

# First experiences with STPA in a Radiation Oncology Department

---

J. Daartz, J Kang



MASSACHUSETTS  
GENERAL HOSPITAL  
RADIATION ONCOLOGY



HARVARD  
MEDICAL SCHOOL

**Volpe**

The National Transportation Systems Center

# Overview

In collaboration with J. Kang (Volpe)

- Conducted STPA of a part of routine clinical workflow at MGH
- Repeated with the introduction of new software
- Used SafetyHat for analysis

Safety **HAT**



Volpe



## Disclaimer

The views expressed in this presentation are those of the authors and do not necessarily represent the official policy or position of the U.S. Department of Transportation or U.S. Government.

## Introduction

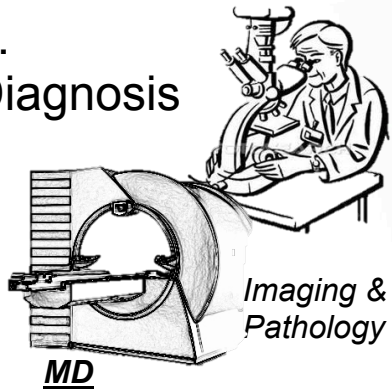
Radiotherapy has evolved fairly rapidly since use of CT became routine

For the majority of patients the process now looks something like this:

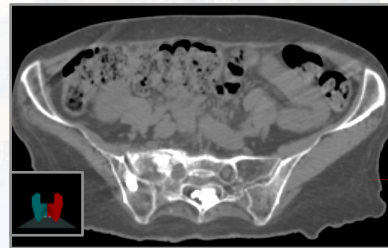


# Introduction

## 1. Diagnosis

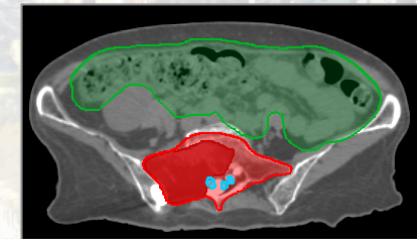


## 2. CT for treatment planning



CT Technicians

## 3. Target definition



more Imaging  
MD

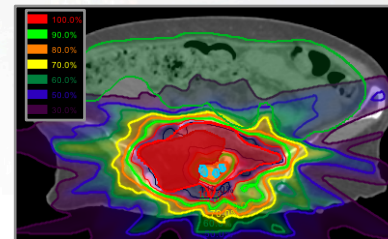


## 5. Treatment(s)



Radiotherapy Technicians

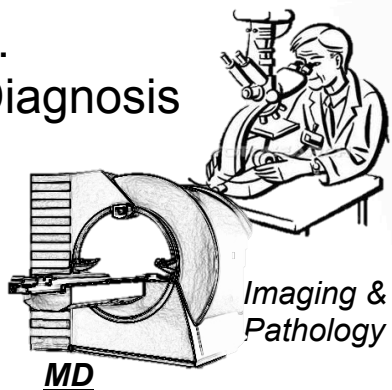
## 4. Treatment planning



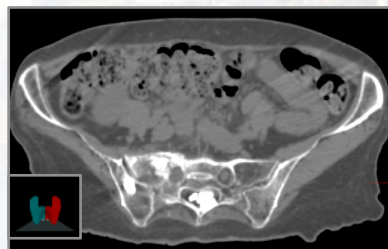
Dosimetrists & Physicists

# Introduction

## 1. Diagnosis

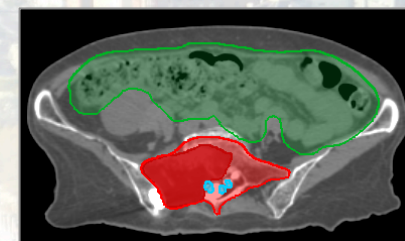


## 2. CT for treatment planning



CT Technicians

## 3. Target definition



more  
Imaging

MD

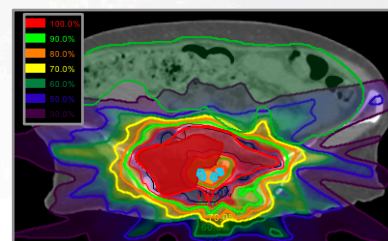


## 5. Treatment(s)



Radiotherapy  
Technicians

## 4. Treatment planning



Dosimetrists &  
Physicists

0.  
Behind the Scenes:  
QA, upgrades, maintenance



# Introduction

Problem:

each of those steps happens in its own environment: different vendors, own data bases, software, data transfer protocols, ...

1.  
Diagnosis

2.  
CT for  
treatment  
planning

3.  
Target  
definition

4.  
Treatment  
planning

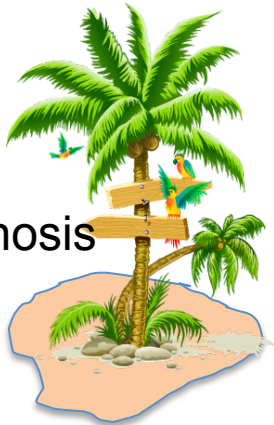
5.  
Treatment(s)

# Introduction

## Problem:

each of those steps happens in its own environment: different vendors, own data bases, software, data transfer protocols, ... in short, each island owns its own representation of the patient

1.  
Diagnosis



2.  
CT for  
treatment  
planning



3.  
Target  
definition



4.  
Treatment  
planning



5.  
Treatment(s)

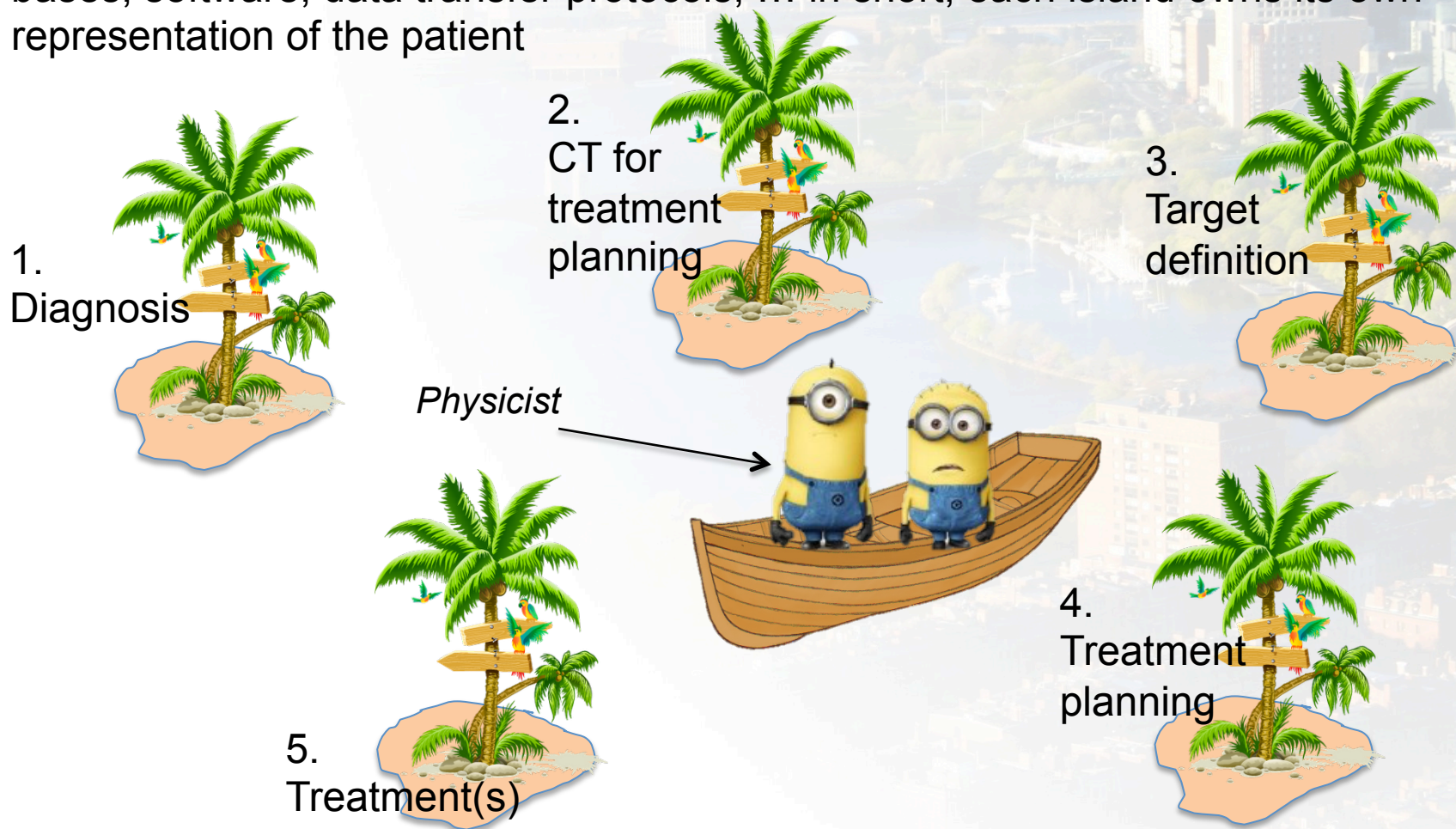




# Introduction

## Problem:

each of those steps happens in its own environment: different vendors, own data bases, software, data transfer protocols, ... in short, each island owns its own representation of the patient



## Introduction

The interconnectivity problem causes a large fraction of the problems we are facing in Radiotherapy.



