A System Safety Approach to Assuring Air Operations Against Cyber Disruptions

26 March, 2013

William E. Young, Jr, Col, USAF
PhD Candidate, Engineering Systems Division
Complex Systems Research Lab
Advisor: Prof N. Leveson

WYOUNG@MIT.EDU

Spoiler

Securing networks is a tactical fight; our "cyber"

vulnerabilities (induced by dependencies on information

and control provided by networks) are a strategic choice

based on how mission is designed

Overview

- Differences from basic STPA
- My research problem
- Thinking behind STAMP & relation to cyber
- Planned approach

My goal is to provide a useful methodology to:

(1) Assess a candidate air campaign mission concept's information/ control dependencies and vulnerabilities

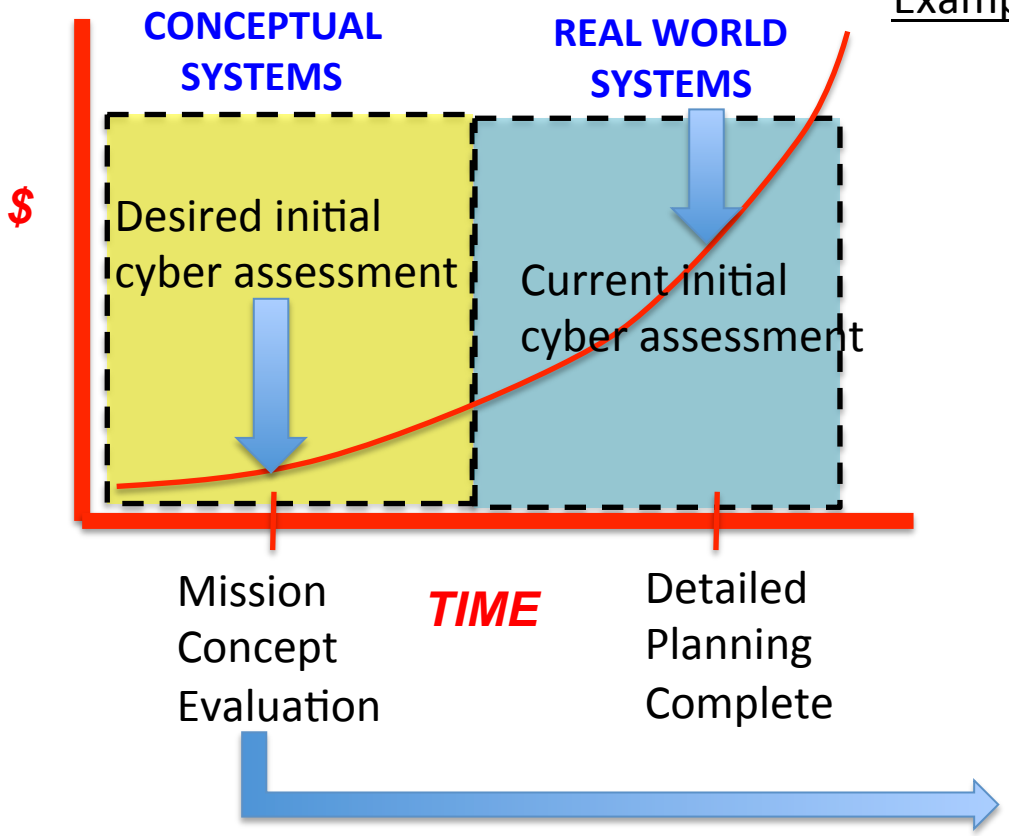
(2) Facilitate redesign of mission concept in light of information/ control vulnerabilities to better meet Air Commander's vision

How is My Research Different?

