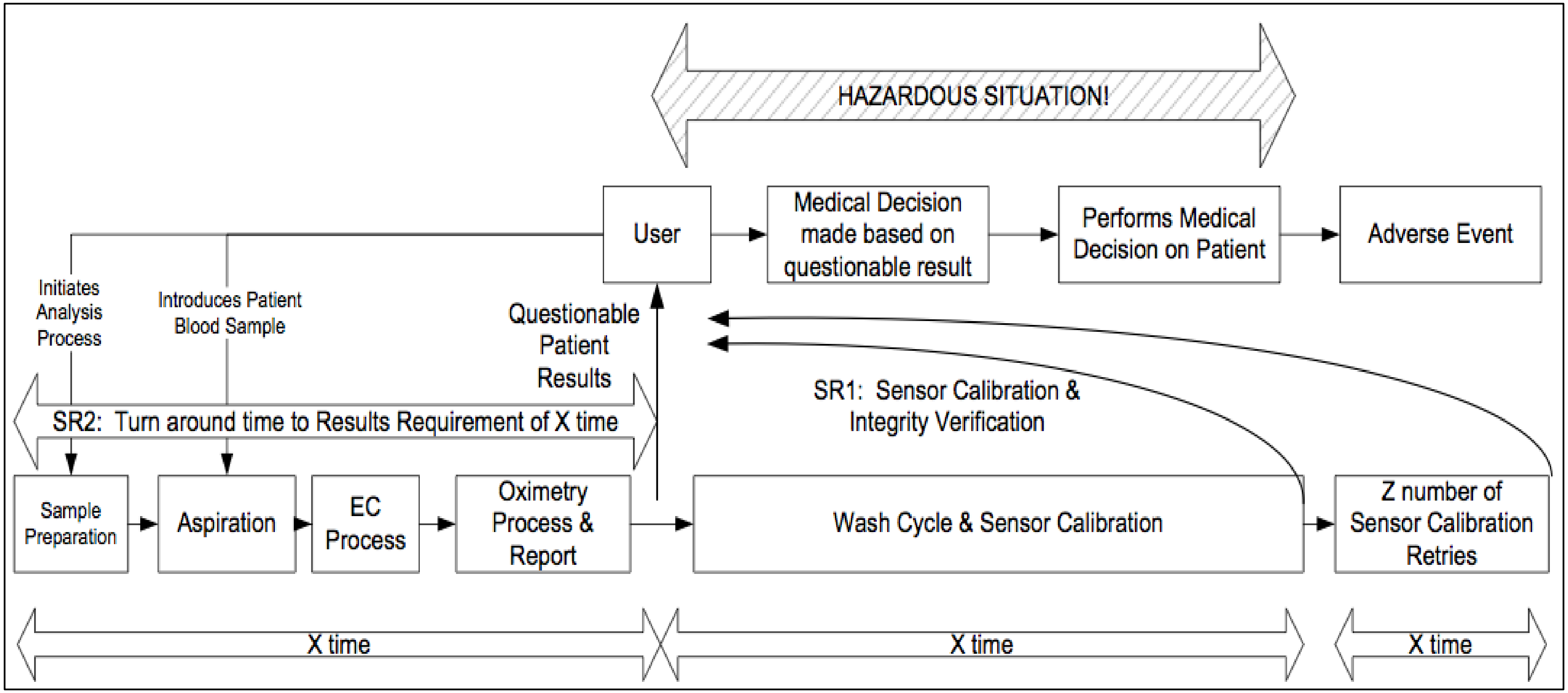



User Level System Control Structure
Operator
Graphic User Interface
General Master Controller
Confirmation Signal
α
β
γ
δ
Thesis Scope Boundary
Internal System Control Structure
General Master Controller
Control Commands
System & Oximetry Controller
Confirmation Signal
Fluidic Controller
EC Sensor Controller
Intra-Controller System Control Structure
General Master Controller
System & Oximetry Controller
LCD Touchscreen Monitor
Sensor
Hard Drive
Operator Requested Control Process
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
Motor Signal
Aspirator
Sample & Calibrant Fluid Introduction Control Process
Rotary Valve
Rotary Valve Signal
Calibrant & Air Introduction Control Process
Valve 1
Valve 1 Signal
EC Sensor Controller Actuator
Oximeter Selection Control Process
Valve 2
Valve 2 Signal
EC Sensor Controller Sensor
Mixing Control Process
Pump
Pump Motor Flag Signal
Fluid Selection Control Process
Fluid Transport Control Process
EC Sensor Controller
Conductive Sensors
Multimeter
Electrolyte Group A Sensors
Electrolyte Group B Sensors
Conductivity Recording
Multimeter
Multimeter
Potentiometric 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 12/14/2011

CAST Results

- Identified 175+ causes of hazards in 6 control loops
  - Nine causes of hazards directly related to case accident
  - Generalized into 3 categories:
    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.

