Safety Science 122 (2020) 104519

Contents lists available at ScienceDirect

Safety Science

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

Using a systems-theoretic approach to analyze safety in radiation therapy-first steps and lessons learned

Natalia Silvis-Cividjian[a,*], Wilko Verbakel[b], Marjan Admiraal[c]

[a] Computer Science Department, Faculty of Science, Vrije Universiteit, de Boelelaan 1081, 1081HV Amsterdam, The Netherlands
[b] Department of Radiation Oncology, Cancer Center Amsterdam, Amsterdam UMC, Location Vrije Universiteit Medisch Centrum (VUmc), De Boelelaan 1117, 1081 HV Amsterdam, The Netherlands
[c] Department of Radiation Oncology, Amsterdam UMC, Location Vrije Universiteit Medisch Centrum (VUmc), De Boelelaan 1117, 1081 HV Amsterdam, The Netherlands

ARTICLE INFO

Keywords:
Hazard analysis
Radiation oncology
IMRT
Systems-theoretic accident model
STAMP
STPA
HFMEA

ABSTRACT

Radiation therapy is an important technique to treat cancer. Due to the high occupational risks involved, the process is subject to severe safety regulations and standards. However, these standards do not mandate the usage of a particular hazard analysis method. The *de facto* methods currently used are the reliability theory-based Fault Tree Analysis (FTA) and Healthcare Failure Mode and Effects Analysis (HFMEA). Systems Theoretic Process Analysis (STPA) is a new, essentially different hazard analysis method, based on systems theory. Although successfully applied in many industries, there are only a few reports on STPA implementation in radiation therapy.

This paper contributes to filling this gap with a preliminary assessment of STPA applied to a mature Intensity Modulated Radiation Therapy (IMRT) process. The analysis was conducted by a team consisting of two experts in radiation therapy and one software systems engineer, with little domain knowledge. 142 potentially unsafe control actions were identified and compared with the results of an earlier HFMEA. The main lesson we have learned is that a graphical, system-wise modeling of the analyzed process, although challenging for beginners, is a powerful instrument to catch the same and even other, new hazards. A causal analysis of a subset of these newly found hazards has led to meaningful and valuable risk mitigation measures. These results suggest considering STPA as a viable option for safety analysis in radiation therapy. We expect that this top-down, well-structured way of analysis can especially be advantageous for safety assessment in early design phases, when an HFMEA is not possible yet, because most of system's implementation and behavior is still unknown.

1. Introduction

Radiation therapy, or simply radiation therapy (RT), is an important medical technique that uses ionizing radiation to treat cancer. Due to occupational risks that come along (Ford and Evans, 2018), demonstrated by a few notorious accidents (Leveson and Turner, 1993) (Borras, 2006), RT processes and products are regulated by severe safety standards and procedures (International Atomic Energy Agency, 2014). For example, all the hardware equipment involved needs to regularly undergo quality assurance (QA) procedures, and proofs of the process risk assessment must be provided in order to obtain permission to proceed (Pawlicki et al., 2011; Huq et al., 2016). The problem is that current RT safety standards do not enforce any particular safety assessment method to use. Highly recommended and widely used in this field is the Healthcare Failure Mode and Effects Analysis (HFMEA) method (Olch, 2014; Huq et al., 2016; DeRosier, 2002). FMEA (Arnzen, 1966) is a bottom-up hazard analysis method that in essence estimates, using probability theory, the effects of each component's malfunctioning (failure mode). The question asked for each component is "How often would this component fail, and what will happen *if* it fails? Subsequently, mitigation measures are formulated for the failure modes with the highest estimated risk. The method is successful when analyzing hardware failures, but has difficulties to estimate the probability of failure in case of human operators or the very ubiquitous modern software. The System Theoretic Accident Modeling Process (STAMP) (Leveson, 2012) is a different attempt to approach safety, based on systems- and control theory, instead of the traditional reliability theory. The novelty consists in modeling any process as a *system*, in which controllers interact with controlled processes in terms of control actions and feedback, as illustrated in Fig. 1.

In this holistic view, safety becomes an emerging system property, guarded by safety constraints. As a result, accidents are caused not by

[*] Corresponding author.
E-mail address: n.silvis-cividjian@vu.nl (N. Silvis-Cividjian).

https://doi.org/10.1016/j.ssci.2019.104519
Received 12 July 2018; Received in revised form 12 July 2019; Accepted 8 October 2019

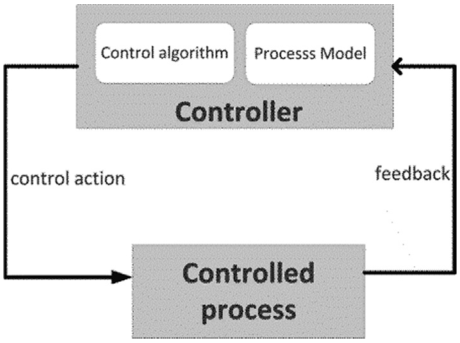

Fig. 1. A generic control structure used in STAMP to graphically model a system. The controller is positioned above the controlled process. Control actions are modelled using up-down arrows, while feedback is modelled using down-up arrows.

individual hardware-, software- or human component faults, but by *control* flaws, be they safety constraints violations, or simply a lack of these constraints' enforcement.

STAMP promises to better understand modern accidents causality and to discover interesting system hazards, using tools such as Systems Theoretic Process Analysis (STPA), and Causal Analysis based on STamp (CAST). This promise is substantiated by an increasing number of published reports, showing positive STAMP experiences in a variety of industries (Ishimatsu et al., 2014), (Alemzadeh et al., 2015), (Allison et al., 2017), (Kwon and Leveson, 2017), (Abdulkhaleq et al., 2017).

Radiation therapy is a process practiced in a complex socio-technical system, and therefore very suitable to be analyzed using STAMP. However, except for a few examples, (Pawlicki et al., 2016) and (Blandine, 2013), evaluation experiments of using STAMP in RT are rare.

We report on a small-scale research, conducted at the VUmc academic hospital in Amsterdam that contributes to the meager STPA-RT body of knowledge. We analyzed the safety of a mature Intensity Modulated Radiation Therapy (IMRT) process, and we compared, where possible, the STPA outcomes with the results of a recent HFMEA. Two research questions needed to be answered, typical to experiments that investigate the capabilities of a new hazard analysis technique.

RQ1. What characterizes the STPA analysis when conducted in a radiation therapy department?

RQ2. Does STPA bring any added value in radiation therapy, compared to HFMEA?

This paper is a report of our journey, which started with the necessary skepticism, passed through the typical STPA critical moments, and eventually resulted in a new insight into the applicability of a systems- theoretic approach to RT safety analysis.