- Apply STPA to a system derived from the commander's mission concept
- Focus on making the logical information and control dependencies implied by mission concept explicit
- High-level control model developed using Soft Systems Methodology
- *Unsafe Control Actions* treated as mission cyber vulnerabilities
- *Classic Control Flaws* considered destructive cyber effects

Apply STPA on a *mission concept system* focusing on cyber as control, not cyber as technology

Problem: Cyber Vulnerabilities Addressed Late in Campaign Design



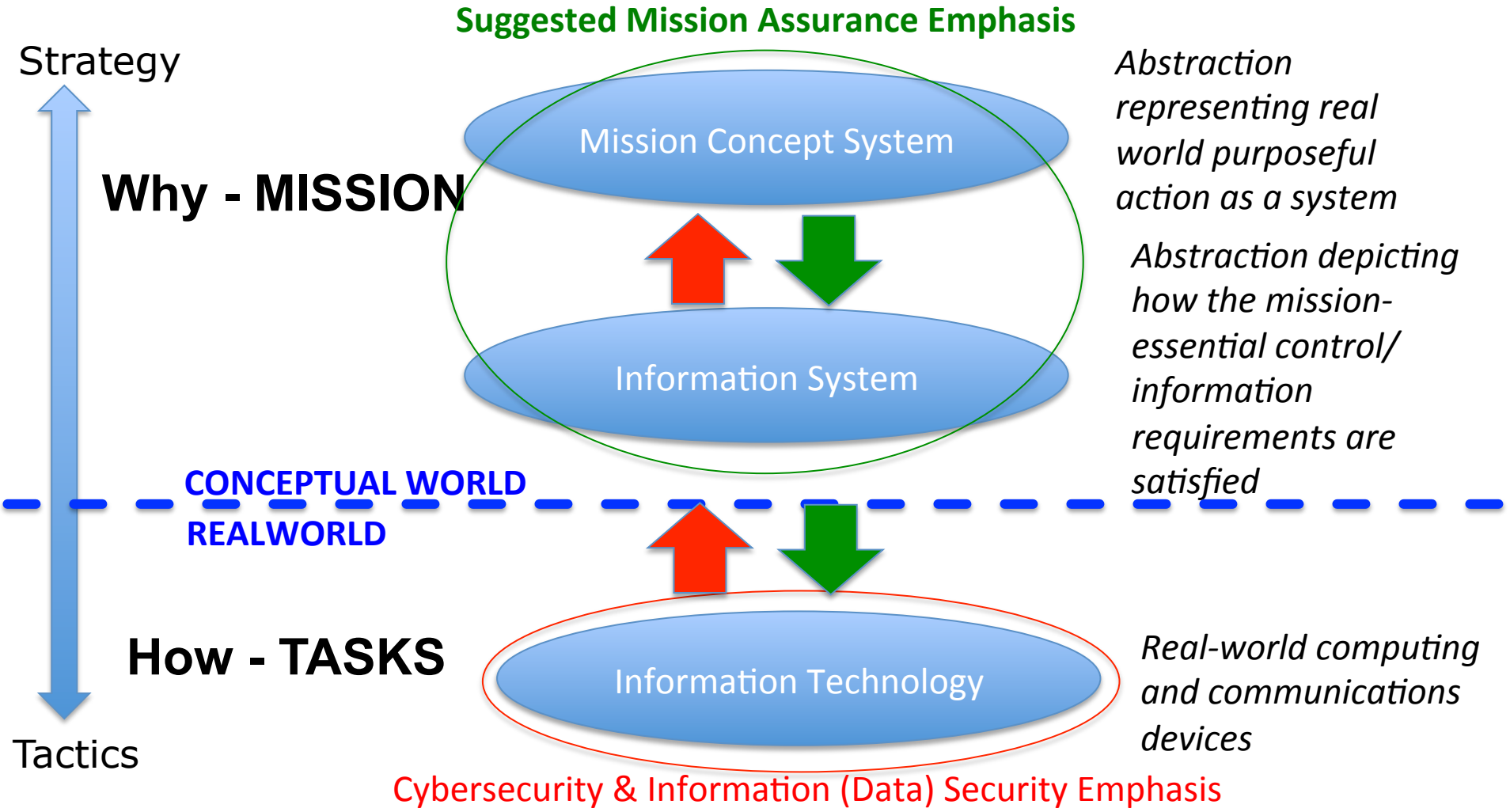
Example Concept Decision and Evaluation Matrix

Criteria		
Surprise	3	1
Flexibility	5	2
External Support	2	2
Risk (Cyber)	?	?

