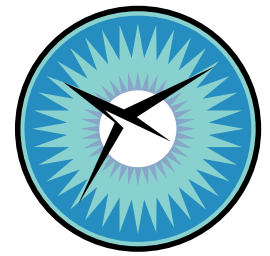


National Aeronautics  
and Space Administration

NATIONAL  
INSTITUTE OF  
AEROSPACE



# Integrating Uninhabited Aerial Systems into the NAS



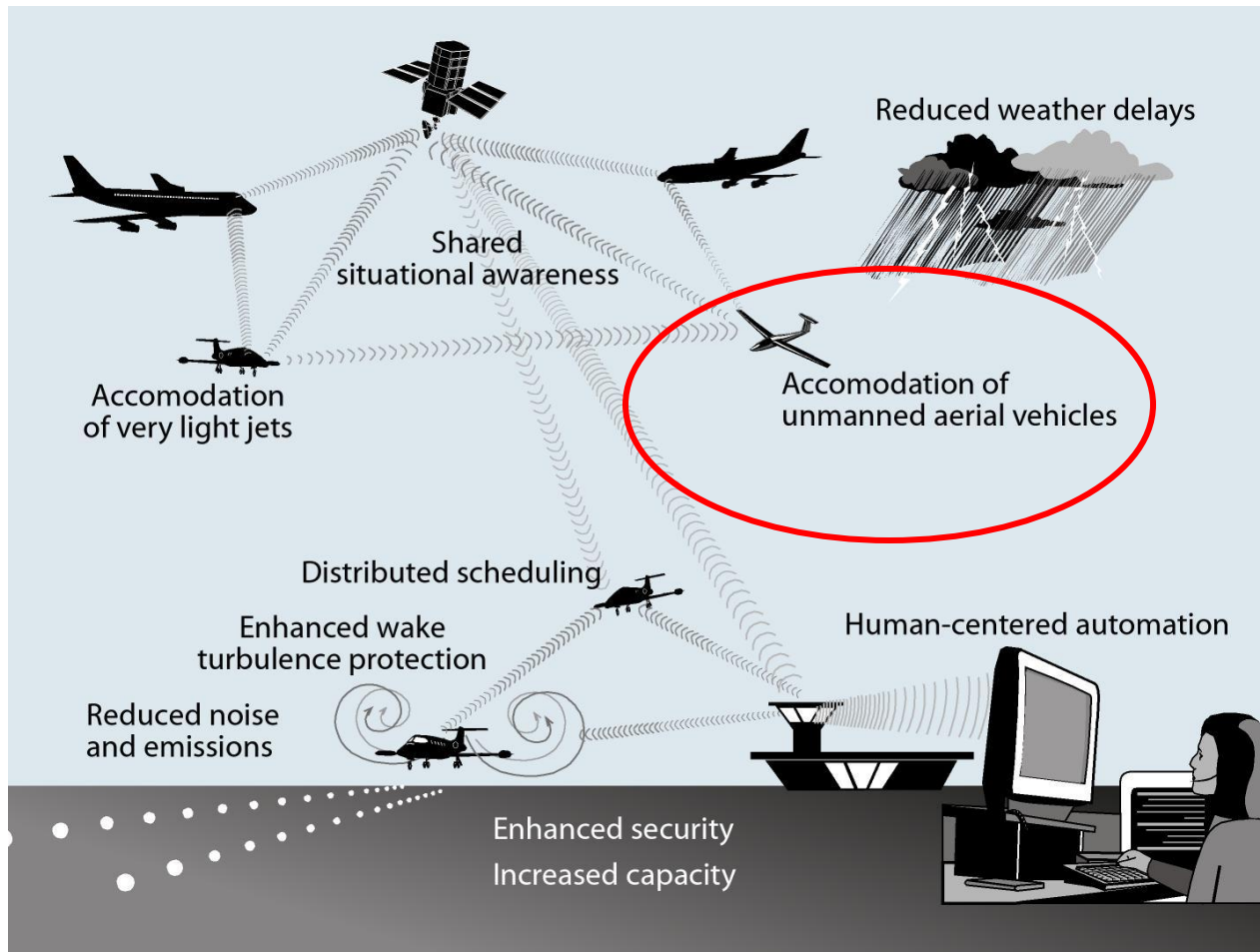
Natasha A. Neogi

1<sup>st</sup> 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)



