Hazard Analysis (FMEA & STPA)

Todd Pawlicki, Ph.D.

UC San Diego
RADIATION ONCOLOGY

Joint IAEA-ICTP training on patient safety in radiotherapy
Trieste, Italy
24 – 28 November, 2014

Hazard (Risk) Analysis

- How do I identify safety hazards that are not immediately obvious?
- Two cases
  - New equipment and/or process
  - Existing equipment and/or process
- Different strategies for hazard analysis
  - Failure Modes & Effects Analysis (FMEA)
  - System Theoretic Process Analysis (STPA)
  - There are more, but we'll focus on FMEA & STPA

Hazard Analysis

Start with a piece of equipment and/or a process.

How would you assess *and communicate* the safety aspects in this case?

FMEA

First, answer some simple questions

- What could go wrong?
  - Surf board slips out from underneath him and he hits his head
  - Lands on the surf board but falls and skins his knee
  - Brother knocks him off bed and he hits his head

- How severe would it be?
  - Use a scale of 1 – 10 where 10 means most severe
  - Let's use **8** out of 10

A couple more simple questions

- What is the likelihood that this will occur?
  - Surf board slips out from underneath him and he hits his head
  - Use a scale of 1 – 10 where 10 is the most likely
  - Let's use **6** out of 10

- What is the likelihood that we can detect *and* prevent this from happening?
  - Use a scale of 1 – 10 where 10 means a low likelihood
  - Let's use **9** out of 10

Let’s Review

- What could go wrong?
  - Surf board slips out from underneath him and he hits his head
- How severe would it be?
  - **8** out of 10
- What is the likelihood that this will occur?
  - **6** out of 10
- What is the likelihood that we can detect *and* prevent this from happening?
  - **9** out of 10

UC San Diego
RADIATION ONCOLOGY

Failure Mode, S, O, & D values

- What could go wrong? **FAILURE MODE**
  - Surf board slips out from underneath him and he hits his head
- How severe would it be?
  - **8** out of 10 **SEVERITY = 8**
- What is the likelihood that this will occur?
  - **6** out of 10 **OCCURANCE = 6**
- What is the likelihood that we can detect *and* prevent this from happening?
  - **9** out of 10 (lack of) **DETECTABILITY = 9**

Risk Priority Number (RPN)

- RPN = Severity x Occurrence x Detectability
- For our example, **RPN = 8 x 6 x 9 = 432**
- Now go back and do the same for the other failure modes
- Rank the RPN's, take action on the highest RPN values

Failure Modes and Effects Analysis

- A consistent approach to understand and characterize your risk exposure
  - Allows you to prioritize risk mitigation efforts
- An effective method to communicate and work to address risk
  - Existing risk as well as effects of mitigation efforts
  - Rank RPNs and take action to mitigate risky steps
- Designed to be a prospective tool but can be use retrospectively

Tips for Performing an FMEA

- Identifying unambiguous failure modes

- Recognize shortcomings of component-base probabilistic failure models
  - The RPN values are not absolute

- Don’t get bogged down in the details
  - Group discussions here can be as valuable as the analysis itself

Safety Improvement

The eventual outcome of a FMEA

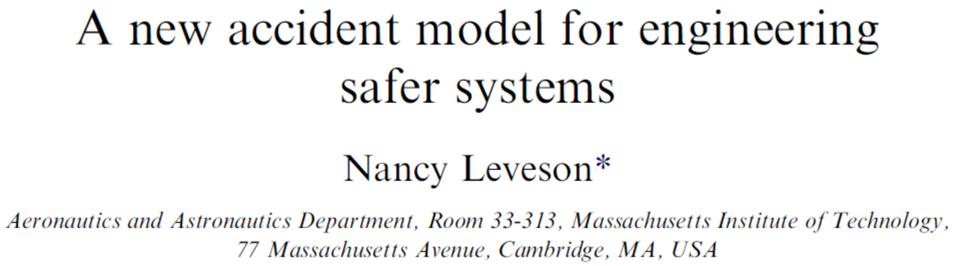
Pillows!

STPA

(not ‘simplified’ yet)

- Systems Theoretic Process Analysis

- Based on Systems Theory (STAMP)
  - Equipment and processes are coupled
  - Any change in the system may affect many areas
    - Law of unintended consequences



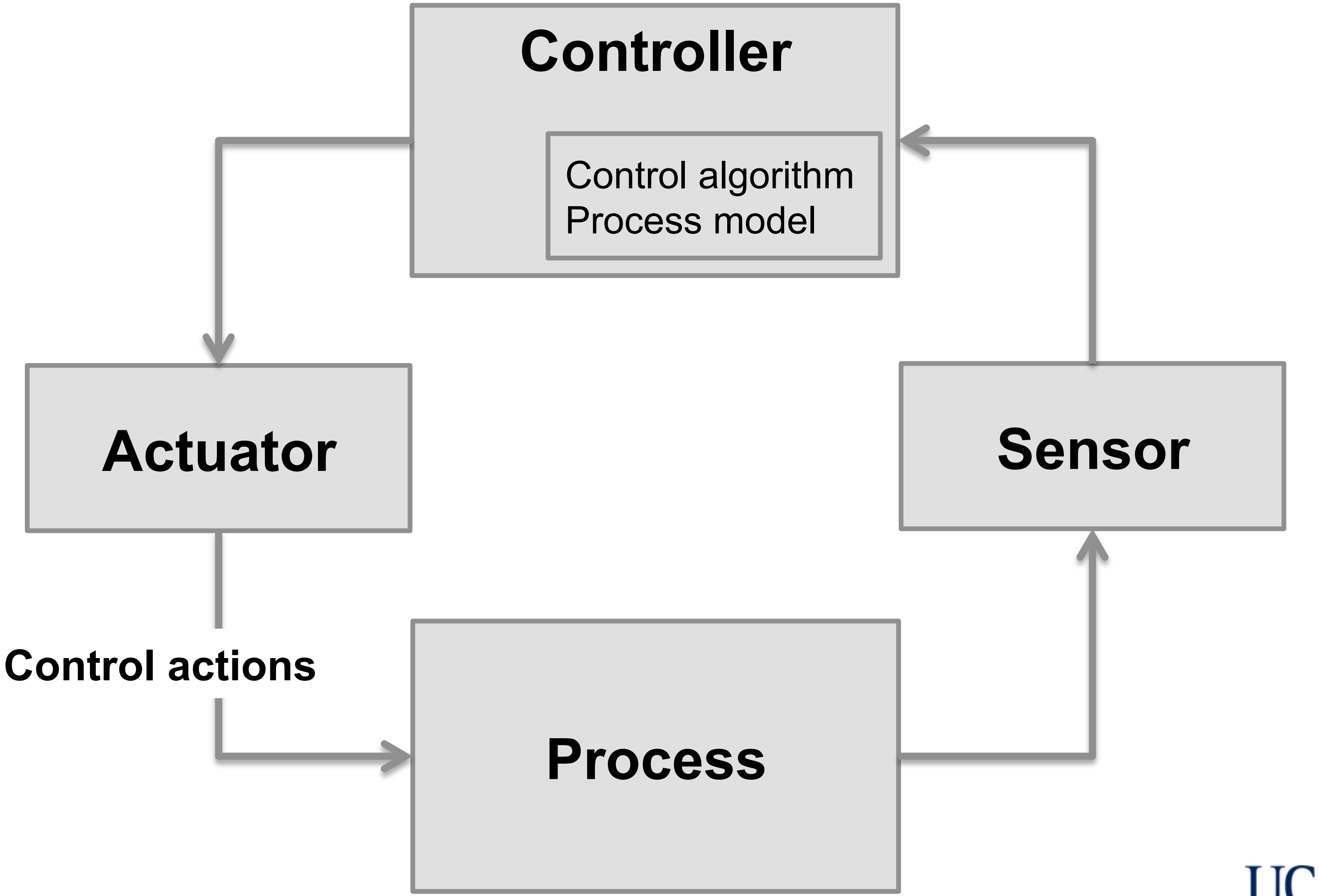
A new accident model for engineering
safer systems

Nancy Leveson*

Aeronautics and Astronautics Department, Room 33-313, Massachusetts Institute of Technology,
77 Massachusetts Avenue, Cambridge, MA, USA

Safety Science 42 (2004) 237–270

STPA is based on Control Structures



SYSTEMS THEORETIC HAZARD ANALYSIS (STPA) APPLIED TO THE RISK REVIEW OF COMPLEX SYSTEMS: AN EXAMPLE FROM THE MEDICAL DEVICE INDUSTRY

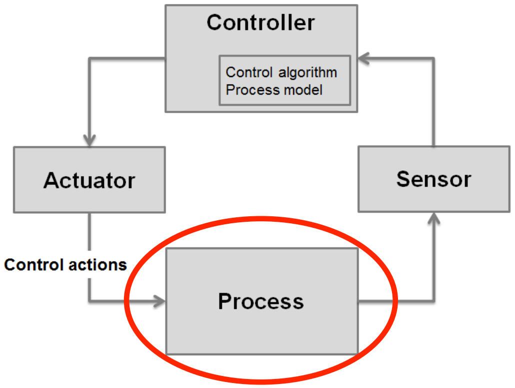
by
Blandine Antoine

M. Sc. Nuclear Engineering, University of California Berkeley, 2005
Dipl. Ing. Ecole Polytechnique, 2006
M.P.A. Ecole Nationale des Ponts et Chaussées, 2007

Submitted to the Engineering Systems Division
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
February 2013

Proton therapy at the PROSCAN facility (Paul Scherrer Institute)

STPA Procedure

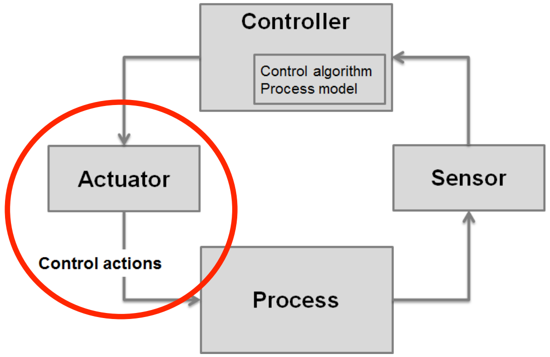


- System description
  - High-level understanding of the process and/or equipment you are analyzing

