Medical Physics
The International Journal of Medical Physics Research and Practice

Application of systems and control theory-based hazard analysis to radiation oncology

Todd Pawlicki, Aubrey Samost, Derek W. Brown, Ryan P. Manger, Gwe-Ya Kim, and Nancy G. Leveson

Citation: Medical Physics **43**, 1514 (2016); doi: 10.1118/1.4942384
View online: http://dx.doi.org/10.1118/1.4942384
View Table of Contents: http://scitation.aip.org/content/aapm/journal/medphys/43/3?ver=pdfcov
Published by the American Association of Physicists in Medicine

Application of systems and control theory-based hazard analysis to radiation oncology

Todd Pawlicki[a)]
Department of Radiation Medicine and Applied Sciences, UC San Diego, 3385 Health Sciences Drive, La Jolla, California 92093

Aubrey Samost
Engineering Systems Division, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02142

Derek W. Brown, Ryan P. Manger, and Gwe-Ya Kim
Department of Radiation Medicine and Applied Sciences, UC San Diego, 3385 Health Sciences Drive, La Jolla, California 92093

Nancy G. Leveson
Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02142

(Received 4 August 2015; revised 31 January 2016; accepted for publication 6 February 2016; published 26 February 2016)

Purpose: Both humans and software are notoriously challenging to account for in traditional hazard analysis models. The purpose of this work is to investigate and demonstrate the application of a new, extended accident causality model, called systems theoretic accident model and processes (STAMP), to radiation oncology. Specifically, a hazard analysis technique based on STAMP, system-theoretic process analysis (STPA), is used to perform a hazard analysis.
Methods: The STPA procedure starts with the definition of high-level accidents for radiation oncology at the medical center and the hazards leading to those accidents. From there, the hierarchical safety control structure of the radiation oncology clinic is modeled, i.e., the controls that are used to prevent accidents and provide effective treatment. Using STPA, unsafe control actions (behaviors) are identified that can lead to the hazards as well as causal scenarios that can lead to the identified unsafe control. This information can be used to eliminate or mitigate potential hazards. The STPA procedure is demonstrated on a new online adaptive cranial radiosurgery procedure that omits the CT simulation step and uses CBCT for localization, planning, and surface imaging system during treatment.
Results: The STPA procedure generated a comprehensive set of causal scenarios that are traced back to system hazards and accidents. Ten control loops were created for the new SRS procedure, which covered the areas of hospital and department management, treatment design and delivery, and vendor service. Eighty three unsafe control actions were identified as well as 472 causal scenarios that could lead to those unsafe control actions.
Conclusions: STPA provides a method for understanding the role of management decisions and hospital operations on system safety and generating process design requirements to prevent hazards and accidents. The interaction of people, hardware, and software is highlighted. The method of STPA produces results that can be used to improve safety and prevent accidents and warrants further investigation. © *2016 American Association of Physicists in Medicine.* [http://dx.doi.org/10.1118/1.4942384]

Key words: STPA, risk, hazard, safety, radiosurgery

1. INTRODUCTION

The process of radiation oncology occurs within a complex sociotechnical system that is heavily reliant on human operators. This reality contributes to deviations in care[1] and catastrophic accidents.[2,3] Recognizing this situation, safety management and prospective risk assessment by failure modes and effects analysis (FMEA) and fault tree analysis (FTA) are actively being promoted by the American Association of Physicists in Medicine.[4] Formal risk analysis techniques have been applied to radiation oncology over a decade ago using root-cause-analysis trees, process trees, and FTA to analyze brachytherapy errors.[5] More recently, FMEA has been applied to a department-wide risk assessment effort.[6] There have also been efforts to study the implementation of FMEA and FTA techniques in radiation oncology.[7–15] Existing studies also give reason to at least question the reliability and validity of FMEA results.[16–18] It is therefore worthwhile to investigate other risk assessment strategies.

Hazard or risk analysis involves identifying the causes of accidents in order to use that information to eliminate or control them. The analysis requires a search process. If all possible system states could be identified, then the risk analysis could find all possible hazardous scenarios.

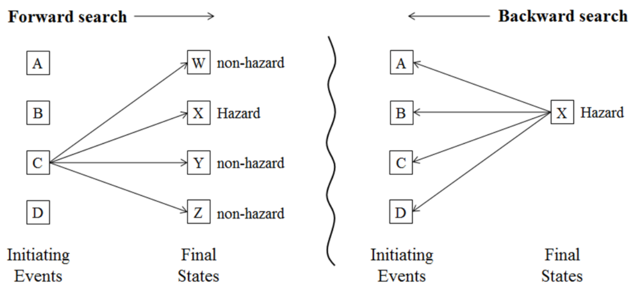

FIG. 1. Schematic comparison of forward (inductive) and backward (deductive) search used in hazard or risk analysis.

Unfortunately, such an exhaustive search is never possible in a real system due to the enormous number of states that complex systems can potentially reach, particularly when component failures are considered in addition to the designed behavior. As shown in Fig. 1, two possible alternative search approaches have been used *in lieu* of being able to identify all hazardous causes by complete analysis. These search techniques can be characterized as either forward (inductive) or backward (deductive).

Forward search techniques start from some initiating event, usually some type of failure, and identify the final states that can result. FMEA is an example of a hazard or risk analysis technique that employs an inductive or forward search. It is not feasible to consider combinations of failures (considering all single failures are extremely time consuming) so for practical reasons, only single failures are considered.

Deductive search techniques, including FTA and the technique called STPA described in this paper, start from a hazardous state and work backward to identify paths to that hazard. Backward search is theoretically more economical than forward search because only hazardous paths are explored and not all paths forward from a failure (which may not lead to hazardous behavior). Unlike forward search, backward search can find combinations of initiating events that lead to the hazard. FTA identifies combinations of system component failures and faults that lead to the hazard and models the relationships between multiple failures and faults using Boolean logic. FTA is limited in the types of interactions that can be included in the analysis and only identifies accident causes involving component failures and faults. Many accidents in complex systems involve design errors, where no system components may fail but the designers inadvertently create flawed designs and procedures. Design errors are not found by search techniques that only look at failures or faults because design errors may not involve any failures but simply the "correct" (as designed) execution of a flawed process or unsafe interactions among system components that are each operating as intended.

Human behavior is realistically modeled as a feedback control loop where the next action is affected by the environment (context) in which it occurs and by the results of the previous action rather than as a linear sequence of steps without taking into account feedback from previous steps.[19] Accident causality models based on systems theory have been developed to address the shortcomings of the failure-based models.[20] One such model, systems-theoretic accident model and processes (STAMP), treats safety as a system control problem rather than a component failure problem.[21] The idea is to ensure that constraints on the behavior of the system (safety constraints) are enforced by the operation of the system as a whole. For example, a safety constraint for radiation oncology is that the patient never receives a larger (or smaller) dose than is prescribed and safe. A safe treatment system should enforce that constraint, that is, control the amount of radiation the patient receives. Accidents can occur when the system controls created to prevent overdoses are not effective. The STAMP model of accident causality was designed to allow software, human behavior, organizational culture, and process changes over time to be included naturally in the hazard analysis while also including failure of process steps and system components.

System theoretic process analysis (STPA) is a deductive hazard analysis method based on STAMP. The goal of STPA is to identify how the safety constraints may be inadequately controlled in a particular setting and to provide the information to create more effective controls and thus reduce or eliminate accidents. The purpose of this work is to demonstrate the applicability of STPA to hazard analysis in a clinical setting. The development and characteristics of STPA are described for use in radiation oncology by focusing on a clinical example. To help provide a qualitative assessment of the STPA methodology, an FMEA is also performed on the same clinical example.

2. METHODS

In systems theory, systems or processes are modeled as hierarchical levels of control where each level of the system controls the behavior of the level below.[22–24] It is assumed that safety is jeopardized when the controls and controllers do not enforce safe behavior, thus allowing accidents to occur.

Control theory is a basic engineering concept. Figure 2 illustrates a typical feedback control loop (drawn for clarity

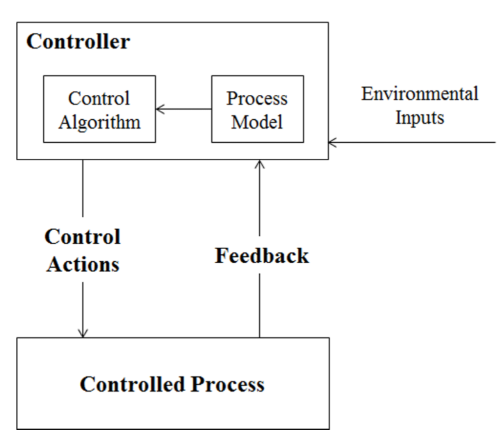

FIG. 2. A standard engineering feedback control loop for a controlled process. The downward arrow represents the actions by the controller to control the process. The upward arrow represents the feedback that the controller receives from the controlled process. The control algorithm contains a comparison of the current state of the process with the desired state and generates control actions necessary to bring them into alignment. The process model is the controller's understanding of the current state of the controlled process.

and consistency with systems theory) where controllers issue control actions that impact the behavior of a controlled process.[22–24] In return, the controller gets feedback about the impact of the control action and the current state of the controlled process. For example, the medical physicist provides a treatment plan and gets feedback from the radiation oncologist about the status of the treatment plan. Using this feedback information about the effectiveness of the control action and the current state of the controlled process, modifications or additional plans may be developed.