## Introduction

The interconnectivity problem causes a large fraction of the problems we are facing in Radiotherapy.

For instance:  
ensuring the patient is treated based on the correct CT

## Introduction

The interconnectivity problem causes a large fraction of the problems we are facing in Radiotherapy.

For instance:

ensuring the patient is treated based on the correct CT

there are multiple pathways for this error scenario, e.g.:

- treatment plan done on a scan acquired for a prior treatment
- multiple CTs acquired in the same CT session
- used CT of a different patient with same diagnosis
- ....



# Introduction

## State of affairs

# Introduction

## State of affairs

Two major efforts to improve:

- data format: DICOM 2<sup>nd</sup> generation -> to standardize the kind of information recorded
- interoperability: IHE-RO -> to standardize the interpretation of the DICOM standard



# Introduction

## State of affairs

Two major efforts to improve:

- data format: DICOM 2<sup>nd</sup> generation -> to standardize the kind of information recorded
- interoperability: IHE-RO -> to standardize the interpretation of the DICOM standard

What about hazard analysis?

- practically non-existent in RadOnc clinics
- professional organizations (AAPM, ASTRO) are beginning to advocate for hazard analysis of all clinical workflows (e.g. AAPM TG 100)

## STPA - Motivation

We decided to use STPA is the promise of improved applicability to systems built of a large number of independent hardware/software and human components.

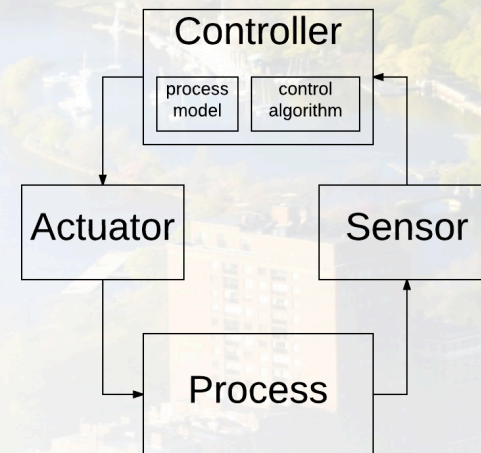
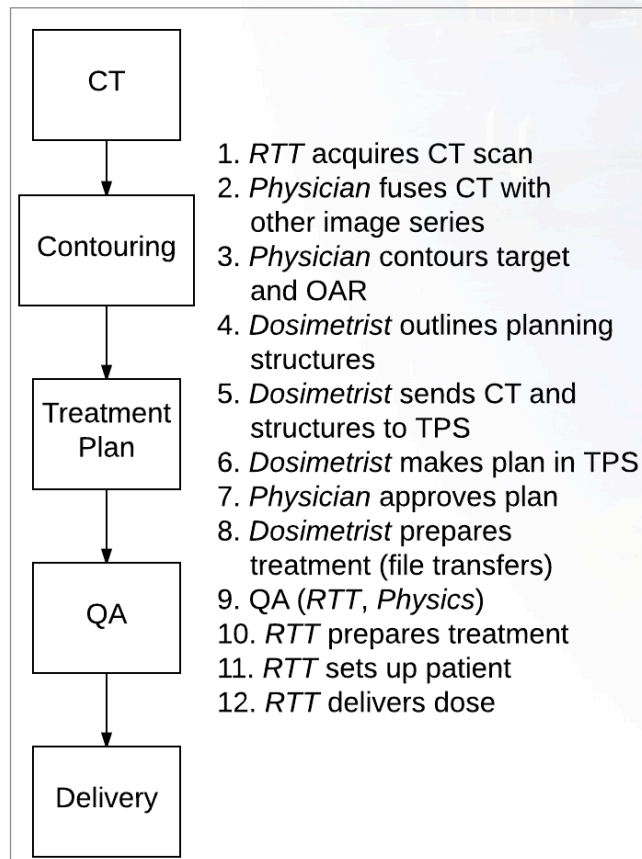
Also of note, we are physicists, not safety engineers. So whatever method we use has to be doable by non-experts.

SafetyHat promised easy execution of the analysis.



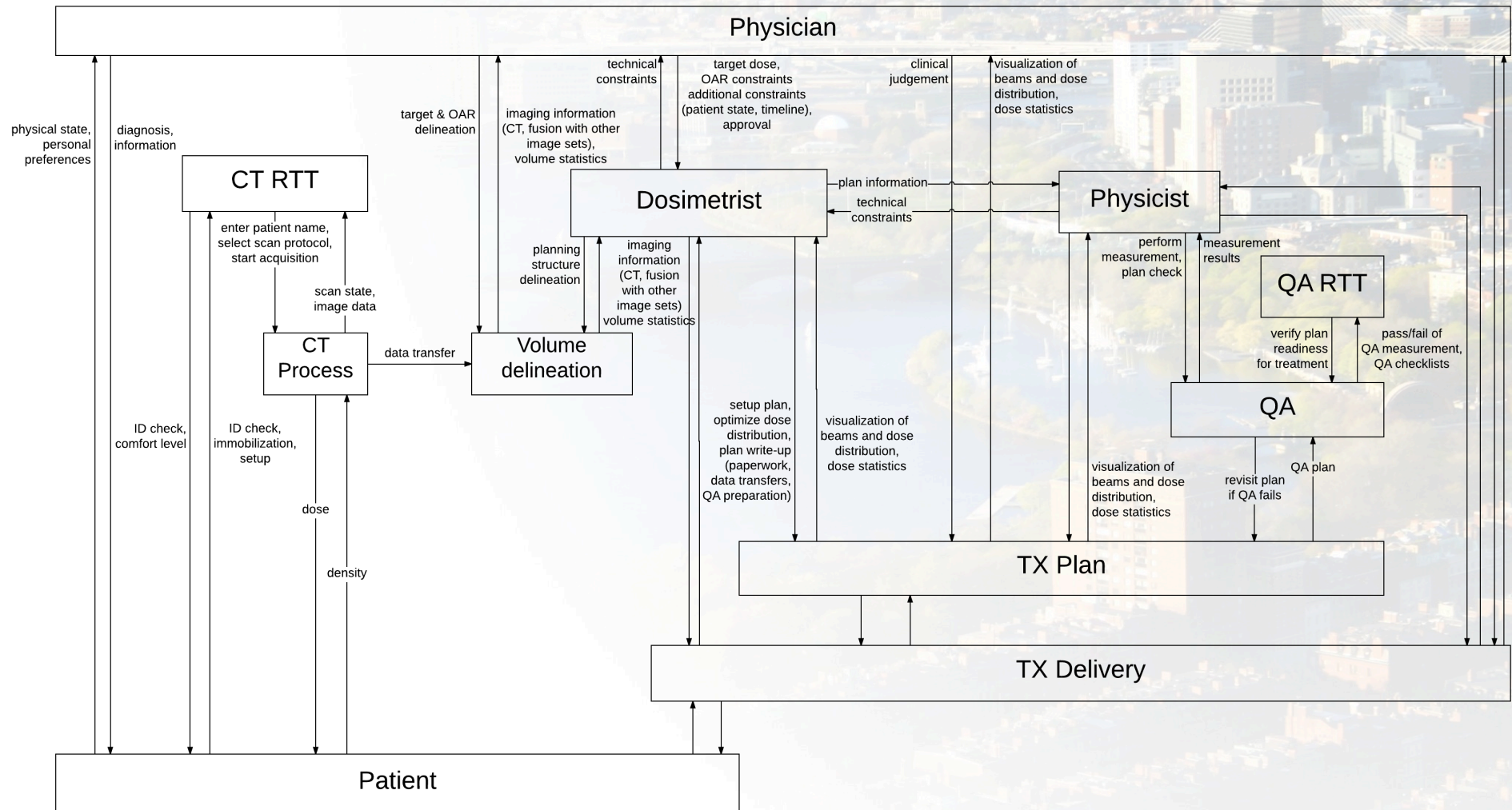
## STPA – Control Diagram

Learning curve:  
start with process map, evolve to control  
diagram that follows the basic STPA structure



