# System Safety Engineering

Nancy Leveson
John Thomas

# What were some of the causal factors in the Uberlingen accident?

# Uncoordinated "Control Agents"

**"SAFE STATE"**
**TCAS provides coordinated instructions to both planes**

**Control Agent (TCAS)**

**Instructions**

**Instructions**

Source: Public Domain. OpenClipArt.

**Control Agent (ATC)**

# Uncoordinated “Control Agents”

**“SAFE STATE”**
**ATC provides coordinated instructions to both planes**

**Control Agent (TCAS)**

Source: Public Domain. OpenClipArt.

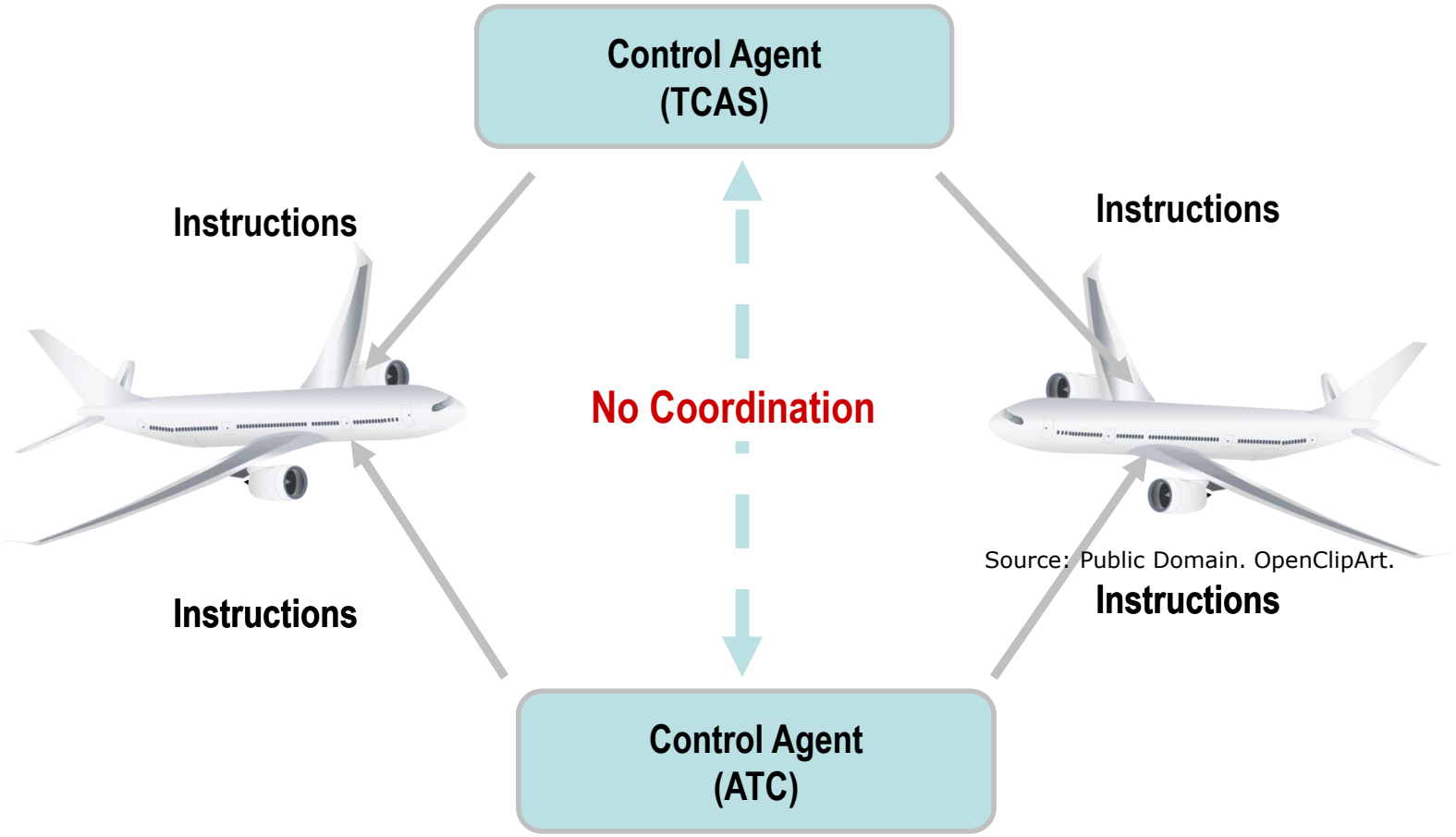
**Instructions**

**Instructions**

**Control Agent (ATC)**

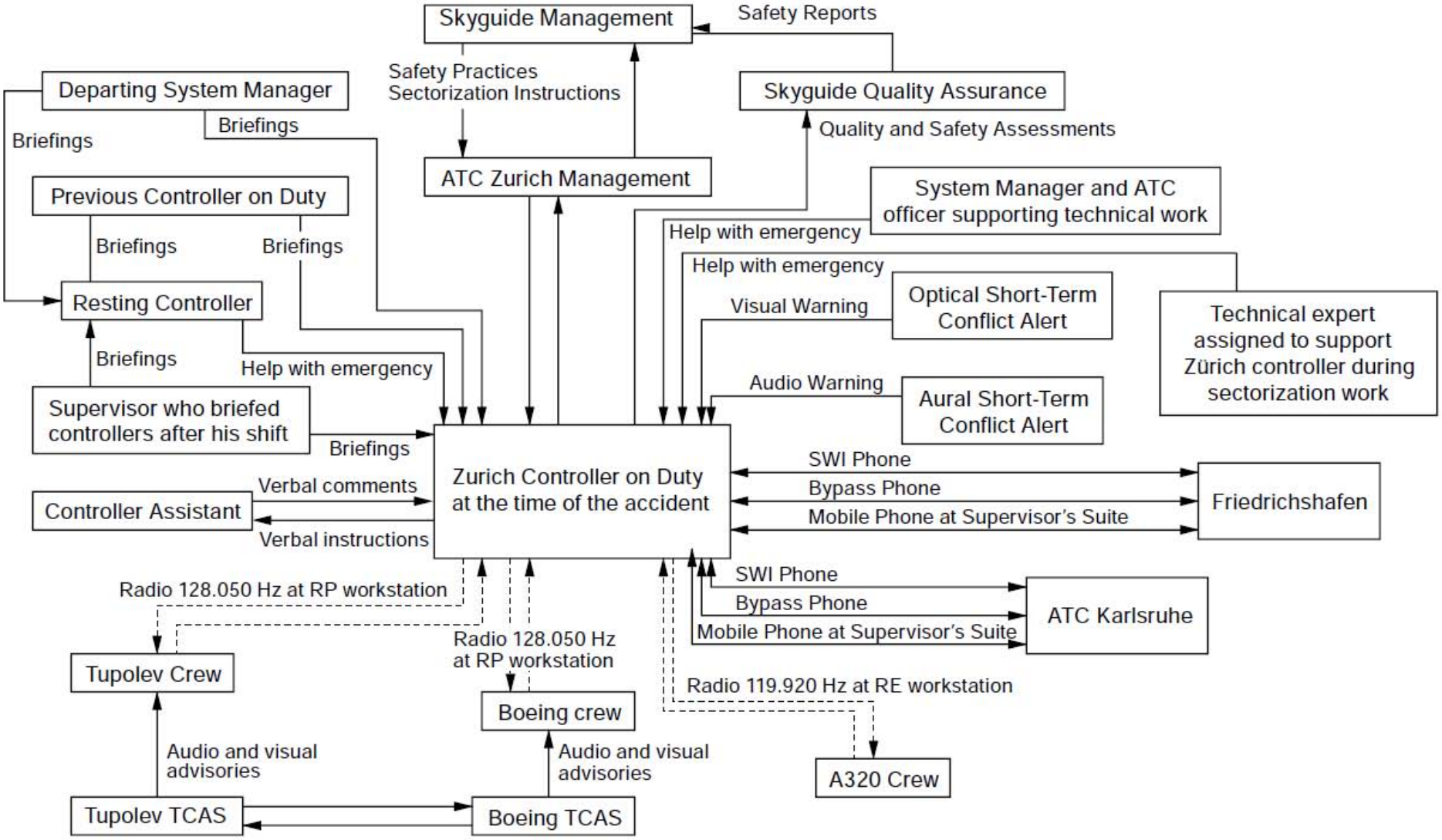
# Uncoordinated "Control Agents"