The controller includes both an algorithm and a process model that is used to determine the appropriate control action to provide. The process model, control algorithm, and safety responsibilities of the controller need to be described. If the controller is a human, some type of human-oriented decision-making process serves as the algorithm. The decision about the appropriate control action is at least partly based on a model of the current state of the controlled process. The process model is kept up to date by feedback from the process and other environmental inputs. For humans, the process model is usually called a "mental model." Human decisions and control actions are strongly affected by the equipment and the environment and are based on factors other than simple fixed steps.[25,26] For example, based on their training, experience, and specific information about the patient combined with department equipment and the environment, the medical physicist generates a treatment plan. Feedback will be provided during or after the plan is completed, which is used to update the controller's (i.e., medical physicist's) mental model to reflect the current state of the controlled process (i.e., planning and treatment). Process controllers also learn and improve their decision-making processes and mental models about proper treatment over time.

The individual control loops are part of a larger hierarchical safety control structure. Control loops differ from a process map in that the steps are not drawn in chronological order but are modeled as a series of control actions. Figure 3 shows an example of a high-level safety control structure for a radiation oncology department. In Fig. 3, regulatory processes control the vendors and the hospital management and each level control the level below via the control actions listed on the downward arrows. The regulators provide standards and policies for equipment production and treatment provision using that equipment. Accreditation and licensing are other types of control actions by regulators. Hospital and department controllers get feedback in terms of incident reports and various types of performance data. That feedback should be used to alter their future behavior (control actions), for example, requiring that equipment designs or the procedures for using the equipment be altered. The vendors have control over the safety of the equipment they provide and the hospital management and operations provide controls over treatment

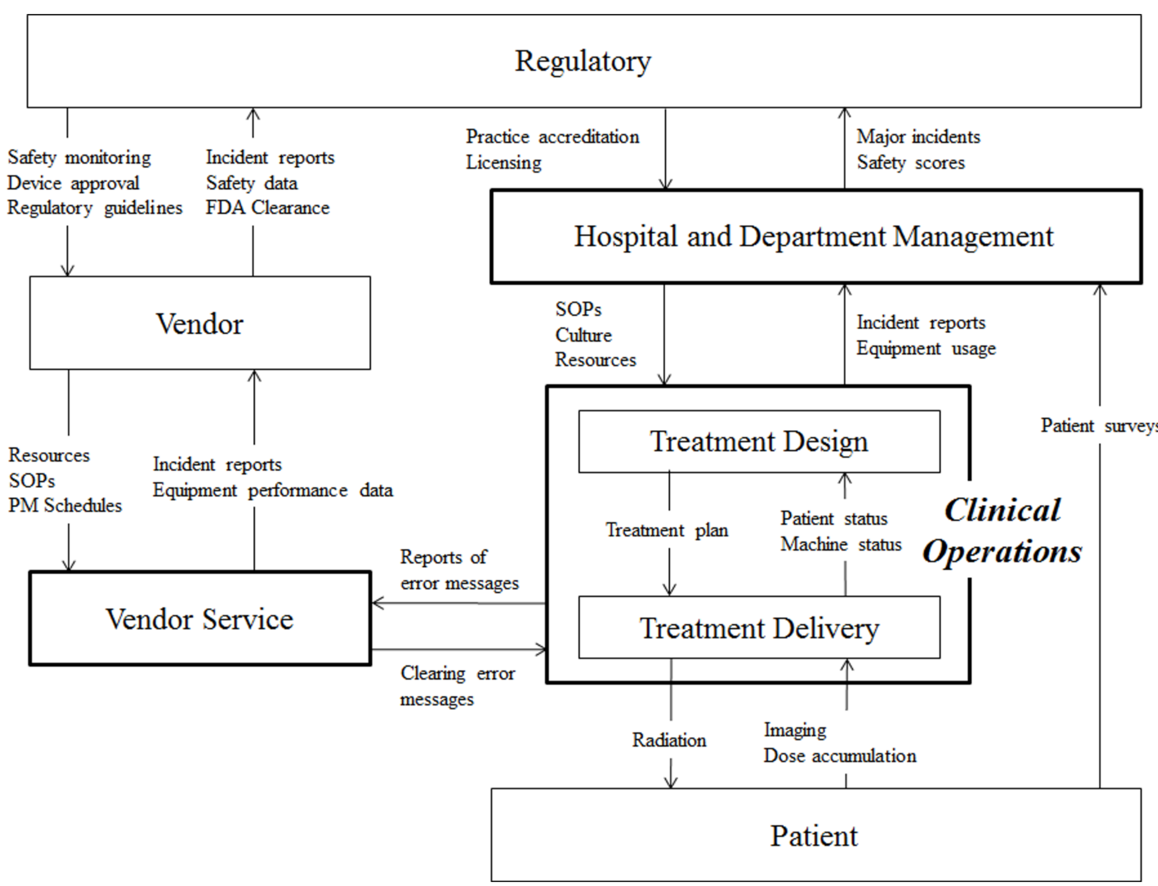

Fig. 3. Example high-level control structure for radiation oncology (PM = preventative maintenance, FDA = Food and Drug Administration, SOP = standard operating procedure).

delivery. With this basic background information, the steps used in STPA are described next.

2.A. Create a system description

The first step is simply to create a description of the system being analyzed, including all organizational and system components. The goal is to define and specify the scope of the analysis.

2.B. Create a list of high-level accidents (*A*)

An accident is defined as an unacceptable loss involving mission, life, health, equipment, or money. Creating the high-level accident list can be accomplished by reviewing publicly available past accidents, data from an incident learning system, or brainstorming sessions. Domain knowledge can be helpful but is not essential because subtle deviations of care are not relevant in defining the high-level accidents. In radiation oncology (or any domain), the defined accidents (losses) will almost always be the same. For example, patient or healthcare worker injury or equipment damage are losses that can be used in all areas of healthcare. Accidents or losses may be prioritized with respect to importance.

2.C. Create a list of system hazards (*H*)

A hazard is a state of the system that would lead to one of the identified accidents given worst case conditions. For example, a hazard may be incorrect patient treatment being administered. While such treatment may not always lead to an accident (loss), under the worst case conditions, it could. The analysis will later identify those conditions and identify the scenarios that could lead to an accident.

A small number of high-level hazards (typically less than 10–12) is usually identified at the beginning. Identifying a large number of hazards would mean that the list is too detailed, which can lead to missing hazards, redundancies, and mixing up causes and effects. The short, high-level list will later be refined into more detailed information if needed. A stepwise refinement process, where more detailed hazards are generated, is easier to review and find omissions or mistakes. The same list of high-level hazards will typically apply to all radiation oncology facilities.

2.D. Create the safety control structure

The next step in STPA is to create the hierarchical control structure (Fig. 3) and associated control actions and known feedback. Missing feedback that can lead to hazards will be identified by the analysis. Construction of the safety control structure model is facilitated by using the system description from Sec. 2.A. Most radiation oncology operations are similar in terms of the high-level control structure and thus existing models can be used and simply modified to match the specifics of the particular hospital or system being analyzed. In addition, the control loops can first be described in terms of high-level controllers and then later refined into more detailed descriptions. Figure 3 shows high-level controllers for treatment design and treatment delivery. These are refined into more detailed control loops to be presented in Sec. 3.

The output of this part of the procedure is a model of the safety control structure, including more detailed individual control loops with associated control actions. Also to be identified at this stage is the process model and safety responsibilities for each controller.

As previously mentioned, the hierarchical control model is very different than a process map. A control model describes the overall function being performed, but there is no separation into sequential steps nor any specification of an ordering of the control actions. In some processes, control actions can be done in different orders without affecting the outcome of the process. If an order of actions is required, then it is implied in the control model where a specific input is required before the next action is taken. A process map specifies a procedure as a number of sequential steps and naturally limits flexibility in how process goals are achieved. In practice, steps in a process are often taken in a different order than what is specified in a process map, for a variety of good or bad reasons. The safety of the procedure should not be compromised by this reality.

2.E. Identify unsafe control actions (UCAs)

Hazards usually result from UCAs, for example, inadequate treatment provided to a patient, incorrect positioning of patients, or exposure of staff to radiation. The first step in the analysis (which is done on the model created in Sec. 2.D) is to identify what types of unsafe control actions can occur.

There are four possible types of unsafe control: (1) a control action not being provided can lead to a hazard, (2) a control action can be provided that leads to a hazard, (3) control actions can be provided at the wrong time or in the wrong order, and (4) a continuous control action can be stopped too soon or applied too long. Examples of each type of unsafe control are presented in Sec. 3.

Identifying the conditions under which control actions become unsafe is the first step in the analysis process. The next step is to determine how the identified conditions could occur and then eliminating those causes from the system or introducing controls to mitigate their impact if elimination is not possible.

The identified conditions under which control actions are unsafe can also be used to generate high-level safety requirements for the entire treatment system, including the safety requirements for regulation, management, treatment planning, and treatment delivery.

2.F. Determine how each unsafe control action could occur

Potential causes for UCAs are determined by identifying the ways in which each UCA might occur, that is, by creating causal scenarios for each UCA that was developed in Sec. 2.E. A causal scenario should include the context in which the UCA could occur. There is likely more than one scenario per UCA and includes things such as improperly performing equipment, process drifts or mistakes, and human cognitive biases. Besides identifying scenarios leading to unsafe control actions, one other type of unsafe behavior needs to be included in the causal analysis and that is when a safe control action is correctly issued but never executed. The causes here typically involve component failures.

