Safety Science 118 (2019) 772–782

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

A system safety approach for tomographic treatment

Shinichi Yamaguchi*, John Thomas

Massachusetts Institute of Technology, 77 Massachusetts Ave. Rm 33-407, Cambridge, MA, United States

ARTICLE INFO

Keywords:
Tomographic treatment
TomoTherapy
System safety
Hazard analysis
FMEA
STPA

ABSTRACT

In recent years, technology in the medical industry has been advancing to provide safe and systematic medical care. However, medical technologies and treatments have also become more complicated, presenting new challenges for the traditional approaches used to engineer safety-critical systems. This research compares one of the most popular approaches in the medical device industry, Failure Mode and Effect Analysis (FMEA), with a relatively new method, System-Theoretic Process Analysis (STPA), in the context of a tomographic treatment system. STPA is found to be an effective means to ensure the quality of TomoTherapy and to conduct a holistic hazard analysis including both human and technical factors. A comparison of STPA and FMEA results found that STPA can identify a larger set of causal scenarios. The interactions of humans, hardware, and software were highlighted through the new STPA approach.

1. Introduction

State-of-the-art medical technology has been advancing rapidly to provide physicians, nurses, and medical staff with more effective medical treatments. Medical devices have become more complex, and strict safety standards have been created to govern the treatment processes. One of the most popular methods currently used to ensure the quality of medical devices is Failure Modes and Effects Analysis (FMEA), and many medical device companies have been applying FMEA to their products. FMEA was identified as a powerful tool in radiation oncology by Task Group 100 of the American Association of Physicists in Medicine (AAPM) (Huq et al., 2008). FMEA approach was also recommended by the International Commission on Radiological Protection (ICRP) as a resource for improving the safety of patients undergoing modern radiation therapy treatments (ICRP, 2009).

Despite current efforts, the FDA reports that many medical devices have led to healthcare accidents and are being recalled every year due to reasons such as radiation errors (Johnson, 2016). Analysis techniques like the widely-applied FMEA use a failure-based model that identifies and evaluates potential single-point failures but may miss more complex causes of accidents like design flaws, complex human factors issues, non-failed components that interact in unforeseen ways, and combinations of failures. New accident causality models have been developed to address these shortcomings, like the Systems-Theoretic Accident Model and Process (STAMP) model based on systems theory (Leveson, 2004) and new hazard analysis methods like the Systems Theoretic Process Analysis (STPA) (Leveson, 2012; Leveson and Thomas, 2018).

TomoTherapy is a type of tomographic treatment system that is used throughout the world. The additional complexity has been challenging the traditional methods used to ensure medical device safety (Accuray Incorporated, 2018). In recent years, several tomographic treatment systems were found to cause radiation errors and the accidents were reported (the ST. Cloud Times, 2016). Although FMEA is commonly used to anticipate safety problems in radiation treatment systems and prevent these accidents, there is a concern that important factors may be overlooked. For example, Broggi et al. applied FMEA to radiation treatment system called TomoTherapy for safety analysis as previous research. However, this research focused on human factors, so other important factors like requirements and design errors may not be fully considered (Broggi et al., 2013, 2015). In this research, we apply STPA to TomoTherapy to evaluate its effectiveness and to compare the results with those of FMEA.

2. Research overview

2.1. Accident model

Systems Theoretic Accident Model and Process (STAMP) is a new system-theoretic accident model, which replaces the traditional chain-of-events model underlying most current accident investigation, prevention, and assessment procedures. The STAMP model includes

* Corresponding author at: Graduate School of System Design and Management, Keio University, Collaboration Complex, 4-1-1 Hiyoshi, Kouhoku-ku, Yokohama, Kanagawa 223-8526, Japan.
E-mail addresses: syama@keio.jp (S. Yamaguchi), jthomas4@mit.edu (J. Thomas).

https://doi.org/10.1016/j.ssci.2019.05.041
Received 2 November 2018; Received in revised form 7 May 2019; Accepted 27 May 2019
0925-7535/ © 2019 Elsevier Ltd. All rights reserved.

hardware, software, organizations, management, human decision-making, and migration of systems which will eventually reach states of heightened risk over time (Leveson, 2012).

STAMP is based on systems theory and control theory (Leveson, 2004). STAMP recognizes that accidents are more than a chain of events, and they involve complex dynamic processes. STAMP treats accidents not as a failure problem but as a control problem, and STAMP focuses on preventing accidents by enforcing constraints on component behavior and interactions. STAMP treats accidents holistically and identifies more causes of accidents beyond faults and failures such as unsafe interactions among components, complex human and software behaviors, design errors, and flawed requirements like in software-related accidents. In short, accidents are caused by inadequate control in the system.

2.2. Analysis Method: System Theoretic process analysis (STPA)

System-Theoretic Process Analysis (STPA) is a new method for hazard analysis based on the STAMP causality model. STPA provides a method of systematically identifying inadequate controls in a system and scenarios that lead to hazards. While traditional techniques like FMEA were created to analyze component failures and the losses that can result, STPA was designed to address the increasingly common component interaction accidents. These accidents can result from design flaws or unsafe interactions among operational components). STPA has four main steps, as described in the STPA Handbook (Leveson and Thomas, 2018).

Step 1. Define Purpose of the Analysis

During this first step, the basic accidents that must be prevented are identified. For example, a loss of life must be prevented. The rest of the STPA process will identify the causes that can lead these accidents. The system boundary is also defined in this step, and system-level hazards are identified. System-level hazards are system states or conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss (Leveson and Thomas, 2018).

