Illustrate the Need for UAS Cybersecurity Oversight & Risk Management A11L.UAS.95_A58

Research Project Description

- To address proactively the need to have UAS Cybersecurity Oversight and Risk Management processes.
- Approach: Perform a literature survey; develop a framework or process for cybersecurity risk management; and test the framework or process.
- Current PoP: 1/1/2022 – 4/30/2024

Sponsor Anticipated Outcome

- Literature review outlining state-of-the-art
- Oversight and Risk Management processes for UAS Cybersecurity oversight
- Testing and analysis results from tools and processes

Critical Milestones

- Task 1: Literature Review & Industry Engagement
- Task 2: Illustrate the Need for UAS Cybersecurity Oversight and Risk Management
- Task 3: Test Cybersecurity Oversight Tool or Process
- Task 4: Final Report and Final Briefing

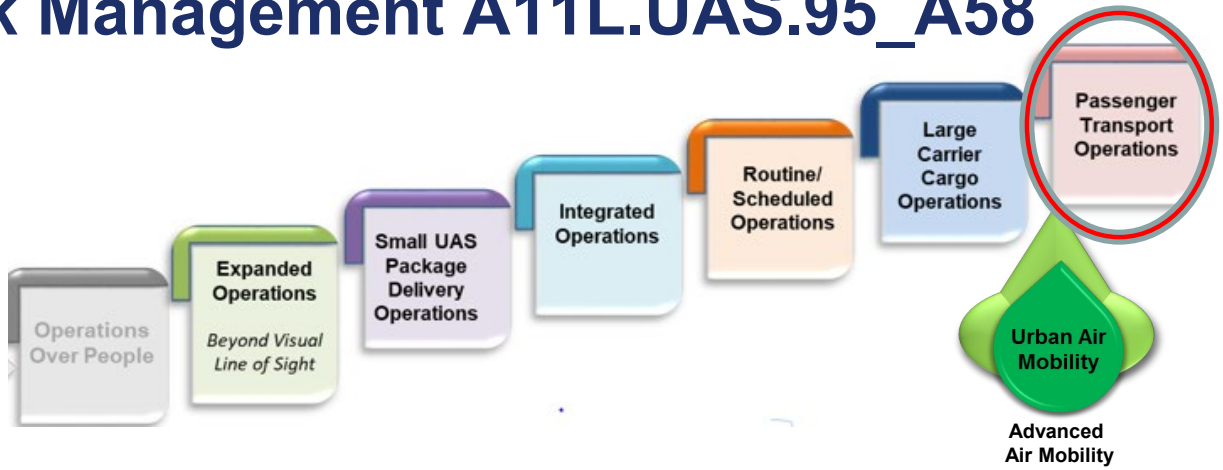
Research Accomplishments in FY22

- Held Kickoff Meeting – 2/17/2022

Illustrate the Need for UAS Cybersecurity Oversight & Risk Management A11L.UAS.95_A58

Recent Accomplishments

- *FY22_Q2*
  - *Kick-off Meeting*



Research Collaboration Team		
ANG-C21 Technical Monitor		
Matthew Novak, ANG-C21		
AUS-300 Sponsor Liaison (Co- Sponsor)	**Customer (Co-Sponsor)**	
Richard Lin, AUS-310	Sabrina Saunders-Hodge, AUS-300	
Research Execution Team		
ASSURE – KU	ASSURE – OrSU	ASSURE – DU

A58: Research Approach

- **<u>TASK 1: Literature Review and Industry Engagement – KU, OrSU, DU (Jan 2022)</u>**

- **Subtask(s):**
- Task 1-1: Review GAO-19-105 report on Identify, Protect, Detect, Respond, Recover approach
- Task 1-2: Review publicly available information from other reports concerning Risk Management Assessment elements, concerns and best practices
- Task 1-3: Engage industry partners in identifying best practices

- **Exit Criteria:**
- Draft Literature Review Report

- **Task Deliverable(s):**
- Literature Review

A58: Research Approach

- **Task 1-1: Review GAO-19-105 report on Identify, Protect, Detect, Respond, Recover approach**

