Using STAMP to Prevent Accidents in Radiation Therapy

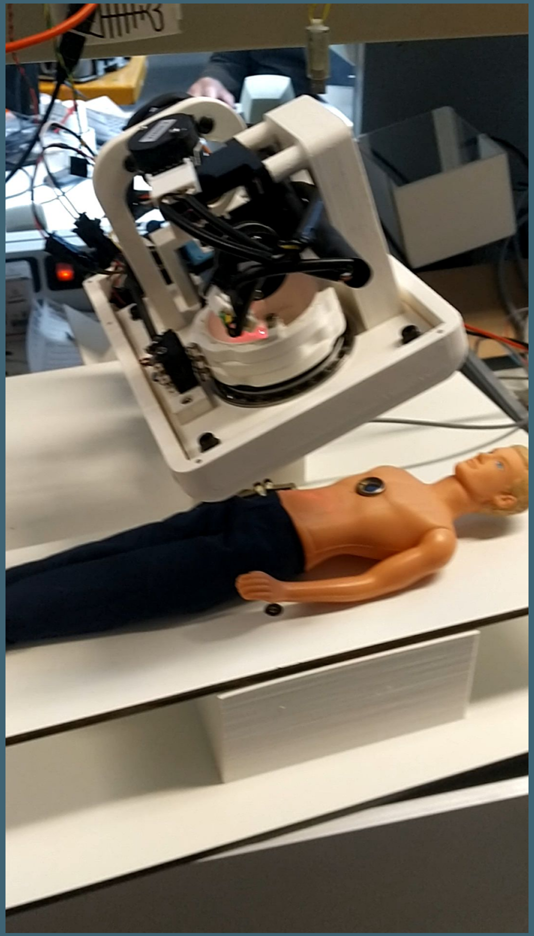
Natalia Silvis-Cividjian

ICCR-2024, Lyon

VU VRIJE UNIVERSITEIT AMSTERDAM

Rationale

- We are teaching CS students how to test software, for functionality and safety
- We use Therac-25 RT accidents to sensitize students
- We use STAMP to generate safety test scenarios and analyze accidents
- We used STAMP for safety analysis in RT
- STAMP is a rising star in industry, but not in RT



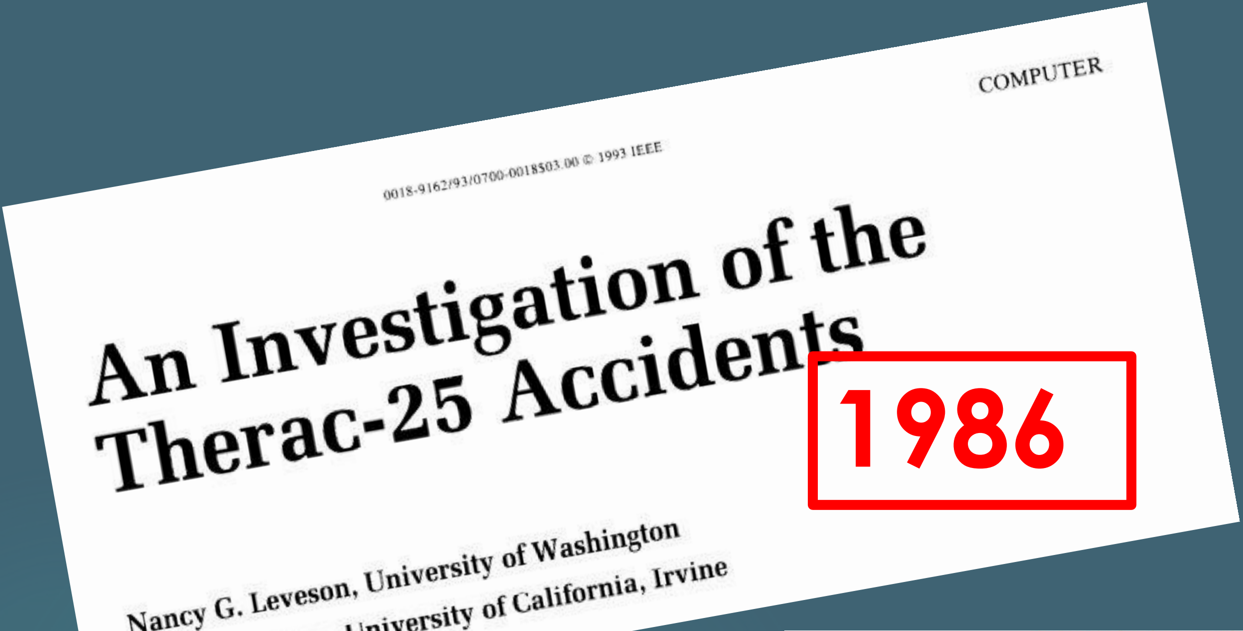
How to use STAMP in RT?

What did we learn from using STAMP in RT?

Outline

- STAMP philosophy
- STAMP for hazard analysis
- STAMP to understand accidents
- Lessons and future plans

Historical Accidents



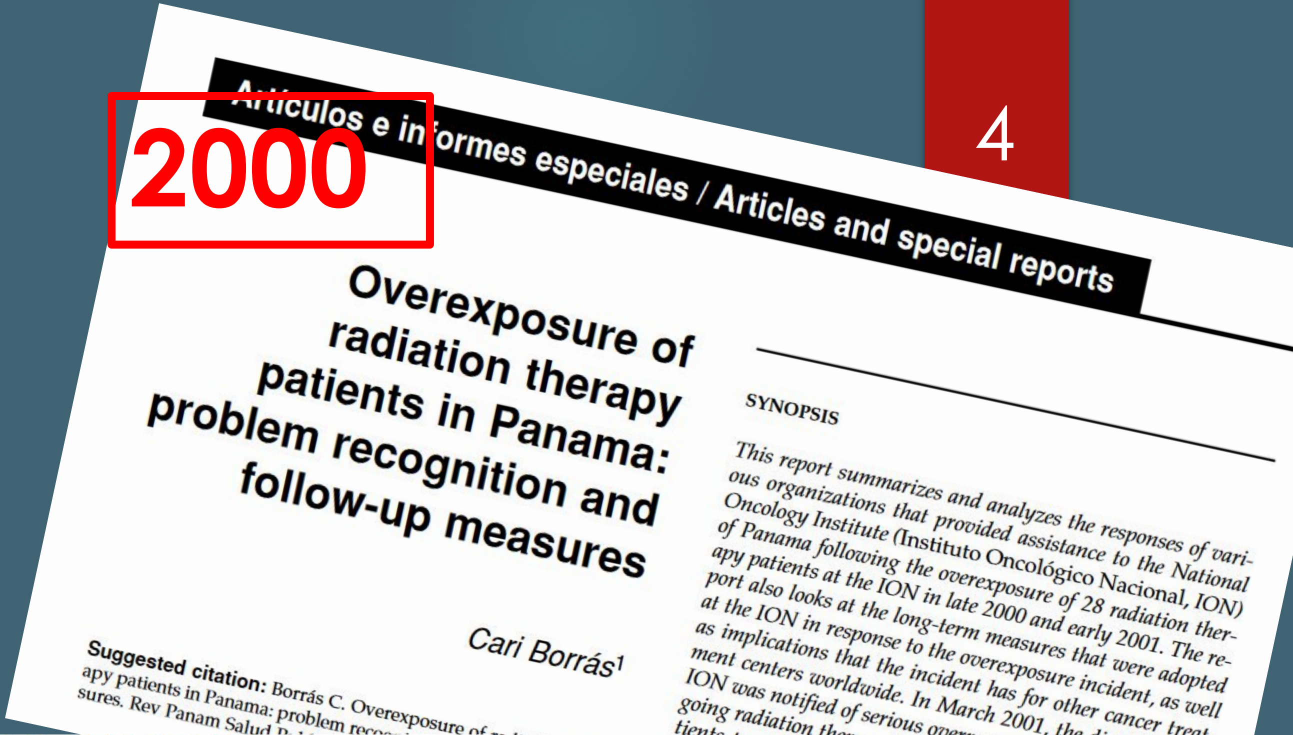
0018-9162/93/0700-0018$03.00 © 1993 IEEE

COMPUTER

An Investigation of the Therac-25 Accidents

Nancy G. Leveson, University of Washington
Clark S. Turner, University of California, Irvine

