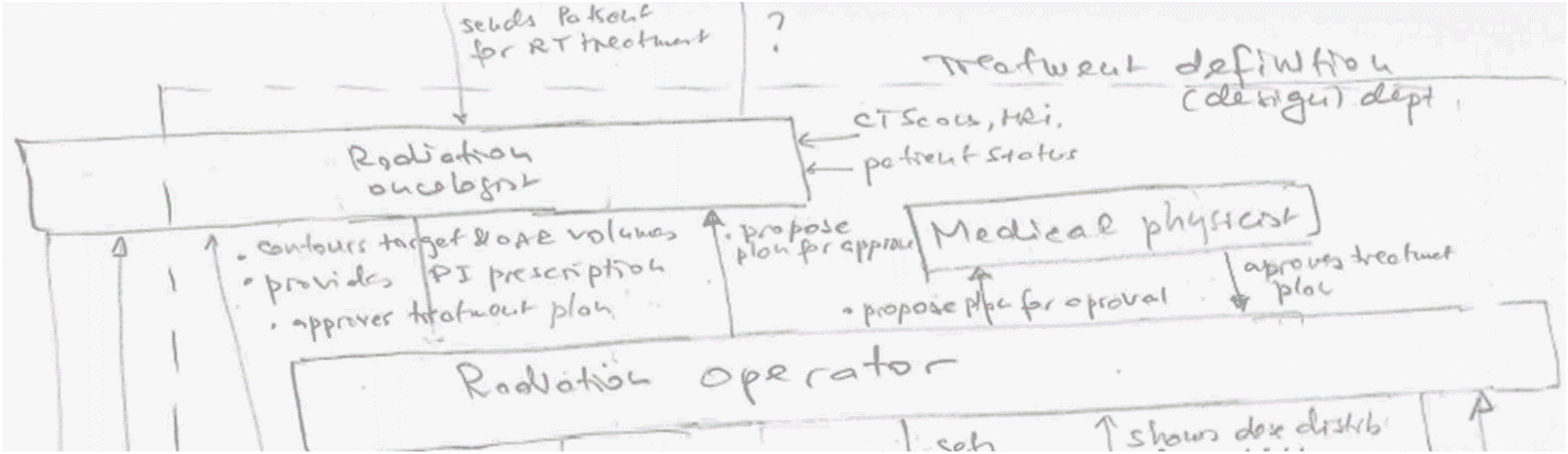


Application of STPA in Radiation Therapy: a Preliminary Study

Natalia Silvis-Cividjian

Wilko Verbakel

Marjan Admiraal

vrije Universiteit amsterdam

VUmc VU University Medical Center Amsterdam

MIT STAMP Workshop 2018

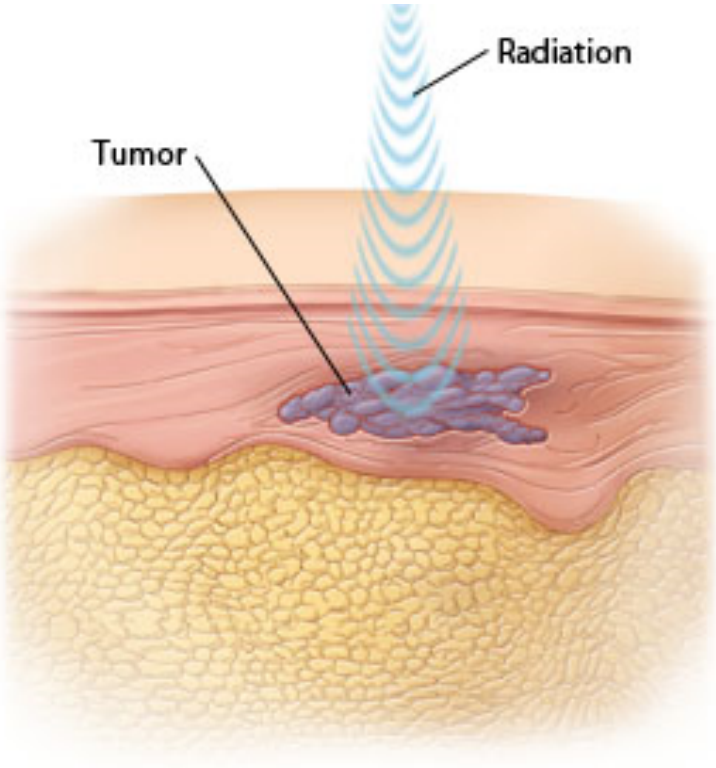
Vrije Universiteit (VU) campus
Amsterdam, The Netherlands

VU medical center

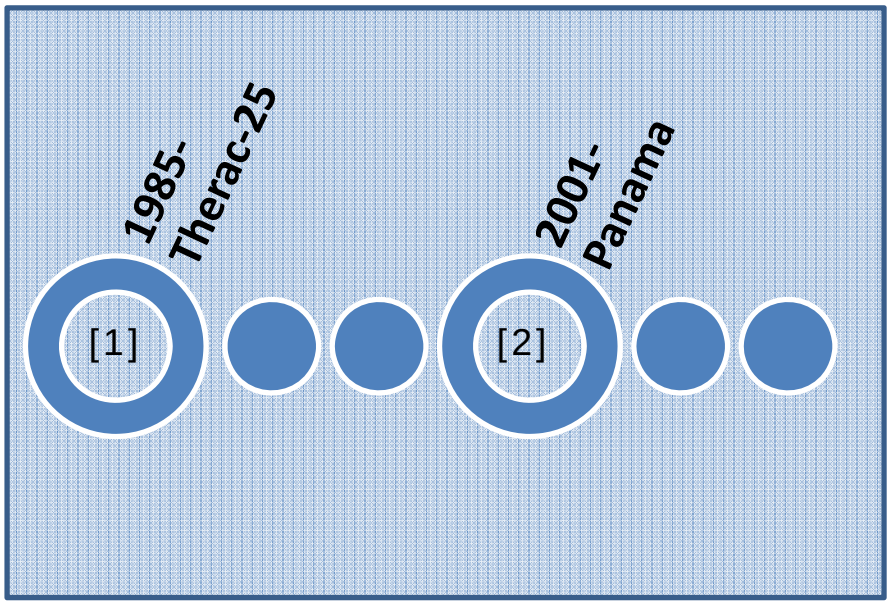
VU Computer Science Dept

Radiation Therapy (RT)

Principle



Overexposure accidents



1.Leveson & Turner, IEEE Computer. (1993)
2.Borras, Rev Panam Salud Publica. (2006)

Objective

- RT safety standards recommend FMEA and FTA
- STAMP is a rising star in industry, but not in RT

How does it 

and 

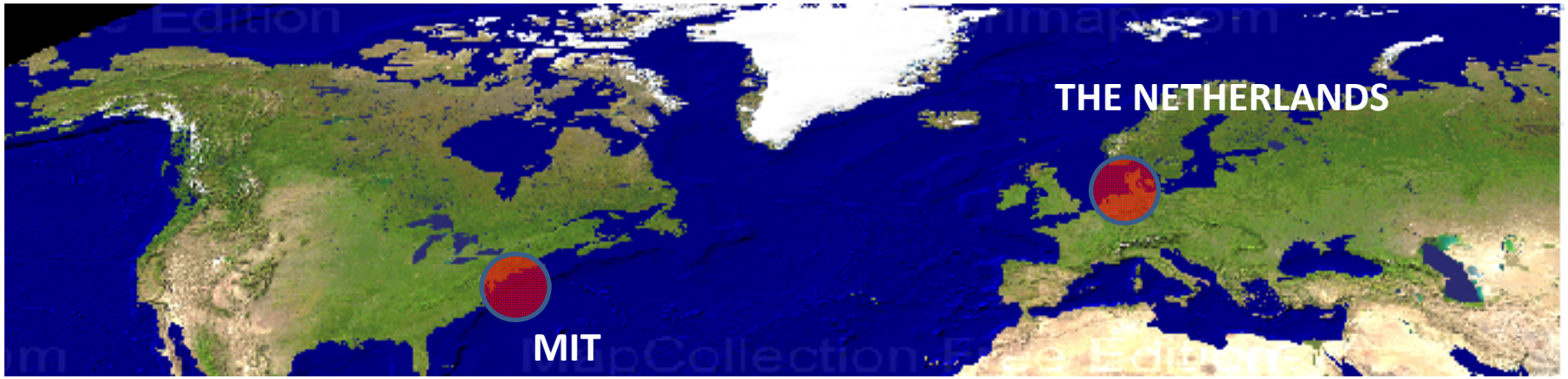
to introduce STAMP in RT?