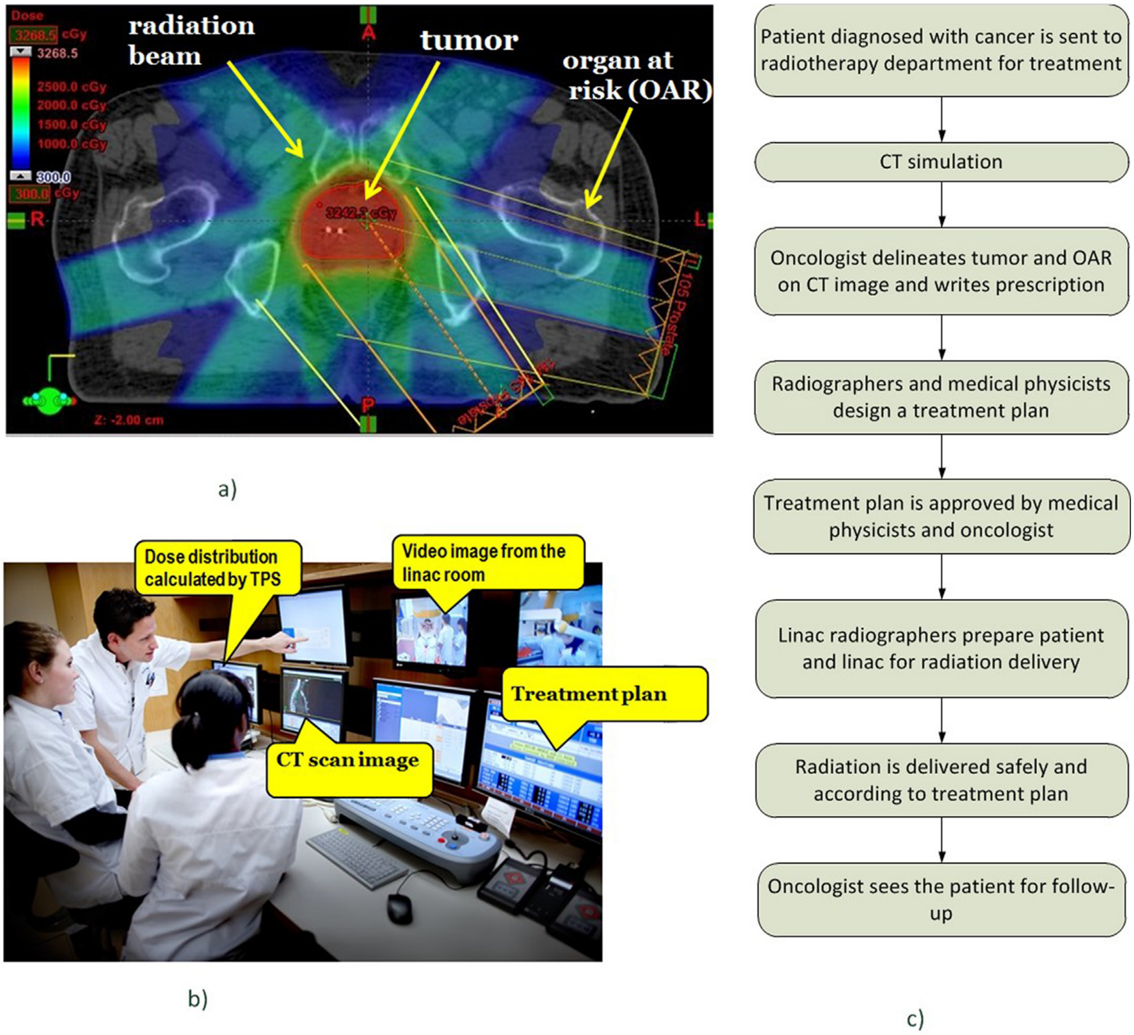
Dose
3268.5 cGy
3268.5
2500.0 cGy
2000.0 cGy
1500.0 cGy
1000.0 cGy
300.0
300.0 cGy
radiation beam
tumor
organ at risk (OAR)
A
R
L
P
3242.3 cGy
Z: -2.00 cm
a)
Dose distribution calculated by TPS
Video image from the linac room
Treatment plan
CT scan image
b)
Patient diagnosed with cancer is sent to radiotherapy department for treatment
CT simulation
Oncologist delineates tumor and OAR on CT image and writes prescription
Radiographers and medical physicists design a treatment plan
Treatment plan is approved by medical physicists and oncologist
Linac radiographers prepare patient and linac for radiation delivery
Radiation is delivered safely and according to treatment plan
Oncologist sees the patient for follow-up
c)

Fig. 2. (a) The IMRT geometry of exposure. Red colour indicates a high dose in the tumor, blue indicates a low dose in OAR (Based on: http://acfro.com/what-to-expect-during-your-treatment/radiation-therapy-imrtigrt-oncology-physicial-therapy/). (b) Illustration of an IMRT treatment delivery team at work. (c) The IMRT process workflow.

The remainder of the paper is organized as follows. Section 2 describes the analyzed IMRT process. Section 3 describes the STPA-IMRT experiment and elaborates on some dilemmas which any beginner is expected to encounter in a similar quest. Section 4 summarizes and discusses our findings and lessons learned. Finally, Section 5 outlines our conclusions and future work.

2. Intensity Modulated radiation therapy (IMRT)

About 40% of world population will be diagnosed with cancer at some point during their lifetimes (IKNL Integraal Kankercentrum, 2017). The disease manifests through a local uncontrolled growth of abnormal cells that result in a tumor, which can often spread to the rest of the body. If malignant and not treated, this will eventually contribute to a patient's death. Typical medical treatments aim to reduce or eliminate malignant tumors by means of chemotherapy, surgery and/or radiation therapy. *Intensity Modulated Radiation Therapy* (IMRT) is a form of high-precision radiation therapy, aiming to apply a maximal dose in the tumor, while protecting surrounding healthy organs (lungs, eyes, heart), called *organs at risk* (OAR) (see Fig. 2a). Nowadays, the treatment often takes place in a computer-controlled linear accelerator (linac) that rotates its gantry around the immobilized patient, while targeting the tumor with multiple beams, coming from many directions (Verbakel et al., 2009; Otto, 2008) (Veldeman et al., 2008). The beams' shape and position are modulated by a multi-leaf collimator (MLC) during the gantry rotation.

The IMRT process, in the form of a Volumetric Modulated Arc Therapy (VMAT) treatment workflow, can be described as follows (see Fig. 2b and c). After the patient is seen by the radiation oncologist, a fixation is made, if needed, followed by a CT-scan taken in treatment position. A radiation oncologist delineates the tumor(s) and OAR on CT-scan images. Next, the oncologist specifies clinical parameters, such as desired dose in the tumor and dose limits to OAR, summarized in a prescription, called *physician intent (PI)*. Based on this PI, the treatment design team of radiographers and medical physicists, by using inverse planning, devises a *treatment plan* that specifies how the radiation beams are positioned and shaped, during the rotation of the gantry around the patient. Basically, a planning radiographer runs an (usually iterative) process of (1) virtually positioning the gantry collimators relatively to the tumor and OAR contours, and (2) calculating the resulted doses using a computer program, called Treatment Planning System (TPS). This optimization process stops when the dose distributions in both tumor and OAR match the values required in PI. The resulted treatment plan is peer-reviewed, approved, and sent further to the treatment delivery team. The treatment plan delivery is usually fractionated, meaning that the total dose is delivered in multiple fractions, using a treatment device. During each session, a team of radiographers prepares the patient for treatment, acquires 2D or 3D kV images for accurate positioning and operates the linac, to deliver the planned radiation treatment. During the radiation dose delivery, the patient is monitored by video cameras. Along the course of treatment, the oncologist regularly sees the patient for follow-up. All the RT-related patient digital information (CT-, X-ray and MRI- images, PI, treatment plan and technical parameters of radiation delivery) are stored in a shared oncologic information database.

3. STPA applied to the IMRT process

3.1. The STPA methodology

STPA is a new hazard analysis method aiming to identify all possible hazardous situations and craft measures to prevent them from happening. The final goal is to create a safer system or process.

STPA starts with Step 0, in which the analyst must identify the goals of the analysis, by first determining what kinds of high-level accidents the stakeholders wish to prevent and defining the high-level hazardous states that could lead to those accidents. Based on the input from the domain experts, the analyzed process then needs to be graphically modeled using hierarchical safety control structures. STPA modeling uses a top-down approach. It starts with a high-level control structure, and works its way down, by adding new controllers and controlled processes.

