A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems

Martin "Trae" Span

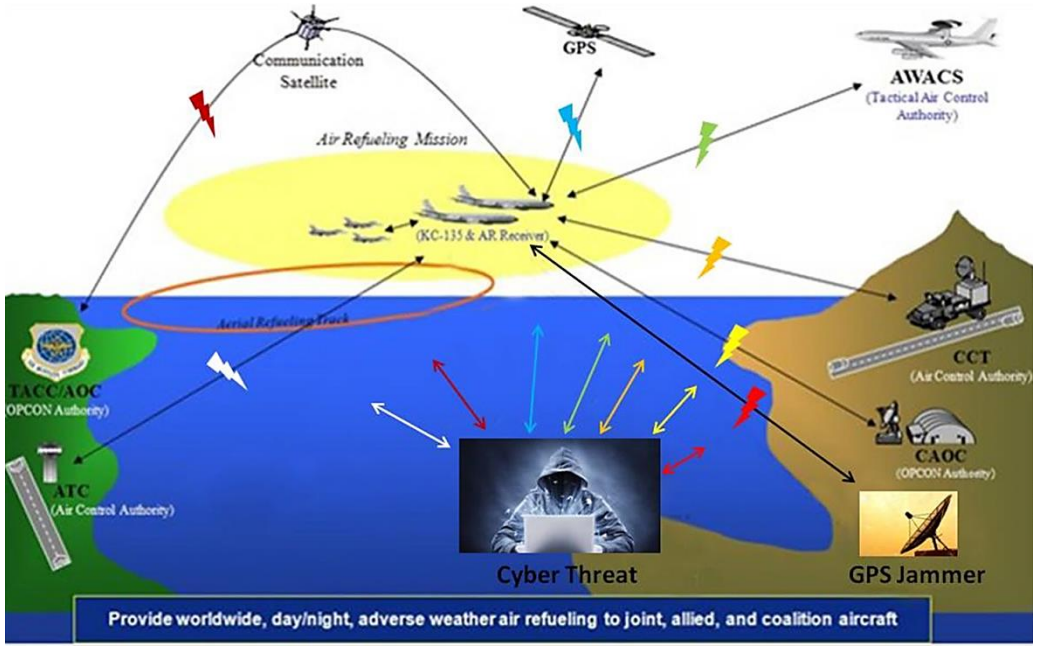
Motivation

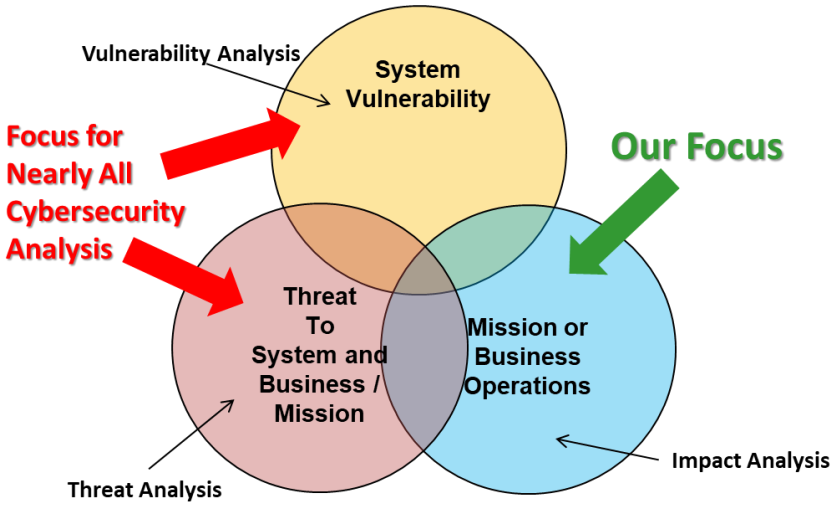
- Cyber-Physical Complex Systems are vulnerable
  - Current cybersecurity approaches are limited in effectiveness and usability
- Legacy weapons systems are not designed for cyber threats or cyber resiliency
- DoD and Congressional Mandates: NDAA Sec 1647– Requirement and funding to access major weapon systems
- U. S. Air Force Cyber Resiliency Office for Weapons Systems (CROWS)
  - Air Force Cyber Campaign Plan
    - "Bake in" for new acquisitions,
    - Mitigate critical vulnerabilities in fielded systems
    - LOA 3: Recruit, Hire, and **TRAIN** workforce

Right Image from CROWS 5/17 overview

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?

