STPA-Sec Aerial Refueling Case Study

Capt. Martin "Trae" Span
Lt. Col Logan O. Mailloux
Col William Young

27 March 2018

Disclaimer: The views expressed are those of the author(s) and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

Overview

- Motivation
- Case Study Overview
- Case Study Results
- Recommendations
- Significance
- Summary

Motivation

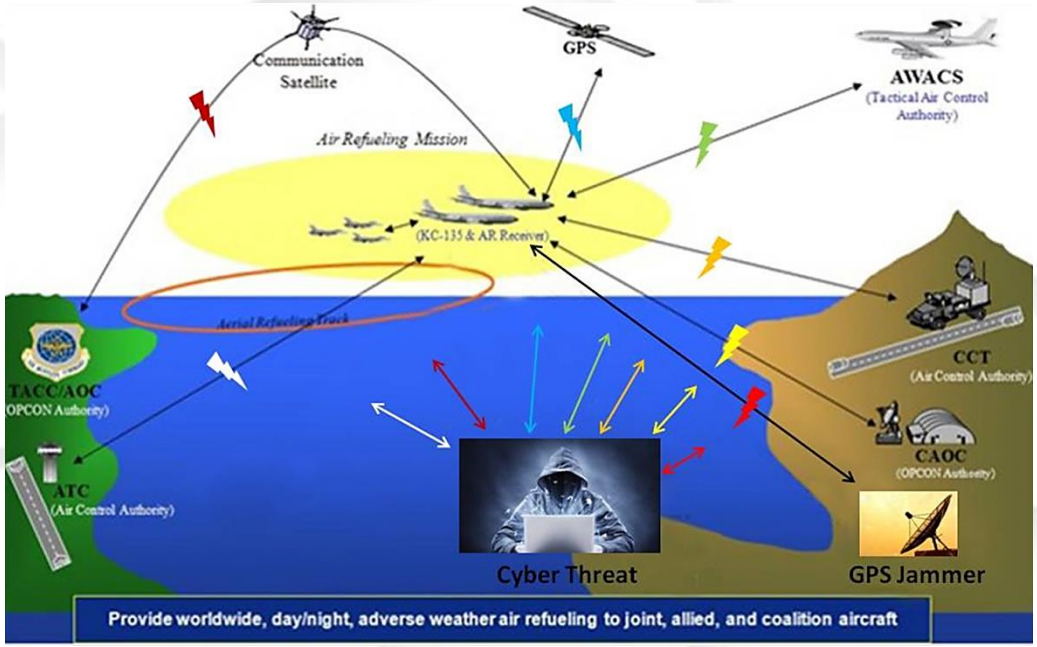
- Cybersecurity is critical for successful mission operations; published cyber-physical system vulnerabilities
- Legacy weapon systems not designed for cyber threats and cyber resiliency
- Increasingly intelligent adversaries
- DoD and Congressional Mandates: NDAA Sec 1647-- Requirement and funding to access major weapon systems
  - USAF Cyber Resiliency Office for Weapons Systems (CROWS)
  - USAF Cyber Campaign Plan
    - "Bake in" for new acquisitions,
    - Mitigate critical vulnerabilities in fielded systems
    - LOA 3: Recruit, Hire, and **TRAIN** workforce