- Currently reviewing GAO-19-105
  - Identify, Protect, Detect, Respond, Recover serves as an organization mechanism
  - Too abstract to capture UAS specific requirements and issues
  - Framework will refine the more general structure
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 from National Institute of Standards and Technology
  - Describe their current cybersecurity posture
  - Describe their target state for cybersecurity
  - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
  - Assess progress toward the target state
  - Communicate among internal and external stakeholders about cybersecurity risk

- **Current Status:** Reviewing GAO-19-105 and NIST Framework Document

A58: Research Approach

- **Task 1-2: Review publicly available information from other reports concerning Risk Management Assessment elements, concerns and best practices**

- Start from recently completed A38 Study
- Search for UAS-specific literature
  - Frameworks and approaches
  - Issues and examples
  - Examine proxy systems with similar architectures
  - Cyberphysical is particularly important
- Controlling paper explosion
  - Identify sources (ACM, IEEE, AIAA, Oakland, USENIX, etc.)
  - Limit to 10 years in the past
  - UAS-specific literature
  - UAS frameworks and approaches
  - UAS issues and examples
- Focus on mapping to GAO and NIST documents
  - Established ontology for organizing information
  - Initial NIST framework for refinement

- **Current Status:** Gathering and classifying papers and public literature

A58: Research Approach

- **Task 1-3: Engage industry partners in identifying best practices**

- Engage KU security advisory board
  - Garmin – Aerospace security lead (Dan Hine)
  - Collins Aerospace – System security lead (David Hardin, Darren Cofer)
  - T-Mobile – Wireless Communication and 5G (Lyle Paczkowski)
  - Arm – Security architecture (James Flack)

- **Current Status:**
  - Contacted Garmin, initiated discussions
    - Mitch Trope (Security Lead, Aerospace)
    - Dan Hein (Security Lead, Garmin)
  - Contacted Collins Aerospace, discussions planned
    - David Harden (Formal Methods Lead)
    - Darren Cofer (Research Fellow)
  - T-Mobile on hold
    - Company reorg moving people
  - Arm on hold
    - Company reorg moving people

A58: Research Approach

- **<u>TASK 2: UAS Cybersecurity Oversight and Risk Management – KU, DU, OrSU (Apr 2022)</u>**

- **Subtask(s):**
- Task 2-1: Framework Definition
- Task 2-2: Dynamic Analysis
- Task 2-3: Static Analysis
- Task 2-4: Cyberphysical Analysis

- **Exit Criteria:**
- Create a report detailing a Tool or Process that can be used for UAS Cybersecurity Oversight and Risk Management.

- **Task Deliverable(s):**
- UAS Cybersecurity Oversite and Risk Management Tool and/or Process

A58: Research Approach

- **<u>TASK 3: Test Cybersecurity Oversight Tool or Process– KU, DU, OrSU (Apr 2022)</u>**
- **Subtask(s):**
- Task 3-1: Dynamic Performance Testing
- Task 3-2: Cyberphysical Security Testing
- Task 3-3: Resource Aware Testing
- Task 3-4: Penetration Testing
- Task 3-5: Student Engagement
- Task 3-6: Flight

- **Exit Criteria:**
- Create a report detailing the scenarios developed, results of the table-top simulation or live-test event, and lessons learned

- **Task Deliverable(s):**
- Report on scenarios, simulations, live testing and lessons learned

A58: Research Approach

- **<u>TASK 4: Peer Reviewed Final Report and Final Briefing– KU, DU, OrSU (Oct 2023)</u>**

- **The performers will write a final report documenting:**
  - 1. The Cybersecurity Oversight Tool or Process
  - 2. The process and results of testing the Cybersecurity Oversight Tool or Process
  - 3. Areas of need and future research
- **Deliver software and hardware developed for the research effort.**

- **Exit Criteria:**
- Summarize and aggregate all of the previous reports into a final report package for the overall project.

- **Task Deliverable(s):**
- Peer Reviewed Final Report