System Safety Engineering

Nancy Leveson

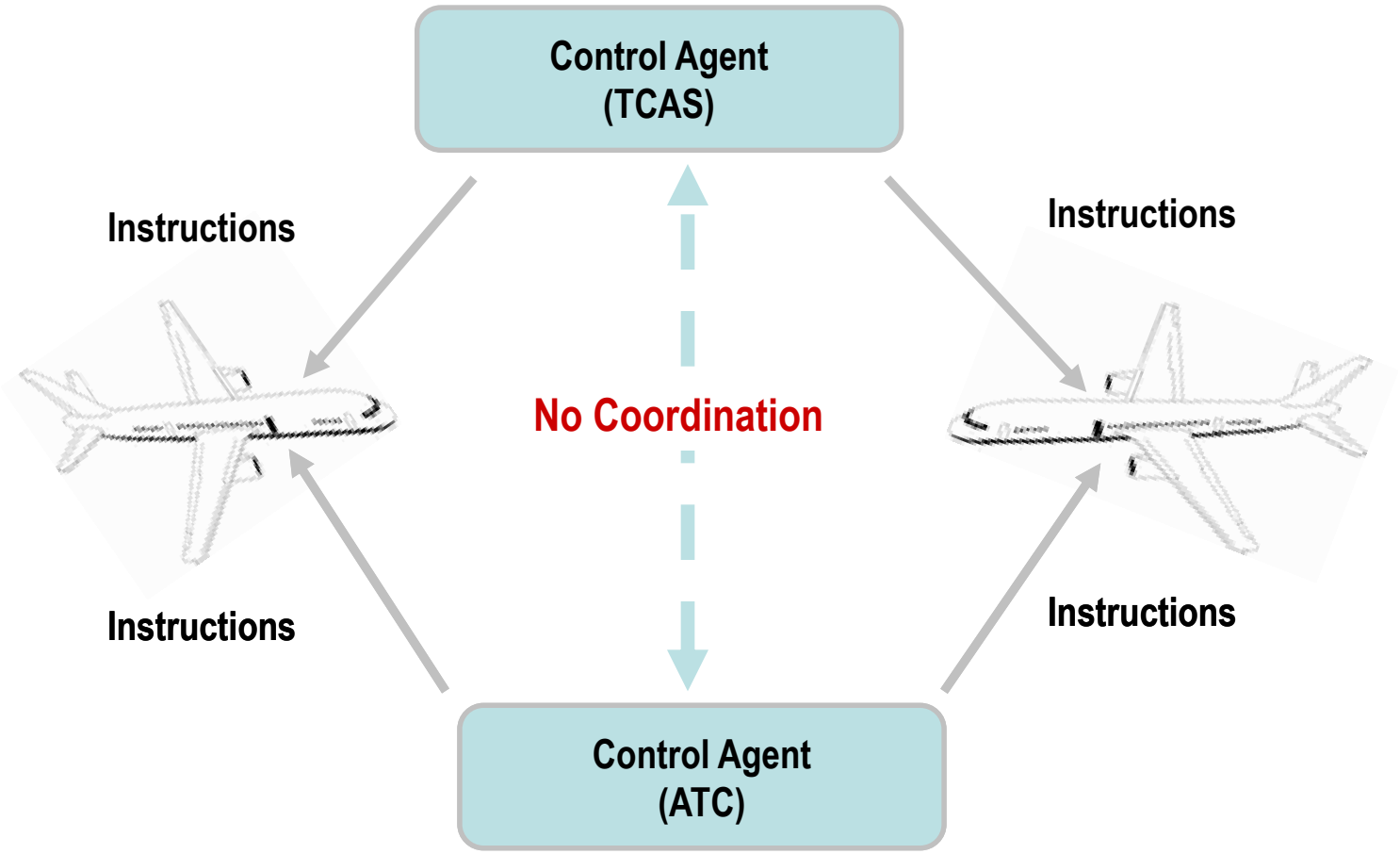
Watch Citichem Video

Jot down the causal factors as you watch

What were some of the causal factors in the video?

Uncoordinated “Control Agents”

“UNSAFE STATE”
BOTH TCAS and ATC provide uncoordinated & independent instructions



To understand and prevent accidents, must consider system as a whole

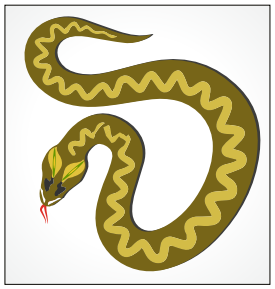


Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

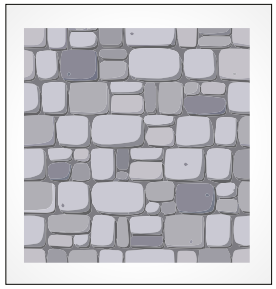


Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

And so these men of Hindustan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right
And all were in the wrong.

John Godfrey Saxe (1816-1887)

Image by MIT OpenCourseWare.

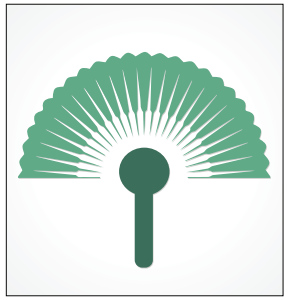


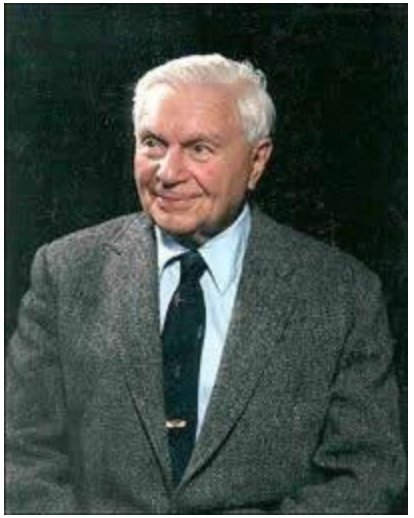
Image by MIT OpenCourseWare.

Image by MIT OpenCourseWare.

Jerome Lederer (1968)

"Systems safety covers the total spectrum of risk management. It goes *beyond the hardware* and associated procedures of systems safety engineering. It involves:

- Attitudes and motivation of designers and production people,
- Employee/management rapport,
- The relation of industrial associations among themselves and with government,
- Human factors in supervision and quality control,
- The interest and attitudes of top management,



- The effects of the legal system on accident investigations and exchange of information,
- The certification of critical workers,
- Political considerations
- Resources
- Public sentiment

And many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.”

Root Cause Seduction

- Accidents always complex, but usually blamed on human operators
- Cannot prevent them unless understand ALL the factors that contributed
- Always additional factors (sometimes never identified)
  - Equipment failure and design
  - Procedures
  - Management decisions
  - Etc.

Root Cause Seduction

- Assuming there is a root cause gives us an illusion of control.
  - Usually focus on operator error or technical failures
  - Ignore systemic and management factors
  - Leads to a sophisticated “whack a mole” game
    - Fix symptoms but not process that led to those symptoms
    - In continual fire-fighting mode
    - Having the same accident over and over

Primary Class Topics

- Learning from accidents
- Preventing Accidents
  - Hazard Analysis
  - Design for Safety

Detailed Plan for the Class

- Go over schedule, assignments, grading, etc.

16.63J / ESD.03J System Safety
Spring 2016