1986



rtículos e informes especiales / Articles and special reports

2000

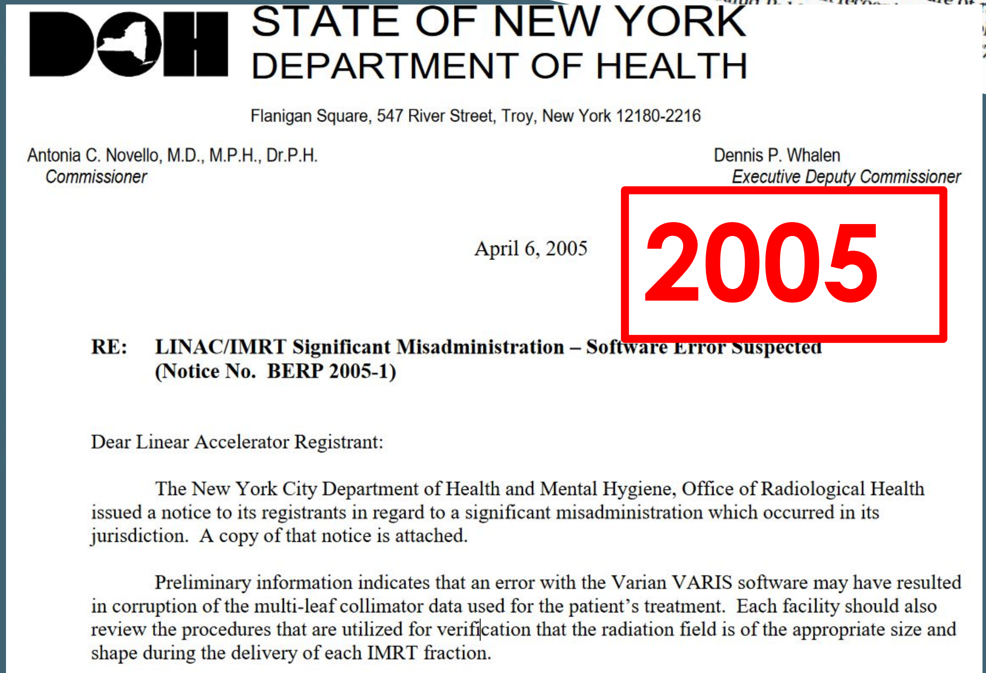
Overexposure of radiation therapy patients in Panama: problem recognition and follow-up measures

Cari Borrás[1]

Suggested citation: Borrás C. Overexposure of radiation ther-apy patients in Panama: problem recog ... llow-up mea-sures. Rev Panam Salud P ... 7.

SYNOPSIS

This report summarizes and analyzes the responses of various organizations that provided assistance to the National Oncology Institute (Instituto Oncológico Nacional, ION) of Panama following the overexposure of 28 radiation therapy patients at the ION in late 2000 and early 2001. The report also looks at the long-term measures that were adopted at the ION in response to the overexposure incident, as well as implications that the incident has for other cancer treatment centers worldwide. In March 2001, the director of the ION was notified of serious overreactions in patients undergoing radiation therapy for cancer treatment. Of the 478 patients treated for pelvic cancers between August 2000 and March 2001, 3 of them had died, possibly from an overdose of radiation. In response, the Government of Panama invited international experts to carry out a full investigation of the situation. Medical physicists from the Pan American Health Organization (PAHO) were among those invited. They as-



DOH STATE OF NEW YORK
DEPARTMENT OF HEALTH

Flanigan Square, 547 River Street, Troy, New York 12180-2216

Antonia C. Novello, M.D., M.P.H., Dr.P.H.
Commissioner

Dennis P. Whalen
Executive Deputy Commissioner

April 6, 2005

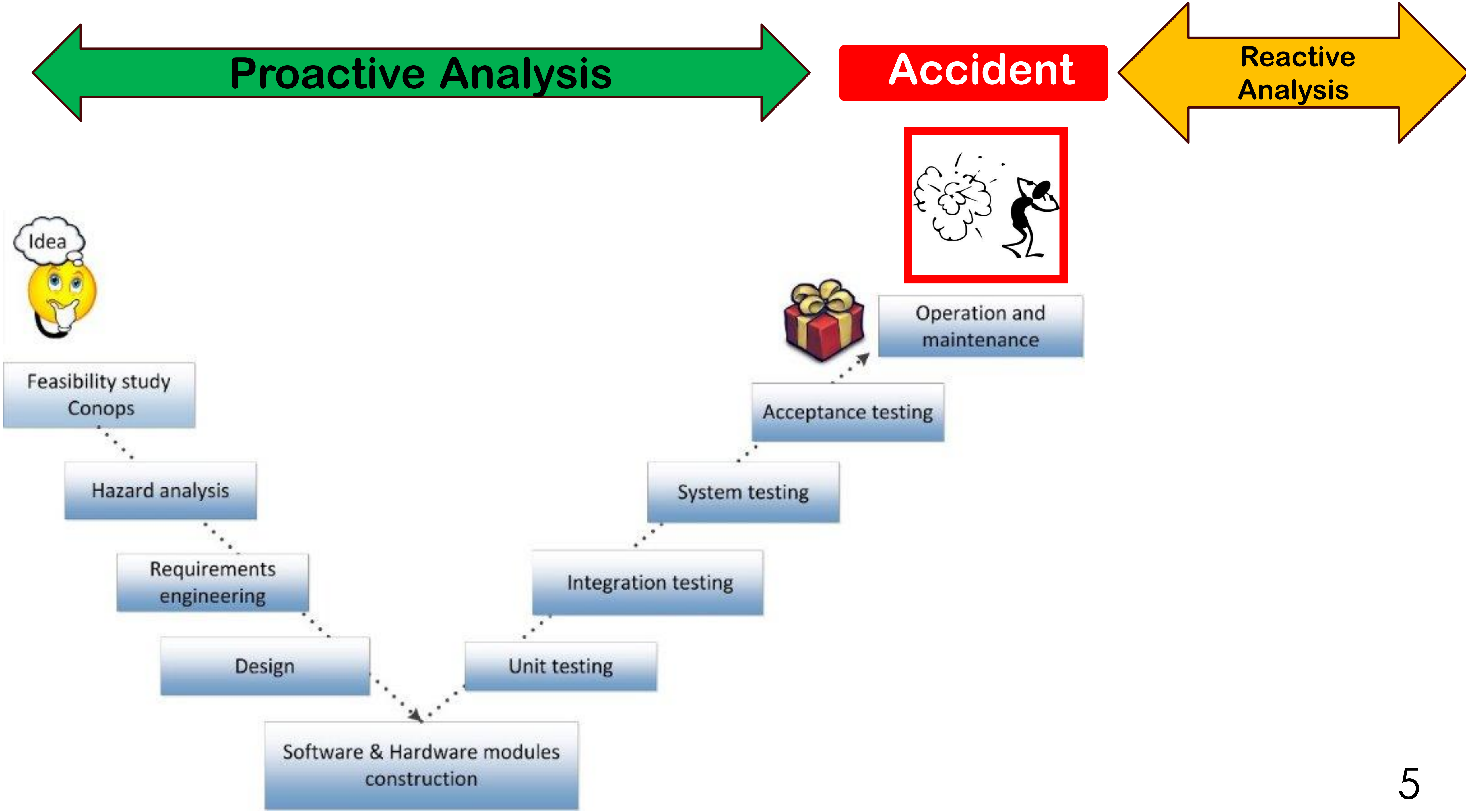
2005

RE: LINAC/IMRT Significant Misadministration – Software Error Suspected (Notice No. BERP 2005-1)

Dear Linear Accelerator Registrant:

The New York City Department of Health and Mental Hygiene, Office of Radiological Health issued a notice to its registrants in regard to a significant misadministration which occurred in its jurisdiction. A copy of that notice is attached.

Preliminary information indicates that an error with the Varian VARIS software may have resulted in corruption of the multi-leaf collimator data used for the patient's treatment. Each facility should also review the procedures that are utilized for verification that the radiation field is of the appropriate size and shape during the delivery of each IMRT fraction.