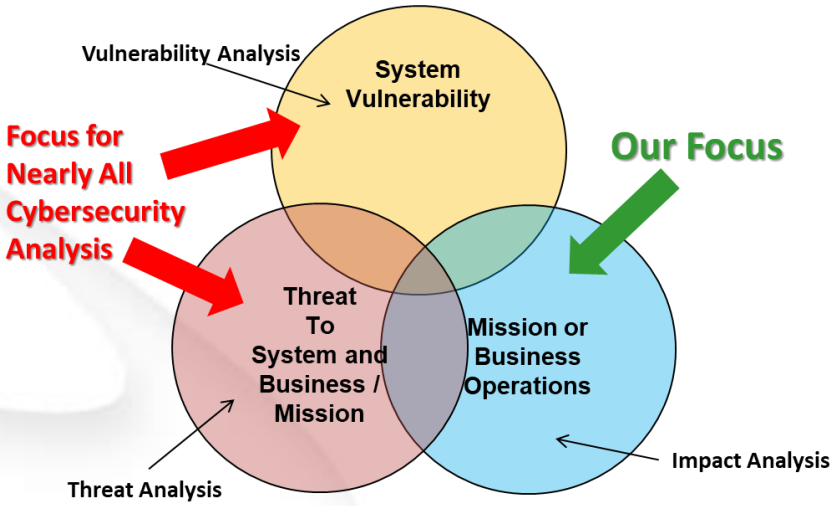
Research Objectives

- How can STPA-Sec be tailored to enable the development of security requirements and design criteria?
- How executable is STPA-Sec for USAF warfighting Systems?
- What recommendations can be made to increase the utility and ease the use of STPA-Sec?

STPA-Sec Case Study

- Demonstrate utility of STPA-Sec to USAF Aerial Refueling concept
- Use KC-X early (2010) documentation: Information Security Plan and System Requirements Document
  - Pre Design Documentation