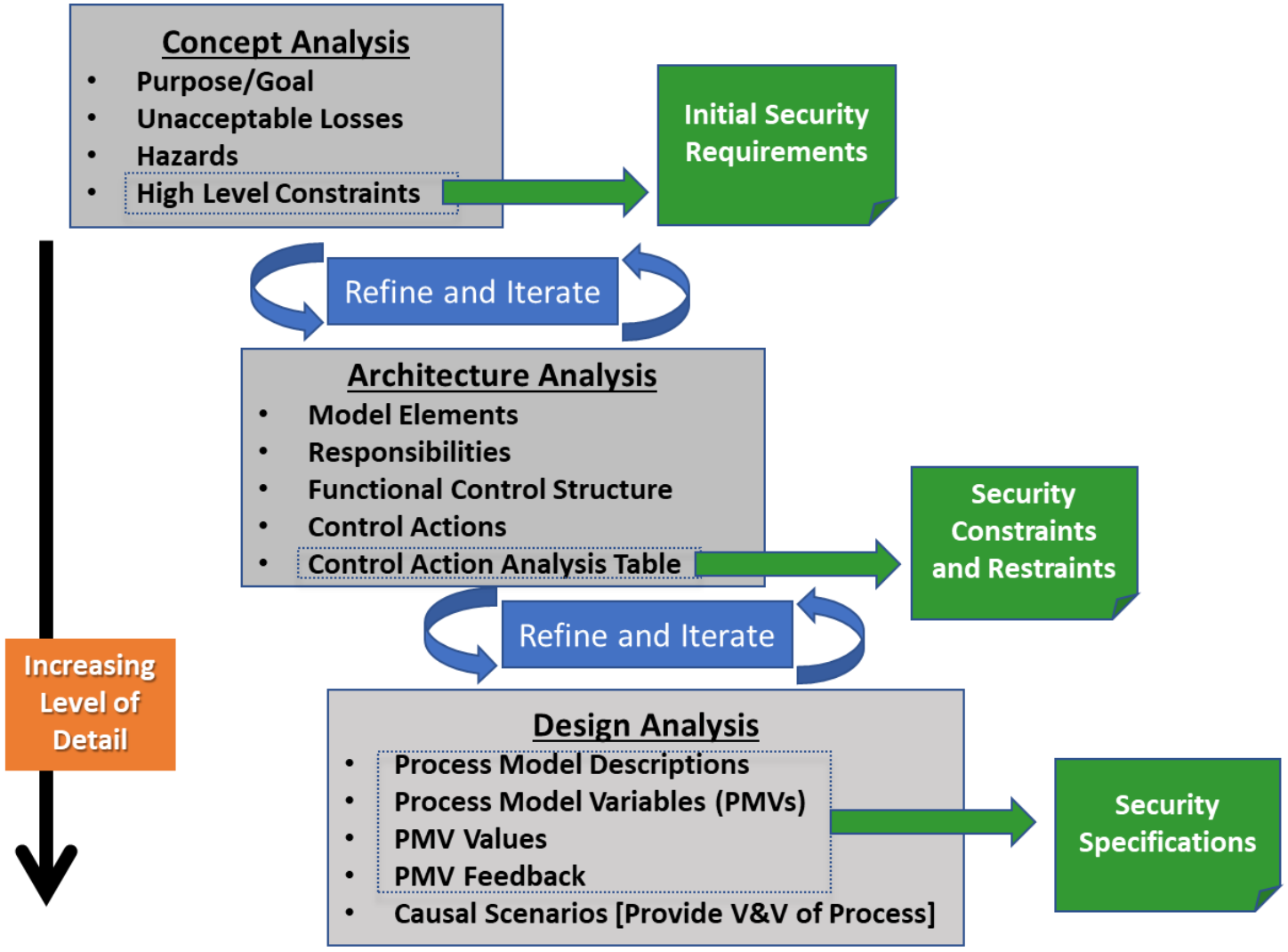




Right Image from Col Young CNW 2017

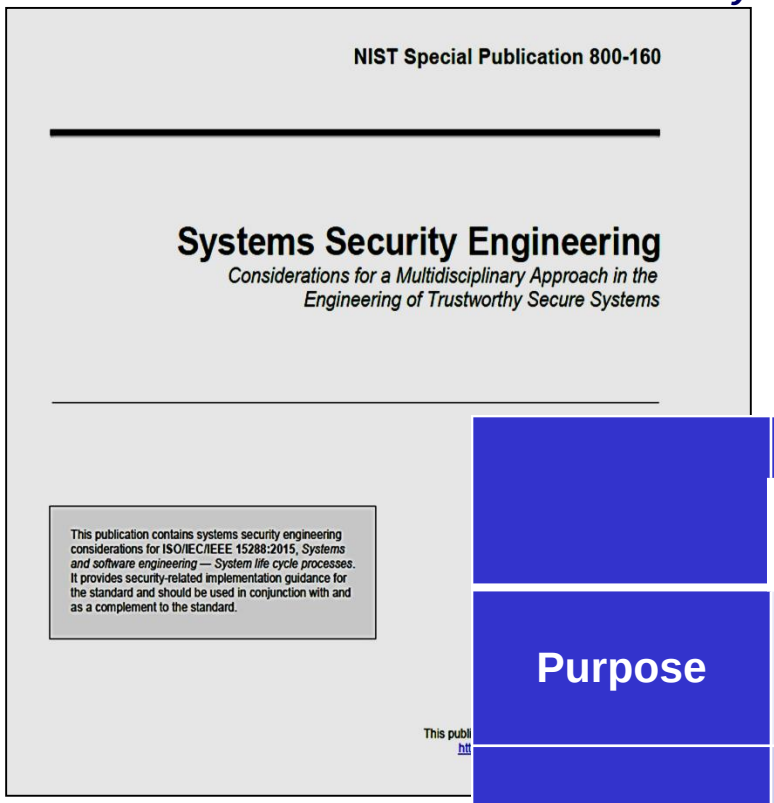
STPA-Sec Tailored Approach

The AFIT of Today is the Air Force of Tomorrow.



Mapping to NIST SP 800-160 Processes

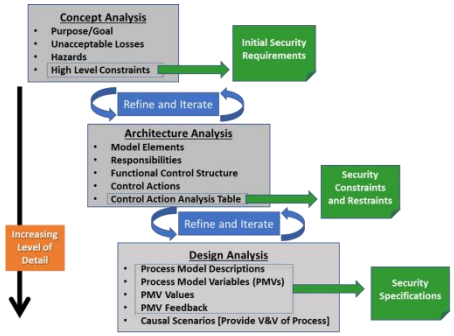
The AFIT of Today is the Air Force of Tomorrow.


NIST Special Publication 800-160

Systems Security Engineering

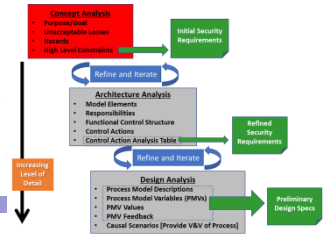
Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

This publication contains systems security engineering considerations for ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*. It provides security-related implementation guidance for the standard and should be used in conjunction with and as a complement to the standard.



