A System Safety Analysis of Tomographic Treatment

by

Shinichi Yamaguchi

M.S., Fundamental science and technology, Keio University, 2003
B.E., Applied physics and physic-informatics, Keio University, 2001

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2017

Signature of Author: Signature redacted

Shinichi Yamaguchi
System Design and Management Program
May 12, 2017

Certified by: Signature redacted

Nancy Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: Signature redacted

Joan Rubin
Executive Director
System Design and Management Program

[Page intentionally left blank]

A System Safety Analysis of Tomographic Treatment

by

Shinichi Yamaguchi

Submitted to the System Design and Management Program
on May 12, 2017 in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

ABSTRACT

In recent years, the technology in the medical industry has been advancing to provide safe and systematic medical care. However, the system of medical technologies and treatments has become more complicated year by year, which increases the risks of defects in the system. For example, the U.S. Food and Drug Administration's Center for Devices and Radiologic Health has reported recalls of medical devices that may lead to serious injury or death because of malfunctions. To reduce the risks, developers and makers of medical devices have been applying a wide spectrum of methodologies to improve quality. However, the growing complexity of medical systems, including devices, medical staff, organizations, and regulators, causes problems that the current safety engineering techniques are inadequate to prevent, which can result in tragic medical accidents. Therefore, it is important to apply new approaches to ensure the system safety of medical devices.

This thesis compares Failure Mode and Effect Analysis (FMEA) and System-Theoretic Process Analysis (STPA). STPA is one of the analysis techniques based on the systems-theoretic approach of system safety (STAMP) to identify what should be done to establish the design safety of medical systems. Presently, FMEA, as a risk management technique, is widely used as a major methodology to ensure the safety of medical devices; therefore, it is worth comparing with STPA as a fundamental methodology.

This thesis identifies the basic design of tomographic treatment and applies STPA to the TomoTherapy system. This tomographic treatment system treats hard-to-reach tumors and reduces radiation exposure to nearby healthy tissues. To ensure the quality of TomoTherapy, STPA is an effective means to conduct hazard analyses because STPA holistically analyzes the safety of this system, considering both human and mechanical factors. After that, I compare the results of STPA and FMEA. STPA analysis found 99 unsafe control actions, 10 causal scenarios, and 29 possible requirements, in contrast with FMEA, which identified a total of 74 failure modes. The potential causes of failure in the results of FMEA include only human factors. However, STPA analyzes the system from various viewpoints, such as the physical system, human factors, organization, management, and so on. Thus, it can be seen that STPA can be used as a technique to identify potential causes as causal scenarios more comprehensively than FMEA.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics

[Page intentionally left blank]

ACKNOWLEDGMENTS

I am immensely grateful to my thesis advisor, Professor Nancy Leveson of the Department of Aeronautics and Astronautics at Massachusetts Institute of Technology (MIT), for her generous attention and respectful consideration. She showed me a new way to look at system safety through my research and her classes, and when I asked her to become my thesis advisor, she gladly accepted my request, stating her passion for my research interest. She consistently allowed this paper to be my own work, but steered me in the right direction.

I also would like to thank Dr. John Thomas of the Department of Aeronautics and Astronautics at MIT, who gave me valuable insights in the conceptual stage of my research. Always, he gave me clear and proper suggestions about my research and system safety that led me in the right direction. Without his passionate participation and input, this research could not have been successfully formulated or conducted.

Finally, I must express my very profound gratitude to my employer, Canon Incorporated, my friends, and especially my family and parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you for being great traveling partners on this valuable journey.

Shinichi Yamaguchi
Cambridge, Massachusetts
May 2017

Contents

Chapter 1. Introduction 8

1.1 Overview of FDA 8

1.2 FDA regulations in medical field and radiological region 10

1.3 Purpose of this analysis and my strategic question 11

1.4 References 12

Chapter 2. Literature Review of Hazard Analysis 14

2.1 Failure Mode and Effect Analysis (FMEA) 14

2.2 Fault Tree Analysis (FTA) 17

2.3 Hazard and Operability study (HAZOP) 20

2.4 STAMP (STPA) 21

2.3 References 24

Chapter 3. Tomographic Treatment System as a Case Study Overview 25

3.1 Tomographic Treatment 25

3.2 TomoTherapy 26

3.3 System Structure of TomoTherapy 30

3.3.1 Treatment Room 30

3.3.2 Operator Station 32

3.3.3 Data Server Room 33

3.3.4 Mechanical Room 34

3.3.5 Treatment Planning Room 35

3.4 Safety Information of TomoTherapy 35

3.5 References 38

Chapter 4. Application result of FMEA 40

4.1 Overall 40

4.2 Materials and Methods 40

4.3 Results 41

4.4 References 56

Chapter 5. STPA Application 57

5.1 System Description 57

5.2 Defining Accidents and Hazards 58

5.3 Description of the Hierarchical Safety Control Structure 60

5.4 Performing STPA Step 1 Analysis 65

5.4.1 Identifying Unsafe Control Actions (UCA) 65

5.4.2 System Constraints 89

5.5 Performing STPA Step 2 Analysis 112

5.5.1 Identifying Causal Scenarios 112

5.5.2 Causal Scenarios for the control loop between human controllers 113

5.5.3 Causal Scenarios for the control loop between system controllers 121

5.5.4 Causal Scenarios for the control loop between a human controller and a system controller 125

5.6 References 133

Chapter 6. Discussion and Conclusion 134

6.1 Discussion 134

6.2 Conclusion 139

6.3 Future Work 140

6.4 References 141

Chapter 1. Introduction

Currently, it is important to provide physicians, nurses, and medical staff with more effective medical treatments. For this purpose, state-of-the-art medical technology used for medical devices has been advancing rapidly. With that, medical devices have become more complex, and the treatment processes also have to be executed with strict safety standards. Therefore, it is quite crucial to provide safer devices to prevent medical accidents and hazards. For this reason, I believe, it is useful to analyze system safety using a new type of accident model based on systems theory.

1.1 Overview of FDA

The Food and Drug Administration (FDA) is the oldest comprehensive consumer protection agency in the U. S. federal government. As for its origin, the appointment of Lewis Caleb Beck in the Patent Office around 1848 carried out chemical analyses of agricultural products, a function that the newly created Department of Agriculture inherited in 1862.

Although it was not known by its present name until 1930, FDA's modern regulatory functions began with the passage of the 1906 Pure Food and Drugs Act, a law that took a quarter-century in the making that prohibited interstate commerce in adulterated and misbranded food and drugs.

Harvey Washington Wiley, Chief Chemist of the Bureau of Chemistry in the Department of Agriculture, had been the driving force behind this law and headed its enforcement in the early years, providing basic elements of protection that consumers had never known before that time.

The FDA and its responsibilities have undergone a metamorphosis since 1906. Also, the marketplace itself, the sciences undergirding the products the agency regulates, and the social, cultural, political, and economic changes that have formed the context for these developments, all have witnessed upheavals over the past century. However, just like in the past, the core public health mission of the agency remains unchanged. [1]

The FDA consists of the Office of the Commissioner and four directorates overseeing the core functions of the agency: Medical Products and Tobacco, Foods and Veterinary Medicine, Global Regulatory Operations and Policy, and Operations.

FDA has the following responsibilities:

- Protecting the public health by assuring that foods (except for meat from livestock, poultry and some egg products which are regulated by the U.S. Department of Agriculture) are safe, wholesome, sanitary and properly labeled; ensuring that 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 product innovations for public health.

FDA's responsibilities extend to the 50 states in the U.S., the District of Columbia, Puerto Rico, Guam, the Virgin Islands, American Samoa, and other U.S. territories and possessions [2]

1.2 FDA regulations in medical field and radiological region

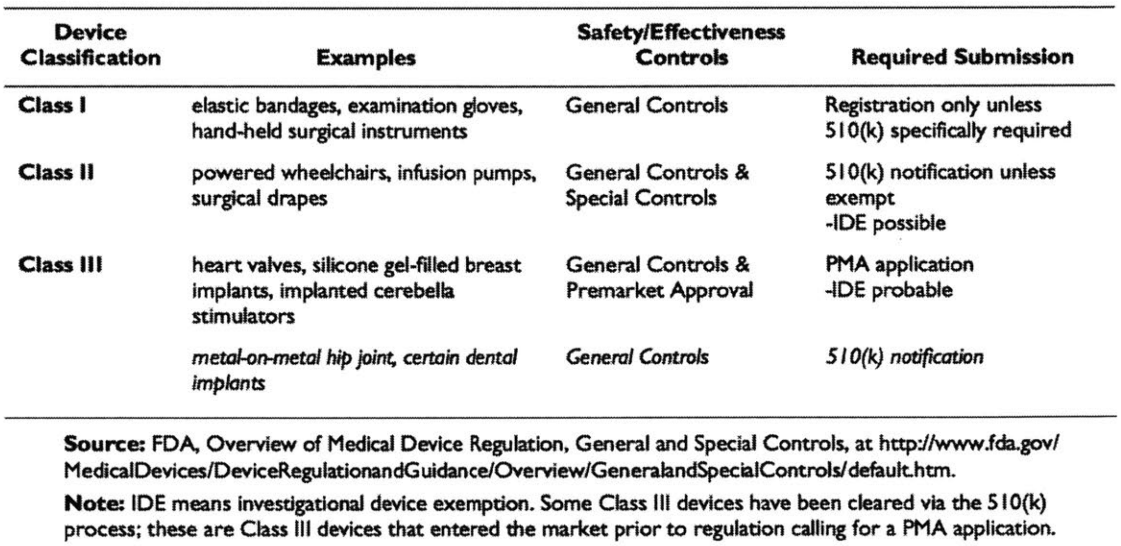
In daily life, people use products that are regulated by the FDA's Center for Devices and Radiological Health (CDRH), such as wearing contact lenses, testing blood sugar levels, and so on. The CDRH protects people who live in the U.S. with safeguards that ensure people can live knowing that the medical devices and radiological products are safe enough to use, and more importantly, that those devices and products work as intended. [3]

Some radiation-emitting products, such as X-ray machines and computed tomography (CT) scanners, are medical devices by way of distinction. Actually, they are used in medical procedures. Other radiation-emitting products, such as TVs and microwave ovens, are not used medically; and therefore, they are regulated by the FDA under a different law.

Medical devices are classified and regulated according to their complexity and degree of risk to the public. For example, devices that are life-supporting, life-sustaining, or implanted, such as pacemakers, must receive FDA approval before they can be marketed. [4]

The FDA has established classifications and examples as shown in Table 1.1. Under the terms of the Medical Device Amendments of 1976 (MDA, P.L. 94-295), FDA classified all medical devices that were on the market at the time of enactment—the preamendment devices—into one of three classes. Congress provided definitions for the three classes—Class I, Class II, and Class III—based on the risk (low-, moderate-, and high-risk respectively) to patients posed by the devices. [5]

Table 1.1. Medical Device Classification cited from [5]



Device Classification	Examples	Safety/Effectiveness Controls	Required Submission
Class I	elastic bandages, examination gloves, hand-held surgical instruments	General Controls	Registration only unless 510(k) specifically required
Class II	powered wheelchairs, infusion pumps, surgical drapes	General Controls & Special Controls	510(k) notification unless exempt -IDE possible
Class III	heart valves, silicone gel-filled breast implants, implanted cerebella stimulators	General Controls & Premarket Approval	PMA application -IDE probable
	metal-on-metal hip joint, certain dental implants	*General Controls*	*510(k) notification*

Source: FDA, Overview of Medical Device Regulation, General and Special Controls, at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/GeneralandSpecialControls/default.htm.

Note: IDE means investigational device exemption. Some Class III devices have been cleared via the 510(k) process; these are Class III devices that entered the market prior to regulation calling for a PMA application.

Based on these classifications, a manufacturer must obtain FDA's prior approval or clearance before marketing any medical devices in the United States. FDA's Center for Devices and Radiological Health (CDRH) is primarily responsible for medical device's premarket review. Another center, the Center for Biologics Evaluation and Research (CBER), regulates devices associated with blood collection and processing procedures, cellular products, and tissues. [5]

1.3 Purpose of this analysis and my strategic question

To ensure the quality of medical devices, many approaches can be applied. Specifically, FMEA is one of the major means for system safety of medical devices, and many medical device companies have been applying FMEA to their products. However, according to the FDA site, many medical devices have been causing healthcare accidents and are recalled every year due to reasons such as radiation errors accident.

[6] Thus, that means the current safety engineering techniques, such as the widely-applied FMEA in the medical industries, are inadequate in preventing tragic medical accidents. Therefore, it is important to apply new approaches to ensure system safety for medical devices.

To ensure the quality of medical devices, I believe that STAMP is an effective means to conduct hazard analyses of medical devices because STAMP holistically analyzes the safety of the system from two aspects, which are human factors and mechanical factors. In this research, as a case study, I applied STPA to radiation treatment system called TomoTherapy, and compared its results with those of FMEA.

Therefore, I defined my strategic question of this research as "Is STPA a more effective means to be used to design safer medical devices than the traditional means in the current medical industry?." The primary objective of my research is to answer this strategic question by comparing major traditional methodologies with STPA.

1.4 References

[1] U.S. FOOD&DRUG ADMINISTRATION (2015), "History," available at: http://www.fda.gov/AboutFDA/WhatWeDo/History/

[2] U.S. FOOD&DRUG ADMINISTRATION (2015), "FDA Fundamentals," available at: http://www.fda.gov/AboutFDA/Transparency/Basics/ucm192695.htm

[3] U.S. FOOD&DRUG ADMINISTRATION (2006), "Medical Device and Radiological Health Regulations Come of Age," available at: https://www.fda.gov/aboutfda/whatwedo/history/productregulation/medicaldeviceandradiologicalhealthregulationscomeofage/default.htm

[4] U.S. FOOD&DRUG ADMINISTRATION (2015), “Classify Your Medical Device,” available at:

https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/

[5] Judith A. Johnson (2016), “FDA Regulation of Medical Devices,” available at:

https://fas.org/sgp/crs/misc/R42130.pdf

[6] the ST. Cloud Times (2016), “Lawsuits allege radiation errors,” available at:

http://www.advisen.com/tools/fpnproc/fpns/articles_new_2/P/271732451.html?rid=271732451&list_id=2

Chapter 2. Literature Review of Hazard Analysis

Currently, various industries use a wide spectrum of risk management techniques. The following introduces a brief overview of FMEA, FTA, HAZOP, STPA. FMEA and STPA are compared because FMEA is mainly used for safety analysis of medical devices, and STPA is a new technique.

2.1 Failure Mode and Effect Analysis (FMEA)

The Failure Mode and Effect Analysis [1] is one of the more popular and common methods in the realm of system safety. This is widely used and applied in various industries all over the world. The FMEA can specifically evaluate system safety using a bottom-up approach, and it focuses on finding failure modes. The FMEA examines systems at the component level, so the FMEA can identify and evaluate potential single-point failures. Also, FMEA finds chains of failure that lead to accidents, so it is based on a "domino chain event model" or "event-based model".

There are basically two types of FMEA. These types are mainly distinguished by the target of the analysis than the actual analysis itself. The approach is fundamentally different between the two.

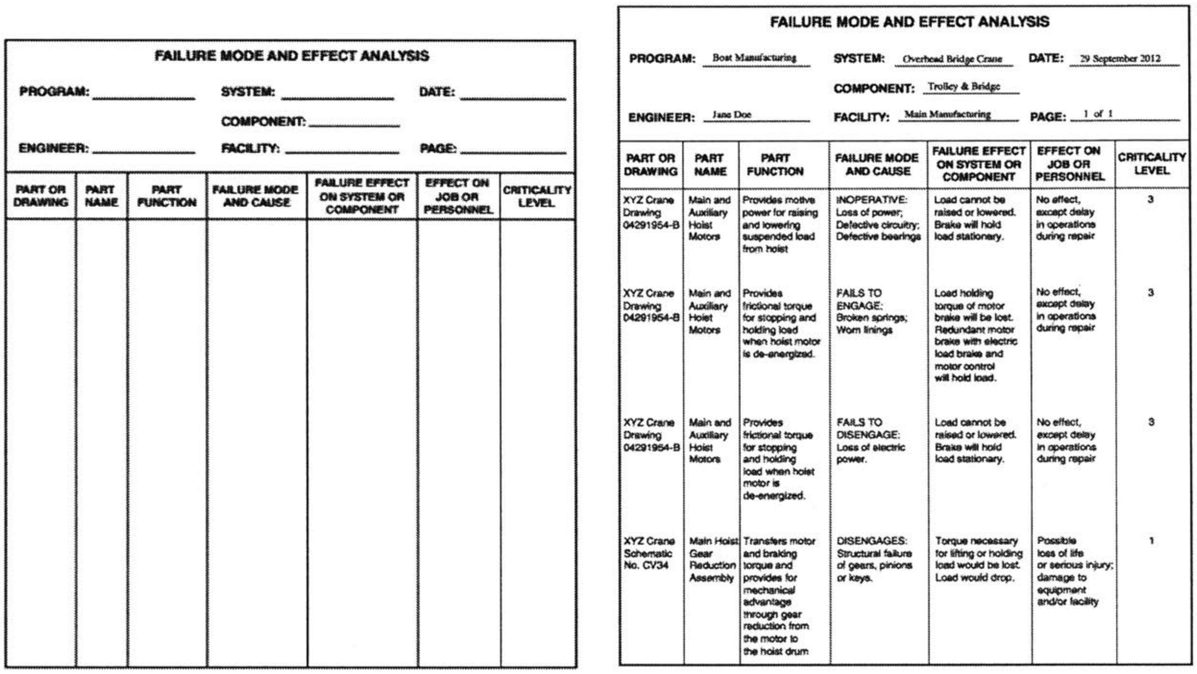
The first type is called the functional FMEA. This FMEA uses the deductive reasoning approach. On the other hand, the second type, which is called the hardware or detailed FMEA, utilizes the inductive approach by identifying common failure modes and examining the effects of those failures on various system levels such as the whole system, subsystems, and so on.

The functional FMEA is used for any subsystems that exist or may exist within the whole system. As a focusing point, the functional FMEA will evaluate subsystems respectively, and try to identify the effect of any failures among the subsystems. The second one, hardware FMEA, is more common. It examines actual system assemblies, subassemblies, each component of the whole system, and other related system hardware, which is performed at the earliest possible phase in the product or system life cycle. As with the functional FMEA, the reliability of the system design is evaluated by the hardware FMEA. The hardware FMEA tries to identify single-point failures within a system that might result in failure of that system as well as all other potential failures.

To perform an FMEA, the analysis needs to have certain detailed data. The following shows the data.

- Design drawings
- System schematics
- Functional diagrams
- Previous analytical data (if available)
- System descriptions
- Lessons learned data
- Manufacturer's component data/specifications
- Preliminary hazard list (if available)
- Preliminary hazard analysis
- Other system analyses previously performed

About the FMEA report, its format is shown in the following as a sample. This format contains various important information: introductory information, definitions section, system description, and critical assessment.



FAILURE MODE AND EFFECT ANALYSIS

PROGRAM: ____________ SYSTEM: ____________ DATE: ____________

COMPONENT: ____________

ENGINEER: ____________ FACILITY: ____________ PAGE: ____________

PART OR DRAWING	PART NAME	PART FUNCTION	FAILURE MODE AND CAUSE	FAILURE EFFECT ON SYSTEM OR COMPONENT	EFFECT ON JOB OR PERSONNEL	CRITICALITY LEVEL

FAILURE MODE AND EFFECT ANALYSIS

PROGRAM: Boat Manufacturing SYSTEM: Overhead Bridge Crane DATE: 29 September 2012

COMPONENT: Trolley & Bridge

ENGINEER: Jane Doe FACILITY: Main Manufacturing PAGE: 1 of 1

PART OR DRAWING	PART NAME	PART FUNCTION	FAILURE MODE AND CAUSE	FAILURE EFFECT ON SYSTEM OR COMPONENT	EFFECT ON JOB OR PERSONNEL	CRITICALITY LEVEL
XYZ Crane Drawing 04291954-B	Main and Auxiliary Hoist Motors	Provides motive power for raising and lowering suspended load from hoist	INOPERATIVE: Loss of power; Defective circuitry; Defective bearings	Load cannot be raised or lowered. Brake will hold load stationary.	No effect, except delay in operations during repair	3
XYZ Crane Drawing 04291954-B	Main and Auxiliary Hoist Motors	Provides frictional torque for stopping and holding load when hoist motor is de-energized.	FAILS TO ENGAGE: Broken springs; Worn linings	Load holding torque of motor brake will be lost. Redundant motor brake with electric load brake and motor control will hold load.	No effect, except delay in operations during repair	3
XYZ Crane Drawing 04291954-B	Main and Auxiliary Hoist Motors	Provides frictional torque for stopping and holding load when hoist motor is de-energized.	FAILS TO DISENGAGE: Loss of electric power.	Load cannot be raised or lowered. Brake will hold load stationary.	No effect, except delay in operations during repair	3
XYZ Crane Schematic No. CV34	Main Hoist Gear Reduction Assembly	Transfers motor and braking torque and provides for mechanical advantage through gear reduction from the motor to the hoist drum	DISENGAGES: Structural failure of gears, pinions or keys.	Torque necessary for lifting or holding load would be lost. Load would drop.	Possible loss of life or serious injury; damage to equipment and/or facility	1

Figure 2.1. Sample worksheet of the FMEA and the partially completed FMEA worksheet for the crane system cited from [1]

The FMEA is a popular reliability engineering technique. It examines failure modes and their effects on either each component, the whole system or the subsystem. However, the FMEA does not take into consideration the human factors element, software element or multiple failures within a system. For these analyses, it is recommended to use other types of system safety analysis tools and techniques.