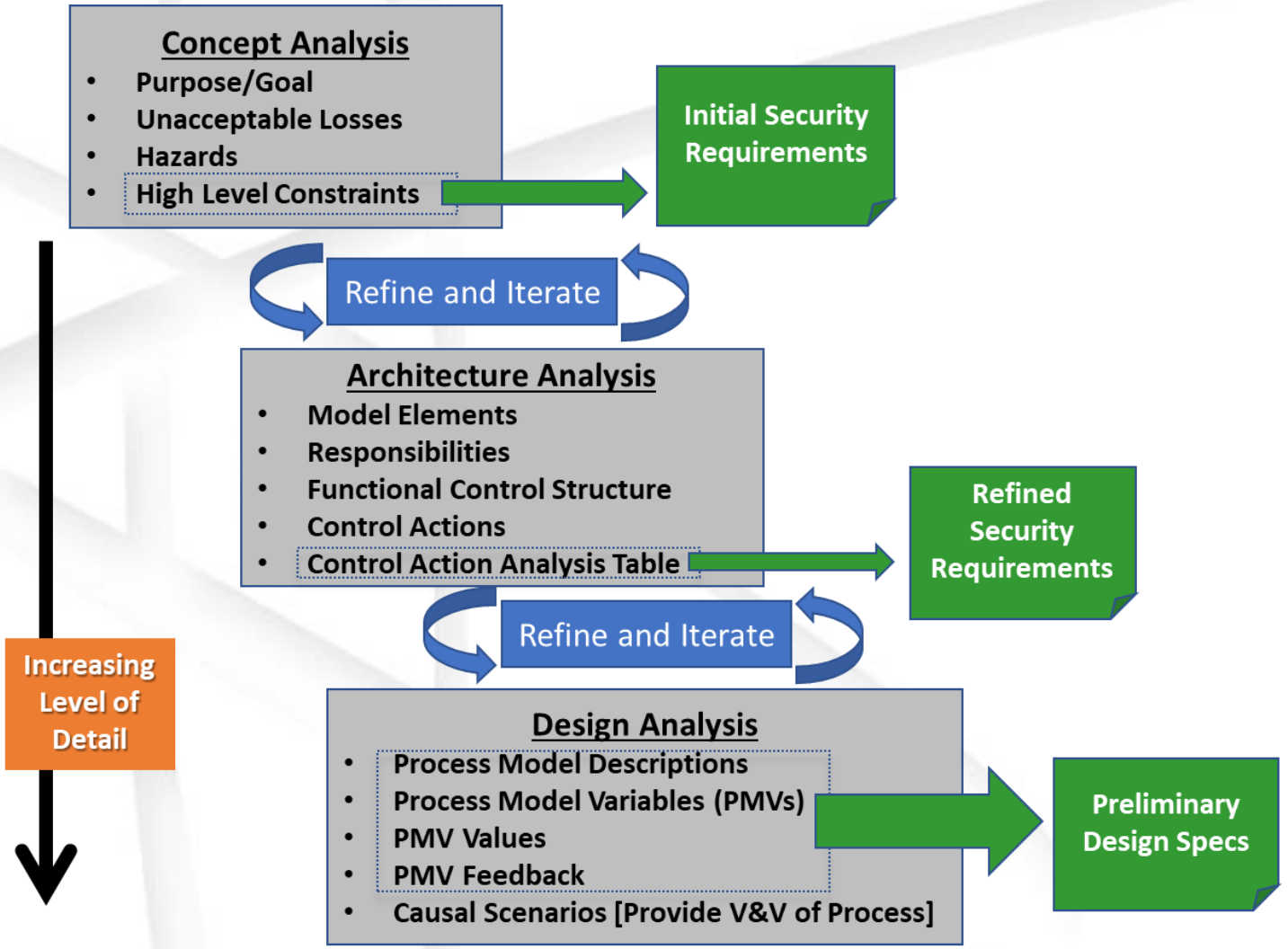




Right Image from Col Young CNW 2017

STPA-Sec Tailored Approach

The AFIT of Today is the Air Force of Tomorrow.



STPA-Sec Tailored Approach

The AFIT of Today is the Air Force of Tomorrow.

CONCEPT ANALYSIS

Step	Description
1. Define the SoI's purpose and goal	Capture the mission statement and key activities of the system: 1) A system to: (What) 2) By Means of: (How) 3) In Order to: (Why)
2. Identify unacceptable losses	Define high level, intolerable system outcomes to key stakeholders (e.g., loss of life, injury, damage to equipment, reputation, mission, etc.).
3. Identify hazards	Identify system states that when coupled with worst case conditions lead to an unacceptable loss.
4. Develop system security constraints	Develop mission-informed security constraints that prevent the system from entering hazardous states. These constraints are synonymous with early safety, security, and resiliency functional requirements.

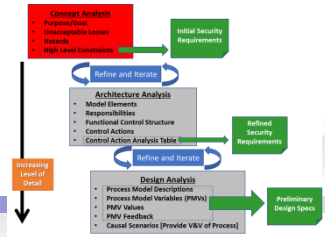
ARCHITECTURE ANALYSIS

Step	Description
1. Identify Model Elements	Identify actor(s), controller(s), and controlled process(es) for the SOI at the desired level of abstraction.
2. Identify Each Model Elements' Responsibilities	Capture the description and actions planned to be taken for the model elements identified.
3. Draw the FCS	Provide a visual functional-level depiction of the SoI. Depicts the model elements and control relationships between them.
4. Identify Control Actions (CA)	Captures (in verb form) the actions necessary for each element to execute their responsibilities.
5. Complete the Control Action Analysis Table	This table systematically enumerates which hazards are caused by each CA identified in step 4.

DESIGN ANALYSIS

Step	Description
1. Develop Process Model Descriptions	Describes the decision logic ("in plain English") for executing a given CA.
2. Identify Process Model Variables (PMV)	Process Model Variables are measurable indicators of the conditions that trigger a CA.
3. Identify PMV Values	PMV values are all the possible values a PMV can be assigned both acceptable and hazardous.
4. Identify PMV Feedback	Identifies which sensors provide PMV values to the actors and controller for decision making.
5. Carry out Causal Scenarios	Brainstorm how a specific implementation of the system may be compromised. Identifies critical CAs and validates the thoroughness of the model, CAs, and constraints.

Phase 1: Conceptual Analysis



The AFIT of Today is the Air Force of Tomorrow.