Once the system-level hazards are identified, system-level constraints are identified by inverting the condition in the hazard. These system-level constraints are the highest-level behaviors that the system (however it is implemented) will need to prevent in order to avoid losses. The system-level constraints are independent of the implementation, which may not yet be known when this step is performed. In later steps, lower-level constraints and requirements will be defined for controllers and other components of the system. The lower-level constraints will specify the component behaviors that are needed to enforce these system-level constraints.

Step 2. Model the Control Structure

A control structure models the feedback control loops in the system and explains the hierarchy of control in the system. Interactions are captured as feedback and control paths. The control structure usually begins at a very abstract level and is iteratively refined to capture more detail about the system. An example of a simple control structure is shown in Fig. 1.

Step 3. Identify Unsafe Control Actions

The control actions in the control structure need to be analyzed to identify how they could lead to the accidents and hazards defined in the first step. These unsafe control actions are used to create functional requirements and constraints for the system. Four types of unsafe control are considered in this step:

- Control actions required for safety are not provided
- Unsafe control actions are provided, leading to a hazard
- Potentially safe control actions are provided too early, too late, or out of order
- Control actions are applied too long or stopped too soon

Step 4. Identify Causal Scenarios

The last step identifies the reasons why unsafe control might occur in the system. Causal scenarios describe how control actions, feedback, flawed beliefs, and other factors may arise together to cause the hazards in the first step. Some scenarios will include important component failures that can lead to hazards, as in an FMEA, but scenarios may also describe interactions that lead to hazards without any component failures—such as components that operate exactly as designed and required but the design and requirements were based on incorrect assumptions.

Two types of causal scenarios must be considered:

1. Scenarios that explain how Unsafe Control Actions might occur
2. Scenarios that explain how safe control actions could be improperly executed or not executed, leading to hazards

Type 1: Identifying scenarios that lead to Unsafe Control Actions

These scenarios are identified by starting with an Unsafe Control Action and working backward to identify factors that could cause the controller to provide (or not provide) that a control action. Scenarios that lead to Unsafe Control Actions may involve:

1-1 Unsafe controller behavior and decision-making
2-1 Inadequate feedback and other information

Type 2: Identifying scenarios in which control actions are improperly executed or not executed

Hazards can be caused by Unsafe Control Actions, but they can also be caused without an Unsafe Control Action if safe control actions are improperly executed or not executed. To create these scenarios, we must consider factors that affect the control path as well as factors that affect the controlled process:

2-1 Scenarios involving the downstream control path
2-2 Scenarios related to the downstream controlled processes

Once causal scenarios are identified, they can be used to create additional requirements, identify mitigations, drive the architecture, make design recommendations and new design decisions (if STPA is used during development), evaluate/revisit existing design decisions and identify gaps (if STPA is used after the design is finished), define test cases and create test plans, develop leading indicators of risk, and so on. In this research, this process was used to identify hazardous scenarios and requirements for the TomoTherapy system.

Regarding the identification of causal scenarios for human controllers, we use the new model proposed by Thomas (Thomas and France, 2016) to guide the analysis and anticipate causes related to human mental models of the current process state, process behavior, and environment (Fig. 2). The model also examines how mental models change over time (“Mental Model Updates”) and how humans use mental models to provide control actions. For more information about this human model, see (Thomas and France, 2016) and (France, 2017a, 2017b).

2.3. Comparison criteria

This research compares the results of FMEA with STPA, both applied to a tomographic treatment system. The causal taxonomies in Appendix D from the work by Ford et al. (2012) are used to compare results—these taxonomies are based on consensus recommendations for incident learning database structures in radiation oncology (Ford et al., 2012). The aim of these causal taxonomies is to facilitate the identification of all root causes and contributory factors that govern an incident and to reduce a human subjective judgement among users.

The higher-level categories are used to categorize and compare results of FMEA and STPA in this research. The categories are as follows: Organizational management, Technical (physical system, software,