Outline

- Preparatory steps
- Off we go!
- Results
- Conclusions and recommendations
- Future work

A simple system

- Oosterschelde storm surge barrier in NL
- Moveable sluice-type of gate doors
- Automatically close when water level > 3m



Risk management?

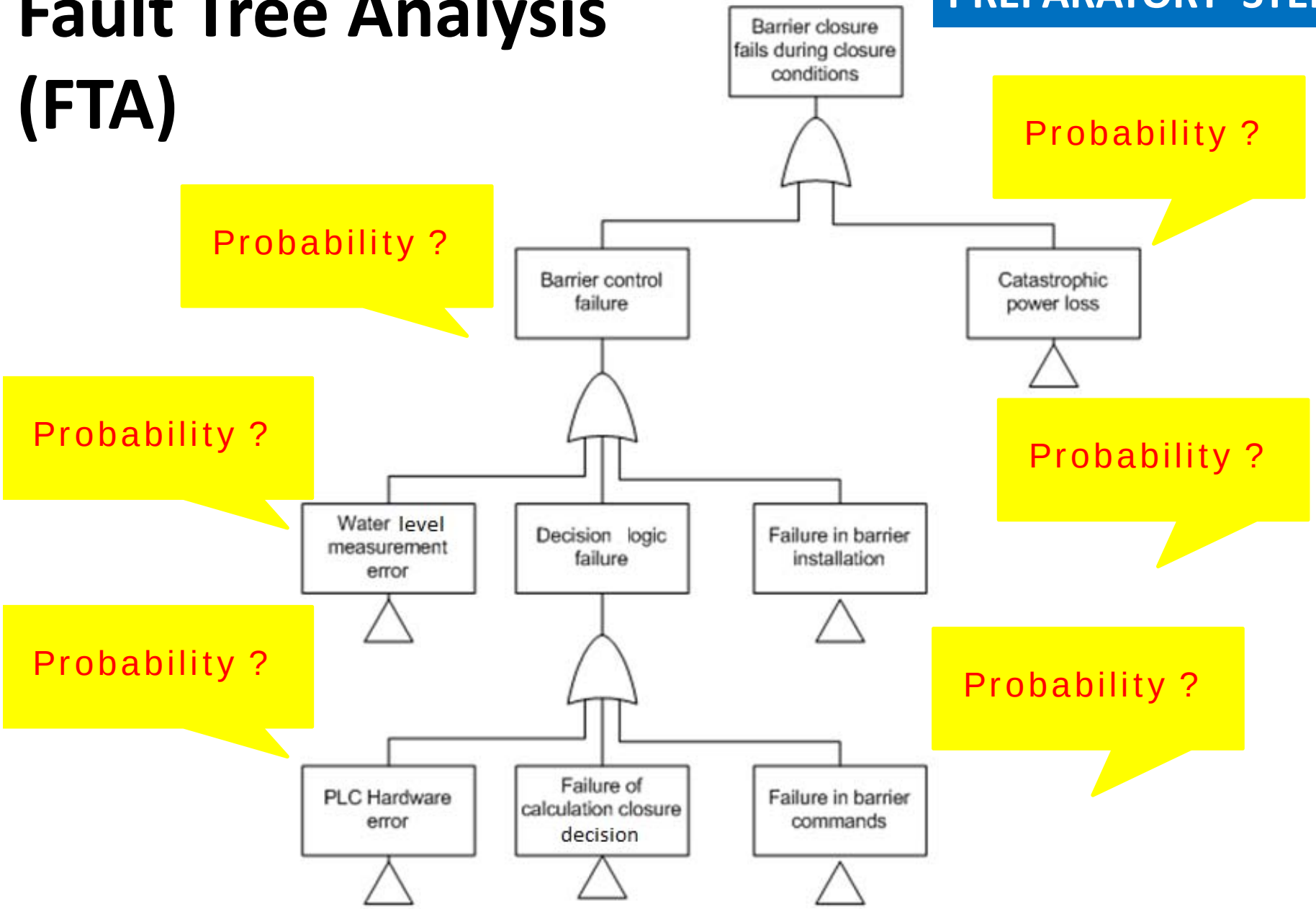
An accident

Hazard analysis techniques

- Fault Tree Analysis (FTA)
- Failure Mode and Effect Analysis (FMEA)
- System Theoretic Process Analysis (STAMP-STPA)

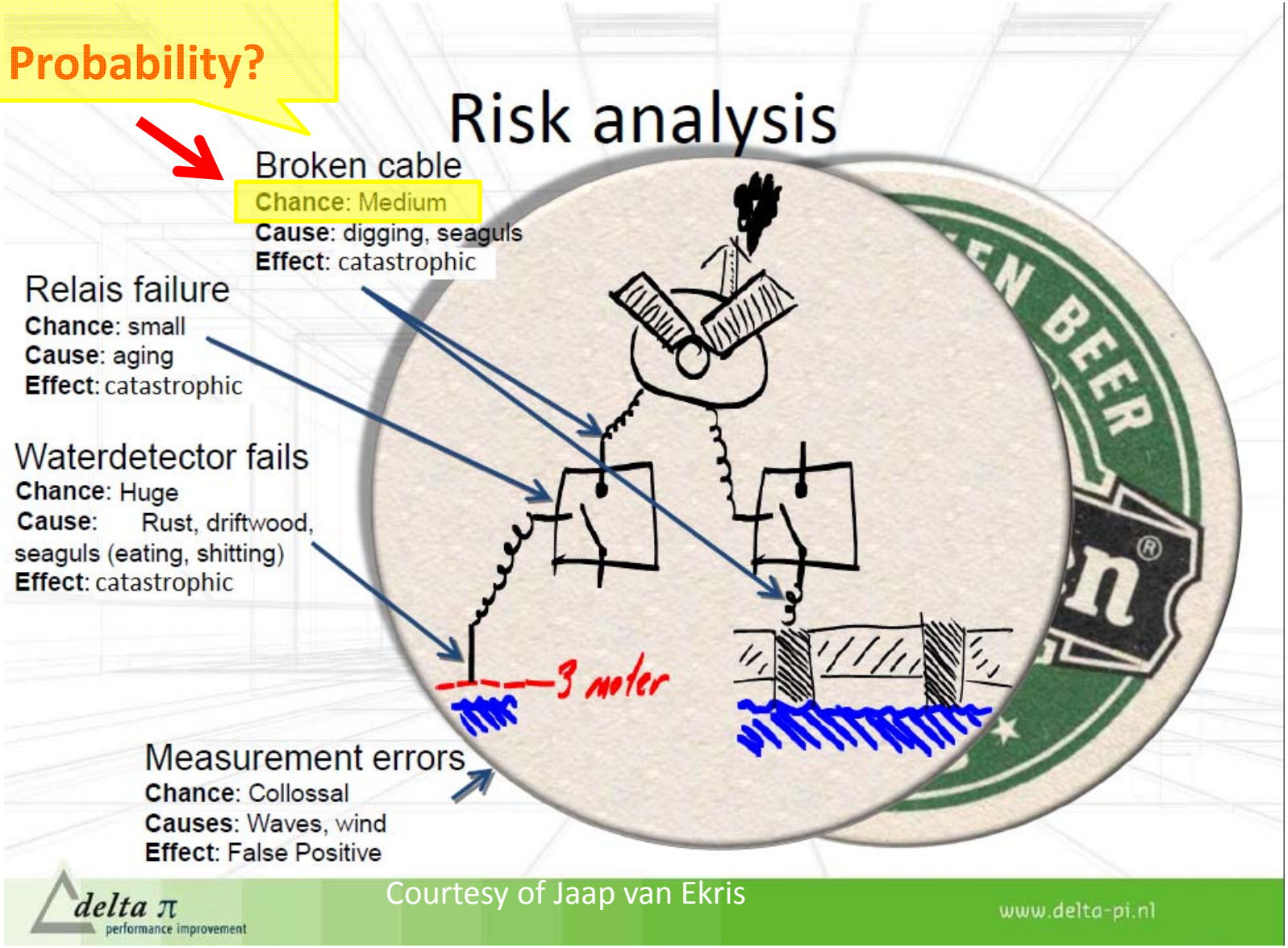
Fault Tree Analysis (FTA)