Purpose	A System to	Provide worldwide aerial refueling
Method	By Means of	Flying, Refueling, and Mission Planning
Goal	In order to	Enable the Air Force Mission to meet Joint Capability Areas via refueling and airlift: Force Enable, Force Extend, Force Multiply

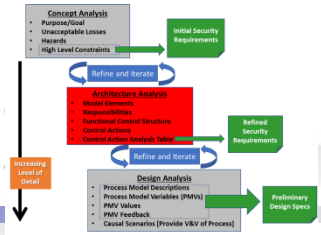
Hazard to Loss Cross Walk Table		**L1 Death or Human injury**	**L2 Damage to or loss of aircraft**	**L3 Unable to Complete Mission**
H1	Flying to Close to other aircraft/out of position	X	X	X
H2	Violation of Altitude/clearance from terrain	X	X	X
H3	Unable to evade enemy threats	X	X	X
H4	Msn critical systems not functional when required			X

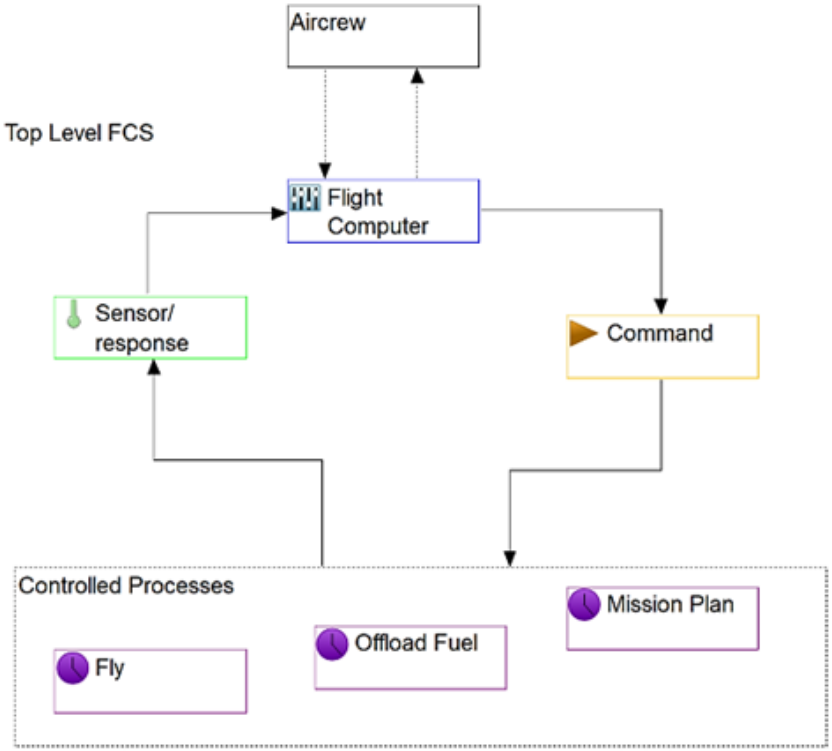
	Initial Security Constraints	**Hazard Mapped to**
1	A/C must maintain minimum safe separation distance	H1
2	Must have minimum mission critical safety systems functional to attempt AR	H1
3	A/C must maintain minimum safe altitude limits	H2
4	Must have minimum mission critical safety systems functional for terrain flight	H2
5	Must maintain integrity of mission critical warning and deterrence systems	H3
6	Msn critical systems must be available when required to perform primary msn	H4