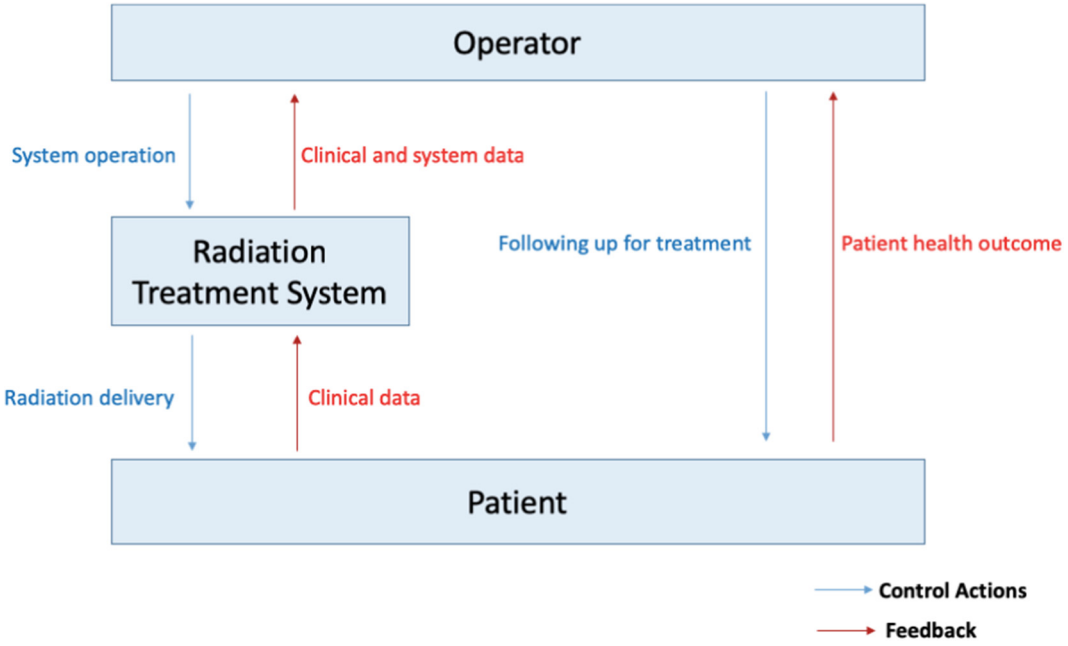

Fig. 1. Example of a simple control structure.

etc.), Human behavior of individual staff, Patient-related circumstances, External factors (beyond facility control), Procedural issues, Other.

2.4. Tomographic treatment system (TomoTherapy)

TomoTherapy® Highly Integrated Adaptive Radiotherapy (HI-ART) is one popular tomographic treatment system used throughout the world.

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 is also used when it is important to avoid certain nearby 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 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). It is sometimes referred to as helical TomoTherapy due to the path the beam takes and the pitch factor.

Generally, radiation therapy is developed with a strong reliance on the homogeneity of dose distribution throughout the tumor. TomoTherapy utilizes sequential delivery of radiation to different parts of the tumor, known as “field matching”, which raises two important issues. First, this method 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. Secondly, 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 issue requires close attention to the position of the target throughout treatment delivery.

In general, a TomoTherapy system will: (Cancer Treatment Centers of America, 2017)

- Perform 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

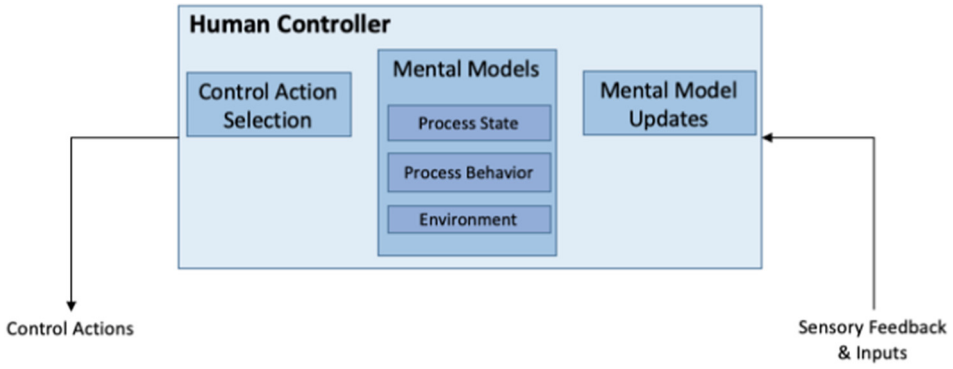

Fig. 2. Extended model of the human controller.

plans and coordinates treatment delivery.

3. Applying STPA to TomoTherapy

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

1. Define Purpose of the Analysis (Accidents and Hazards)
2. Model the Control Structure
3. Identify Unsafe Control Actions
4. Identify Causal Scenarios

3.1. Define the purpose of the analysis

The first step is to identify the goals of the system and the basic accidents (losses) that must be prevented There are two main goals of this system:

G1: Provide radiation treatment for patients

G2: Exposes patients to minimal radiation needed for efficient radiation therapy

In STPA, an accident is defined as 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 becomes worse for patients (e.g. tumor progression)

Next, the system-level hazards that lead to the accidents are identified. In STPA, a hazard is defined as a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. In Table 1 below, we defined the hazards relevant to stakeholders including medical practitioners and patients. The hazards are then used to create system-level constraints, shown in Table 2.

3.2. Model the control structure

After the system-level hazards have been identified, a hierarchical control structure for the system is modeled. In STPA, a safety control structure is composed of hierarchically organized feedback control loops.

Fig. 3 shows the existing safety control structure (level 1) with an organizational layer at the top. In total, we modeled 12 controllers and 5 control actions in this control structure.

In this analysis, we include the operation layer and the physical system layer because they are often overlooked before an accident occurs.

Five rooms are normally required for TomoTherapy: the treatment room, the operator station, the data server room, the mechanical room, and the treatment planning room (Accuray Incorporated, 2014).

Using the information mentioned in "TomoTherapy HTM Series Site Planning Guide," the existing physical system's safety control structure is depicted below (Fig. 4). Also, the explanation about each controller is described in Table 3. The data server does not belong to the category as a control component because it is simply a communication channel.

3.3. Identify unsafe control actions

Unsafe Control Actions (UCA) were analyzed based on the level 2 safety control structure (Fig. 4), which includes 8 controllers and 26 control actions. Focusing on the operation layer and physical system layer, a total of 99 UCAs were identified using the STPA methodology described above. These UCAs 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. Tables 4 and 5 show a partial set of UCAs that were identified. The control actions are closely related to the A1 accident, which is the most serious for patients.

From these UCAs, 81 safety constraints were identified for TomoTherapy to prevent the system hazards H1-H6. A partial list of safety constraints for human operators and automation is shown in Tables 6 and 7.