PREPARATORY STEPS



Courtesy of Jaap van Ekris (Delta Pi)

Failure Mode and Effect Analysis (FMEA)



Courtesy of Jaap van Ekris

FMEA

FMECA Storm Surge Barrier

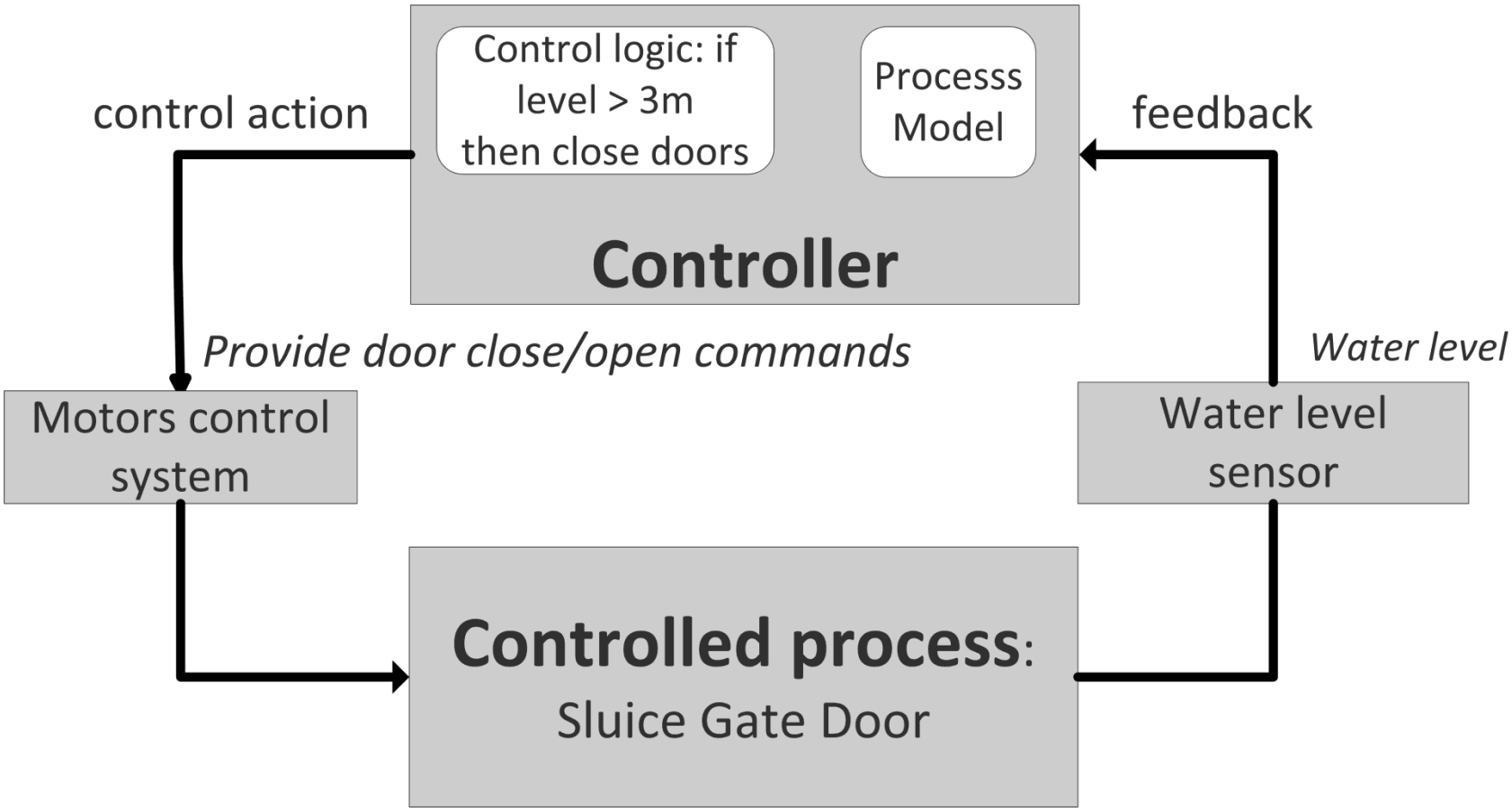
Function	Failure Mode	Causes	Local Effects	System Effects	Criticality	Detection	Mitigating Measures
Meet	Verkeerde output	Logische fout	Onterecht open	Sluiting blijft uit	Catastrophic	None	Multiprogramming
	Vertraagde output	PLC error	delayed sluit	Sluiting vertraagd	Beperkt	None	
	Geen output	Hangen applicatie	Geen sluiting	Sluiting blijft uit	Catastrophic	None	Deadlock detectie
	Spontane output	Schakelfout	onterecht sluiten	Onterechtesluit	False Positive	None	
Stuur	Verkeerde output	Logische fout	Onterecht open	Sluiting blijft uit	Catastrophic	None	Multiprogramming
	Vertraagde output	PLC error	delayed sluit	Sluiting vertraagd	Beperkt	None	
	Geen output	Hangen applicatie	Geen sluiting	Sluiting blijft uit	Catastrophic	None	Deadlock detectie
	Spontane output	Schakelfout	onterecht sluiten	Onterechtesluit	False Positive	None	
...	...	...	...	...	...	...	...
	...	...	...	...	...	...	...
	...	...	...	...	...	...	...
	...	...	...	...	...	...	...

Control Wrong output Fault in logic Doors open Catastrophic

STAMP

- STAMP uses a different accident causality model
- It models each process as a system.
- It does NOT calculate probabilities. All hazards are equally important and need to be prevented with control constraints by design.

STPA Step 0. Model the system with safety control structure



STPA Step 1.Identify hazards (Unsafe Control Actions)

Control action (CA)	CA not given	Incorrect CA is given	CA is given at the wrong time or wrong order	CA is stopped too soon or applied too long
Provide door close/open command	Door close command is not given when level > 3m	Door open command is given when water level is >3m	Door close command given long after water has reached 3m and is rising Door open command much too late, long after the water level is safe	Door closed stopped too soon (door not completely closed) when level is > 3m

STPA Step2. Causal scenarios and corrective measures

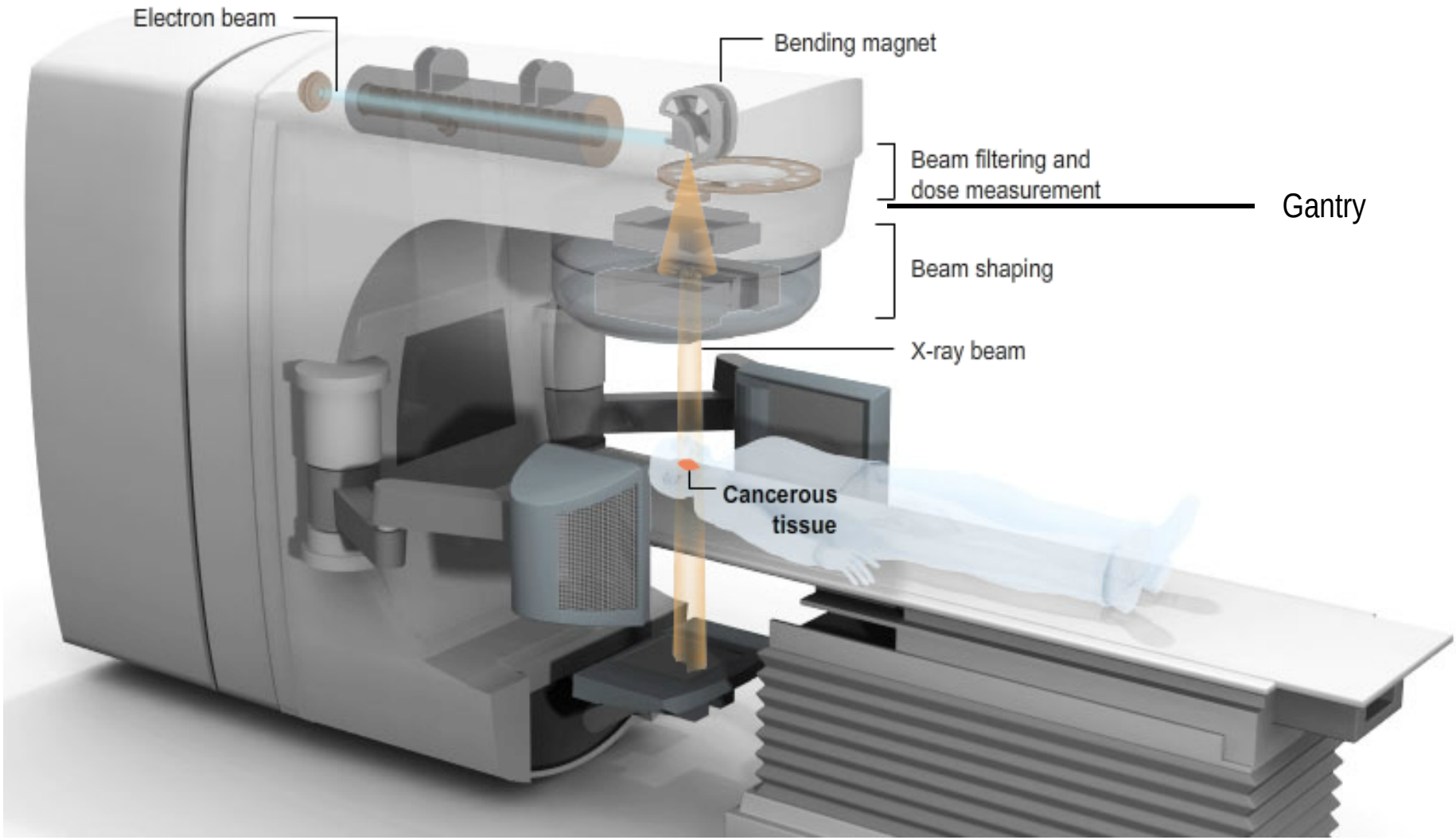
- **UCA:** The water is 4 m high and one door is open. **Why?**
- Possible reason: Sensor wire is broken and makes the controller think that the water level is safe (0m).
- Corrective measure : The decision to open the door should not rely only on one sensor.