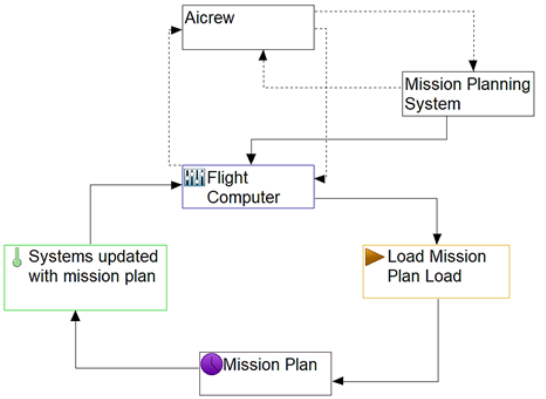
Initial Security Requirements

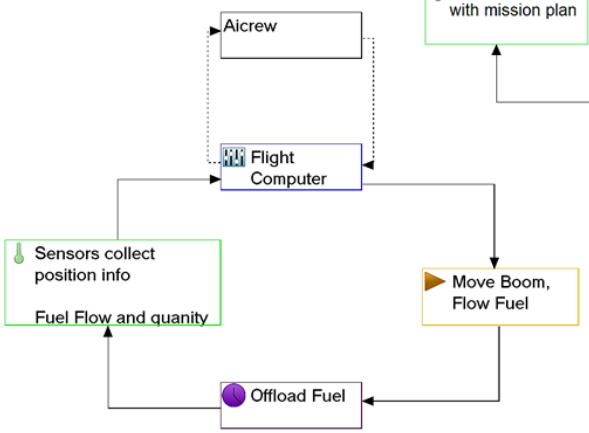
Phase 2: Architectural Analysis Functional Control Structure

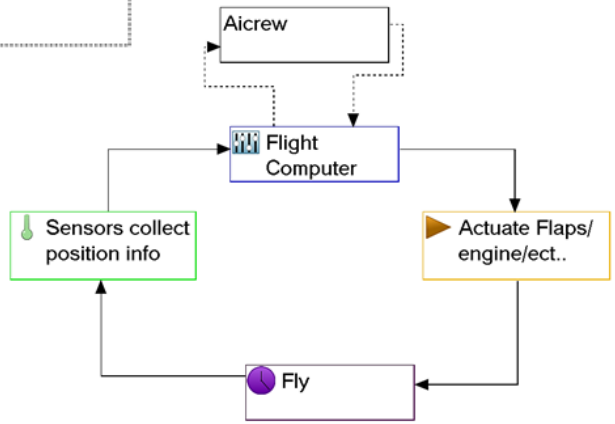
The AFIT of Today is the Air Force of Tomorrow.



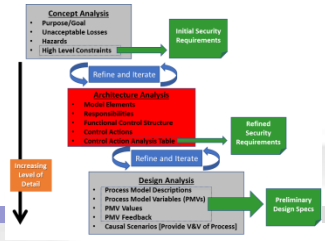








Architectural Analysis Control Actions

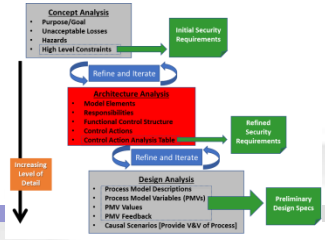


The AFIT of Today is the Air Force of Tomorrow.

KC-X CONTROL ACTIONS			
Control Action	Activity	Performer	Description
1. Position Mx	Fly	Aircrew/ Computer	Adjust position- heading change, takeoff, land, climb, descend. Computer included for autopilot functions
2. Velocity Mx	Fly	Aircrew/ Computer	Change Velocity- accelerate, decelerate, climb, descend. Computer included for autopilot functions
3. Communicate	Fly	Aircrew/ Computer	Radio and digital(i.e. ACARS, IFF) to other A/C , ATC and ground assets. Access and communicate in net centric environment.
4. Precontact	Offload Fuel	Aircrew/ Computer	Instructing both crews on proper position to begin AR. Solution independent to allow for human direction or computer aided position information
5. Contact	Offload Fuel	Aircrew/ Computer	Receiver connected to begin refueling. Solution Independent of human vs. computer to allow automation as desired
6. Breakaway	Offload Fuel	Aircrew/ Computer	Command to disengage either when complete or in case of emergency. Solution Independent of human vs. computer to allow automation as desired
7. Prepare OPS	Mission Plan	Aircrew/ external mission planning system	Reviews mission tasking, intel, and weather. Interacts with external mission planning system to create mission plan file
8. Distribute OPS	Mission Plan	Aircrew/ Computer	Aircrew inserts cartridge into jet, also provides crew briefings and coordination for mission plan. Computer distributes mission plan files to A/C systems

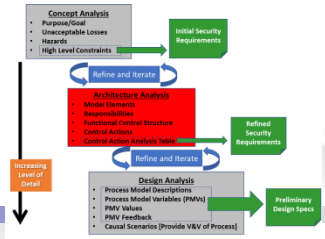
Architectural Analysis
Control Action Analysis Table

The AFIT of Today is the Air Force of Tomorrow.