# 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

Airborne	Ground
FAA regulates airborne systems	FAA acquires and regulates ground systems
Aircraft, engines, propellers certified in compliance with FARs	FAA provides ATC via CNS equipment commissioned icw FAA Orders & Contracts

# 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 Preliminary System Safety Assessment Failure Modes and Effects Analysis
SAE ARP 4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems	Particular Risks Analysis Common Mode Analysis System Safety Assessment <b>STAMP/STPA?</b>

**Allocation of Requirements to Hardware & Software: (RTCA)/DO254 & /DO-178B**

---

# FAR Part (23,25).1309 Equipment, Systems, and Installations

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Allowable Probabilities and Software and Complex Hardware Design Assurance Levels					
Part 23 Class I	No Requirement	<10 <sup>-3</sup> Level D	<10 <sup>-4</sup> Level C/D	<10 <sup>-5</sup> Level C/D	<10 <sup>-6</sup> Level C
Part 23 Class II	No Requirement	<10 <sup>-3</sup> Level D	<10 <sup>-5</sup> Level C/D	<10 <sup>-6</sup> Level C/D	<10 <sup>-7</sup> Level C
Part 23 Class III	No Requirement	<10 <sup>-3</sup> Level D	<10 <sup>-5</sup> Level C/D	<10 <sup>-7</sup> Level C	<10 <sup>-8</sup> Level B/C
Part 23 Class IV Commuter	No Requirement	<10 <sup>-3</sup> Level D	<10 <sup>-5</sup> Level C/D	<10 <sup>-7</sup> Level B/C	<10 <sup>-9</sup> Level A/B
Part 25 Transport	No Requirement	<10 <sup>-5</sup> Level D	<10 <sup>-5</sup> Level C/D	<10 <sup>-7</sup> Level B/C	<10 <sup>-9</sup> Level A/B

- 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**

from FAA Advisory Circulars, 23.1309: System Safety Analysis and Assessment, and 25.1309: System Design & Analysis

Thanks to Kelly Hayhurst, Jeff Maddelon and Chuck Johnson

# But for a UAS...

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
<b><i>UAS Class I?</i></b>	<b><i>No Requirement</i></b>	<b><i>?</i></b>	<b><i>?</i></b>	<b><i>?</i></b>	<b><i>?</i></b>
<b><i>UAS Class II?</i></b>	<b><i>No Requirement</i></b>	<b><i>?</i></b>	<b><i>?</i></b>	<b><i>?</i></b>	<b><i>?</i></b>
<b><i>...</i></b>	<b><i>No Requirement</i></b>	<b><i>?</i></b>	<b><i>?</i></b>	<b><i>?</i></b>	<b><i>?</i></b>



# Hmmm...Need Insight (and Data)

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazard
		?	?	
...	<i>Requirement</i>			?
				?

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  $10^{-9}$ !!



# Overview

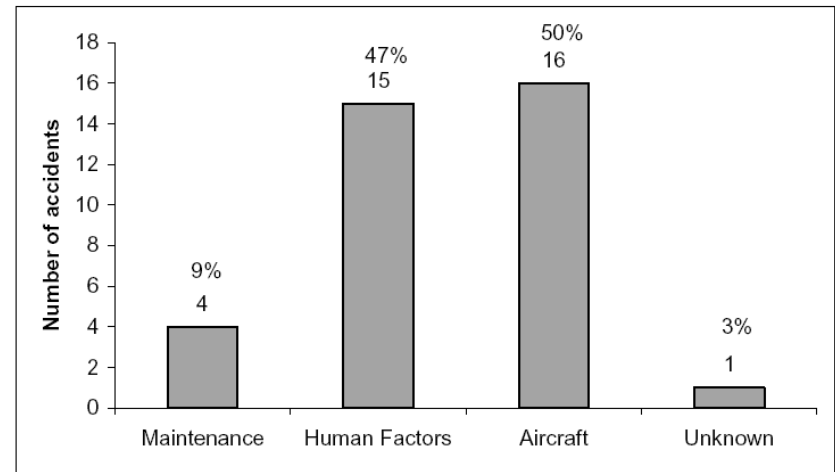
---

- 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).