Conclusion so far

- STPA detects hazards in a more systematic way
- However, for simple systems, STPA seems to find the same hazards and recommendations as FTA or FMEA.
- So why bother?
- RT team is skeptical, but willing to give it a try

OFF WE GO!

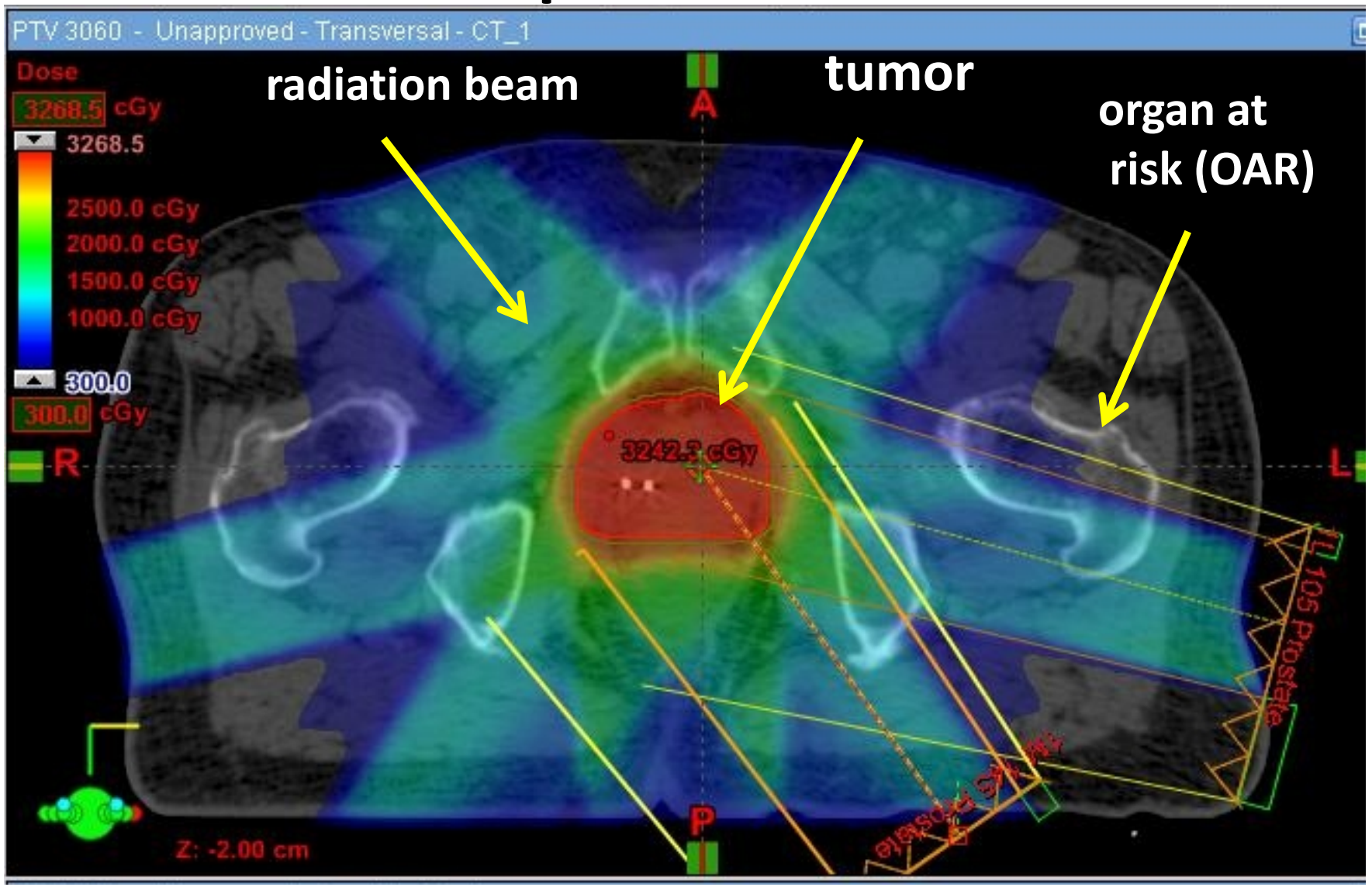
Intensity Modulated Radiation Therapy (IMRT)



Source: http://www.nytimes.com/interactive/2010/01/22/us/Radiation.html

IMRT Treatment plan

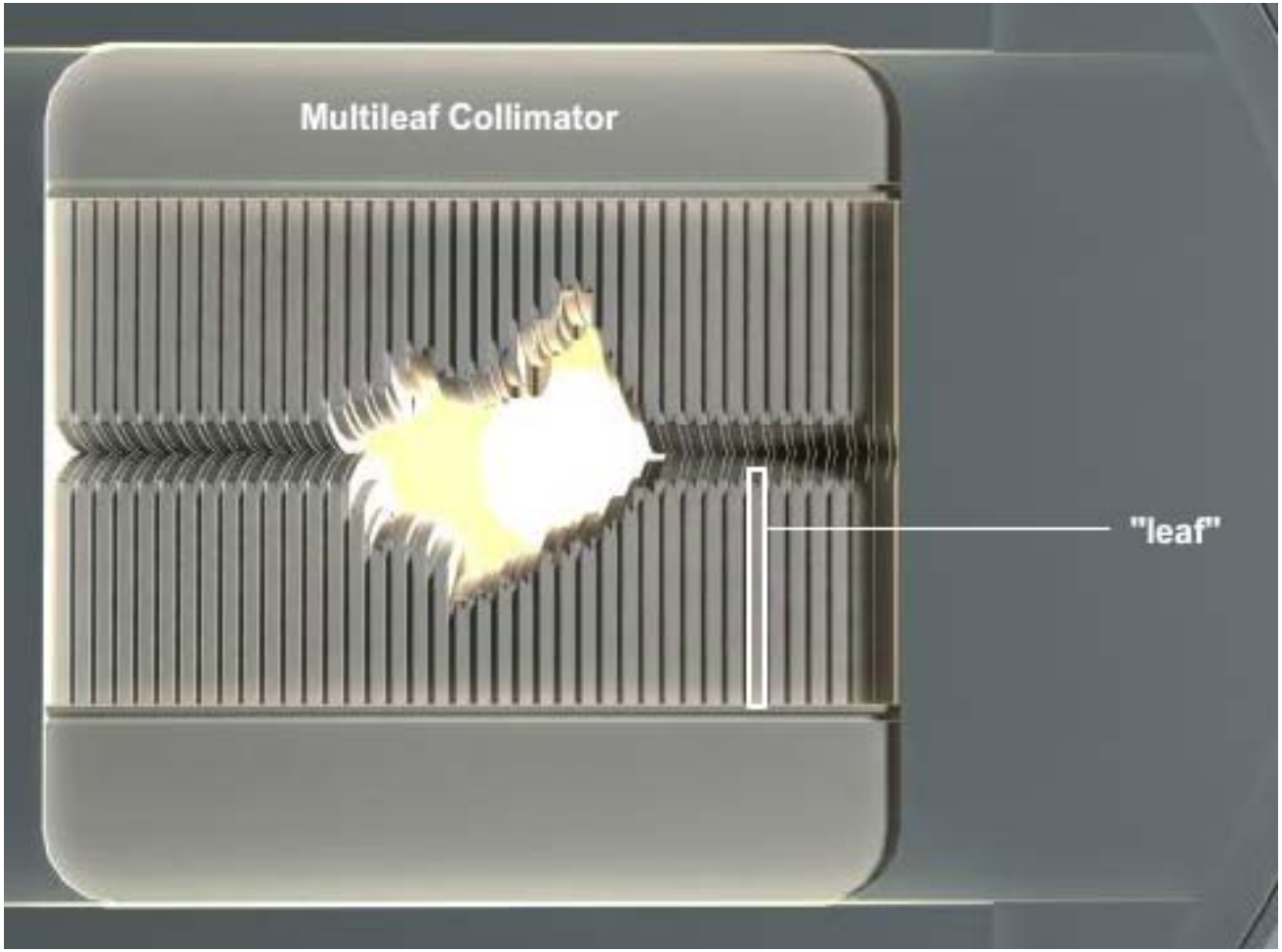
OFF WE GO!