While there is not yet any rigorously defined method for creating causal scenarios, there are templates and heuristics to help identify them. For example, they can be developed in part by considering the following potential causes: (i) the process model is incomplete or inconsistent (how could this occur?), (ii) flaws in the control algorithm, perhaps because the software or human was not informed about the complete requirements for the algorithm, (iii) delayed, missing, or incorrect process inputs or outputs including controller-to-controller communication problems, (iv) feedback that is delayed, missing, or wrong including measurement inaccuracies, (v) equipment or component failure or simply process drifts caused by changing human behavior over time as they get more familiar with the procedures and start to take short cuts, and (vi) unidentified or out-of-range process disturbances.

For this work, two members of the team brainstormed a list of ways that each UCA could occur. These were considered a list of initial causal scenarios. The initial scenarios were then checked by talking to a broader team of radiation oncologists, therapists, and physicists. Finally, the two team members went back to identify the context(s) that could lead to the initial scenarios.

2.G. Failure modes and effects analysis

A bullet point list outlining the new radiosurgery procedure was provided to the analysis team for developing the FMEA. The team was experienced in performing FMEA and also completely independent of the STPA analysis team. The methodology used to perform the FMEA was based on the streamlined approach of Ford *et al.*[11] The analysis was performed as follows:

1. Create a process map that describes the steps involved in the proposed treatment process.
2. For each step in the proposed treatment process, ask "What could go wrong?" The result of this is a series of failure modes. There could be multiple failure modes for each process step.
3. For each failure mode, ask "How could this have gone wrong?" The result of this is a number of causes for each failure mode. There could be multiple causes for each failure mode.
4. Determine the severity (S), probability of occurrence (O), and likelihood of detection (D) values for each failure mode/cause following TG-100 tables and calculate the risk priority number (RPN) for each failure mode/cause combination.
5. Use the risk priority number to rank the failure modes. Review the top failure modes (risk priority number $\geq$300).

The physicists described the proposed treatment process, and the facilitator (one of the physicists) created the process map that was distributed to the analysis group for review. The analysis group consisted of two physicists, one physics resident, two therapists, two dosimetrists, and one radiation oncologist. The list of top failure modes (i.e., those having a risk priority number $\geq$300) was distributed to the analysis team and individuals were asked to propose corrective actions for each failure mode/cause. The analysis team reconvened at a single in-person meeting to discuss and finalize the proposed corrective actions.

3. RESULTS

3.A. System description

Cranial stereotactic radiosurgery is now routinely performed in a minimally invasive or noninvasive (i.e., frameless) mode.[27] One method of frameless radiosurgery is to use an open mask with a real-time optical surface imaging and monitoring system.[28] Surface monitoring refers to the use of a structured light pattern that is projected on the surface of the patient and imaged using a three camera system and algorithm to determine a three dimensional surface map that is compared to a reference surface map. This system can be used to determine the translations and rotations of the patient relative to a reference surface map in real-time. This type of frameless radiosurgery treatment process involves a consultation with a radiation oncologist, acquisition of an MR scan for target delineation, acquisition of a treatment planning CT scan (CT simulation), treatment planning, and then the patient returns to the department for treatment. The patient makes three trips to the radiation oncology department (consultation, CT simulation, and treatment). Reducing the number of trips to the department would be helpful for patients and their families and would also free up time on the CT simulator. The proposal is to create a new Linac-based radiosurgery procedure that omits the CT simulation. Technology advancements have reached the point where this is now possible.

The proposed new procedure involves only two trips to the radiation oncology department and includes the following: consultation with the patient is performed as usual followed by an MR scan for target delineation. After the MR scan, the radiation oncologist delineates the target and critical structures and provides the prescription to the medical physicist. The medical physicist then creates a preplan based on the MR scan. Once the MR preplan is approved by the radiation oncologist, the patient is scheduled for treatment. Upon arrival to the department for treatment, the patient proceeds directly to the Linac room. Surface monitoring is initiated and a cone beam CT (CBCT) acquired. The MR and MR preplan are then fused to the CBCT, which indicates the patient's actual position relative to the isocenter. The final treatment plan is calculated on the CBCT (and reoptimized if necessary). The treatment is then immediately delivered to the patient.

In compressing the workflow, traditional safety checks may be removed or changed in nature, technological limits will be pushed, and new sources of time pressure and communication problems may be introduced. New software and immobilization technologies will be needed. All of these aspects indicate the need for a prospective hazard analysis that would guide the development of a new procedure such as this.

3.B. High-level accidents

After the system description, the list of high-level accidents (i.e., losses) was created. The list for radiation oncology is the following:

($A1$) The patient is injured or killed from overexposure or undertreatment.
($A2$) A nonpatient is injured or killed by radiation.
($A3$) Damage or loss of equipment.
($A4$) Physical injury to a patient or nonpatient during treatment.

These accidents were deemed as important to the system and serve as a focus for the analysis.

3.C. High-level hazards

A list of high-level hazards was created that could lead to the high-level accidents. The hazards relate to the accidents and frame the rest of the analysis. The list created is the following:

($H1$) Wrong dose: Dose delivered to patient is wrong in either amount, location, or timing ($A1$).
 ($H1.1$) Right patient, right dose, wrong location.
 ($H1.2$) Right patient, wrong dose, right location.
 ($H1.3$) Right patient, wrong dose, wrong location.
 ($H1.4$) Wrong patient.
($H2$) A nonpatient is unnecessarily exposed to radiation ($A2$).
($H3$) Equipment is subject to unnecessary stress ($A3$).
($H4$) Persons are subjected to nonradiological injury ($A4$).

3.D. Control loops and control actions

Figure 3 presents high-level control loops for a radiation oncology department. Regulatory is at the top and refers to any external bodies that the hospital, department, or vendor is required to satisfy such as the Joint Commission, the Food and Drug Administration, and the Nuclear Regulatory Commission. To scope the hazard analysis, it was deemed appropriate to include only hospital and department management, vendor

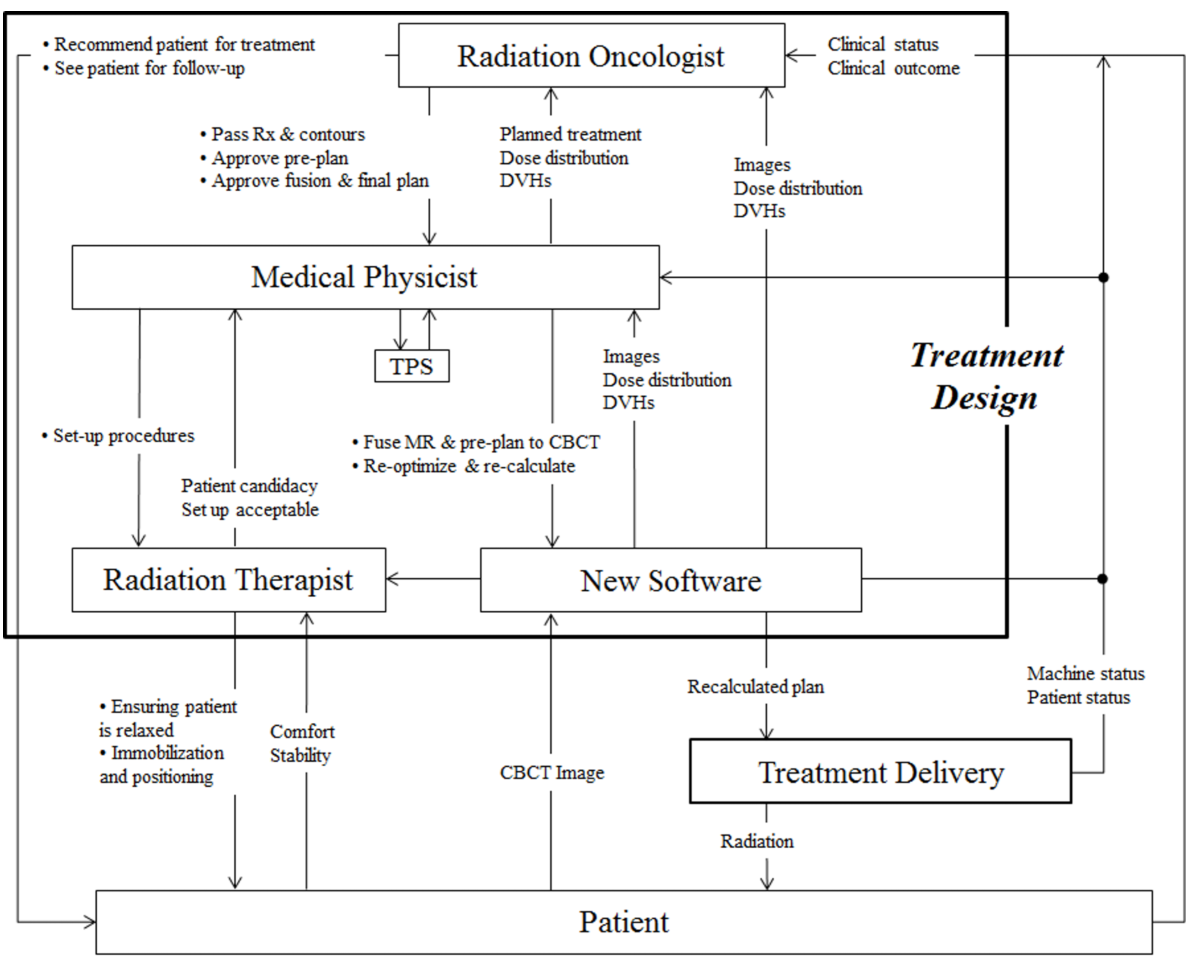

FIG. 4. Details of the treatment design controller of Fig. 3 (Rx = prescription, MRI = MR scan, CBCT = cone beam computed tomography, TPS = conventional treatment planning system).

service (not the vendor itself), and clinical operations in this study.