As soon as the level of detail is considered sufficient, Step1 can start that identifies all the possible hazards. In STPA, a hazard is considered to be an unsafe control action (UCA) or a safe control action that was correctly given, but has never been executed.

The STPA methodology offers a very systematic way to find all possible hazards, divided in five categories: (1) Control action not given, (2) An incorrect control action is given, (3) Control action was given at the wrong time (too soon, too late), (4) The control action was given with a wrong duration (too long, too short) and (5) Control action was given, but has not been executed.

The result of Step1 is a list of hazards that may need to be further prioritized. Prioritization is a very sensible step, that requires a lot of domain knowledge, with serious consequences in case important hazards are inadequately discarded.

Step 2 follows, where for each possible hazard, the STPA team brainstorms to craft causal scenarios. The question that has to be answered here is: "How can this hazard happen?". From these scenarios, STAMP recommends setting up a number of corrective measures to prevent hazards from happening. The goal is not to change human behavior by punishment or telling people "not to do this" (Leveson 2012; Dekker 2014), but to improve or even redesign the analyzed system. In the next sections, we will describe the way we conducted the STPA of the VUmc IMRT process.

3.2. STPA-Step 0: Modeling the process with safety control structures

In any RT process, one identifies approximately the same high-level accidents and hazards involved (Blandine 2013; Pawlicki et al. 2016). We identified for the VUmc IMRT process the following high-level accidents:

A1. Patient injured or killed from radiation exposure

A2. A non-patient is injured or killed by radiation exposure

A3. Damage or loss of equipment

A4. Physical damage to patient or non-patient during treatment (not from radiation)

A5. Patient dies because the treatment is delayed

and the following high-level hazards:

H1. Wrong radiation delivery to patient (linked to accident A1) that can be split in:

H1. 1. Under-dose
H1. 2 Over-dose
H1. 3 Right dose, in a wrong fractioning
H1. 4. Right dose to the wrong volume
H1. 5. Right dose to the wrong patient

*H2. A non-patient (staff) is unnecessarily exposed to radi*ation (linked to accident A2)

H3. Equipment is subject to unnecessary stress (linked to accident A3)

H4. Persons are subject to non-radiological injury (linked to accident A4)

H5. Process failures are detected too far downstream in the process workflow (linked to accident A5)

Next, the IMRT workflow was graphically modeled in terms of hierarchical safety control structures. This crucial step, although clearly described in the STPA guidelines, turned out to be in our case not so straightforward. For example, the first question we faced when drawing the control structures was: ***What goes in a controller box?*** In a simple technical system, the controller is easy to be identified - it is the computer, or more precisely the microcontroller on which the control

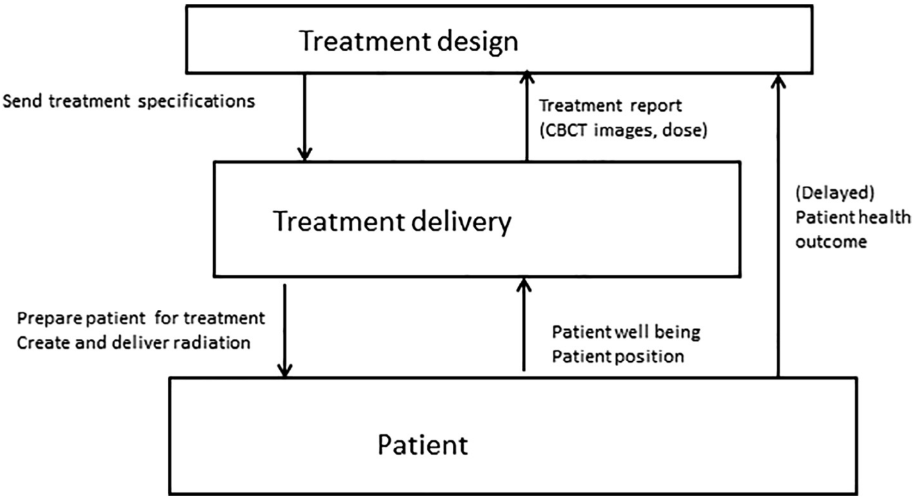

Fig. 3. A high-level safety control structure of the IMRT process.

software algorithm is running. Radiation therapy is, however, a complex socio-technical *process*, practiced by a team of humans (medical doctors, radiographers, medical physicists, patients) interacting with data (documents, digital images, personal data, etc), software and technical equipment. The answer to this first question can be given if one realizes that a control structure is not a description of the software or hardware *architecture*, but a representation of the *functions* that a system must perform, and how these functions relate to each other. Controllers are therefore functionalities, and not specific people or system components. The best way is therefore to start by drawing a very high-level control structure of the radiation therapy facility, as shown in Fig. 3. In this high-level description of the IMRT process, one can identify two primary functions, namely (1) treatment design and (2) treatment delivery. These functionalities can be graphically modeled with the *Treatment Design* controller, that devises the treatment specifications, and the *Treatment Delivery* controller, that gives the radiation treatment accordingly. The *Patient* is positioned at the bottom of the control structure in Fig. 3, modelled as a process controlled by the *Treatment delivery* controller. The treatment delivery team treats the patient while monitoring the well-being, and reports back to the treatment design team after the treatment completion. The high-level safety control structure in Fig. 3 is almost identical to the one generated in (Pawlicki et al.2016).

The next question raised in this context was ***Should a software component, such as the shared oncologic information database, also be included in the model?*** We decided not to treat it as such for now. The reason was that in most cases, this component only stores data and gives warnings, without taking crucial decisions. However, RT incidents often happen due to malfunctioning of this particular type of information system. Therefore, in a more detailed analysis, and especially in case one expects to add new functionality to this type of software component, we think that STPA should include it as well.

Next, the analysis allows to zoom in the *Treatment design* and *Treatment delivery* controllers, by building two new, lower-level control structures, shown in Fig. 4 and Fig. 5. While doing this, we faced the following question: ***Which level of granularity to use at each refinement step?*** The problem is that, happy to know already so much about the analyzed process, beginners (including us!) tend to specify all the known actors with separate controllers in this next, lower-level control structure. It is a challenge to exercise restraint in populating a control structure with too many controllers in one single refinement iteration. A good solution in this direction is to cumulate actors with similar functionality into one controller, for the time being. For example, in Fig. 4 we cumulated all the radiographers working in the treatment planning team, in one controller, labeled *Planning radiographers*. Also control actions can be cumulated. For example, the control action *Prepare patient for treatment* in Fig. 5, actually cumulates many separate actions, including accompanying the patient to the linac, applying shielding and patient positioning and immobilization. Luckily, STPA adopts a top-down approach that enables zooming in on the functionality of subsystems expected or known to be critical.

Control action or feedback? For an STPA beginner, it is often difficult to decide what a certain process activity is: a control action or a feedback. A hint that helps is to remember that control actions are *verbs*, a kind of commands or directives. On the other hand, a feedback is a *noun*, state information, or sensor measurement, something that makes the controller adapt its process model. For example, how to model the fact that the oncologist delineates the tumor contours on the CT-scan images and composes a treatment prescription? The correct answer in this case, is that these activities should be modeled as a control action, meaning a *command* to the radiographer to make a treatment plan, (see Fig. 4). This decision might seem rather counterintuitive to both beginner analyst and domain experts, because in reality there is no such verbal command given. Another dilemma we encountered was on how to model the fact that the post-planning radiographer retrieves the treatment plan approved by the medical physicist from the database, and annotates it with linac setup notes. Is this annotated plan a control action towards the treatment delivery team, or a feedback towards the medical physicist? The answer in this case depends on what the medical physicist is doing with the annotated plan. If they review it afterwards, then the annotated plan is a feedback to the medical physicist; if not, then it is a control action issued by the post-planner towards treatment delivery, like shown in Fig. 4.