- Imagine a list of accidents
  - Can be thought of as losses; usually 3-5 items

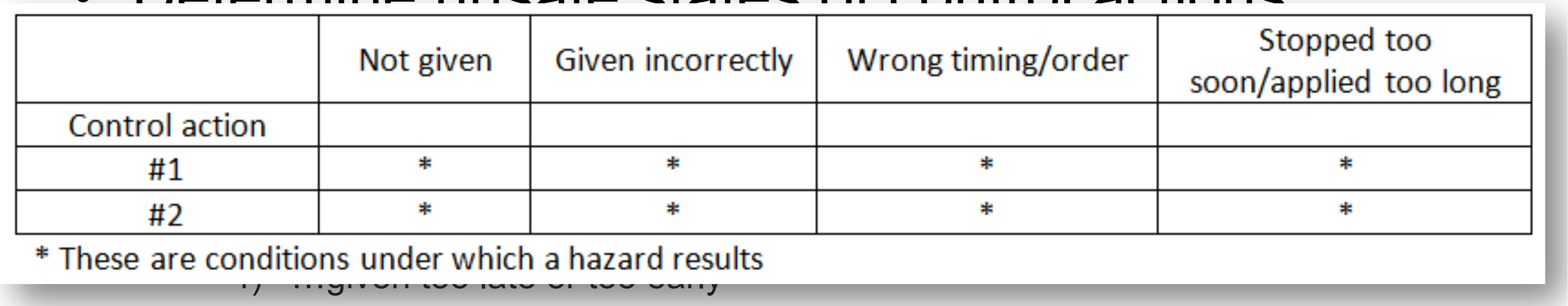
- Imagine a list of hazards
  - A process and/or equipment condition that would lead to a loss
  - Each hazard is an anchor point for the rest of the analysis

STPA Procedure



- Create a list of controls
  - An item or entity that influences the process and/or equipment being analyzed

- Determine unsafe states of control actions



	Not given	Given incorrectly	Wrong timing/order	Stopped too soon/applied too long
Control action				
#1	*	*	*	*
#2	*	*	*	*

* These are conditions under which a hazard results

4) …given too late or too early

  - Called “Step 1” of STPA

UC San Diego
Radiation Oncology

STPA Procedure

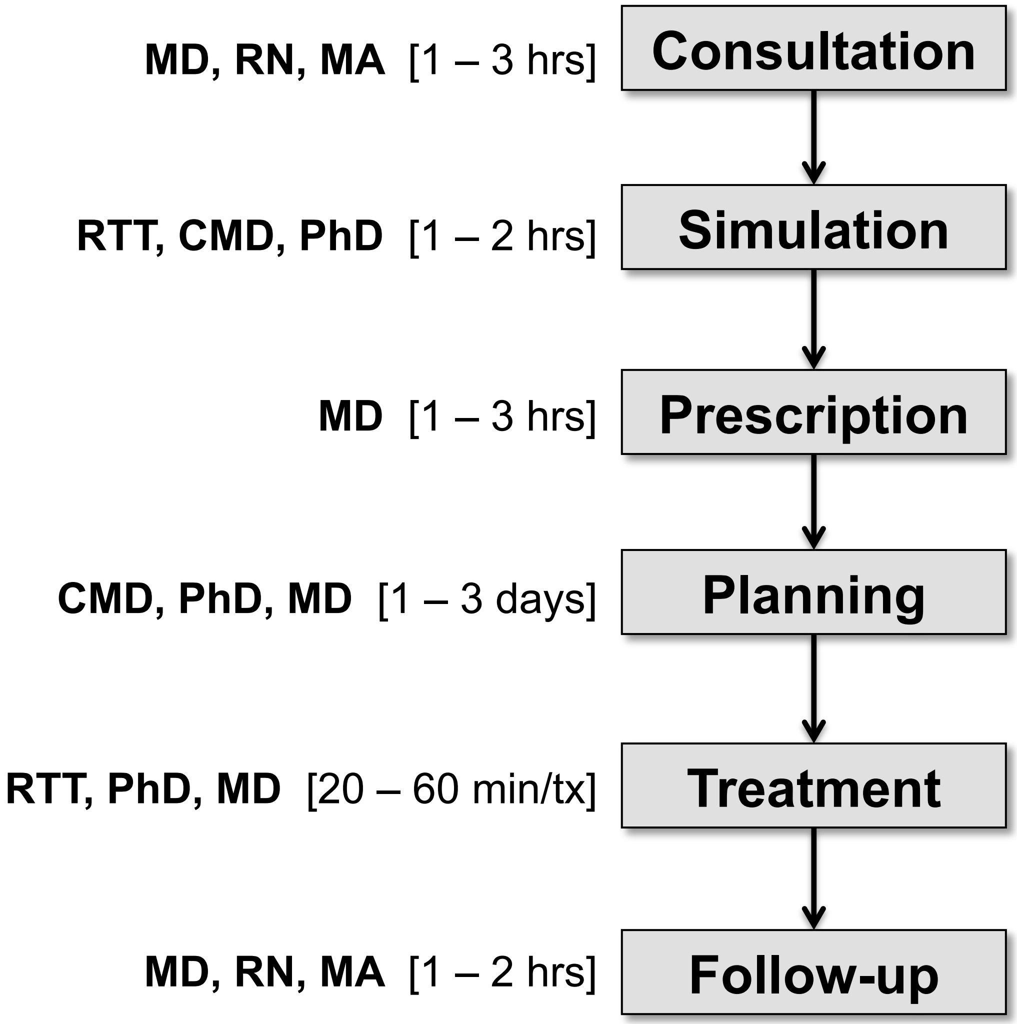
- Determine how each unsafe control action state could occur
  - This is “What can go wrong?” …similar to FMEA failure modes
  - Called “Step 2” of STPA

- The last part is to convert the previous bullet into a list of process and/or equipment requirements