3.4. Identify causal scenarios

The next step is to identify scenarios by analyzing why unsafe control actions might occur in the system and how otherwise safe control actions might not be executed or followed properly.

Unsafe control actions can occur 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. While component failure-based hazard analysis techniques identify causes related to failures, STPA allows the analyst to identify causes due to both component failures and other factors like requirements and design errors. For example, the component may not fail and may satisfy its requirements completely but those requirements may be incorrect or incomplete, perhaps because the

Table 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)	The equipment does not work properly or breaks down due to unnecessary loading time, speed, power, etc.
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 radiation treatment

Table 2
System-level constraints.

Hazard ID	System-level constraints
H1	SC1: The correct treatment areas must be exposed to the correct amount of radiation
H2	SC2: Non-patients such as medical practitioners and operators must not be exposed to radiation emitted from the device
H3	SC3: The radiation treatment system must not damage people physically during its operation or treatment
H4	SC4: The equipment must work properly not to be subject to unnecessary loading time, speed, power, etc.
H5	SC5: Environment around the equipment must not be exposed to radiation emission from the equipment
H6	SC6: Radiation treatment must be provided only for patients who need radiation treatment

designer misunderstood how the system components would interact or did not account for human errors.

This step produces Causal Scenarios that explain how hazards and accidents could occur. For example, consider "UCA 11-2: The operator provides start command to the workstation when the wrong patient is present". Fig. 5 shows the specific control loop for UCA11-2 using technical information from Accuray (Accuray Incorporated, 2014). Fig. 5 also uses the human controller model proposed by Thomas (Thomas and France, 2016) to guide the analysis and anticipate causes related to human mental models of the current process state, process behavior, and environment, as explained in Section 2.2.

The following scenarios were identified:

UCA 11–2: The operator provides the start command to the workstation when the wrong patient is present

Causal Scenario 1: The operator provides the start command to the 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.

Different types of potential requirements can be created based on causal scenarios. For example, requirements can be defined for operational procedures, human operator responsibilities, the technical system, and for testing.

Possible Requirement 1_1: The nurse shall make sure wrong patients do not enter the treatment room by checking the name, date of birth, state, etc.

Possible Requirement 1_2: The operator shall ask the spelling of the patient's full name.

Possible Requirement 1_3: 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_4: The system shall lock until the patient's wrist band is scanned and it matches the patient ID in the treatment file.

Possible Requirement 1_5: The system shall be tested to verify that the system remains locked when the patient ID in the treatment file

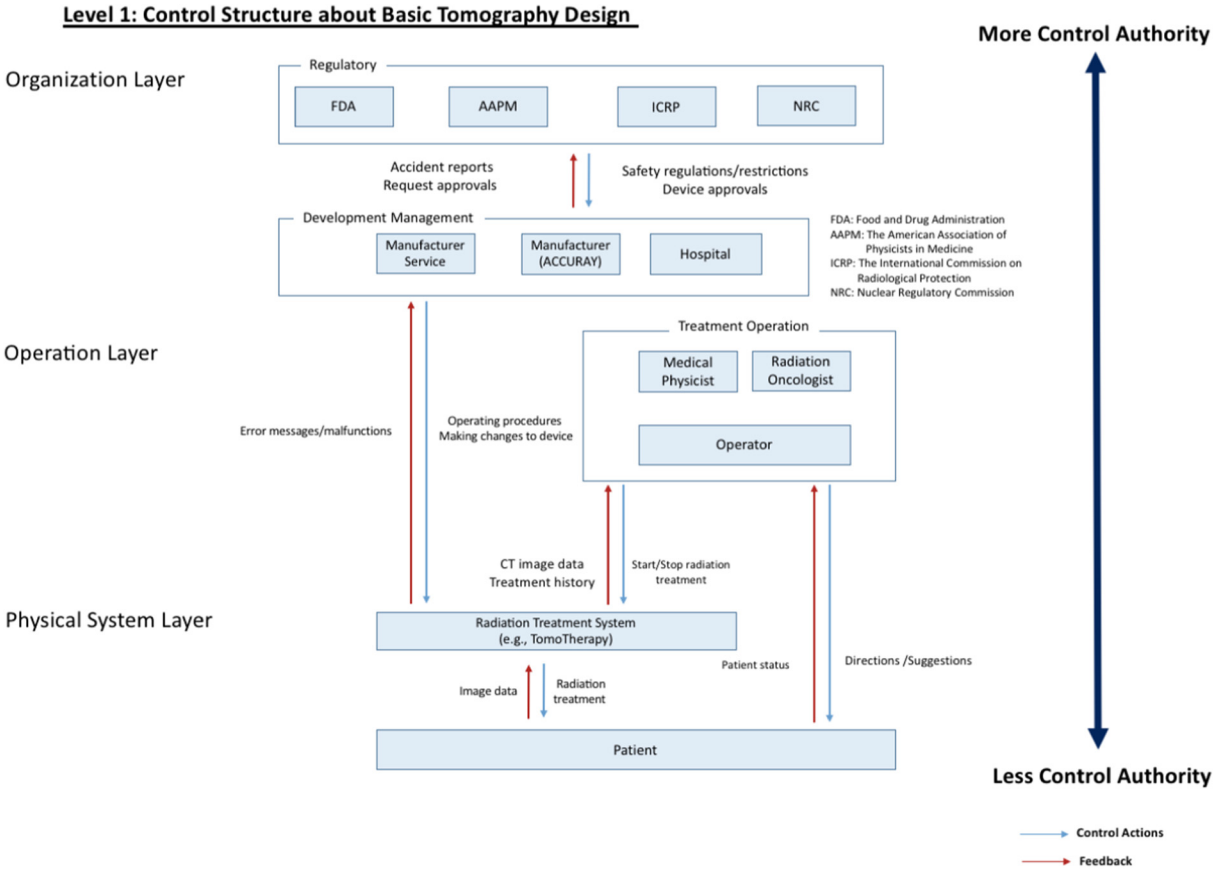

Fig. 3. Existing safety control structure – Level 1.