Conflict of Constraints

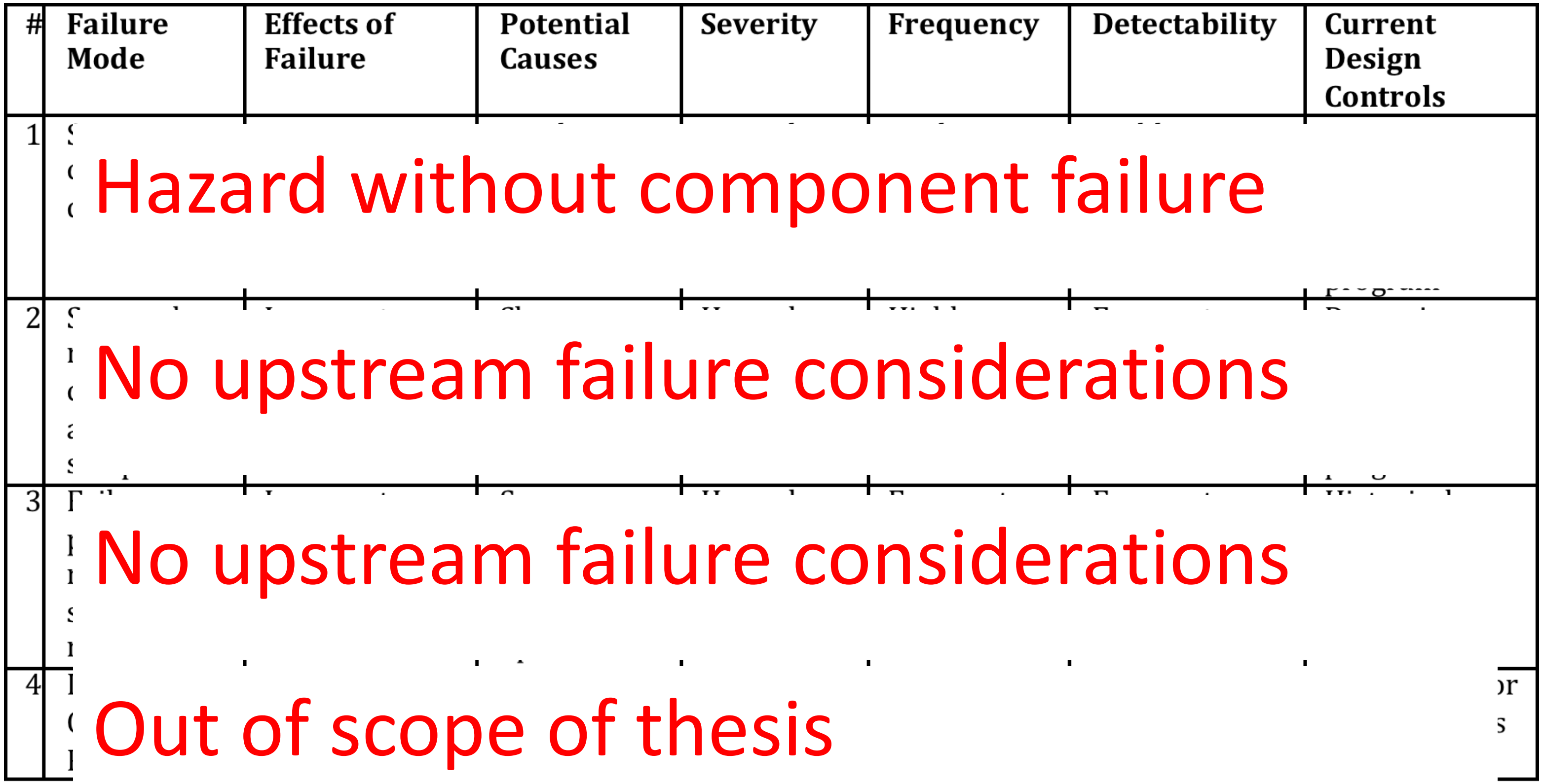

HAZARDOUS SITUATION!
User
Medical Decision made based on questionable result
Performs Medical Decision on Patient
Adverse Event
Initiates Analysis Process
Introduces Patient Blood Sample
Questionable Patient Results
SR1: Sensor Calibration & Integrity Verification
SR2: Turn around time to Results Requirement 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

New Safety Design Requirements

#	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.

FMECA vs CAST Gap Analysis

- Initial FMECA analysis identified ~70 causes of hazards
  - 4 causes hazards related to case accident



#	Failure Mode	Effects of Failure	Potential Causes	Severity	Frequency	Detectability	Current Design Controls
1							
2							
3							
4							

Hazard without component failure

No upstream failure considerations

No upstream failure considerations

Out of scope of thesis

FMECA vs CAST Gap Analysis

FMECA Results

- 70+ causes of hazards
- Team of Experts
- Extended Time dedication (Months/Years)
- Identified only single fault cause of hazards

CAST Results

- 175+ causes of hazards found (limited)
- Single Semi-Expert (Author)
- Shorter Time dedication (Weeks/Month)
- Identified complex causes of hazards, multiple failures, and no component failure that lead to a hazard.

Conclusion

- Case company was dutiful in performing the industry standard FMECA risk analysis
  - However, case accident still occurred
- CAST identified hazards in Control Structure
  - Quantity: Voluminous findings
  - Quality: Complex, multiple, and no component failure
- CAST findings could have prevented case accident with a systems approach

Conclusion to Thesis

"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?"

YES

Thank you to Dr. Qi Hommes & Prof Leveson!

Questions?

Contact:
Email: vbalgos@sloan.mit.edu
LinkedIn