Source: http://acfro.com/what-to-expect-during-your-treatment/radiation-therapy-imrtigrt-oncology-physicial-therapy/

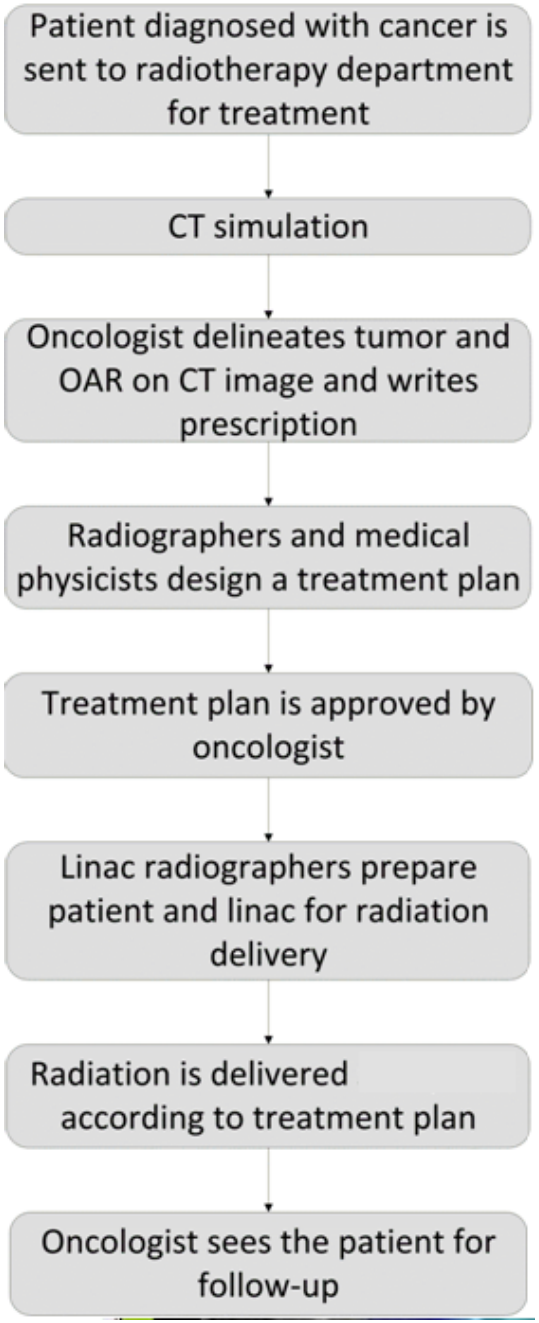
OFF WE GO!

Multileaf Collimator (MLC)



Source: http://www.nytimes.com/interactive/2010/01/22/us/Radiation.html

OFF WE GO!



IMRT flowchart

OFF WE GO!

Photo: **Radiotherapy facility at VUmc Amsterdam**

OFF WE GO!

Research questions

- **RQ1. How difficult is it to apply STPA for hazard analysis in RT?**
  - Can an outsider conduct it?
  - Will it add excesive workload for RT dept?
  - What shall we do with all the thousands of hazards we'll find?
  - Can we speed up the analysis by reusing artifacts from other RT centers?
- **RQ2. What is the added value of STPA vs. HFMEA?**
  - Compare STPA with an existing HFMEA

OFF WE GO!

Step 0. High-level accidents

- A1. Patient injured or killed from radiation exposure
- A2. A non-patient is injured or killed by radiation
- A3. Damage or loss of equipment
- A4. Physical damage to patient or non-patient during treatment (not from radiation)

Sources:

Pawlicki, Todd, Aubrey Samost, Derek W. Brown, Ryan P. Manger, Gwe-Ya Kim, and Nancy G. Leveson. 2016. 'Application of systems and control theory-based hazard analysis to radiation oncology', *Medical Physics*, 43: 1514-30

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

OFF WE GO!

Step 0. Graphical modeling

This is what the beginner analist is hearing:

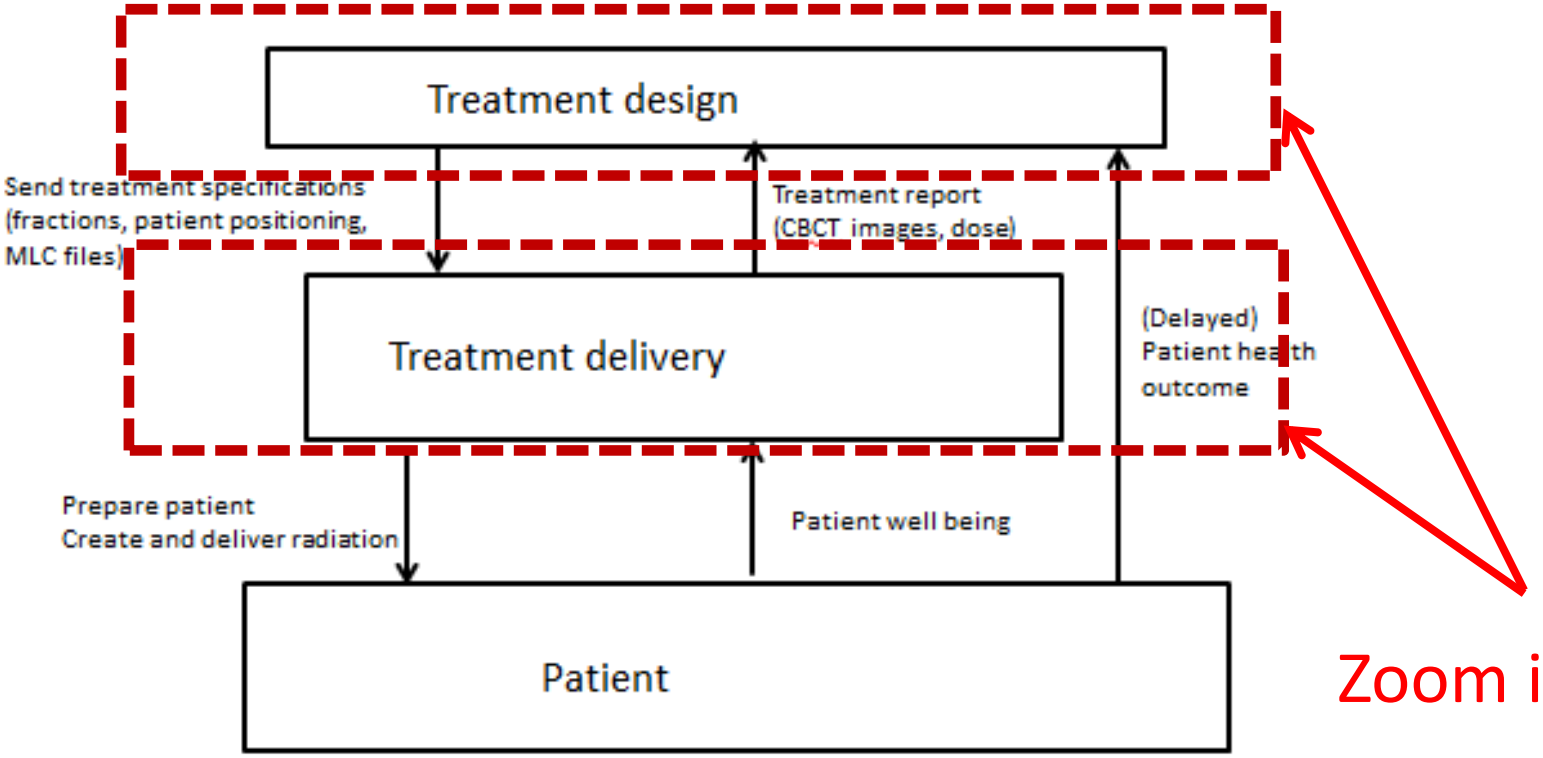
- Oncologist fills a CT simulation request in ARIA
- CT radiographer makes and saves CT images in ARIA
- Oncologist writes a treatment prescription in ARIA
- Radiographer makes a treatment plan and saves it in ARIA
- Medical physicist approves the plan in ARIA
- ARIA is a huge database shared by treatment planning and delivery

