

Assignment 4: Finish CAST analysis

Reading:

ESW p357-367 (more info about analyzing individual components using CAST)

Finish CAST:

Submit a 10-15 minute presentation of your CAST analysis. This includes:

Revise your hazard (optional)

- Make sure it describes the overall state of the system, and not specific behavior of an individual component like software, engines, pilots, etc.

Refine and update your control structure

- Include control action and feedback arrows. Label each arrow with the particular actions/information they represent. Add controllers if necessary to capture any additional causes you found.

Analyze the physical process/system. Identify:

- Safety responsibilities of physical system (what must it do)
- Physical controls (what design features were meant to fulfill the safety responsibilities)
- Failures and inadequate controls (what went wrong)
- Contextual factors (why did those things go wrong)

Analyze at least 2 controllers in the control structure (remember that a controller can be automated software, human operator, human manager, or an organization like FAA or congress). For at least 2 controllers, identify:

- Safety-related responsibilities (what goals they should achieve)
- Unsafe Decisions and Control Actions (what they did that was unsafe)
- Process model flaws (what did they believe about the system that explains their actions)
- Context (what other factors - pressures, incentives, history, etc. - explain their actions)

Please feel free to use any external resources you can find in addition to the official accident report to perform your CAST analysis. Be sure to cite all the materials you used.

MIT OpenCourseWare
<http://ocw.mit.edu>

16.63J / ESD.03J System Safety
Fall 2012

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.