Cyber Mission Assurance using STPA

William E. Young, Jr (Col, USAF), PhD Student,

Start: Sept 2011
Research Group: Complex Systems Research Lab (MIT)
Advisor: Prof Nancy Leveson

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Workshop on
Who Controls Cyberspace?
MIT, November 6 and 7, 2012

Problem

From Cyber Security to Mission Assurance

Improving Campaign Mission Assurance
How can we complete campaign mission across a wide range of degradations?

Current gaps:
1) Emergent system properties ignored
2) Assurance restricted to tactical level
3) Ignores Operational (campaign) Design

Solution:
1) Use systems thinking
2) Leverage safety-guided design

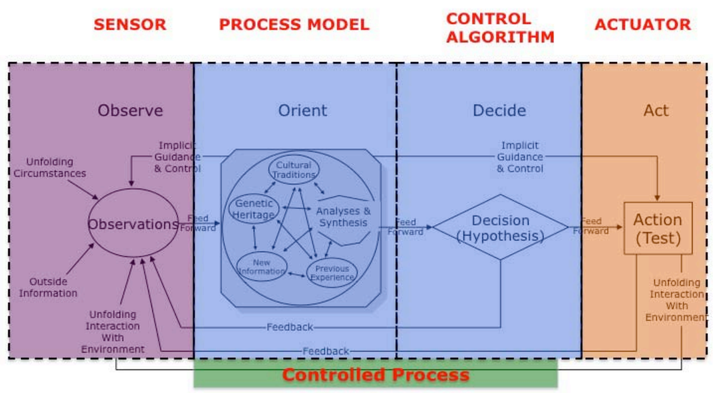
Method

*System-Theoretic Process Analysis—**(STPA)***

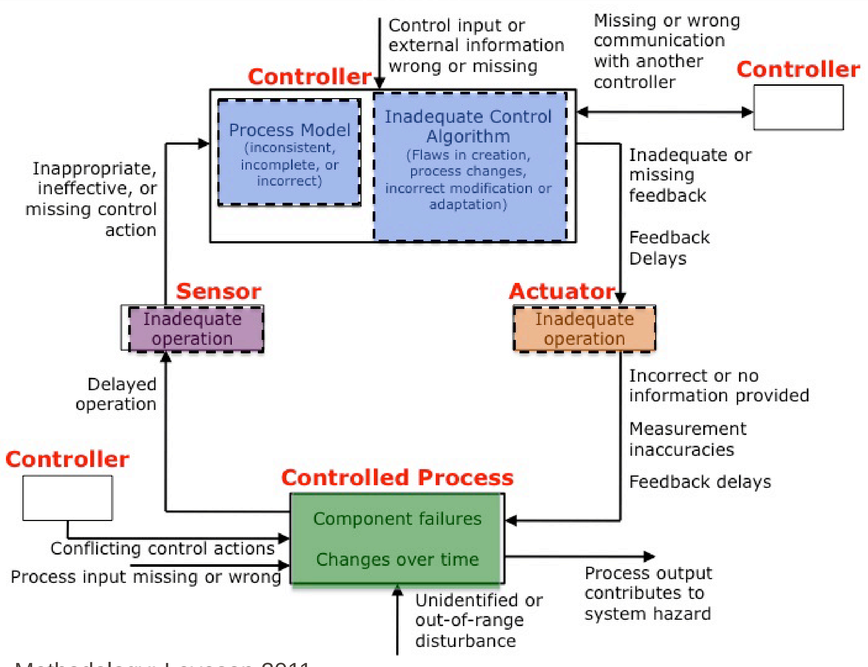
- Identify system goals, accidents & hazards
- Create control structure
- Create process model
- Identify unsafe control actions:
  - providing causes hazard
  - not providing causes hazard
- Identify critical threat scenarios
- Redesign system & iterate

The Research

STPA Operationalizes USAF Cyber Construct

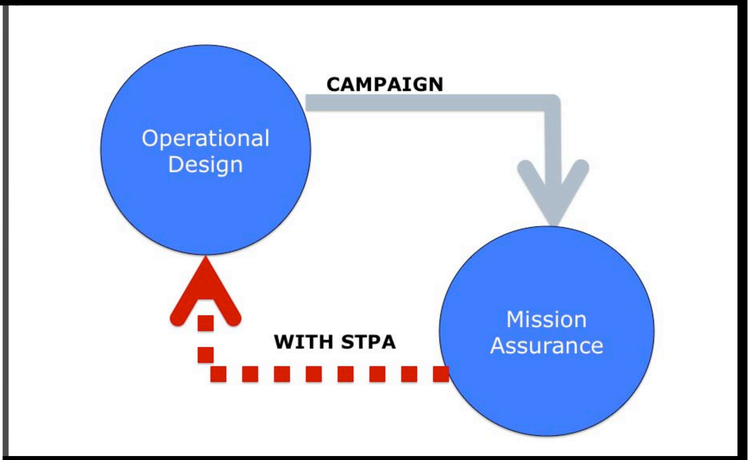


Use STPA to Find & Correct Campaign Design Flaws



Methodology: Leveson 2011

Preliminary Results



Remaining Research

- Finish STPA of representative campaign design (& modifying STPA for military context)
- Conduct pilot experiments
- Prepare materials for training workshops
- Conduct experiments on design groups (STPA, control) in cyber-focused exercises measuring design "faults" (potential degrades mission cannot survive)

Thank You!

This research is partially funded by MIT Lincoln Laboratory's Cyber Systems Assessment Group. Any opinions, findings, & conclusions or recommendations expressed are those of the author and do not necessarily reflect the views of MIT Lincoln Labs or the USAF. Also, I extend my deepest appreciation to the many members of the Complex Systems Research Lab, Lincoln Labs Divisions 1, 6 & 10 & Group 69, Prof Nancy Leveson, Prof Stuart Madnick and Allen Moulton.