In several manufacturing sectors as well as in aviation, FMEA is a prospective risk analysis approach routinely employed. In recent years, FMEA was identified as a powerful tool in modern radiation oncology by the Task Group 100 of the American Association of Physicists in Medicine. [2]

The use of the FMEA approach is also recommended by the International Commission on Radiological Protection (ICRP) as a resource for improving the safety of patients undergoing modern radiation therapy treatments. [3]

2.2 Fault Tree Analysis (FTA)

The Fault Tree Analysis (FTA) is one of the most popular hazard analysis techniques. [1] FTA is a top-down search method, and it is widely used in a wide spectrum of industries. FTA utilizes the deductive method of logic based on the chain of events model. In this technique, an undesirable event is put on the tree structure diagram as a top event. From this, the analyst begins to identify the specific events which contributed to the top event, and a fault tree can be constructed. In other words, FTA applies Boolean logic to identify how lower level events could be combined to produce upper level system states. The goal of FTA is to identify causes of the hazardous event.

To construct Boolean logic, numerous symbols are used. Figure 2.2 shows the basic symbols used during the FTA process.

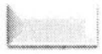
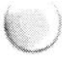
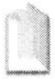
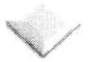
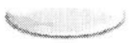
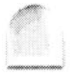
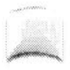
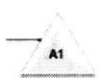
SYMBOL	NAME	DESCRIPTION
	RECTANGLE	TOP EVENT; SECONDARY OR CONTRIBUTING EVENTS; A SYSTEM STATE REQUIRING MORE INVESTIGATION ON LOWER LEVELS
	CIRCLE	BASIC FAULT EVENT; NO FURTHER DEVELOPMENT REQUIRED
	HOUSE	NOT A FAULT EVENT; AN EVENT THAT IS EXPECTED TO OCCUR UNDER NORMAL OPERATION
	DIAMOND	UNDEVELOPED EVENT; ONE THAT, EITHER BY CHOICE OR NECESSITY, WILL NOT BE DEVELOPED FURTHER
	OVAL	AN EVENT THAT PLACES QUALIFIED CONDITIONS ON THE FAULT SEQUENCE
	AND GATE	DESCRIBES AN OPERATION WHERE ALL INPUT EVENTS MUST OCCUR FOR THE OPERATION TO OCCUR
	OR GATE	DESCRIBES AN OPERATION WHERE ONE OR MORE OF THE INPUT EVENTS CAN OCCUR IN ORDER FOR THE OUTPUT TO OCCUR
	TRANSFER GATE	USED TO SHOW LOGIC FLOW BETWEEN TWO PARTS OF THE FAULT TREE;TRANSFERS EVERYTHING UNDER THE EVENT IT IS ATTACHED TO; REFERENCE IS MADE BY AN ALPHANUMERIC CODE

Figure 2.2. Standard FTA Symbology

Two types of fault trees will be constructed using the symbols to demonstrate the use of the system safety analytical technique. The first, which will be referred to as a positive fault tree analysis, will identify the events necessary to achieve a top desired event of no accidents. The second will be constructed to show those events or conditions which will lead to a top undesired event. This is called negative fault tree. In the following, the first and second one were shown in Figures 2.3 and 2.4 as samples of FTA analysis respectively.

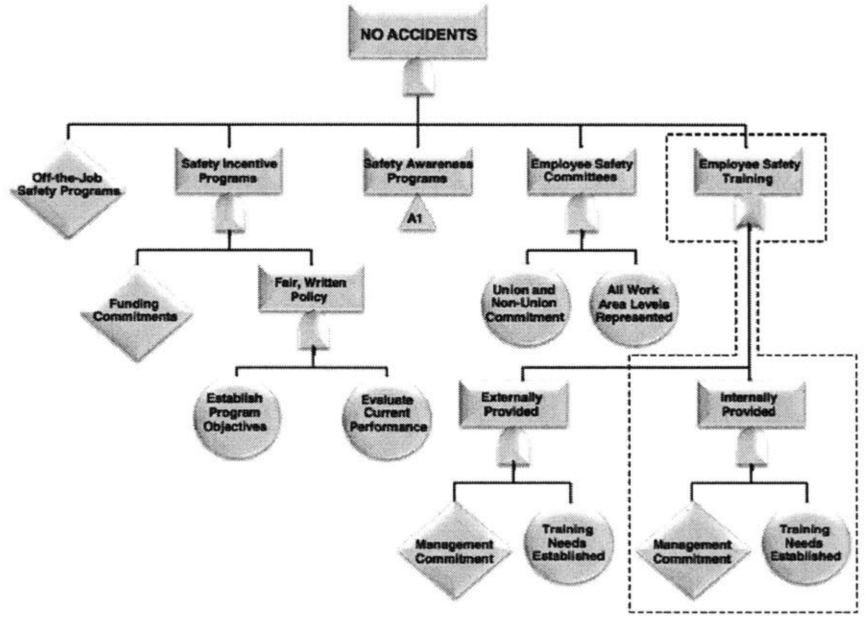

NO ACCIDENTS
Off-the-Job Safety Programs
Safety Incentive Programs
Safety Awareness Programs
A1
Employee Safety Committees
Employee Safety Training
Funding Commitments
Fair, Written Policy
Union and Non-Union Commitment
All Work Area Levels Represented
Establish Program Objectives
Evaluate Current Performance
Externally Provided
Internally Provided
Management Commitment
Training Needs Established
Management Commitment
Training Needs Established

Figure 2.3. Sample of a Positive Fault Tree Analysis

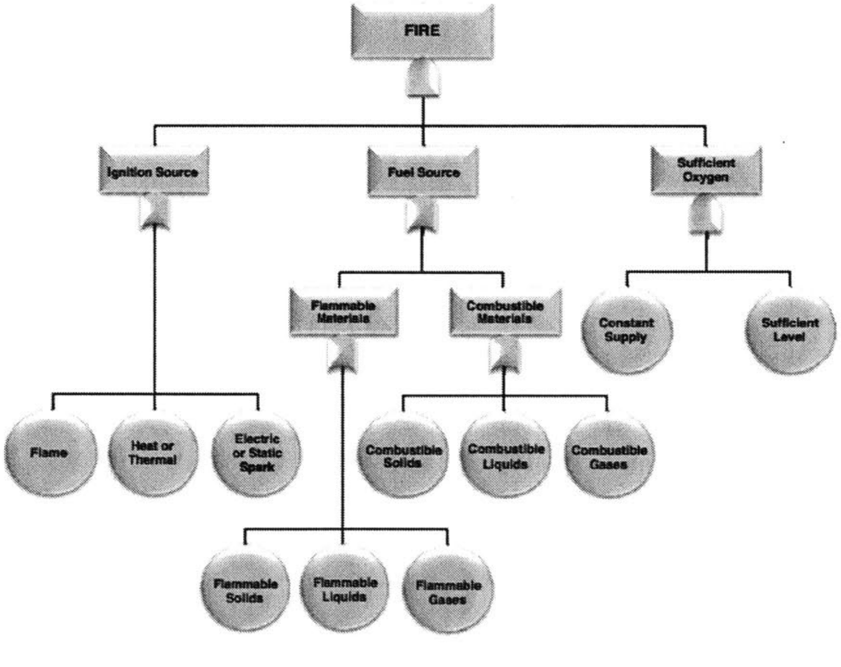


Figure 2.4. Sample of a Negative Fault Tree Analysis

Regarding the strength of FTA, it enables analysists and developers to analyze only the failures relevant to top-level events by capturing combinations of failures. In addition, FTA provides a graphical format to promote the understanding of the analysis results. Using FTA, analysts can think about the target system in great detail during the construction of the tree diagram. Moreover, finding minimum cut sets provides insight into weak points, such as common mode failures, of complex systems

2.3 Hazard and Operability study (HAZOP)

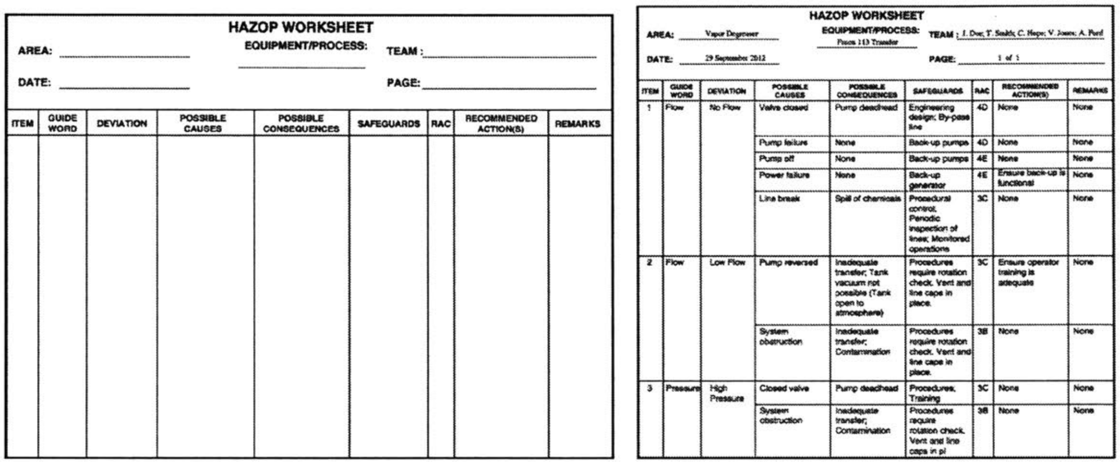
A hazard and operability study (HAZOP) is a structured and systematic examination of a complex planned or existing process or operation for the identification and evaluation of problems that may represent risks to personnel or equipment. HAZOP was first developed in the U.K. for use in the chemical industry during the 1960s. In 1994, the below four primary objectives were mentioned. [1]

1. To identify the causes of all deviations of changes from the intended design function.
2. To determine all major hazards and operability problems associated with any identified deviations
3. To decide whether action is required to control the hazard or operability problems.
4. To ensure that the actions decided upon are implemented and documented.

Especially, HAZOP is used not only for safety, but efficient operations. Also, HAZOP is based on analyzing the chain of failure events.

Figure 2.5 provides examples of a typical HAZOP Worksheet and the partially complete HAZOP worksheet for the vapor degreaser system, respectively.

Regarding the strength of HAZOP, HAZOP is easy to apply for analysis since HAZOP is a simple method that can uncover complex accidents. In addition, it is applicable to new designs and new design features. Moreover, HAZOP is performed by a diverse study team and facilitators. This method defines team composition and roles. Also, it encourages the cross-fertilization of different disciplines.



HAZOP WORKSHEET

AREA: ____________ EQUIPMENT/PROCESS: ____________ TEAM : ____________

DATE: ____________ PAGE: ____________

ITEM	GUIDE WORD	DEVIATION	POSSIBLE CAUSES	POSSIBLE CONSEQUENCES	SAFEGUARDS	RAC	RECOMMENDED ACTION(S)	REMARKS

HAZOP WORKSHEET

AREA: Vapor Degreaser EQUIPMENT/PROCESS: Freon 113 Transfer TEAM : J. Doe; T. Smith; C. Hope; V. Jones; A. Ford

DATE: 29 September 2012 PAGE: 1 of 1

ITEM	GUIDE WORD	DEVIATION	POSSIBLE CAUSES	POSSIBLE CONSEQUENCES	SAFEGUARDS	RAC	RECOMMENDED ACTION(S)	REMARKS
1	Flow	No Flow	Valve closed	Pump deadhead	Engineering design; By-pass line	4D	None	None
			Pump failure	None	Back-up pumps	4D	None	None
			Pump off	None	Back-up pumps	4E	None	None
			Power failure	None	Back-up generator	4E	Ensure back-up is functional	None
			Line break	Spill of chemicals	Procedural control; Periodic inspection of lines; Monitored operations	3C	None	None
2	Flow	Low Flow	Pump reversed	Inadequate transfer; Tank vacuum not possible (Tank open to atmosphere)	Procedures require rotation check. Vent and line caps in place.	3C	Ensure operator training is adequate	None
			System obstruction	Inadequate transfer; Contamination	Procedures require rotation check. Vent and line caps in place.	3B	None	None
3	Pressure	High Pressure	Closed valve	Pump deadhead	Procedures; Training	3C	None	None
			System obstruction	Inadequate transfer; Contamination	Procedures require rotation check. Vent and line caps in pl	3B	None	None

Figure 2.5. Sample HAZOP worksheet and the partially complete HAZOP worksheet for the vapor degreaser system cited from [1]

2.4 STAMP (STPA)

Systems Theoretic Accident Model and Process (STAMP) is a new system-theoretic model of accidents, which replaces the traditional chain-of-events model underlying most current accident investigation, prevention, and assessment procedures. The model of STAMP includes hardware, software, organizations, management, human decision-making, and migration of systems which will eventually reach states of heightened risk over time. [4]

STAMP is based on systems theory and control theory. Complex systems are shown as hierarchical structure like Figure 2.6. [5] Accidents are more than a chain of events, and they involve complex dynamic processes. STAMP treats accidents not as a failure, but as a control problem, so STAMP focuses on preventing accidents by enforcing constraints on component behavior and interactions. STAMP treats accidents holistically and identifies more causes of accidents, such as, component failure accidents, unsafe interactions among components, complex human and software behaviors, design errors, and flawed requirements like software-related accidents. In short, accidents are caused by inadequate control in the system.

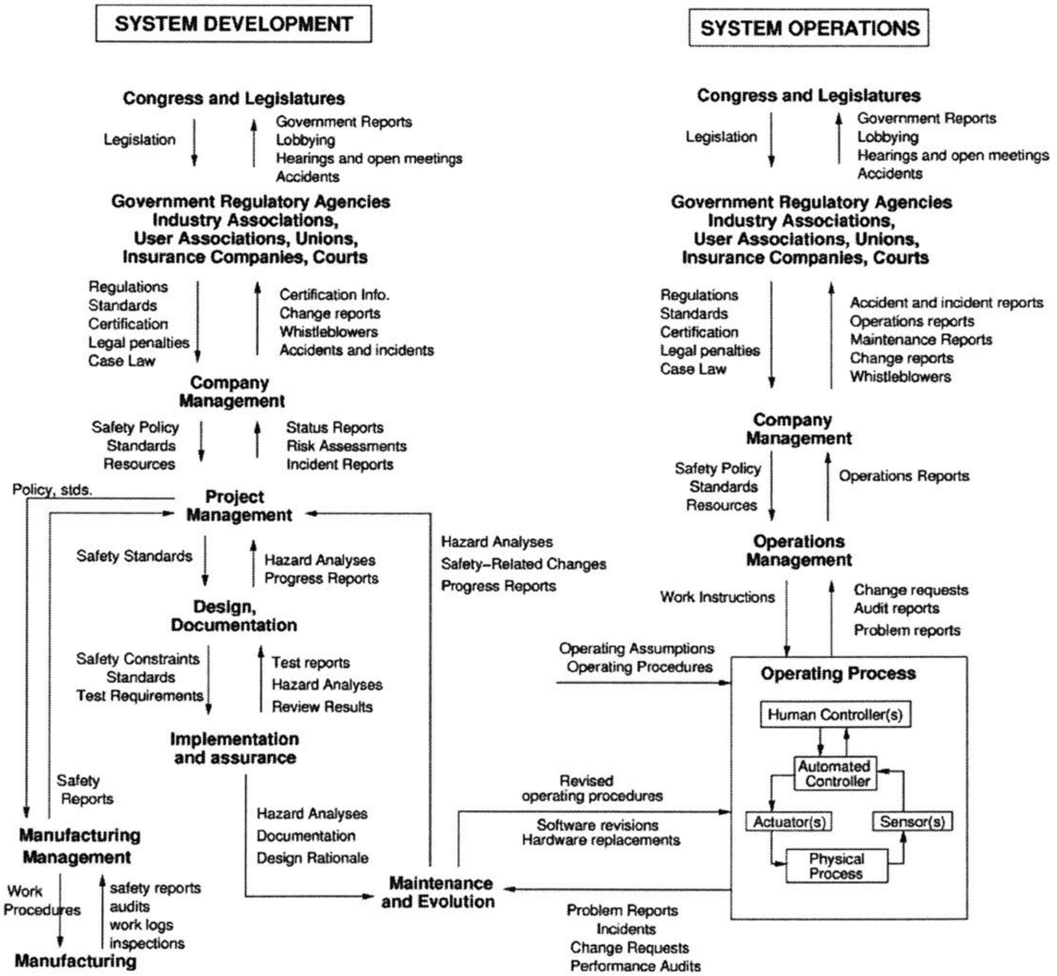


Figure 2.6. Generic example of a hierarchical control structure cited from [5]

System-Theoretic Process Analysis (STPA) is a new approach to hazard analysis based on the STAMP causality model. STPA is the way in which we can find inadequate controls in a design of the system. STPA identifies scenarios leading to identified hazards. These scenarios lead to losses so they should be eliminated or controlled. Many traditional techniques were designed to prevent component failure accidents. However, STPA was designed to address the increasingly common component interaction accidents. These accidents can result from design flaws or unsafe interactions among operational components. [6]

STPA has mainly two steps. [4]

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur due to:
    a. A control action required for safety is not provided or not followed;
    b. An unsafe control action is provided;
    c. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequences;
    d. A control action required for safety is stopped too soon or applied too long.
2. Determine how each potentially hazardous control action identified in Step 1 could occur.
    a. For each unsafe control action, identify scenarios that could cause the unsafe control actions. Controls and mitigation measures need to be designed if they do not already exist or evaluate existing measures when the analysis is being performed on an existing design.

For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.

b. Consider how the designed controls could degrade over time and build in protection, including

  I. Management of change procedures to ensure safety constraints are enforced in planned changes.

  II. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operational audits and controls so that unplanned changes that violate the safety constraints can be detected.

  III. Accident and incident analysis to trace anomalies to the hazards and to the system design.

2.3 References

[1] Jeffrey W. Vincoli. (2014), "Basic Guide to System Safety, Third Edition," Wiley.

[2] Huq MS, Fraass BA, Dunscombe PB et al (2008)., "A method for evaluating quality assurance needs in radiation therapy," Int J Radiat Oncol Biol Phys. 2008, 71 (1 Suppl): S170-S173.

[3] International Commission on Radiological Protection (2009), "Preventing accidental exposures from new external beam radiation therapy technologies," Annals of the ICRP 39(4).

[4] Nancy G. Leveson (2012), "Engineering a safer world: systems thinking applied to safety," MIT Press.

[5] Nancy G. Leveson (2003), "A New Accident Model for Engineering Safer Systems," Safety Science.

[6] Nancy G. Leveson (2013), "An STPA Primer," available at http://sunnyday.mit.edu/STPA-Primer-v0.pdf

Chapter 3. Tomographic Treatment System as a Case Study Overview

In this chapter, tomographic treatment is described by the physical system structure including safety information of the system. As a concrete existing system, TomoTherapy is used as the target device for my analysis.

3.1 Tomographic Treatment

Tomography is a term that combines "tomos" with "graphien." "Tomos" is a Greek word, and is defined as a section or slice. Also, "graphien" means to measure or write. In academic fields like archeology, oceanography, astrophysics, material science, and others, tomography is widely used. However, it is best known for Medical Imaging (MI), and its applications are essential for cancer physicians and researchers. Providing 3D views of internal anatomical structures of patients, like bones and organs, by MI tomography helps preventions against cancer. [1]

Cancer widely exists in various parts of the human body. Before using MI technologies, it was quite difficult for physicians to find and detect a wide spectrum of cancer. For this, they had to execute exploratory surgeries. Because of advancement of virtual MI, they mainly rely on detecting cancer using tomographic images without examination of anatomical structures.

There are mainly two types of tomography, namely, basic X-ray tomography and computed tomography. In the first, X-ray that can produce two dimensional, black and white images of skeletal structures as well as views of denser tissues is used for tomography. Using basic X-ray tomography, radiologists and other clinical specialists create a sectional image of anatomical structures. MI technicians can utilize subtle or distinct variations in the movement of the X-ray source and film to indicate specific focal planes that concentrate on the anatomical structure that clinicians want to check.