Proactive Analysis

Accident

Reactive Analysis

Idea

Feasibility study Conops

Hazard analysis

Requirements engineering

Design

Software & Hardware modules construction

Unit testing

Integration testing

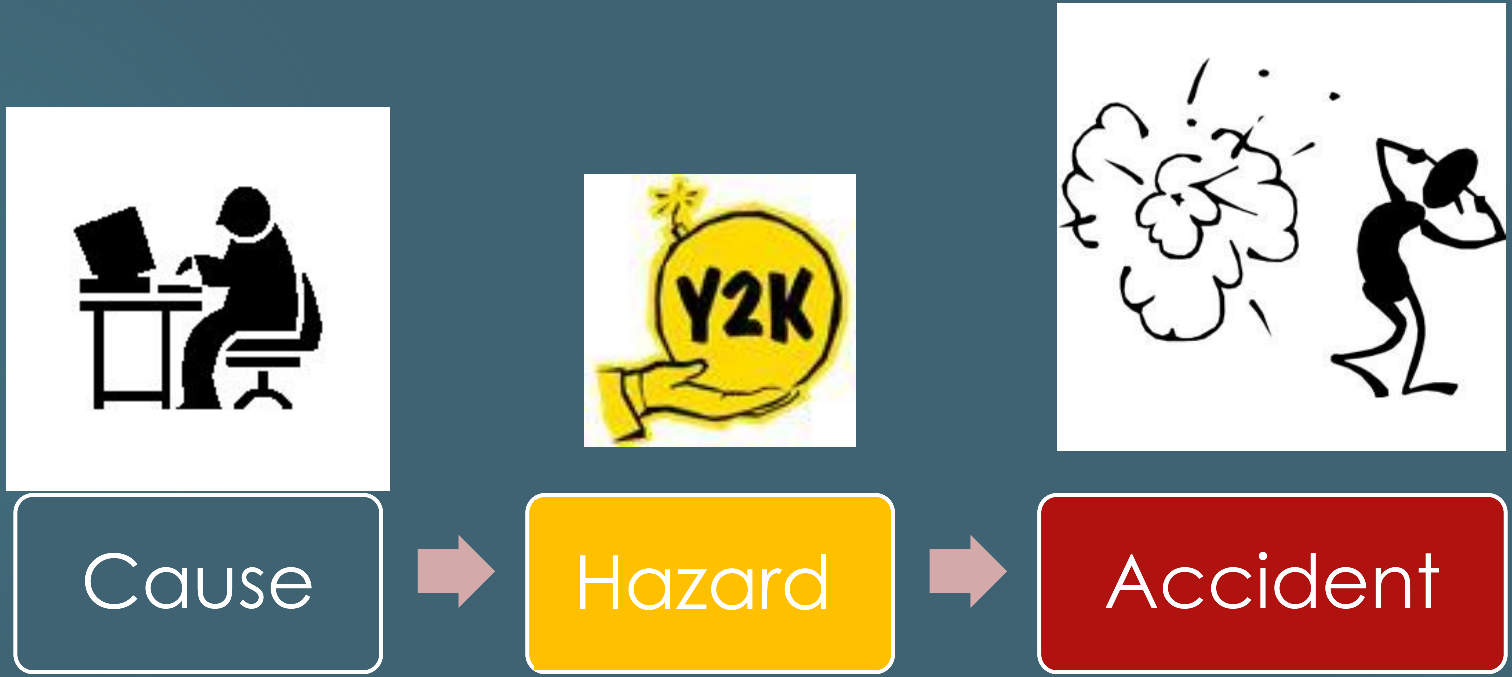
System testing

Acceptance testing

Operation and maintenance

Safety analysis methods

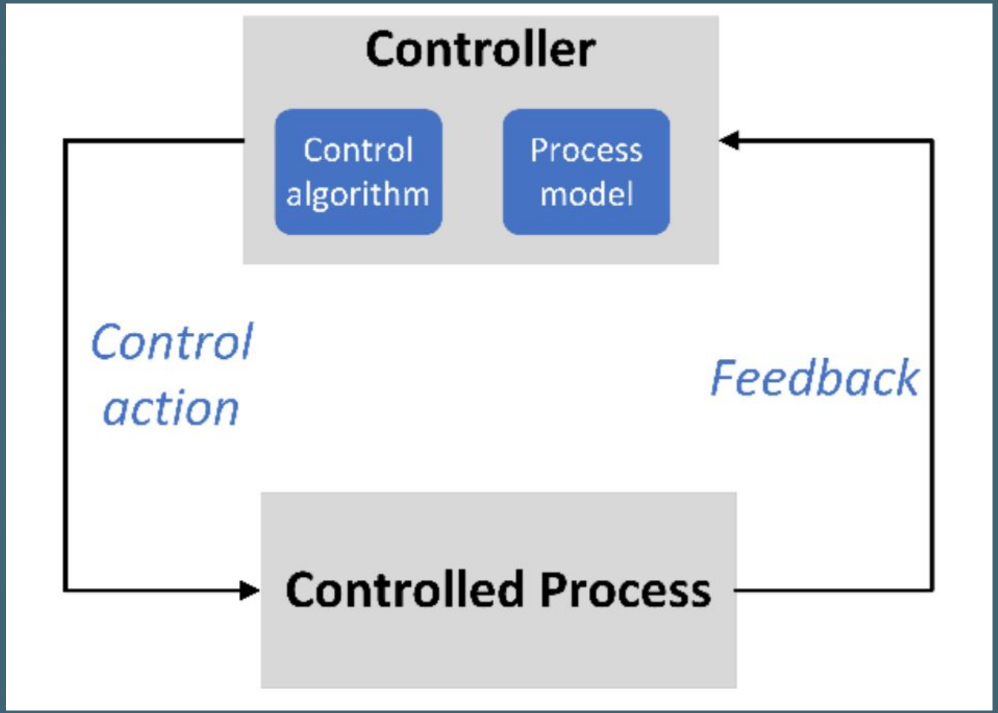
- Traditional: FTA, FMEA, (H)FMEA, HAZOP, root-cause
- New: Systems-Theoretic Accident Model and Processes (STAMP) (Leveson 2004)



Cause → Hazard → Accident

STAMP philosophy I

- “Accidents happen not because of components failures, but because of control flaws”



A safety control structure

STAMP philosophy II

- “Any accident is caused by one of the following hazards:”
- Control action Not Given
- Wrong control action Given
- Control action Given, but not in sync
- Control action applied too long, or stopped too soon
- Control action Given, but not executed

Outline

- STAMP philosophy
- STAMP for hazard analysis
- STAMP to understand accidents
- Lessons and future plans

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*

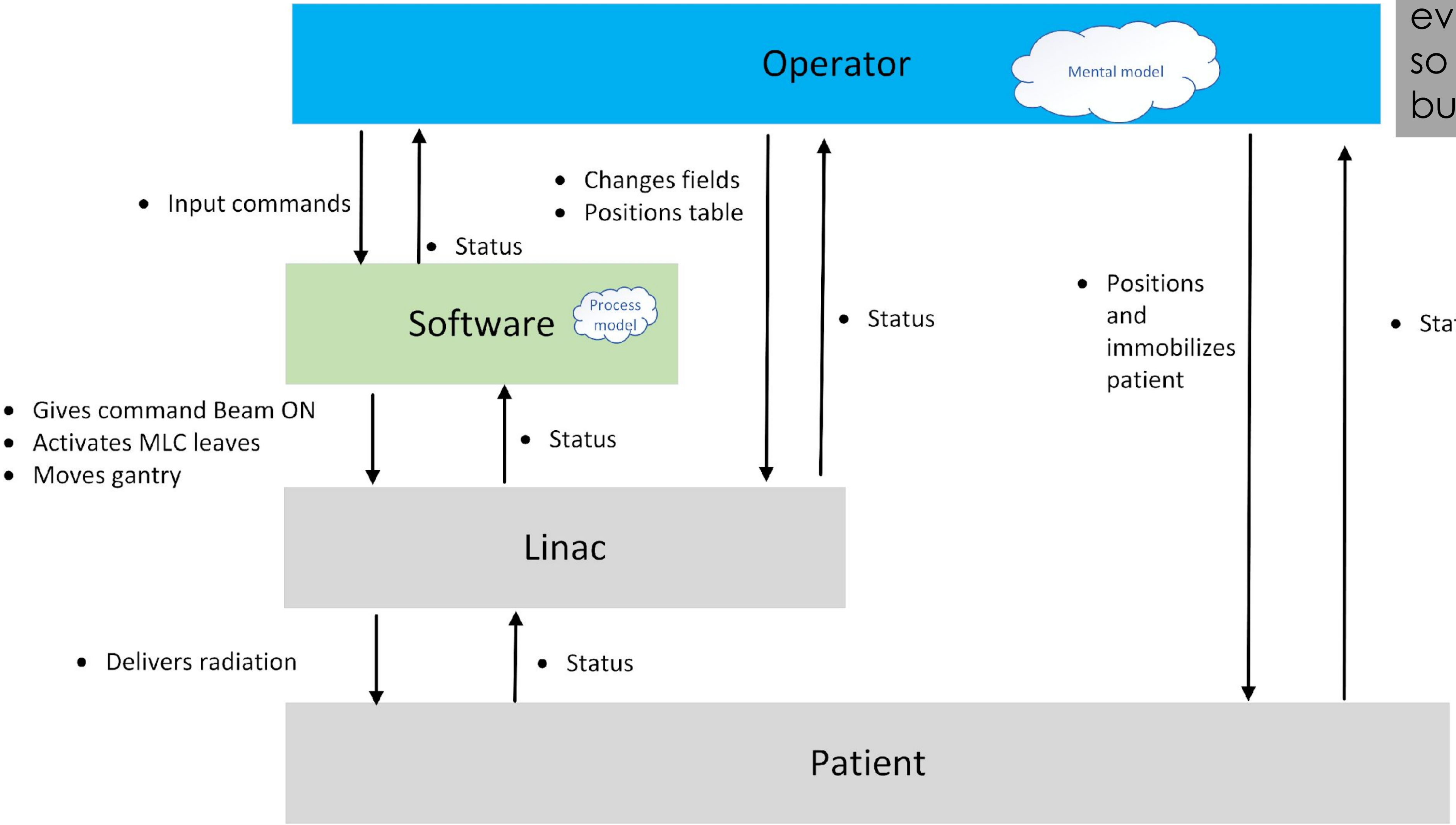
Possible Accidents (Nightmares)