FMEA and STPA

- Let’s apply FMEA and STPA prospectively on a new radiotherapy technique

Conventional Procedure



MD, RN, MA [1 – 3 hrs] **Consultation**

RTT, CMD, PhD [1 – 2 hrs] **Simulation**

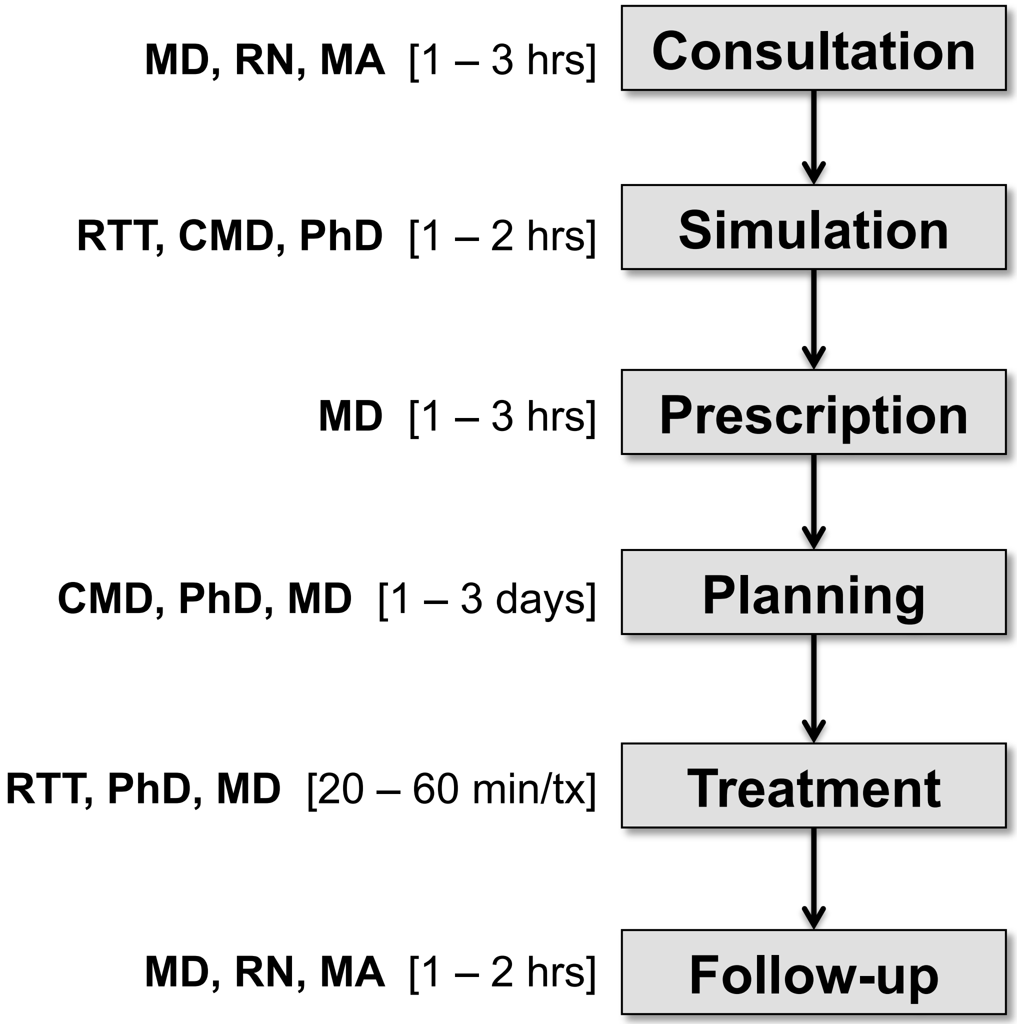
MD [1 – 3 hrs] **Prescription**

CMD, PhD, MD [1 – 3 days] **Planning**

RTT, PhD, MD [20 – 60 min/tx] **Treatment**

MD, RN, MA [1 – 2 hrs] **Follow-up**

Current Problems



MD, RN, MA [1 – 3 hrs] **Consultation**

RTT, CMD, PhD [1 – 2 hrs] **Simulation**

MD [1 – 3 hrs] **Prescription**

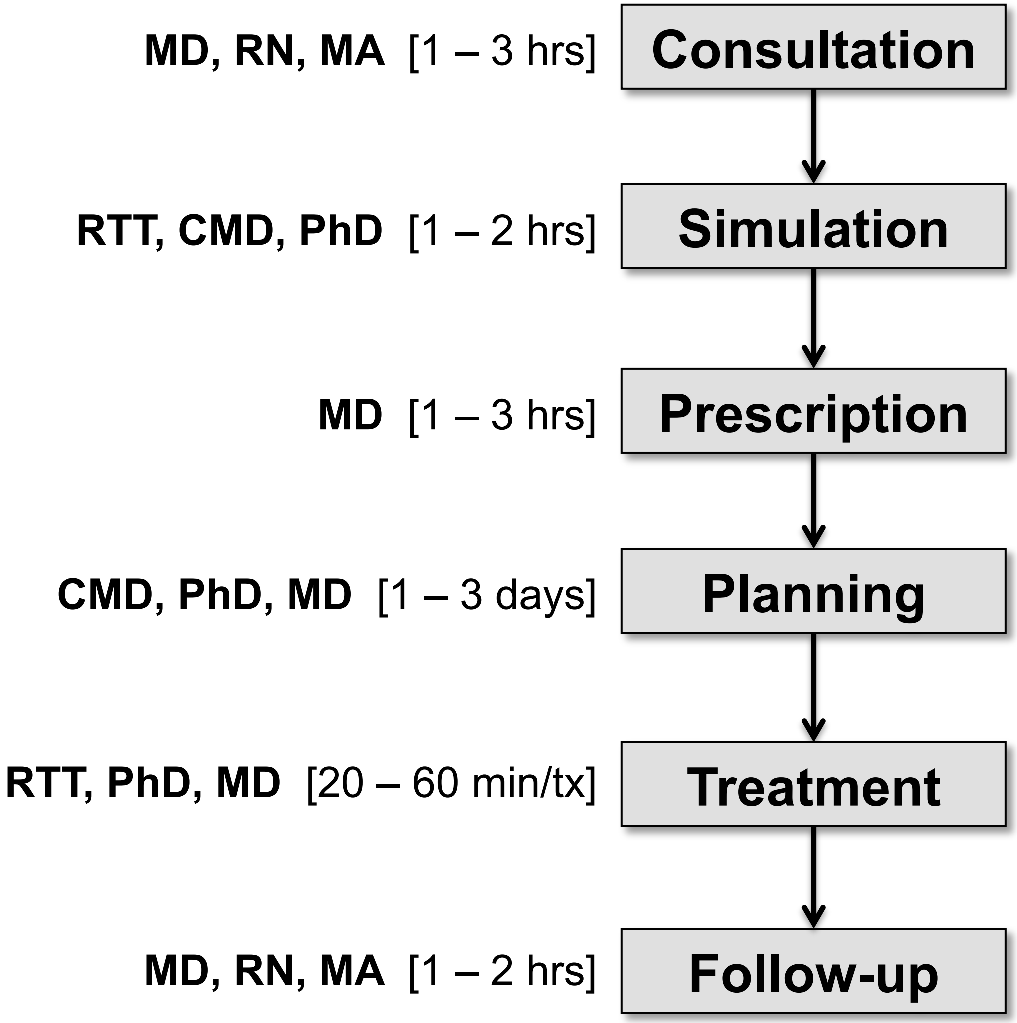
CMD, PhD, MD [1 – 3 days] **Planning**

RTT, PhD, MD [20 – 60 min/tx] **Treatment**

MD, RN, MA [1 – 2 hrs] **Follow-up**

- Several days before patient gets a treatment
- Patient makes several trips to the department
- Error associated with patient setup every day
- Multiple hands-offs over time

Proposed New Procedure



MD, RN, MA [1 – 3 hrs] Consultation

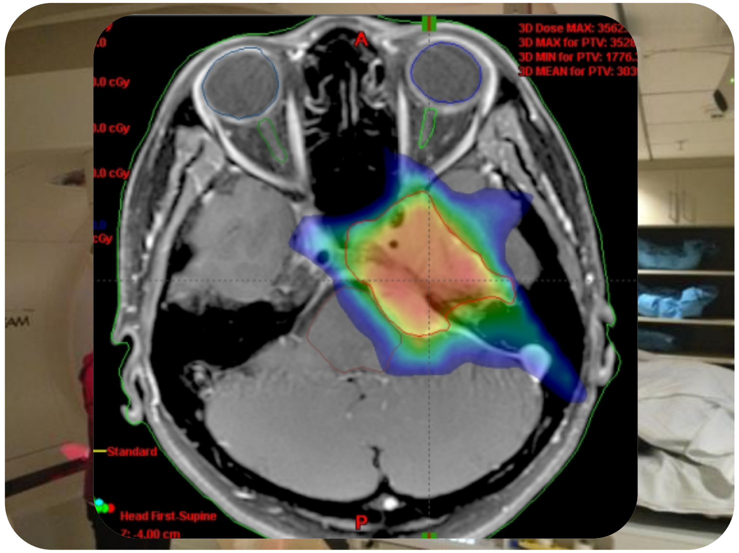
RTT, CMD, PhD [1 – 2 hrs] Simulation

MD [1 – 3 hrs] Prescription

CMD, PhD, MD [1 – 3 days] Planning

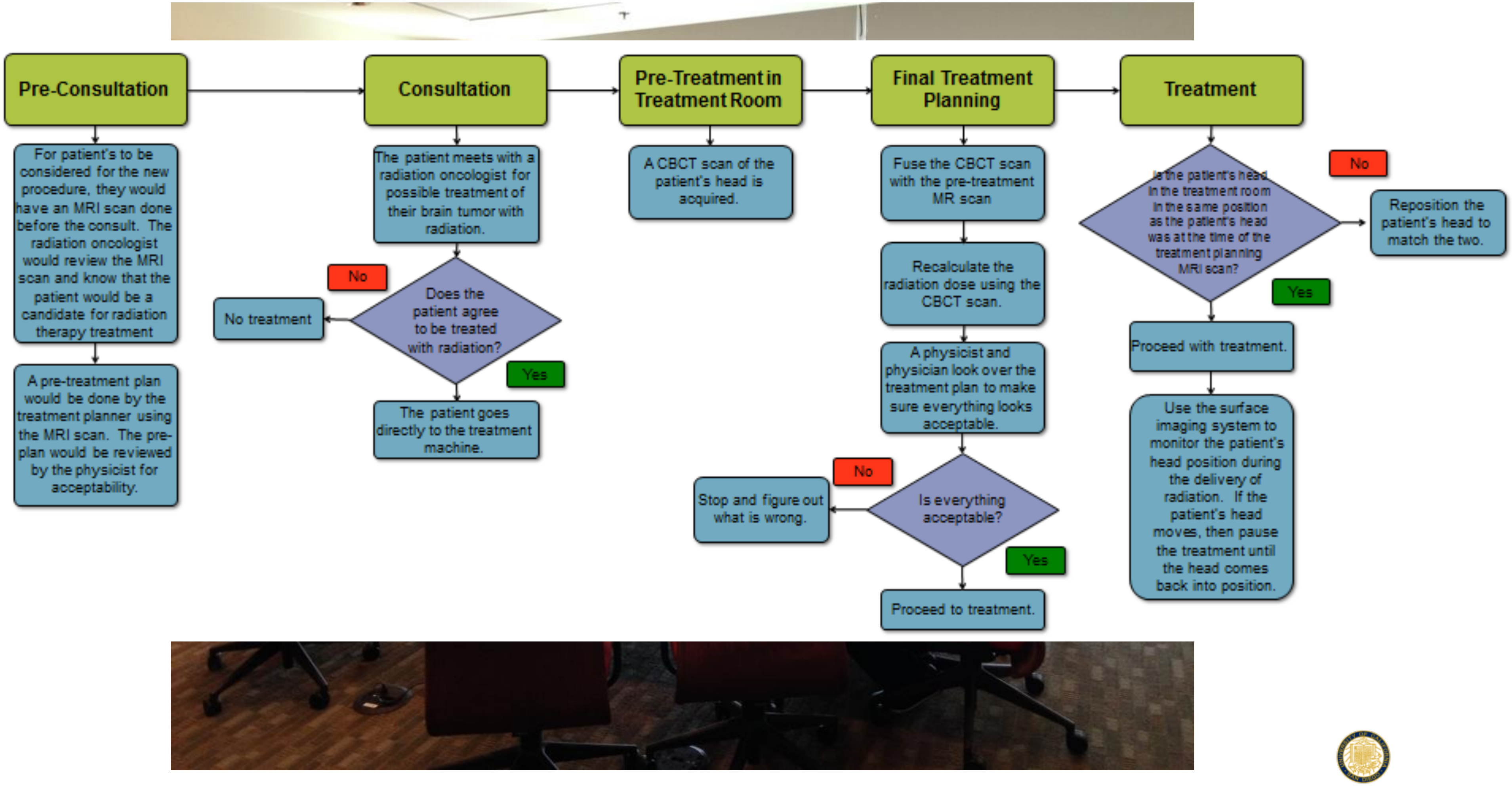
RTT, PhD, MD [20 – 60 min/tx] Treatment

MD, RN, MA [1 – 2 hrs] Follow-up



UC San Diego
RADIATION ONCOLOGY

Our FMEA Approach



Pre-Consultation

For patient's to be considered for the new procedure, they would have an MRI scan done before the consult. The radiation oncologist would review the MRI scan and know that the patient would be a candidate for radiation therapy treatment

A pre-treatment plan would be done by the treatment planner using the MRI scan. The pre-plan would be reviewed by the physicist for acceptability.

Consultation

The patient meets with a radiation oncologist for possible treatment of their brain tumor with radiation.

Does the patient agree to be treated with radiation?

No

No treatment

Yes

The patient goes directly to the treatment machine.