In the 1930s, the first basic X-ray tomography was designed by the radiologist, Alessandro Vellabona. It has proven that the medical images produced using basic X-ray tomography are precious to oncologists who first need to confirm the presence of cancer in the process of deciding on appropriate treatment for patient's disease. Nowadays, various and advanced variations of tomography are used through the application of tomographic reconstruction algorithms working on a computer.

Computed tomography (CT) can create high resolution, 3D medical images of the interior of a solid target through use of an extensive series of standard, 2D X-ray images that are captured around a single axis of rotation. A narrow beam of x-rays is aimed at a patient and quickly rotated around the body, and then, produce signals that are processed by the machine's computer to produce cross-sectional images, which is also called "slices" of the body. The images of slices are called tomographic images. The images contain more detailed information than conventional X-rays. Once a number of successive slices are collected by the machine's computer, they can be digitally "stacked" together to form a 3D image of the patient that allows for easier identification and location of basic structures as well as possible tumors or abnormalities. Use of CT has increased dramatically over the last two decades in many countries. [2]

3.2 TomoTherapy

There are many tomographic treatment systems. TomoTherapy® Highly Integrated Adaptive Radiotherapy (HI-ART) is one of the tomographic treatment systems used all over the world. It shares a lot of technology with CT scanners. It has been known as computerized tomography. In the following, some of its capabilities are listed: [3]

- TomoTherapy will do a quick CT scan before each treatment starts, to ensure the patient is correctly aligned.
- A thin beam rotates around the body, entering from many directions. This results in thousands of little beamlets of different intensities entering the body, converging on the tumors.
- A powerful multiple-processor computer calculates the treatment plans and coordinates treatment delivery.
- TomoTherapy can treat large or small tumors, single or multiple tumors, one region of the body or several regions, to the same dosage in every area or to multiple different dosages.
- TomoTherapy can avoid certain organs. Specialists can avoid the salivary glands and treat the throat tumor, avoid the spinal cord and re-treat the spinal bone, avoid the kidneys and treat the pancreas.

TomoTherapy is actually a form of intensity modulated radiation therapy (IMRT). TomoTherapy has been particularly valuable for the following conditions:

- Re-treating previously irradiated areas of the body
- Treating multiple metastases simultaneously
- Treating all metastases throughout the body simultaneously
- Treating a wide spectrum of cancer such as lung cancers, breast cancers, and prostate cancers

Many radiation oncologists are reluctant to give radiation repeatedly to the same part of the patient's body that has already received radiation in the past. It can be dangerous to re-irradiate, since users could risk complications such as excessive scarring, ulceration or pain. However, TomoTherapy is a good choice for re-treating tumors that have already been irradiated. TomoTherapy is so targeted, and it can make it safer to re-irradiate, because the surrounding healthy tissues will receive less radiation dose.

In the history of TomoTherapy, Helical TomoTherapy was developed at the University of Wisconsin more than 20 years ago, with the purpose of integrating an intensity-modulated radiotherapy (IMRT) machine with a highly image-guided system, useful to verify the setup of the patient just before the treatment. [4], [5]

Currently, more than 280 TomoTherapy treatment centers are available worldwide and among the approximately 80 centers in European countries, most of them are located in France and Italy. [6]. TomoTherapy combines an advanced form of IMRT, with the accuracy of CT scanning technology, all in one machine.

With this advanced technology, a specialist can give powerful and precise radiation beams to treat tumors that exist in the areas that are hard to reach. Using built-in CT scanning to confirm the shape and position of the tumor before each treatment, TomoTherapy reduces radiation exposure to healthy tissues and organs.

Before every treatment, advanced scanning technology provides a 3D image of the treatment area, so the radiation beams can be targeted according to the size, shape and location of the tumors on that specific day.

During treatment, the specialist can adjust the intensity and direction of the radiation beams in real time. The revolutionary "slice therapy" approach treats tumors one layer at a time. In short, side effects are often minimized because less radiation reaches healthy tissues and organs. Many cancer patients who have reached their maximum tolerance dose of traditional radiation may be a candidate for TomoTherapy radiation.

The steps of TomoTherapy are described below.

As a pre-planning and planning stage, before each treatment, a therapist takes a verification CT image (VRCT) of the treatment site to check the exact size, shape and location of the tumor. Some tumors change shape or even shift position from day-to-day. Based on the first VRCT images taken, the therapist may change patient's position or move the couch slightly to make sure the treatment targets the correct area.

After the VRCT image is taken, a physician decides how much radiation the tumor should receive, and calculates acceptable levels of radiation for surrounding, healthy tissues. From here, the TomoTherapy is configured to the appropriate pattern, position and intensity of radiation for patients' treatment. The couch then carries the patients through the machine once again, this time more slowly, as the system delivers radiation treatment.

After that, TomoTherapy combines IMRT with a spiral delivery pattern. During radiation treatment, radiation is delivered by a linear accelerator that rotates many times around the patient. The linear accelerator also moves in association with a device, called a multi-leaf collimator (MLC), that's part of the system. The MLC has two sets of interlaced leaves that modulate radiation beams while the patient is being moved slowly through the center of the machine's ring while lying on the machine's couch. As the radiation is being delivered, it is constantly modulated to target the exact size and shape of patients' cancer, including multiple sites at the same time.

The procedure usually takes about 15 minutes. It is important that the patient moves as little as possible during the actual treatment. It is painless and feels no different from having a CT scan or an X-ray taken. They may hear a clicking noise and the hum of the machine. These are normal sounds that the system makes. The patient will not feel or see the treatment as it is being performed. Data from the treatment is totally integrated in the system.

3.3 System Structure of TomoTherapy

System structure of TomoTherapy is available at "Hi-Art System Physics Guide" [7]. Based on this guide, the physical system structure is described in the following.

3.3.1 Treatment Room

The treatment room of TomoTherapy typically contains the following components.

- Gantry and Equipment Enclosures: The rotating gantry assembly generates and delivers radiation to patients, with the enclosures covering the gantry. The equipment enclosures are detachable and can roll forward for service access. Gantry has many mechanical features:
  - ➢ Degrees of rotation: Rotates around IEC-y axis, continuous rotation
  - ➢ Direction of rotation: Clockwise viewed from the foot of the couch

- ➢ Rotation angle accuracy: Within 0.5 degrees
- ➢ Speed of rotation: Varies; dependent upon plan
- ➢ Controls: Rotational speed set during treatment planning
- ➢ Source to axis distance: 85 cm
- ➢ Mechanical to radiation isocenter offset: Included in beam model (within accuracy 0.25 mm)
- ➢ Mechanical isocenter stability: < 0.4 mm
- ➢ Position indicators: 5-axis laser system
- ➢ Isocenter height: 113 cm typical (dependent upon finished flooring)
- ➢ Cooling: Integrated cooling system eliminates the need for facility-chilled water loop

- Treatment Couch: The standard treatment couch is used to position the patient during treatment using automatic patient positioning technology.
- Power Distribution Unit (PDU): The Power Distribution Unit (PUD) isolates the power source for all critical accuracy components in the treatment vault and control area and provides power to system components.
- Laser Positioning System: A laser positioning system is used in the treatment room to accurately position patients on the treatment couch. There are a total of seven lasers included within the TomoTherapy System
- Intercom Speaker System: The intercom speaker and all its components allow the patient and clinician to communicate during treatment

There are additional items that can be supplied by users:

- Steel or aluminum plates and mountings for the patient positioning lasers
- Radiation warning lights including cables and a power connection (within 48-240 VAC range)
- Emergency off/ emergency stop buttons and cabling

- Door interlock or reset switch and cabling (1 required depending on vault entry configuration)
- Closed circuit TV cameras (CCTV)

3.3.2 Operator Station

The operator station can be configured in many ways, depending upon the site layout and desire of the customer. Typically, it includes the following equipment.

- Step Down Transformer Unit: The step-down transformer is mounted underneath the counter on a customer-supplied shelving unit.
- Operator Station Status Console: Device that allows the customer to operate the emergency stop, key switch for image/program/treatment options, start button, stop button, radiation on notification.
- Operator Station Workstation: The operator station is the computer workstation that the technologists use for calibration, patient positioning, registration, imaging, and treatment. The control station is composed of a computer, flat screen monitor, and keyboard.
- Intercom Speaker System: It is the intercom desk control unit.
- Printer: This is just a standard laser-jet printer.

There are additional items that can be supplied by users:

- Main Power Disconnect
- EO (Emergency Off) Push Button: It should be installed on the wall in the control room.
- Phone with Long Distance Access: The phone is used for routine service and emergency communication.
- Closed Circuit TV (CCTV) Monitoring System

- Customer Network Data Port with Internet Access or Wireless Internet Access: To be used by ACCURAY personnel during system installation and service activities.
- Emergency Components.
- Physics Conduit Port (Dosimetry Tube) into the Treatment Room: This port is used for running Quality Assurance and Commissioning tools and equipment cables between the control room and the treatment room. It is typically a 4-inch (100 millimeters) conduit that runs from the top of the control room desk to the lower wall of the treatment room at a 45-degree angle, both vertically and horizontally, with access boxes and/or doors on either end.

3.3.3 Data Server Room

The data server room location can be configured in many ways, depending upon the site layout, and the desire of the customer. The data server room is intended to hold the server rack required for the TomoTherapy.

The supplied item a Data Server Unit: The data server unit is where patient data is imported and stored, and the optimization engine is where dose optimization and dose calculations are performed.

There are additional items that can be supplied by users as follows.

- Air Conditioning Unit
- Network Connections
- Electrical equipment such as thermostats, temperature sensors, and etc.

3.3.4 Mechanical Room

The mechanical room is typically located near the treatment room and is intended to hold the mechanical equipment required for TomoTherapy.

- Compressed Air Line: The facility must supply a dedicated oil-free air compressor. In the floor of the treatment room, there is a copper compressed air line from the facility-supplied oil-free air compressor.
- Air Compressor and Tank: Installation of a delicate, facility-supplied oil-free air compressor to meet the flow-rate and quality requirements is required. Also, it is recommended to install a scroll compressor. The facility must supply a 60-gallon (227-liter) or greater air tank and install it in the mechanical room near the air compressor. It sets the air tank to automatically purge for four to five seconds every 30 minutes
- Common Supplier: Atlas Copco, model SF-6-FF
- Dryer: The facility must supply a dryer to maintain a dew point of 34 to 40 Fahrenheit (1 to 4 Celsius). If mechanical room is not adjacent to the treatment room, a secondary dryer may be required to eliminate condensation.
- Inline Air Regulator: Installation of an inline air regulator in an unobstructed and accessible location in the treatment room is required. If unable to place it in the treatment room, it needs to have installation of the inline air regulator in the mechanical room with the air compressor. Installation of an inline shut-off valve between the air compressor and the air regulator is required.

3.3.5 Treatment Planning Room

The treatment planning room can be anywhere and be configured in many ways, depending upon the site layout and desire of the customer. It is important that this room be ready for equipment and setup prior to system installation. Typically, the treatment planning room includes the following equipment.

- Treatment Planning System: The planning station is the computer workstation where the clinician analyzes patients' computed tomography (CT) image data and uses them to create an optimized treatment plan. The facility must have an on-site CT device that generates DICOM images.
- Printer: Standard laser-jet printer.
- Network Connections.
- Vidar Scanner/ Film Analyzer: In addition to standard computer components, the treatment planning room may include a Vidar scanner and a film analyzer workstation.

3.4 Safety Information of TomoTherapy

Improper use of TomoTherapy would cause serious injury or death for patients and users because it is a radiation device. According to the published Physics Guide of Hi-Art System, there are safety descriptions about General Safety, Couch Load, Laser Beam Safety, Radiation Safety, Pinch Points, Electrical Safety, Use of Quality Assurance Procedures, Modifications to Machine Data Files, and Integrity of Calibration and Commissioning Files. The safety measures are listed below:

[General Safety]

- Only properly trained personnel should operate TomoTherapy.
- Make sure all signs required by local codes for the operation of a radiation device and the presence

of radiation are posted.

- When operating TomoTherapy, always follow the procedures and monitoring requirements established by a facility's radiation safety officer.
- Make sure all gantry enclosures are in place before operating TomoTherapy.
- Make sure all safety mechanisms are functioning correctly as specified in "Quality Assurance" of "Hi-Art System Physics Guide".
- Obey all safety descriptions in this section

[Couch Load]

- Excessive couch sag can cause inaccurate delivery of radiation. Couch of TomoTherapy is not designed to support a load greater than 200kg (440 lbs).

[Laser Beam Safety]

- Lasers are used with TomoTherapy to help users correctly position patient's shadow for use with its procedures described in "Hi-Art System Physics Guide". Looking directly into the laser beams can result in permanent retinal damage. Never look directly into the laser beams.
- The potential for incorrect patient positioning and serious injury to the patient during treatment can occur if the lasers that are designed specifically for TomoTherapy are not used. Users do not use any other laser equipment to perform the instructions described in "Hi-Art System Physics Guide".

[Radiation Safety]

- The delivery system generates radiation during quality assurance procedures. To avoid unnecessary exposure to radiation, the treatment room must be unoccupied. Before the entrance is secured, make sure there are no personnel in the treatment room.

[Pinch Points]

- Pinch points, which are created by movement of the patient couch, can cause serious injury:
  - ➢ When using the couch controls on the positioning control panel of TomoTherapy, make sure that users say clear of moving parts.
  - ➢ If necessary, press the stop button on positioning control panel to stop movement of the couch.

[Electrical Safety]

- Connection of non-compliant peripherals to TomoTherapy can compromise the electrical safety of the components and result in serious injury to the patient or operator:
  - ➢ Only peripherals in compliance with IEC 60950, and approved by TomoTherapy Incorporated, should be connected to TomoTherapy
  - ➢ Always call TomoTherapy Incorporated before connecting peripheral accessories

[Use of Quality Assurance Procedures]

- Treating a patient with a quality assurance procedure can cause serious injury to the patient. These types of procedures must be performed only by a qualified radiation oncology physicist employed by a user's facility. Creation and delivery of these procedures is restricted to physicist, super user, and service engineer user types.
- Do not treat a patient with a quality assurance procedure intended for machine commissioning and calibration purposes.

[Modifications to Machine Data Files]

- Modifications to machine data files, performed by unqualified personnel, can result in serious injury to the patient during treatment. Modification of data files are to be done by qualified personnel in accordance with accepted practices and protocols relevant to specific machine applications and usage. The following points should be understood:
  - ➢ The quality of treatment delivered to the patient is critically dependent upon the accuracy of the data representing the properties of the delivery system.
  - ➢ If machine data is modified, the new machine definition must be representative of the machine properties.
  - ➢ Safety-related features associated with the machine definition such as radiation output checking, should never be disabled in machine data that is to be used in clinical deliveries. Such changes can result in inaccurate delivery of radiation and serious injury to the patient.

[Integrity of Calibration and Commissioning Files]

- Treatments based on incorrect calibration or commissioning data may result in serious injury or death to the patient. After TomoTherapy has been commissioned, do not alter any calibration of commissioning data files on the Optimization Server. If there has been a significant change to the dosimetric properties of the machine, it is recommended to contact TomoTherapy Incorporated for assistance.

3.5 References

[1] Mesothelioma Aid (2017), "Tomography Applications in Cancer Diagnosis, Prognosis Treatment, and Research," available at http://www.mesothelioma-aid.org/tomography.htm

[2] Rebecca Smith-Bindman et al. (2009), "Radiation Dose Associated with Common Computed Tomography Examinations and the Associated Lifetime Attributable Risk of Cancer," Arch Intern Med. 2009 Dec 14; 169(22): 2078–2086.

[3] Cancer Treatment Centers of America (2017), "What is TomoTherapy," available at: http://www.brachytherapy.com/tomotherapy.aspx

[4] Mackie T.R. et al. (1993), "Tomotherapy: a new concept for the delivery of dynamic conformal," Med. Phys. 20, 1709-1719.

[5] Mackie T.R. et al. (1999), "Tomotherapy," Semin. Radiat. Oncol.9, 108-117.

[6] ACCURAY (2017), "Treatment Centers," available at: http://www.accuray.com/treatment-centers

[7] Accuray Incorporated (2014), "TomoTherapy H^{TM} Series Site Planning Guide."

Chapter 4. Application result of FMEA

The aim of the application of the failure mode and effects analysis (FMEA) approach was to assess the risks for patients during the three important phases in TomoTherapy.

4.1 Overall

According to the analysis by Broggi et al, [1] [2] FMEA was applied to identify all the sub-processes involved in the stages of (A) preplanning imaging and volume determination, (B) treatment planning and (C) delivery. This analysis consisted of three steps: 1) identification of the involved sub-processes; 2) identification and ranking of the potential failure modes, together with their causes and effects, using the risk probability number (RPN) scoring system; and 3) identification of additional safety measures to be proposed for process quality and safety improvement. In this analysis, a total of 104 failure modes were identified: 38 in the stage of preplanning imaging and volume determination, 36 in the stage of planning, and 30 in the stage of delivery.

4.2 Materials and Methods

In their analysis, FMEA was applied to identify all the sub processes involved in the stages of (A) preplanning imaging and volume determination, (B) treatment planning and (C) delivery. After that, the potential failure modes including their causes and effects, were identified and ranked in order of importance. The ranking of the failure modes was carried out by using the risk probability number (RPN) system. RPN is obtained as a product of three indices: the occurrence rate (O), the severity rate (S) and the detectability rate (D). In addition, a ten-point scale was used to score each category, ten being the number indicating the most severe, most frequent, and least detectable failure mode, respectively. The ranking proposed by Ford et al. [3] were used as its guidelines. Also, the risk probability number (RPN) was calculated as the product of the three attributes: RPN = O x S x D. The value RPN = 125 was considered as a threshold below which the risk can be considered acceptable.

The analysis was carried out by a working group of five people: three medical physicists and two radiation oncologists, and by two additional external physicists with experience and competence in radiation protection and in risk management strategies for radiotherapy.

4.3 Results

The process trees developed by the group is shown in Figures 4.1, 4.2 and 4.3. The process consists of three main process steps and 74 sub-processes (30 sub-processes in the pre-planning and volume determination stage, 28 sub-processes in the planning stage and 16 sub-processes in the delivery stage).

