Integrating Uninhabited Aerial Systems into the NAS

Natasha A. Neogi
1st STAMP/STPA Workshop at MIT
April 19th, 2012

Thanks to: Paul Miner, Kelly Hayhurst, Jeff Maddalon, Cesar Munoz, Jae Kim, Cladiu Danilov, Matthew Clark, Siva Banva (WP-AFB)
NextGen (Utopia)

- Reduced weather delays
- Accommodation of unmanned aerial vehicles
- Shared situational awareness
- Accommodation of very light jets
- Distributed scheduling
  - Enhanced wake turbulence protection
  - Reduced noise and emissions
- Human-centered automation
- Enhanced security
- Increased capacity
Overview

- Motivation and Certification
  - Or ‘Why is it so hard to get a COA’?
- UAVs and Accidents
  - Military Perspectives (WP-AFB)
- STAMP and Implications
  - Global Hawk
- Issues and Conclusions
  - 3Cs (Classification, Criteria, Communication)
Aviation Regulations

- Title 14 Codes for Federal Regulation: Federal Aviation Regulations (FARs) covered in Parts 1-200
  - Part 23: Airworthiness standards for Normal, Utility, Acrobatic, and Commuter Aircraft
  - Part 25: Airworthiness standards for Transport Aircraft
  - Part 91: General Operating & Flight Rules
  - Parts 61,141: Pilot Licensing

<table>
<thead>
<tr>
<th>Airborne</th>
<th>Ground</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAA regulates airborne systems</td>
<td>FAA acquires and regulates ground systems</td>
</tr>
<tr>
<td>Aircraft, engines, propellers certified in compliance with FARs</td>
<td>FAA provides ATC via CNS equipment commissioned icw FAA Orders &amp; Contracts</td>
</tr>
</tbody>
</table>
Ground vs Airbourne

- CNS/ATM ground system compliance is more application specific
  - ADS-B etc.

- Software Guidelines similar
  - RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification
  - RTCA/DO-278, Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance

What about Ground Based CNS components of UAS? e.g., Networked Communications…
Airbourne System Automation

- Aircraft must be airworthy (Part 91.7): Type Certificate
- Airworthiness requirements specific to avionics in FAR Parts (23,25,27,29).(1301,1309)

| SAE ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment | Functional Hazard Assessment
Failure Modes and Effects Analysis
Particular Risks Analysis
Common Mode Analysis
System Safety Assessment
STAMP/STPA? |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SAE ARP 4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems</td>
<td></td>
</tr>
</tbody>
</table>

Allocation of Requirements to Hardware & Software: (RTCA)/DO254 & /DO-178B
FAR Part (23,25).1309 Equipment, Systems, and Installations

- These targets drive requirements for redundancy and rigor in design and development of systems and equipment.

- Compliance with these requirements drives the *cost* of systems and equipment.

<table>
<thead>
<tr>
<th>Classification of Failure Conditions</th>
<th>No Safety Effect</th>
<th>Minor</th>
<th>Major</th>
<th>Hazardous</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allowable Probabilities and Software and Complex Hardware Design Assurance Levels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part 23 Class I</td>
<td>No Requirement</td>
<td>&lt;10^{-3} Level D</td>
<td>&lt;10^{-4} Level C/D</td>
<td>&lt;10^{-5} Level C/D</td>
<td>&lt;10^{-6} Level C</td>
</tr>
<tr>
<td>Part 23 Class II</td>
<td>No Requirement</td>
<td>&lt;10^{-3} Level D</td>
<td>&lt;10^{-5} Level C/D</td>
<td>&lt;10^{-6} Level C/D</td>
<td>&lt;10^{-7} Level C</td>
</tr>
<tr>
<td>Part 23 Class III</td>
<td>No Requirement</td>
<td>&lt;10^{-3} Level D</td>
<td>&lt;10^{-5} Level C/D</td>
<td>&lt;10^{-7} Level C</td>
<td>&lt;10^{-8} Level B/C</td>
</tr>
<tr>
<td>Part 23 Class IV Commuter</td>
<td>No Requirement</td>
<td>&lt;10^{-3} Level D</td>
<td>&lt;10^{-5} Level C/D</td>
<td>&lt;10^{-7} Level B/C</td>
<td>&lt;10^{-9} Level A/B</td>
</tr>
<tr>
<td>Part 25 Transport</td>
<td>No Requirement</td>
<td>&lt;10^{-5} Level D</td>
<td>&lt;10^{-5} Level C/D</td>
<td>&lt;10^{-7} Level B/C</td>
<td>&lt;10^{-9} Level A/B</td>
</tr>
</tbody>
</table>


- Thanks to Kelly Hayhurst, Jeff Maddelon and Chuck Johnson
But for a UAS...

