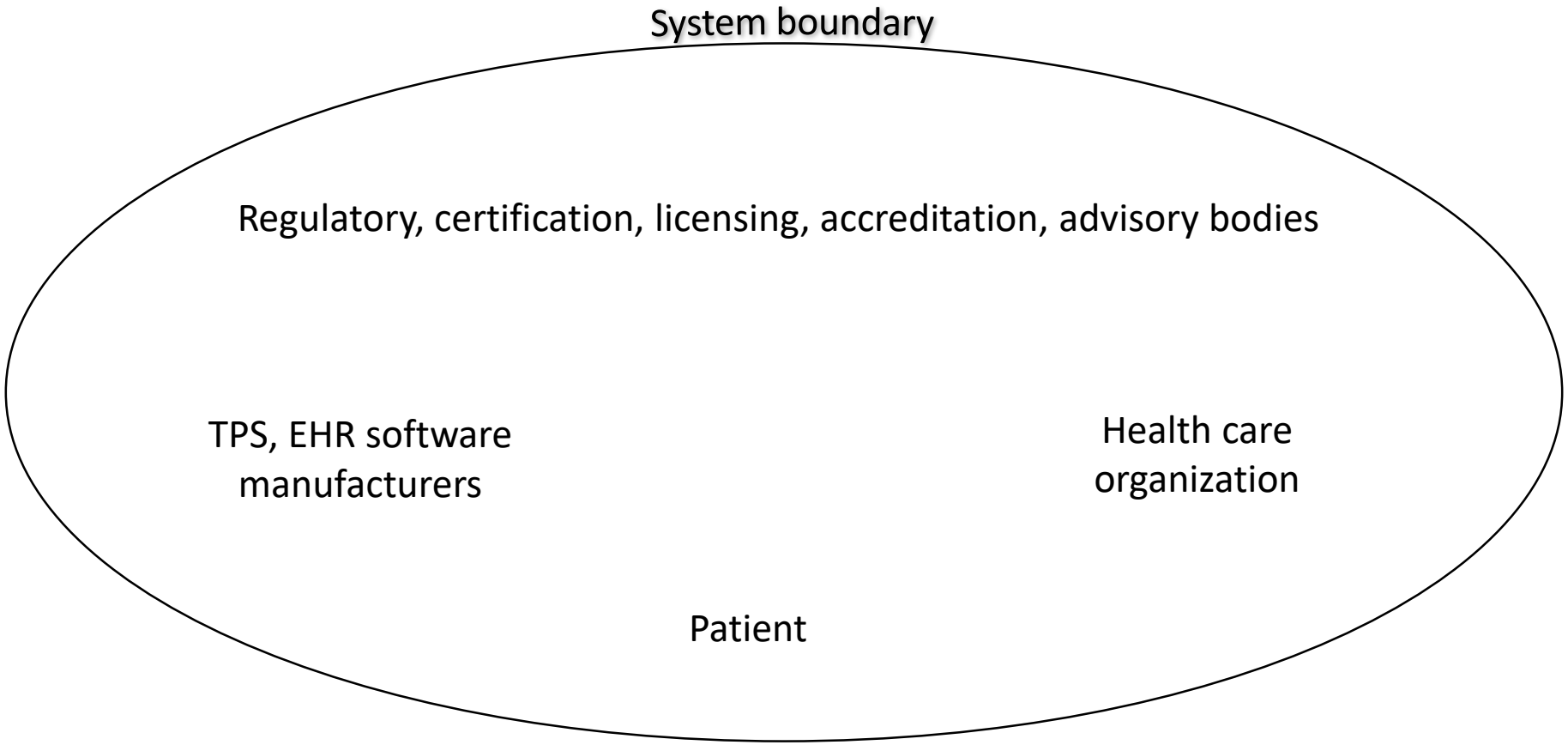
A short quiz on common mistakes in CAST/STPA

Lawrence Wong

L_wong@mit.edu

Let’s pretend that we are doing an analysis on radiation oncology – a specialty in medicine



(TPS = Treatment Planning System; EHR = Electronic Health Record)

Common mistakes when defining hazard(s)

- Definition Hazard: A system state or set of conditions that, together with specific environmental conditions, can lead to an accident or loss. (CAST Handbook p.10)

- Common **mistakes** when identifying hazards (adapted fr. STPA Handbook p.20)
  - Hazards referring to individual components of the system
  - Hazards **not** referring to the overall system and system state
  - Hazards **not** referring to factors that can be controlled by the system designers and operators
  - Hazards including ambiguous or recursive words, e.g., “unsafe”, etc.

Common mistakes when defining hazard(s) (2)

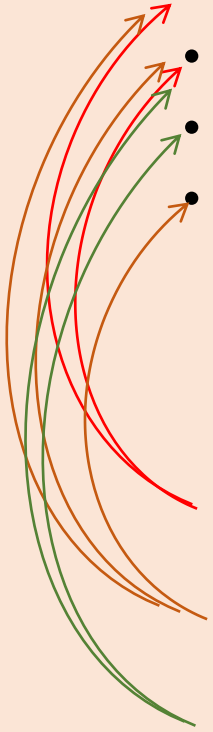
- Common **mistakes** when identifying **hazards** (STPA Handbook p.20)
  - Hazards referring to individual components of the system
  - Hazards **not** referring to the overall system and system state
  - Hazards **not** referring to factors that can be controlled by the system designers and operators
  - Hazards including ambiguous or recursive words, e.g., “unsafe”, etc.