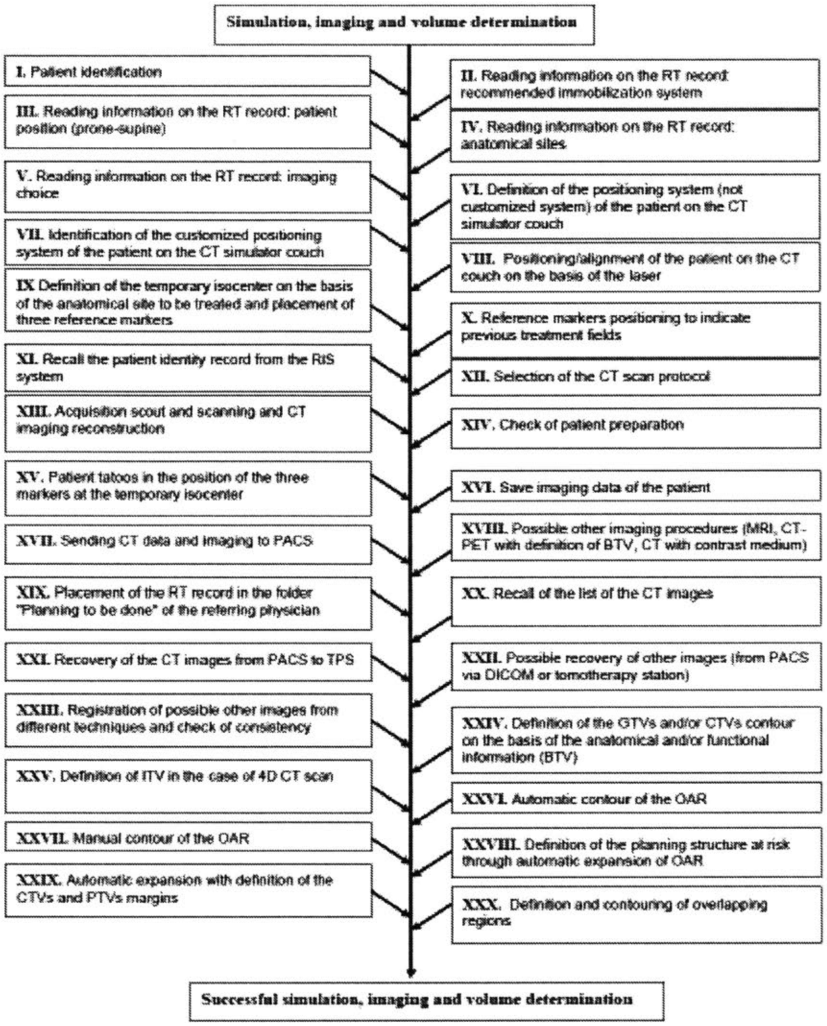

Simulation, imaging and volume determination
I. Patient identification
II. Reading information on the RT record: recommended immobilization system
III. Reading information on the RT record: patient position (prone-supine)
IV. Reading information on the RT record: anatomical sites
V. Reading information on the RT record: imaging choice
VI. Definition of the positioning system (not customized system) of the patient on the CT simulator couch
VII. Identification of the customized positioning system of the patient on the CT simulator couch
VIII. Positioning/alignment of the patient on the CT couch on the basis of the laser
IX Definition of the temporary isocenter on the basis of the anatomical site to be treated and placement of three reference markers
X. Reference markers positioning to indicate previous treatment fields
XI. Recall the patient identity record from the RIS system
XII. Selection of the CT scan protocol
XIII. Acquisition scout and scanning and CT imaging reconstruction
XIV. Check of patient preparation
XV. Patient tatoos in the position of the three markers at the temporary isocenter
XVI. Save imaging data of the patient
XVII. Sending CT data and imaging to PACS
XVIII. Possible other imaging procedures (MRI, CT-PET with definition of BTV, CT with contrast medium)
XIX. Placement of the RT record in the folder "Planning to be done" of the referring physician
XX. Recall of the list of the CT images
XXI. Recovery of the CT images from PACS to TPS
XXII. Possible recovery of other images (from PACS via DICOM or tomotherapy station)
XXIII. Registration of possible other images from different techniques and check of consistency
XXIV. Definition of the GTVs and/or CTVs contour on the basis of the anatomical and/or functional information (BTV)
XXV. Definition of ITV in the case of 4D CT scan
XXVI. Automatic contour of the OAR
XXVII. Manual contour of the OAR
XXVIII. Definition of the planning structure at risk through automatic expansion of OAR
XXIX. Automatic expansion with definition of the CTVs and PTVs margins
XXX. Definition and contouring of overlapping regions
Successful simulation, imaging and volume determination

Figure 4.1. Sub-processes of the preplanning imaging and volume determination stage in TomoTherapy cited from [1]

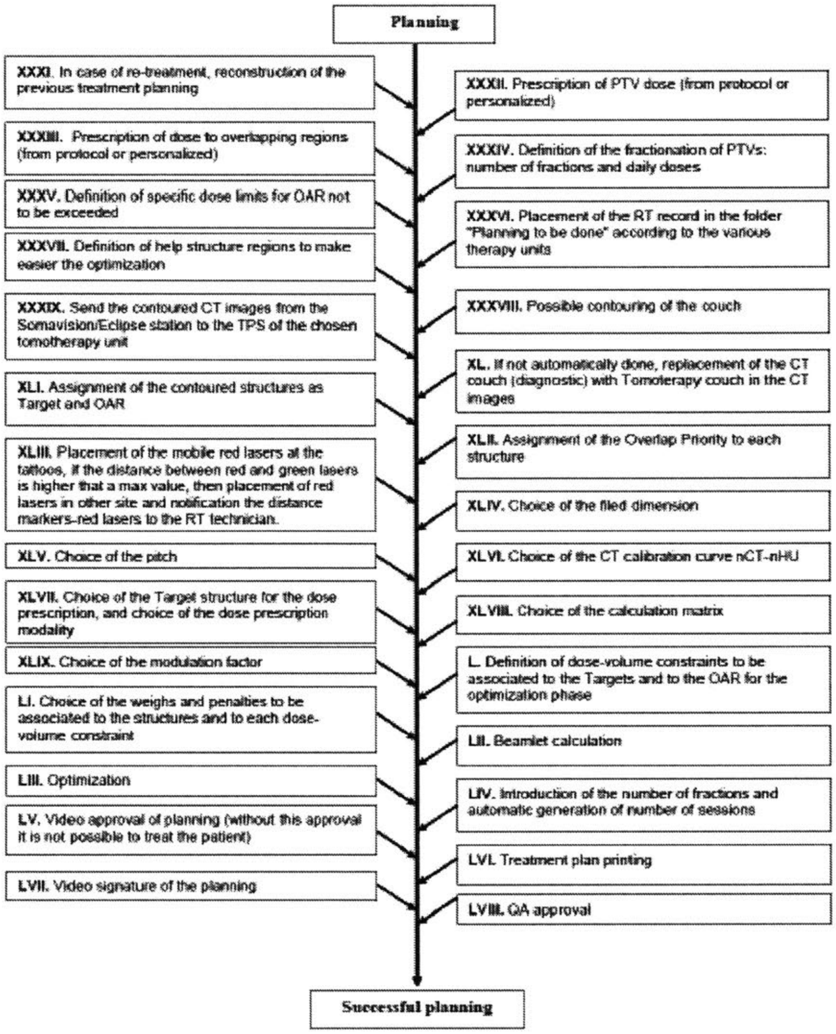

Planning
XXXI. In case of re-treatment, reconstruction of the previous treatment planning
XXXII. Prescription of PTV dose (from protocol or personalized)
XXXIII. Prescription of dose to overlapping regions (from protocol or personalized)
XXXIV. Definition of the fractionation of PTVs: number of fractions and daily doses
XXXV. Definition of specific dose limits for OAR not to be exceeded
XXXVI. Placement of the RT record in the folder "Planning to be done" according to the various therapy units
XXXVII. Definition of help structure regions to make easier the optimization
XXXVIII. Possible contouring of the couch
XXXIX. Send the contoured CT images from the Somavision/Eclipse station to the TPS of the chosen tomotherapy unit
XL. If not automatically done, replacement of the CT couch (diagnostic) with Tomoterapy couch in the CT images
XLI. Assignment of the contoured structures as Target and OAR
XLII. Assignment of the Overlap Priority to each structure
XLIII. Placement of the mobile red lasers at the tattoos, if the distance between red and green lasers is higher that a max value, then placement of red lasers in other site and notification the distance markers-red lasers to the RT technician.
XLIV. Choice of the filed dimension
XLV. Choice of the pitch
XLVI. Choice of the CT calibration curve nCT-nHU
XLVII. Choice of the Target structure for the dose prescription, and choice of the dose prescription modality
XLVIII. Choice of the calculation matrix
XLIX. Choice of the modulation factor
L. Definition of dose-volume constraints to be associated to the Targets and to the OAR for the optimization phase
LI. Choice of the weighs and penalties to be associated to the structures and to each dose-volume constraint
LII. Beamlet calculation
LIII. Optimization
LIV. Introduction of the number of fractions and automatic generation of number of sessions
LV. Video approval of planning (without this approval it is not possible to treat the patient)
LVI. Treatment plan printing
LVII. Video signature of the planning
LVIII. QA approval
Successful planning

Figure 4.2. Sub-processes of the planning stage in TomoTherapy cited from [1]

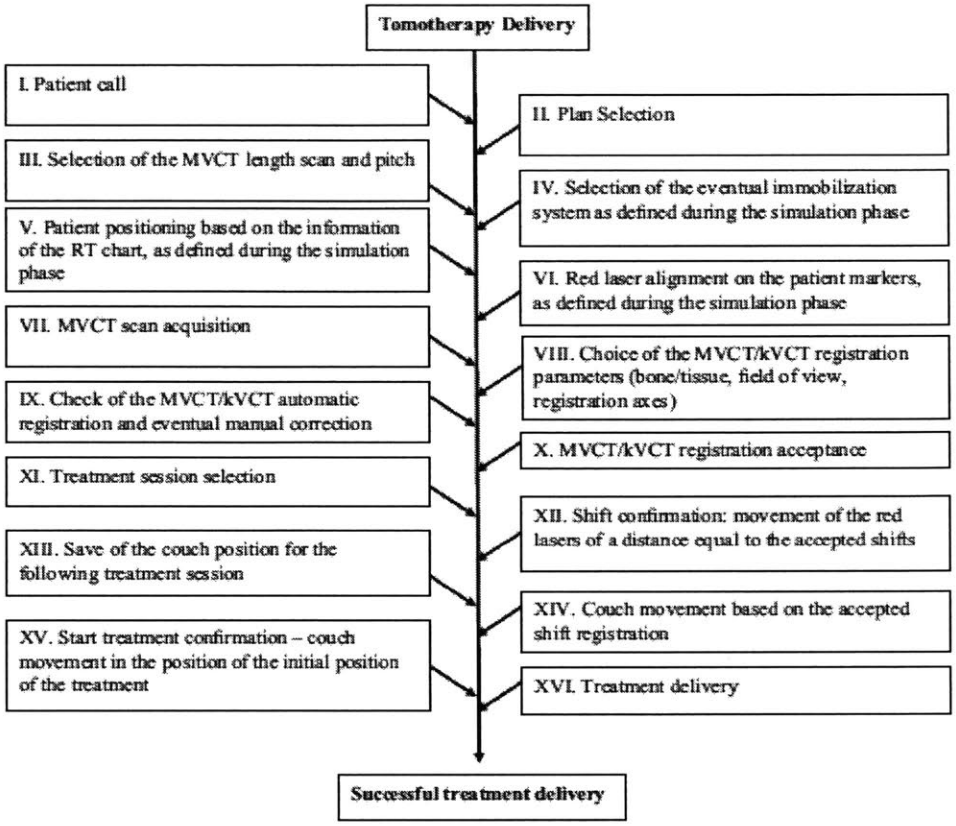

Tomotherapy Delivery
I. Patient call
II. Plan Selection
III. Selection of the MVCT length scan and pitch
IV. Selection of the eventual immobilization system as defined during the simulation phase
V. Patient positioning based on the information of the RT chart, as defined during the simulation phase
VI. Red laser alignment on the patient markers, as defined during the simulation phase
VII. MVCT scan acquisition
VIII. Choice of the MVCT/kVCT registration parameters (bone/tissue, field of view, registration axes)
IX. Check of the MVCT/kVCT automatic registration and eventual manual correction
X. MVCT/kVCT registration acceptance
XI. Treatment session selection
XII. Shift confirmation: movement of the red lasers of a distance equal to the accepted shifts
XIII. Save of the couch position for the following treatment session
XIV. Couch movement based on the accepted shift registration
XV. Start treatment confirmation – couch movement in the position of the initial position of the treatment
XVI. Treatment delivery
Successful treatment delivery

Figure. 4.3. Sub-processes of the delivery stage in TomoTherapy cited from [2]. In cases of treatment interruption such as system crash, after generation of the completion procedure and patient repositioning in the starting position, the process will start again from step XV.

A total of 104 failure modes were identified: 38 in the stage of preplanning and volume determination, 36 in the stage of planning, and 30 in the stage of delivery.

21 failure modes were characterized by a RPN score higher than 80. Ten of them, shown in Table 4.1, were identified in the stage of preplanning imaging and volume determination. Also, 11 failures having an assigned RPN >80 were identified in the stage of planning and shown in Table 4.2. In addition, nine were judged to be of this concern (RPN > 80) in the stage of delivery, which is shown in Table 4.3.

Table 4.1. *Application of failure mode and effects analysis for the preplanning imaging and volume determination stage in TomoTherapy cited from [1]. Failure modes having an assigned RPN of 80 are reported.*

Sub process	No	Potential Failure Mode	Potential Causes of Failure	Potential Effects of Failure	O	S	D	RPN
VIII Positioning/alignment of the patient on the CT couch on the basis of the laser	1	Wrong definition of the isocenter	Inadequate CT laser alignment	Systematic shift of the patient position	4	8	3	96
X Reference markers positioning to indicate previous treatment fields	2	Missing marker positions	Lack of attention or incomplete compilation of the RT record	Previous treatment not taken into consideration/suboptimal planning	4	8	3	96
XXIII Registration of possible other images	3	Wrong registration	Consistency not verified	Wrong planned target volume(PTV)) and organs at risk (OAR) definition	3	7	5	105

from different techniques and check of consistency								
XXIV Definition of the gross tumor target volumes (GTVs) and/or clinical target volumes (CTVs) contour on the basis of the anatomical and/or functional information (BTV)	4	Wrong CTV definition	Lack of attention/inadequate skill	Wrong dose distribution	3	7		105
XXV Definition of internal target volume (ITV) in the case of 4D CT	5	Incorrect ITV construction	Lack of attention/inadequate skill	Wrong PTV	3	6	5	90

acquisition								
XXVI Automatic contour of the OAR	6	Missing OAR definition	Lack of attention/inadequate skill	Unintended normal tissue irradiation	3	8	5	120
XXVII Manual contour of the OAR	7	Missing OAR definition	Lack of attention/inadequate skill	Unintended normal tissue irradiation	3	8	5	120
XXVIII Definition of the planning structure at risk through automatic expansion of OAR	8	Wrong expansion	Lack of attention/inadequate skill	Unintended normal tissue irradiation	3	5	6	96
XXIX Automatic expansion with definition of the CTVs and PTVs	9	Wrong expansion	Lack of attention/inadequate skill	Unintended normal tissue irradiation	3	5	6	96

margins								
XXX Definition and contouring of overlapping regions	10	Wrong/missed definition	Lack of attention/inadequate skill or not detailed information on previous treatment	Unintended normal tissue irradiation or wrong dose distribution	4	7	5	140

Table 4.2. *Application of failure mode and effects analysis for the planning stage in TomoTherapy cited from [1]. Failure modes having an assigned RPN of 80 are reported.*

Sub process	No	Potential Failure Mode	Potential Causes of Failure	Potential Effects of Failure	O	S	D	RPN
XXXII Prescription of PTV dose (from protocol or personalized)	11	Wrong prescription in the record	Lack of attention/inadequate skill	Wrong dose delivery	3	8	4	96
XXXIII Prescription of dose	12	Wrong prescription in the	Lack of attention/inadequate skill	Possible wrong dose distribution/wrong dose	3	8	4	96

to overlapping regions (from protocol or personalized)		record		delivery				
XXXIV Definition of the fractionation of PTVs: number of fractions and daily doses	13	Wrong prescription in the record	Lack of attention/inadequate skill	Wrong dose delivery	3	8	4	96
XXXV Definition of specific dose limits for OAR, not to be exceeded	14	Wrong prescription in the record	Lack of attention/inadequate skill	Unintended normal tissue irradiated	3	8	4	96
XXXVIII Possible contouring of the couch	15	Incorrect dose calculation	Incorrect positioning in the imaging	Wrong dose delivery	2	6	7	84

XL If not automatically done, replacement in the imaging of the CT couch (diagnostic) with TomoTherapy couch	16	Incorrect dose calculation	Incorrect introduction of the couch position in the CT images	Wrong dose delivery	2	6	8	96
XLII Assignment of the Overlap Priority to each structure	17	Wrong assignment	Lack of attention/inadequate skill	Wrong dose distribution	4	7	7	196
XLVI Choice of the calibration curve nCT-nHU	18	Wrong choice (kV-MV)	Lack of attention/inadequate skill	Wrong dose calculation/wrong dose delivery	2	8	9	144
	19	Wrong choice (kV-kV)	Lack of attention/inadequate skill	Wrong dose calculation/wrong dose delivery	2	5	9	90

XLVIII Choice of the calculation matrix	20	Suboptimal choice	Lack of attention/inadequate skill	Suboptimal treatment	3	5	6	90
LIV Introduction of the number of fractions and automatic generation of number of sessions	21	Wrong or not performed choice (erroneous use of the default value)	Lack of attention/inadequate skill	Wrong dose delivery	3	8	6	144

Table 4.3*. Application of failure mode and effects analysis for the delivery stage in TomoTherapy cited from [2]. Failure modes having an assigned RPN of 80 are reported.*

Sub process	No	Potential Failure Mode	Potential Causes of Failure	Potential Effects of Failure	O	S	D	RPN
I Patient all	1	Wrong patient identification	Lack of attention	Wrong treatment for a single session	84	7	2	6

		(with the same anatomical site)			
	2	Delivery of a single procedure and not "double procedure" in cases where the daily dose (hypo-fractionatio n schedule) cannot be delivered in a single procedure	Lack of attention and /or inadequate radiotherapy (RT) chart compilation	Wrong dose delivery for several fractions. Impact on the radiobiological effect	8 3 7 168
	3	Delivery of a single procedure and not "double procedure" in cases where the	Lack of attention and /or inadequate RT chart compilation	Wrong daily dose delivery. Impact on the radiobiological effect	5 3 7 105

		daily dose (hypo-fractionation schedule) cannot be delivered in a single procedure						
	4	Plan selection of the wrong patient (same anatomical site but not yet treated)	Lack of attention	Wrong treatment for a single session	7	2	6	84
VIII Choice of the kilovoltage CT (kVCT)/megavoltage CT (MVCT) registration parameters	5	kVCT/MVCT automatic registration in 6 directions (and not in 4)	Lack of attention and/or inadequate skill	Wrong patient positioning/alignment and not correspondent to the visible and approved kVCT/MVCT matching	4	4	8	128

(registration axis)								
IX Check of the kVCT/MVCT automatic registration and eventual manual correction	6	Wrong kVCT/MVCT matching	Inadequate skill	Wrong patient positioning/alignment, wrong dose delivery	5	4	9	180
X kVCT/MVCT registration acceptance	7	The "Accept" option is not selected on the treatment console	Lack of attention and/or inadequate skill	Loss of all the information concerning the registration, inadequate treatment	4	4	8	128
XIV Couch movement based on accepted shift registration	8	"Setup" button not pressed, no couch movement	Lack of attention	Inadequate daily delivered dose	4	4	8	128
XVI Treatment delivery	9	Temporary treatment delivery	TomoTherapy unit interruption/crash	Wrong patient repositioning with the consequent wrong	8	4	6	192

		interruption with the possibility of completing the procedure		dose delivery	

Note that the only causes considered are human (operator) error and not hardware failures or software errors.

4.4 References

[1] S.Broggi et al. (2013), “Application of failure mode and effects analysis (FMEA) to pretreatment phases in TomoTherapy,” J.Appl. Clin. Med. Phys. 14, 265-277.

[2] S.Broggi et al. (2015), “Application of failure mode and effect analysis to tomotherapy treatment delivery,” Radioprotection 50(3), 171-175.

[3] Ford EC, Gaudette R, Myers L et al. (2009), “Evaluation of safety in radiation oncology setting using failure mode and effects analysis,” Int J Radiat Oncol Biol Phys. 2009;74(#):852-58.

Chapter 5. STPA Application

In this chapter, STPA is applied to TomoTherapy, a radiation delivery system. Overall, STPA can be divided into the following processes:

1. System Description
    I. Goals of the system
    II. Accidents in the past
2. Accident and Hazard Identification
3. Descriptions of the hierarchical safety control structure that already exists or needs to be created
4. Identification of Unsafe Control Action Analysis (On STPA Step1)
5. Causal Scenario Analysis (On STPA Step2)

5.1 System Description

This first step is to sum up a description of a target system. This description should focus on the system from both aspects of the organizational side as well as the mechanical side including software.

TomoTherapy is a type of therapy in which radiation is aimed at a tumor from many different directions. The patient lays on a table and is moved through a machine shaped like a ring. The radiation source in the machine rotates around the patient in a spiral pattern. Before radiation, a three-dimensional image of the tumor is taken. This helps doctors to find the highest dose of radiation that can be used to kill off tumor cells while causing lesser damage to nearby cell tissue.

TomoTherapy is a form of computed tomography (CT) guided by intensity modulated radiation therapy (IMRT). Also, it is called helical TomoTherapy.

Generally, radiation therapy has developed with a strong reliance on homogeneity of dose distribution throughout the tumor. TomoTherapy embodies the sequential delivery of radiation to different parts of the tumor, which raises two important issues.

First of all, this method is known as "field matching" and brings with it the possibility of a less-than-perfect match between two adjacent fields with a resulting hot and/or cold spot within the tumor. For the second issue, if the patient or tumor moves during this sequential delivery, then again, a hot or cold spot will result. The first issue can be minimized by the use of a helical motion of the CT x-ray source and the fan beam angle and collimator width, as in spiral CT. The second requires close attention to the position of the target throughout treatment delivery.

(I) Goals of the system

The two main goals of this system:

G1: Develop a radiation therapy device that provides radiation treatment for patients

G2: Design a radiation therapy system that exposes patients to less radiation for efficient radiation therapy

(II) Accidents in the past

Until now, there are no records about recalls or reported accidents about TomoTherapy.