Successfully assuring air operations begins with careful evaluation and selection of mission concept

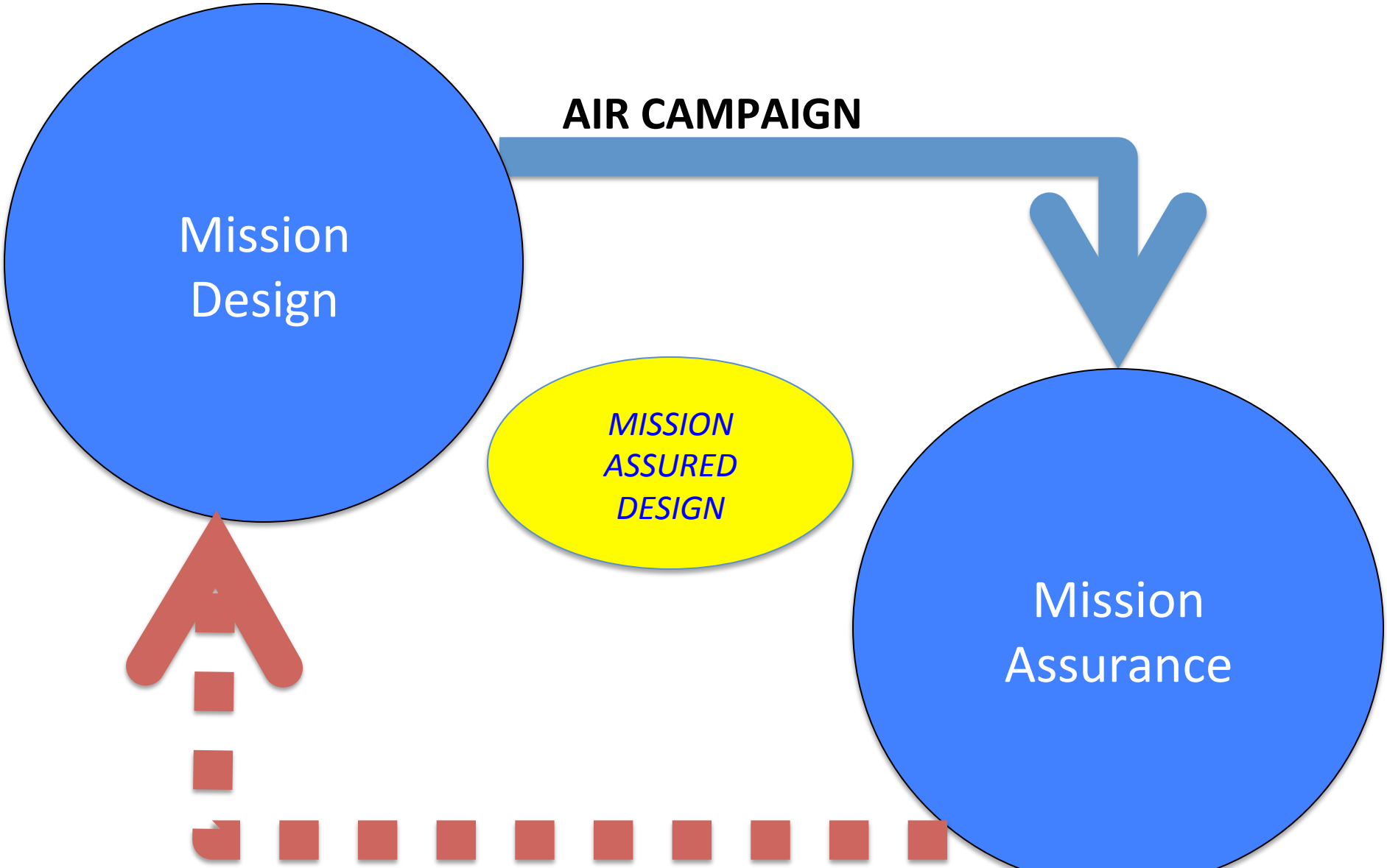
Reference: Joint Staff, 2011

Systems, Information Systems, Information Technology



Tasks --- data and signals; Mission--information & control