These are his questions:

- What goes in a controller box?
- Which level of granularity?
- What is a control action and what is a feedback?

OFF WE GO!

High-level control structure

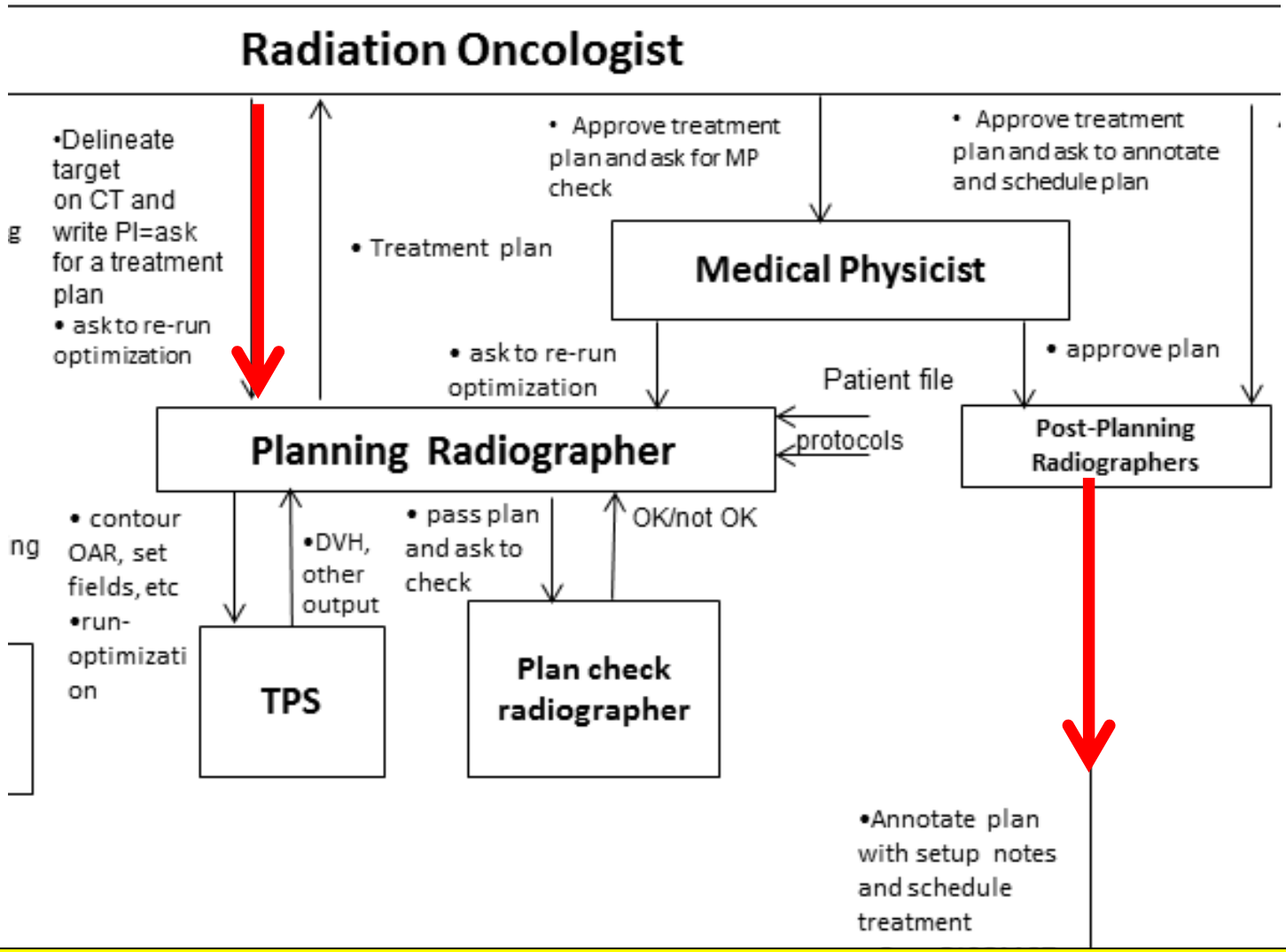


Zoom in later

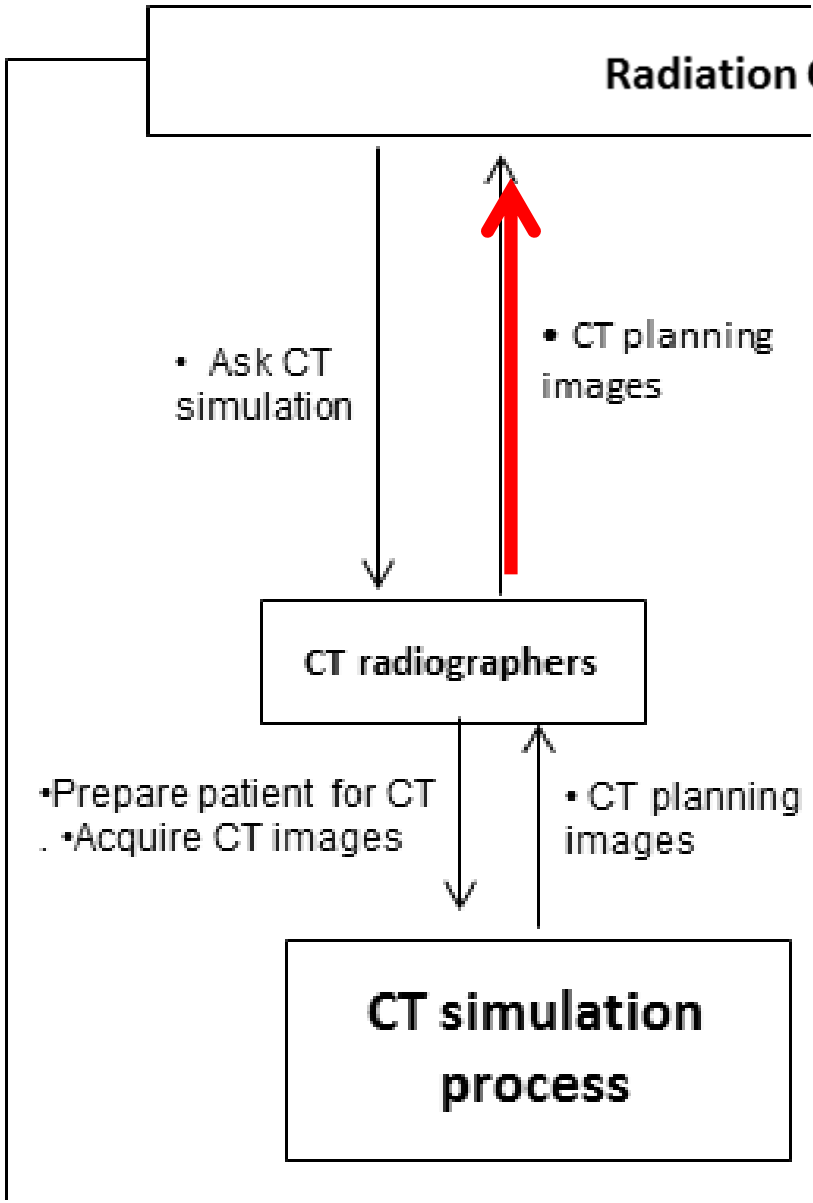
First high-level control structure

Cumulate more actors in one controller. A controller is not a person, but a representation of a functionality

OFF WE GO!