5.2 Defining Accidents and Hazards

Before any hazard analysis can take place, foreseeable accidents and hazards that can potentially lead to accidents must be identified. According to "Engineering a Safer World", [1] an accident is defined as being an undesired and unplanned event that results in a loss, including a loss of human life or injury, property damage, environmental pollution, mission loss, financial loss, and so on. For the purpose of this analysis, the relevant accidents are identified as follow:

A1: Loss of life or serious damage of patients by radiation exposure under the treatment

A2: Loss of life or serious damage of non-patients by radiation exposure during the treatment

A3: Loss of life or serious injury of people by physical damage (not radiation exposure) during the radiation treatment

A4: Loss or damage to the device (mission failure)

A5: Radiation emission to the environment

A6: Condition becoming worse for patients

In Table 5.1 below, I defined the hazards which might be of importance to the stakeholders, including medical practitioners and patients. In addition, I also mentioned the safety constraints of this system.

Table 5.1. Hazards and Definitions

Hazard	Definition
H1. Patients are exposed to wrong amount of radiation (A1)	(a) exposed to too much radiation (b) exposed to too little radiation (c) wrong area exposed to radiation
H2. Non-patients are exposed to radiation (A2)	Non-patients such as medical practitioners and operators are wrongly exposed to radiation emitted from the device
H3. The radiation treatment system damage people physically (A3)	People are injured by the device during its operation or treatment (non-radiological injury)

H4. Equipment is subject to unnecessary loading time, speed, power, and etc. (A4)	Due to unnecessary loading time, speed, power, etc. the equipment does not work properly or breaks down
H5. Environment is exposed to radiation (A5)	Environment around the equipment is exposed to radiation emission from the equipment
H6. Radiation treatment is not provided (A6)	Radiation treatment is not provided for the patient who needs urgent radiation treatment

5.3 Description of the Hierarchical Safety Control Structure

After the system-level hazards have been identified, a hierarchical control structure for the system should be created. It is necessary to consider both the organizational structure and the physical system control structure in terms of two aspects—the software and hardware. According to STPA, a safety control structure is composed of hierarchically organized feedback control loops. The three figures below show simple safety control structures, from level 0 to level 1 (Figures 5.1 and 5.2).

Figure 1 shows the existing safety control structure (level 0) with a controller in the organization layer at the top. In total, I found 12 controllers and 5 control actions in this control structure.

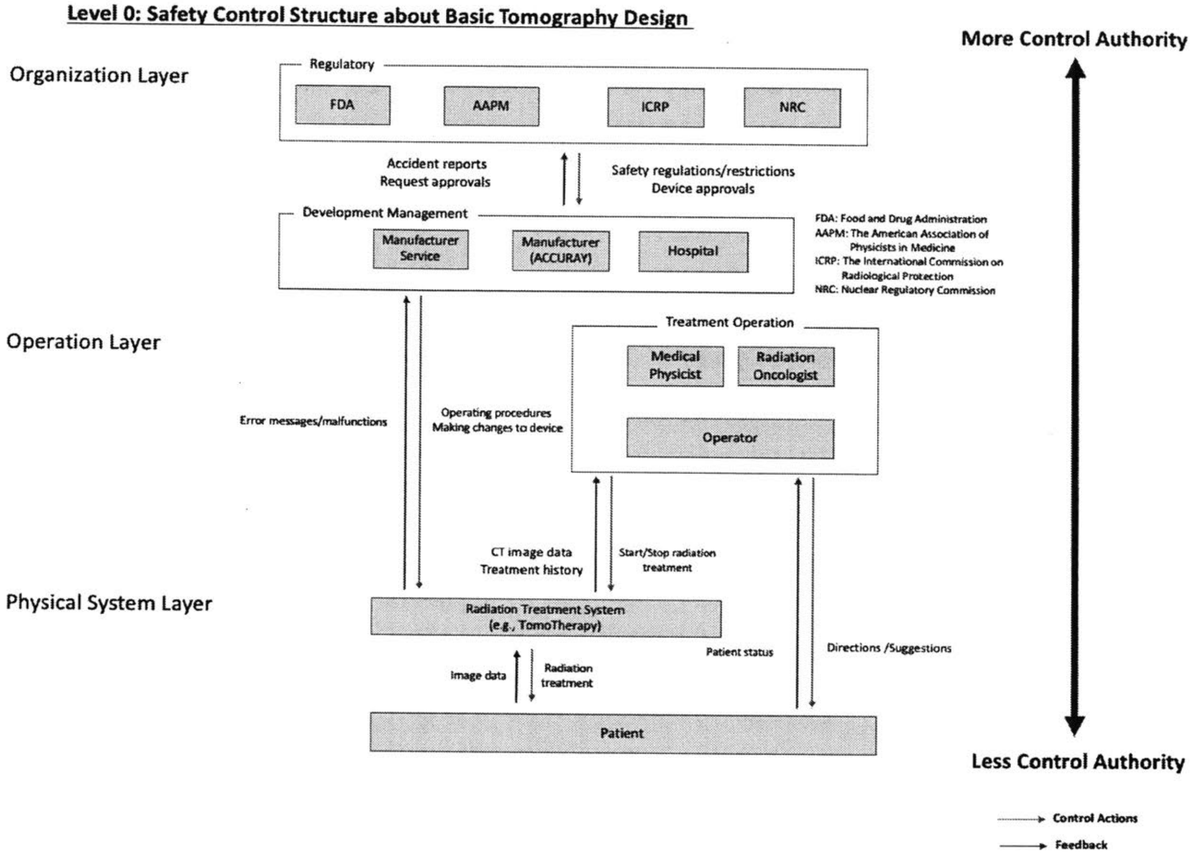


Figure 5.1. Existing safety control structure – Level 0

In this analysis, I am focusing on the operation layer and the physical system layer because accidents often happen in these two stages.

To set up TomoTherapy, it is required to have five rooms; they are the treatment room, the operator station, the data server room, the mechanical room, and the treatment planning room. The explanation of the five rooms is described in Chapter 3.

Using the information mentioned in Section 3.3, the existing physical system's safety control structure is depicted below (Figure 5.3). Also, the explanation about each controller is described in Table 5.2.

Regarding the data server, it does not belong to the category as a control component. It is simply a communication channel.

Table 5.2 Explanation about controllers

No.	Controller	Role	Control Action
1	Radiation Oncologist	Provide his/her special knowledge for radiation treatment, such as dose distribution, and ways to optimize the treatment plan. Also, taking care of a patient and giving recommendations to have radiation treatment	- Giving suggestions for radiation treatment - Giving advice and follow-up care for patients
2	Medical Physicist	Provide his/her clinical knowledge to prepare a treatment plan and evaluate the setup of patients. Also, giving knowledge about imaging technique and technology/skills	- Giving a treatment plan - Requesting an optimization of the treatment plan
3	Operator (Therapist)	According to the latest treatment plan, the operator is responsible to execute radiation treatment using the operator station, and	-Verifying the right patient's identification -Giving directions to a patient, such as "get ready," "be still,"

		giving directions to a patient before and during the treatment	immobilization, position, and etc. -Applying the latest treatment plan - Analyzing a patient's data, such as CT image data, treatment plan, treatment history -Starting/Stopping radiation treatment
4	Operator Station	Sending commands to make treatment plan and operate the treatment system to provide proper radiation treatment for patients according precisely to the operator's created treatment plan. Also, controlling the treatment room condition to prepare proper environment for the radiation treatment via the mechanical support system	-Creating treatment plan using the treatment planning system -Checking and controlling treatment room conditions -Setting calibration/patient positioning/registration/imaging and treatment -Controlling the operation such as starting the radiation treatment, emergency stopping, checking the work status, and etc.
5	Treatment Planning	Make patients' treatment plan according to the direction of	-Providing treatment plan with the treatment system

	System	operator via the operator station, and send command to store data regarding treatment plans and patient	
6	Treatment System	Treatment system provides the execution of radiation treatment for a patient that precisely adheres to his/her treatment plan, and the treatment system sends patients' obtained CT image data and anatomical structure data to the data server	- Storing CT image data and anatomical structure data to the data server -Giving radiation treatment to a patient (move gantry, on/off Multi-Leaf Collimator (MLC), on/off Linear Accelerator (LA), on/off beam stop)
7	Mechanical Support System	Intended to hold the mechanical equipment required for the TomoTherapy and to regulate the condition of the treatment system according to the directions from the operator station	-Regulating room condition of the treatment system
8	Patient	Need to have radiation treatment to recover from his/her health condition	-

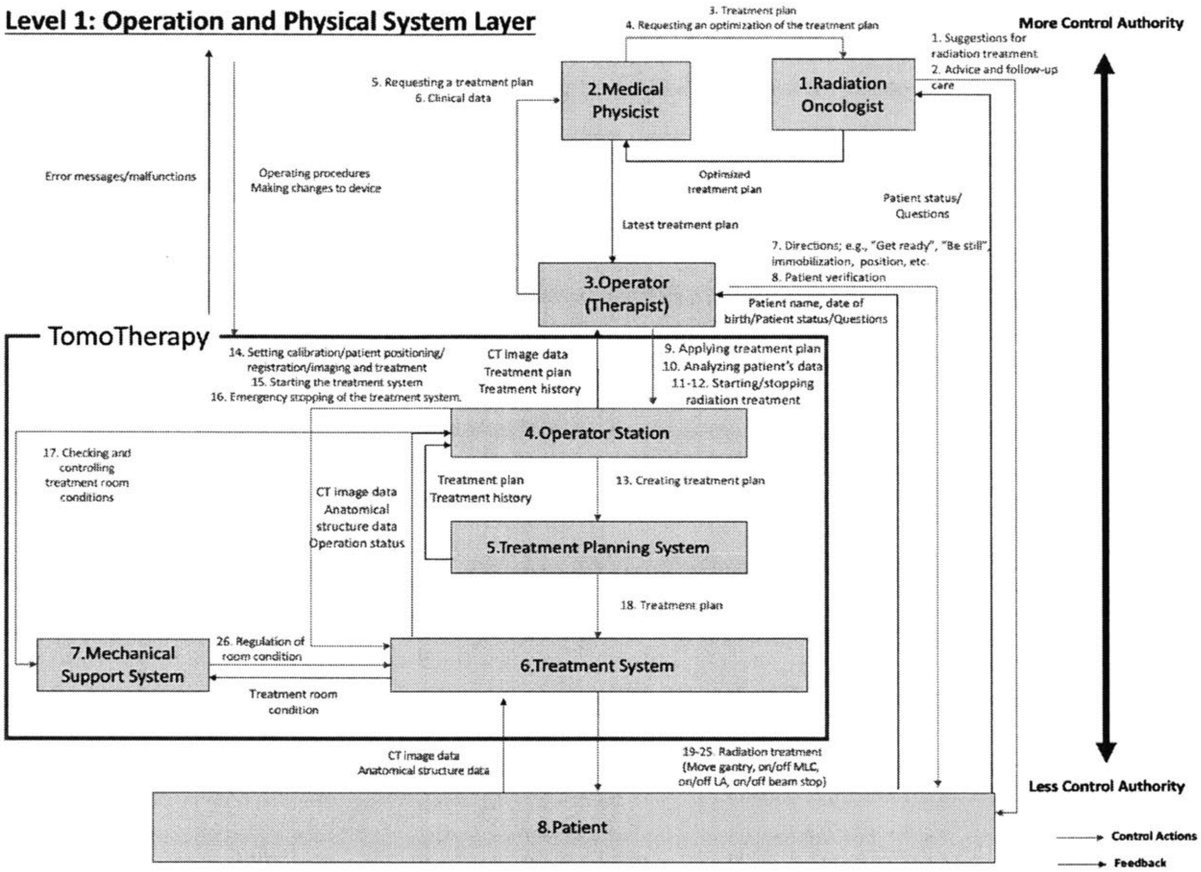

Level 1: Operation and Physical System Layer
3. Treatment plan
4. Requesting an optimization of the treatment plan
More Control Authority
1. Suggestions for radiation treatment
2. Advice and follow-up care
5. Requesting a treatment plan
6. Clinical data
2.Medical Physicist
1.Radiation Oncologist
Error messages/malfunctions
Operating procedures
Making changes to device
Optimized treatment plan
Patient status/ Questions
Latest treatment plan
7. Directions; e.g., "Get ready", "Be still", immobilization, position, etc.
8. Patient verification
3.Operator (Therapist)
Patient name, date of birth/Patient status/Questions
TomoTherapy
14. Setting calibration/patient positioning/ registration/imaging and treatment
15. Starting the treatment system
16. Emergency stopping of the treatment system.
CT image data
Treatment plan
Treatment history
9. Applying treatment plan
10. Analyzing patient's data
11-12. Starting/stopping radiation treatment
4.Operator Station
17. Checking and controlling treatment room conditions
CT image data
Anatomical structure data
Operation status
Treatment plan
Treatment history
13. Creating treatment plan
5.Treatment Planning System
18. Treatment plan
26. Regulation of room condition
7.Mechanical Support System
6.Treatment System
Treatment room condition
CT image data
Anatomical structure data
19-25. Radiation treatment (Move gantry, on/off MLC, on/off LA, on/off beam stop)
Less Control Authority
8.Patient
Control Actions
Feedback

Figure 5.3. Existing safety control structure – Level 1

(Operation Layer and Physical System Layer)

5.4 Performing STPA Step 1 Analysis

5.4.1 Identifying Unsafe Control Actions (UCA)

Based on the STPA analysis using the level 1 safety control structure (Figure 2), I have identified the unsafe control actions (UCA) for TomoTherapy as illustrated in Table 5.3 in STPA Step 1. In this analysis, I listed 8 controllers and 26 control actions for STPA. Focusing on the operation layer and physical system layer, a total of 99 UCAs have been identified; they include the five listed control actions that were considered to be important for hardware interactions, a human operator, and the automated software for the radiation treatment system.

Table 5.3. Unsafe control actions (UCAs)

No.	Control action	Not providing causes hazard	Providing causes hazard	Incorrect timing / ordering	Stopped too soon / Applied too long
1	Giving suggestions for radiation treatment *(human operator)*	[UCA 1-1-a] The radiation oncologist does not give suggestions, such as the recommendation of having radiation treatment for a patient when he or she needs radiation treatment [H6] [UCA 1-1-b] The radiation oncologist	[UCA 1-2-a] The radiation oncologist gives suggestions for radiation treatment to a different patient who does not need radiation treatment [H1] [UCA 1-2-b] The radiation oncologist gives wrong suggestions, which	[UCA 1-3] The radiation oncologist gives suggestions for radiation treatment to the right patient who already had enough radiation treatment [H1]	- (The duration needed to provide suggestions for radiation treatment does not cause hazards)

		does not give suggestions, such as the recommendation to terminate radiation treatment for a patient under the circumstances when the patient does not need radiation treatment anymore [A1]	causes problems like wrong dosage, wrong tumor position, and etc, regarding radiation treatment for the correct patient [H1]		
2	Giving advice and follow-up care for patients *(human operator)*	[UCA 2-1] The radiation oncologist does not give advice and follow-up care in a situation where the condition of a patient is not good [H1]	[UCA 2-2-a] The radiation oncologist gives advice and follow-up care to the wrong patient [H1] [UCA 2-2-b]	- (The timing/ordering when providing the treatment plan does not cause hazards)	- (The duration needed to provide advice and care does not cause hazards)

			The radiation oncologist gives the wrong advice and follow-up care to the right patient [H1]		
3	Providing treatment plans that are not evaluated and optimized *(human operator)*	[UCA 3-1] The medical physicist does not provide a treatment plan that should be optimized by radiation specialists, such as a radiation oncologist [H1]	[UCA 3-2] The medical physicist provides the wrong treatment plan, which is older or that of a different patient [H1]	[UCA 3-3] The medical physicist provides the treatment plan to the radiation oncologist after the radiation treatment [H1]	- (The duration needed to provide the treatment plan does not cause hazards)
4	Requesting an optimization of the treatment plan	[UCA 4-1] The medical physicist	[UCA 4-2] The medical physicist	[UCA 4-3] The medical physicist	- (The duration of requests for an optimization of the treatment

	(human operator)	does not request an optimization of the un-optimized treatment plan when the proper dose of radiation is needed for a patient [H1]	requests an optimization of the un-optimized treatment plan regarding the wrong patient when the proper dose of radiation is needed for the correct patient [H1]	requests an optimization of the treatment plan after the radiation treatment [H1]	plan does not cause hazards)
5	Requesting a treatment plan *(human operator)*	[UCA 5-1] The operator does not request an initial or the latest treatment plan [H1]	[UCA 5-2] The operator requests the treatment plan of the wrong patient [H1, H6]	[UCA 5-3] The operator requests the latest treatment plan after the radiation treatment [H1, H6]	- (The duration of requesting for a treatment plan does not cause hazards)
6	Providing a patient's clinical data	[UCA 6-1] The operator does not	[UCA 6-2-a] The operator provides	[UCA 6-3] The Operator provides	- (The duration of providing a patient's clinical data does not

	(human operator)	provide a patient's clinical data [H1, H6]	clinical data of the wrong patient [H1, H6] [UCA 6-2-b] The operator provides old clinical data of the right patient [H1, H6]	the latest patient's clinical data after the radiation treatment [H1, H6]	cause hazards)
7	Giving directions about a patient's preparation for radiation treatment and a patient's status for the treatment e.g., Get ready, Be still, immobilization,	[UCA 7-1] The operator does not give directions, such as "get ready," "be still," immobilization, position, etc. about a patient's preparation for radiation treatment and a	[UCA 7-2] The operator gives the wrong directions, such as "get ready," "be still," immobilization, position, etc. about a patient's preparation for radiation treatment and a	[UCA 7-3-a] The operator gives additional directions regarding "get ready," "be still," immobilization, position, etc. about a patient's preparation	[UCA 7-4] The operator stops giving directions regarding "get ready," "be still," immobilization, position, etc. too soon before the radiation treatment finishes

	positioning *(human operator)*	patient’s status for the treatment, subsequently leading to wrong radiation emission to the wrong position when treating tumors [H1]	patient’s status for the treatment [H1]	during the radiation treatment [H1] [UCA 7-3-b] The operator gives directions about a patient’s status regarding “get ready,” “be still,” immobilization, position, etc. when it is no longer relevant needed for the treatment [H1]	
8	Verifying the right	[UCA 8-1]	[UCA 8-2]	[UCA 8-3]	-

	patient's identification *(human operator)*	The operator does not provide start command to workstation when the right patient is present [H1, H6]	The operator provides start command to workstation when the wrong patient is present [H1, H6]	The operator provides start command to workstation after the radiation treatment [H1, H6]	(The duration of the verification does not cause hazards)
9	Applying a treatment plan *(human operator)*	[UCA 9-1] The operator does not apply a treatment plan when operating the operator station [H1, H6]	[UCA 9-2-a] The operator applies the wrong patient's treatment plan [H1] [UCA 9-2-b] The operator applies an old or un-optimized	[UCA 9-3] The operator applies the latest treatment plan after the radiation treatment that required the use of the latest treatment plan [H1, H6]	- (The duration of applying a treatment plan does not cause hazards)

			treatment plan that causes improper radiation to a patient [H1]		
10	Analyzing a patient's data, such as CT image data, treatment plan, treatment history *(human operator)*	[UCA 10-1] The operator does not analyze the patient's data for diagnosis conducted by the medical physicist and the radiation oncologist [H1, H6]	[UCA 10-2-a] The operator analyzes the wrong patient's data for diagnosis conducted by the medical physicist and the radiation oncologist [H1, H6] [UCA 10-2-b] The operator mistakenly analyzes old patient's	[UCA 10-3] The operator analyzes a patient's data for diagnosis conducted by the medical physicist and the radiation oncologist before having the latest data [H1]	[UCA 10-4] The operator stops analyzing a patient's data for diagnosis conducted by the medical physicist and the radiation oncologist too soon when a detailed analysis is required [H1]

			data for diagnosis conducted by the medical physicist and the radiation oncologist [H1]		
11	Starting radiation treatment *(human operator)*	[UCA 11-1] The operator does not start radiation treatment [H6]	-	[UCA 11-3-a] The operator starts radiation treatment too early before the patient is ready for the treatment [H1] [UCA 11-3-b] The operator delays the start of a patient's	- (This action does not have duration)

				radiation treatment even when the patient is ready for the treatment [H1]	
12	Stopping radiation treatment *(human operator)*	[UCA 12-1] The operator does not stop the radiation treatment [H1]	-	[UCA 12-3-a] The operator stops the radiation treatment too soon when the treatment actually needs more time to finish [H1] [UCA 12-3-b] The operator stops the radiation treatment too	- (This action does not have duration)

				late when the treatment should be finished sooner [H1]	
13	Creating treatment plan based on the given treatment plan to the system	[UCA 13-1] The operator station does not create a treatment plan [H6]	[UCA 13-2] The operator station creates a wrong treatment plan, such as the wrong patient's treatment plan, the treatment plan created from an older patient's information, etc [H1]	-	[UCA 13-4] The operator station starts to create a treatment plan. However, the time it took to create the plan is too long, and automatically cancels its creation [H4, H6]
14	Setting parameters such as calibration/patient	[UCA 14-1] The operator station	[UCA 14-2-a] The operator station	[UCA 14-3-a] The operator station	[UCA 14-4] The operator station takes too

	positioning/registration/imaging/treatment for patients needed the treatment system	does not set parameters, such as calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system [H1]	assigns the wrong parameters for the correct patient, such as calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system [H1] [UCA 14-2-b] The operator station sets the wrong patient's parameters of calibration/patient positioning/registration/imaging/treatment for	sets the parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system after the treatment [H1] [UCA 14-3-b] The operator station sets the parameters of calibration/patient positioning/registration/imaging/treatment for patients who need	long to set the parameters of calibration/patient positioning/registration/imaging/treatment, and automatically cancels its setting [H4, H6]

			patients who need the treatment system [H1] [UCA 14-2-c] The operator station sets older parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system [H1]	the treatment system during the treatment [H1]	
15	Starting the treatment system	[UCA 15-1] The operator station does not provide start command when the patient is aligned and	[UCA15-2] The operator station provides the start command when the patient is not aligned and	[UCA 15-3] The operator station provides start command before the patient is aligned and	-

		ready [H6]	ready [H1]	ready [H1]	
16	Emergency stopping of the treatment system	[UCA 16-1] The operator station does not provide emergency stop command when the patient is no longer aligned properly in the treatment system [H1, H5]	[UCA 16-2] The operator station provides emergency stop command when there is no emergency [H1, H6]	[UCA 16-3] The operator station provides emergency stop command before completing the radiation treatment [H1]	-
17	Checking and managing the treatment room conditions	[UCA 17-1] The operator station does not check and control the treatment room conditions [H1, H2, H3, H4, H5, H5]	[UCA 17-2] The operator station checks and controls the treatment room conditions inadequately [H1, H2, H3, H4, H5,	[UCA 17-3] The operator station checks and controls the treatment room conditions adequately after the treatment	[UCA 17-4] The operator station stops to check and control the treatment room conditions too soon [H1, H2, H3, H4, H5, H6]