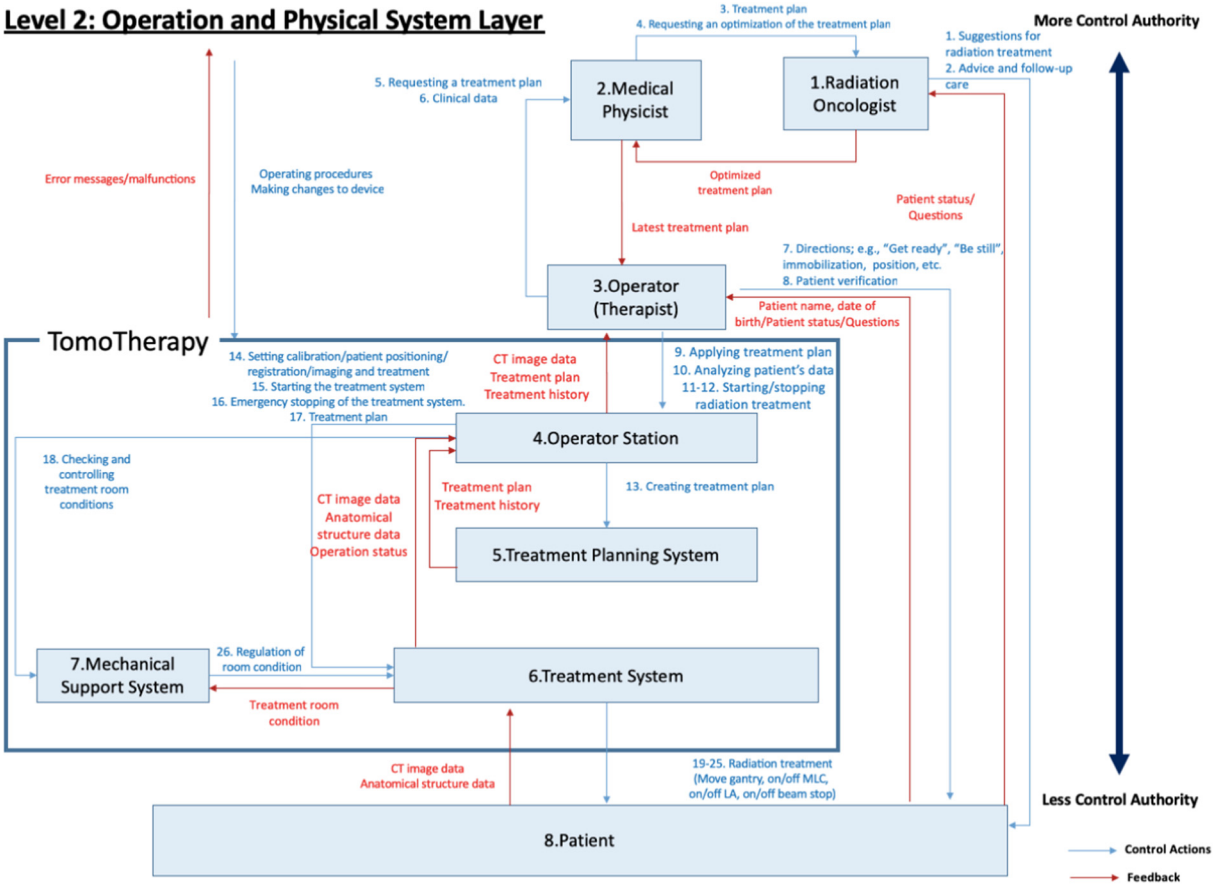

Fig. 4. Existing safety control structure – Level 2. (Operation Layer and Physical System Layer).

does not match the scanned wrist band.

Causal Scenario 2: The operator provides the start command to the workstation when the wrong patient is present. 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 auditory processing disorder, speech disorder, 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: An alternative means of patient verification (other than oral) must be allowed

Possible Requirement 2_2: The operator shall reconfirm the patient profile before the patient enters the room.

Possible Requirement 2_3: The operator station shall automatically show the patient profile including a picture of the patient via its console before the patient is allowed to enter the room.

Possible Requirement 2_4: The system shall provide a means for visual verification that the current patient on the couch in the treatment room matches the picture from the patient profile.

Causal Scenario 3: The operator provides the start command to the 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 the 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 the room unless the 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.

Table 3
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 giving directions to a patient before and during the treatment	-Verifying the right patient's identification -Giving directions to a patient, such as "get ready," "be still," 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 a 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 system	Make patients' treatment plan according to the direction of an operator via the operator station, and send command to store data regarding treatment plans and patient	-Providing treatment plan with the treatment system
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 TomoTherapy and to regulate the room conditions of the treatment system such as heating, cooling and humidity by supplying a dedicated oil-free air compressor, air tank, compressed air line, dryer and inline air regulator 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	–

Causal Scenario 5: The operator provides the start command to the 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.