<table>
<thead>
<tr>
<th>Classification of Failure Conditions</th>
<th>No Safety Effect</th>
<th>Minor</th>
<th>Major</th>
<th>Hazardous</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UAS Class I?</strong></td>
<td>No Requirement</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td><strong>UAS Class II?</strong></td>
<td>No Requirement</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>...</td>
<td>No Requirement</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

- Thanks to Kelly Hayhurst, Jeff Maddelon and Chuck Johnson
Hmmm...Need Insight (and Data)

<table>
<thead>
<tr>
<th>Classification of Failure Conditions</th>
<th>No Safety Effect</th>
<th>Minor</th>
<th>Major</th>
<th>Hazardous</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAS Class I?</td>
<td>No Requirement</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>UAS Class II?</td>
<td>No Requirement</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

... Requirement

We don’t have sufficient evidence to say these things are safe! Maybe we should be more conservative!

A UAS has no one on board – so my UAS does not need to comply with $10^{-9}$!!

-Thanks to Kelly Hayhurst, Jeff Maddelon and Chuck Johnson
Overview

- Motivation and Certification
  - Or ‘Why is it so hard to get a COA’?
- UAVs and Accidents
  - Military Perspectives (WP-AFB)
- STAMP and Implications
  - Global Hawk
- Issues and Conclusions
  - 3Cs (Classification, Criteria, Communication)
US Army: Hunter Aircraft (32)

- Twin-engine, short-range (144 nm) tactical aircraft
  - Payload capacity: 200 lb
  - Endurance: 1200 nm
  - Weight: 1600 pounds
  - Wingspan: 29 ft
  - Ceiling: 15,000 ft,
  - Cruise: 100 kts
  - Cost: $1.2M (Schaefer, 2003).

- Hunter takes off (20%) and lands (47%) using an External Pilot (EP) standing next to the runway in visual contact with the aircraft
  - Reverse control issues
  - Autopilot display (IP) vs (EP) control

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
US Army: Shadow Aircraft (24)

- **Shadow 200 short-range surveillance aircraft**
  - Payload capacity: 60 lbs
  - Endurance: 68nm
  - Wingspan: 9 ft
  - Weight: 330 lbs
  - Ceiling: 14,000 ft
  - Cruise: 82 kts
  - Cost: $325,000

- **Shadow does not use an external pilot, depends on a launcher for takeoffs and an automated landing system for recovery (Tactical Automated Landing System).**
  - GCS pilot has no visual/sensors on a/c during landing (engine kill error)

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
Navy Pioneer RQ-2 Aircraft (239)

- Single-engine, propeller-driven aircraft
  - Payload capacity: 72 lbs
  - Endurance: 400 nm
  - Wingspan: 17 ft
  - Weight: 452 lbs
  - Ceiling: 15,000 ft
  - Cruise: 80 kts
  - Cost: $650,000

- Pioneer requires an EP for takeoff (10%) and landing (68%)
  - 3 mode GCS: autonomous, IP(flight)/autopilot(waypoint), joystick

- Since 1985 it has logged over 20,000 hr flight time
  - Aircrew coordination, weather related, enemy action

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
## Predator MQ-(1,9) Specifications

Flown from within a GCS: joystick, rudder pedals, forward looking camera (30°)

<table>
<thead>
<tr>
<th></th>
<th>MQ-1</th>
<th>MQ-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gross Weight</td>
<td>2,250 lbs</td>
<td>10,000 lbs</td>
</tr>
<tr>
<td>Length</td>
<td>28.7 ft</td>
<td>36.2 ft</td>
</tr>
<tr>
<td>Wingspan</td>
<td>48.7 ft</td>
<td>64 ft</td>
</tr>
<tr>
<td>Ceiling</td>
<td>25,000 ft</td>
<td>45,000 ft</td>
</tr>
<tr>
<td>Radius</td>
<td>400 nm</td>
<td>400 nm</td>
</tr>
<tr>
<td>Endurance</td>
<td>24 + hrs</td>
<td>24 + hrs</td>
</tr>
<tr>
<td>Payload</td>
<td>450 lb</td>
<td>750 lb (internal)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3000 lb (external)</td>
</tr>
<tr>
<td>Cruise Speed</td>
<td>70 kts</td>
<td>220 kts</td>
</tr>
<tr>
<td>Aircraft cost (w/out sensors)</td>
<td>$2.4 M</td>
<td>$6 M</td>
</tr>
<tr>
<td>System Cost (4 Avs)</td>
<td>$26.5 M</td>
<td>$47 M</td>
</tr>
</tbody>
</table>