The clinical operations controller is divided into treatment design and treatment delivery controllers. The treatment design controller involves creating the general procedures and the treatment plan that will be eventually delivered to the patient. The process being modeled here is the development of the MR preplan for the patient, bringing the patient to the treatment room for positioning, and then creating a final optimized plan. The optimized plan is then sent to the treatment delivery controller so treatment can proceed. The analysis was focused on the controllers whose roles change in the new process and where a reasonable chance of affecting change is possible. For example, changing regulatory agencies or vendor equipment design is not likely to happen in the short term. Treatment design and treatment delivery controllers include the radiation oncologist, the medical physicist, and the radiation therapist as well as all of the equipment and software used in the new procedure. This includes both existing equipment and software as well as equipment and software that may need to be developed.

The high-level control loops (treatment design and treatment delivery) of Fig. 3 were refined to include more detail as shown in Fig. 4 and in the Appendix (Fig. 6). By using multiple levels of refinement, complex safety control structures can be more easily understood. In the remaining Sec. 3, the "Treatment Design" box of Fig. 3 is described and control action 4.1 (shown in Table I) is presented in detail, namely,

TABLE I. List of the controllers, job functions, safety responsibilities, and associated control actions as part of the STPA for the new Linac-based radiosurgery procedure.

Controller	Function performed	Safety responsibilities	Control actions
Radiation oncologist	The radiation oncologist uses his medical and specialty knowledge when evaluating the patient for treatment and uses the dose distribution, DVHs, and imaging for setup and optimal treatment plan	• Ensure that radiation, the Rx and contours are appropriate to treat the patient's disease • Verify that the final plan and patient setup are acceptable prior to treatment • Observe and manage any unexpected complications during and after treatment	• Pass prescription and contours • Approve preplan • Approve fusion and final plan • Recommend patient for treatment • See patient for follow-up
Medical physicist	The medical physicist uses his knowledge of treatment planning system, fusion algorithms, and imaging techniques to prepare treatment plans and evaluate patient setup	• Ensure that the plan (Linac instructions) is able to be delivered without error and that equipment is functioning properly • Verify that the treatment plan meets the radiation oncologist's Rx and has all the necessary information for the radiation therapist	• Set-up procedures • Fuse MR and preplan to CBCT • Reoptimize and calculation • Send new plan to RT EMR • Schedule for treatment
Radiation therapist	The radiation therapist uses his clinical experience and knowledge to interact with and position the patient per the setup protocol and execute treatment per the treatment plan	• Ensure the patient is comfortable and follows instructions for treatment • Ensure that the patient is setup per the treatment plan and procedures are followed as designed • Verify that the equipment is functioning properly during the treatment	• Ensuring patient is relaxed • Immobilization and positioning • Acquire CBCT • Mode up final plan • Initiate treatment • Halt treatment
Hospital administration	The hospital administrators set productivity goals for the department and use patient census, satisfaction surveys, and billing data from the department to evaluate department performance as well as provide staffing and equipment to achieve those goals	• Ensure that the department has sufficient resources to perform the treatments • Verify that the department has appropriate resources to meet performance goals	• Set performance expectations • Provide staff and equipment resources
Department administration	The department administrators use feedback from the staff and the incident learning system to understand needs to perform daily activities as well as set department culture	• Ensure that the treatment policy and procedures are documented and accessible • Ensure that appropriate resources are allocated for the procedure • Ensure that the department follows a safety culture	• Approve standard operating procedures • Allocate staff and equipment resources • Create and maintain department culture • Maintain equipment and procedures
Clinical operations team	The planning and treatment teams address anomalous equipment behavior in part by providing the vendor with feedback when faults or error messages arise	• Notify appropriate persons or vendor when anomalous equipment behavior is detected	• Staff notify vendor of an issue

the medical physicist control action to *fuse MR and preplan to CBCT*.

Figure 4 shows the detailed control structure of the Treatment Design box in Fig. 3. The control loops of Fig. 4 include the assessment of the patient to provide a recommendation for the use of radiation oncology to treat the patient's disease using the new radiosurgery procedure. Also included are the MR preplan and the modification to the preplan on the day of treatment including a dose calculation on the CBCT and possible reoptimization if the calculated dose distribution is not acceptable.

The medical physicist controller can provide five types of control actions. Prior to implementation of the new SRS procedure, the medical physicist leads a team to define the set-up procedures. The medical physicist uses the MR scan, the preplan, and the CBCT as process input and the first action is to fuse the MR scan and preplan to the CBCT. The medical physicist uses his process model, which includes clinical experience, to ensure the CBCT quality is acceptable and the patient is in an appropriate position. The second action is to reoptimize (if necessary) and calculate the dose distribution on the CBCT. The medical physicist also uses his knowledge of the software to perform and analyze the MR and preplan fusion to the CBCT and then to review the final dose calculation results by comparing them to the MR preplan. Based on the acceptability of this comparison, the medical physicist may initiate a reoptimization and subsequent dose calculation and repeat the review process. Once the medical physicist is comfortable with the treatment plan, the radiation oncologist will be notified to review the plan and use their clinical knowledge and experience to approve the final plan to treat the patient. The radiation oncologist will also be comparing the treatment plan to the MR preplan results and may require knowledge of how to use the fusion software.

3.E. Unsafe control actions (STPA step 1)

For the twenty three (23) control actions shown in Table I, there were 83 conditions under which the control actions could be unsafe. The UCAs for the medical physicist controller are shown in Table II. New software will be developed to perform the fusion (MR and preplan to the CBCT) and used to determine the quality of the fusion.

For the *set-up procedures* control action and *fuse MR and preplan to CBCT* actions, there is a UCA for each of the four possible unsafe conditions of the control action. For control action *Reoptimize and calculate*, there are four UCAs but none for the state of "given at the wrong time or wrong order" which

TABLE II. STPA step 1 table of UCAs for the *medical physicist controller* (see Figs. 3 and 6 in the Appendix).

Control action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Setup procedures	The SOPs are not communicated to the new radiation therapist when the radiation therapist changes linear accelerator coverage ($H1$, $H2$, $H5$)	The SOPs are incorrect or incorrectly communicated when the procedure is introduced into clinical use ($H1$, $H2$, $H5$) The SOPs do not get updated and/or communicated when there is a planned process modification ($H1$, $H2$, $H5$)	The CBCT-only SRS program is started before the SOPs are completed ($H1$, $H2$, $H5$)	The SOPs are finalized before getting input from all team members (radiation oncologists, medical physicists, radiation therapists, schedulers) ($H1$, $H2$, $H5$)
Fuse MR and preplan to CBCT	The medical physicist does not perform the fusion when the images (and MR preplan) are ready ($H1$)	The medical physicist fuses the images and MR preplan incorrectly when using the fusion software ($H1$)	The images are fused before the final or most recent CBCT is acquired and transferred for fusion ($H1$)	The fusion takes too long when transferring images or using the fusion software ($H1$)
Reoptimize and calculate	Suboptimal treatment occurs when a suboptimal MR pre-plan is scheduled for treatment ($H1$)	An inaccurate dose calculation is provided when the medical physicist uses the software to perform the calculation ($H1$)	N/A	Reoptimization or calculation takes too long when using the treatment planning software ($H1$) Reoptimization ends before completed after the medical physicist initiates the optimization ($H1$)
Send new plan to RT EMR		The wrong patient's final plan is sent to the Linac when the final plan has been approved by the radiation oncologist ($H1$)	The final plan is not available at the Linac when the patient is positioned correctly and ready for treatment ($H1$)	
Schedule for treatment	The medical physicist does not schedule the final plan for treatment when it is approved ($H1$)	The medical physicist schedules the final plan for treatment with too many or too few fractions when using the RT EMR scheduling software ($H1$)	The medical physicist takes too long to schedule the plan for treatment after it has been approved by the radiation oncologist ($H1$)	

is similar to the *schedule for treatment* control except it has only three UCAs. The *send new plan to RT EMR* control has UCAs for the control action given incorrectly and the control action given at the wrong time or wrong order. The remaining results are presented in the Appendix (Tables V–IX).

3.F. UCA causal scenarios (STPA step 2)

This step determined why the UCAs might occur, that is, the causal scenarios leading to those unsafe control actions. This information was used to generate design and operational requirements and controls to prevent the unsafe control actions. There were no assumptions made as to any existing controls such as pretreatment physics QA checks. This allowed for the new radiosurgery procedure to be evaluated for hazards without being encumbered by existing procedures, which may or may not be relevant.