3.3. STPA-Step1: Identifying possible hazards

After all the control structures have been built at the desired level of detail, one needs to identify a set of possible hazards, including all the unsafe control actions (UCAs), and all safe, yet never carried out control actions. In STPA all possible UCAs can be generated in a systematic way, by building for each control action, a table similar to Table 1. For example, here we show how we generated all possible hazards related to the control action *Run re-optimization*, performed by the controller *Planning radiographer* modeled in the *Treatment design* control structure.

For a few critical control actions, we extended the analysis by using a combinatorial coverage of all the process variables that describe the process model, following the work of Blandine (Blandine, 2013). For example, for the controller *Linac Radiographer* and its very critical control action *Start/resume the treatment*, illustrated in Fig. 5, we used the process variables shown in Table 2.

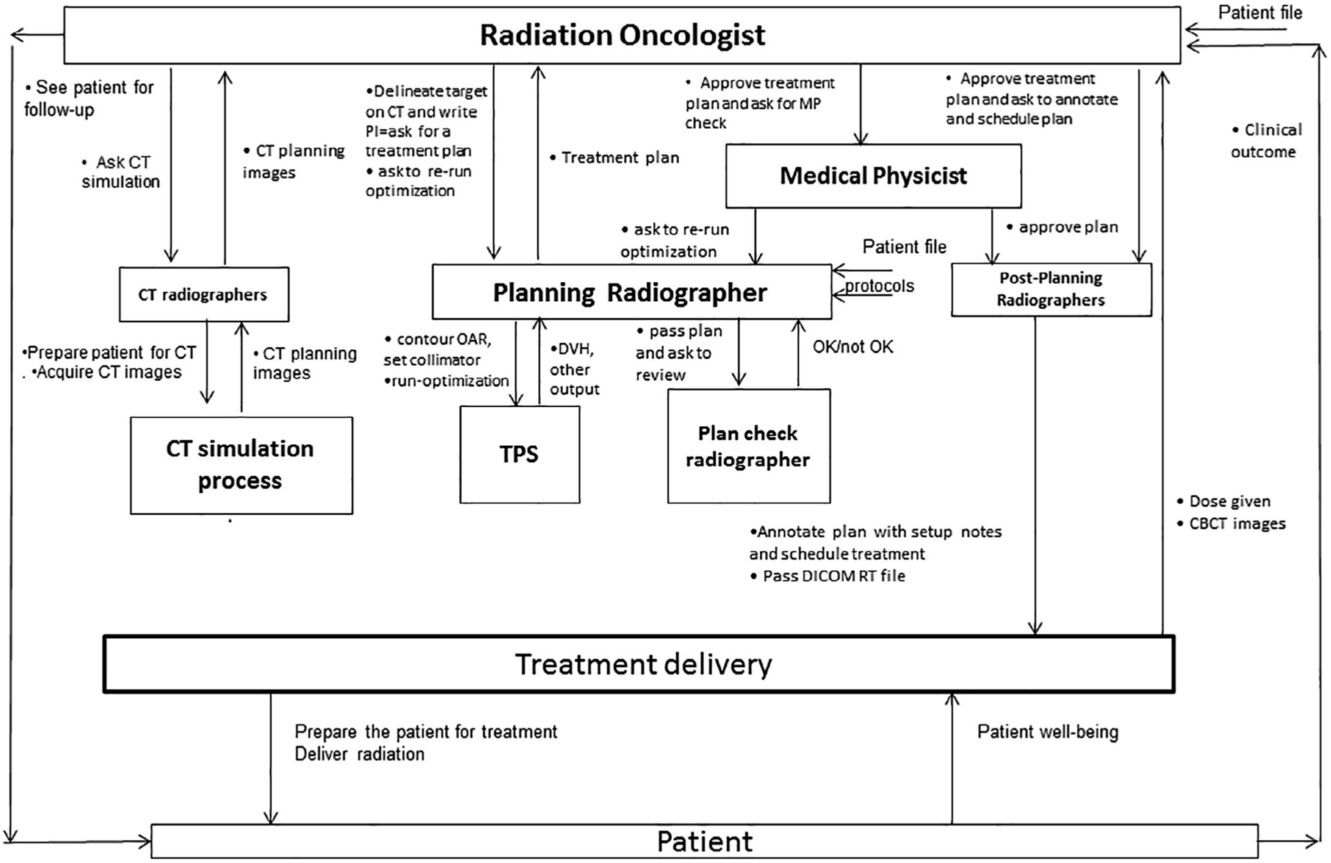
Radiation Oncologist
Patient file
• See patient for follow-up
• Ask CT simulation
• CT planning images
•Delineate target on CT and write PI=ask for a treatment plan
• ask to re-run optimization
• Treatment plan
• Approve treatment plan and ask for MP check
• Approve treatment plan and ask to annotate and schedule plan
• Clinical outcome
Medical Physicist
• ask to re-run optimization
• approve plan
Patient file
protocols
CT radiographers
Planning Radiographer
Post-Planning Radiographers
•Prepare patient for CT . •Acquire CT images
• CT planning images
• contour OAR, set collimator
•run-optimization
•DVH, other output
• pass plan and ask to review
OK/not OK
CT simulation process
TPS
Plan check radiographer
•Annotate plan with setup notes and schedule treatment
• Pass DICOM RT file
• Dose given
• CBCT images
Treatment delivery
Prepare the patient for treatment
Deliver radiation
Patient well-being
Patient

Fig. 4. A lower-level control structure for the *Treatment design* controller.