Which of the following show(s) some common mistakes?

a) The dosimetrist failed to fuse MR image to CT for contouring
b) The linear accelerator was unsafe
c) A geomagnetic storm was heading towards Earth

Common mistakes when defining hazard(s) (3)

- Common **mistakes** when identifying **hazards** (STPA Handbook p.20)
  - Hazards referring to individual components of the system
  - Hazards **not** referring to the overall system and system state
  - Hazards **not** referring to factors that can be controlled by the system designers and operators
  - Hazards including ambiguous or recursive words, e.g., “unsafe”, etc.



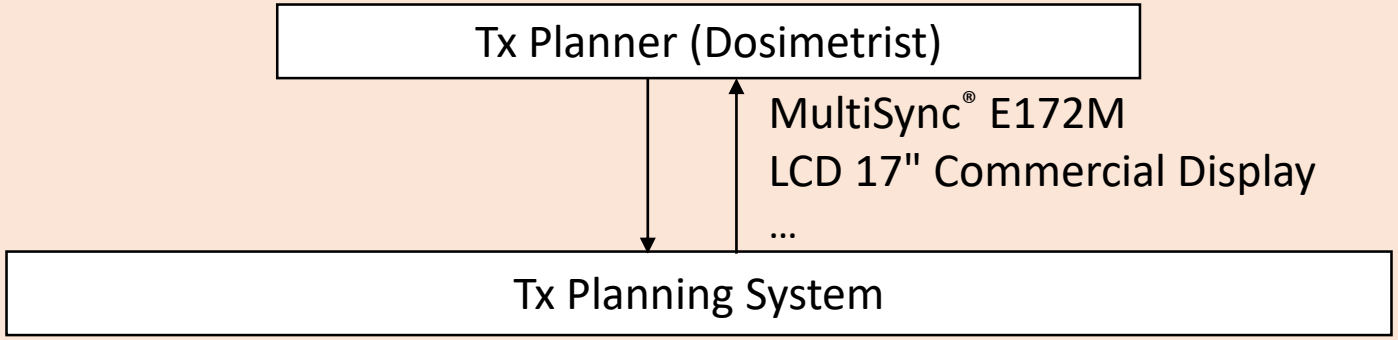
Which of the following show(s) some common mistakes? All!

a) The dosimetrist failed to fuse MR image to CT for contouring
b) The linear accelerator was unsafe
c) A geomagnetic storm was heading towards Earth

Common mistakes when modeling safety control structure

- Common **mistakes** in a control structure (adapted fr. STPA Handbook p.34)
  - Label describes a specific implementation instead of functional information
  - Ambiguous and vague labels, e.g., “command”, “feedback”, when the actual information is known
  - Physical process not controlled by one or more controllers
  - …
  - Defined too narrowly (CAST Handbook p.47)

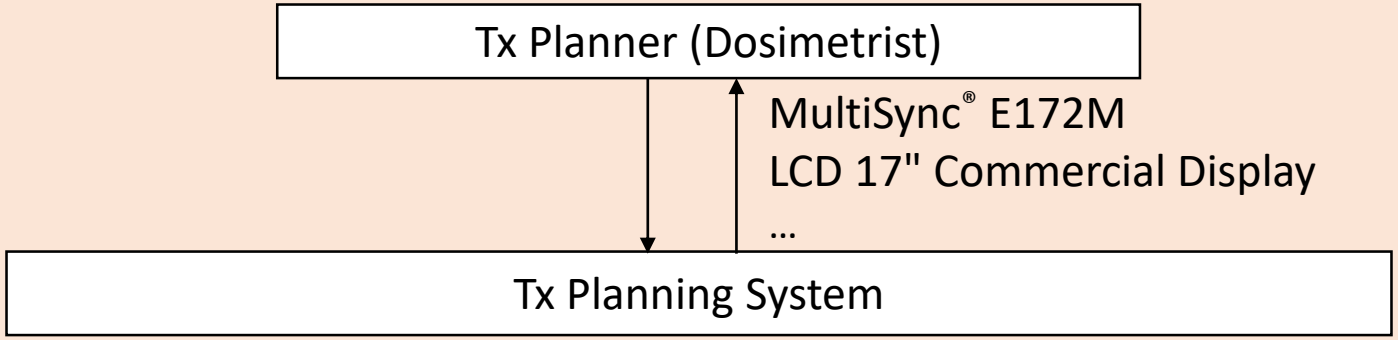
Common mistakes when modeling safety control structure (2)



Which of common mistakes does this control loop embody?

a) Label describes a specific implementation instead of functional information
b) Ambiguous and vague labels, e.g., “command”, “feedback”, when the actual information is known
c) Physical process not controlled by one or more controllers

Common mistakes when modeling safety control structure (3)



Which of common mistakes does this control loop embody?

a) Label describes a specific implementation instead of functional information
b) Ambiguous and vague labels, e.g., “command”, “feedback”, when the actual information is known
c) Physical process not controlled by one or more controllers