Pre-Treatment in Treatment Room

A CBCT scan of the patient's head is acquired.

Final Treatment Planning

Fuse the CBCT scan with the pre-treatment MR scan

Recalculate the radiation dose using the CBCT scan.

A physicist and physician look over the treatment plan to make sure everything looks acceptable.

Is everything acceptable?

No

Stop and figure out what is wrong.

Yes

Proceed to treatment.

Treatment

Is the patient's head in the treatment room in the same position as the patient's head was at the time of the treatment planning MRI scan?

No

Reposition the patient's head to match the two.

Yes

Proceed with treatment.

Use the surface imaging system to monitor the patient's head position during the delivery of radiation. If the patient's head moves, then pause the treatment until the head comes back into position.

Scales for O, S, and D Values

- Occurrence
  - 10 Very likely to occur (1 in 100)
  - 8 Very likely to occur (1 in 1000)
  - 6 Likely to occur (1 in 10,000)
  - 3 Unlikely to occur (1 in 100,000)
  - 1 Very unlikely to occur (1 in 1,000,000)
- Detection
  - 10 Very unlikely to be able to stop it (1 in 100,000)
  - 8 Very unlikely to be able to stop it (1 in 1,000)
  - 6 Unlikely to be able to stop it (1 in 100)
  - 3 Likely to be able to stop it (1 in 10)
  - 1 Very likely to be able to stop it (1 in 2)
- Severity
  - 10 A dosimetric/volumetric error (>10%)
  - 8 A dosimetric/volumetric error (between 2 and 10%)
  - 6 A dosimetric/volumetric error (<2%)
  - 3 A major workflow issue with no direct patient involvement
  - 1 A minor workflow issue with no direct patient involvement

Failure Modes, O, S, D, and RPNs

- Fuse CBCT scan with pre-treatment MR scan
  - Not fused correctly or done poorly; leads to incorrect treatment
    - **O = 4, S = 10, D = 10; RPN = 400**
  - Wrong patient or wrong scan fused; leads to incorrect treatment
    - **O = 3, S = 8, D = 1; RPN = 24**

- Recalculated dose on CBCT scan
  - Poor quality CBCT leads to incorrect dose
    - **O = 3, S = 8, D = 3; RPN = 72**
  - Homogeneous dose calculation used instead of heterogeneous dose calc.
    - **O = 1, S = 4, D = 6; RPN = 24**

O, S, D, and RPNs

- Physicist plan review
  - Prescription incomplete or ambiguous; leads to incorrect treatment
    - **O = 3, S = 6, D = 6; RPN = 108**

- Physician plan review
  - Different physician reviews the plan
    - **O = 3, S = 10, D = 10; RPN = 300**

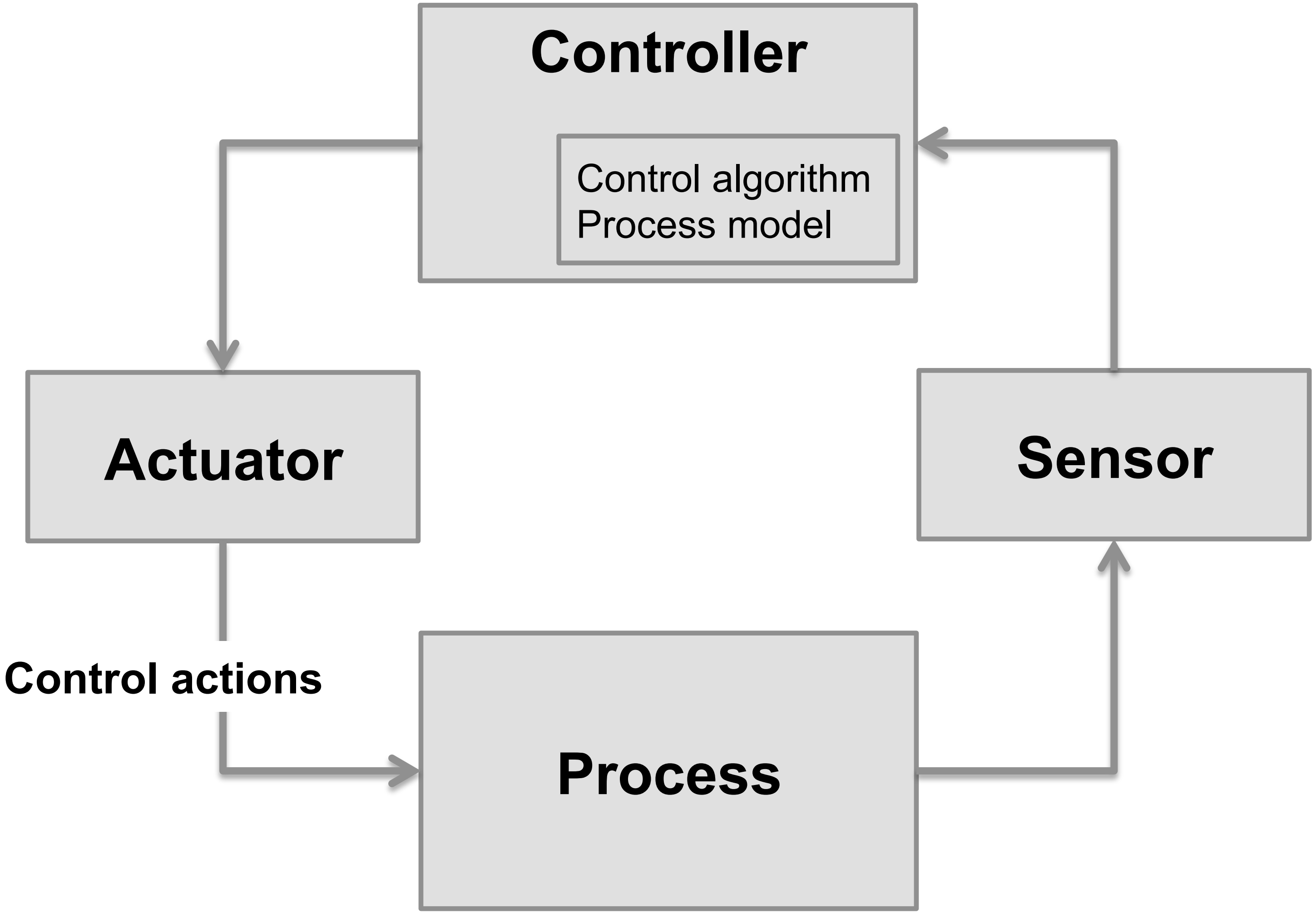
RPN Ranking

- (400) Not fused correctly or done poorly; leads to incorrect treatment
- (300) Different physician reviews the plan
- (108) Prescription incomplete or ambiguous; leads to incorrect tx
- (72) Poor quality CBCT leads to incorrect dose
- (24) Homogeneous dose calculation used instead of hetero calc.
- (24) Wrong patient or wrong scan fused; leads to incorrect treatment

Next Steps for FMEA

- Follow-up on ambiguous failure modes
- Complete O, S, and D scoring and ranking
- Make recommendations on how best to mitigate the highest failure modes

STPA


Controller
Control algorithm
Process model
Actuator
Sensor
Control actions
Process

Accidents (Losses)

A1: Patient injured or killed from radiation exposure

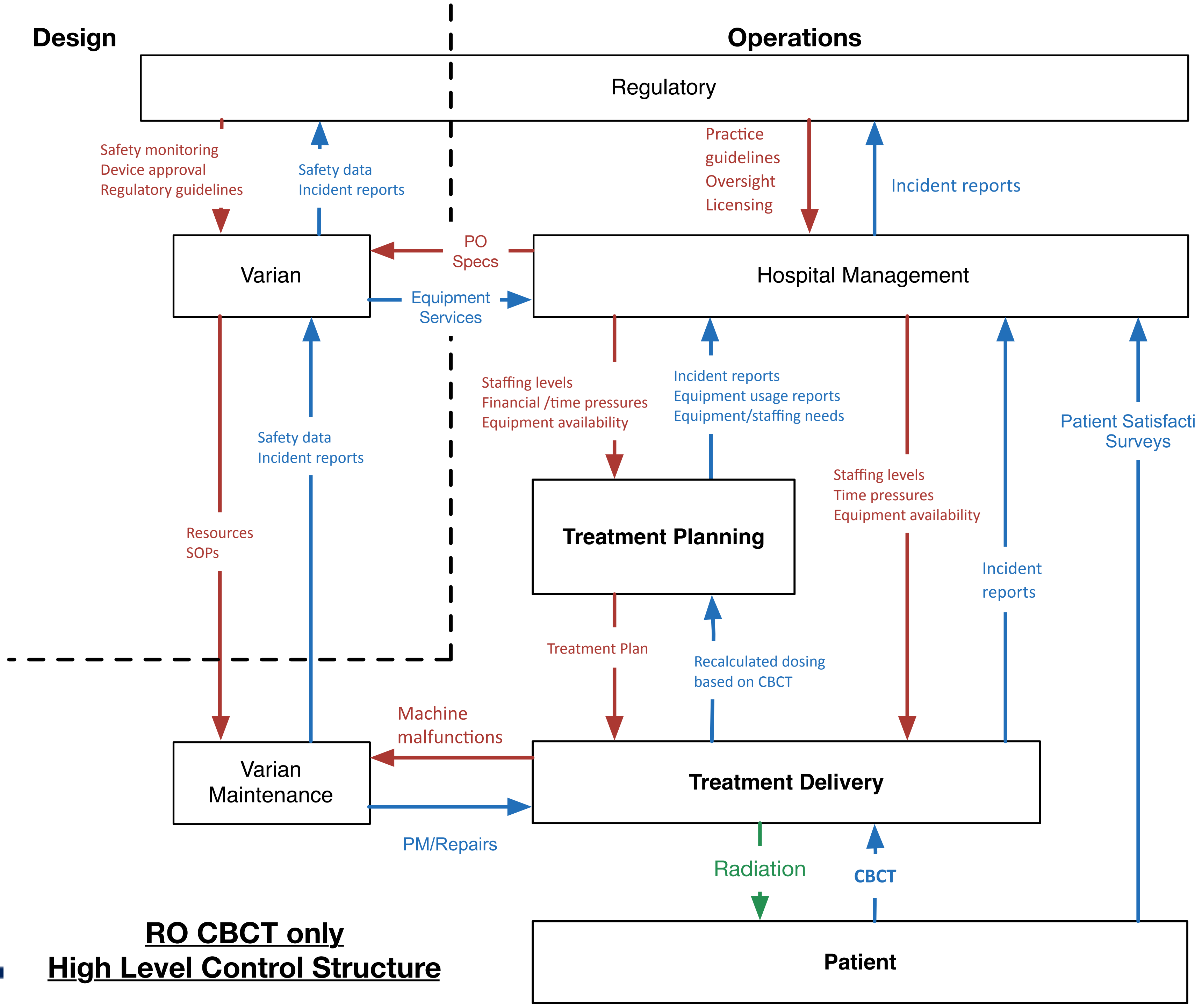
A2: Staff injured or killed by radiation