			H6]	[H1, H2, H3, H4, H5, H6]	
18	Providing treatment plan to the treatment system	[UCA 18-1] The treatment planning system does not provide treatment plan to the treatment system when the radiation treatment is needed [H6]	[UCA 18-2-a] The treatment planning system provides the treatment plan of the wrong patient to the treatment system when the radiation treatment is needed [H1] [UCA 18-2-b] The treatment planning system provides the old treatment plan of the right patient to the treatment system when	[UCA 18-3] The treatment planning system provides the treatment plan to the treatment system after the radiation treatment is executed [H1, H6]	[UCA 18-4-a] The treatment planning system takes too long to send commands to provide the treatment plan to the treatment system, and the command is pending [H1, H6] [UCA 18-4-b] The treatment planning system stops to send command to provide treatment plan too soon to the treatment system, and does not complete its application process [H1, H6]

			the radiation treatment is needed using the latest optimized treatment plan by the radiation oncologist (changing dose of radiation, tumor position, etc.) [H1]		
19	Move gantry motor	[UCA 19-1] The treatment system does not move the ring gantry motor into the treatment position before starting the treatment [H6]	[UCA 19-2-a] The treatment system moves the ring gantry motor into the treatment position when there is no treatment scheduled [H4] [UCA 19-2-b]	[UCA 19-3] The treatment system moves the ring gantry motor into the treatment position after delivering therapeutic radiation [H1]	[UCA 19-4-a] The treatment system stopped moving the ring gantry motor into the treatment position too soon [H1] [UCA 19-4-b]

			The treatment system moves the ring gantry motor with a target position that does not match the treatment position. [H1]		The treatment system moves the ring gantry motor into the treatment position too far [H1]
20	Turn MLC on	[UCA 20-1] The treatment system does not provide the MLC on command when starting the treatment [H1]	-	[UCA 20-3] The treatment system provides the MLC on command after delivering therapeutic radiation [H1]	-
21	Turn MLC off	[UCA 21-1]	[UCA 21-2]	-	-

		The treatment system does not provide the MLC off command when the necessary treatment dose has been reached [H1]	The treatment system provides the MLC off command the MLC when the modulated and shaped radiation beams are needed [H1]		
22	Turn LA on	[UCA 22-1] The treatment system does not provide the LA on command when starting the treatment [H6]	[UCA 22-2-a] The treatment system provides the LA on command when the patient is not aligned and ready [H1]	[UCA 22-3] The treatment system provides the LA on command before the patient is aligned and ready [H1]	-

			[UCA 22-2-b] The treatment system provides the LA on command when treatment was not started by the operator station [H1]		
23	Turn LA off	[UCA 23-1] The treatment system does not provide the LA off command when the necessary treatment dose has been reached [H1]	[UCA 23-2] The treatment system provides the LA off command when there is no treatment stopping command [H1]	[UCA 23-3] The treatment system provides the LA off command before completing the treatment [H1]	-
24	Engage beam stop	[UCA 24-1-a]	[UCA 24-2]	[UCA 24-3]	-

		The treatment system does not provide the Engage Beam stop command when the necessary treatment dose has been reached [H1] [UCA 24-1-b] The treatment system does not provide the Engage Beam stop command when there is an emergency [H1]	The treatment system provides the Engage Beam stop command when treatment is not finished [H6]	The treatment system provides the Engage Beam stop command after delivering therapeutic radiation [H1]	

25	Disengage beam stop	[UCA 25-1] The treatment system does not provide the Disengage Beam stop command when the necessary treatment dose has been reached [H1]	[UCA 25-2] The treatment system provides the Disengage Beam stop command when treatment is finished [H1]	[UCA 25-3] The treatment system provides the Disengage Beam stop command before completing the treatment [H1]	-
26	Regulating room condition	[UCA 26-1] The mechanical support system does not regulate room conditions [H1, H2, H3, H4, H5, H6]	[UCA 26-2] The mechanical support system regulates room condition under incorrect parameters to maintain the condition of the treatment room	[UCA 26-3] The mechanical support system regulates the condition of the treatment room after the treatment [H1, H2, H3, H4, H5,	[UCA 26-4-a] The mechanical support system stops regulating the condition of the treatment room too soon [H1, H2, H3, H4, H5, H6] [UCA 26-4-b]

			[H1, H2, H3, H4, H5, H6]	H6]	The mechanical support system stops to regulate the condition of the treatment room for too long [H1, H2, H3, H4, H5, H6]

5.4.2 System Constraints

I also created system constraints from the UCAs in the following table. I identified 81 safety constraints of TomoTherapy in this step of STPA, which would be essential to prevent the system hazards listed above as H1-H6.

Table 5.4. Safety Constraints

No.	Unsafe Control Action (UCA)	Safety constraints
1	[UCA-1-1-a] The radiation oncologist does not give suggestions, such as the recommendation of having radiation treatment for a patient when he or she needs radiation treatment	[SC-1-1-a] The radiation oncologist must give proper and clear suggestions such as the recommendation of having radiation treatment for a patient when he or she needs radiation treatment
2	[UCA 1-1-b] The radiation oncologist does not give suggestions, such as the recommendation to terminate radiation treatment for a patient under the circumstances when the patient does not need radiation treatment	[SC-1-1-b] The radiation oncologist must give suggestions, such as the recommendation to terminate radiation treatment for a patient under the circumstances when the patient does not need radiation treatment

	anymore	any more
3	[UCA 1-2-a] The radiation oncologist gives suggestions for radiation treatment to a different patient who does not need radiation treatment	[SC-1-2-a] The radiation oncologist must provide proper and clear suggestions for radiation treatment to a right patient who needs radiation treatment
4	[UCA 1-2-b] The radiation oncologist gives wrong suggestions, which causes problems like wrong dosage, wrong tumor position, and etc, regarding radiation treatment for the correct patient	[SC-1-2-b] The radiation oncologist must give correct suggestions, which will not cause problems like wrong dosage, wrong tumor position, and etc., regarding radiation treatment for the correct patient
5	[UCA 1-3] The radiation oncologist gives suggestions for radiation treatment to the right patient who already had enough radiation treatment	[SC 1-3] The radiation oncologist must give suggestions to terminate the radiation treatment to the right patient who already had enough radiation treatment
6	[UCA 2-1] The radiation oncologist does not give advice and follow-up care in a situation	[SC-2-1] The radiation oncologist must give advice and follow-up care in a situation where the

	where the condition of a patient is not good	condition of a patient is not good
7	[UCA 2-2-a] The radiation oncologist gives advice and follow-up care to the wrong patient	[SC 2-2-a] The radiation oncologist must give advice and follow-up care to the right patient
8	[UCA 2-2-b] The radiation oncologist gives the wrong advice and follow-up care to the right patient	[SC 2-2-b] The radiation oncologist must give the correct advice and follow-up care to the right patient
9	[UCA 3-1] The medical physicist does not provide a treatment plan that should be optimized by radiation specialists, such as a radiation oncologist	[SC 3-1] The medical physicist must provide a treatment plan that is optimized by radiation specialists, such as a radiation oncologist
10	[UCA 3-2] The medical physicist provides the wrong treatment plan, which is older or that of a different patient	[SC 3-2] The medical physicist must provide the right treatment plan
11	[UCA 3-3] The medical physicist provides the	[SC 3-3] The medical physicist must provide the

	treatment plan to the radiation oncologist after the radiation treatment.	treatment plan to the radiation oncologist before the radiation treatment
12	[UCA 4-1] The medical physicist does not request an optimization of the un-optimized treatment plan when the proper dose of radiation is needed for a patient	[SC 4-1] The medical physicist must request an optimization of un-optimized treatment plan when the proper dose of radiation is needed for a patient
13	[UCA 4-2] The medical physicist requests an optimization of the un-optimized treatment plan regarding the wrong patient when the proper dose of radiation is needed for the correct patient	[SC 4-2] The medical physicist must request an optimization of the un-optimized treatment plan regarding the right patient when the proper dose of radiation is needed for the correct patient
14	[UCA 4-3] The medical physicist requests an optimization of the treatment plan after the radiation treatment	[SC 4-2] The medical physicist must request an optimization of the treatment plan before the radiation treatment
15	[UCA 5-1] The operator does not request an initial or the latest treatment plan	[SC 5-1] The operator must request an initial or the latest treatment plan

16	[UCA 5-2] The operator requests the treatment plan of the wrong patient	[SC 5-2] The operator must request the treatment plan of the right patient
17	[UCA 5-3] The operator requests the latest treatment plan after the radiation treatment	[SC 5-3] The operator must request the latest treatment plan before the radiation treatment
18	[UCA 6-1] The operator does not provide a patient's clinical data	[SC 6-1] The operator must provide a patient's clinical data
19	[UCA 6-2-a] The operator provides clinical data of the wrong patient	[SC 6-2-a] The operator must provide clinical data of the right patient
20	[UCA 6-2-b] The operator provides old clinical data of the right patient	[SC 6-2-b] The operator must provide the latest clinical data of the right patient
21	[UCA 6-3] The Operator provides the latest patient's clinical data after the radiation treatment	[SC 6-3] The operator must provide the latest patient's clinical data before the radiation treatment

22	[UCA 7-1] The operator does not give directions, such as “get ready,” “be still,” immobilization, position, etc. about a patient’s preparation for radiation treatment and a patient’s status for the treatment, subsequently leading to wrong radiation emission to the wrong position when treating tumors	[SC 7-1] The operator must give directions, such as “get ready,” “be still,” immobilization, position, etc. about a patient’s preparation for radiation treatment and a patient's status for the treatment, subsequently leading to right radiation emission to the right position when treating tumors
23	[UCA 7-2] The operator gives the wrong directions, such as “get ready,” “be still,” immobilization, position, etc. about a patient’s preparation for radiation treatment and a patient’s status for the treatment	[SC 7-2] The operator must give the right directions such as “get ready,” “be still,” immobilization, position, etc. about a patient’s preparation for radiation treatment and a patient’s status for the treatment
24	[UCA 7-3-a] The operator gives additional directions regarding “get ready,” “be still,” immobilization, position, etc. about a	[SC 7-3-a] The operator must give additional directions regarding “get ready,” “be still,” immobilization, position, etc. about a

	patient's preparation during the radiation treatment	patient's preparation before the radiation treatment
25	[UCA 7-3-b] The operator gives directions about a patient's status regarding "get ready," "be still," immobilization, position, etc. when it is no longer relevant needed for the treatment	[SC 7-3-b] The operator must give directions about a patient's status regarding "get ready," "be still," immobilization, position, etc. when it is needed for the treatment
26	[UCA 7-4] The operator stops giving directions regarding "get ready," "be still," immobilization, position, etc. too soon before the radiation treatment finishes	[SC 7-4] The operator must give right directions regarding "get ready," "be still," immobilization, position, etc. property under the radiation treatment
27	[UCA 8-1] The operator does not provide start command to workstation when the right patient is present	[SC 8-1] The operator must provide start command to workstation when the right patient is present
28	[UCA 8-2] The operator provides start command to workstation when the wrong patient is	[SC 8-2] The operator must not provide start command to workstation when the wrong

	present	patient is present.
29	[UCA 8-3] The operator provides start command to workstation after the radiation treatment	[SC 8-3] The operator must provide start command to workstation before the radiation treatment
30	[UCA 9-1] The operator does not apply a treatment plan when operating the operator station	[SC 9-1] The operator must adhere to a treatment plan when operating the operator station
31	[UCA 9-2-a] The operator applies the wrong patient's treatment plan	[SC 9-2-a] The operator must apply the right patient's treatment plan
32	[UCA 9-2-b] The operator applies an old or un-optimized treatment plan that causes improper radiation to a patient	[SC 9-2-b] The operator must apply the latest optimized treatment plan that provides proper radiation to a patient
33	[UCA 9-3] The operator applies the latest treatment plan after the radiation treatment that required the use of the latest treatment plan	[SC 9-3] The operator must apply the latest treatment plan before the radiation treatment that required the use of the latest treatment plan

34	[UCA 10-1] The operator does not analyze the patient's data for diagnosis conducted by the medical physicist and the radiation oncologist	[SC 10-1] The operator must analyze the patient's data for diagnosis conducted by the medical physicist and the radiation oncologist
35	[UCA 10-2-a] The operator analyzes the wrong patient's data for diagnosis conducted by the medical physicist and the radiation oncologist	[SC 10-2-a] The operator must analyze the right patient's data for diagnosis conducted by the medical physicist and the radiation oncologist
36	[UCA 10-2-b] The operator mistakenly analyzes old patient's data for diagnosis conducted by the medical physicist and the radiation oncologist	[SC 10-2-b] The operator must analyze the latest patient's data for diagnosis conducted by the medical physicist and the radiation oncologist
37	[UCA 10-3] The operator analyzes a patient's data for diagnosis conducted by the medical physicist and the radiation oncologist before having the latest data	[SC 10-3] The operator must analyze a patient's data for diagnosis conducted by the medical physicist and the radiation oncologist after having the latest data

38	[UCA 10-4] The operator stops analyzing a patient's data for diagnosis conducted by the medical physicist and the radiation oncologist too soon when a detailed analysis is required	[SC 10-4] The operator must complete analyzing a patient's data for diagnosis conducted by the medical physicist and the radiation oncologist until an expected result is obtainable when a detailed analysis is required
39	[UCA 11-1] The operator does not start radiation treatment when a patient and TomoTherapy are ready	[SC 11-1] The operator must start radiation treatment when a patient and TomoTherapy are ready
40	[UCA 11-3-a] The operator starts radiation treatment too early before the patient is ready for the treatment	[SC 11-3-a] Same as SC 11-1
41	[UCA 11-3-b] The operator delays the start of a patient's radiation treatment even when the patient is ready for the treatment	[SC 11-3-b] Same as SC 11-1
42	[UCA 12-1]	[SC 12-1]

	The operator does not stop the radiation treatment	The operator must stop the radiation treatment when the treatment is finished
43	[UCA 12-3-a] The operator stops the radiation treatment too soon when the treatment actually needs more time to finish	[SC 12-3-a] The operator must execute the radiation treatment by when the treatment is finished
44	[UCA 12-3-b] The operator stops the radiation treatment too late when the treatment should be finished sooner	[SC 12-3-b] Same as SC-12-1
45	[UCA 13-1] The operator station does not create a treatment plan	[SC 13-1] The operator station must create a treatment plan
46	[UCA 13-2] The operator station creates a wrong treatment plan, such as the wrong patient's treatment plan, the treatment plan created from an older patient's information, etc.	[SC 13-2] The operator station must create a right treatment plan
47	[UCA 13-4] The operator station starts to create a	[SC 13-4] Same as SC 13-2

	treatment plan. However, the time it took to create the plan is too long, and automatically cancels its creation	
48	[UCA 14-1] The operator station does not set parameters, such as calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system	[SC 14-1] The operator station must set parameters, such as calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system
49	[UCA 14-2-a] The operator station assigns the wrong parameters for the correct patient, such as calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system	[SC 14-2-a] The operator station must assign the right parameters for the correct patient, such as calibration/patient position/registration/imaging/treatment for patients who need the treatment system
50	[UCA 14-2-b] The operator station sets the wrong patient's parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system	[SC 14-2-b] The operator station must set the parameters for the right patient in terms of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system

51	[UCA 14-2-c] The operator station sets older parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system	[SC 14-2-c] The operator station must set latest parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system
52	[UCA 14-3-a] The operator station sets the parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system after the treatment	[SC 14-3-a] The operator station must set the latest parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system before the treatment
53	[UCA 14-3-b] The operator station sets the parameters of calibration/patient positioning/registration/imaging/treatment for patients who need the treatment system during the treatment	[SC 14-3-b] Same as SC 14-3-a
54	[UCA 14-4] The operator station takes too long to set the parameters of calibration/patient	[SC 14-4] Same as SC 14-3-a

	positioning/registration/imaging/treatment, and automatically cancels its setting	
55	[UCA 15-1] The operator station does not provide start command when the patient is aligned and ready	[SC 15-1] The operator station must provide start command when the patient is aligned and ready
56	[UCA 15-2] The operator provides the start command when the patient is not aligned and ready	[SC 15-2] The operator station must not provide the start command when the patient is not aligned and ready
57	[UCA 15-3] The operator station provides start command before the patient is aligned and ready	[SC 15-3] The operator station must provide start command after the patient is aligned and ready
58	[UCA 16-1] The operator station does not provide emergency stop command when the patient is no longer aligned properly in the treatment system	[SC 16-1] The operator station must provide emergency stop command when the patient is no longer aligned properly in the treatment system

59	[UCA 16-2] The operator station provides emergency stop command when there is no emergency	[SC 16-2] The operator station must not provide emergency stop command when there is no emergency
60	[UCA 16-3] The operator station provides emergency stop command before completing the radiation treatment	[SC 16-3] The operator station provides emergency stop command after completing the radiation treatment
61	[UCA 17-1] The operator station does not check and control the treatment room conditions	[SC 17-1] The operator station must check and control the treatment room conditions adequately
62	[UCA 17-2] The operator station checks and controls the treatment room conditions inadequately	[SC-17-2] Same as SC 17-1
63	[UCA 17-3] The operator station checks and controls the treatment room conditions adequately after the treatment	[SC 17-3] The operator station must check and control the treatment room conditions adequately before the treatment

64	[UCA 17-4] The operator station stops to check and control the treatment room conditions too soon	[SC 17-4] The operator station must stop to check and control the treatment room conditions properly
65	[UCA 18-1] The treatment planning system does not provide treatment plan to the treatment system when the radiation treatment is needed	[SC 18-1] The treatment planning system must provide treatment plan to the treatment system when the radiation treatment is needed
66	[UCA 18-2-a] The treatment planning system provides the treatment plan of the wrong patient to the treatment system when the radiation treatment is needed	[SC 18-2-a] The treatment planning system must provide the treatment plan of the right patient to the treatment system when the radiation treatment is needed
67	[UCA 18-2-b] The treatment planning system provides the old treatment plan of the right patient to the treatment system when the radiation treatment is needed using the latest optimized treatment plan by the radiation	[SC 18-2-b] The treatment planning system must provide the latest treatment plan of the right patient to the treatment system when the radiation treatment is needed using the latest optimized treatment plan by the

	oncologist (changing dose of radiation, tumor position, etc.)	radiation oncologist (changing dose of radiation, tumor position, etc.)
68	[UCA 18-3] The treatment planning system provides the treatment plan to the treatment system after the radiation treatment is executed	[SC 18-3] The treatment planning system must provide the treatment plan to the treatment system before the radiation treatment is executed
69	[UCA 18-4-a] The treatment planning system takes too long to send commands to provide the treatment plan to the treatment system, and the command is pending	[SC 18-4-a] The treatment planning system must send commands to provide the treatment plan to the treatment system
70	[UCA 18-4-b] The treatment planning system stops sending commands to provide the treatment plan too soon to the treatment system, and does not complete its application process	[SC 18-4-b] Same as SC 18-4-a
71	[UCA 19-1] The treatment system does not move the	[SC 19-1] The treatment system must move the ring

	ring gantry motor into the treatment position before starting the treatment	gantry motor into the treatment position before starting the treatment
72	[UCA 19-2-a] The treatment system moves the ring gantry motor into the treatment position when there is no treatment scheduled	[SC 19-2-a] The treatment system must not move the ring gantry motor into the treatment position when there is no treatment scheduled
73	[UCA 19-2-b] The treatment system moves the ring gantry motor with a target position that does not match the treatment position.	[SC 19-2-b] The treatment system must not move the ring gantry motor with a target position that does not match the treatment position.
74	[UCA 19-3] The treatment system moves the ring gantry motor into the treatment position_ after delivering therapeutic radiation	[SC 19-3] The treatment system must move the ring gantry motor into the treatment position_ while delivering therapeutic radiation
75	[UCA 19-4-a] The treatment system stopped moving the ring gantry motor into the treatment position too soon	[SC 19-4-a] The treatment system must not stop moving the ring gantry motor into the treatment position too soon
76	[UCA 19-4-b]	[SC 19-4-b]