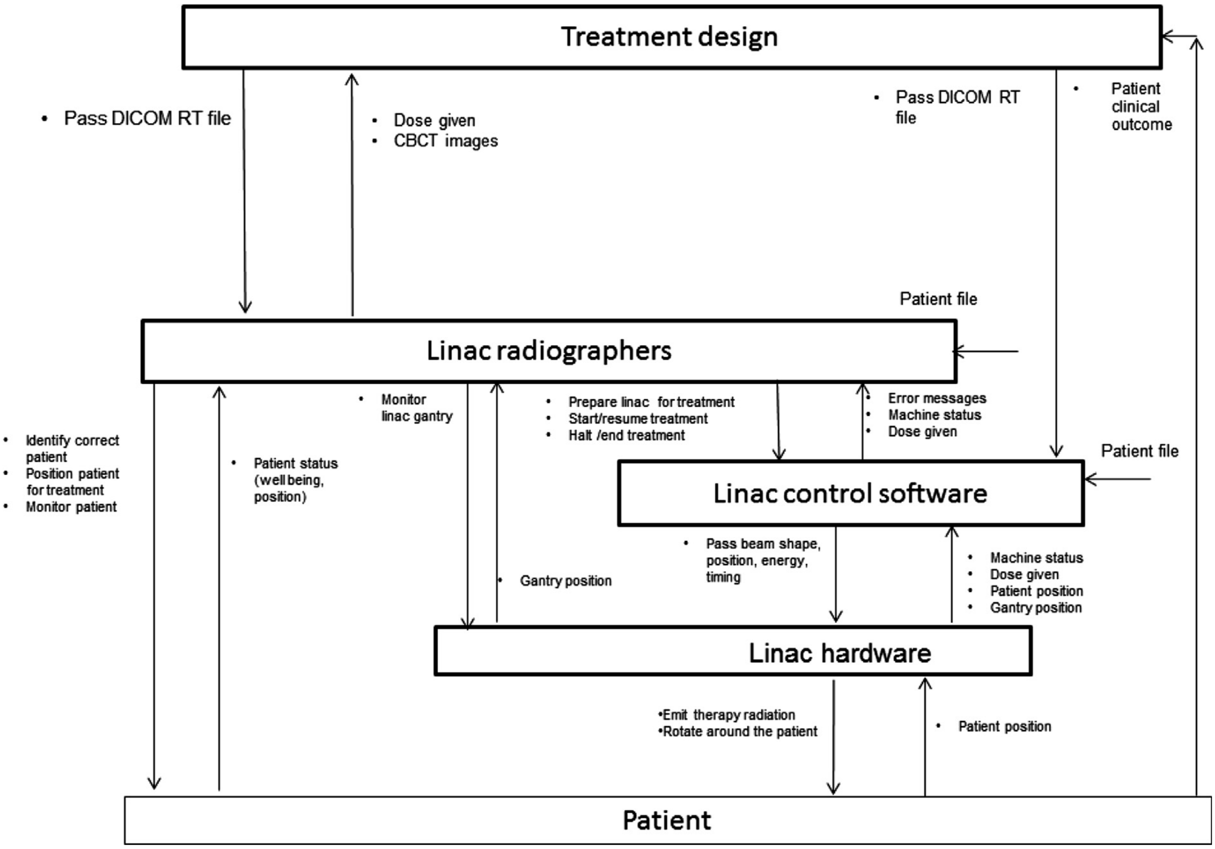

Fig. 5. A lower-level control structure for the *Treatment delivery* controller.

Table 1
All possible UCAs for the *Planning radiographer* controller from the *Treatment design* control structure.

Control action	The control action is not given	An incorrect control action is given	The control action is given at the wrong time	The control action given with wrong duration
Run re-optimization	Planning radiographer does not execute re-optimization when asked	Planning radiographer runs re-optimization with wrong parameters	Planning radiographer starts re-optimization too soon, before *all* the target and OAR have been delineated. Planning radiographer re-optimizes the plan long after the peer reviewing asked for it	Planning radiographer keeps on applying re-optimization even after the peer reviewers approved the plan. Planning radiographer stops the re-optimization process too soon (the same like does not execute re-optimization)

This approach helped us to discover additional UCAs. For example, instead of *The treatment is initiated before it is appropriate to give a signal to start treatmen*t, as reported without using process variables in (Pawlicki et al.), we identified the following, more detailed set of hazards:

- The linac radiographer starts/resumes the treatment too early, before there is a patient
- The linac radiographer starts/resumes treatment too early, before there is a plan
- The linac radiographer starts/resumes treatment too early, before the patient is correctly positioned
- The linac radiographer starts/resumes treatment too early before the linac equipment is ready.

Eventually, we ended up with a set of 142 identified hazards.

3.4. STPA-Step2: Identifying causal scenarios and formulating corrective measures

In order to evaluate the potential of STPA for defining corrective measures, the STPA analyst in our experiment brainstormed together with two medical physicists of the RT team, and together they created possible causal scenarios for the first 10 UCAs out of 142 found in STPA-Step1 (see Table 3). Next, for these causal scenarios, the STPA team formulated recommendations for corrective mitigation measures. Each corrective measure was categorized as targeting for software (SW), for human-related procedures (H), or for organization (O), as shown in Table 4.

Incidents in RT happen mainly because of human errors (Huq et al. 2016). This motivated us to go one step further and apply the human-engineering STPA extension, as recently proposed by Thomas & France (Thomas and France 2016), to understand *why* human operators might cause unsafe situations. For instance, we investigated the causal scenarios for the *Planning radiographer* controller in Fig. 4 and its *UCA 34*: *Planning radiographer runs re-optimization with wrong parameters (OAR contours, collimator settings, etc)*. Let us describe the situation in more detail. When a new treatment plan must be devised, the radiographer receives a treatment prescription from the radiation oncologist and a protocol from the organization, with guidelines on how to position the gantry collimator jaws relatively to the tumor, on the CT scan image. However, it happens in practice that a plan reviewer discovers that the collimator jaws have been positioned in a way that deviates from the protocols. This is a potential hazardous situation that might create a suboptimal treatment plan. The question here is *why* this human controller (the planning radiographer), free of any bad intentions, does contribute to a potentially hazardous situation? To answer this question, the new STPA extension for human controllers proposes to look into the following groups of causes.

(1) *Incorrect estimate about the process state.* It might happen that either treatment prescription or protocols are ambiguous, which allows for a wrong interpretation by the radiographer. Interestingly, this scenario involves other controllers as well (oncologists, medical physicists), and this avoids to point out on a single “guilty” person. Or, it might be that the radiographer *thinks* that his unorthodox way of collimator jaws positioning is better than the one prescribed in the protocol, because it could result in a lower dose in the OAR. Which up to this point, is a perfectly correct judgment. However, by doing this, the radiographer *overlooks* that radiation hot-spots could be created elsewhere in the body, which is an undesired, dangerous consequence. Another scenario could be that the radiographer is interrupted (eg. by a phone or pager call, or a handover to another radiographer) and restarts the interrupted planning procedure from a wrong point.
(2) *Incorrect belief about the process behavior.* It is possible that the

Table 2
Process variables and their values for the control action *Start/resume Treatment.*

Process variable	Person close to the beam	Patient readiness	Treatment plan	Equipment readiness	Facility mode	Treatment status
Possible value	Yes/No	No patient /Ready/Not ready	Right/Wrong/None	Ready/Not ready	Therapy/QA	No treatment/In progress/Halted

radiographer is not experienced and does not have enough knowledge of what TPS really can do. In this case, they introduce their own knowledge, and *make assumptions* about the TPS process, which unfortunately are not correct.

(3) *Flaws in the mental model updates*. The radiographer could base their decisions on previous experiences of using the same incorrect collimator positioning in the past, without any problems at that time.

This was just a short exercise. A full understanding of human behavior requires also here, like in any other safety-critical process, a more extensive research, for example by tactfully interviewing all the human operators involved in the RT process.

4. Findings and discussion

RQ1. What characterizes the STPA analysis when conducted in a radiation therapy department?

The first research question actually raised more sub-questions, such as *"Where are beginner analysts struggling the most?" and "Does the analysis add an excessive workload on the (already very busy) RT team?".*

Especially in the beginning of the analysis, we struggled with the rather counter-intuitive, systems-wise graphical modeling of the IMRT process. Nevertheless, we managed to overcome these difficulties due to help from the STAMP community, and by studying similar STPA-RT reports (Pawlicki et al. 2016; Blandine 2013). However, these reports analyzed a different type of RT process and moreover, the division of roles in their RT team was slightly different. Therefore, we can conclude that although some parts of the existing reports could be reused, a lot of details in the STPA modeling needed to be tailored to our own IMRT process.

For us, the most remarkable result was that an analyst with a computer engineering, instead of RT background, could obtain a correct list of potential hazards and a few sensible safety recommendation specific to a radiation therapy workflow. This required a relatively short time, with about 20 man-hours from only two domain specialists. For comparison, the HFMEA at that time was conducted in a larger team (10 RT practitioners) and required 200 man-hours to analyze the risks of a full IMRT process. We are aware that a fair comparison is not possible because our STPA did not target the whole IMRT process. However, these results, together with STPA being a top-down approach, make us hypothesize that especially STPA-Step 0 (Process modeling) and STPA–Step 1 (Unsafe Control Actions) can be conducted by a system specialist with less RT domain knowledge when compared to HFMEA. This might be useful for example when a new software module has to be implemented in a RT treatment machine. In this case, a system- or software engineer can start the STPA hazard analysis alone, with little input from domain experts, thus reducing the experts' load in this phase. An HFMEA in contrary, needs from the beginning time-intensive brainstorm meetings involving RT representatives with extensive experience with the clinical process.