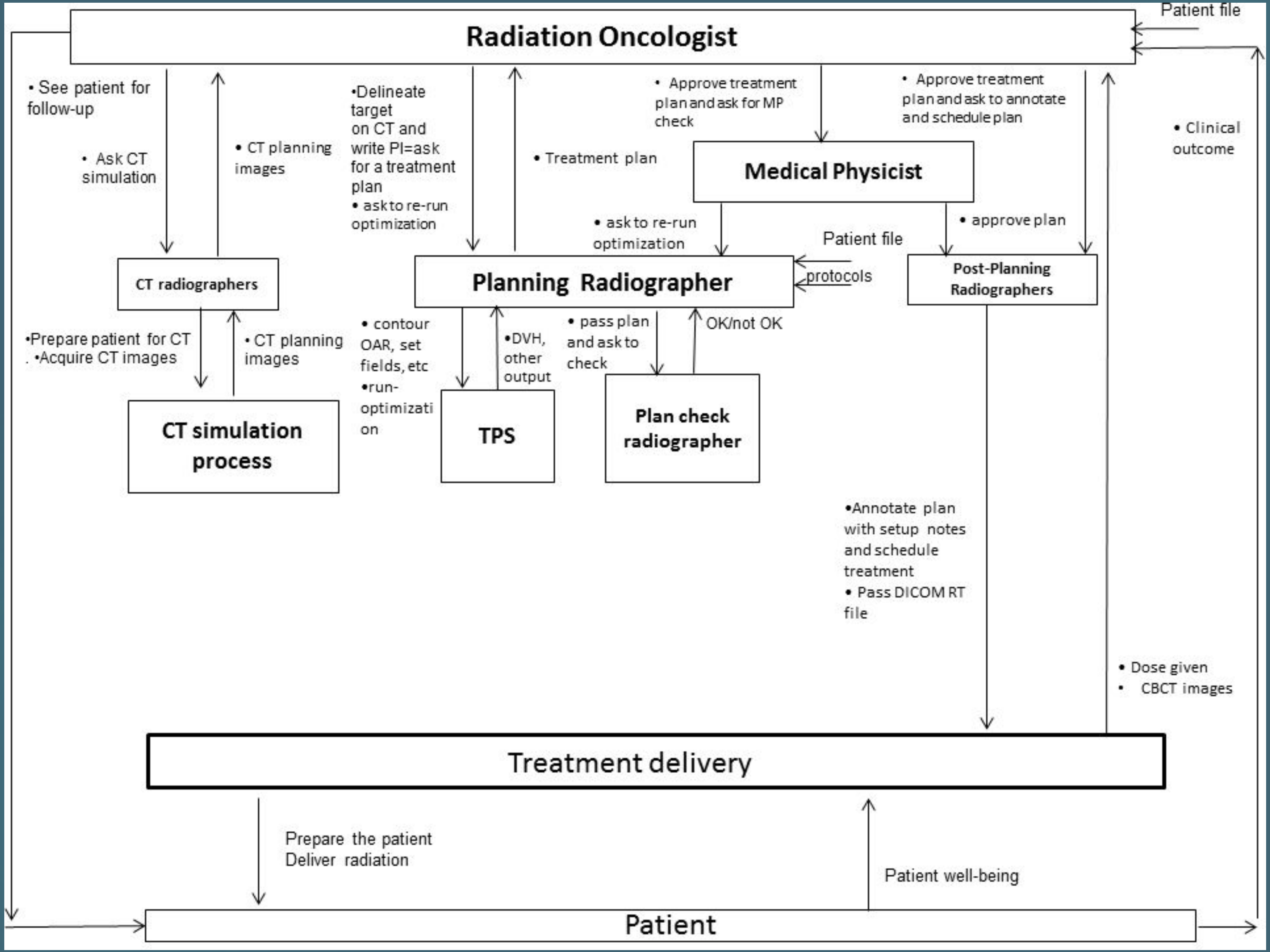
- A1. Patient injured or killed from radiation exposure
- A2. A non-patient is injured or killed by radiation exposure
- A3. Damage or loss of equipment
- A4. Physical damage to patient or non-patient during treatment (not from radiation)
- A5. Patient dies because the treatment is delayed)(new)

Inspired from: 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

STPA-Step 1. Draw a control structure

Mental model: “I think everything is set correctly, so I press the Beam ON button”





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 fields, etc
- run-optimization
- DVH, other output
- pass plan and ask to check

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
Deliver radiation

Patient well-being

Patient

From: Silvis-Cividjian, N., Verbakel, W., & Admiraal, M. (2020).

STPA-Step 2.Unsafe control actions (=hazards)

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
RTT optimizes treatment plan		RTT designed a suboptimal plan	RTT sends the plan to treatment delivery before it has been approved	RTT optimizes the plan too long

Plus: CA given but never executed

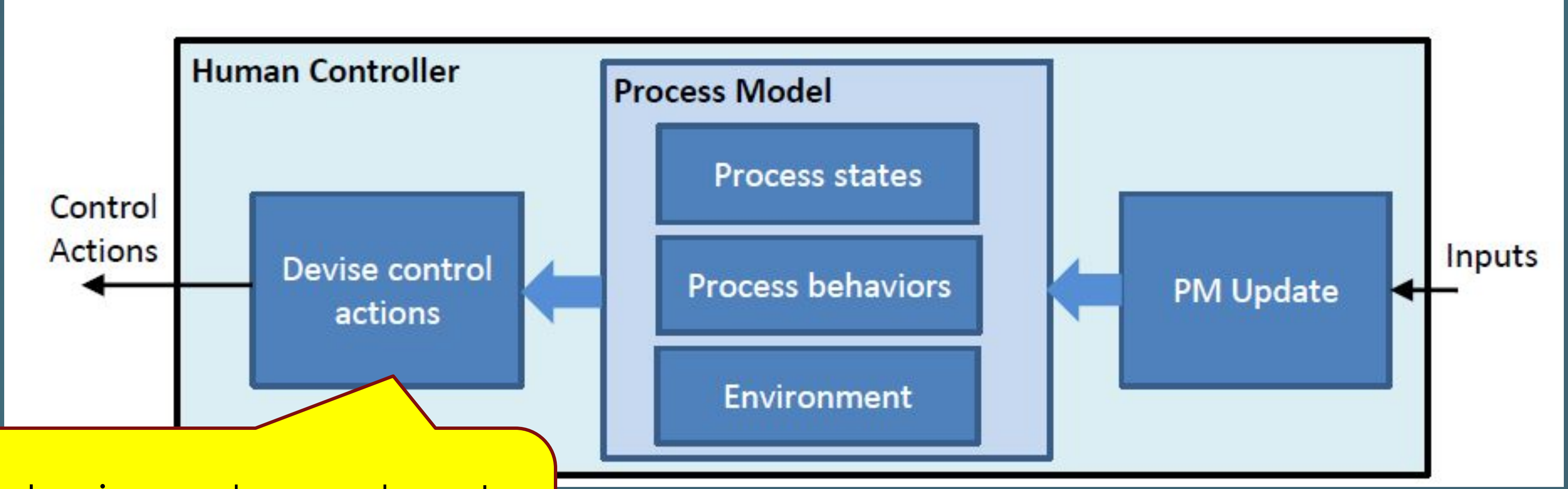
STPA-Step 3. Causal scenarios

- Answer the question Why? Which scenarios could lead to each hazard?

Extended STAMP model for human controllers

[Thomas & France, 2016]

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



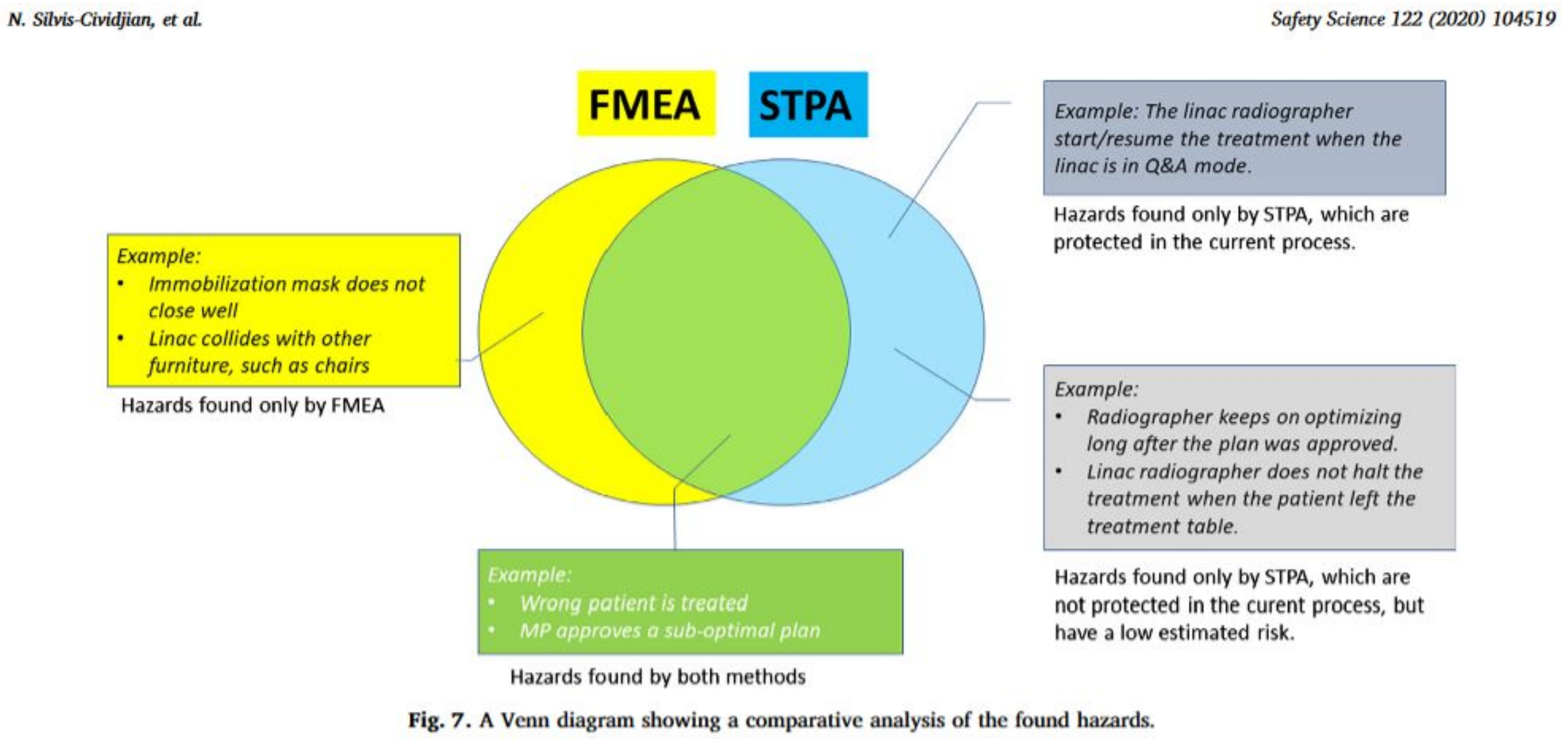
"The plan is good enough, so I stop optimization (and send it back to oncologist) "