A3: Damage to equipment

A4: Physical injury to patient or staff during treatment (not from radiation)

High Level Hazards

- **H1** Wrong Dose
  - Dose delivered to patient is wrong in either amount, location, or timing
    - 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** Staff is unnecessarily exposed to radiation
- **H3** Equipment is subject to unnecessary stress
- **H4** Persons are subjected to the possibility of non-radiological injury



Design

Operations

Regulatory

Safety monitoring
Device approval
Regulatory guidelines

Safety data
Incident reports

Practice
guidelines
Oversight
Licensing

Incident reports

Varian

PO
Specs

Equipment
Services

Hospital Management

Staffing levels
Financial /time pressures
Equipment availability

Incident reports
Equipment usage reports
Equipment/staffing needs

Safety data
Incident reports

Patient Satisfaction
Surveys

Staffing levels
Time pressures
Equipment availability

Resources
SOPs

Treatment Planning

Incident
reports

Treatment Plan

Recalculated dosing
based on CBCT

Machine
malfunctions

Varian
Maintenance

Treatment Delivery

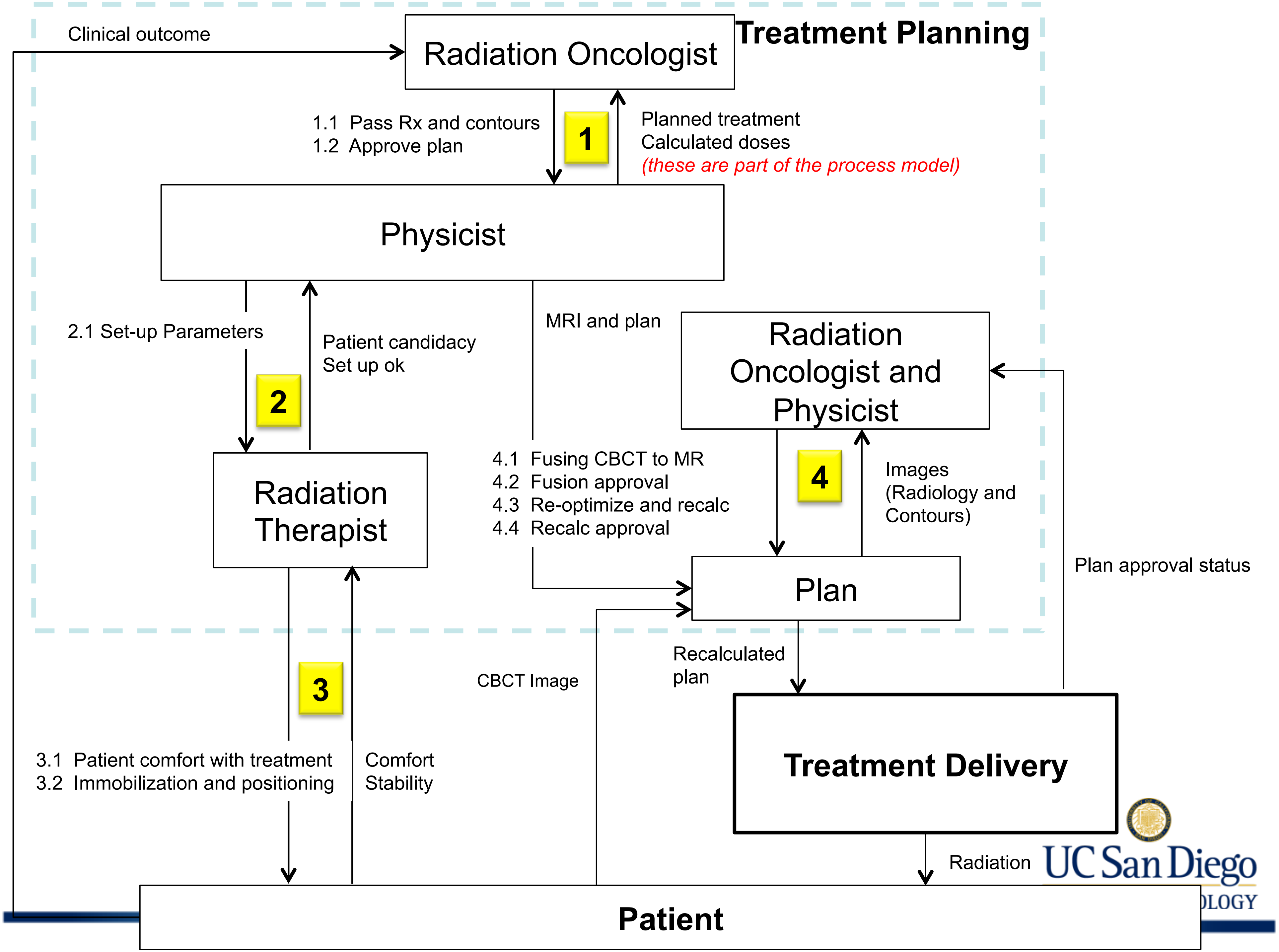
PM/Repairs

Radiation

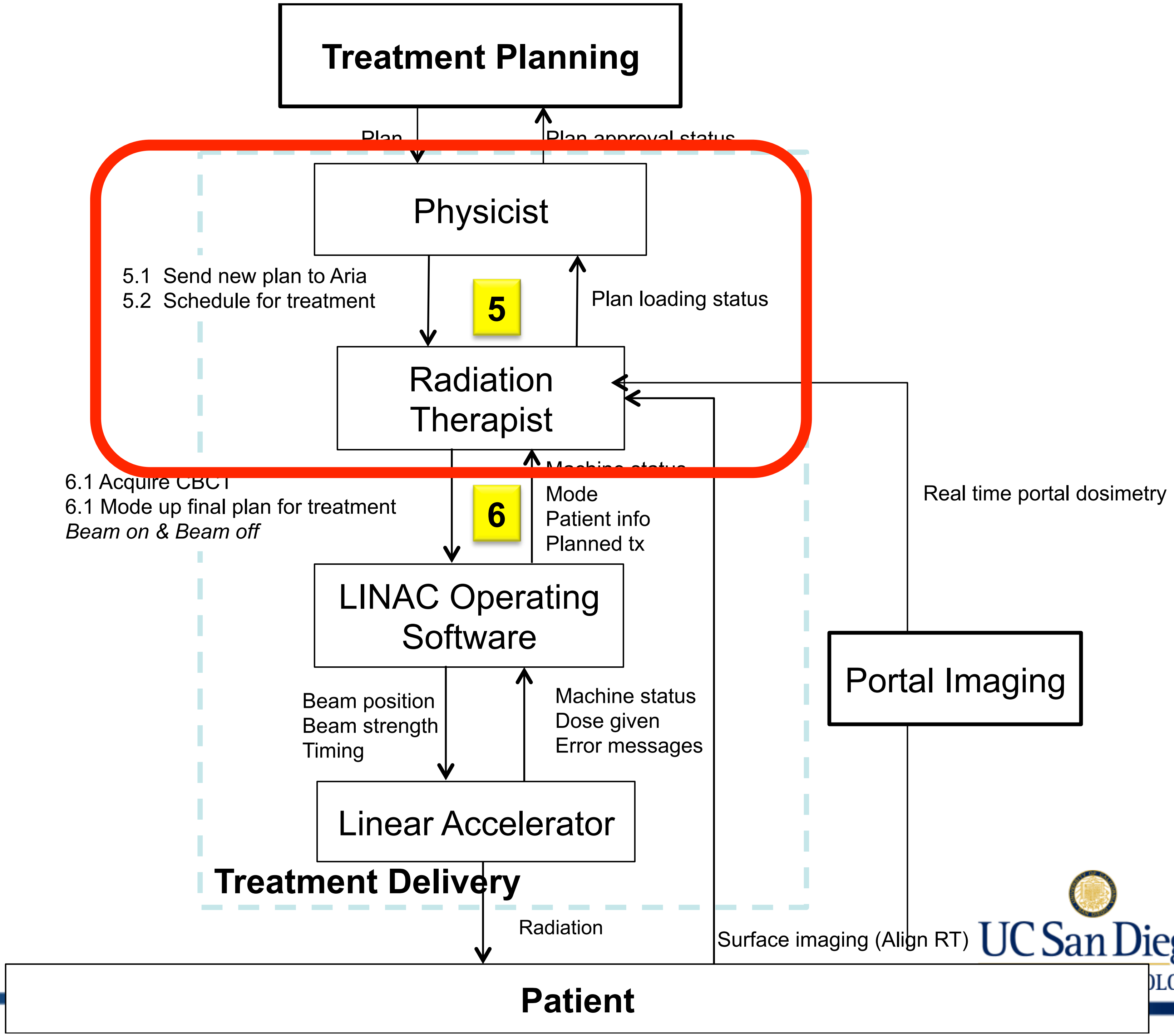
CBCT

Patient

RO CBCT only
High Level Control Structure



UC San Diego
[illegible]OLOGY



Treatment Planning

Plan

Plan approval status

Physicist

5.1 Send new plan to Aria
5.2 Schedule for treatment

5