	The treatment system moves the ring gantry motor into the treatment position too far	The treatment system must not move the ring gantry motor into the treatment position too far
77	[UCA 20-1] The treatment system does not provide the MLC on command when starting the treatment	[SC 20-1] The treatment system must provide the MLC on command when starting the treatment
78	[UCA 20-3] The treatment system provides the MLC on command after delivering therapeutic radiation	[SC 20-3] The treatment system must provide the MLC on command while delivering therapeutic radiation
79	[UCA 21-1] The treatment system does not provide the MLC off command when the necessary treatment dose has been reached	[SC 21-1] The treatment system must provide the MLC off command when the necessary treatment dose has been reached
80	[UCA 21-2] The treatment system provides the MLC off command the MLC when the modulated and shaped radiation beams are needed	[SC 21-2] The treatment system must not provide the MLC off command the MLC when the modulated and shaped radiation beams are needed

81	[UCA 22-1] The treatment system does not provide the LA on command when starting the treatment	[SC 22-1] The treatment system must provide the LA on command when starting the treatment
82	[UCA 22-2-a] The treatment system provides the LA on command when the patient is not aligned and ready	[SC 22-2-a] The treatment system must not provide the LA on command when the patient is not aligned and ready
83	[UCA 22-2-b] The treatment system provides the LA on command when treatment was not started by the operator station	[SC 22-2-b] The treatment system must not provide the LA on command when treatment was not started by the operator station
84	[UCA 22-3] The treatment system provides the LA on command before the patient is aligned and ready	[SC 22-3] The treatment system must provide the LA on command after the patient is aligned and ready
85	[UCA 23-1] The treatment system does not provide the LA off command when the necessary treatment dose has been reached	[SC 23-1] The treatment system must provide the LA off command when the necessary treatment dose has been reached

86	[UCA 23-2] The treatment system provides the LA off command when there is no treatment stopping command	[SC 23-2] The treatment system must not provide the LA off command when there is no treatment stopping command
87	[UCA 23-3] The treatment system provides the LA off command before completing the treatment	[SC 23-3] The treatment system must provide the LA off command after completing the treatment
88	[UCA 24-1-a] The treatment system does not provide the Engage Beam stop command when the necessary treatment dose has been reached	[SC 24-1-a] The treatment system must provide the Engage Beam stop command when the necessary treatment dose has been reached
89	[UCA 24-1-b] The treatment system does not provide the Engage Beam stop command when there is an emergency	[SC 24-1-b] The treatment system must provide the Engage Beam stop command when there is an emergency
90	[UCA 24-2] The treatment system provides the Engage Beam stop command when treatment is not finished	[SC 24-2] The treatment system must not provide the Engage Beam stop command when treatment is not finished

91	[UCA 24-3] The treatment system provides the Engage Beam stop command after delivering therapeutic radiation	[SC 24-3] The treatment system must provide the Engage Beam stop command before delivering therapeutic radiation
92	[UCA 25-1] The treatment system does not provide the Disengage Beam stop command when the necessary treatment dose has been reached	[SC 25-1] The treatment system must provide the Disengage Beam stop command when the necessary treatment dose has been reached
93	[UCA 25-2] The treatment system provides the Disengage Beam stop command when treatment is finished	[SC 25-2] The treatment system must not provide the Disengage Beam stop command when treatment is finished
94	[UCA 25-3] The treatment system provides the Disengage Beam stop command before completing the treatment	[SC 25-3] The treatment system must provide the Disengage Beam stop command after completing the treatment
95	[UCA 26-1] The mechanical support system does not regulate room conditions	[SC 26-1] The mechanical support system must regulate room conditions
96	[UCA 26-2]	[SC 26-2]

	The mechanical support system regulates room condition under incorrect parameters to maintain the condition of the treatment room	The mechanical support system must regulate room condition under correct parameters to maintain the condition of the treatment room
97	[UCA 26-3] The mechanical support system regulates the condition of the treatment room after the treatment	[SC 26-3] The mechanical support system must regulate the condition of the treatment room during the treatment
98	[UCA 26-4-a] The mechanical support system stops regulating the condition of the treatment room too soon	[SC 26-4-a] Same as SC 26-3
99	[UCA 26-4-b] The mechanical support system stops to regulate the condition of the treatment room for too long	[SC 26-4-b] Same as SC 26-3

5.5 Performing STPA Step 2 Analysis

5.5.1 Identifying Causal Scenarios

The next step is to analyze how each unsafe control action could happen in the system. In other words, this step determines the reasons why the UCAs may happen, which are called causal scenarios. [1]

For example, a controller might not provide a control action when needed or might provide an unsafe one because of an inadequate control algorithm or an inconsistent, incomplete, or incorrect process model of the controlled process or system state. This flawed process model could, in turn, result from inadequate, incorrect, missing, or delayed feedback from sensors. Sensors may not operate as expected due to feedback delays, measurement inaccuracies, or missing sensor information from the controlled process. There is also the possibility that a correct control action could cause safety problems due to delayed operation from an actuator or component failures, resulting in an unsafe system state.

Another reason for accidents is that a safe control action is provided, but it is not executed correctly. The hazard causes identified by component failure-based hazard analysis techniques are those such as a failure in the execution of a control command. STPA, however, also allows the analyst to identify causes that do not result from failure but from requirements and design errors, i.e., the component behavior satisfies its requirements but those requirements are incorrect, perhaps because the designer forgot about or misunderstood how the system components would interact and work together or did not account for human errors.

In the safety control structure, there are three types of control loops, such as between human controllers, a human controller and a system controller, and system controllers.

This time, Causal Scenarios were generated for the three types of the identified UCAs in STPA Step 1 of the TomoTherapy. I selected the below three control loops because they are closely related to the A1 accident, which is the most serious for patients. As a result, the causal scenarios were identified in this Step 2 analysis.

5.5.2 Causal Scenarios for the control loop between human controllers

For example, the causal scenarios for "UCA 8-2: The operator provides start command to workstation when the wrong patient is present" is shown in the following. To identify these scenarios, detailed information is used in the following table (Table 5.5). Figure 5.4 shows the specific control loop for UCA8-2. By using this diagram, it is possible to find causal scenarios.

Table 5.5. Detailed system information for the communication between the operator and the patient [2]

Component	Description
Intercom Desk Control Unit	The intercom desk control unit is placed at the Operator Station countertop. The wired conduit and terminating with RJ45 connectors as called out in the site-specific drawings have to be installed. The installation engineers will install the desk control unit and connect to the termination points.
Intercom Speaker System	The intercom speaker and all its components allow the patient and clinician to communicate during treatment. The speaker is wall mounted behind the patient on isocenter at 7 ft-6 in (2286 mm) above the finished floor. The maximum length of the signal conduit between the speaker and the back of the gantry cannot exceed 15 ft-0 in (4570 mm). It needs to be prepared for: the supply and installation of the conduit for the microphone cable connection, a CAT5 (or higher) signal cable running between the speaker unit in the Treatment Room and the Control Room, and junction boxes [termination point(s)] in the bunker and in the Control Room, as called out in the site-specific drawings. The best practice is to terminate the CAT5 cable (or equivalent) with RJ45 outlets (female connectors) both in the Treatment Room and in the Control Room. These

	terminations must be installed in close proximity to the intercom speaker unit in the Treatment Room and the desktop unit in the Control Room - to allow for short patch cords connections to these components. The installation engineers will install and connect the speaker and associated components.

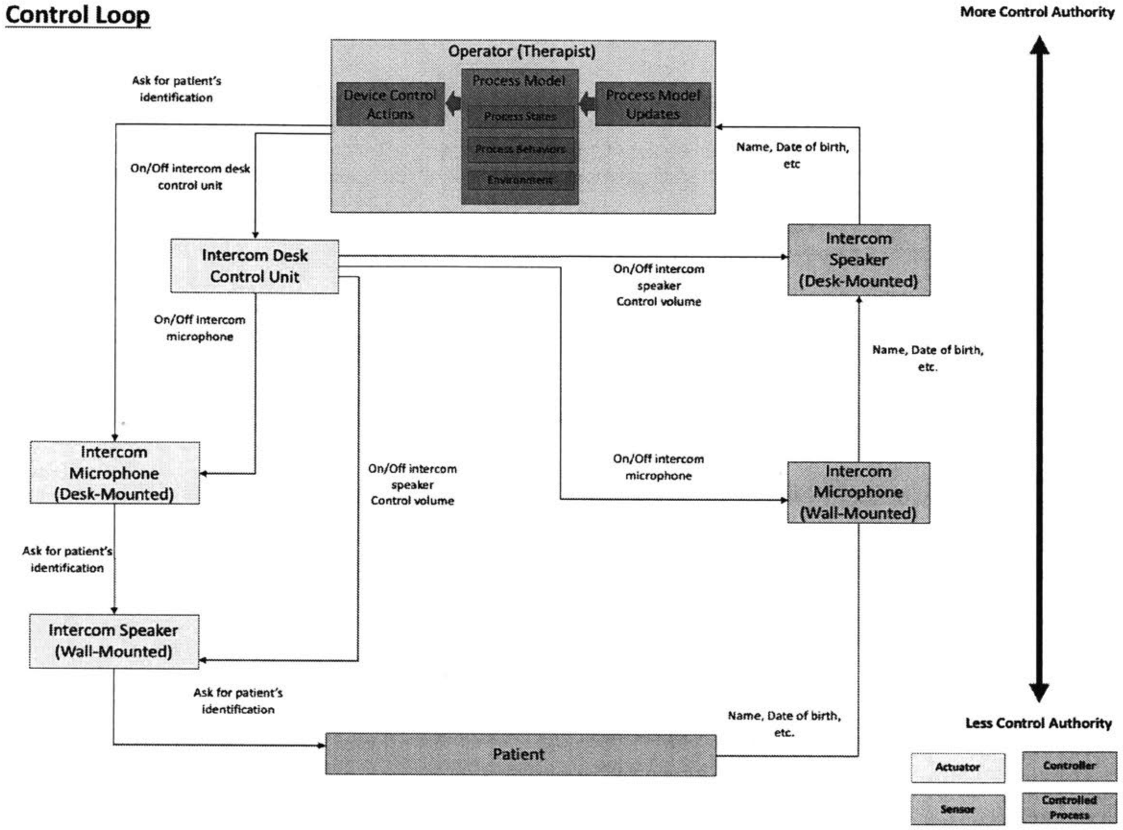

Control Loop
More Control Authority
Operator (Therapist)
Device Control Actions
Process Model
Process States
Process Behaviors
Environment
Process Model Updates
Ask for patient's identification
On/Off intercom desk control unit
Name, Date of birth, etc
Intercom Desk Control Unit
On/Off intercom speaker Control volume
Intercom Speaker (Desk-Mounted)
On/Off intercom microphone
Name, Date of birth, etc.
Intercom Microphone (Desk-Mounted)
On/Off intercom speaker Control volume
On/Off intercom microphone
Intercom Microphone (Wall-Mounted)
Ask for patient's identification
Intercom Speaker (Wall-Mounted)
Ask for patient's identification
Name, Date of birth, etc.
Patient
Less Control Authority
Actuator
Controller
Sensor
Controlled Process

Figure 5.4. Control Loop for UCA 8-2

UCA 8-2: The operator provides start command to workstation when the wrong patient is present

Causal Scenario 1: The operator provides start command to workstation when the wrong patient is present. This will occur if the operator incorrectly believes the right patient is present (process model flaw). This incorrect belief could be caused if:

- The patient incorrectly answers "yes" when asked if they are patient X. This could happen if the patient has a similar sounding name to another patient, or if the operator speaks to the wrong patient (e.g., if the intercom connects to the wrong room)

- The operator speaks to the correct patient, but the wrong patient later enters the room before treatment.

Possible Requirement 1 1: The operator shall ask the spelling of the patient's full name.

Possible Requirement 1 2: As a technical system design, the treatment room shall be connected to one operator workstation and one intercom unit to prevent the intercom unit from connecting to multiple rooms.

Possible Requirement 1 3: The nurse shall make sure wrong patients do not enter the treatment room by checking the name, date of birth, state, etc.

Causal Scenario 2: The operator provides start command to workstation when the wrong patient is present. The operator incorrectly believes the right patient can speak the language. The operator asks for the patient's identification during the patient call. However, the patient cannot answer the question because the patient cannot hear or speak adequately due to diseases, or speaks a language that is different from that of the operator. As a result, the operator does not verify the patient's identification during the patient call.

Possible Requirement 2_1: The operator shall reconfirm the patient profile before the patient enters the room.

Possible Requirement 2_2: The operator station has the function to automatically show the patient profile via its console before the patient is allowed to enter the room.

Causal Scenario 3: The operator provides start command to workstation when the wrong patient is present. This could happen if the operator incorrectly believes the treatment schedule did not change. The operator may not know there is a last-minute schedule change among patients because a medical staff forgets to inform the operator of the schedule. As a result, the operator does not verify the right patient's identification during the patient call.

Possible Requirement 3_1: The nurse shall inform the operator when there was a last-minute schedule change.

Possible Requirement 3_2: The system like patient schedule management system shall inform the operator the schedule change on the console, which the operator is viewing.

Causal Scenario 4: The operator provides start command to workstation when the wrong patient is present. This will occur if the operator incorrectly believes the right patient is present (process model flaw). This incorrect belief could be caused if:

- The operator believed the ID was previously verified by someone else. This could happen because the ID was verified at the reception desk before entering the treatment room.
- There is an operator shift change, and the previous operator forgets to notify the new operator that the patient has not been verified yet.

Possible Requirement 4_1: The operator shall check whether the right patient is present in the treatment room and record the fact as a file.

Possible Requirement 4_2: The operator station shall have the button about whether the operator verifies the right patient. Without pushing the button, the operator cannot start the treatment system.

Possible Requirement 4_3: The patient's name, date of birth, and state shall be checked and verified at the reception desk, before entering the treatment room, and before treatment is started.

Possible Requirement 4_4: The treatment door may have the button whether the patient ID was verified before entering the room. By using this button, the nurse allows the patient enters the room. The patient will not be allowed to enter room unless patient ID is verified.

Possible Requirement 4_5: When a shift change occurs, the current operator shall give the record that the patient has not been verified yet to the new operator.

Possible Requirement 4_6: If the operator station does not allow treatment to start due to patient verification, then it will inform the operator of the reason treatment was not started.

Causal Scenario 5: The operator provides start command to workstation when the wrong patient is present. This could happen if the operator does not know the wrong patient is present. The operator may not know the wrong patient is present because of a hardware failure in the intercom system such as the snapping of the microphone cable or CAT5 cable, etc.

Possible Requirement 5 1: The operator shall check whether the intercom system works correctly or not before providing start command for the right patient's verification.

Possible Requirement 5 2: The intercom desk control unit shall have the function to automatically detect the hardware failure in the intercom system when it starts.

5.5.3 Causal Scenarios for the control loop between system controllers

For example, the causal scenarios for "UCA 16-1: The operator station does not provide emergency stop command when the patient is no longer aligned properly in the treatment system" is shown in the following. To identify these scenarios, detailed information is used in the following table (Table 5.6). Figure 5.5 shows the specific control loop for UCA16-1. By using this diagram, it is possible to find causal scenarios.

Table 5.6. Detailed system information for the operator station [2]

Component	Description
Step-Down Transformer	The step-down transformer is mounted underneath the counter on a customer-supplied shelving unit. It needs to be prepared for installing the under counter shelf to support the size and weight.
Operator Station Status Console	A device that allows the operator to operate the emergency stop, key switch for image/program/treat options, start button, stop button, and radiation on notification.
Operator Station Workstation	The Operator Station is the computer workstation that the technologists use for calibration, patient positioning, registration, imaging and treatment. The control station is composed of a computer, flat screen monitor, and keyboard.

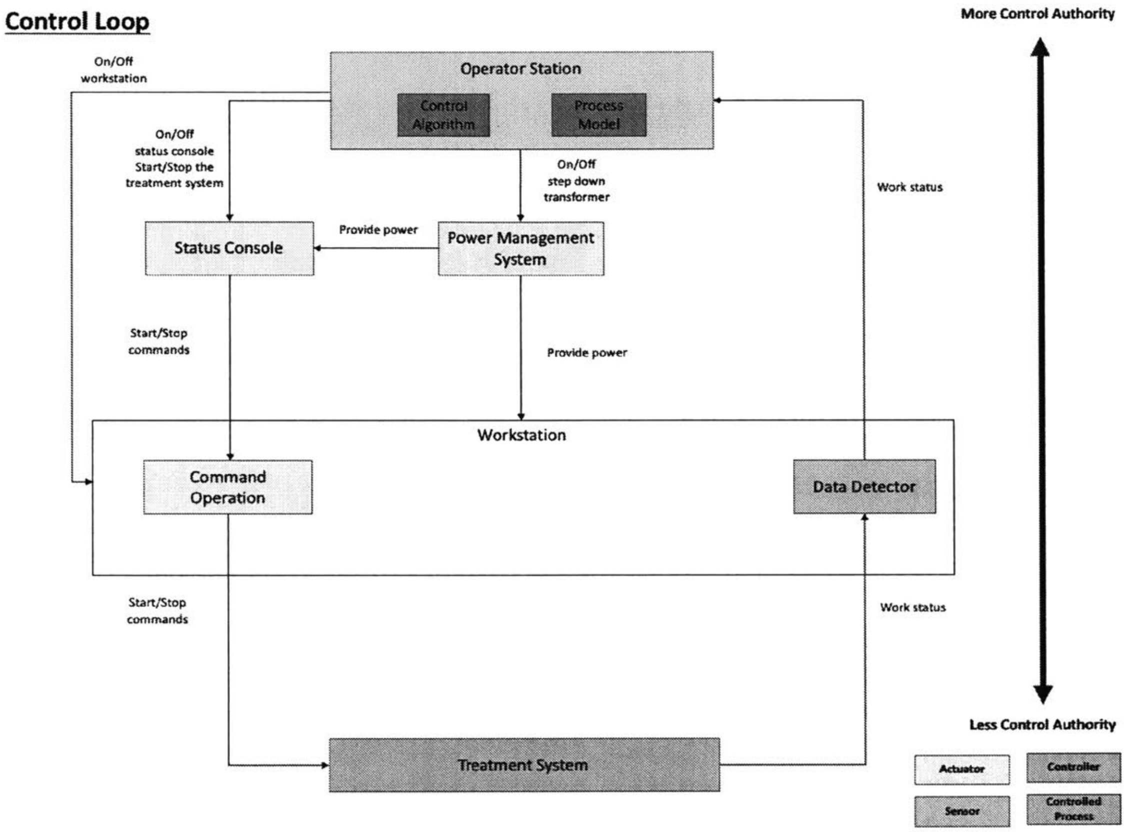


Figure 5.5. Control Loop for UCA-16-1

UCA 16-1: The operator station does not provide emergency stop command when the patient is no longer aligned properly in the treatment system

Causal Scenario 1: The operator station does not provide emergency stop command when the patient is no longer aligned properly in the treatment system. This will occur if the operator station incorrectly believes the patient is aligned properly in the treatment system. This incorrect belief could be caused if the patient moves after treatment is started.

Possible Requirement 1 1: The operator shall monitor the movement of the patient during treatment. The movement must be monitored directly through a window or indirectly through a pan, tilt, and zoom camera that must be displayed on the operator workstation monitor.

Possible Requirement 1 2: The treatment couch must have the function to detect the patient's movement automatically. If this movement is detected, the treatment stops forcibly.

Possible Requirement 1 3: The flexible air pad for head, arms, body, and legs must be used to physically keep the patient still.

Causal Scenario 2: The operator station provides emergency stop command, but the treatment does not stop. The emergency stop command may not reach the workstation due to delays in data transmission through the network, the snapping or disconnection of the cable. If the emergency stop command reaches the workstation, it may not be executed due to hardware failure or if the workstation powers down before the command is executed.