For the 83 UCAs, there were 472 causal scenarios identified. As one example, some causal scenarios for the medical physicist's unsafe provision of the control action *fuse MR and preplan to CBCT* are the following:

Scenario 1. The CBCT scan does not get to the new software because the CBCT is not automatically stored correctly or sent to the new software and imported.

Scenario 2. The CBCT scan does not get to the new software because the person assigned to the task forgets to transfer, or otherwise process, the CBCT scan for the next step.

Scenario 3. The medical physicist is distracted by issues related to the case or otherwise preoccupied with other noncase related clinical issues and the case proceeds in a suboptimal way without the medical physicist's input because the radiation oncologist does the fusion without sufficient knowledge about how the new software works.

Scenario 4. The medical physicist does not know where to find the software or how to use it because there is inadequate training for the medical physicist on how to use the software.

Scenario 5. The medical physicist does not know where to find the software or how to use it because the medical physicist is new or not otherwise experienced and there is no sufficient competency assessment procedure.

Scenario 6. There is a software crash that the medical physicist cannot recover from because the error message is nonexistent or not helpful and the vendor software service is slow to respond with expert assistance. An assumption is made that if the software can be restarted again, then all future operations will be safe, which is not necessarily true.

To provide some context for the 472 causal scenarios generated by the STPA for the new radiosurgery procedure, the causal scenarios were mapped onto the causality table in Appendix D from the consensus recommendations for incident learning database structures in radiation oncology.[29] The breakdown of causality is provided in Table III and compared to those identified by the FMEA performed on the same system. The "other" causality category was largely related to issues of software use, case delays, or other general workflow related issues that did not fit in one of the other categories.

TABLE III. Causal scenarios were mapped onto the causality table in Appendix D from the consensus recommendations for incident learning database structures in radiation oncology (Ref. 29). The causal scenarios were grouped into the higher level categories found in Appendix D as shown in this table.

Causality category	STPA	FMEA
Organizational management	164 (35%)	8 (6%)
Technical	89 (19%)	31 (24%)
Human behavior of individual staff	68 (14%)	53 (40%)
Patient-related circumstances	20 (4%)	4 (3%)
External factors (beyond facility control)	0 (0%)	0 (0%)
Procedural issues	101 (21%)	36 (27%)
Other	30 (6%)	0 (0%)
Total	472 (100%)	132 (100%)

3.G. Failure modes and effects analysis

The process map developed by the group is shown in Fig. 5. It consists of 5 main process steps and 20 subprocesses and describes the process in sufficient detail to allow a focused analysis of each step in the process.

Overall, there were 132 failure modes/causes identified during the analysis. Table IV lists failure modes with risk priority numbers >300. These are indicated in Fig. 5 by the numbered ellipses. The numbers inside the ellipses correspond to the failure modes as listed in Table IV. Grouped into the main process steps, the number of failure modes were the following: *preconsultation* had 51 (39%), *consultation* had 7 (5%), *pretreatment in treatment room* had 25 (19%), *final treatment planning* had 32 (24%), and *treatment* had 17 (13%).

There were seven other failure modes for eight different steps with RPN = 300 ($S = 10$, $O = 3$, and $D = 10$). The *step*, *substep,* and failure mode for each is provided in the following list:

- *Pretreatment—in treatment room*
  - Surface imaging is used to set baseline patient position.
    - Baseline patient position set incorrectly.
- *Final treatment planning*
  - Fuse CBCT scan with pretreatment MR scan.
    - Incorrect fusion because the wrong algorithm was used or not checked.
  - Physicist reviews plan.
    - Passing the plan even though normal tissue doses were exceeded.
- *Treatment*
  - Confirm patient position using surface imaging.

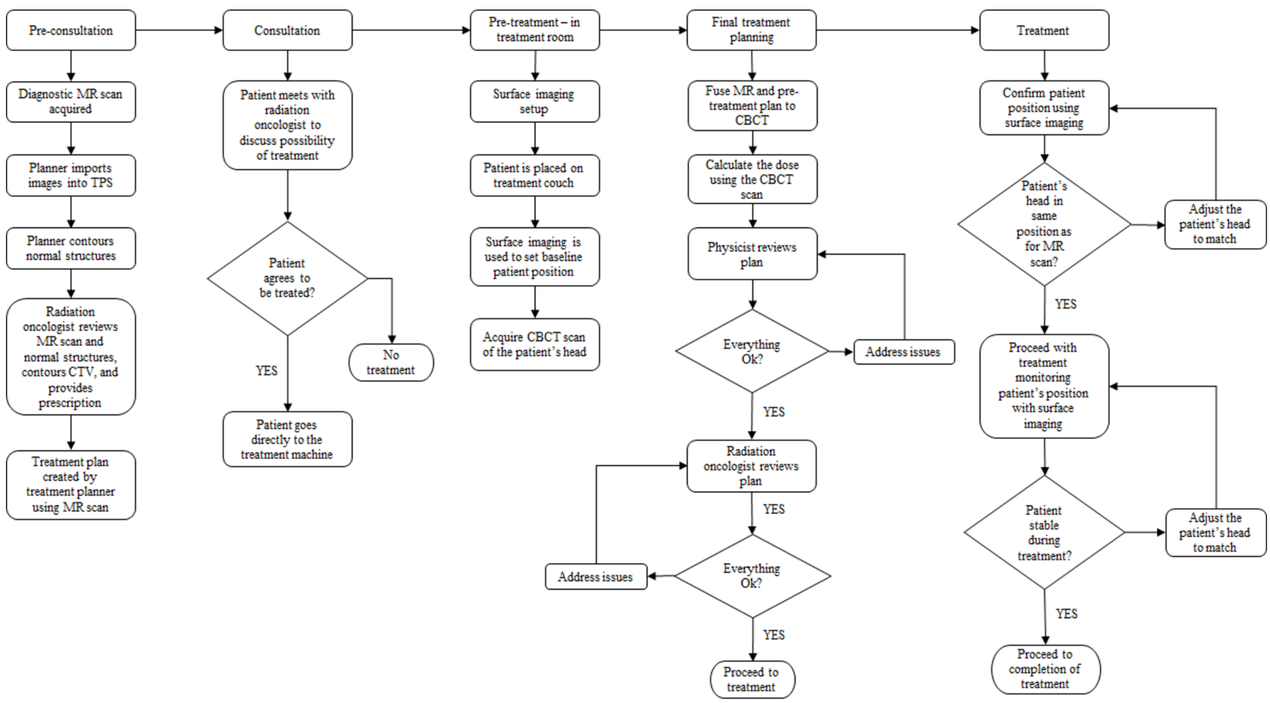

FIG. 5. Flowchart used for FMEA of the new radiosurgery procedure. The numbered ovals next to the process step are failure modes described in Table IV. The empty ovals next to the process step are for RPN = 300 and the failure modes are described in the text.

   * Patient positioned incorrectly because surface imaging system does not register motion.
- Adjust the patient's head to match CBCT.
   * Surface imaging indicates patient is correctly positioned when they are not.
- Use surface imaging to monitor head position during delivery
   * Patient's head motion is not correct from the surface imaging system.
   * Surface imaging indicates that the patient's head is out of alignment but the beam is not stopped.
- Patient stable during treatment?
   * Surface imaging indicates that the patient's head is out of alignment but the beam is not stopped.

The analysis team that performed the FMEA also mapped the failure modes onto the causality table[26] and the breakdown is shown in Table III. There were no external factors identified by either method as it was not explicitly included in the analyses.

4. DISCUSSION

In previous work, STPA has been applied to a medical device used in proton therapy[30] and other healthcare settings including radiation oncology.[31] The novel aspect of the current work is the application and assessment of STPA from the clinical perspective. The STPA for the new radiosurgery procedure resulted in six controllers, ten control loops, and 23 control actions. The safety responsibilities related to each controller are shown in Table I. Besides obvious equipment failures, frequently identified hazards were time pressures and communication issues. Other, perhaps nonobvious, recurring hazards were the lack of training and competency assessment as well as keeping the staff educated about the new procedure. Designing clinical tools such that normal workflow is facilitated rather than inhibited would be important to mitigate hazards. This was also realized early on in the analysis and to address time pressures and communication issues, new software should be created that facilitates many routine planning functions. The new software was built into the control loops as shown in Fig. 3 and was explicitly part of the hazard analysis.

Pursuing this work from a clinical perspective has highlighted some differences between FMEA and STPA. Even though both FMEA and STPA end up with causal scenarios, how one arrives at those causal scenarios is very different. Therefore, the two approaches should not be expected to give the same results. STPA facilitates a hazard analysis on a truly *de novo* treatment strategy because it does not require a strict definition of how it will be operationalized. FMEA can oversimplify human behavioral failure modes because after creating the process map, the analyst then determines what could go wrong at each step of the process. This is different from determining what are the unsafe interaction conditions of the people and equipment in a process. Nevertheless, there could be hazards that are not identified by either FMEA (reliability theory-based method) or STPA (systems theory-based method). The challenge is that there is no way of validating the completeness of any hazard analysis. Any such analysis is subject to the limitations of the analysts as well as things like time available. It is very possible that problems can still occur that were not identified or that the protection against the identified hazards is inadequate in practice.

TABLE IV. Failure modes and potential causes that result in risk priority numbers >300.