Plan loading status

Radiation Therapist

6.1 Acquire CBCT
6.1 Mode up final plan for treatment
Beam on & Beam off

6

Machine status
Mode
Patient info
Planned tx

LINAC Operating Software

Beam position
Beam strength
Timing

Machine status
Dose given
Error messages

Linear Accelerator

Treatment Delivery

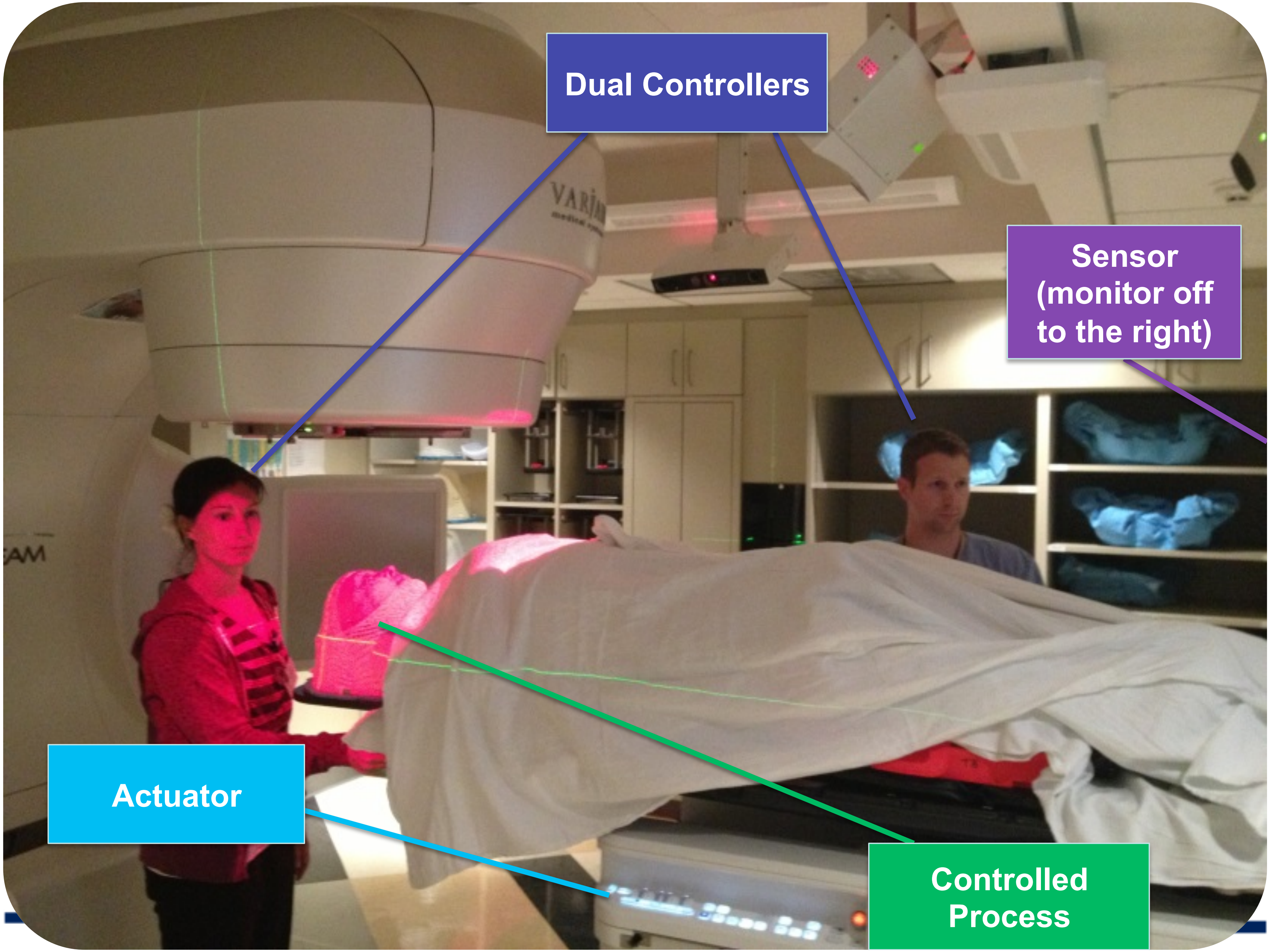
Radiation

Surface imaging (Align RT)

Real time portal dosimetry

Portal Imaging

Patient



Dual Controllers

Sensor (monitor off to the right)

Actuator

Controlled Process

STPA Step 1 – Approach

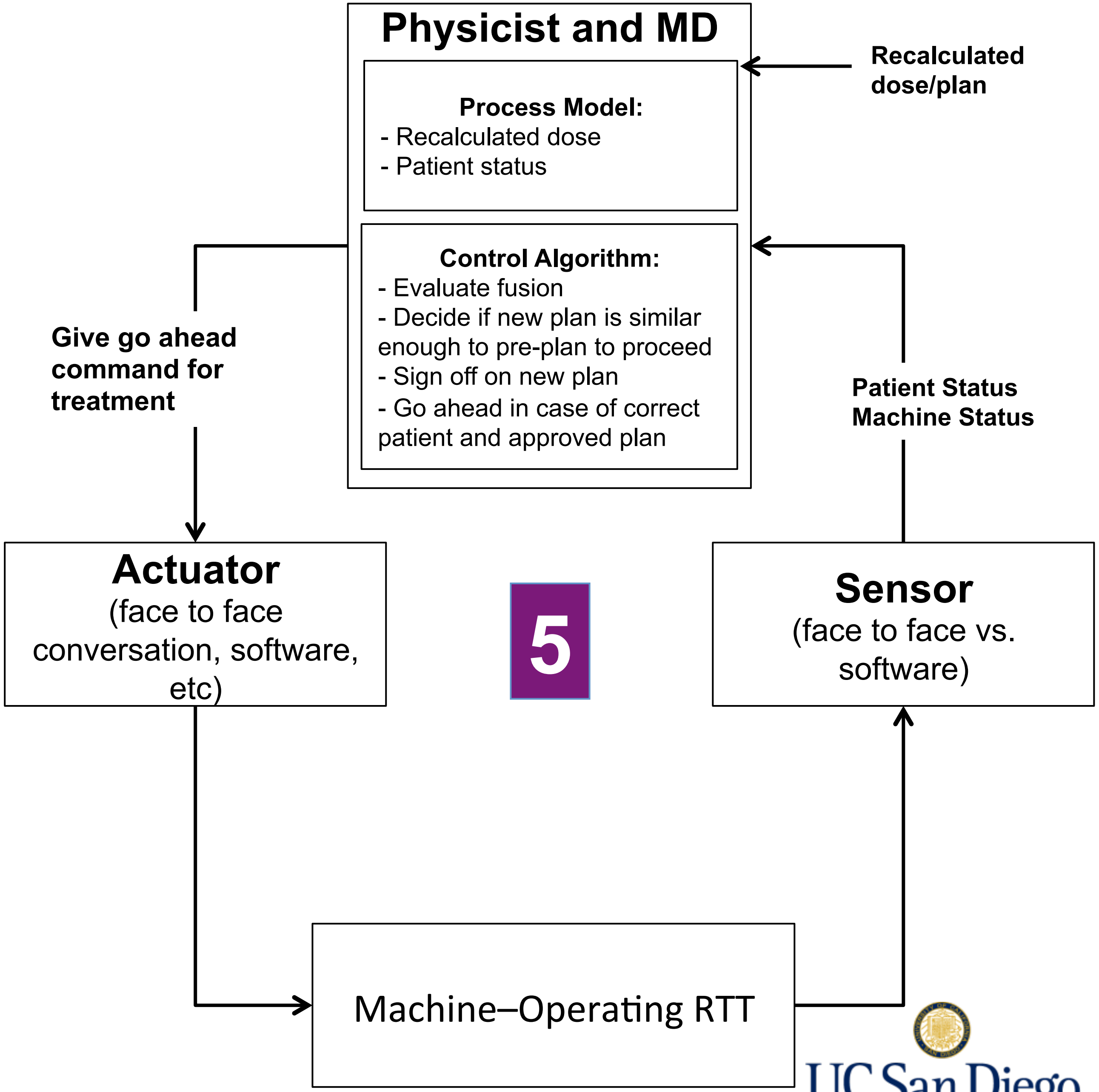
- We analyzed the system from a differential perspective
  - What is different in this new workflow compared to the existing workflow?

- This helped focus us on particular pieces of the system that were most relevant to UCSD

- We completed typical Step 1 tables for each loop in the structure

Process Map

1. Physicist fuses CBCT to MRI scan and checks contours
2. Physicist creates a new plan using CBCT
3. Physicist checks the new plan and treatment parameters
4. Physician reviews and approves/rejects the contours and new plan
5. Physician and physicist give go ahead command for treatment



Physicist and MD

Process Model:
- Recalculated dose
- Patient status

Control Algorithm:
- Evaluate fusion
- Decide if new plan is similar enough to pre-plan to proceed
- Sign off on new plan
- Go ahead in case of correct patient and approved plan