Possible causal scenarios

- *Incorrect belief of the process state.*
  - PI or protocols are ambiguous and not clear , RTT does not dare to ask for help
  - RTT *thinks* that their way of collimator positioning is better, but they *overlook* that radiation hot spots are created
  - RTT was interrupted by a telephone call or pager, and as a result *forgets* where they were in the planning procedure.

Step 4. Mitigation measures

- Mitigation measures: Can be operated (1) in procedures, (2) in software, (3) in hardware.
- Example: Change the procedure and enforce RTT to ask the help of a superior in max two days
- Use reminders
- Use AI?



N. Silvis-Cividjian, et al.

Safety Science 122 (2020) 104519

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

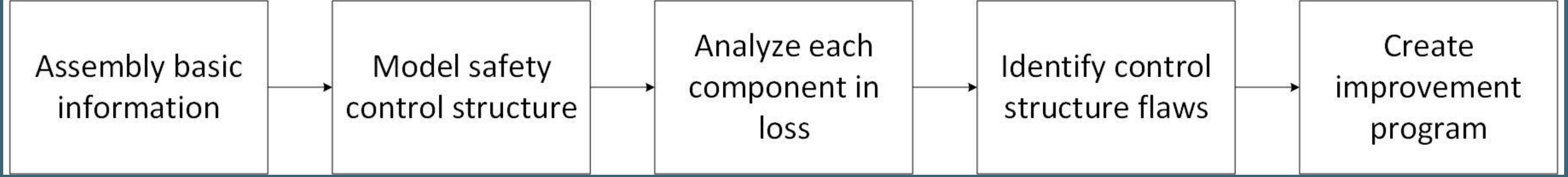
Fig. 7. A Venn diagram showing a comparative analysis of the found hazards.

STAMP-STPA evaluation

- Can find more hazardous situations than FMEA
- Identifies other organizational factors and actors except the RTT, shares the responsibility
- Can start early, before implementation
- Needs less time and domain knowledge (can be conducted by a computer scientist)

Outline

- STAMP philosophy
- STAMP for hazard analysis
- ● STAMP to understand accidents
- Lessons and future plans



Assembly basic information → Model safety control structure → Analyze each component in loss → Identify control structure flaws → Create improvement program

[Leveson, CAST Handbook, 2019]

The Boyhood of Raleigh by Sir John Everett Millais, oil on canvas, 1870.A seafarer tells the young Sir Walter Raleigh and his brother the stor...

Controller	Responsability	Contribution
RTT	**Saves treatment data in ARIA**	**Did not save treatment data**
Linac software	**Assist RTT in treatment delivery**	**Did not ask: “Are you sure you do not want to save the file?”**
Physics team	Writes protocols on what to do if a linac is defect	
Safety management	Trains staff for emergency situations	
Software manufacturer	Tests the linac software for degraded conditions, such as a defect linac, an avalanche of error messages, users in panic, etc	
More?		

VU VRIJE UNIVERSITEIT AMSTERDAM

UCA: Radiographer did not save the treatment data. WHY?

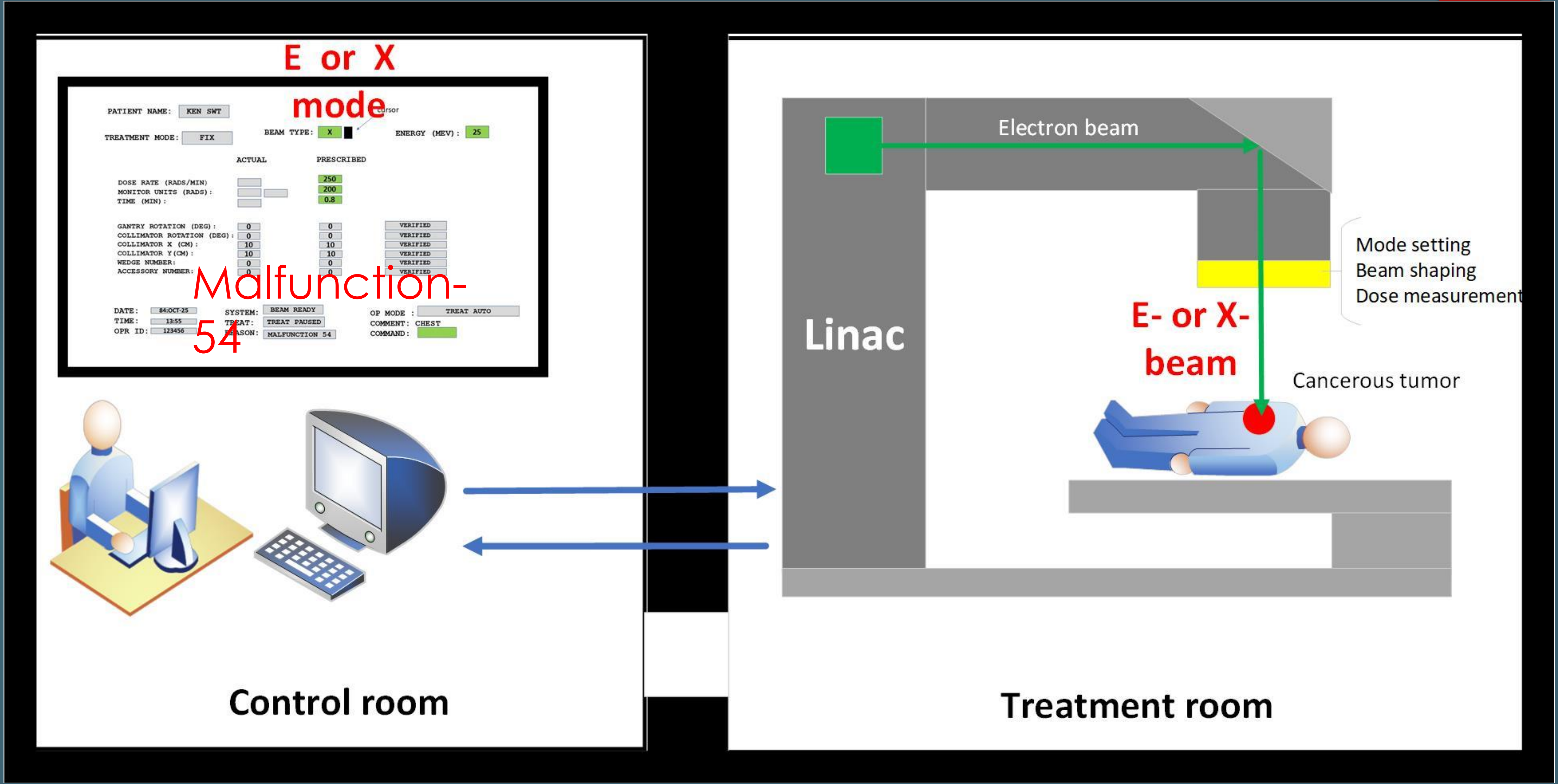
Possible Mental model flaws

Maybe software asked: "Do you want to delete data?" RTT was used to answer with Yes to all pop-up windows. So he probably answered Yes.

Maybe RTT expected the software to ask first :"Are you sure you want to delete the data?"

Maybe RTT assumed he can solve all tasks simultaneously and that everybody expects this. Did not want to disappoint the colleagues. Usually this worked.