No.	Process step	Potential failure mode	Potential cause of failure mode	Effect of potential failure mode	*S*	*O*	*D*	RPN
1	Final treatment planning—fuse the CBCT scan with pretreatment MR scan	MR fused incorrectly to pretreatment CBCT	Registration error	Suboptimal dose distribution for the patient's anatomy	10	6	9	540
2	Preconsultation—radiation oncologist review and contour of MR scan	Target not contoured correctly	Previous treatment not accounted for	Patient receives an overdose to the normal tissues	10	6	8	480
3	Preconsultation—provides prescription	Incorrect prescription	Resident or secondary radiation oncologist enters incorrect prescription, not checked by the primary radiation oncologist	Patient receives a suboptimal dose to the target	10	6	8	480
4	Preconsultation—provides prescription	Incorrect prescription	Radiation oncologist does not have all the information and a previous treatment is not accounted for	Patient receives an overdose to the normal tissues	10	5	9	450
5	Preconsultation—provides prescription	Incorrect prescription	Radiation oncologist distracted and enters the wrong dose and/or number of fractions	Patient receives the wrong dose	10	5	8	400
6	Final treatment planning—radiation oncologist reviews plan	Plan passes review with errors	Radiation oncologist does not have all the information and a previous treatment is not accounted for	Patient receives the wrong dose	10	4	9	360
7	Preconsultation—radiation oncologist review and contour of MR scan	Normal structures approved but incorrect	Radiation oncologist trusted dosimetrist, did not carefully check structures	Patient receives an overdose to the normal tissues	8	5	8	320

There was some similarity in the FMEA and STPA results. Equipment failures or otherwise catastrophic errors were similar. These included things such as poor imaging, imaging or delivery systems not working, and incorrect use of equipment. There were also some human behavior issues identified with both approaches such as a covering radiation oncologist not being familiar with the patient or procedure. FMEA identified the potential for equipment collisions and several specific failures, e.g., all the ways that a physics plan check could miss something such as incorrect MUs, insufficient PTV coverage, incorrect energy, and suboptimal gradient index. As previously mentioned, hazards uniquely identified by STPA were the importance of competency training and assessment, various time pressures for different controllers, and workflow issues related to possible changes in the procedure over time. Some larger hazard categories identified as important in the STPA but not included in the FMEA were not seeing the patient in follow-up thus potentially missing subtle late effects that could indicate a problem with the new procedure, adequate communication with the vendor in expeditiously resolving equipment issues during the procedure, department administration effects, and hospital administration effects. Each of these resulted in its own control loop and a total of nine control actions. It is not obvious how effects of poor administration could be brought into an FMEA, which is reflected in the 6% of failure mode being included in the organization management category of Table III.

It is interesting to note that both analysis teams were given the same general goals of the new procedure but the FMEA team ultimately did not include new software to facilitate the proposed procedure even though it was contemplated during their meetings. In the FMEA version of the analysis, the procedure required a therapist to get the patient's head in the same position for treatment as was true for the MR scan. Therefore, a failure mode of "head position not reproducible—leads to difficulties performing registration" would not show up in the STPA version of the analysis because new software is assumed that would adapt the plan to the patient's current position as determined by CBCT. On the other hand, different failure modes/causes could have been identified had the FMEA team included new software in the analysis. However, this would require analyzing a process that is not well-defined and not suitable for the FMEA methodology. One last point on the comparison is that TG-100 recommends using both tools (in addition to process mapping). In this work, STPA was compared to FMEA rather than TG-100. However, it is noted that while FTA is a deductive approach and FMEA is an inductive approach, they cannot simply be thought of as complementary tools that when used together provide a complete analysis to cover all possible failure modes. Future work should include testing of multiple different hazard analysis tools such as HAZOP, ETA, and TG-100.

For the STPA, one of the unsafe control actions for the therapists is acquiring the CBCT after the patient has been lying on the table for a long time. This is clearly not a failure of the hardware, software, or human behavior and most likely would not cause any harm at all. In fact, it happens routinely in many clinics. But, this does put the system in an unsafe state and thus should be considered a hazard that needs to be mitigated. The unsafe control action "patient on the table for a long time before the CBCT" could also have been identified as a potential cause of a failure in FMEA but only if the analysis team identifies a specific failure mode that leads to this conclusion. At a high level, this scenario can be characterized as a failure but it would be an oversimplification to conclude that any single aspect of the process failed. Accidents can, and frequently, do happen as a result of system components interacting in a suboptimal way even though there has not been an explicit failure.

The hierarchical control structures developed in STPA can provide unique documentation of how a system operates, where the unsafe control actions (and scenarios) are linked to their associated hazards, thus lending traceability between the design specifications and hazards. Therefore, the STPA output can be used to develop a risk management plan as part of a comprehensive quality management strategy. Ultimately, the STPA causal scenarios generated from the identified unsafe control actions will be translated into design requirements or safety constraints. These requirements or constraints should prevent potentially dangerous interactions of the system components (people, processes, and equipment) if implemented in the system design. The exact methodology or format of the requirements may depend on who is receiving the recommendations. For example, formatting a list of constraints for internal departmental use may be significantly different than a list of requirements for a vendor's engineering team. The requirements can also serve as a bridge between the clinical workflow designers and other domain experts such as the software engineers and human design experts. Because some software and equipment do not yet exist to support this new treatment procedure described in this research, any associated risks found at this stage could be either designed out of the system or given proper controls.

It should be pointed out that nurses were not included in the current analysis even though nurses have important safety responsibilities for any radiation oncology treatment. This was a decision made by the STPA analysis team to scope the project. There was no evaluation done on how this might have affected the results. Similarly, it is not possible to comment on how the team size for the creation of causal scenarios (e.g., two individuals doing the majority of the brainstorming and being "checked" by a broader audience) or effort required affects the results. Even with the FMEA and STPA comparison, a study would need to be developed that is specifically designed to answer those questions, which is beyond the scope of this work. Efficiency, completeness, and ease of use may be a concern in selecting an analysis technique and this topic can be the subject of future work.

Finally, while only a single example of STPA for a clinical case is presented in this work, the STPA procedures are generalizable to all aspects of radiation oncology for analyzing both new processes as well as existing processes. For an existing process, the STPA steps would be the same. Since the process would already exist, the analysis might be more straightforward because the process would be better understood than would be for a new process. There would also be an even better knowledge of existing hazards.

5. CONCLUSION

All hazard models and risk assessment techniques are meant to provide a framework to characterize and identify potential sources of accidents that are not immediately obvious. As a clinical tool for prospective hazard analysis, STPA worked quite well but is a new way of thinking about the problem. The interaction of people, hardware, and software is highlighted through the STPA procedure in a way that is uniquely different from FMEA. STPA provides a hierarchical model for understanding the role of management decisions in impacting system safety so that a system design requirement can be traced back to the hazard and accident that it is intended to mitigate. Management decisions can also be straightforwardly included in the risk analysis. Further investigation of STPA is warranted for radiation oncology safety improvement and quality management.

ACKNOWLEDGMENT

This work was supported in part by a research grant from Varian Medical Systems to investigate Linac-based CBCT-only online cranial SRS/SRT treatments.

APPENDIX: CONTROL STRUCTURES AND STEP 1 TABLES

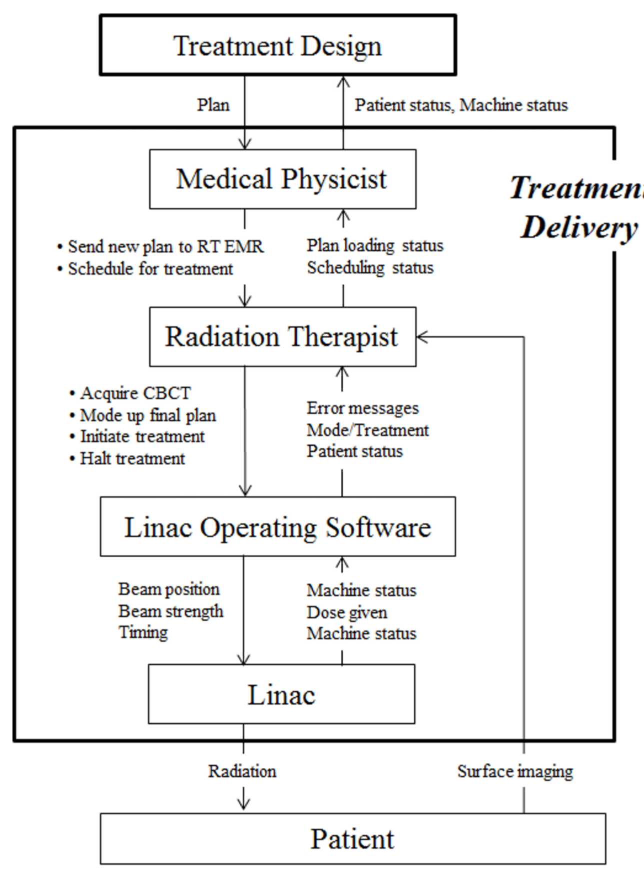

FIG. 6. Details of the treatment delivery controller of Fig. 3.

Table V. STPA step 1 table of UCAs for the radiation oncologist controller (see Figs. 4 and 6).