KC-X CONTROL ACTION ANALYSIS TABLE.					
CA#	Control Action	Not providing causes Hazard	Providing Causes Hazard	Too Early/too late, wrong order	Stopping too soon/applying too long
1	Position Mx (Aircrew)	Not Providing Position MX is Hazardous if in a critical phase of flight [H1, H2, H3]		Position MX is Hazardous if done too early or too late in a critical phase of flight [H1, H2, H3]	Position MX is Hazardous if stopped to soon or applied to long in a critical phase of flight [H1, H2, H3]
2	Velocity Mx	Not Providing Velocity MX is Hazardous if in a critical phase of flight [H1, H2, H3]		Velocity MX is Hazardous if done too early or too late in a critical phase of flight [H1, H2, H3]	Velocity MX is Hazardous if stopped to soon or applied to long in a critical phase of flight [H1, H2, H3]
3	Communicate	Not Providing Communication is Hazardous if in a critical phase of flight(takeoff, landing, joining refueler) [H1, H3]		Communication too late is Hazardous if in a critical phase of flight(takeoff, landing, joining refueler) [H1, H3]	Communication stopped too soon (clipped transmission) is Hazardous if in a critical phase of flight [H1, H3]
4	Precontact	Not Providing Precontact is Hazardous as a A/C could be out of position and damage equipment [H1,H4]		The wrong sequence for Precontact is Hazardous if in a critical phase of refueling setup [H1,H4]	
5	Contact		Providing Contact is hazardous if attempted during an unsafe position [H1]	Providing Contact out of sequence is hazardous if attempted during an unsafe position [H1]	
6	Breakaway	Not providing Breakaway is hazardous if unsafe position occurs [H1]		Not providing Breakaway on time is hazardous if unsafe position occurs [H1]	
7	Prepare OPS	Not providing Prepare OPS is hazardous in almost all scenarios (no planned route, no deconflicts, no mission plan loaded on systems…) [H1,H2,H3,H4]			
8	Distribute OPS	Not providing Distribute OPS is hazardous in almost all scenarios (no filed flight plan, no crew briefing, no mission plan loaded on systems…) [H1,H2,H3,H4]	Providing Distribute OPS is hazardous when malware or intentionally incorrect information is distributed to systems [H1,H2,H3,H4]		

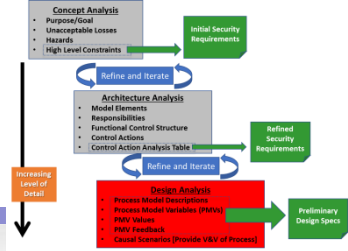
Architectural Analysis Output
Refined Security Constraints



Refined Security Requirements

Refined Security Constraints – Output of Architectural Analysis	
Hazardous Control Actions	**Required System Constraint**
Not Providing POSITION MX Commands is Hazardous if in a critical phase of flight [H1, H2, H3]	POSITION MX commands must be provided during critical phases of flight
POSITION MX commands are Hazardous if done too early or too late in a critical phase of flight [H1, H2, H3]	POSITION MX Commands must be executed within a specified time of the maneuver requirement
Providing CONTACT is hazardous if attempted during an unsafe position [H1]	CONTACT Command must only be provided if both aircraft are in a safe position ready for AR
Providing CONTACT out of sequence is hazardous if attempted during an unsafe position [H1]	CONTACT Command must not be issued or received after the BREAKAWAY Command has been issued until the aircraft have resumed a safe position

Phase 3: Design Analysis



The AFIT of Today is the Air Force of Tomorrow.