4. FMEA application to assure safety in TomoTherapy

FMEA was applied to TomoTherapy by a professional team in 2013 and 2015. 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. According to the analysis by Broggi et al. (2013, 2015), FMEA was applied to identify all the sub-processes involved in the stages of preplanning imaging and volume determination, treatment planning and 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, the process trees were developed. The process consists of three main process steps and 74 sub-processes (30 sub-processes in the preplanning and volume determination stage, 28 sub-processes in the planning stage and 16 sub-processes in the delivery stage). After that, 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.

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. (2009) were used as its guidelines. Also, the risk probability number (RPN) was calculated as the product of the three attributes: $RPN = O \times S \times D$. The value $RPN = 125$ was considered as a threshold below which the risk can be considered acceptable. About their result, 21 failure modes were characterized by an RPN score higher than 80.

For example, in TomoTherapy deliver stage, incorrect patient identification was identified during the patient call (RPN = 84). The most severe potential consequence could be the treatment of the wrong patient with the same anatomical site. Also, during plan selection, the recognized potential failure was the selection of the plan of the wrong patient, with the same anatomical site to be treated, but not yet treated or not scheduled for the same day. The potential cause of the two failures was "lack of attention," and the potential effects of failure were "wrong treatment for a single session" (Broggi et al., 2015).

The analysis was carried out by a professional 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.

5. Comparing the results of STPA and FMEA

In this research, STPA was applied to TomoTherapy. As a result, six

Table 4
Partial list of Unsafe Control Actions (UCAs) for a human operator.

No.	Control action	Not providing causes hazard	Providing causes hazard	Incorrect timing/ordering	Stopped too soon/applied too long
11	Start command (human operator)	[UCA 11-1] The operator does not provide the start command to the workstation when the right patient is present [H1, H6]	[UCA 11-2] The operator provides start command to workstation when the wrong patient is present [H1, H6]	[UCA 11-3] The operator provides start command to workstation after the radiation treatment has begun [H1, H6]	- (The duration of the verification does not cause hazards)

system-level constraints, 99 UCAs, 88 safety constraints, 10 causal scenarios, and 33 possible requirements were identified. On the other hand, FMEA identified a total of 74 failure modes, and 30 potential causes of failures.

Table 8 compares the results found with FMEA and STPA. The categories for this table were adapted based on the causality table (Ford et al., 2012; Pawlicki et al., 2016). In examining the results of FMEA, the failure modes identified by Broggi et al. in 2013 and 2015 were mapped to each category of Table 8.

According to these results, it can be observed that FMEA was mainly focusing on two categories, namely, “technical (physical system)” 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 technical (physical system), technical (others), human factors, circumstances, procedure, etc. The technical (others) causal category includes various factors such as software, testing, failure handling, etc. (Ford et al., 2012).

FMEA identified failure modes based on linear process trees and did not consider the behaviors of the entire system. In reality, accidents can be caused by many controllers including those in a physical system, software, human operator, organization, etc. and these controllers have complicated relationships. STPA uses the control structure model to include these controllers and their interactions in the safety analysis. The results of STPA were found to cover a broader range of accident causes than FMEA. More specifically, STPA found causal scenarios involving physical system characteristics, software interactions, human behavior, gaps in the technical system, procedural issues, and patient-related circumstances.

When comparing the results of STPA with those of FMEA, STPA uncovered additional causes that led to additional requirements. For example, using FMEA, “wrong patient identification (with the same anatomical site)” was found as a potential failure mode. The potential cause of failure was “lack of attention,” and the potential effects of failure were “wrong treatment for a single session (Broggi et al., 2015). STPA identified similar results in the causal scenarios for UCA 11-2. While FMEA just found one case of the failure to relay the right patient’s identification, but STPA found five related scenarios that contain more information than that of the results of the FMEA. As a result, four additional requirements were identified in terms of an operational procedure and a technical system requirement: “Possible Requirement 1_2: The operator shall ask the spelling of the patient’s full name” and “Possible Requirement 1_3: The treatment room shall be connected to one operator workstation and one intercom unit to prevent the intercom unit from connecting to multiple rooms” and “Possible Requirement 1_4: The system shall lock until the patient’s wrist band is scanned and it matches the patient ID in the treatment file” and “Possible Requirement 1_5: The system shall be tested to verify that the system remains locked when the patient ID in the treatment file does not match the scanned wrist band.”

FMEA mainly focused on a human error with the aim of optimizing quality management workflow in the previous analysis. FMEA identified and evaluated potential single-point failures. On the other hand, STPA highlighted the interaction of human, hardware, and software. For example, in the sub-process “Patient call” at the TomoTherapy delivery stage, one of the potential FMEA failure modes was “Plan selection of the wrong patient, with the same anatomical site to be treated, but not yet treated or not scheduled for the same day” caused by “Lack of attention.” As a result, if that failure is not detected by the Mega-Volt Computed Tomography (MVCT) scan acquisition, the wrong treatment for a single session may occur. This indicated that FMEA simply identified and evaluated potential sing-point failure in terms of a human operator. On the other hand, STPA scenarios like Causal Scenario 1 for UCA 11-2 considered the interaction among the operator, patient, and intercom system including hardware (speakers, microphones, cables, etc.) and its embedded software to operate the system. Thus, it is evident that STPA can be used as a technique to identify

Table 5
Partial list of Unsafe control actions (UCAs) for software.

No.	Control action	Not providing causes hazard	Providing causes hazard	Incorrect timing/ordering	Stopped too soon/ applied too long
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]	–

Table 6
Partial list of safety constraints for a human operator.