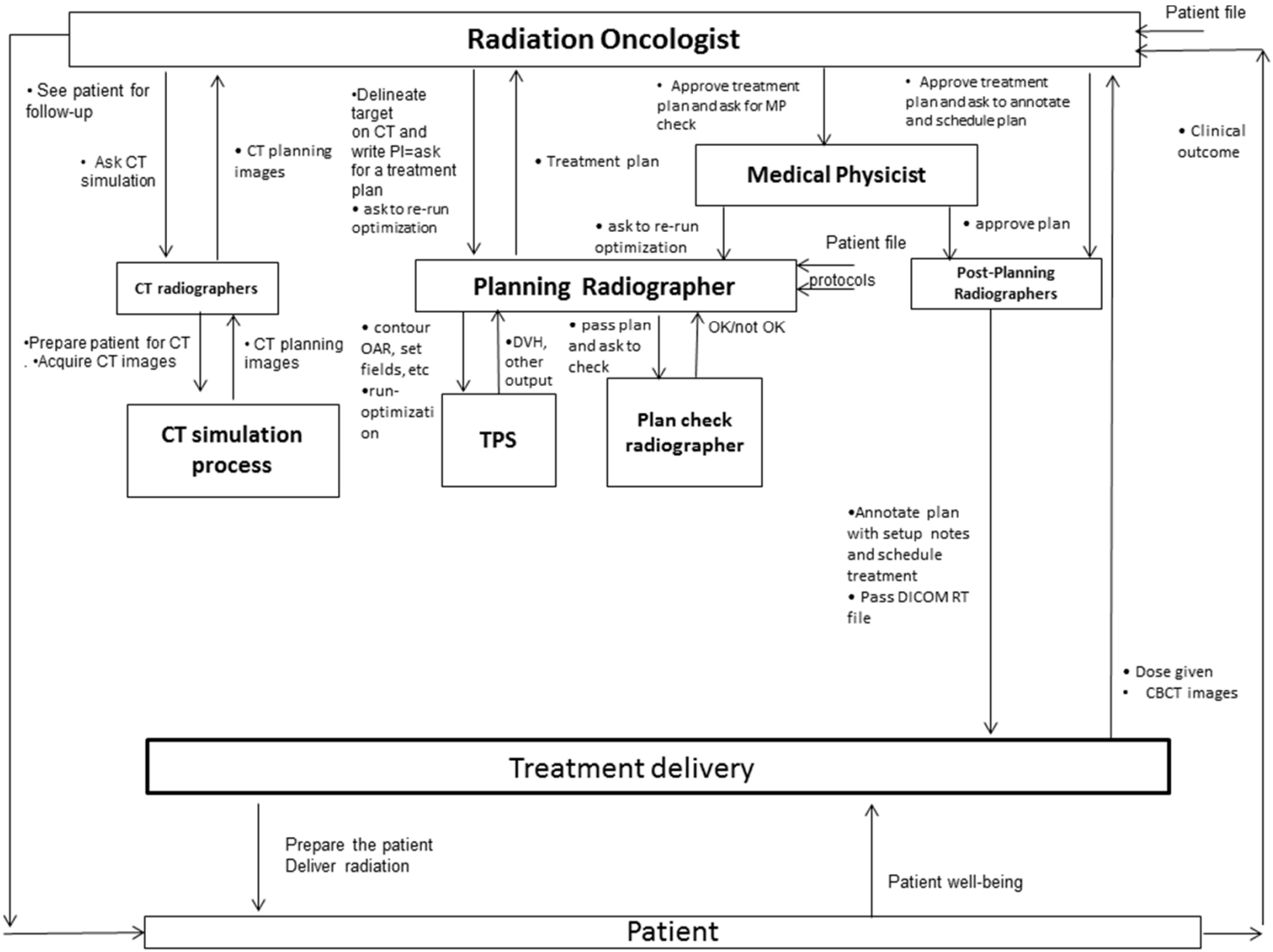
"Oncologist writes a PI " is modeled with a **control action** to radiographer to make a treatment plan



OFF WE GO!

"CT radiographer saves images in ARIA" is modeled as **feedback** to oncologist

Hint: control actions are *verbs*, a kind of commands. Feedback is a *noun*, something that makes the controller adapt its process model.



Control structure for Treatment Design controller

OFF WE GO!

Step 1. Identifying possible hazards

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 optimization with wrong parameters	Planning radiographer starts optimization too soon, before the targets and OARs have been delineated Planning radiographer re-optimizes the plan long after the peer reviewing asked for it	Planning radiographer keeps on applying 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)

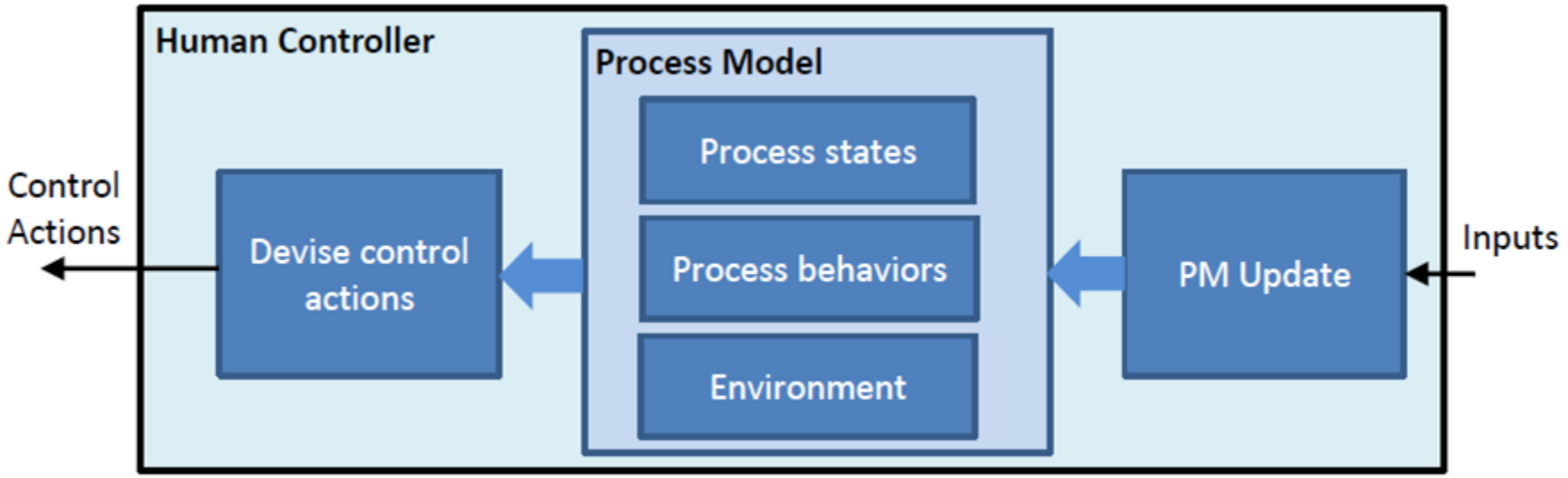
OFF WE GO!

Step2. Causal scenarios and corrective measures

ID	UCA	Causal scenarios	Corrective measures
1	Oncologist wrote a wrong CT prescription	Did not have complete anatomic info at that time, and later forgot	1. Create templates in software 2. Oncologist should be present during CT scan

OFF WE GO!

