A New Approach to System Safety Engineering

Nancy G. Leveson, MIT

System Safety Engineering: Back to the Future


© Copyright Nancy Leveson, Aug. 2006
Uncoordinated “Control Agents”

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

Control Agent (TCAS)

Instructions

No Coordination

Control Agent (ATC)

Instructions
Components surrounding Controller in Zurich

- Skyguide Management
  - Official Instructions on Sectorization Work & Enforcement of Safety Practices
  - Safety Reports

- ACC Zurich Management
  - Official Instructions on Sectorization Work & Enforcement of Safety Practices
  - Quality and Safety Assessments

- Skyguide CoC (Quality Assurance)
  - System Manager and ATC Officer Supporting Technical Work
  - Help with Emergency Situation
  - Visual Warning

- Optical STCA
  - Help with Emergency Situation

- Aural STCA
  - Help with Emergency Situation
  - Visual Warning

- SW-02 Phone
- Bypass Phone
- Mobile Phone at Supervisor's Suite

- UAC Karlsruhe

- Friedrichshafen

- Departing System Manager
  - Briefings

- Previous controller on duty
  - Briefings

- Resting controller
  - Briefings
  - Supervisor who Briefed Controllers at 21:00 hrs After His Shift

- Controller Assistant
  - Briefings
  - Verbal instructions
  - Radio 128.050 MHz at RP workstation
  - Radio 119.920 MHz at RE workstation

- TU154M Crew
  - Audio and Visual Advisories

- TU154M TCAS

- B757-200 Crew
  - Audio and Visual Advisories

- B757-200 TCAS

- A320 Crew
Links degraded due to poor and unsafe practices
Links lost due to sectorization work
Links lost due to unusual situations:
Tupulov Crew

- Safety Requirements and Constraints
  - Must follow TCAS mandate

- Context in which decisions were made
  - Flying over Western Europe (TCAS is mandatory)
  - TU Crew doesn’t have radio communication with Boeing Crew
  - Flight Crew has no simulator experience with TCAS
  - Flight Training is unclear on what to do in case of conflict between ATC/TCAS
  - Flying at night

- Inadequate Decisions and Control Actions
  - Reliance on optical contact
  - Ignores minority report from spare member of the crew
  - Follows controller instructions rather than TCAS

- Mental Model Flaws
  - Optical illusion of distance
  - Belief that “ATC is aware of everything that is happening”
  - Belief that pilot, not TCAS has the last said in the evasion action
  - Understanding of TCAS as “a backup system” rather than a “final resort”
Zurich ATC Operations

• Safety Requirements and Constraints
  – Maintain safe separation between planes in airspace

• Context in which decisions were made
  – Phone system prevented communication from other ATCs
  – Inadequate radar coverage
  – Insufficient personnel (only one controller)
  – Unaware of TCAS and/or impact of TCAS during a RA
  – Etc.

• Inadequate Decision and Control Actions
  – Failure to communicate with DHL plane
  – Failure to adequately monitor situation

• Mental Model Flaws
  – Unaware of conflicting TCAS procedures between Russian and European pilots
  – Etc.
Regulatory Agencies (FAA, CAA, Eurocontrol)

(No significant influence on accident according to the report)

- **Safety Requirements (Responsibilities)**
  - Clearly articulate procedures for compliance with TCAS RA’s.
  - Clearly articulate right of way rules in airspace.
  - Define the role of air traffic controllers and pilots in resolving conflicts in the presence of TCAS.

- **Flawed Control Actions**
  - AIP Germany regulations not up to date for current version of TCAS.
  - Procedural instruction for the actions to be taken by the pilots (from AIP Germany) in case of an RA not worded clearly enough.
  - LuftVO – Air Traffic Order – Pilots are granted a freedom of decision which is not compatible with the system philosophy of TCAS II, Version 7 – use of term “recommendation” is inadequate.

- **Reasons for Flawed Control Actions, Dysfunctional Interactions**
  - Overlapping control authority by several nations & organizations.
  - Asynchronous evolution between regulatory guidance documents and adopted technology.