Example: Therac-25 accidents

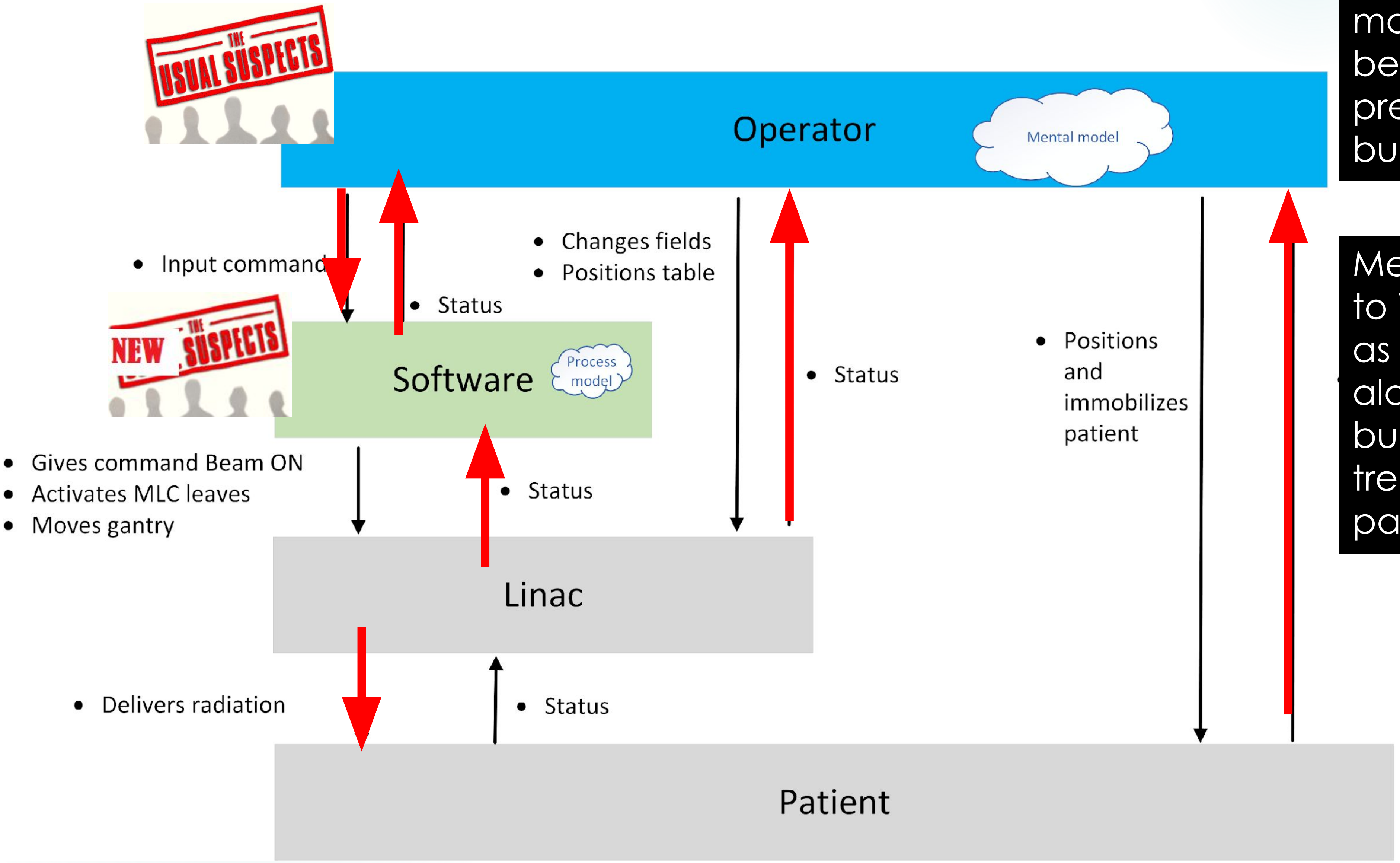


```
PATIENT NAME:  KEN SWT
TREATMENT MODE:  FIX          BEAM TYPE:  X  ▮          ENERGY (MEV):  25

                                ACTUAL        PRESCRIBED
  DOSE RATE (RADS/MIN)                          250
  MONITOR UNITS (RADS):                         200
  TIME (MIN):                                   0.8

  GANTRY ROTATION (DEG):         0              0       VERIFIED
  COLLIMATOR ROTATION (DEG):     0              0       VERIFIED
  COLLIMATOR X (CM):            10             10       VERIFIED
  COLLIMATOR Y (CM):            10             10       VERIFIED
  WEDGE NUMBER:                  0              0       VERIFIED
  ACCESSORY NUMBER:              0              0       VERIFIED

DATE:    84:OCT-25     SYSTEM:  BEAM READY          OP MODE :  TREAT AUTO
TIME:    13:55         TREAT:   TREAT PAUSED        COMMENT:   CHEST
OPR ID:  123456        REASON:  MALFUNCTION 54      COMMAND:
```

Interviewing a Therac-25 witness

Silvis-Cividjian, Hager. Speak Memory! Analyzing Historical Accidents to Sensitize Software Testing Novices, *ICSE-SEET 2023.*

Control structure



Mental model: "I see Beam Ready, I think the machine is in E mode, becaus I typed E, so I press the Beam ON button"

Mental model: "I am used to ignore error messages as they are all false alarms. So I press Proceed button to resume treatment after the pause.

Causal scenarios

- Unsafe control action#1:
  - RTT hit Beam ON when system was not safe. Why?
- Causal Scenarios. Beam Ready message was displayed. RTT thought (wrongly) that the machine was fully in E mode so they Hit Beam ON.
- Mitigation: software should know what hardware is doing at all times.
- Unsafe control action#2:
  - After Malfunction-54 pause, RTT hit Proceed when it was not safe. Why?
- Causal scenario. Ion chamber was saturated, intercom system was malfunctioning, “Malfunction 54” message was too cryptical (just said Dose error), operator was used to get more than 5 false error messages per day and started to ignore them.
- Mitigation measure: Software should generate informative error messages. Proceed after pause should be done only by authorized persons.

STAMP-CAST for RT

- STAMP-CAST easily finds the same major problems as traditional methods
- However, CAST can find new causality that takes the blame from the shoulders of the usual suspects.
- Good guidance to continue generating tactful questions during investigations when traditional analysis stops, especially for human operators.
- Software plays an important role in preventing but also creating accidents.

Outline

- STAMP philosophy
- STAMP for hazard analysis
- STAMP to understand accidents
- ● Lessons and future plans

Lessons learned after using STAMP

- STAMP is suitable for proactive and reactive analysis in RT
- This can be achieved with less resources and domain knowledge.
- STAMP can be applied early, before the implementation.
- Software is not perfect and should be considered as an actor in an RT risk analysis.

Future plans

- Use STAMP to analyze recent incidents in RT
- Build tools to assist safety analysis in RT
- Understand the interaction of RTTs with software

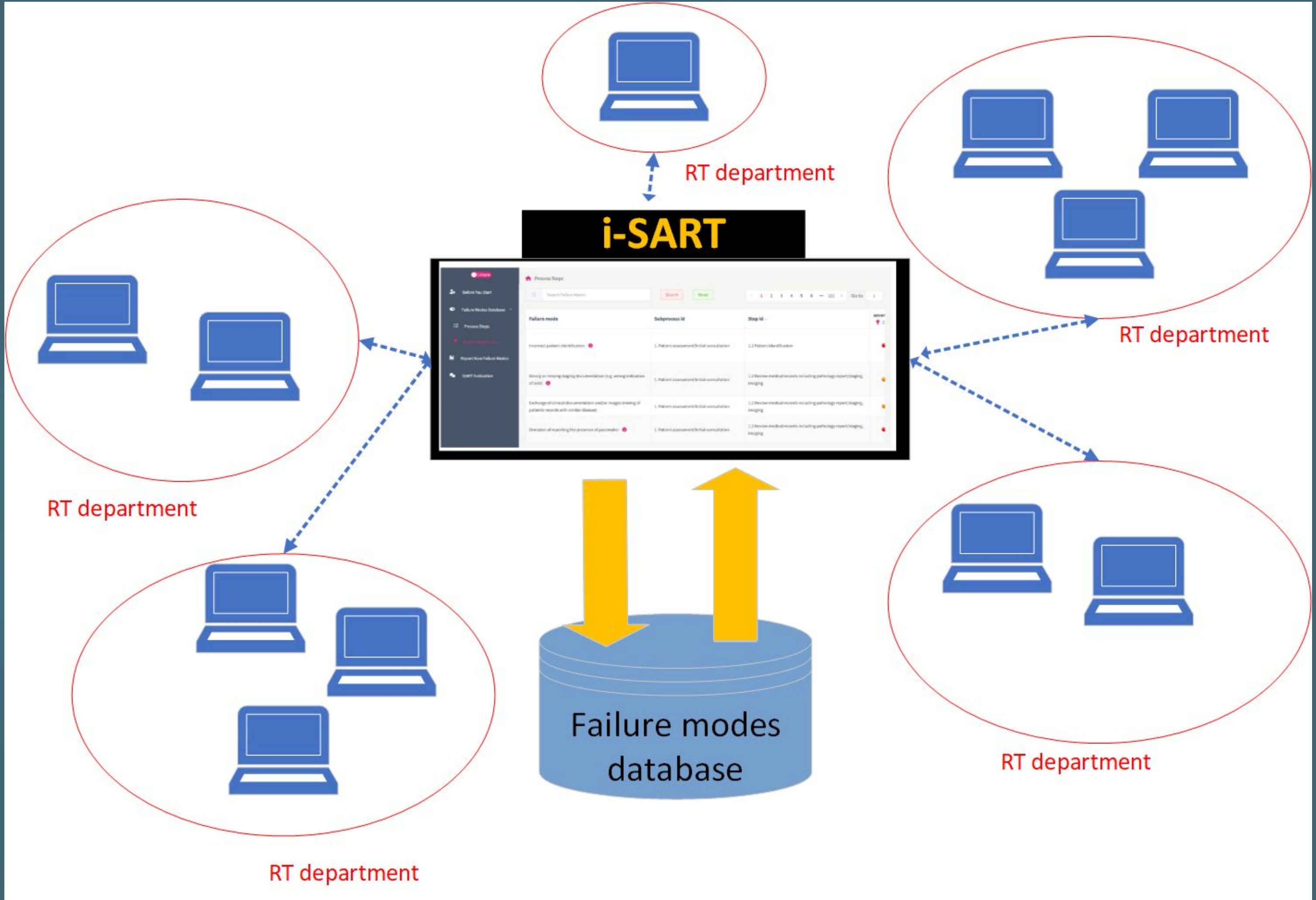
1. Analyze recent RT incidents

Let's create a community to learn from RT incidents!

