16.63 Assignment 9 / 10

Begin STPA Analysis on Roller Coaster

Disney has used your FTA and FMEA to design better roller coaster cars, but they would now like a more comprehensive analysis that can include automated software controllers, human operators, and even the role of park management. Your next task is to perform an STPA analysis on the roller coaster system as a whole including not only the car but also the track, embarking and disembarking procedures, automated controllers, and higher-level human controllers.

For this pilot study you may choose the specific system details to be analyzed (or invent your own roller coaster system), but it should be representative of a generic amusement park.

Resources

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

To get you started, two optional references have been uploaded to the Online materials

- General description of a Matterhorn Bobsled Ride
- Powerpoint slides about controlling coasters (including operational, development, and political aspects)

Reading

ESW p87-93, 211-220

(assignment deliverables on next page)

Deliverables

The following deliverables must be submitted for this analysis

- Word document
    - 3-4 pages <u>single spaced</u>
    - Description of the system you are analyzing
        - Physical hardware implementation (car, brakes, track zones, etc.)
        - Automation (What parts are controlled automatically? How?)
        - Operations (What do operators do? How do they interact with physical hardware, automated systems, passengers, etc.?)
        - Management (roles, responsibilities, interaction with operators, etc.)
    - Define the Accidents (losses)
    - Define the System Hazards
    - Create the control structure
        - Include about 10 boxes
            - At least 5 controllers
            - At least 1 sensor and 1 actuator
        - Include each of the following:
            - Physical hardware components
            - Automation
            - Human operators
            - Management
        - Label all feedback and control paths
    - Begin STPA Step 1
        - Choose 2 control actions from the control structure
        - Create a basic table showing how each control action could be unsafe
            - Not providing causes hazard
            - Providing causes hazard
            - Wrong timing or order causes hazard
            - Stopped too soon or applied too long
- Powerpoint presentation
    - ~5-10 minutes
    - Summarize each of the above

16.630J / ESD.03J System Safety
Fall 2012