Recalculated dose/plan

Give go ahead command for treatment

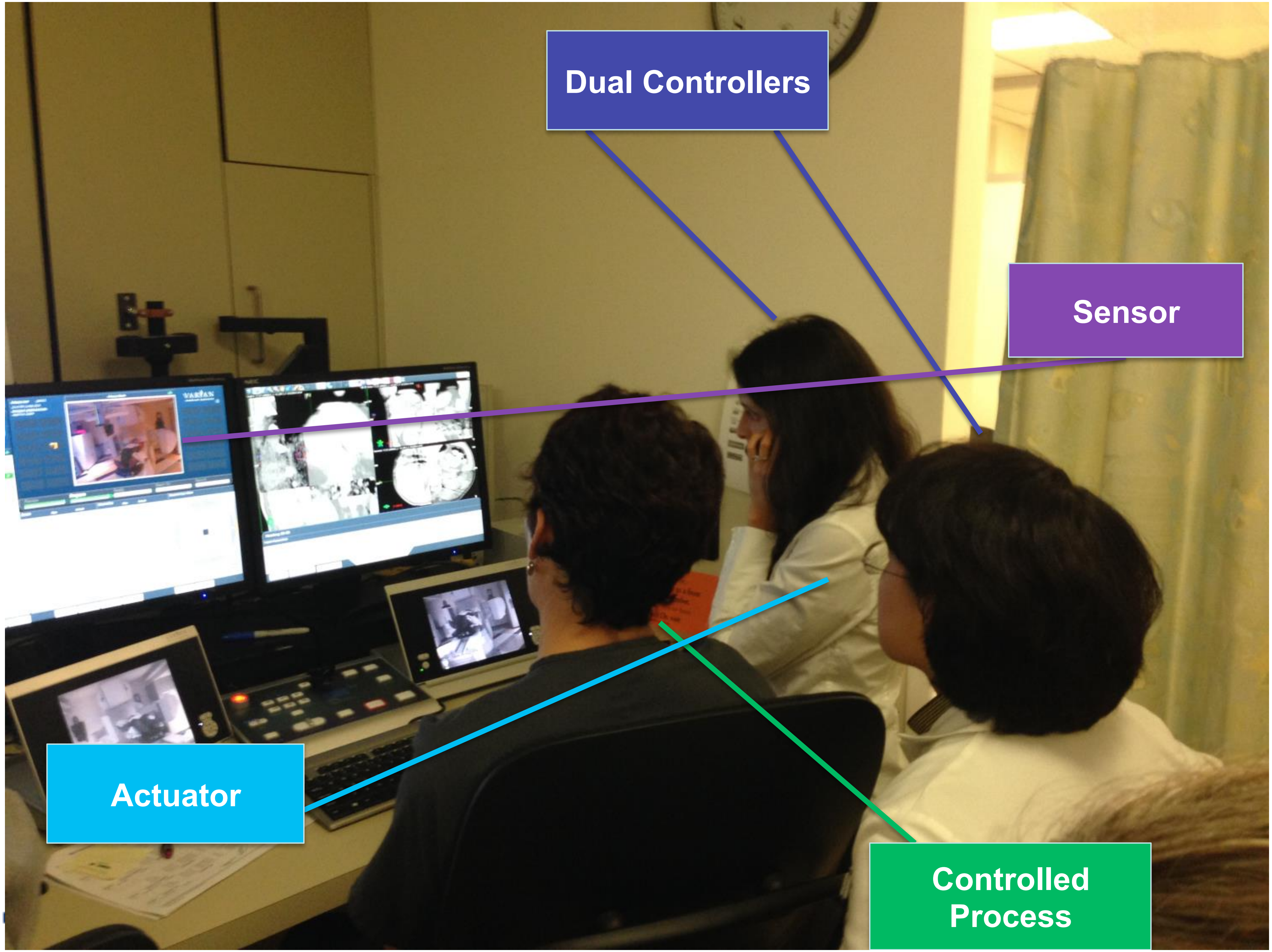
Patient Status
Machine Status

Actuator
(face to face conversation, software, etc)

5

Sensor
(face to face vs. software)

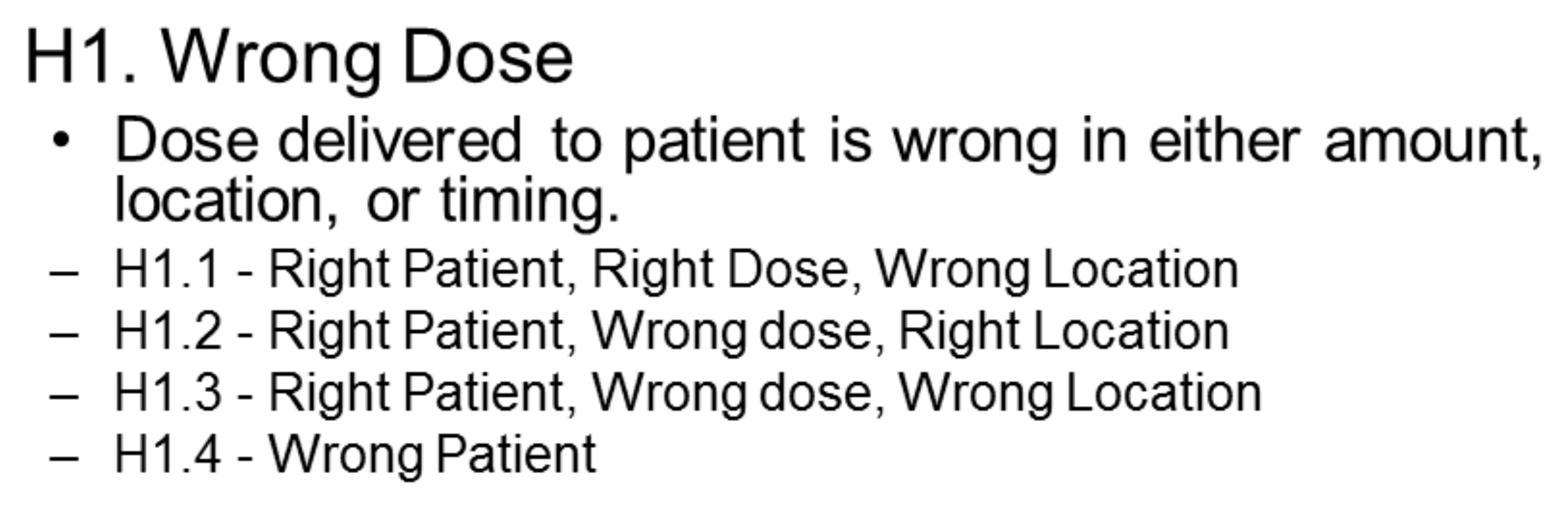
Machine–Operating RTT


Dual Controllers
Sensor
Actuator
Controlled Process

STPA Step 1

5

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/ Order Causes Hazard	Stopped Too Soon or Applied Too



H1. Wrong Dose

- Dose delivered to patient is wrong in either amount, location, or timing.
  - 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

STPA Step 1 – Results 5

- Found 40 Unsafe Control Actions out of 9 control actions analyzed

- Example of unsafe control actions (UCAs)
  - Incomplete file transfer: implicated in prior overdoses during treatment
  - **Recalculated plan approval takes too long**
    - This balances time pressure in making this decision with the constraint that the patient simply cannot remain motionless that long

STPA Step 2 – Process 5

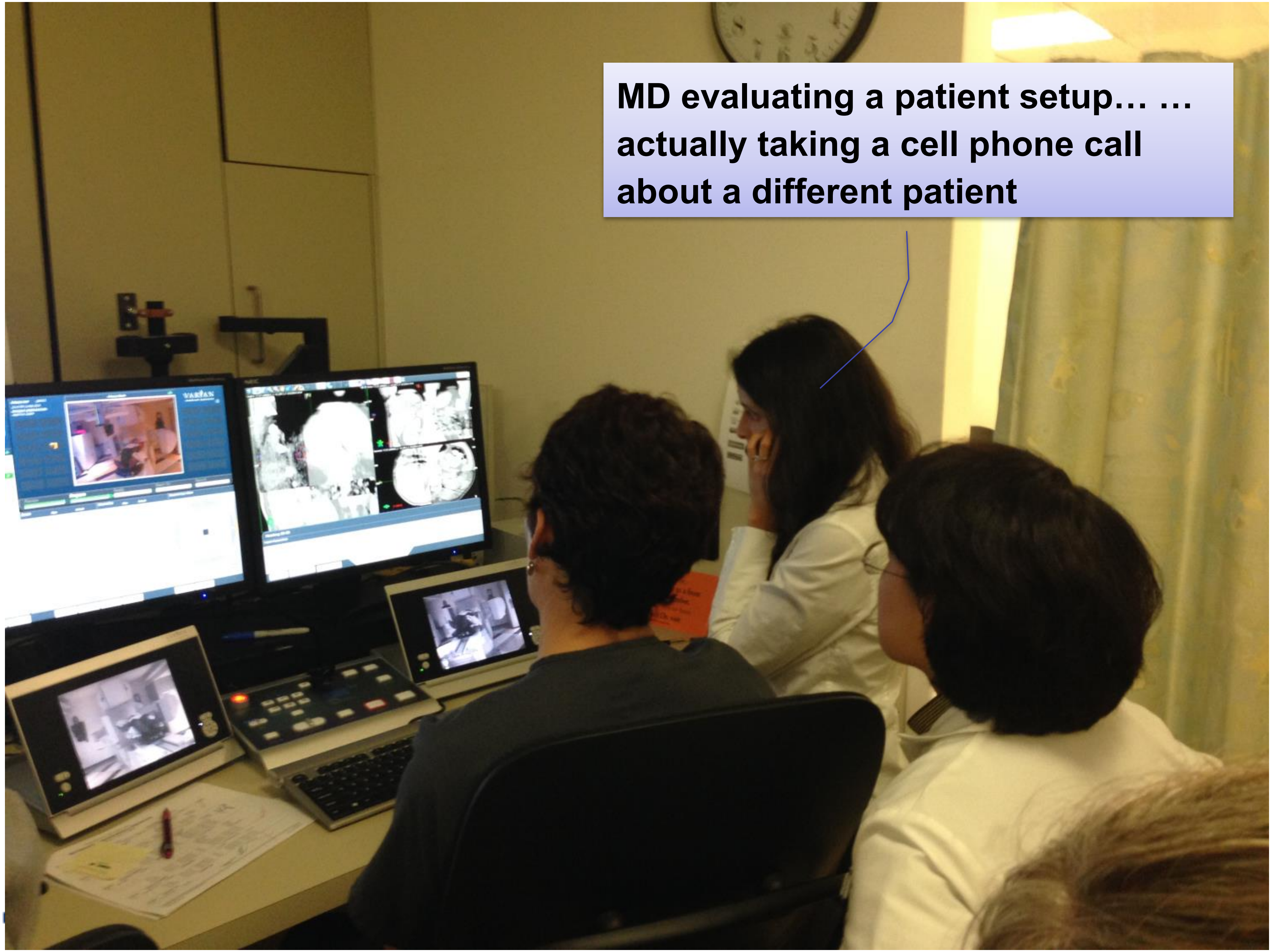
- MIT served as facilitators to walk UCSD through the control loop
  - Loops completed in random order to focus the scenarios to the UCA being analyzed
- Used spreadsheets
  - Links the scenarios to the UCA, the position in the control loop, and the hazard
  - Helpful for translating these into safety constraints for each role in the system