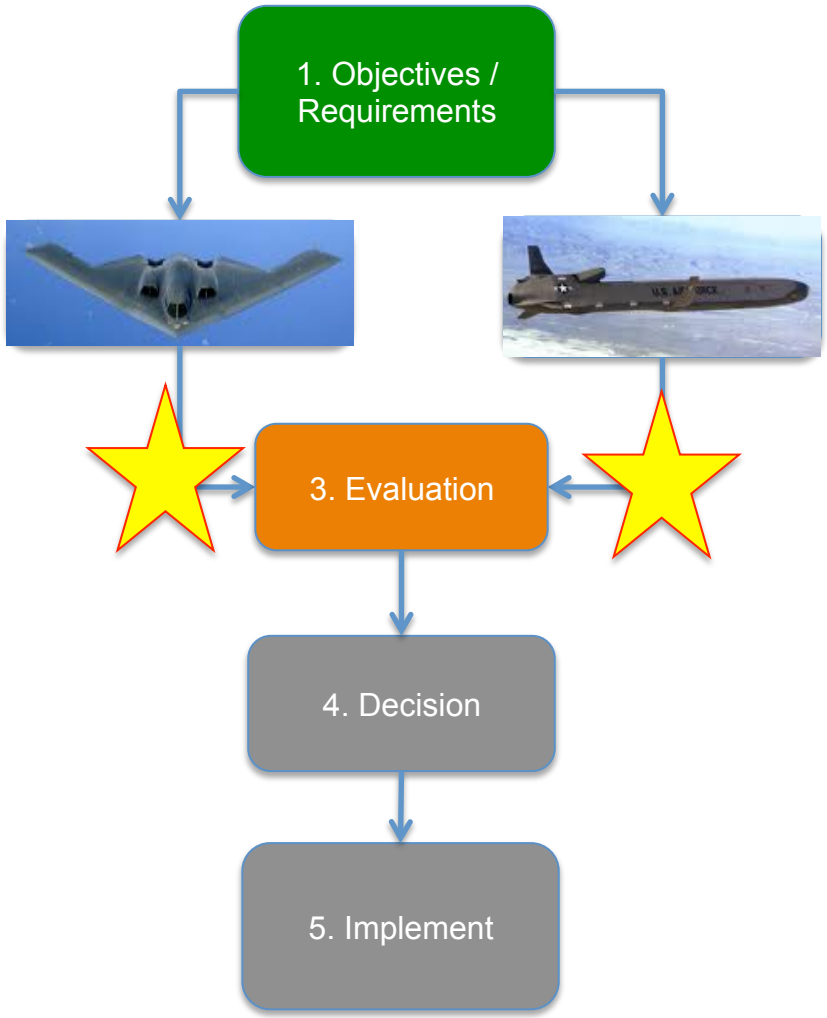
Reference: Checkland, 1995; Checkland and Howell 1998



NEW FORM OF *CYBER RED TEAMING* USING COMPLEX SYSTEMS SAFETY APPROACH

Adapted From: Leveson, 2011

New STPA-based Intervention



Intervention Requirements:

1. Represent mission concept as a control system diagram

2. Analyze control system diagram for flaws (vulnerabilities)

= New Intervention

SSM: Concept to Control-based System Model

Conceptual System Description

Conceptual System Diagram

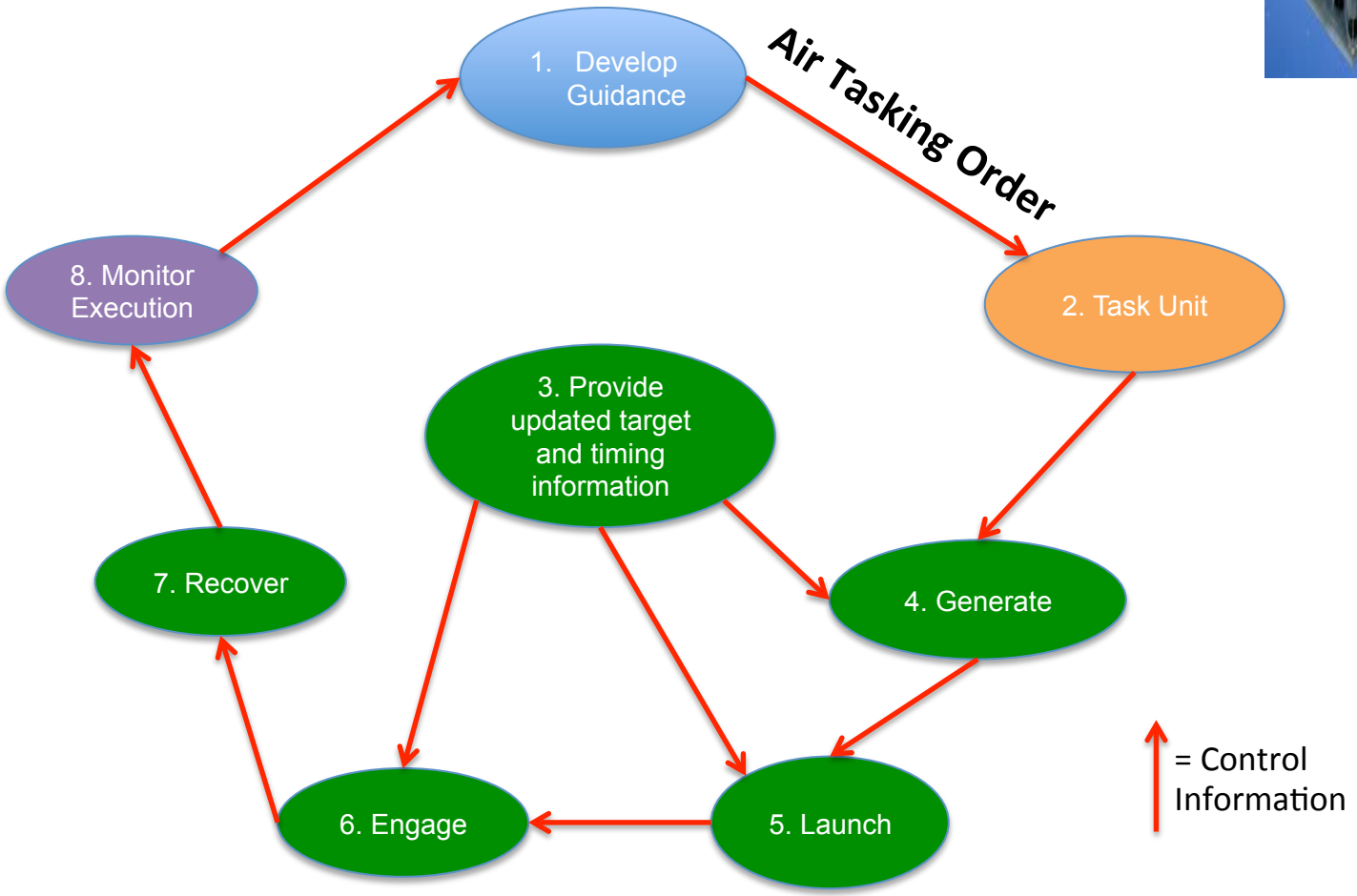
System Control Structure Analysis

Hazardous Scenario Identification

Abbreviated sample description:

"Air Commander owned and directed system to prevent adversary aircraft from launching by finding and destroying emerging command and control (C2) targets."

Simplified sample conceptual diagram



STPA: Identify Vulnerabilities in Systems Model

Conceptual System Description

Conceptual System Diagram

System Control Structure Analysis

Hazardous Scenario Identification

Control Information	Wrong	Missing	Early / Late	Extended/ Shortened
Control Information 1	Vulnerability		Vulnerability	
Control Information 2		Vulnerability		
Control Information 3	Vulnerability			
Control Information 10				

Criteria		
Surprise	3	1
Flexibility	5	2
External Support	2	2
Risk ***(Vulnerabilities)***	***4***	***5***

Control vulnerabilities from STPA tables provide air planners a systemic, structured, defensible risk score

QUESTIONS or COMMENTS

- Thank you for your attention
- My contact information
  - William.Young@MIT.Edu (student email)
  - William.Young@LL.MIT.Edu (Lincoln Labs email)

MUCH MORE DETAIL Tomorrow Evening at Poster Session!

A System Safety Approach to Assuring Air Operations Against Cyber Disruptions

26 March, 2013

William E. Young, Jr, Col, USAF
PhD Candidate, Engineering Systems Division
Complex Systems Research Lab
Advisor: Prof N. Leveson