	STPA-Sec Phases		
	Concept Analysis	Architectural Analysis	Design Analysis
Purpose	Determine Initial Security Requirements	Determine "Design-To" Constraints and Restraints	Determine "Build-To" Criteria
NIST 800-160 SSE Processes	• BA - Business Analysis • SN - Stakeholder Needs • SA - Systems Analysis	• SR - System Requirements Definition • AR - Architectural Definition • SA - Systems Analysis	• DE - Design Definition • SA - Systems Analysis

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

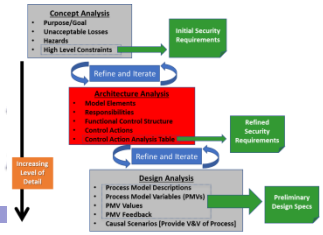
Hazard to Loss Cross Walk Table		**L1 Death or Human injury**	**L2 Damage to or loss of aircraft**	**L3 Unable to Complete Mission**
H1	Flying to Close to other aircraft/out of position	X	X	X
H2	Violation of Altitude/clearance from terrain	X	X	X
H3	Unable to evade enemy threats	X	X	X
H4	Msn critical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

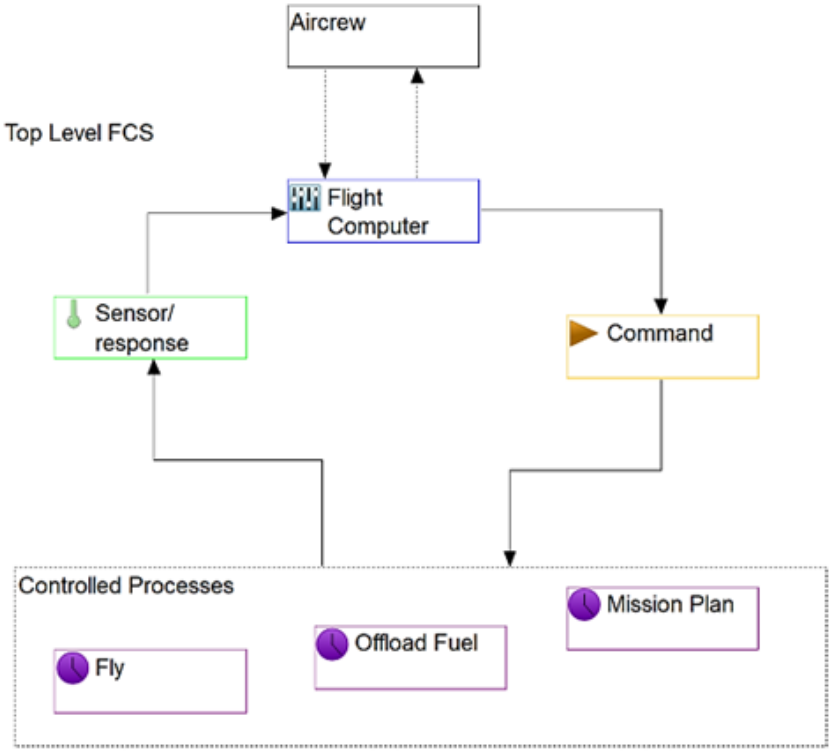
	Initial Security Constraints	**Hazard Mapped to**
1	A/C must maintain minimum safe separation distance	H1
2	Must have minimum mission critical safety systems functional to attempt AR	H1
3	A/C must maintain minimum safe altitude limits	H2
4	Must have minimum mission critical safety systems functional 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