STPA Step 2 – Results

5

Unsafe Control Action: Wrong re-calculation plan issued

Scenario for Algorithm	*Associated Hazard*
MD looks at wrong patient description	1.3
Data corrupted during analysis	1.1
Head sides "flipped" during analysis	1.2
Image is corrupted	1.1
Wrong patient	1.3
Wrong patient as multiple cases are worked on simultaneously	1.3
Reviewed plan inadequately (comprehensive review not done)	1.1
Mistakes caused by time pressure to get analysis done before patient moves	1.1
MD/PhD interaction: MD says go, PhD has reservations but feels PhD cannot speak up	1.1
MD and PhD in different locations and **have low quality discussion about approving re-calculation plan**	1.1
Review MR fusion to CBCT, decides it is close enough and it isn’t	1.1



MD evaluating a patient setup… …
actually taking a cell phone call
about a different patient

Constraints and Requirements

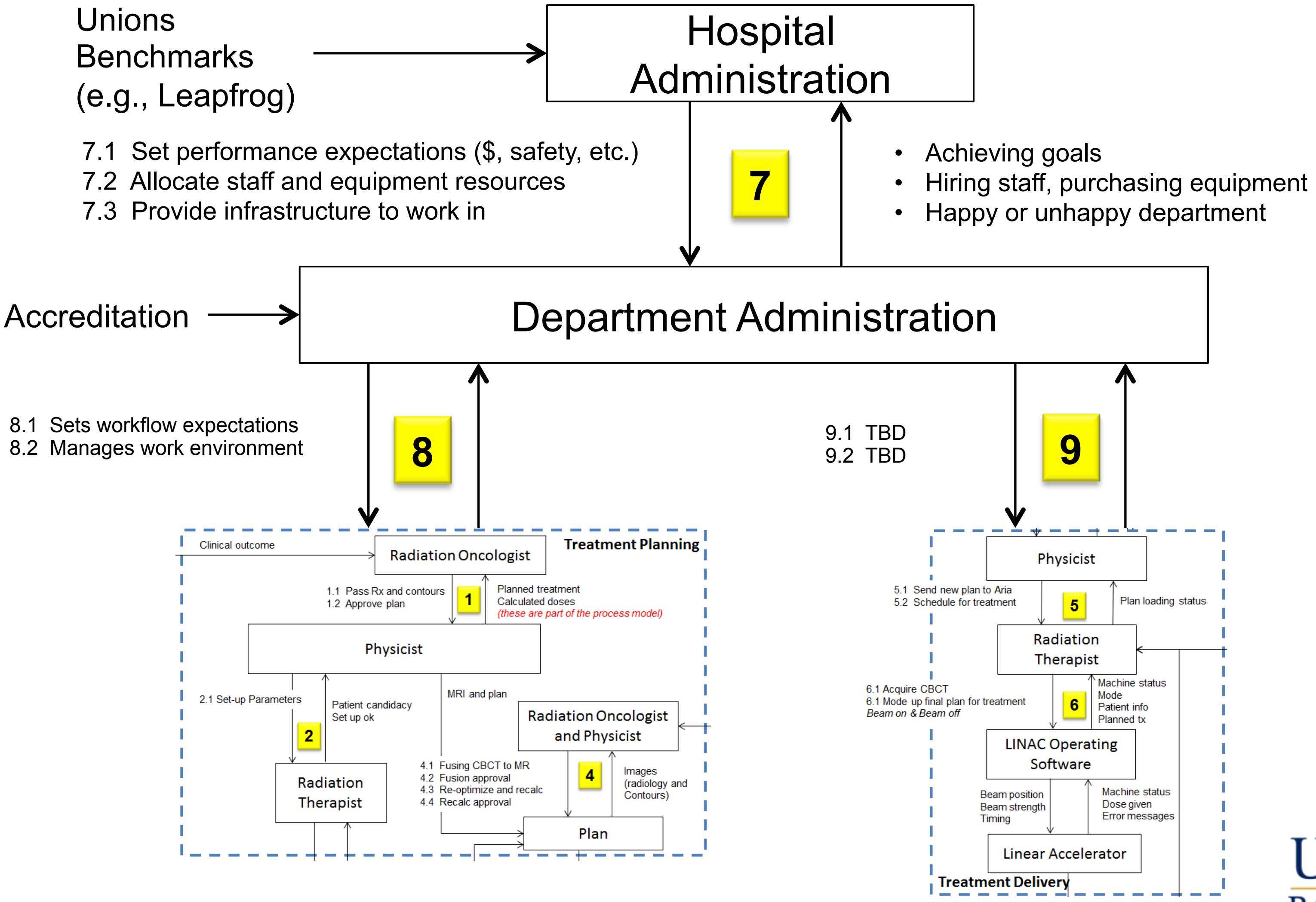
- Step 2 scenarios translated into either constraints or design requirements
- General principle:
  - Write constraints for each person or piece of equipment
  - Break it down by function
  - Include the intention behind the constraint

Software Requirements – Example

- **R–8**
  - Software must complete calculations within 2 minutes

- Intent
  - There are no good studies out there looking at how long patients can remain in one position.
  - We have anecdotal evidence from a previous related study that healthy volunteers can remain still (within 1.5 mm and 0.5 degrees) for about 20 min.
  - Therefore, adding two minutes to the total procedure time is reasonable time lengthen of the procedure for the extra step.

Expand Analysis



Unions
Benchmarks
(e.g., Leapfrog)

Hospital Administration

7.1 Set performance expectations ($, safety, etc.)
7.2 Allocate staff and equipment resources
7.3 Provide infrastructure to work in

7

- Achieving goals
- Hiring staff, purchasing equipment
- Happy or unhappy department

Accreditation

Department Administration

8.1 Sets workflow expectations
8.2 Manages work environment

8

9.1 TBD
9.2 TBD

9

Treatment Planning

Clinical outcome

Radiation Oncologist

1.1 Pass Rx and contours
1.2 Approve plan

1

Planned treatment
Calculated doses
(these are part of the process model)

Physicist

2.1 Set-up Parameters

2

Patient candidacy
Set up ok

Radiation Therapist

MRI and plan

Radiation Oncologist and Physicist

4.1 Fusing CBCT to MR
4.2 Fusion approval
4.3 Re-optimize and recalc
4.4 Recalc approval

4

Images
(radiology and Contours)

Plan

Physicist

5.1 Send new plan to Aria
5.2 Schedule for treatment

5

Plan loading status

Radiation Therapist

6.1 Acquire CBCT
6.1 Mode up final plan for treatment
Beam on & Beam off

6

Machine status
Mode
Patient info
Planned tx

LINAC Operating Software

Beam position
Beam strength
Timing

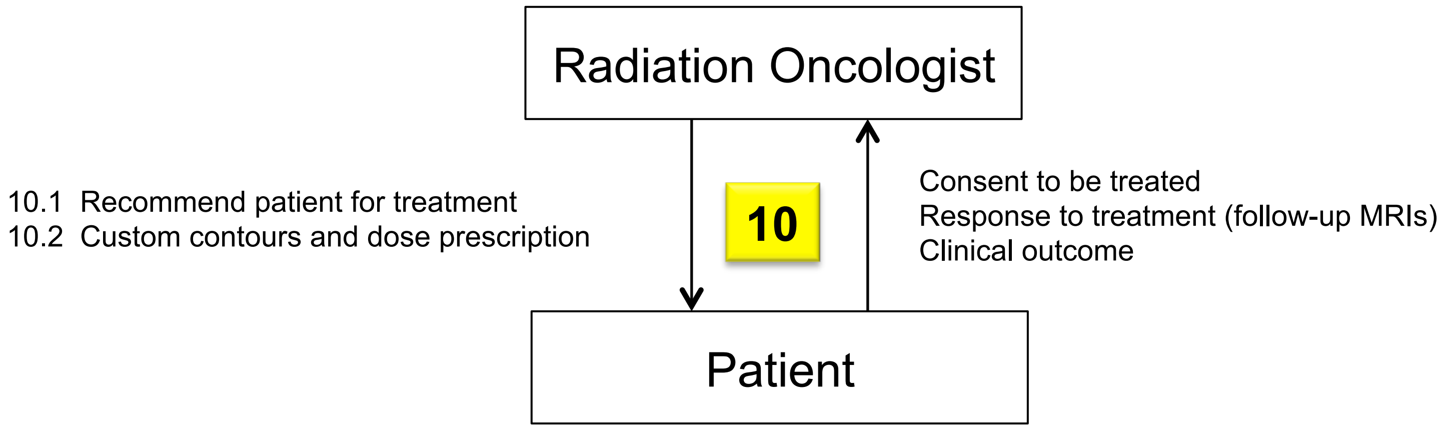
Machine status
Dose given
Error messages

Linear Accelerator

Treatment Delivery

UC San Diego
RADIATION ONCOLOGY

Expand Analysis



Radiation Oncologist

10.1 Recommend patient for treatment
10.2 Custom contours and dose prescription

10

Consent to be treated
Response to treatment (follow-up MRIs)
Clinical outcome

Patient

Impressions of the Techniques

FMEA	STPA
Treats safety as a probabilistic failure problem	Treats safety as a hierarchical control problem
Component focused	Systems focused
Relatively simple	Complicated
Can be time consuming	Definitely time consuming

Summary

- More patients are at risk from poor quality than we may realize (quality trap)

- For non-engineers, performing an STPA is more complex than FMEA
  - May hinder acceptance and use

- No “show stoppers” have been identified for the new radiosurgery treatment approach
  - But will require redesign of some well established processes