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
US Air Force: Predator MQ1, MQ-9 (15)

- GCS Handoff: Mishap Crew incorrectly ordered checklist accomplishment → engine and stability augmentation kill (uncommanded dive and crash)
- Pilot accidentally activated a program that erased the internal random access memory onboard the aircraft during flight.
- Menu selection allocation associated with function keys on the GCS keyboard: controlling the lights on the predator is similar to commanding an engine kill
- Problems with HUD, HDD, Alerts/Alarms, Autopilot
  - HUD: vision, attitude & RPM indicator, symbology lacks contrast
  - HDD: commands unprotected, too many levels, inconsistent operational value ranges
  - No indication on the HUD of status of autopilot, no override

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
UAV Accidents

- Summary of causes of Military UAV accidents

Overview

- Motivation and Certification
  - Or ‘Why is it so hard to get a COA’?
- UAVs and Accidents
  - Military Perspectives (WP-AFB)
- STAMP and Implications
  - Global Hawk
- Issues and Conclusions
  - 3Cs (Classification, Criteria, Communication)
US Air Force: Globalhawk (3)
## Globalhawk Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>RQ-4A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>26,750 lbs</td>
</tr>
<tr>
<td>Length</td>
<td>44.4 ft</td>
</tr>
<tr>
<td>Wingspan</td>
<td>116.2 ft</td>
</tr>
<tr>
<td>Ceiling</td>
<td>65,000 ft</td>
</tr>
<tr>
<td>Radius</td>
<td>5,400 nm</td>
</tr>
<tr>
<td>Endurance</td>
<td>32 hrs</td>
</tr>
<tr>
<td>Payload</td>
<td>1,950 lbs</td>
</tr>
<tr>
<td>Cruise Speed</td>
<td>345 kts</td>
</tr>
<tr>
<td>Aircraft Cost</td>
<td>$20 M</td>
</tr>
<tr>
<td>System Cost</td>
<td>$57 M</td>
</tr>
</tbody>
</table>

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
Global Hawk: Accident of Note

- Pilot and crew actions pre-programmed
  - Mission planning process begins 270 days a priori
  - Mission planners become actively involved 90 days prior to flight
  - Takes 3-5 weeks to write a flight plan
  - Validation takes 10 days, starts 18 days a priori to flight

- Aircraft suffered from in-flight problem with temperature regulation of avionics, landed at preprogrammed alternative airport for service

- Taxi speed of 155 kts was commanded at this waypoint (automated mission planning software)
  - Hex status reports

OSD UAS Airspace Integration Plan March 2011, Communications from WPAFB 2010-2012, Manning et al., The role of human causal factors in U.S. Army unmanned aerial vehicle accidents. 2004
Accident and Hazard

- **Accident**
  - Class A: An accident in which the resulting total cost of property damage is $1,000,000 or more; an aircraft or missile is destroyed, missing, or abandoned; or an injury and/or occupational illness results in a fatality or permanent total disability. (US Army Classification System)

- **Hazard**
  - Loss or damage of secure asset for prolonged duration, rendering mission incomplete/ineffective.

- **Safety Constraint**
  - The safety control structure must prevent loss of asset or mission compromise. Additionally, structure must prevent the exceeding of power/dynamic actuation/structural limits of asset.
DoD Stakeholders
- Office of Undersecretary of Defense AT&L
- Policy Board on Federal Aviation
- AF (Service) UAS Program Offices
- Joint UAS CoE & National Guard
- Defense Standardization Program Office
- US JFCOM (also PACCOM etc.)

Non-DoD Stakeholders
- FAA
- DHS
- NASA
- Civil Standards Development Organizations
- UAV Manufacturers (Northrup Grumman etc.)
- AOPA
- IATA, UPS, FedEx
- ICAO
- NATCA, IAFATCA
- NATO

Inter-Agency Organizations
- JPDO
- NAS ExCom

Flow of Information:
- Flight Plans/Procedures
- Regulations
- Clearances
- NAS Restrictions
Mission Planning System Dynamics

- Secretary of the Air Force (OUSAF Decision-Making)
- Strategic Routes
- Mission Planning and Operations (AF) Decision-Making
- UAS COE
- PBFA
- Mission Implementation
- Tactical Plan Implementation: Targets
- Mission Validation Plan
- Software and Hardware Onboard Implementation
  - Technical Personnel Resources and Experience
  - Available Onboard Resources Maintenance Personnel
  - System Development and Safety Analysis Completion
- Mission Pressure Loop
- Safety and Mission Assurance
- Safety Management Loop
- R1: Mission Execution Crew and Monitors
- R2: Mission Validation Plan
Operational Mission Planning:
Safety Requirements and Constraints: Provide a strategic and tactical plan that services targets with given route.

