16.63 Assignment 11

Continue STPA Analysis

Continue your STPA analysis. Apply the rigorous UCA method to identify additional unsafe control actions that may have been omitted from the table in your previous assignment. Translate UCAs into safety constraints. Perform STPA Step 2 to find causal factors that violate safety constraints.

Resources

As before, seek and use any information you can find online for this assignment. Cite any resources used.

Reading

ESW p220-226

Deliverables

The following deliverables must be submitted for this analysis

- Word document
  - 3-4 pages single spaced
  - Accidents (losses)
  - System Hazards
  - Control structure
  - STPA Step 1 (rigorous method)
    - Choose 2 control actions from the control structure
      - At least 1 should be a control action you analyzed in the last assignment
    - Create Type 1 and Type 2 tables for both control actions
    - Define safety constraints from UCAs identified
    - For each safety constraint, note the hazard(s) it helps prevent
  - STPA Step 2
    - Choose 2 UCAs
    - For each UCA, identify factors that could cause the UCA. Consider:
      - Control algorithm
      - Process model
      - Feedback path (including any sensors)
      - Other inputs (e.g. from other controllers, multiple conflicting controllers, etc.)
    - For the corresponding 2 safety constraints, identify factors that could violate the constraint without a UCA. Consider:
      - Control path (including any actuators)
      - Controlled process
      - Other inputs (e.g. commands from other controllers, external disturbances, etc.)
- Powerpoint presentation
  - ~5-10 minutes
  - Summarize each of the above

16.63J / ESD.03J System Safety
Fall 2012