# STPA – Control Diagram

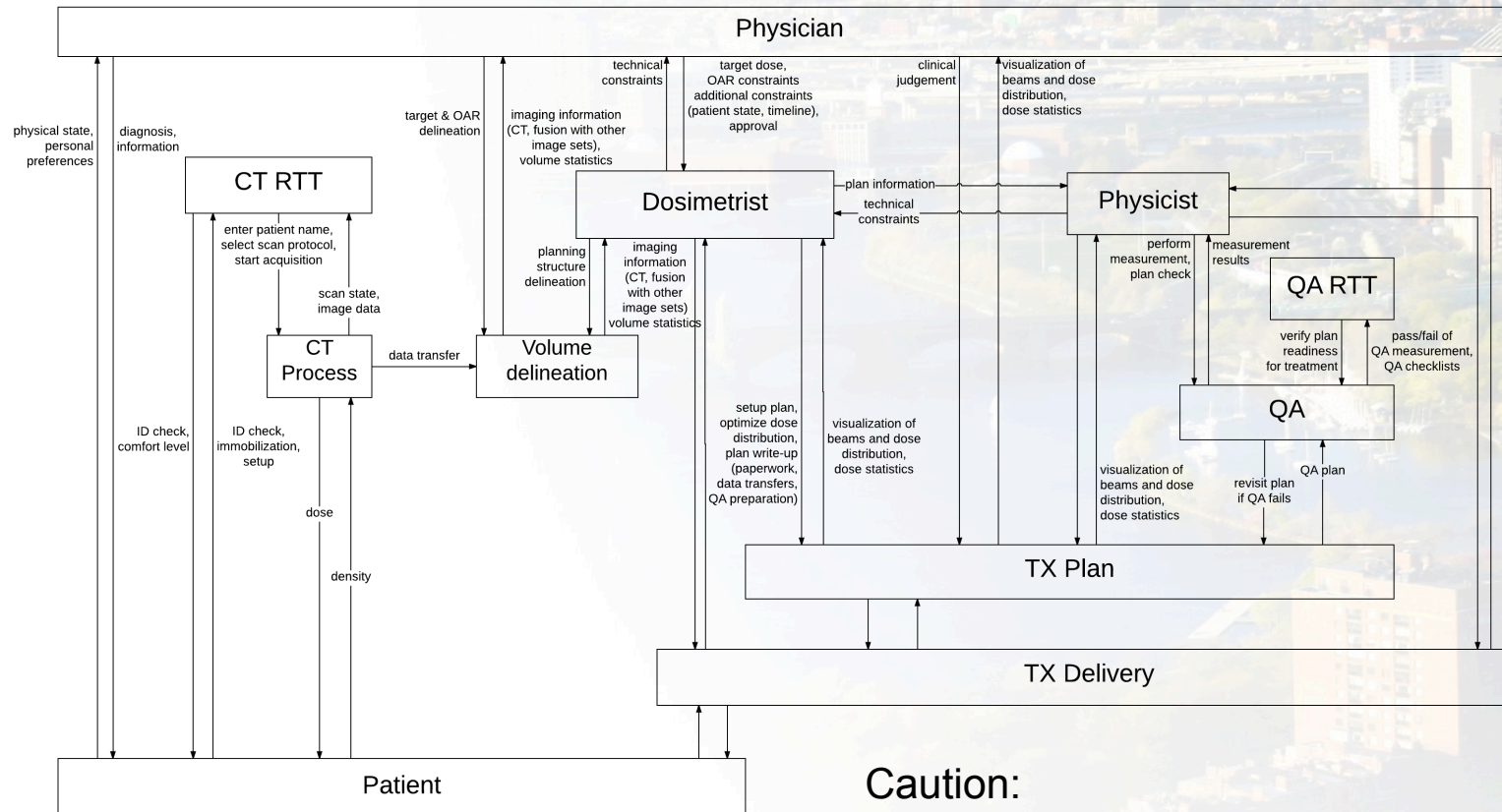
## Focus on: Treatment Planning





# STPA – Control Diagram

## Focus on: Treatment Planning

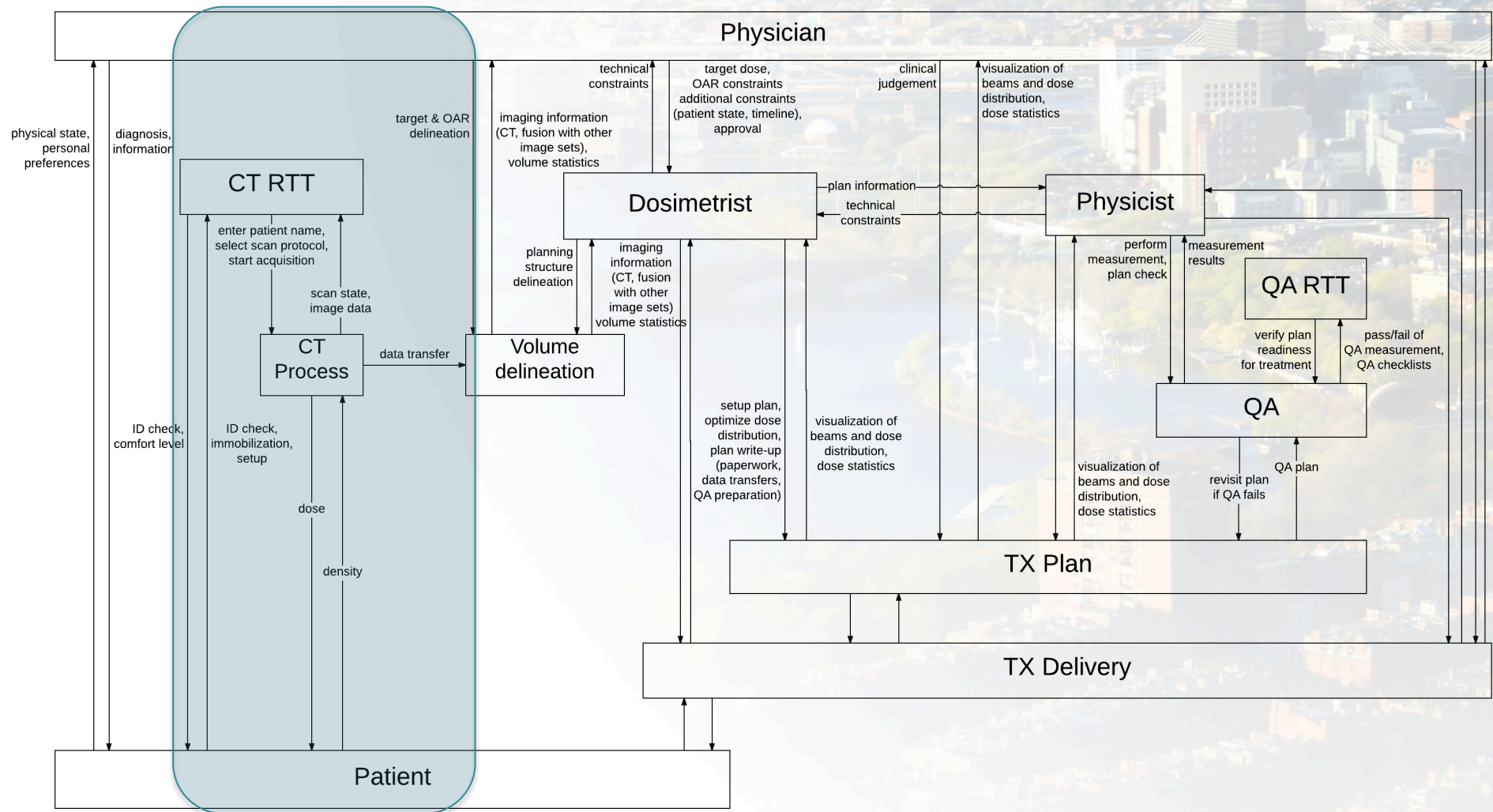


### Caution:

- squeezing too much detail into one diagram
- when creating higher-resolution diagrams it is easy to lose connections
- bias of preparer will influence the diagram