**"UNSAFE STATE"**
**BOTH TCAS and ATC provide uncoordinated & independent instructions**



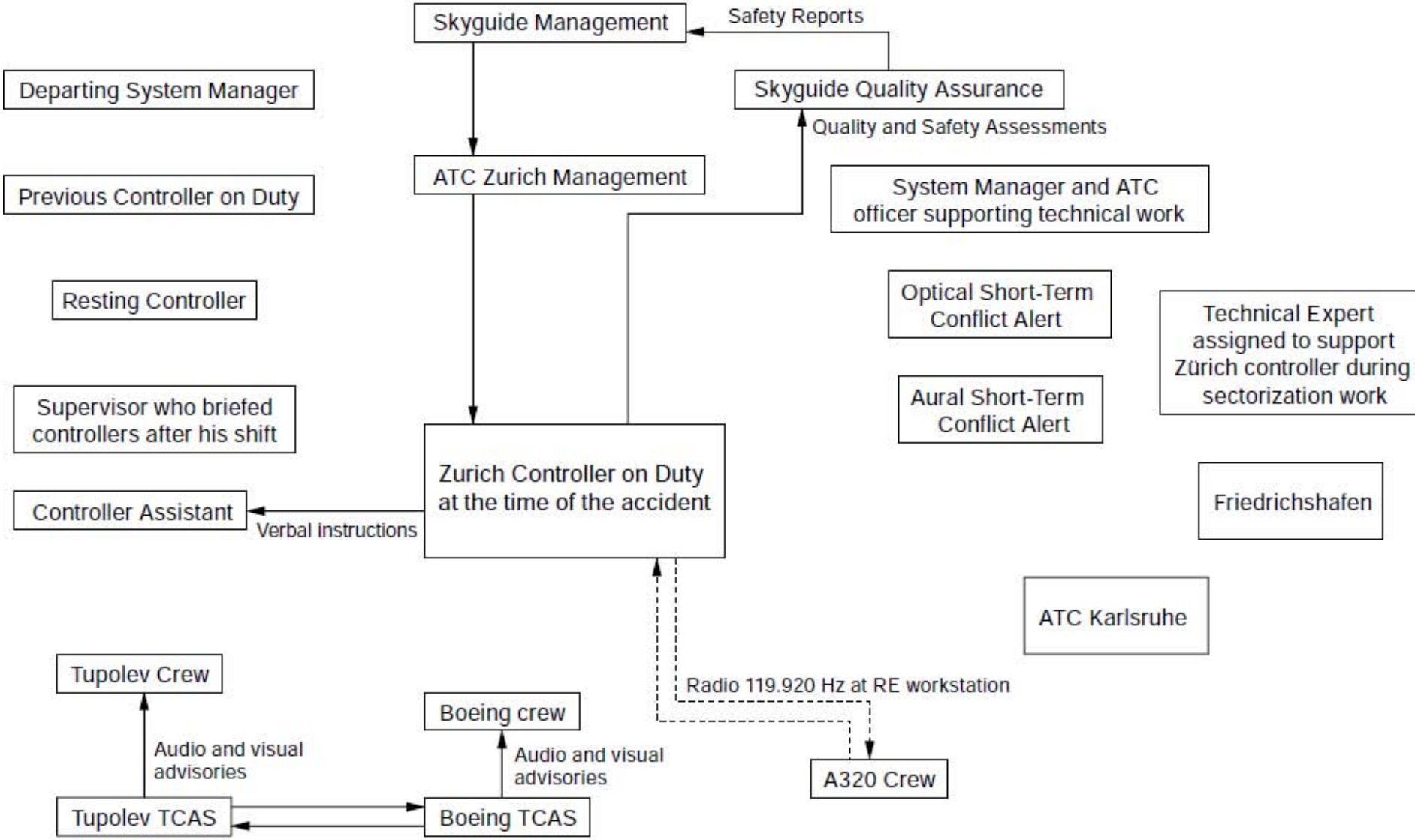

Source: Public Domain. OpenClipArt.