Unsafe Control Action (UCA)	Safety constraints
[UCA 11-1] The operator does not provide the start command to the workstation when the right patient is present	[SC 11-1] The operator must provide start command to the workstation when the right patient is present
[UCA 11-2] The operator provides the start command to the workstation when the wrong patient is present	[SC 11-2] The operator must not provide the start command to the workstation when the wrong patient is present.
[UCA 11-3] The operator provides start command to workstation after the radiation treatment has begun	[SC 11-3] The operator must provide start command to workstation before the radiation treatment has begun

Table 7
Partial list of safety constraints for software.

Unsafe Control Action (UCA)	Safety constraints
[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
[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
[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

potential causes as causal scenarios more comprehensively than FMEA.

6. Comparison to previous work

There are some similarities between these results and previous work by Pawlicki et al. (2016) to compare FMEA and STPA for applications involving radiation therapy. Both efforts found that STPA identified a broader set of causes than FMEA and STPA was more effective at highlighting interactions in the broader system.

However, there are also several differences between this and previous work. Pawlicki et al. (2016) emphasized organizational and operational aspects in a clinic, such as understanding the role of management decisions and hospital operations on system safety. The current study placed more emphasis on treatment delivery, including specific TomoTherapy software control actions and operator (therapist) interactions with the TomoTherapy system. The TomoTherapy system studied here is also different than the Linac system studied by Pawlicki et al. (2016). Although both studies examined applications of radiation therapy, the specific control actions, UCAs, feedback, scenarios, and requirements are different for TomoTherapy than for the system studied in Pawlicki et al. (2016).

Another important difference is the STPA methodology used. This paper explains and follows the process in the STPA Handbook (Leveson and Thomas, 2018), which wasn't available when the previous work was done. The STPA Handbook describes a four-step process and contains additional guidance and criteria than the process used in Pawlicki et al. (2016). For example, the previous work did not specify system-level constraints and did not use the same process for creating causal scenarios based on four types described above. Another methodology difference is that the current work used a new model for human controllers to identify causal scenarios. This current work demonstrates that the new methodology is feasible and applicable to the human and automation interactions in the TomoTherapy system.

One final important difference is that Pawlicki et al. (2016) did not use STPA to identify requirements. In this research, STPA was used to identify requirements in several areas such as hardware, software, human factors. Identifying requirements is an important part of safety engineering and is quite useful for system development.

7. Conclusion

In this research, STPA was applied to the TomoTherapy radiation treatment system. Although STPA is a new method in the clinical field, we found that STPA is efficient and functioned well. On the other hand, FMEA is still popular in the medical field (Huq et al., 2008; ICRP, 2009). Unfortunately, according to the FDA report (Johnson, 2016), many accidents have involved inadequate safety analysis of medical equipment. Medical devices have become more complex, and thus can be more hazardous. To avoid serious accidents, a method that can identify a larger set of causal scenarios and considers complex interactions among system components such as human, hardware, and software is necessary. In this research, it is found that STPA is a more effective means to conduct hazard analyses for medical equipment like TomoTherapy because STPA holistically analyzes both human and mechanical factors. The results of STPA and FMEA were compared, and it was found that FMEA mainly focused on a human error with the aim