# STPA – Control Diagram

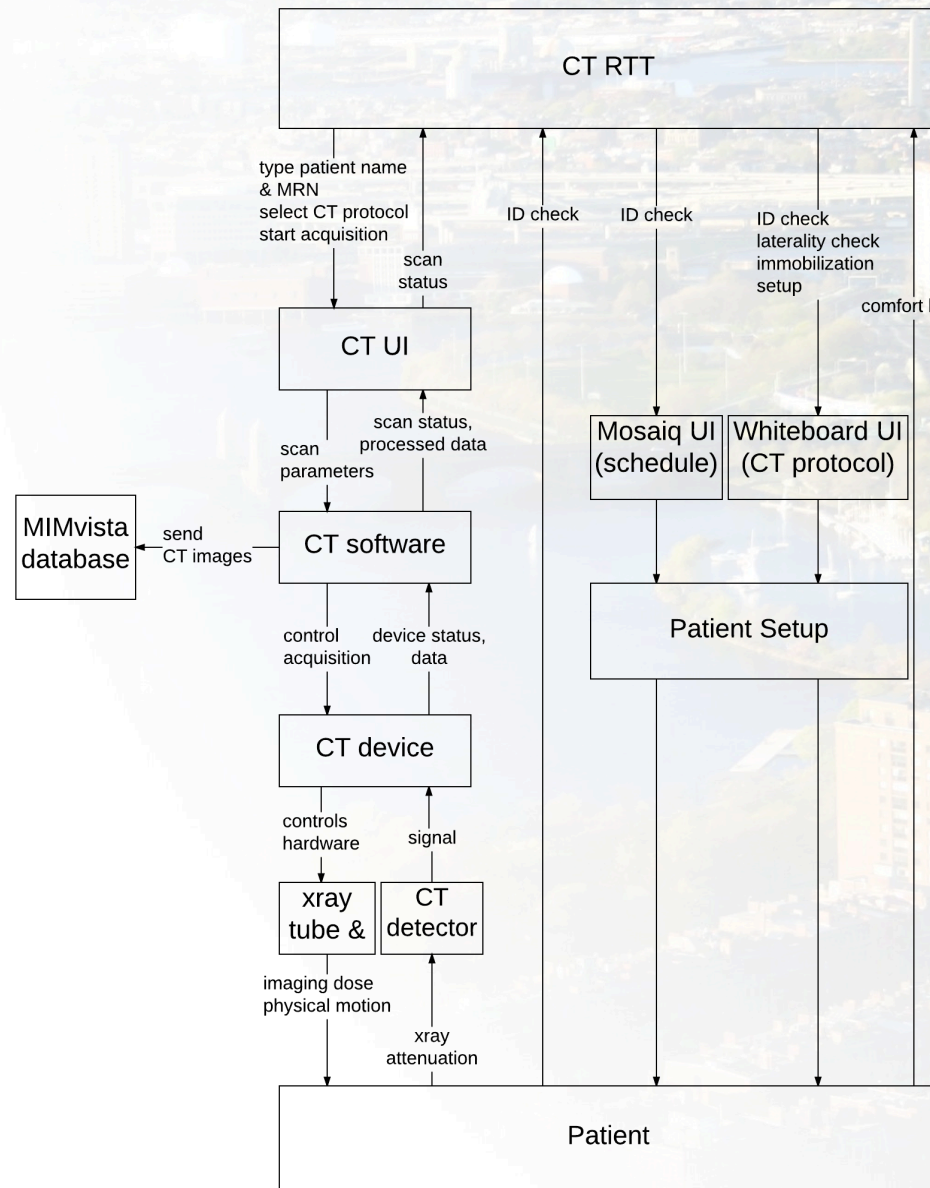
## Focus on: Treatment Planning





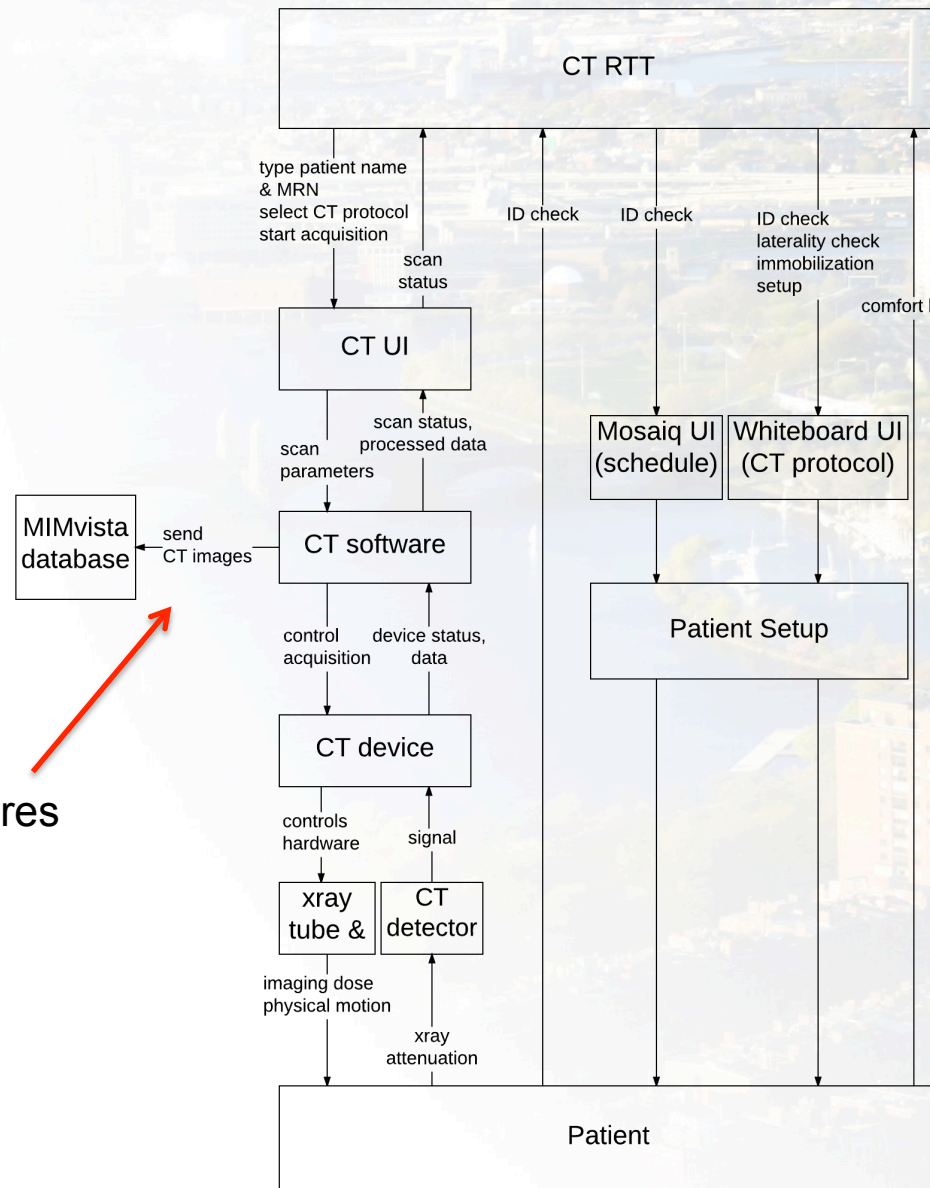
# STPA – Control Diagram

Focus on: CT



# STPA – Control Diagram

Focus on: CT



bad control structures  
easily visible



## STPA – SafetyHat entries



# STPA – SafetyHat entries

## Control Action Input Form

Step: 1 2 3 4 5 6 7 8

Review Existing Control Actions

View Control Actions by Controller

Sort: Order Entered A-Z

CT RTT

setup scan in CT UI

ID check

laterality check

Add New Control Action

Select Controller

CT RTT

Enter Control Action:

setup scan in CT UI

## System Connections Input Form

Step: 1 2 3 4 5 6 7 8

Review Existing System Connections

Existing System Connections

Sort: Order Entered A-Z

From

Type

CT device

CT device

CT imaging detector

CT RTT

Controlled Process

Controller

Sensor

Controller

Controller

Sort: Order Entered A-Z

To

Type

CT software

CT table & xray tube

CT device

Whiteboard UI

Sensor

Actuator

Controller

Actuator

Add New System Connection

Connection Originating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Save As New

Close Form

Modify Existing

Save As New

View Control Structure Diagram

Close Form

Close Form

## System Component Input Form

Step: 1 2 3 4 5 6 7 8

Review Existing System Components

Existing System Components

Sort: Order Entered A-Z

CT device

CT imaging detector

CT RTT

CT software

CT table & xray tube

Add New System Component

Enter Component Name:

CT RTT

Enter a Component Description:

radiological technologist working in computed tomography

on:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:

CT RTT

Type:

Controller

Connection Terminating Component

Name:



# STPA - Accidents

## Accident (or Losses) Input Form

Step: 1 — 2 — 3 — 4 — 5 — 6 — 7 — 8

Review Existing System Accidents or Losses

### Existing System Accidents (or Losses)

Sort: Order Entered ▼ ▲ A-Z ▼ ▲

damage to equipment  
non-radiation, physical harm to patient/staff  
**Patient harmed by radiation**  
Staff harmed by radiation

Add New System Accident or Losses

### Enter System Accident (or Loss):

Patient harmed by radiation

### Enter Detailed Description of the Accident (or Loss):

this means either  
- injury from wrong dose  
- compromised outcome from wrong dose

Delete Existing

Modify Existing

Save As New

Return to Main Menu

Step 3:  
Control Actions

Step 5:  
System Hazards

View Control  
Structure Diagram

Close Form

# STPA - Hazards

## Hazard Input Form

Step: 1 — 2 — 3 — 4 — 5 — 6 — 7 — 8

### Review Existing System Hazards

#### Existing System Hazards

Sort: Order Entered ▼ ▲ A-Z ▼ ▲

- Accidental collision with moving equipment
- Accidental misuse of equipment
- Accidental radiation exposure of staff
- Overdose
- Physical injury due to wrong use of equipment
- Underdose
- Use of equipment outside its specifications
- Wrong location
- Wrong patient

### Add New System Hazard

#### Enter System Hazard:

Accidental collision with moving equipment

#### Enter Detailed Description of Hazard:

#### Select Associated Accident(s):

- Patient harmed by radiation
- Staff harmed by radiation
- non-radiation, physical harm to patient/staff
- damage to equipment

Delete Existing

Modify Existing

Save As New

Return to Main Menu

Step 4:  
System Accidents or Losses

Step 6:  
Unsafe Ctl Action Analysis

View Control  
Structure Diagram

Close Form





# STPA – SafetyHat entries: UCAs

## Unsafe Control Action (UCA) Analysis

Step: 1 — 2 — 3 — 4 — 5 — 6 — 7 — 8

Current Control Action

### Select Controller

CT RTT

### Control Action: 1 of 6

setup scan in CT UI

Control Action  
Analysis Completed

Previous Control Action

Next Control Action

Existing Unsafe Control Actions

### Select Unsafe Control Action Category

Provided, but executed incorrectly

Complete Add Note



### Existing UCAs for Selected Control Action and UCA Category

enter wrong patient MRN/name

enter wrong CT label (site)

use wrong CT protocol

Unsafe Control Action Analysis

### Enter or Select a Detailed Description for UCA

enter wrong patient MRN/name

(All UCAs for Selected Controller)