- Please email me at: n.silvis-cividjian@vu.nl

Together we can make RT safer!

2. Assist safety analysts in RT

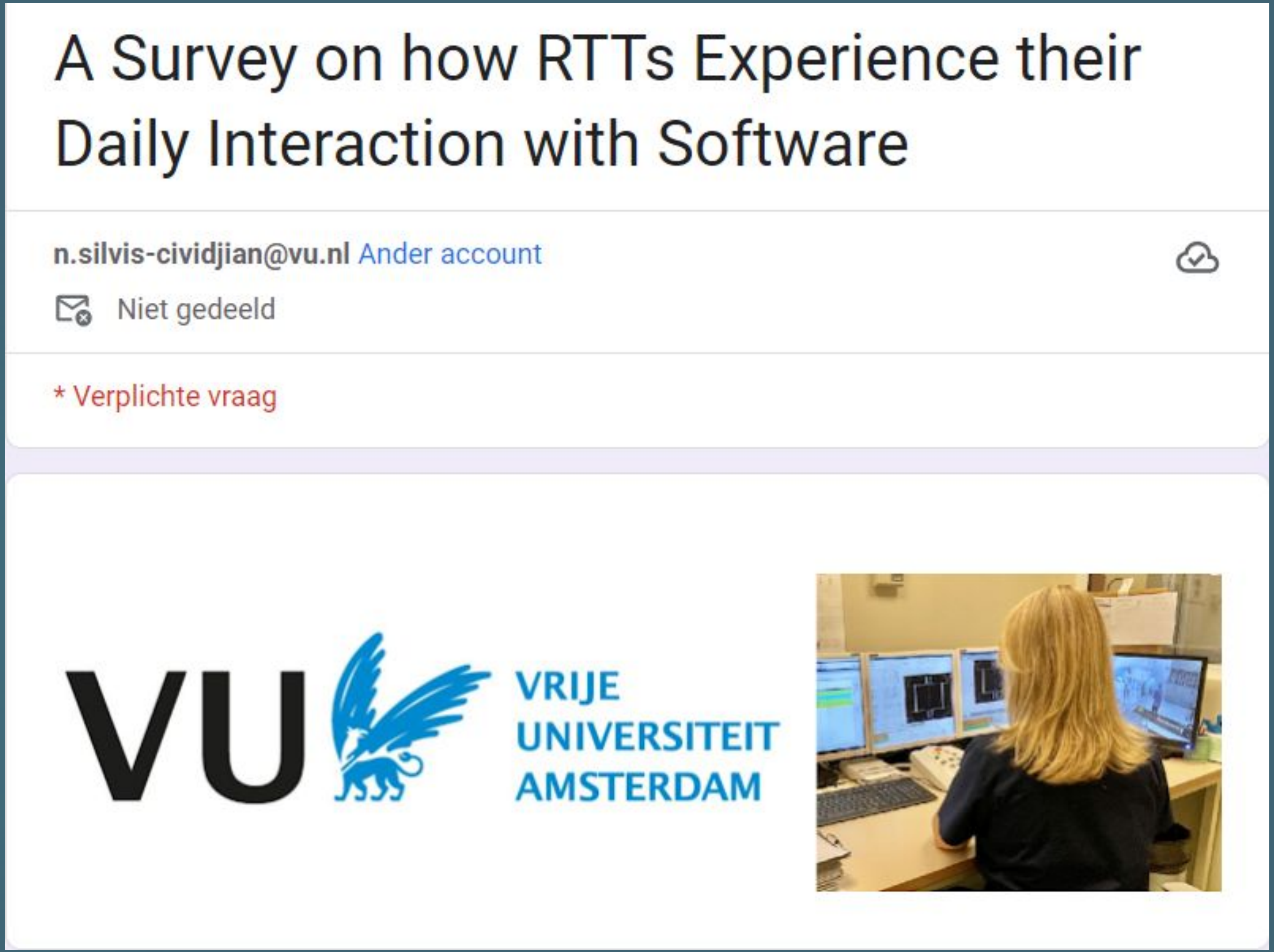


i-SART: A Prototype AI-based Tool to Enhance Patient Safety in Radiotherapy
1. Introduction
2. Materials and Methods
3. Results
4. Current Work
5. Conclusion and Future Work

Silvis-Cividjian, N., Zhou, Y., Sarchosoglou, A., & Pappas, E. (2024). i-SART: An Intelligent Assistant for Safety Analysis in Radiation Therapy. In *BIOSTEC.*

3. Understand the RTT-SW tango

- https://forms.gle/yBJAHDFizTZ3KySu8



A Survey on how RTTs Experience their Daily Interaction with Software

n.silvis-cividjian@vu.nl Ander account

Niet gedeeld

* Verplichte vraag

VU VRIJE UNIVERSITEIT AMSTERDAM

SCAN ME

Results

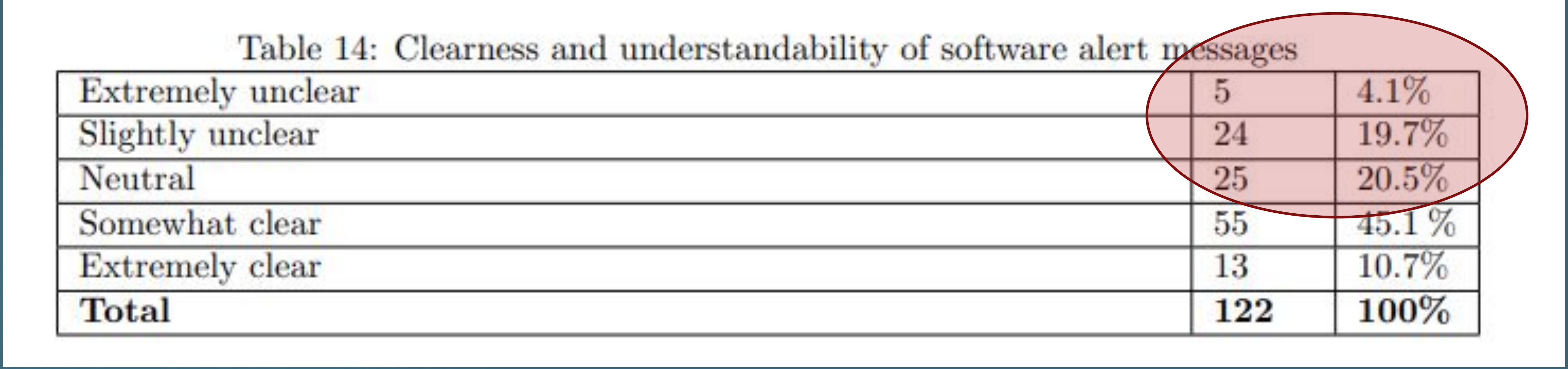


Table 14: Clearness and understandability of software alert messages

Extremely unclear	5	4.1%
Slightly unclear	24	19.7%
Neutral	25	20.5%
Somewhat clear	55	45.1 %
Extremely clear	13	10.7%
Total	**122**	**100%**