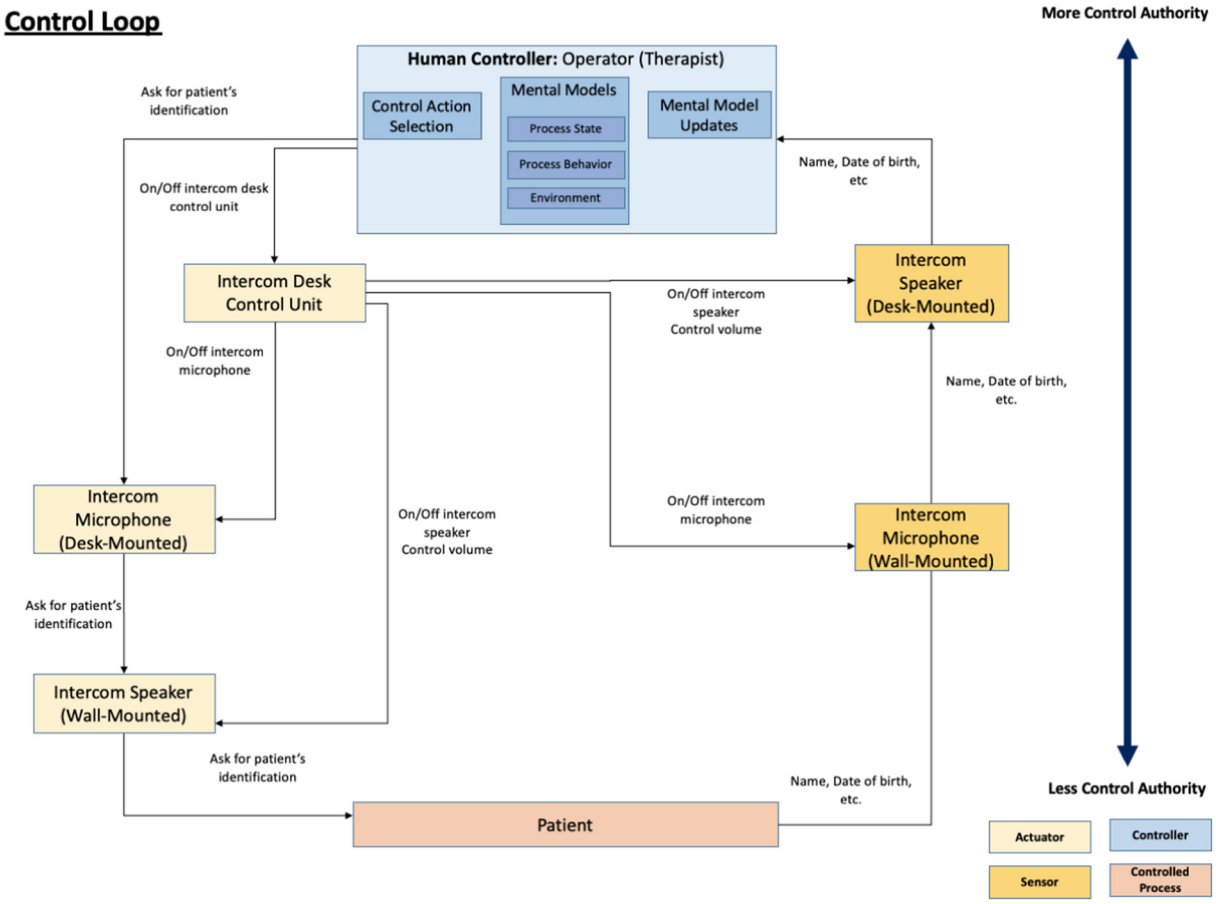

Fig. 5. Control Loop for UCA 11-2.

Table 8
Causality table of the results of STPA and FMEA. (In examining the results of FMEA and STPA, the contents were mapped).

Causality category	FMEA	STPA
Technical (physical system)	13%	30%
Technical (others)	0%	10%
Human behavior of individual staff	87%	40%
Patient-related circumstances	0%	10%
Procedural issues	0%	10%
Total	100%	100%

of optimizing quality management workflow. FMEA identified and evaluated potential single-point failures while STPA identified a larger set of causal scenarios. The interaction of human, hardware, and software was highlighted through the STPA procedure.

Declaration of Competing Interest

None.

Acknowledgements

The authors thank Nancy Leveson from MIT Aeronautics and Astronautics Dept. for her assistance in the direction of this research and the external review of the results.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Appendix A. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ssci.2019.05.041.

References

Accuray Incorporated, 2014. TomoTherapy HTM Series Site Planning Guide. https://www.accuray.com/wp-content/uploads/t-spg-00725.pdf.
Accuray Incorporated, 2018. TomoTherapy. http://www.tomotherapy.com.
Broggi, S., et al., 2013. Application of failure mode and effects analysis (FMEA) to pre-treatment phases in TomoTherapy. J. Appl. Clin. Med. Phys. 14, 265–277.
Broggi, S., et al., 2015. Application of failure mode and effect analysis to tomotherapy treatment delivery. Radioprotection 50 (3), 171–175.
Cancer Treatment Centers of America, 2017. What is TomoTherapy. http://www.brachytherapy.com/tomotherapy.aspx.
Ford, E.C., Gaudette, R., Myers, L., Vanderver, B., Engineer, L., Zellars, R., Song, D.Y., Wong, J., DeWeese, T.L., 2009. Evaluation of safety in a radiation oncology setting using failure modes and effects analysis. Int. J. Radiat. Oncol., Biol., Phys. 74 (3), 852–858.
Ford, E.C., Fong de Los Santos, L., Pawlicki, T., Sutlief, S.,, Dunscombe, P., 2012. Consensus recommendations for incident learning database structures in radiation oncology. Med. Phys. 39 (12), 7272–7290.
Huq, M.S., Fraass, B.A., Dunscombe, P.B., et al., 2008. A method for evaluating quality assurance needs in radiation therapy. Int. J. Radiat. Oncol. Biol. Phys. 71 (1 Suppl), S170–S173.
International Commission on Radiological Protection, 2009. Preventing accidental exposures from new external beam radiation therapy technologies. Annals of the ICRP. 2009; 39(4).
Johnson, Judith A., 2016, FDA Regulation of Medical Devices. https://fas.org/sgp/crs/misc/R42130.pdf.
Leveson, Nancy G., 2004. A new accident model for engineering safer systems. Saf. Sci. 42 (4), 237–270.
Leveson, Nancy G., 2012. Engineering A Safer World: Systems Thinking Applied to Safety. MIT Press.
Leveson, Nancy G., Thomas, John P., 2018. STPA HANDBOOK. http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.
Megan France, 2017. Human-Automation Interaction in STPA. MIT STAMP Conference,

March 2017. http://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/HumansAndAutomationTutorial_MFrance2017.pdf.
Megan France, 2017. Engineering for Humans: A New Extension to STPA, Master's thesis, MIT, Cambridge, MA(US) dissertation.
Pawlicki, Todd, et al., 2016. Application of systems and control theory-based hazard analysis to radiation oncology. Med. Phys. 43 (3), 1514–1530.
The ST. Cloud Times, 2016. Lawsuits allege radiation errors. http://www.advisen.com/tools/fpnproc/fpns/articles_new_2/P/271732451.html?rid=271732451&list_id=2.
Thomas John, France Megan, 2016. Engineering for Humans: STPA Analysis of an Automated Parking System. MIT STAMP Conference, March 2016. http://psas.scripts.mit.edu/home/wp-content/uploads/2016/04/Thomas,France-Engineering_for_Humans.pdf.