### Select Relevant Hazards (if applicable)

Overdose

Underdose

Wrong location

Wrong patient

Accidental radiation exposure of staff

Accidental collision with moving equipment

Delete Existing

Modify Existing

Save As New

Return to Main Menu

Step 5:  
System Hazards

Step 7:  
Causal Factor Analysis

View Control  
Structure Diagram

Close Form





# STPA – SafetyHat entries: Causal factor analysis



Works in progress:  
Causal Factors, which adequately classify human error as  
well technical errors

### Causal Factor Analysis

Step: 1 2 3 4 5 6 7 8

**Unsafe Control Action Details**  
**Controller 1 of 1**  
CT RTT  
**Description 1 of 5**  
ID check failed, wrong patient on CT table  
**UCA Analysis Completed**   
**Associated Hazards:**  
Wrong patient

**Previous Controller** **Previous Record** **Next Record** **Next Controller** **Add Note** 

**Existing Causal Factor Analyses**  
Sort: Order Entered  Component Name A-Z   
**Existing Causal Factors for Selected Unsafe Control Action**

Causal Factor	Component Name or Connection From	Connection To
External control input or information wrong or	CT RTT	
External disturbances	CT RTT	

**Causal Factor Analysis**  
**Select: Component or Connection**  
Component  
**Causal Component**  
CT RTT  
**Component Type**  
Controller  
**Select the Appropriate Causal Factor**  
External disturbances  
**Enter or Select a Causal Factor Description**  
RTT does not notice mismatch of name on white/blue card with patient name on screen  
(All Causal Factor Descriptions for Selected Component / Connection and Causal Factor)  

**Delete Existing** **Modify Existing** **Save As New**

**Return to Main Menu** **Step 6: Unsafe Ctl Action Analysis** **Step 8: Export Data** **View Control Structure Diagram** **Close Form**



# STPA – SafetyHat output: excel file

	A	B	C	D	E	F	G
1	UCA_NO	COMPONE	CONTROL_ACTION	UNSAFE_CONTROL_ACTION	UCA_DESC	HAZARD	NOTE_TEXT
2		CT device	controls hardware	Not provided when needed to maintain safety			
3		CT device	controls hardware	Provided when control action is not needed and unsafe			
4		CT device	controls hardware	Provided, but duration is too long or too short			
5		CT device	controls hardware	Provided, but executed incorrectly			
6		CT device	controls hardware	Provided, but the intensity is incorrect (too much or too little)			
7		CT device	controls hardware	Provided, but the starting time is too soon or too late			
8		CT RTT	ID check	Not provided when needed to maintain safety			
9		CT RTT	ID check	Provided when control action is not needed and unsafe			
10		CT RTT	ID check	Provided, but duration is too long or too short			
11	2	CT RTT	ID check	Provided, but executed incorrectly	ID check failed, wrong patient on CT table	Wrong patient	
12		CT RTT	ID check	Provided, but the intensity is incorrect (too much or too little)			
13		CT RTT	ID check	Provided, but the starting time is too soon or too late			
14		CT RTT	laterality check	Not provided when needed to maintain safety			
15		CT RTT	laterality check	Provided when control action is not needed and unsafe			
16		CT RTT	laterality check	Provided, but duration is too long or too short			
17	3	CT RTT	laterality check	Provided, but executed incorrectly	wrong side of the patient marked	Wrong location	
18		CT RTT	laterality check	Provided, but the intensity is incorrect (too much or too little)			
19		CT RTT	laterality check	Provided, but the starting time is too soon or too late			
20		CT RTT	patient immobilization	Not provided when needed to maintain safety			
21		CT RTT	patient immobilization	Provided when control action is not needed and unsafe			
22		CT RTT	patient immobilization	Provided, but duration is too long or too short			
23		CT RTT	patient immobilization	Provided, but executed incorrectly			
24		CT RTT	patient immobilization	Provided, but the intensity is incorrect (too much or too little)			
25		CT RTT	patient immobilization	Provided, but the starting time is too soon or too late			
26		CT RTT	patient setup for scan	Not provided when needed to maintain safety			
27		CT RTT	patient setup for scan	Provided when control action is not needed and unsafe			
28		CT RTT	patient setup for scan	Provided, but duration is too long or too short			
29		CT RTT	patient setup for scan	Provided, but executed incorrectly			
30		CT RTT	patient setup for scan	Provided, but the intensity is incorrect (too much or too little)			
31		CT RTT	patient setup for scan	Provided, but the starting time is too soon or too late			
32		CT RTT	setup scan in CT UI	Not provided when needed to maintain safety			
33		CT RTT	setup scan in CT UI	Provided when control action is not needed and unsafe			
34		CT RTT	setup scan in CT UI	Provided, but duration is too long or too short			
35	5	CT RTT	setup scan in CT UI	Provided, but executed incorrectly	use wrong CT protocol	Underdose	
36	1	CT RTT	setup scan in CT UI	Provided, but executed incorrectly	enter wrong patient MRN/name	Wrong patient	
37	5	CT RTT	setup scan in CT UI	Provided, but executed incorrectly	use wrong CT protocol	Overdose	
38	4	CT RTT	setup scan in CT UI	Provided, but executed incorrectly	enter wrong CT label (site)	Wrong location	

## Workflow modification through new software

The MGH RadOnc Department is developing an application 'Whiteboard' to manage the workflow electronically:

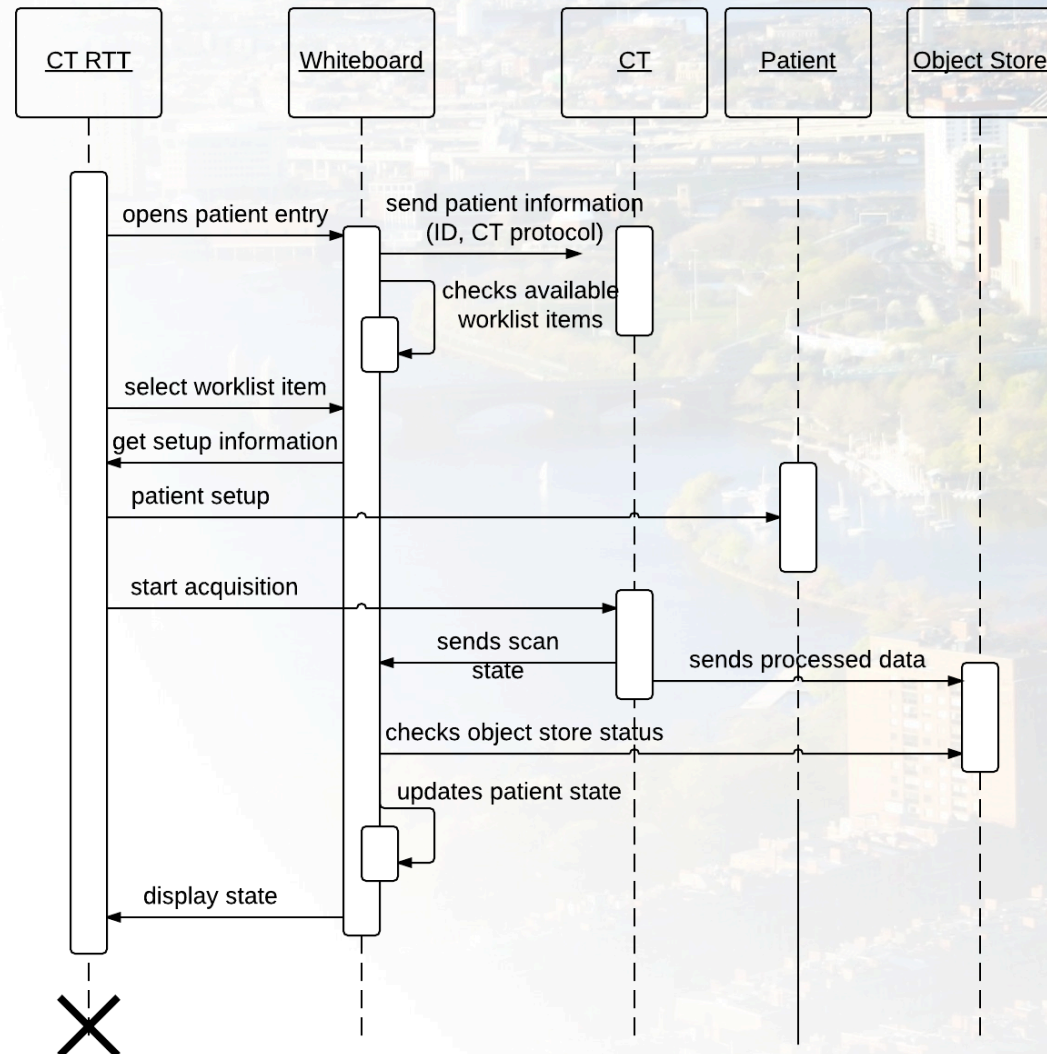
- MD sets up electronic Intake Form -> sets up the expected electronic workflow
- WB keeps track of all data produced for a patient, and status of all tasks in the DICOM 2<sup>nd</sup> G RT course object
- Manages all tasks as a function of context contained in the RT Course instance for a patient
- All data is immutable per DICOM model and always accessible through and instance unique ID