In STPA-Step 2 (Causal scenarios and mitigation measures) the input of domain experts is of paramount importance. This STPA vs. FMEA reasoning can be easily visualized in Fig. 6. The modeling STPA-Step 0 is here clearly visible, with the big advantage that it can be performed by a system engineer alone vs. a brainstorm action in FMEA, where all team members get equally involved from the beginning.

RQ2. Does STPA bring any added value compared to HFMEA?

Our STPA analysis identified 142 possible UCAs related to the investigated IMRT process. In order to answer the second research question RQ2, we compared these hazards with the failure modes resulted from a seven years old HFMEA performed in the same RT-team (see Fig. 7). Moreover, we analyzed a subset of 10 UCAs and formulated causal scenarios and adequate safety recommendations.

We found out that the hazards identified with STPA and HFMEA show a large overlap, which must be reassuring for the VUmc team. For example, we show bellow ten arbitrarily selected hazards found by both methods.

Wrong patient is treated
Oncologist asks a plan based on wrong target contours
CT radiographer does not position and immobilize the patient correctly
CT images are assigned to the wrong patient
Radiographer designed a sub-optimal treatment plan
MP approves a sub-optimal plan
Patient receives radiation before the treatment plan was approved
Patient is wrongly positioned during the radiation delivery
Wrong images are used for treatment table alignment
The linac gantry rotates and hits the patient

Also, we noticed that HFMEA offered a more detailed description of the hazards belonging especially to the category *Wrong command given*. For example, where STPA found an UCA: *Patient is incorrectly immobilized*, HFMEA found different types of specific problems related to patient immobilization, such as *Immobilization mask does not close well.* Or, for the STPA found UCA: *Linac gantry collides with patient or table*, HFMEA found also a more specific failure mode *Linac collides with other furniture, chairs, etc*. These differences can be explained by the deeper domain knowledge present in the HFMEA team, as well as the bottom-up component-oriented character of the FMEA technique. Probably a more low-level STPA modelling would have found these hazards as well.

However, we discovered that STPA offers a more rigorous

Table 3
A subset of ten UCAs that received a detailed causal analysis in STPA-Step2.

ID	Unsafe Control Action (UCA)
1	Radiation oncologist wrote a wrong CT prescription
2	Radiation oncologist asks a CT simulation too long after the patient diagnosed with cancer arrived in the department
3	Radiation oncologist asks a plan based on wrong PI or target contours
4	Radiation oncologist creates the PI or target contours for a different patient
5	Radiation oncologist delineates on a wrong CT image
6	Radiation oncologist asks for a plan before he starts to write the PI and delineate the contours
7	Radiation oncologist asks for a plan long after he wrote the PI and contoured the target on the CT-scan images
8	Radiation oncologist asks for a plan, but did not complete the PI or the target contours
9	Radiation oncologist keeps on asking for plan re-optimization, even when not necessary
10	The patient gets treated though the radiation oncologist did not approve the plan

Table 4
Some examples of UCAs and their associated causal scenarios and corrective measures.

ID	UCA	Causal scenarios	Corrective measures
1	Radiation oncologist wrote a wrong CT prescription.	Oncologist did not have the right information at that time, and after that forgot to update the request. Oncologist asked to image a wrong anatomic area.	1.1 Use templates for CT prescriptions (SW) 1.2. Require the oncologist to be present during the CT scan to indicate exactly what imaging they need (H)
7	Radiation oncologist asks for a plan long after they wrote the PI and contoured the target on CT-scan images.	Oncologist forgot to validate the PI	7.1. Build in a reminder in software for the treatment scheduler (SW) 7.2. Hire a person (logistic manager) to keep overview of the whole workflow and to notify about possible delays (O)

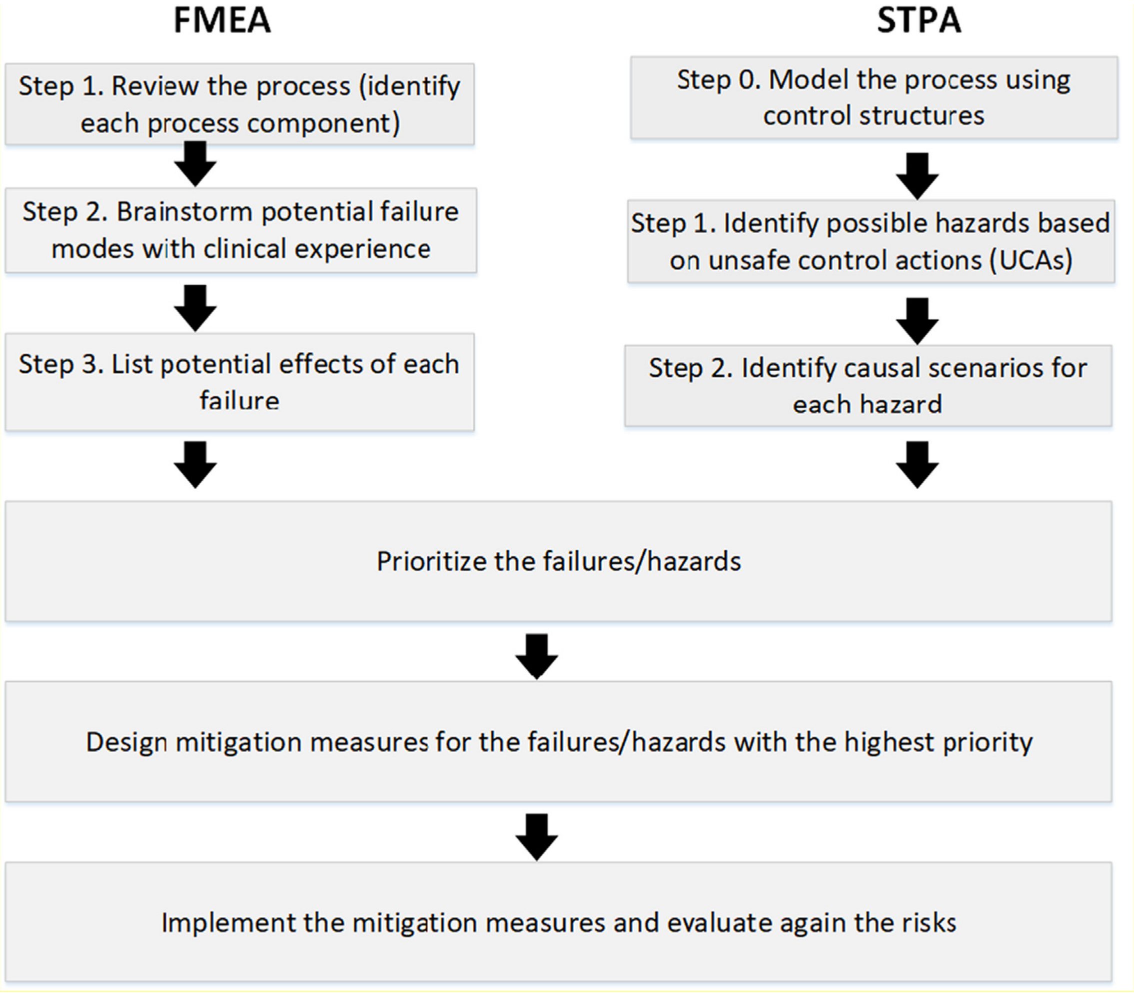
FMEA
STPA
Step 1. Review the process (identify each process component)
Step 2. Brainstorm potential failure modes with clinical experience
Step 3. List potential effects of each failure
Step 0. Model the process using control structures
Step 1. Identify possible hazards based on unsafe control actions (UCAs)
Step 2. Identify causal scenarios for each hazard
Prioritize the failures/hazards
Design mitigation measures for the failures/hazards with the highest priority
Implement the mitigation measures and evaluate again the risks

Fig. 6. The workflow steps for both FMEA and STPA. Note that the workflows differ substantially in the first part.

formulation of hazards, by better separating causes from their effects. For example, a HFMEA failure mode like *Operator forgot to apply position markers*, is formulated in STPA as: UCA 21: *Radiographer did not apply position markers*. This formulation is in our opinion more rigorous and correct, because *forgot* is in fact a causal scenario, and not a hazard. The hazard is that *no position markers were applied*, whereas possible causes could also be that the radiographer did not forget to apply them, but the position markers have fallen, after they have been correctly applied.