Control action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Pass Rx and contours		The radiation oncologist approves the prescription and contours when one or both are suboptimal ($H1.1$–3) The radiation oncologist approves the prescription and contours when it was intended for another patient ($H1.4$)	The medical physicist creates the MR preplan before the final prescription and contours are passed along and are changed upon finalizing by the radiation oncologist ($H1.1$–3)	
Approve MR pre-plan	The patient gets treated even though the radiation oncologist did not approve the MR preplan ($H1$)	The radiation oncologist approves the MR preplan when the preplan is suboptimal ($H1.1$–3) The radiation oncologist approves an optimal MR preplan when it was intended for a different patient ($H1.4$)	The radiation oncologist approves the MR preplan before MR preplan is complete ($H1$) The radiation oncologist is delayed in approving the MR preplan when the MR preplan is ready for review ($H1$)	
Approve fusion and final plan	The fusion and final plan is not checked by the radiation oncologist when either one or both is suboptimal ($H1$)	The radiation oncologist approves the fusion and final plan when either one or both is suboptimal ($H1$)	The fusion and or final plan is approved after the plan has been scheduled for treatment ($H1$) The radiation oncologist approves a fusion and or plan before the final plan is completed ($H1$)	The fusion and final plan approval is delayed when they are ready to be checked ($H1$)
Recommend patient for treatment		The radiation oncologist recommends the patient for the new procedure when they are not a suitable case ($H1$)	The radiation oncologist recommends the patient for the new procedure when the new procedure is not available ($H1$)	
See patient in follow-up	The radiation oncologist does not see the patient after the treatment has been delivered ($H1$)	The radiation oncologist incorrectly assesses the complications after treatment ($H1$)	The radiation oncologist sees the patient in follow-up too soon after treatment ($H1$) The radiation oncologist sees the patient in follow-up too long after treatment ($H1$)	The follow up visit is hurried and the radiation oncologist does not notice a complication that is related to the new procedure ($H1$)

TABLE VI. STPA step 1 table of UCAs for the *radiation therapist controller* (see Figs. 4 and 6).

Control Action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Ensuring patient is relaxed	The radiation therapist does not ensure candidacy of patient when the patient is actually non-ideal for this treatment ($H1.1$ and $H2$)	A junior or otherwise inexperienced radiation therapist incorrectly identifies the patient status when meeting the patient ($H1.1$ and $H2$)	The radiation therapist assesses patient's comfort with treatment (i.e., ability to hold still) after the patient is already on table and immobilized making stopping less likely if the patient is not ideal ($H1.1$ and $H2$)	
Immobilization and positioning	The radiation therapist does not reposition or immobilize when the patient is not securely positioned ($H1$)	The radiation therapist does not position the patient per the SOP when setting up the patient for treatment ($H1.1$ and $H2$)	The radiation therapist takes a long time to position the patient when setting up the patient for treatment ($H1.1$ and $H2$)	
Acquire CBCT	The radiation therapist does not acquire the CBCT when the patient is positioned on the treatment table ($H1.1$–3)	The radiation therapist acquires the CBCT when the patient is not in the correct position ($H1.1$–3) The radiation therapist acquires the CBCT with the wrong scan parameters ($H1$)	The radiation therapist acquires the CBCT too quickly when the patient is not relaxed ($H1.1$–3) The radiation therapist acquires the CBCT after the patient has been lying on the table for a long time ($H1.1$–3)	
Mode up final plan for treatment	The radiation therapist does not mode up the final plan for treatment when it is ready ($H1$)	The radiation therapist modes up the wrong plan for treatment when working at the treatment console ($H1$)	The radiation therapist modes up the final plan for treatment before it is approved or scheduled ($H1$) The radiation therapist takes too long to mode up the final plan for treatment when working at the treatment console ($H1$)	
Initiate treatment		The wrong plan is delivered to the patient when the treatment is initiated ($H1$) The final plan is incorrect in some parameter(s) when the treatment is initiated ($H1.1$–3) There is a problem with the Linac when the treatment is started (or restarted) ($H1$)	The treatment is initiated before it is appropriate to give the signal to start treatment ($H1.1$–3) The start of treatment is delayed after the signal is given to start treatment ($H1.1$–3) The treatment is appropriately ready to proceed but the signal to start is not given ($H1.1$–3)	
Halt treatment	The therapist does not halt the treatment when it is indicated to do so ($H1.1$–3)	The therapist halts the treatment when the best course of action is to allow the treatment to continue ($H1.1$–3)		The therapist halts the treatment for a long time when it can be safely resumed ($H1.1$–3)

TABLE VII. STPA step 1 table of UCAs for the *hospital administration controller* (see Fig. 7).

Control Action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Set performance expectations (financial and safety)	Hospital administration does not provide safety and financial expectations for the department when planning new procedures ($H3$ and $H4$)	Hospital administration provides conflicting safety and financial expectations when the expectations are requested ($H1$, $H3$, and $H4$)		
Provide staff and equipment resources	Hospital administration does not provide staff and equipment resources when they are requested ($H3$ and $H4$)	Hospital administration provides staff and equipment resources at an inadequate level when they are requested ($H1$, $H3$, and $H4$)	Hospital administration takes too long to provide the requested staff and equipment resources when they are requested ($H1$, $H3$, and $H4$)	

TABLE VIII. STPA step 1 table of UCAs for the *department administration controller* (see Fig. 7).

Control Action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Approve standard operating procedures	Department administration does not approve the SOPs when a new procedure is started ($H1$–$H4$)	SOPs are approved when they are incorrect or incomplete ($H1$–$H4$)	SOPs are approved after the procedure has been clinically implemented ($H1$–$H4$)	
Allocate staff and equipment resources	Department administration does not allocate additional staff or equipment when a new procedure is created and additional staff are needed ($H1$–$H4$)	Department administration underestimates the resources needed when starting and maintaining a new procedure ($H1$–$H4$)	Department administration considers allocating resources after the new procedure has started ($H1$–$H4$)	Department administration stops the process of requesting resources for the new procedure when working with the hospital ($H1$–$H4$)
Create and maintain department culture	Department administration does not emphasize a safety culture when starting a new procedure ($H1$–$H4$)	Department administration does not set culture correctly or completely when starting a new procedure ($H1$–$H4$)	Department administration promotes a safety culture after the new procedure has already started ($H1$–$H4$)	Department administration stops promoting the safety culture after the new procedure has been working successfully for a while ($H1$–$H4$)
Maintain equipment and procedures	Department administration does not maintain equipment when a new procedure is used ($H1$–$H4$)	Department administration undermaintains the equipment with inadequate service contract ($H2$–$H4$)		Department administration lets the service contracts lapse when assessing recurring department needs ($H2$–$H4$)

TABLE IX. STPA step 1 table of UCAs for the *clinical operations team controller* (see Fig. 7).

Control action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Staff notifies vendor of an issue	The staff does not notify the vendor of an issue when the equipment is not functioning properly ($H1$–$H4$)	The staff incorrectly notifies the vendor when an issue arises ($H1$–$H4$)		

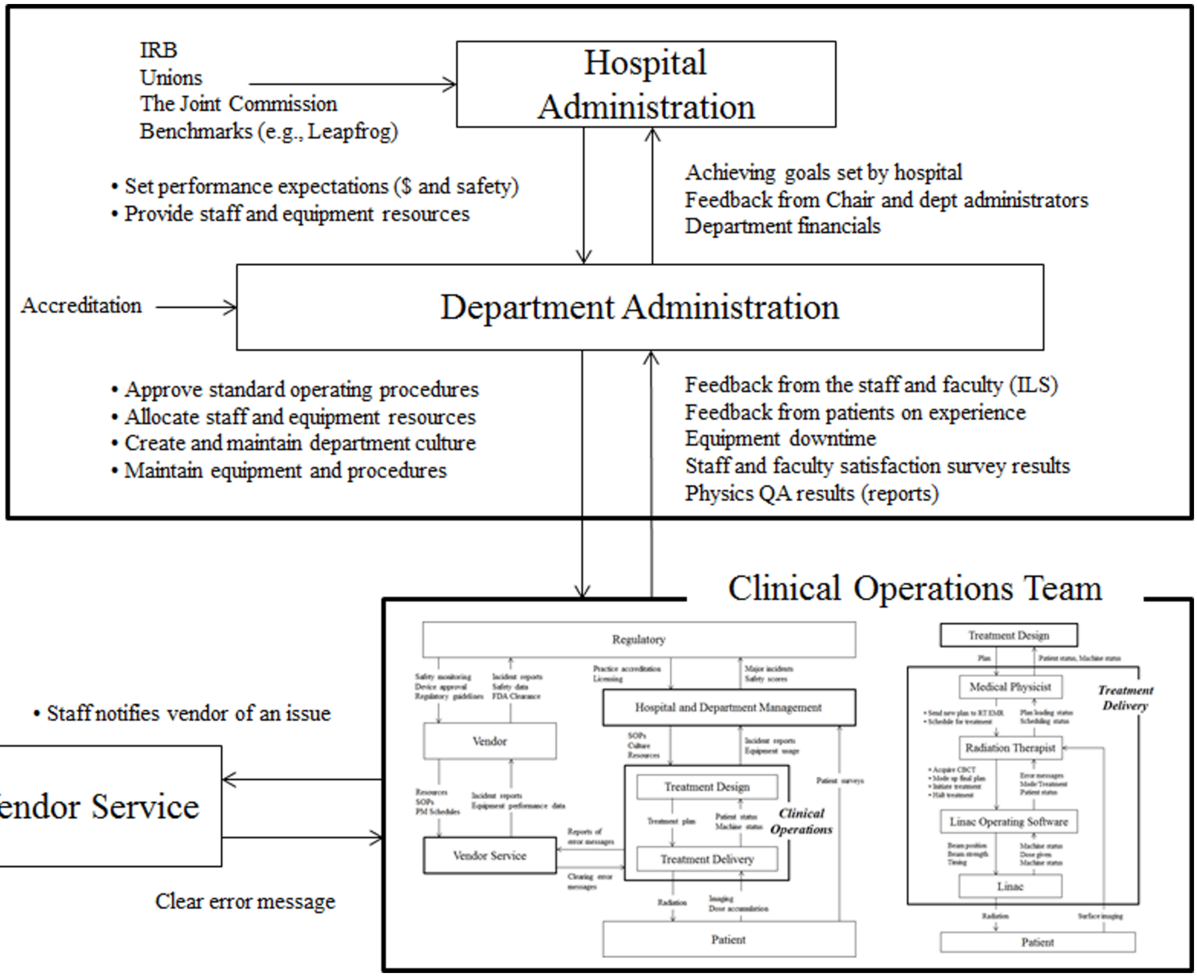

FIG. 7. Details of the hospital and department administration controllers as well as the vendor service controller.