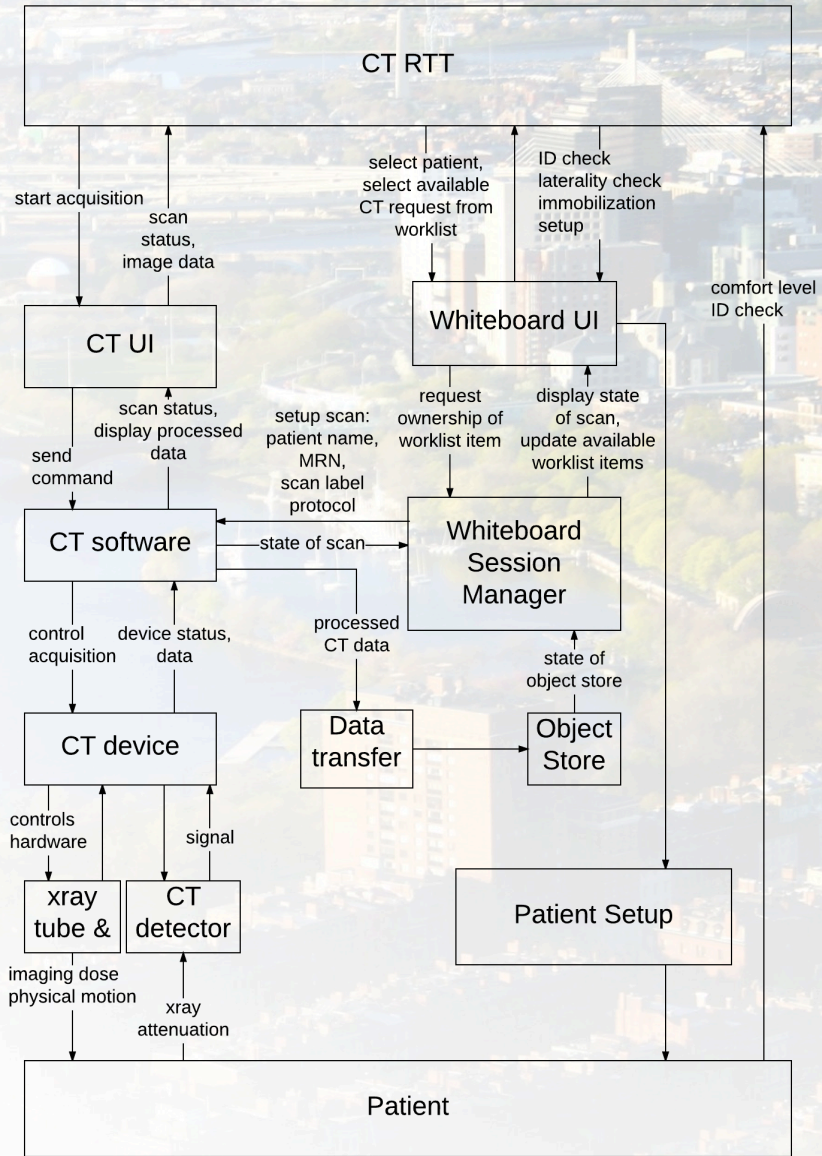
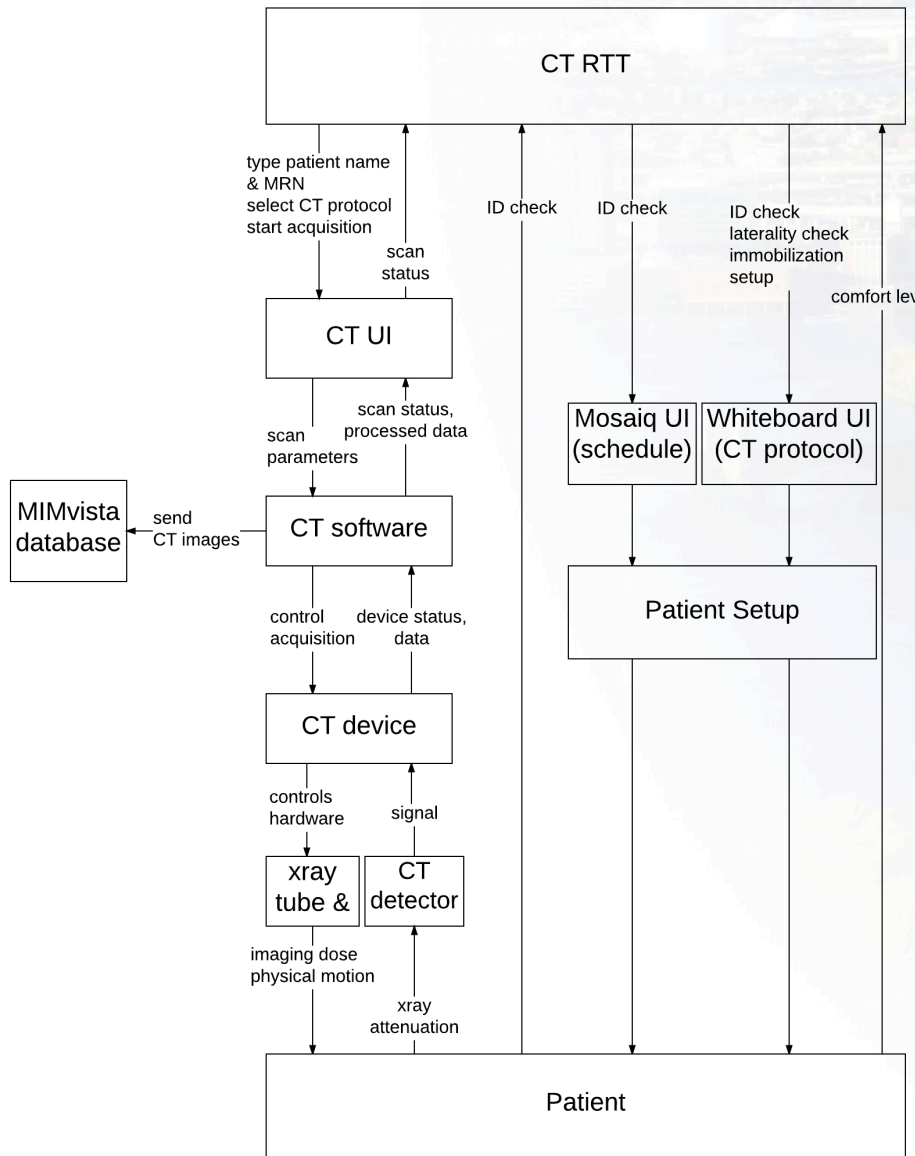
# Workflow modification through new software

For instance:

The CT process

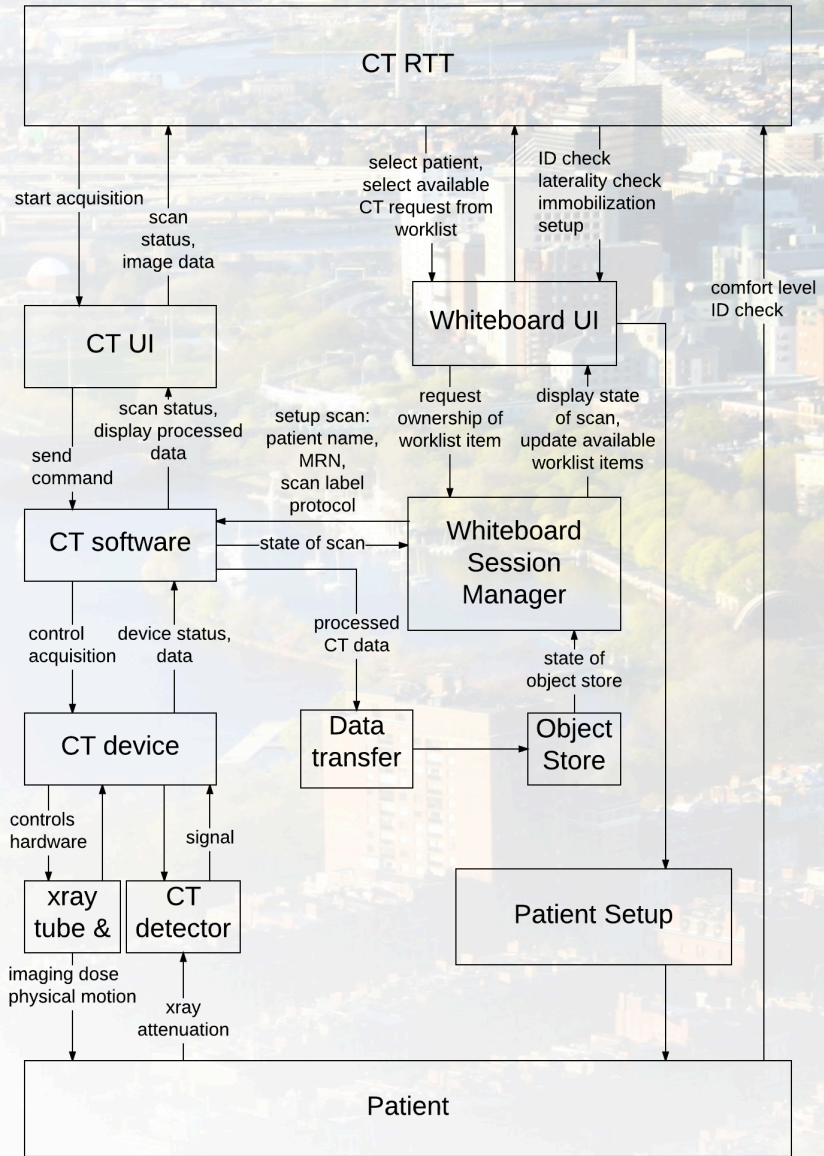
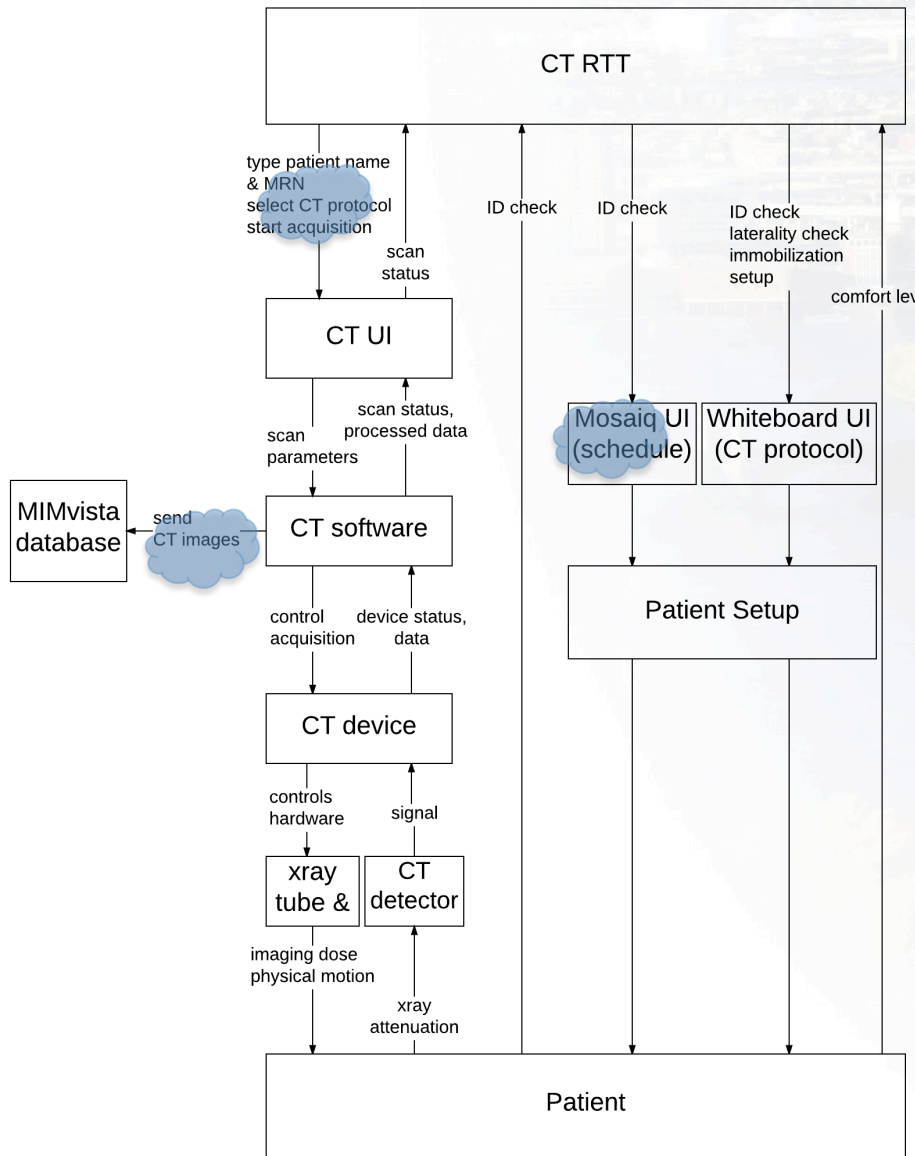