Another interesting observation is that a one-to-one mapping between HFMEA failure modes and STPA UCAs is impossible to achieve. This because some failure modes in HFMEA do not match with any STPA UCAs, but with a STPA causal scenario instead. For example the HFMEA failure mode *No planning check executed* matched in STPA with a *Missing-feedback* type of causal scenario, coming from the *Plan check radiographer* controller, towards the *Planning Radiographer* controller, as illustrated in Fig. 4. The reason is that in STPA control structures, not all operations are modeled as control actions; some operations are modeled as feedback. We think that this does not have implications for safety, as long as the unsafe situation is captured somewhere.

The most important result of our experiment is that STPA found new, unsafe conditions which have not been explored in the previous HFMEA. Most of them are time-related, belonging to the third and fourth column in Table 1. Examples are: UCA 49: *Postplanner sent the plan to treatment delivery before the plan was approved and completed,* or UCA 32: *The CT radiographers start to acquire images long after the patient has been immobilized on the treatment table, without checking if the patient is still in the correct position.*

The fact that STPA discovered more hazards than reported in the old FMEA did not have heavy consequences for the safety of the VUmc IMRT process, because most of these hazards were protected by software or procedures, or were first discovered and later discarded by the HFMEA team, as having a low risk. For example the UCA 124: *The linac*

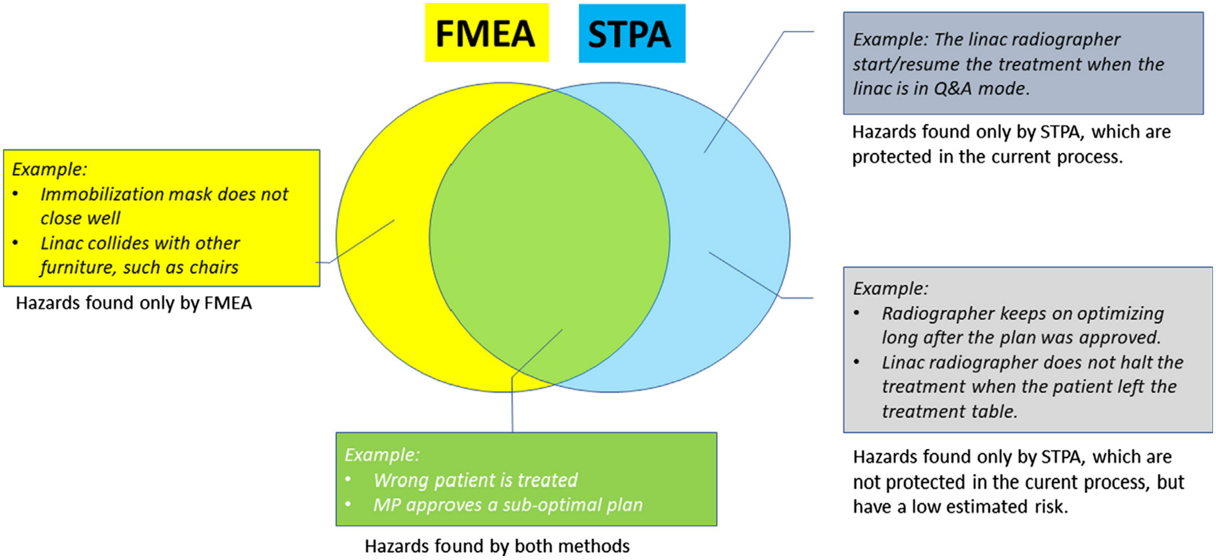
FMEA
STPA
Example: The linac radiographer start/resume the treatment when the linac is in Q&A mode.
Hazards found only by STPA, which are protected in the current process.
Example:
• Immobilization mask does not close well
• Linac collides with other furniture, such as chairs
Hazards found only by FMEA
Example:
• Radiographer keeps on optimizing long after the plan was approved.
• Linac radiographer does not halt the treatment when the patient left the treatment table.
Hazards found only by STPA, which are not protected in the curent process, but have a low estimated risk.
Example:
• Wrong patient is treated
• MP approves a sub-optimal plan
Hazards found by both methods

Fig. 7. A Venn diagram showing a comparative analysis of the found hazards.

radiographer does not halt the treatment when indicated to do so (person in the beam, imminent collision) is safeguarded by procedures (the last staff member who leaves the linac area has to push a red button), or software (emergency stop gets triggered when an imminent collision is detected). Also UCA 116: *The linac radiographer start/resume the treatment when the linac is in Q&A mode* is currently protected in software by passwords for authentication and user interface screens specific for Q&A mode. Good to mention that some of these protection measures have been introduced as a consequence of the old HFMEA.

However, STPA identified also new, unprotected hazards that HFMEA has never found, such as:

UCA 7: *Radiation oncologist asks for a plan long after he wrote the PI and contoured the target on CT-scan images*

UCA 19*: Radiation oncologist sees the patient too long after treatment*

UCA 44: *Planning radiographer keeps on applying optimization in TPS long after peer-reviewers already have approved the plan*

UCA 49*: Post planning radiographer sends the DICOM files to treatment delivery before they are approved and complete*

UCA 110: *The linac radiographer does not start/resume treatment while everything (patient, linac) is otherwise ready*

UCA 124: *The linac radiographer does not halt the treatment when the patient left the treatment table*

Although all these new hazards have safety implications, such as wrong treatment or undesired delays in treatment, the VUmc domain experts qualified them - again - as having a low risk of occurrence. This was possible only because they have been familiar with the IMRT process for many years.

However, this might not be the case in a new RT system or process that still needs to be implemented. In this situation, uncovered hazards might have serious safety-related consequences that can cost lives. Moreover, any FMEA is difficult or even impossible to perform in early design phases, because it is a bottom-up approach that requires a detailed implementation.

Regardless the estimated risk of the found hazards, we consider that in such a safety-critical process as radiotherapy, one must investigate all their possible causal scenarios that will eventually lead to mitigation measures.

Although there was no time and need to perform a complete causal analysis of all the 142 UCAs found in STPA-Step1, the STPA team crafted a number of interesting causal scenarios and safety-related mitigation recommendations for the first 10 hazards from the list. Some of these recommendations are suggesting (1) technical improvements, such as *"Develop machine learning software to automatically evaluate CT scans and assist the oncologist in target and OAR delineation"*, (2) improvements in existing human-related procedures, such as *"If the dose prescribed by the oncologist seems to be technically unfeasible after two trials, then the radiographer should immediately ask the medical physicist for help"* or (3) management and organization improvements, such as *"Create a logistics manager to keep an overview of all workflow tasks and their progress and notify delayed processes",* respectively.

We found some of the newly found hazards especially interesting, because they indicate intriguing and complex human behavior that deserves a more detailed analysis. STPA, as opposed to the HFMEA methodology, does offer support to understand why a human component would make a mistake and thus contribute to an accident. Therefore, for one very critical hazard, UCA 34: *Planning radiographer runs re-optimization with wrong parameters (OAR contours, collimator settings, etc)*, we applied the human-engineering STPA extension, as recently proposed by Thomas & France (Thomas and France, 2016), to understand *why* this human operator might cause an unsafe situation. We described this analysis in Section 3.4. In our opinion the offered guidelines were helpful in getting a better insight in hazardous human behavior. Of course, more research is needed in this direction.