PROCESS MODEL DESCRIPTIONS		
Control Action	Key Activity	Process Model Description / Decision Logic
1. Position Mx	Fly	Execute Position Mx during critical phases of flight
2. Velocity Mx	Fly	Execute Velocity Mx during critical phases of flight
6. Breakaway	Refuel	Issue Breakaway when unsafe position

FULL PROCESS MODEL DESCRIPTION				
CA	Process Model Description	Process Model Variables	Process Model Variable Values	Feedback Information
Breakaway	Issue Breakaway when unsafe position	Separation Distance	In bounds, out of bounds, unknown	Altimeter warning, proximity warning, eyeball

Preliminary Design Specs

- Causal Scenario – Breakaway
  - Turbulence, out of position, poor refueler maneuvering, engine malfunction, ect.
  - In Bounds, Out of Bound, or Unknown

Results

- Conceptual Analysis STPA-Sec is executable on USAF warfighting system
- This work provides widely distributable STPA-Sec reference and detailed example of a USAF aircraft case study
  - Presents a tailored approach for execution
  - Provides recommendations to facilitate STPA-Sec utility to the novice practitioner
- Subjective utility assessment is below:

	Concept Analysis	Architectural Analysis	Design Analysis
Purpose	Determine Security Requirements	Determine Design-To Criteria	Determine Build-To Criteria
Difficulty	Easy	Moderate	Moderate-High
Level of Domain Expertise Req'd	Novice	Advanced	Expert
Level of STPA Expertise Req'd	Low	High	Moderate
Amount of STPA instructional materials available	Numerous	Some	Few
Duration	Hours	Days	Weeks
Number of Steps	4 Steps	5 Steps	5 Steps

Lessons Learned

- How to write hazards – within system bounds
  - Hazard is not the mountain, but the violation of clearance from terrain
- Functional Control Structure Design – start big and decompose as necessary
  - For KC-X provide simple top level then decompose to desired level of detail
- Iterate as often as desired – non linear process, iteration is encouraged!
  - After attempting FCS, revisited key activities for Mission Planning
- Control Actions – start with a larger list of easy to populate actions, then group and abstract up to high level actions
- Abstracting up maintains solution trade space
  - Don’t assume something will be done the way it was before
    - E.g. Breakaway command issues by boom operator (may be computer)

Significance/Future work

- DoD Major Weapons Systems are vulnerable – current approaches for cybersecurity limited in effectiveness and usability
  - NDAA 1647 Assessment of Major Weapons System
  - U. S. Air Force Cyber Resiliency Office for Weapons Systems
  - Air Force Cyber Campaign Plan
    - LOA 3- Train the Workforce
- Future Work
  - Develop training for 800+ USAF Civilian Acquisition Professionals on using STPA-Sec
  - Increase level of detail for KC-X example with SME and PM involvement
  - Execute STPA-Sec example for USAF Space system
    - Current survey did not identify any for satellites
  - Align STPA-Sec with UAF/Integrated Architecture
    - Add capability for executable models

Summary

- Motivation
- Case Study Overview
- Case Study Results
- Lessons Learned
- Significance
- Summary

Questions?

Contact Info:
Martin “Trae” Span: martin.span.1@us.af.mil
Logan Mailloux: logan.mailloux@us.af.mil

In Progress Publications

- *"Cybersecurity Architectural Analysis for Complex Cyber-Physical Systems"*
  - Proposes a definition of Cybersecurity Architectural Analysis
  - Survey and assessment of DoD and Industry architectural analysis approaches

- *"A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems"*
  - Introduces tailored STPA-Sec approach

- *"Conceptual Systems Security Analysis with Aerial Refueling Case Study"*
  - Provides elaboration of tailored approach through KC-X case study
  - Increases usability and provides recommendations for ease of use