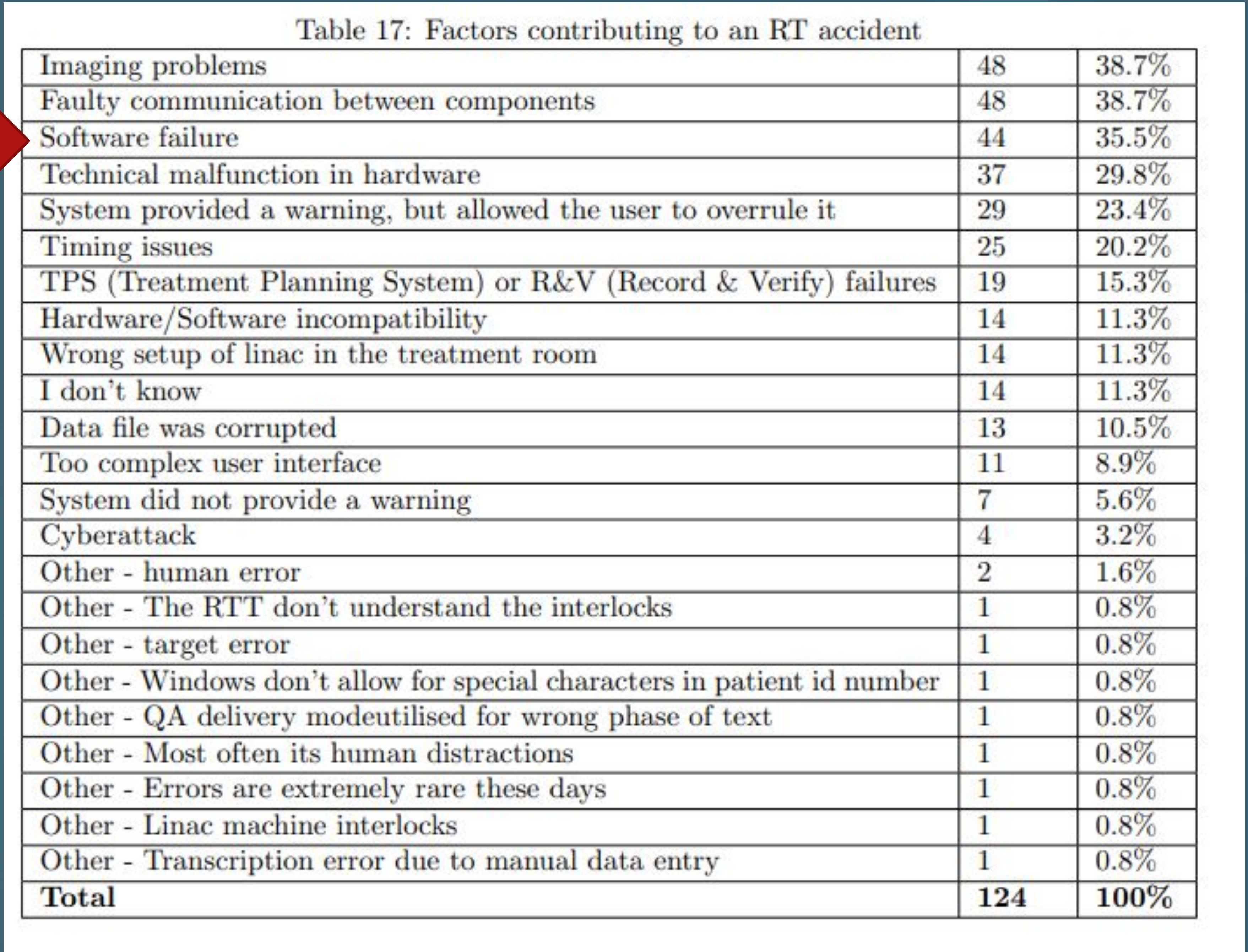


Table 17: Factors contributing to an RT accident

Imaging problems	48	38.7%
Faulty communication between components	48	38.7%
Software failure	44	35.5%
Technical malfunction in hardware	37	29.8%
System provided a warning, but allowed the user to overrule it	29	23.4%
Timing issues	25	20.2%
TPS (Treatment Planning System) or R&V (Record & Verify) failures	19	15.3%
Hardware/Software incompatibility	14	11.3%
Wrong setup of linac in the treatment room	14	11.3%
I don't know	14	11.3%
Data file was corrupted	13	10.5%
Too complex user interface	11	8.9%
System did not provide a warning	7	5.6%
Cyberattack	4	3.2%
Other - human error	2	1.6%
Other - The RTT don't understand the interlocks	1	0.8%
Other - target error	1	0.8%
Other - Windows don't allow for special characters in patient id number	1	0.8%
Other - QA delivery modeutilised for wrong phase of text	1	0.8%
Other - Most often its human distractions	1	0.8%
Other - Errors are extremely rare these days	1	0.8%
Other - Linac machine interlocks	1	0.8%
Other - Transcription error due to manual data entry	1	0.8%
Total	**124**	**100%**

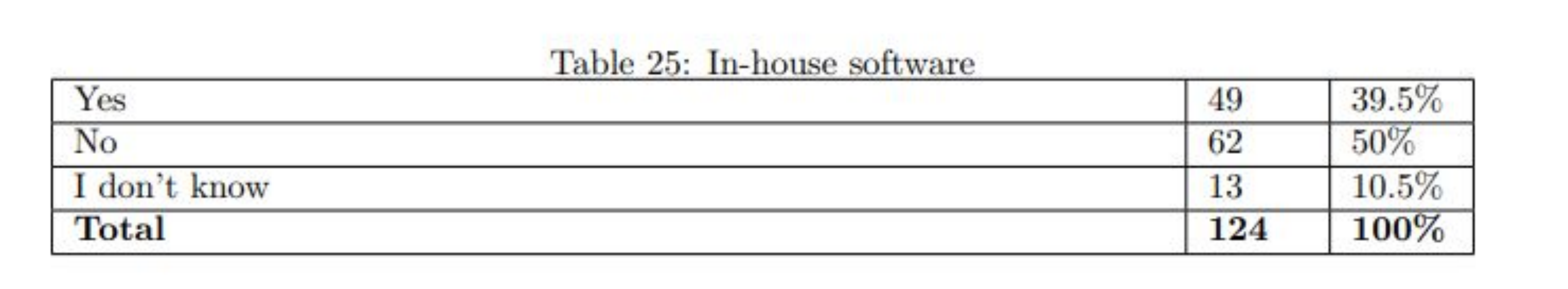


Table 25: In-house software

Yes	49	39.5%
No	62	50%
I don't know	13	10.5%
Total	**124**	**100%**

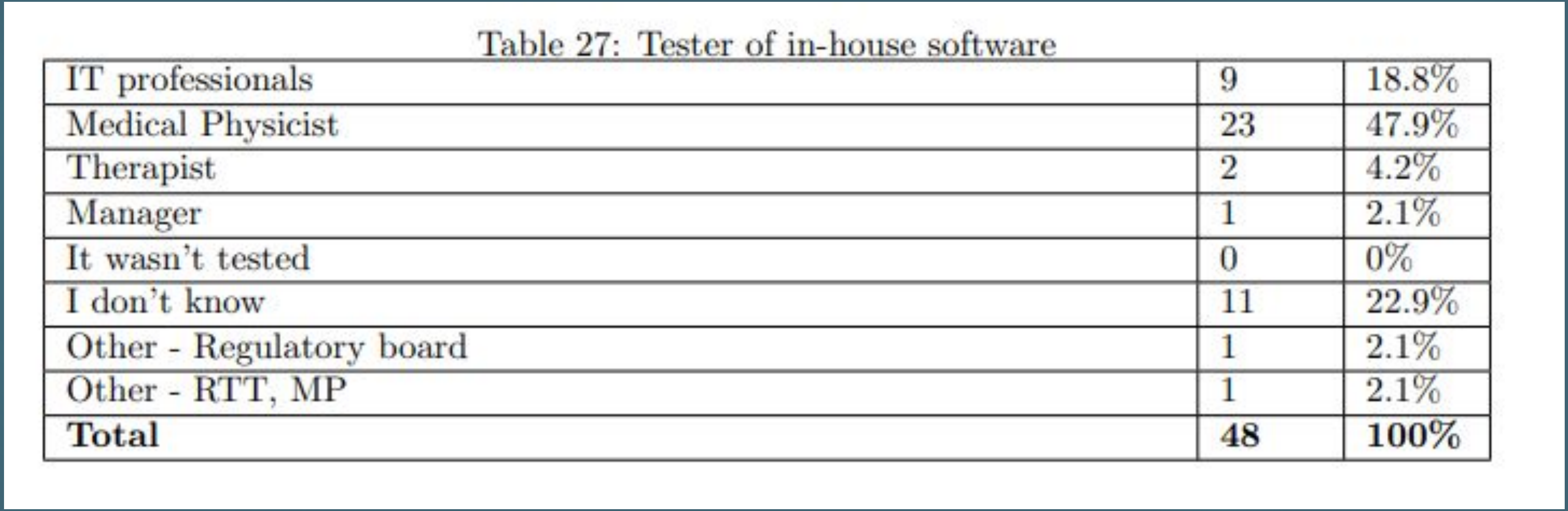


Table 27: Tester of in-house software

IT professionals	9	18.8%
Medical Physicist	23	47.9%
Therapist	2	4.2%
Manager	1	2.1%
It wasn't tested	0	0%
I don't know	11	22.9%
Other - Regulatory board	1	2.1%
Other - RTT, MP	1	2.1%
Total	**48**	**100%**

What can **software makers** do to prevent accidents?

- Think of your end-users. Make clear error messages, low rate of false alarms, avoid alarm fatigue.
- Use AI to mitigate risks
- Test your in-house software
- Analyze incidents created by software and share them with the RT and CS community

Acknowledgements

- ICCR organizers
- Nancy Leveson
- Anastasia Sarchosoglou
- Fritz Hager, Marcel van Herk, Wilko Verbakel, Marjan Admiraal, Greg Salomons, Todd Pawlicki, EFRS, all MPs and RTTs advancing safety awareness in RT

VU VRIJE UNIVERSITEIT AMSTERDAM

VU BUG 01000110 ZOO

SCAN ME

“There is no crime of which I do not deem myself capable.” ***Goethe***

Thank You!