# Communication Links Theoretically in Place in Uberlingen Accident




From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

# Communication Links Actually in Place




From Leveson, Nancy (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, © Massachusetts Institute of Technology. Used with permission.

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

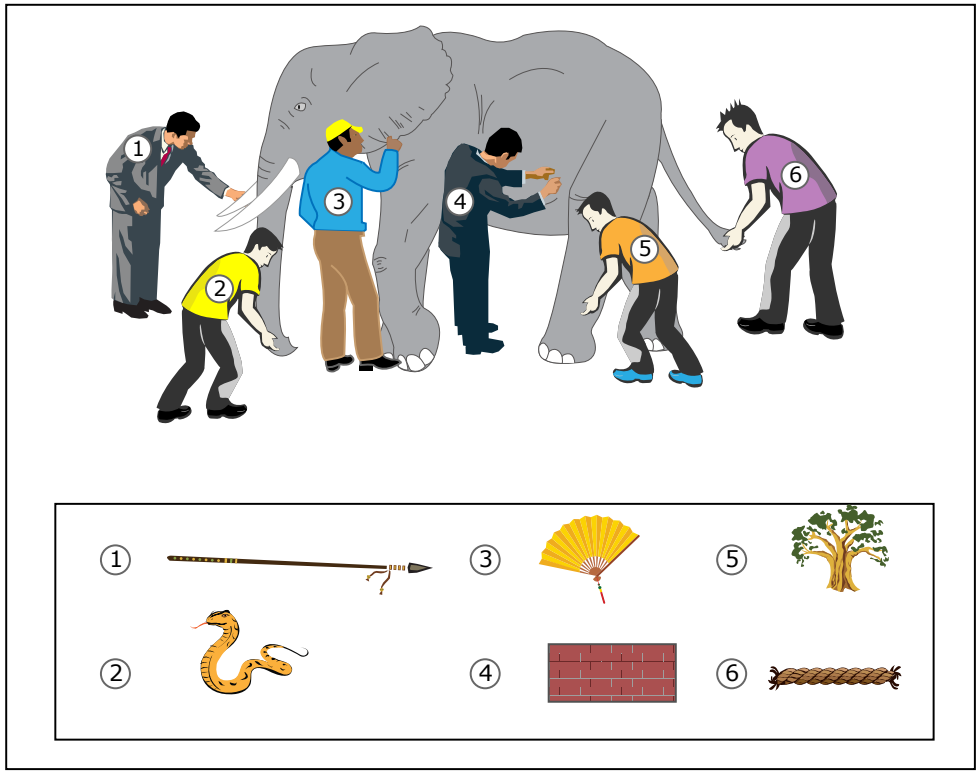



Image by MIT OpenCourseWare.

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)

# 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

# Investigating/Understanding Accidents

- What are ALL the factors involved?
- Are there tools to help us find all the factors?
- How do we minimize hindsight bias?
- How do we learn from accidents in order to prevent them in the future?

# Hazard Analysis

- “Investigating an accident before it occurs”
- Identify potential scenarios
- Worst case analysis vs. average (expected) case analysis
- Use results to prevent losses

# Design for Safety

- Eliminate or control scenarios (causal factors) identified by hazard analysis
- Fault Tolerance
  - Failures will occur
  - Need to make sure they don't result in an accident
- Design to prevent operator error
  - Human errors will occur
  - Need to make sure they don't result in an accident
  - Design so that don't induce human error

# Detailed Plan for the Class

- Go over schedule, assignments, grading, etc.

16.63J / ESD.03J System Safety
Fall 2012