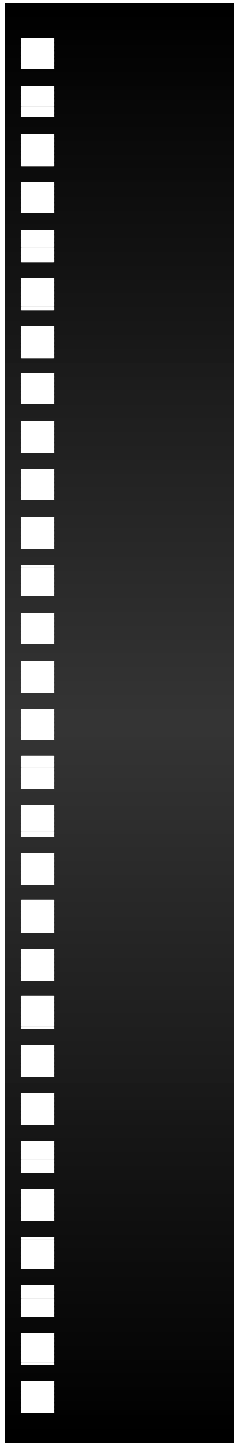
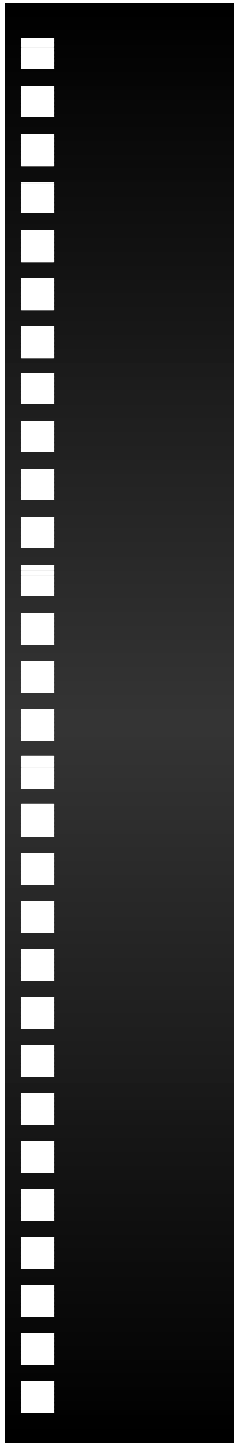


Systems Failure Case Studies

Michael Collins.

18-849, Section B

Spring 1999



Systems Failure Case Studies

- What exists
- A simple taxonomy
- Common horrors
- Conclusions

Hunting Down Resources

- Lots of apocrypha
  - comp.risks, Software Engineering News
  - political issues and spin
- Some good sources
  - *Have* to be studied
  - Air Failures Page

Taxonomy

- Task isn’t finding data, it’s sorting data.
- Taxonomy needed for sorting purposes
- Primitive taxonomies.
  - PGN, lists failures
  - ODC
  - Yours truly

Taxonomy Issues

- It’s never one thing
  - Shrug-off answers : bad design, human error
  - Sorting by keyword
- Validity
  - Urban legends
- Ceiling on consequences
  - Deaths/Cost meaningless past a certain point

Operator Complacency

- Therac-25
  - Cry Wolf
- Chernobyl
  - Experimental Situation
- STS-1 (Counterexample)
  - Alert operators

Lack/Erosion Of Safety Culture

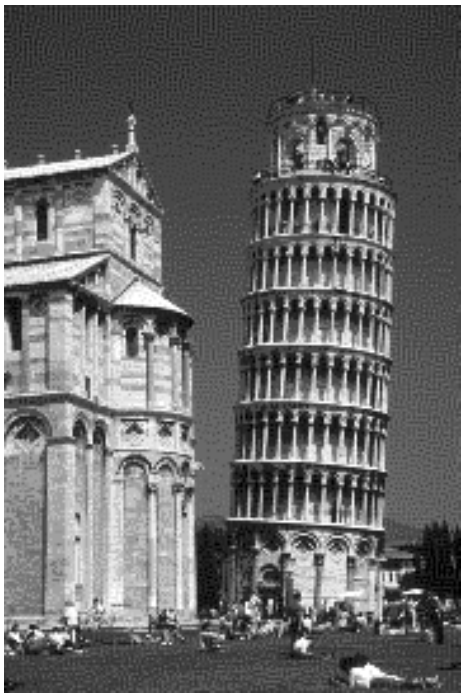
- Ottawa Elevator Death
  - Corporate musical chairs
- Challenger Disaster
  - Operator arrogance
- Bhopal
  - Corporate downsizing

Human Interfaces

- Vincennes Airbus
  - Faulty interpretation of IFF data
- Therac-25
  - Faulty error reporting
- Cali/Puerto Plata
  - Complacency/Complexity

Poor Design

- AP Outage
  - Dual cables
- 1986 Arpanet Outage
  - Single linking cable
- Chernobyl
  - RBMK design



Hysteria

- Sudden Acceleration Syndrome
  - Media exposure
- Year 2000 IV pump
  - Endorsed by speakers
- Year 2000 Fire Truck ladders
  - From the Senate

Subsidiary Issues

- Repair Failures
  - SS-7
- Sabotage
  - Lithuanian Plant
- Language Debate
  - Ariane V
  - AT & T System Runaway, 1990

Conclusions

- *System* failure
  - Very rarely any one thing
  - Failures pile up into catastrophes
- Human factors are critical
  - Morale, security, inspections
  - ICHH Syndrome