[a]Author to whom correspondence should be addressed. Electronic mail: tpaw@ucsd.edu; Telephone: 858-822-6058; Fax: 858-822-6078.

[1]L. B. Marks, K. L. Light, J. L. Hubbs, D. L. Georgas, E. L. Jones, M. C. Wright, C. G. Willett, and F. F. Yin, "The impact of advanced technologies on treatment deviations in radiation treatment delivery," Int. J. Radiat. Oncol., Biol., Phys. **69**(5), 1579–1586 (2007).

[2]N. G. Leveson and C. S. Turner, "An investigation of the Therac-25 accidents," IEEE Transactions on Computers **26**(7), 19–41 (1993).

[3]W. Bogdanich, Radiation Offers New Cures, Ways to Do Harm, The New York Times, 24 January 2010, http://www.nytimes.com/2010/01/24/health/24radiation.html.

[4]B. Thomadsen, D. Brown, E. Ford, S. M. Huq, and F. Rath, "Risk assessment using the TG-100 methodology," in *Quality and Safety in Radiotherapy: Learning the New Approaches in Task Group 100 and Beyond*, edited by B. Thomadsen, P. Dunscombe, E. Ford, S. Huq, T. Pawlicki, and S. Sutlief (Medical Physics Monograph, Madison, WI, 2013), pp. 95–112.

[5]B. Thomadsen, S. W. Lin, P. Lammrich, T. Waller, A. Cheng, B. Caldwell, R. Rankin, and J. Stitt, "Analysis of treatment delivery errors in brachytherapy using formal risk analysis techniques," Int. J. Radiat. Oncol., Biol., Phys. **57**(5), 1492–1508 (2003).

[6]E. C. Ford, R. Gaudette, L. Myers, B. Vanderver, L. Engineer, R. Zellars, D. Y. Song, J. Wong, and T. L. DeWeese, "Evaluation of safety in a radiation oncology setting using failure modes and effects analysis," Int. J. Radiat. Oncol., Biol., Phys. **74**(3), 852–858 (2009).

[7]M. Ciocca, M. C. Cantone, I. Veronese, F. Cattani, G. Pedroli, S. Molinelli, V. Vitolo, and R. Orecchia, "Application of failure mode and effects analysis to intraoperative radiation therapy using mobile electron linear accelerators," Int. J. Radiat. Oncol., Biol., Phys. **82**(2), e305–e311 (2012).

[8]J. R. Perks, S. Stanic, R. L. Stern, B. Henk, M. S. Nelson, R. D. Harse, M. Mathai, J. A. Purdy, R. K. Valicenti, A. D. Siefkin, and A. M. Chen, "Failure mode and effect analysis for delivery of lung stereotactic body radiation therapy," Int. J. Radiat. Oncol., Biol., Phys. **83**(4), 1324–1329 (2012).

[9]A. Kapur, G. Goode, C. Riehl, P. Zuvic, S. Joseph, N. Adair, M. Interrante, B. Bloom, L. Lee, R. Sharma, A. Sharma, J. Antone, A. Riegel, L. Vijeh, H. Zhang, Y. Cao, C. Morgenstern, E. Montchal, B. Cox, and L. Potters, "Incident learning and failure-mode-and-effects-analysis guided safety initiatives in radiation medicine," Front Oncol. **3**, 305 (2013).

[10]D. S. Denny, D. K. Allen, N. Worthington, and D. Gupta, "The use of failure mode and effect analysis in a radiation oncology setting: The Cancer Treatment Centers of America Experience," J. Healthcare Qual. **36**(1), 18–28 (2014).

[11]E. C. Ford, K. Smith, S. Terezakis, V. Croog, S. Gollamudi, I. Gage, J. Keck, T. DeWeese, and G. Sibley, "A streamlined failure mode and effects analysis," Med Phys. **41**(6), 061709 (6pp.) (2014).

[12]L. Masini, L. Donis, G. Loi, E. Mones, E. Molina, C. Bolchini, and M. Krengli, "Application of failure mode and effects analysis to intracranial stereotactic radiation surgery by linear accelerator," Pract. Radiat. Oncol. **4**(6), 392–397 (2014).

[13]J. López-Tarjuelo, A. Bouché-Babiloni, A. Santos-Serra, V. Morillo-Macías, F. A. Calvo, Y. Kubyshin, and C. Ferrer-Albiach, "Failure mode and effect analysis oriented to risk-reduction interventions in intraoperative electron radiation therapy: The specific impact of patient transportation, automation, and treatment planning availability," Radiother. Oncol. **113**(2), 283–289 (2014).

[14]R. T. Jones, L. Handsfield, P. W. Read, D. D. Wilson, R. Van Ausdal, D. J. Schlesinger, J. V. Siebers, and Q. Chen, "Safety and feasibility of STAT

RAD: Improvement of a novel rapid tomotherapy-based radiation therapy workflow by failure mode and effects analysis," Pract. Radiat. Oncol. **5**(2), 106–112 (2015).

[15]R. Manger, A. Paxton, T. Pawlicki, and G.-Y. Kim, "Failure mode and effect analysis and fault tree analysis of surface image guided cranial radiosurgery," Med. Phys. **42**(5), 2449–2461 (2015).

[16]N. A. Shebl, B. D. Franklin, and N. Barber, "Is failure mode and effect analysis (FMEA) reliable?," J. Patient Saf. **9**, 86–94 (2009).

[17]N. A. Shebl, B. D. Franklin, and N. Barber, "Failure mode and effects analysis output: Are they valid?," BMC Health Serv. Res. **12**(1), 150 (2012).

[18]F. Yang, N. Cao, L. Young, J. Howard, W. Logan, T. Arbuckle, P. Sponseller, T. Korssjoen, J. Meyer, and E. Ford, "Validating FMEA output against incident learning data: A study in stereotactic body radiation therapy," Med. Phys. **42**(6), 2777–2785 (2015).

[19]W. Edwards, "Dynamic decision theory and probabilistic information processings human factors," J. Human Factors and Ergonomics Society **4**, 59–74 (1962).

[20]N. Leveson, "A new accident model for engineering safer systems," Saf. Sci. **42**, 237–270 (2004).

[21]N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety* (MIT, Boston, MA, 2012).

[22]W. R. Ashby, *An Introduction to Cybernetics* (Chapman and Hall, London, 1956).

[23]P. Checkland, *Systems Thinking, Systems Practice* (John Wiley & Sons, Hoboken, NJ, 1981).

[24]P. W. Murrill, *Fundamentals of Process Control Theory*, 3rd ed. (Instrument Society of America, Research Triangle Park, NC, 2000).

[25]D. Ariely, *Predictably Irrational* (Harper Collins, New York, NY, 2008).

[26]D. Kahneman, *Thinking, Fast and Slow* (Farrar, Straus, and Giroux, New York, NY, 2011).

[27]A. W. Lightstone, S. H. Benedict, F. J. Bova, T. D. Solberg, and R. L. Stern, "Intracranial stereotactic positioning systems: Report of the American Association of Physicists in Medicine Radiation Therapy Committee Task Group No. 68," Med. Phys. **32**(7), 2380–2398 (2005).

[28]H. Pan, L. I. Cerviño, T. Pawlicki, S. B. Jiang, J. Alksne, N. Detorie, M. Russell, B. S. Carter, K. T. Murphy, A. J. Mundt, C. Chen, and J. D. Lawson, "Frameless, real-time, surface imaging-guided radiosurgery: Clinical outcomes for brain metastases," Neurosurgery **71**, 844–852 (2012).

[29]E. C. Ford, L. Fong de Los Santos, T. Pawlicki, S. Sutlief, and P. Dunscombe, "Consensus recommendations for incident learning database structures in radiation oncology," Med. Phys. **39**(12), 7272–7290 (2012).

[30]B. Antoine, "Systems theoretic hazard analysis (STPA) applied to the risk review of complex systems: An example from the medical device industry," Ph.D. thesis, Engineering Systems Division, Massachusetts Institute of Technology, Boston, MA, 2013.

[31]A. Samost, "A systems approach to patient safety: Preventing and predicting medical accidents using systems theory," M.S. thesis, Engineering Systems Division, Massachusetts Institute of Technology, Boston, MA, 2015.