Possible Requirement 2_1: The operator shall check the workstation and power source works correctly before starting the treatment system.

Possible Requirement 2_2: The operator station shall have secondary power source in case of sudden primary power source defect.

Possible Requirement 2_3: The operator station shall send confirmation message to the operator to indicate if commands were executed or not executed.

5.5.4 Causal Scenarios for the control loop between a human controller and a system controller

For example, the causal scenarios for "UCA-23-1: The treatment system does not provide the LA off command when the necessary treatment dose has been reached" is shown in the following. To identify these scenarios, detailed information shown in Figures 5.6 and Table 5.7 were needed. In addition, using these information, Figure 5.7 shows the specific control loop for UCA23-1. By using this diagram, it is possible to find causal scenarios.

Table 5.7. Detailed system information for the treatment system [3]

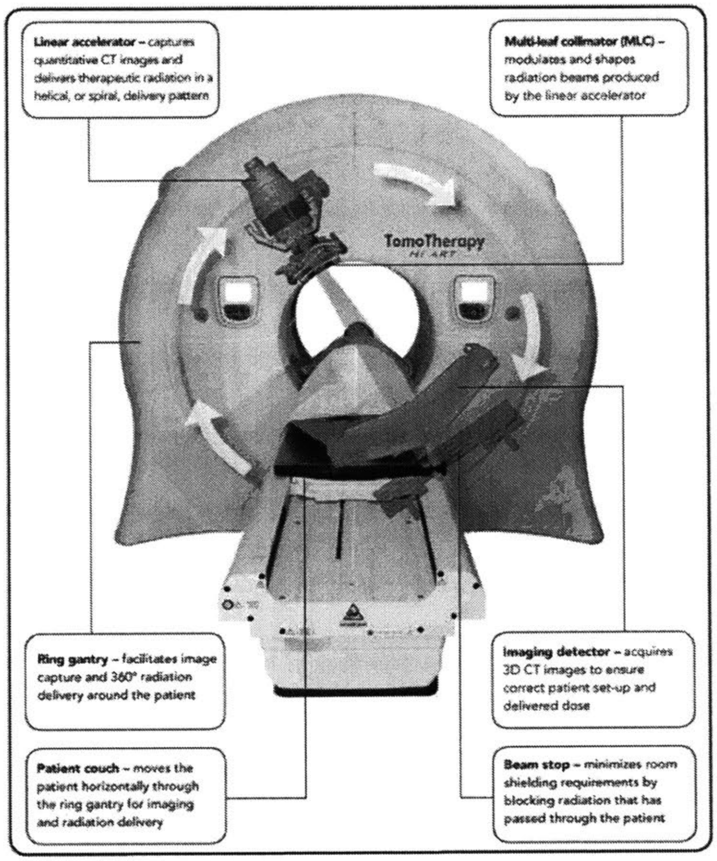
Component	Description
Linear Accelerator (LA)	The linear accelerator is a device that generates external beam radiation that is used both to capture high quality, quantitative images such as CT images and to deliver therapeutic radiation in a helical, or spiral, delivery pattern 360 degrees around the body. The linear accelerator rotates around a rigid circular frame, or ring gantry, that is housed in a protective casing.
Multi-Leaf Collimator (MLC)	The Hi Art system's MLC is attached to the front of the linear accelerator and consists of 64 individual tungsten leaves that move across the beam in less than 20 milliseconds to either block or allow the passage of radiation, effectively shaping the beam as it is emitted. Each leaf's binary movement

	from open to close defines a beamlet of radiation produced by the linear accelerator as the patient passes horizontally through the ring gantry, and the intensity of the beamlet is modulated based on the length of time the leaf is open. The shape of the treatment field is defined by the pattern of all of the beamlets. A typical Hi Art treatment delivers tens of thousands of beamlets.
Ring Gantry	The Hi Art system's rigid ring gantry houses a linear accelerator that circles the patient and enables both CT imaging and radiation therapy to be provided from the same integrated source. The ring architecture enables more precise and more efficient treatments by eliminating the need for the repeated adjustment and re-calibration steps necessitated by imaging and treating the patient on different systems and mechanically adjusting the C-arm to treat from different angles.
Patient Couch	During each treatment session, the patient is positioned on a treatment table, or patient couch and an image of the patient is taken with the CTrue system. The patient couch moves the patient horizontally through the ring gantry for imaging and radiation delivery.
Imaging Detector	The Hi Art system's imaging detector, which is positioned in the ring gantry directly opposite to the linear accelerator, records the amount of radiation that passes through the patient during treatment and acquires 3D CT images. The

	recorded data can be used to verify that the planned dose was accurately delivered.
Beam Stop	It is believed that the Hi Art system contains more radiation shielding, which absorbs radiation, around the linear accelerator than any other linear accelerator currently available. This shielding protects the patient from receiving unwanted radiation leakage to the parts of the body not being treated. The Hi Art system also contains a lead beam stop on the opposite side of the ring gantry from the linear accelerator that absorbs the primary radiation beam after it has passed through the patient. The increased shielding and beam stop limit the amount of radiation that leak from the system into the treatment room, reduces the shielding required in the walls of the facility in which the Hi Art system is located, and protects the patient from unwanted radiation.

The TomoTherapy® Hi Art® Treatment System

The All-in-one Imaging and Radiation Treatment Device



Linear accelerator – captures quantitative CT images and delivers therapeutic radiation in a helical, or spiral, delivery pattern

Multi-leaf collimator (MLC) – modulates and shapes radiation beams produced by the linear accelerator

Ring gantry – facilitates image capture and 360° radiation delivery around the patient

Imaging detector – acquires 3D CT images to ensure correct patient set-up and delivered dose

Patient couch – moves the patient horizontally through the ring gantry for imaging and radiation delivery

Beam stop – minimizes room shielding requirements by blocking radiation that has passed through the patient

Figure 5.6. Detailed system information of the treatment system cited from [3]

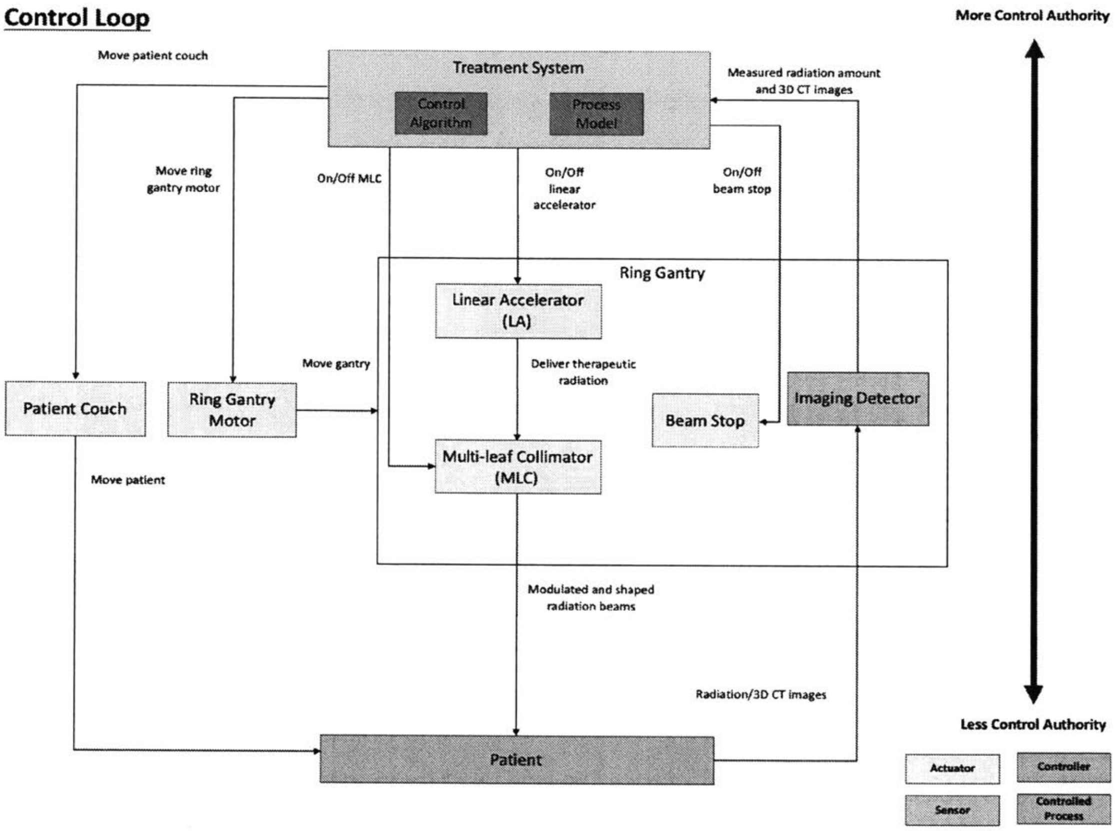


Figure 5.7. Control Loop for UCA-23-1

UCA23-1: The treatment system does not provide the LA off command when the necessary treatment dose has been reached

Causal Scenario 1: The treatment system does not provide the LA off command when the necessary treatment dose has been reached. This will occur if the treatment system incorrectly believes the necessary treatment dose has not been reached. This incorrect belief could be caused if there are changes to daily dose plan or daily dose plan data for the patient. The treatment system would operate according to the unchanged plan or data. The operator may not know the changes before starting the treatment.

Possible Requirement 1 1: The planned and changed amount of dose shall be informed to the operator.

Possible Requirement 1 2: The treatment system must be able to retrieve the latest treatment data, and notify the operator of changes.

Causal Scenario 2: The treatment system does not provide the LA off command when the necessary treatment dose has been reached. This will occur if the treatment system incorrectly believes the necessary treatment dose has not been reached. This incorrect belief could be caused if the actual energy level (Rads/Sec) is lower than indicated by the measured radiation level feedback. As a result, the LA off command will be delayed.

Possible Requirement 2_1: The operator shall monitor the actual energy level in the gantry and adjust the setting of an energy level.

Possible Requirement 2_2: The treatment system must have the capability to detect when the measured energy level is incorrect and differs from the commanded energy level. In this situation, the treatment system must automatically stop treatment and inform the operator of the problem. Treatment must not be restarted while this problem exists.

Causal Scenario 3: The treatment system provides the LA off command when the necessary treatment dose has been reached, but the LA does not turn off. This could be caused by the imaging detector not working properly, and the treatment system cannot verify that the planned dose was accurately delivered. The treatment system does not provide the LA off command by judging the received incorrect data of radiation amount and 3D CT images.

Possible Requirement 3_1: The operator shall visually monitor the working condition of the imaging detector on the workstation screen.

Possible Requirement 3_2: The imaging detector shall have maintenance by mechanical technicians regularly.

Possible Requirement 3_3: The audit program of imaging detect shall be installed to the workstation.

Possible Requirement 3 4: The treatment system must provide a function to test the imaging detector. It must be tested before each patient is treated, and the test results must be provided to the operator. If the test does not pass, the treatment system should not allow treatment to start.

5.6 References

[1] Nancy G. Leveson (2012), "Engineering a safer world: systems thinking applied to safety," MIT Press.

[2] Accuray Incorporated (2014), "TomoTherapy H^{TM} Series Site Planning Guide."

[3] Piper Jaffray et al. (2007), "TomoTherapy Incorporated PROSPECTUS," available at:

http://www.nasdaq.com/markets/ipos/filing.ashx?filingid=4901989

Chapter 6. Discussion and Conclusion

In Chapter 5, STPA was applied to TomoTherapy. As a result, 99 UCAs, 88 safety constraints, 10 causal scenarios, and 29 possible requirements were identified.

6.1 Discussion

Regarding the identified causal scenarios, a causality table including the results of FMEA, shown in Table 6.1, was made and used in the research of Pawlicki et al. [1] This time, I included one additional category of "Physical System" in this table. In examining the results of FMEA, the contents of Tables 4.1, 4.2 and 4.3 were mapped because potential causes and potential effects of failure were identified only for these failure modes.

Table 6.1. Causality table of the results of STPA and FMEA

(In examining the results of FMEA, the contents of Tables 4.1, 4.2 and 4.3 were mapped)

Causality category	FMEA	STPA
Organizational management	0%	0%
Technical	13%	8%
Physical System	0%	25%
Human behavior of individual staff	83%	34%
Patient-related circumstances	0%	25%
External factors (beyond facility control)	0%	0%
Procedural issues	3%	8%

Other	0%	0%
Total	**100%**	**100%**

According to these results, it can be observed that FMEA was mainly focusing on two categories, namely, "technical" and "human behavior of individual staff." On the other hand, STPA can identify various causal scenarios in a wide spectrum of categories from the entire system, including the physical system, human operator, organization, management, etc. Recalling the characteristics of FMEA mentioned in Chapter 2, it focuses on analyzing failure modes based on process trees. This means that FMEA is not a useful way to identify safety requirements for controllers by considering the behaviors of the entire system. As a matter of fact, accidents are caused by various controllers, including those in physical system, human operator, organization, etc. These controllers have complicated relationships. Thus, it is quite important to consider the relationships among these controllers when preparing safety requirements. STPA definitely includes these controllers for safety analysis, so it is very useful for preventing accidents that can happen with a wide spectrum of systems that are tremendously huge and complex. This time, though not so many causal scenarios were identified by focusing on three control loops, it was found that the results of STPA cover the causality category comprehensively. More specifically, STPA found causal scenarios regarding three factors: physical system, human factor, and patient-related circumstance. The total percentage of the three was 84%. Also, STPA found the scenarios categorized as technical and procedural issues. As a matter of fact, past accidents have happened due to a wide spectrum of causal factors. Considering this point, ideally, the system safety analysis must be analyzed comprehensively, including the physical system, human factors, organization, management, and so on.

When comparing the results of STPA with those of FMEA, I focused on several specific results. For example, using FMEA, "wrong patient identification (with the same anatomical site)" was found as a potential failure mode according to Table 4.3. The potential cause of failure was "lack of attention," and the potential effects of failure were "wrong treatment for a single session." STPA also identified similar results, which were mentioned in "causal scenarios for UCA 8-2" in Chapter 5. In this result, FMEA just found one case of the failure to relay the right patient's identification, but STPA found five related scenarios, which contain more detailed information than that of the results of the FMEA. Also, the potential cause of failure in the results of FMEA is mentioned only for human errors. However, STPA analyzes "the right patient identification" in the system from various viewpoints, such as human factors, physical system, and procedures. Thus, it is evident that STPA can be used as a technique to identify potential causes as causal scenarios more comprehensively than FMEA.

In an actual development project, a more easily understood method is preferable. In such a project, workers and companies definitely have to perform their tasks under time restrictions. Under this restriction, analysts have to prioritize the results of a safety analysis. As for determining the priority of causal scenarios found in STPA, I focused on A1 accidents, which cause loss of life or serious damage to patients. This is a very simple scheme for analysts. On the other hand, regarding FMEA, it also found and ranked "the severity rate (S)", "the occurrence rate (O)" and "the detectability rate (D)." This method is very complicated because of considerations with the three rates.

In general, probability is used for the prioritization. Also, the risk rank, such as high, middle, and low, is used. After that, the analyst multiplies the value of probability (%) by the risk rank. However, there is a possibility that any serious accident might happen, regardless of the probability. It is therefore quite important to analyze UCAs and causal scenarios by the listed prioritized results of the accidents under the condition where the number of UCAs and causal scenarios relating accidents and hazards has no limitations. For example, *all* UCAs related to A1 accidents should be analyzed to avoid the accident if A1 is regarded as the most serious accident, and safety analysts and developers should collaborate in identifying all the causal scenarios that may cause those UCAs.

FMEA is a process-based method. By examining Figures 4.1, 4.2 and 4.3, it can be seen that these processes are like a waterfall. This means that changing or adding a process is quite difficult, although it often happens in the development phase and operation phase of the system. On the other hand, STPA is a control-structure-based method, and creates a safety control structure and also causal scenarios based on STAMP. STPA can be used for the development phase, where the requirements and detailed design of the system are not yet fixed. In other words, STPA can be applied during any parts of the development phase.

FMEA is a bottom-up approach. For this analysis, it is necessary to prepare the detailed design of the system. As mentioned above, during development, this requirement is quite onerous because of the changing requirements and design during the development of the system. This means that application of FMEA in the initial development phase is quite demanding. In any recent project, changes in requirements are likely to happen in any development phase. Requirements and designs do not become fixed so early in the development phase. Thus, a safety analysis method that can be applied in any development phase is preferred. In this regard, STPA, as indicated above, is much more useful than FMEA.

When considering spending resources for safety analysis in the latter half of the development phase, it is quite difficult for developers to dedicate time to safety analysis. To prevent future accidents, it is quite crucial to prepare safety requirements early in the development of a system. Developers should allocate time to the early preparation of safety requirements, and include them in the product requirements of the system.

Given these considerations, STPA is a top-down approach. This means that it enables developers to link accidents and hazards directly. In contrast, as I mentioned above, FMEA is a bottom-up approach, so developers cannot intuitively link accidents and hazards with potential effects of failure. This contrast is also tremendously important for preparing to avoid accidents that could happen to the system.

Moreover, by identifying the system's safety constraints that are required to maintain safety from STPA Step 1 and identifying the possible requirements, this analysis initially done in Chapter 5 enables the system to have safety requirements in its developing phase. This point is also quite useful for the development of a complex system. By applying STPA analysis for the human controller and the computer controller, I could identify the safety constraints that must be enforced to ensure safety, and those constraints should be considered as part of the system design requirements. I was also able to identify scenarios beyond the component failures, which enabled me to understand how a human's mental flaws (e.g., belief, past experience) and the contextual factors (e.g., schedule pressure, environmental factors, management pressure) can lead to unsafe control actions that result in a shift of the system's safety towards a more hazardous situation.

The safety constraints that were identified in STPA Step 1 were derived from the control actions of the safety control structure. On the other hand, the possible requirements, which were identified in STPA Step 2, were derived from the components in the safety control structure, such as control actions and feedback. These safety constraints and possible requirements will be used for the product requirements and risk management. In other words, these constraints and requirements would be included in the product requirements or the contingency plans of risk management. Thus, the product development projects have to include these items holistically in their development process. It is quite important to prevent accidents before they happen.

Finally, if analysts repeatedly use STPA, the analysis time decreases drastically from the first time to the second time, from the second time to the third time, and so on, as the analysis proceeds. This point is quite important for actual projects, and it is especially effective for product line development projects. [2]

6.2 Conclusion

In this research, STPA is applied to the radiation treatment system, TomoTherapy. Although in the clinical field, this hazard analysis of STPA is a new method, I found that STPA is efficient and functioned well. On the other hand, FMEA is still popular in the medical field. However, according to the report from the FDA, many accidents have happened due to insufficient safety analysis regarding medical equipment. Medical devices have become more complex, and thus can be more hazardous. To avoid serious accidents, application of a method that can identify safer system requirements is paramount. As a whole, in an actual project, we have to balance time and cost when evaluating how much we should consider the safety requirements while developing the system. In other words, we have to make a trade-off between quality and the length of the development period.

My strategic question was, "Is STPA a more effective means to design safer medical devices than the traditional means in the current medical industry?" Without hesitation, I answer "yes" to this question. I believe that STPA can be used for any developmental phase of medical equipment.

6.3 Future Work

In this research, STPA is applied to the radiation treatment system TomoTherapy. This time, I focused on the "operation and physical system layers." If possible, it would also be quite useful to apply STPA to the "organization layer," including regulatory and development management. Especially, in the development phase of equipment, it is quite important to reveal the ways to communicate and fix requirements of a system among controllers in this layer. For example, the new and changing regulations from the FDA will hugely impact the requirements and functions of the developing system.

Flaws in traditional hazard analysis techniques such as Event Tree Analysis (ETA) and FTA are that they do not work well for complex systems, especially when it comes to software errors, human errors, and system design errors. In addition, such techniques do not usually include organizational and management flaws. The focus of FMEA, ETA, and FTA is limited to failure events and component failures, and does not account for component interaction accidents and organizational factors in the safety control structure. However, for future improvement, we need to compare the results of using STPA with those of other system safety techniques, such as ETA, FTA, HAZOP, and so on.

Moreover, because of time limitations, I could not identify causal scenarios for all the UCAs. Future work that identifies causal scenarios for the rest of the UCAs may help us identify crucial factors that cause hazards and accidents.

Finally, we need to consider how to connect the results of STPA application, such as safety constraints and possible requirements for scenarios, with initial system requirements. This should be a focus in the future for actual development projects.

6.4 References

[1] Todd Pawlicki et al (2016), "Application of systems and control theory-based hazard analysis to radiation oncology," Med Phys. 2016 Mar;43(3):1514-30.

[2] John Thomas (2017), "Implementing STPA Successfully in Industry," 2017 STAMP Workshop Presentations.