# STPA – control chart with and without Whiteboard

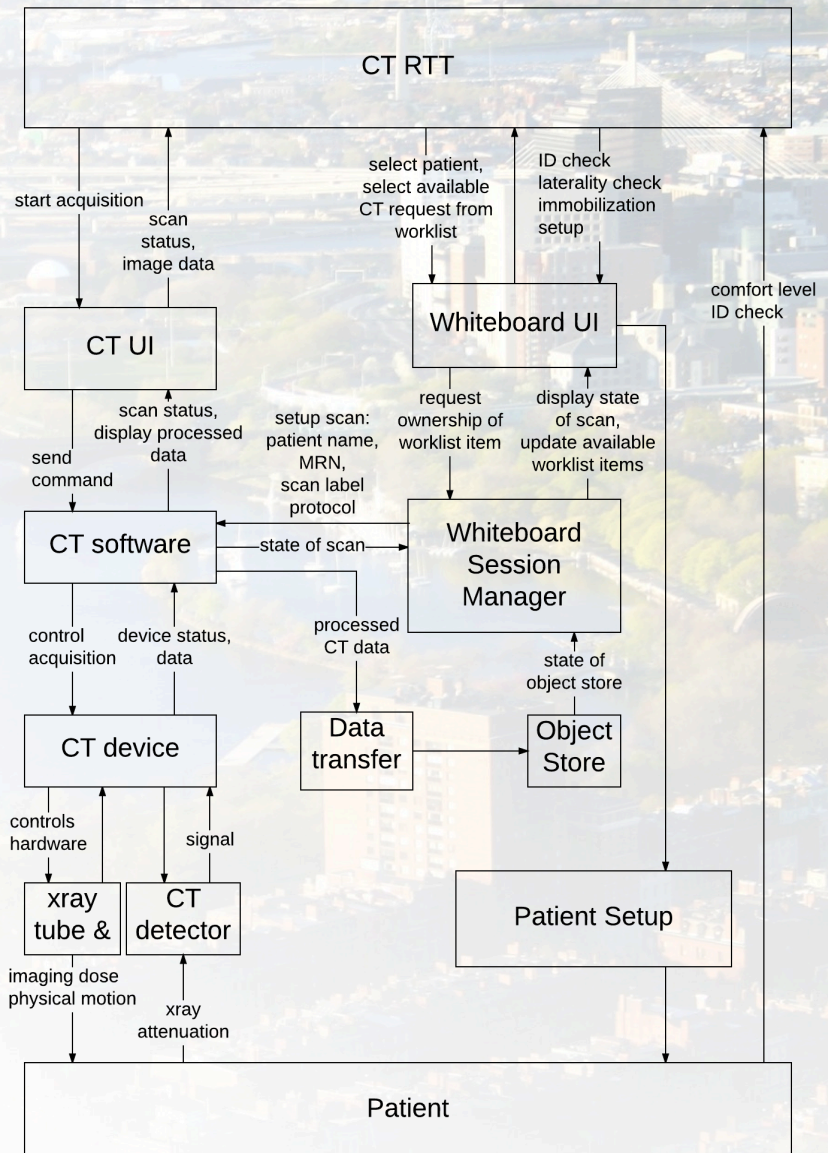




# STPA – control chart with and without Whiteboard



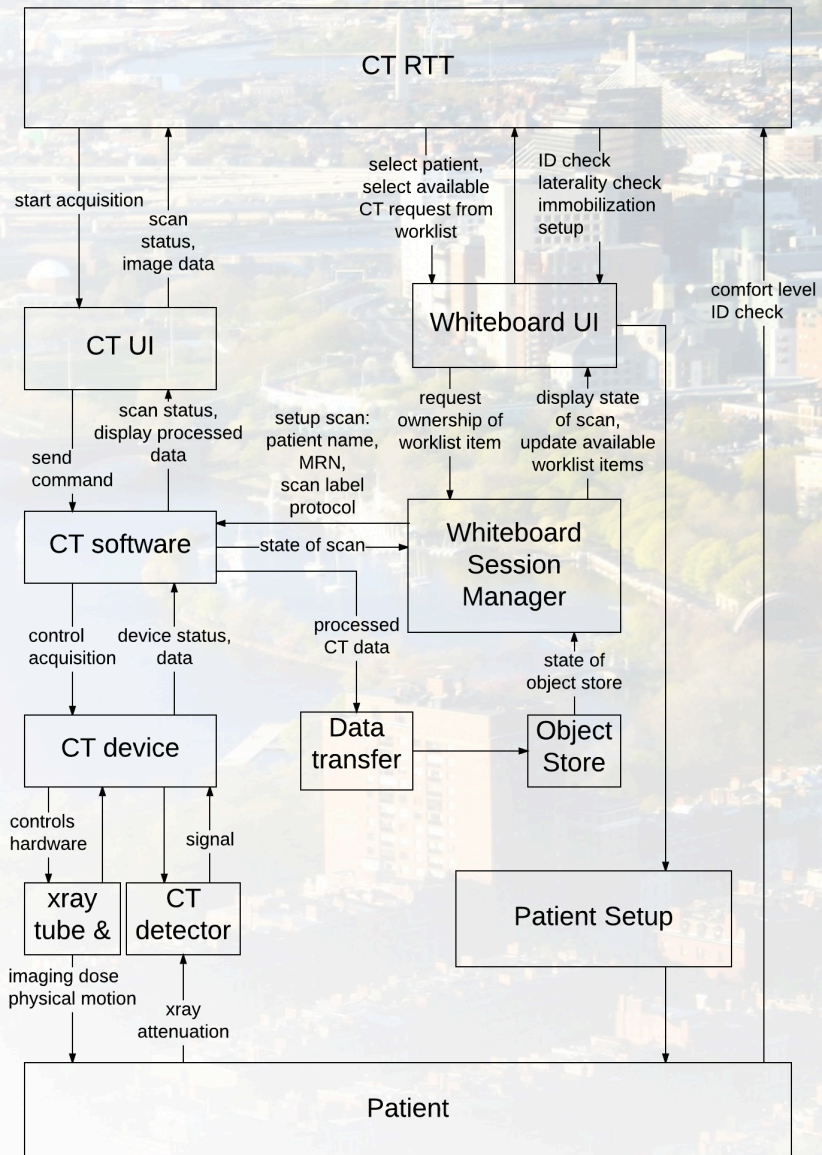
# STPA – control chart with Whiteboard





## STPA – control chart with Whiteboard

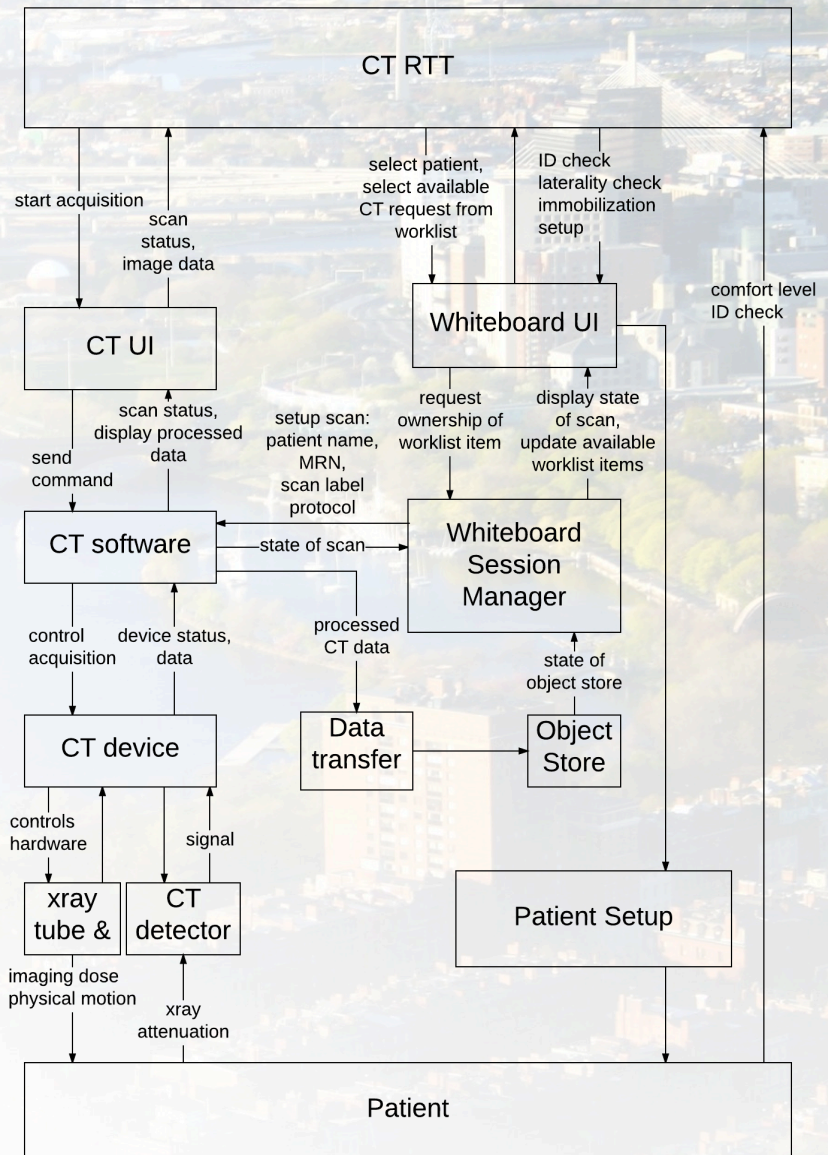
Hoping to inform design requirements for new processes and procedures through STPA.



## STPA – control chart with Whiteboard

Hoping to inform design requirements for new processes and procedures through STPA.

In general: automation, add system constraints, close control loops



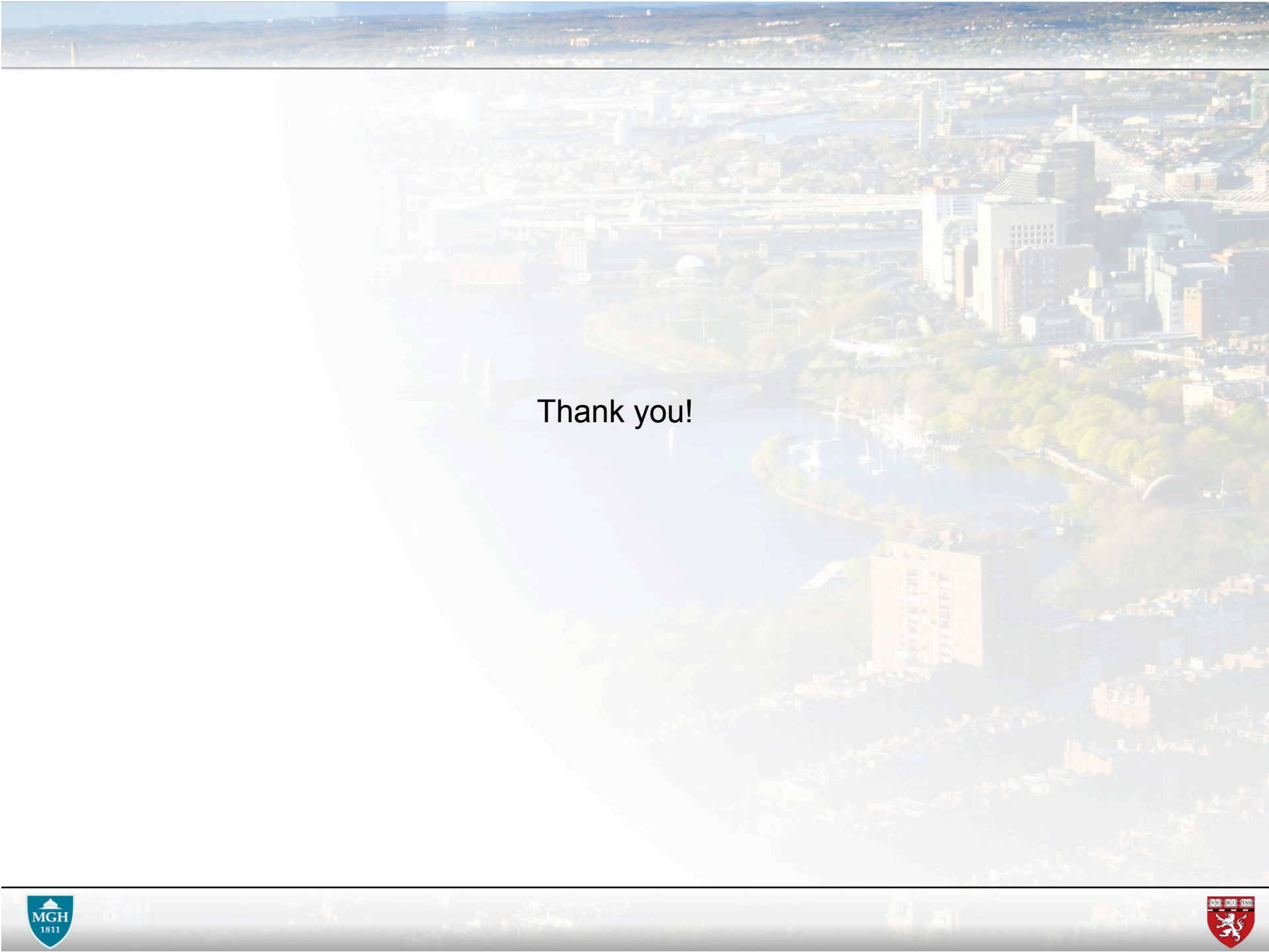


## STPA – next steps

Hoping to inform design requirements for new processes and procedures through STPA.

In general: automation, add system constraints, close control loops

- Settle on set of causal factors
- Finish analysis
- Compare to results when analyzed using FMEA as suggested by AAPM TG 100

An aerial photograph of Boston, Massachusetts, showing the city skyline, the harbor, and the surrounding landscape. The text "Thank you!" is overlaid on the image.

Thank you!