5. Conclusions and future work

The experiment reported in this paper assessed the introduction of STPA to analyze the safety of an IMRT/VMAT process, and estimated which possible added value the method might bring, compared to the traditional HFMEA.

The first lesson we have learned is that RT STPA beginners struggle the most with the graphical modeling required in STPA-Step 0. We experienced this step as a counterintuitive process that requires a radical change of mindset. However, once the control structures-based model reaches the desired level of detail, it becomes a systematic, powerful tool, able to "catch" hazards easier than HFMEA.

Comparison results show that STPA-Step 1 discovered mostly the same hazards as HFMEA. While HFMEA was able to identify very detailed, domain-related hazards of the type "wrong action", STPA proved to be more rigorous in describing the unsafe situations. Most remarkable is that STPA was able to identify some subtle, unexplored unsafe conditions. Most of them are currently protected by software and/or procedures, or have a low estimated risk. Therefore, it was no urgent need to rethink the present safety management policy at RT-VUmc. However, this might not be the case when a new RT system or process needs to be built. In this case, unrevealed hazards might lead to catastrophic results, because a new RT team might not possess the rich experience the VUmc RT team had. Therefore, we think that all the hazards discovered by STPA should be analyzed seriously and measures to mitigate them should be designed.

Next, we practiced STPA-Step2 by conducting a causal investigation of ten newly found unprotected hazards. This led to valuable corrective measures that address software, procedures and organization and can contribute eventually to a safer IMRT process. Moreover, in case of one specific, critical unsafe situation *(Planning radiographer runs re-optimization with wrong parameters),* we found in STPA additional guidance for an interesting, tactful insight into hazardous human behavior. Therefore, we expect that in the future, applying a systems-theoretic safety analysis to a full IMRT process could clarify complex human-related workflow issues.

Finally, it is worth mentioning that the STPA was led by a software systems engineer with considerably less domain-specific knowledge, who could do a lot of work independently from the RT team, especially during the first steps, STPA-Step0 and STPA-Step1.

Given all this, we strongly believe that anytime a hazard analysis is needed for a radiation therapy process, STPA should be considered as a serious candidate, along with the traditional methods. In early stages of development, when many implementation details are still unknown, STPA is in our opinion even a better candidate than HFMEA. The reason for this is because STPA does not rely heavily on the clinical experience with the procedure or on the final implementation in order to start with the analysis.

The STAMP concept is barely known in RT communities and is not yet recommended by current RT safety standards. The experiences and results presented in this paper show its potential, and may invite to further investigation and application of STAMP in radiation therapy.

Acknowledgments

The authors would like to thank Nancy Leveson, Todd Pawlicki, John Thomas, Aubrey Samost and Simon Whiteley, for the inspiring STAMP-related discussions and guidance across different time zones. The VUmc HFMEA-RT team, especially project manager Anke van Mourik, for sharing the results of their hazard and risk analysis. Herbert Bos, for his help in writing the manuscript, and his encouragements to pursue this interdisciplinary research.

Declaration of Competing Interest

The department of radiation oncology has received research grants from Varian Medical Systems outside the submitted work. Wilko Verbakel has received speakers honoraria/travel expenses from Varian Medical Systems.

References

Abdulkhaleq, A., Lammering, D., Wagner, S., Röder, J., Balbierer, N., Ramsauer, L., Raste, T., Boehmert, H., 2017. A Systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles. Procedia Eng. 179, 41–51.

Alemzadeh, H., Chen, D., Lewis, A., Kalbarczyk, Z., Raman, J., Leveson, N., Iyer, R.K., 2015. Systems theoretic safety assessment of robotic telesurgical systems. 34th Int. Conf. Computer Safety, Reliability, and Security (SAFECOMP).

Allison, C.K., Revell, K.M., Sears, R., Stanton, N.A., 2017. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. Saf. Sci. 98, 159–166.

Arnzen, H.E., 1966. Failure modes and effect analysis: A powerful engineering tool for component and system optimization. In: Reliability and Maintainability Conference, pp. 355–371.

Blandine, A., 2013. Systems theoretic hazard analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry. Massachusetts Institute of Technology, Cambridge, MA.

Borras, C., 2006. Overexposure of radiation therapy patients in Panama: problem recognition and follow-up measures. Rev. Panam. Salud. Publica 20 (2–3), 173–187.

Dekker, S., 2014. The field guide to understanding 'Human Error'. CRC Press: London.

DeRosier, J., Stalhandske, E., Bagian, J.P., Nudell, T., 2002. Using health care failure mode and effect analysis. Joint Commission J. Qual. Improvement 27, 248–267.

Ford, E., Evans, S.B., 2018. Incident learning in radiation oncology: A review. Med. Phys. 45, e100–e119.

Huq, M., et al., 2016. The report of Task Group 100 of the AAPM: Application of risk analysis methods to radiation therapy quality management. Med. Phys. 43, 4209–4262.

IKNL Integraal Kankercentrum. 2017. 'Nederlandse Kankerregistratie', Netherlands Comprehensive Cancer Organisation, Accessed aug 2017. http://www.cijfersoverkanker.nl/.

International Atomic Energy Agency, IAEA 2014. Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards. In: IAEA SAFETY STANDARDS SERIES No. GSR Part 3.

Ishimatsu, T., Leveson, N.G., Thomas, J.P., Fleming, C.H., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H., Hoshino, N., 2014. Hazard analysis of complex spacecraft using systems-theoretic process analysis. J. Spacecraft Rockets 51, 509–522.

Kwon, Yisug, Leveson, Nancy, 2017. System theoretic safety analysis of the Sewol-Ho Ferry accident in South Korea. INCOSE Int. Symp. 27, 461–476.

Leveson, N.G., 2012. Engineering a safer world: systems thinking applied to safety. MIT Press, Cambridge, MA, USA.

Leveson, N.G., Turner, C.S., 1993. An investigation of the Therac-25 accidents. Computer 26, 18–41.

Olch, A., 2014. Quality and safety in radiation therapy: learning the new approaches in task group 100 and beyond. Med. Phys. 41, 067301-n/a.

Otto, K., 2008. Volumetric modulated arc therapy: IMRT in a single gantry arc. Med. Phys. 35, 310–317.

Pawlicki, T., Dunscombe, P.B., Mundt, A.J., Scalliet, P., 2011. Quality and safety in radiation therapy. CRC Press.

Pawlicki, T., Samost, A., Brown, D.W., Manger, R.P., Kim, G.Y., Leveson, N.G., 2016. Application of systems and control theory-based hazard analysis to radiation oncology. Med. Phys. 43, 1514–1530.

Thomas, J., France, M., 2016. Engineering for Humans: STPA Analysis of an Automated Parking System. Fifth MIT STAMP Conference, Cambridge, MA.

Veldeman, L., Madani, I., Hulstaert, F., de Meerleer, G., Mareel, M., de Neve, W., 2008. Evidence behind use of intensity-modulated radiation therapy: a systematic review of comparative clinical studies. Lancet Oncol. 9, 367–375.

Verbakel, W.F., Cuijpers, J.P., Hoffmans, D., Bieker, M., Slotman, B.J., Senan, S., 2009. Volumetric intensity-modulated arc therapy Vs. conventional IMRT in head-and-neck cancer: A comparative planning and dosimetric study. Int. J. Radiat. Oncol., Biol. Phys. 74, 252–259.