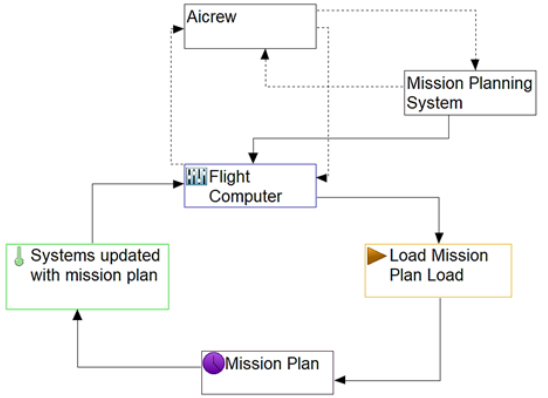
Initial Security Requirements

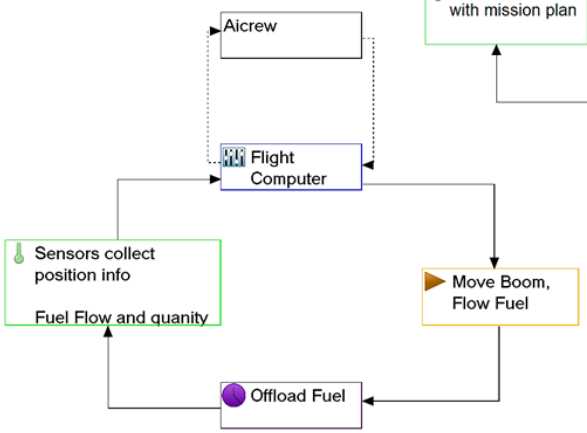
Phase 2: Architectural Analysis Functional Control Structure

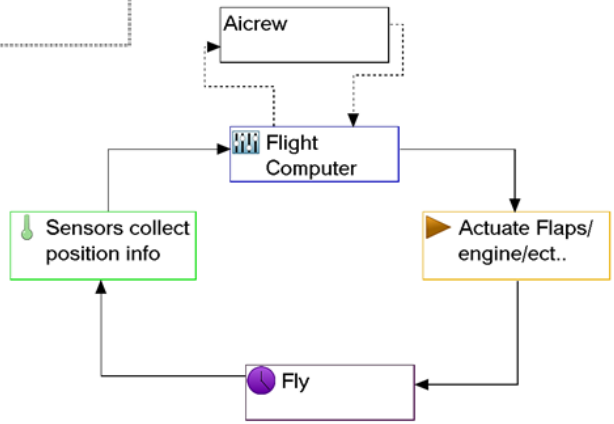
The AFIT of Today is the Air Force of Tomorrow.



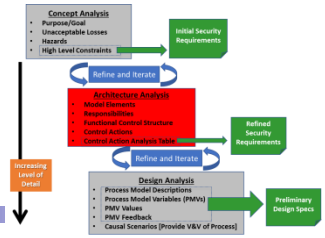








Architectural Analysis Control Actions

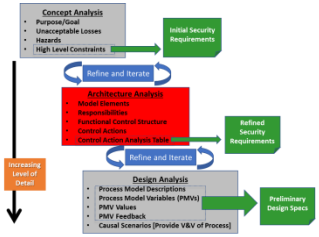


The AFIT of Today is the Air Force of Tomorrow.

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

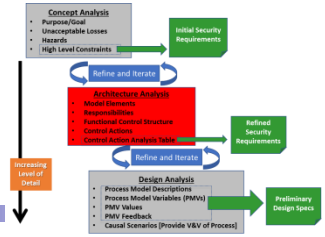
Architectural Analysis
Control Action Analysis Table

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]		

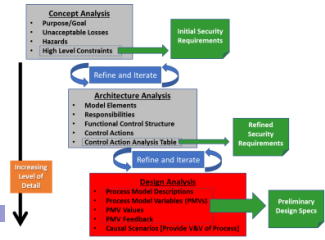
Architectural Analysis Output Security Constraints



Security Constraints and Restraints

Security Constraints and Restraints – 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

Security Specifications

- 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 systems
- This work provides widely distributable STPA-Sec reference and detailed example of a USAF aircraft case study
  - Presents a tailorable approach for execution
  - Provides a detailed example and recommendations to help the practitioner (a non-PhD) perform STPA-Sec
- 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