Assignment 5: Design For Safety principles

Reading:
Read Follensbee - The Fail Safe Concept, Its Origin, and Its Logic

Identify safety principles
For the system in the accident you studied, identify three Design For Safety principles from the lecture and the Follensbee paper that were used in the design. Some principles to consider:
- Redundancy
- Monitoring
- Passive/active protection
- Incremental control
- Lockout
- Lockin
- Interlock
- Safety margins
- Fault tolerance

Feel free to cite external resources aside from the accident report. For each of the three design principles you choose:
- Describe how the design principle was used in your system.
- Note whether the design feature worked as expected or whether it played a role in the accident you studied.
- Comment on the strengths/limitations of that design feature for your particular system.

Submit your findings as a ~5 minute powerpoint presentation.

16.63J / ESD.03J System Safety
Fall 2012