Extended STPA model for human controllers



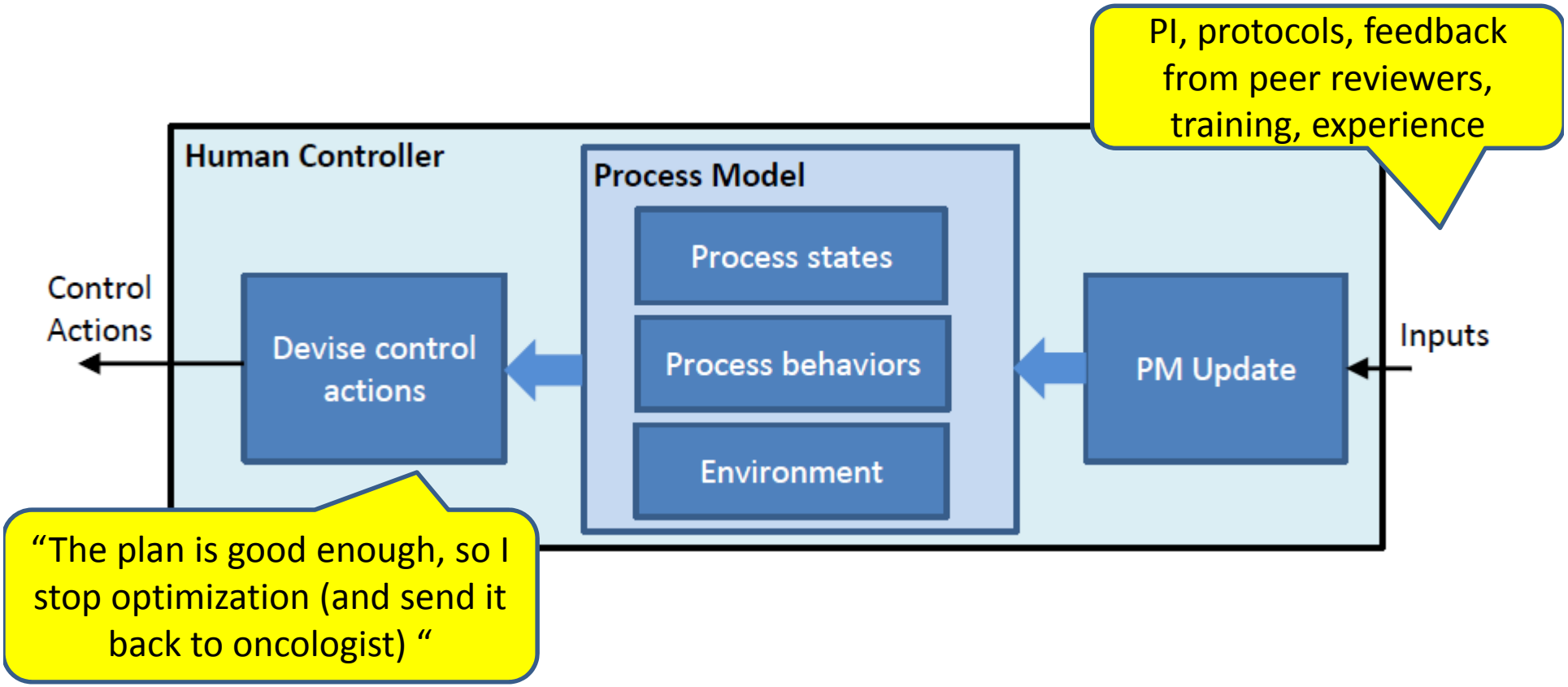
[Thomas & France, 2016]

- **Human controller:** *Planning radiographer*
- **Control action:** *Run optimization in TPS*
- **Control algorithm:** *Delineate OAR and position collimators on CT scan according to procedures and repeat running optimization in TPS until dose distribution is according to PI.*

OFF WE GO!

Causal scenarios

- UCA: *Planning radiographer stops optimization too soon. As result, the plan has wrong parameters (collimator settings)*. **WHY?**



OFF WE GO!

Causal scenarios

- *[1] Incorrect belief of the process state.*
  - PI or protocols are ambiguous and not clear
  - the radiographer *thinks* that his unorthodox way of collimator positioning is better, but he *overlooks* that radiation hot spots are created
  - the radiographer was interrupted by a telephone call or pager, and as a result *forgets* where he was in the plan procedure

OFF WE GO!

Causal scenarios

- *[2] Incorrect belief of the process behavior.*
  - the radiographer is not experienced and makes wrong assumptions about TPS behaviour. He could also ask questions to his superiors, but does not dare.

- *[3] Flaws in the mental model updates*
  - the radiographer used the same incorrect collimator positioning in previous plans without problems
  - he is bored and keen to try new things.

Results

RQ1. How difficult was it to apply STPA in RT?

- Graphical modeling of the process was difficult for beginners. STAMP community helped. Step2 was easier.
- Can an outsider conduct it? YES
- Will it add excesive workload for RT dept? NO
- What to do with all those thousands of hazards? We found 142 UCAs. They should all be analyzed.
- Can we speed up the analysis by reusing artifacts from other RT centers? partially YES.

RQ2. What is the added value of STPA vs HFMEA?

RESULTS

Step1. Hazards identification

- The lists of hazards mostly overlap.
- HFMEA is more detailed in hazards of type "*wrong control action*"
- STPA is more rigurous and separates better causes from effects. Ex: *CT radiographer forgot to apply the tatoos* (FMEA) vs. *CT radiographer did not apply tatoos* (STPA).
- STPA found new, unexplored hazards.
  - *Post-planner sent the plan to delivery team before it was approved and complete.*
  - *The CT radiographers start to acquire images long after the patient has been immobilized on the table.*
  - *Planning radiographer keeps on executing plan optimization even if peer reviewers have already approved the plan* -> Interesting human behaviour

RESULTS

Step 2. Causal scenarios

- STPA offers more guidance in understanding human-related hazards.
  - Ex. *In the scenario "Oncologists's PI is ambiguous'', the oncologist and radiographer share the blame*.
- A causal analysis of UCAs led to valuable correction measures.
  - Technical: *Add a reminder feature for the oncologist in ARIA*
  - Procedural: *If PI seems impossible, ask help from MP after two trials*
  - Managerial: *Create a logistics manager to keep track of the tasks workflow*

RESULTS

Discussion

- HFMEA was more detailed because is a bottom-up, component-based approach, performed by domain experts. STPA is a top-down approach, and was performed by an outsider.

- The comparison is not 100% fair as some hazards were discarded by the HFMEA team because:
  - Focus was different at that time
  - Hazards with low risk (probability of occurrence, severity of consequences) were omitted
  - Knowledge of protection by procedures and software was incorporated in the evaluation of hazards.
    - New processes won't have this knowledge

Conclusions

- It is not easy to persuade RT teams to adopt STPA
- Beginner analists struggle with systems-based modeling

However,

- STPA adds new hazards and safety-related recommendations to existing HFMEA results
- This is achieved with much less resources and domain knowledge

Recommendations

- STPA should be considered as an option anytime a RT safety analysis is needed.
- If the proces is new, use STPA in early stages of development
- If the process is old and already safeguarded by FMEA/FTA , expect first opposition, and eventually more, subtle hazards and valuable corrective measures.
- Efforts to promote STAMP among RT practitioners & manufacturers are still needed

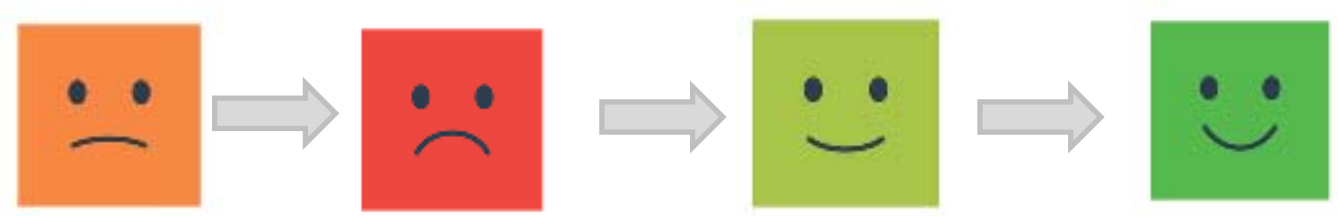
Future work

- Publish the results in Journal of Safety Science
- Apply STPA for new RT processes
- More STAMP-FMEA comparison experiments

Acknowledgements

- Jaap van Ekris (Delta Pi, NL)
- Nancy Leveson (MIT, US)
- Todd Pawlicki (University of California, US)
- John Thomas (MIT, US)
- Aubrey Samost (MIT, US)
- Simon Whiteley (Whiteley Safety Engineering, UK)

This was a story of how we stopped worrying about probabilities and learned to love STAMP….



Thank you!