Context in Which Decisions Made:
Multi-Organizational Team, over different timespans

Inadequate Control Actions: No consistent method to identify priority of contingency plans and values in the face of online user inputs. • No established method to create indexed optional flight plans with current operational values.

Process Model Flaws: Contingency plans are developed far in advance, without clear operational/environmental constraints.

Feedback: Flight plans flown are not annotated with crew intent for analysis

-------------------

Mission Execution Crew:
Safety Requirements and Constraints: Provide a means of online monitoring and intervention during mission.

Context in Which Decisions Made:
A trained operational crew, possibly w/o mission planning experience

Inadequate Control Actions: No consistent method to update execution values during contingency execution• No established method to intervene and override control inputs during immediate term execution.

Mental Model Flaws: Pilot crews would execute contingency plans without reference to prior execution values.

Feedback: No direct means to impact future mission plans for executional efficiency in face of intervention.
Category of Requirements
Inconsistent/Incomplete

- Authority and Autonomy
  - Importance of state feedback information
  - Mode inconsistency
- Sensor and Actuator
  - Latency and delay
- Control software errors
  - Software handling of signal priority
  - Delay in input processing
  - Control software algorithm system dynamic model
- Mental Model/Human System Integration Errors
Overview

- Motivation and Certification
  - Or ‘Why is it so hard to get a COA’?
- UAVs and Accidents
  - Military Perspectives (WP-AFB)
- STAMP and Implications
  - Global Hawk
- Issues and Conclusions
  - 3Cs (Classification, Criteria, Communication)
## Classification Scheme(s)

- **Operational Environment**
  - Urban vs Enroute
- **Levels of Autonomy**
  - Onsite vs Remote pilots
- **Operational Purpose**
  - Frangability
- **Long Term vs. Rapid Deployment**
  - Mission Plan Latencies, Uncertainty

Understand assumptions, rationale, implications to enable cross-comparison

### DoD UAS Groups

<table>
<thead>
<tr>
<th>UAS Groups</th>
<th>Maximum Weight (lbs) (MGTOW)</th>
<th>Normal Operating Altitude (ft)</th>
<th>Speed (kts)</th>
<th>Representative UAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1</td>
<td>0 – 20</td>
<td>&lt;1200 AGL</td>
<td>100</td>
<td>Raven (RQ-11), WASP</td>
</tr>
<tr>
<td>Group 2</td>
<td>21 – 55</td>
<td>&lt;3500 AGL</td>
<td>&lt;250</td>
<td>ScanEagle</td>
</tr>
<tr>
<td>Group 3</td>
<td>&lt; 1320</td>
<td>&lt; FL 180</td>
<td></td>
<td>Shadow (RQ-7B), Tier II / STUAS</td>
</tr>
<tr>
<td>Group 4</td>
<td>&gt;1320</td>
<td>Any Airspeed</td>
<td></td>
<td>Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1AVB), Sky Warrior ERMP (MQ-1C)</td>
</tr>
<tr>
<td>Group 5</td>
<td>&gt; FL 180</td>
<td></td>
<td></td>
<td>Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)</td>
</tr>
</tbody>
</table>

OSD UAS Airspace Integration Plan March 2011
Airworthiness Criteria:
Self Separation

Sense and Avoid +CD&R +Path Planning: Demonstrably Satisfies Safety Criteria in Mixed Operation Environment - i.e., latencies, uncertainties, operations

Flight Rules
Airworthiness
Pilot (Operator) Certification

UAS Merge to Continuous Parallel Landing with Go-Around Execution
Networked Communications

• UAS Communication, Command and Control (C3) architecture must be secure and safe
  – Can contain both ground and airbourne elements
    • Spectrum?
  – Conforming and Byzantine collusive agents must be tolerated

• Integration of safety critical C3 systems and current ATC communication must be handled
  – Continuous availability of CNS for piloted a/c
  – Latency of remote commands bounded

• Human System Integration Issues are the projected leading cause of accidents based on current data
Conclusions

- Need hazard and risk-related data collection to support development of type design criteria and standards
- Need to evaluate a spectrum of separation assurance systems with different functional allocations (levels of authority and autonomy) and their interaction with mixed equipage aircraft
- Human System Integration Issues are the projected leading cause of accidents based on current data
Questions?

Natasha.Neogi@nianet.org