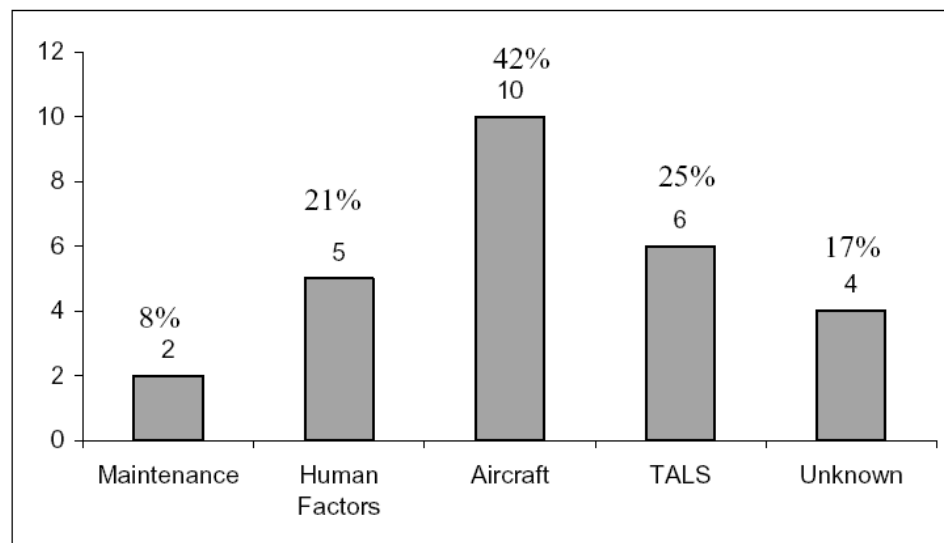
- Hunter takes off (20%) and lands (47%) using an External Pilot (EP) standing next to the runway in visual contact with the aircraft

- Reverse control issues
- Autopilot display (IP) vs (EP) control

# 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

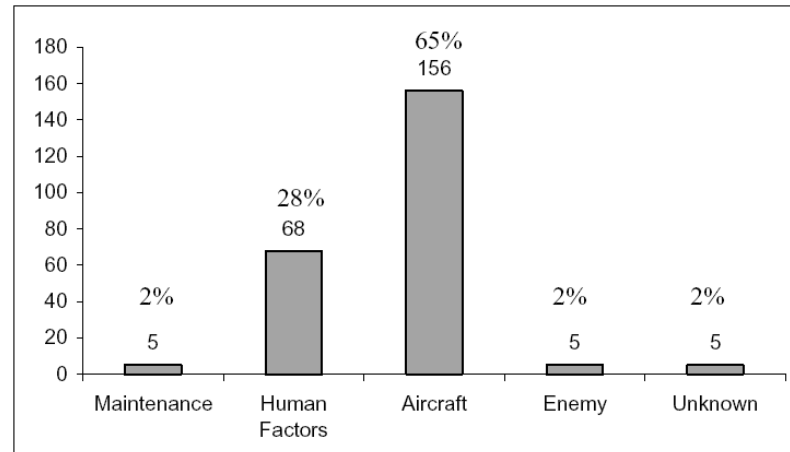


- Shadow does not use an external pilot, depends on a launcher for takeoffs and an automated landing system for recovery (Tactical Automated Landing System).
  - GCS pilot has no visual/sensors on a/c during landing (engine kill error)

# 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

# Predator MQ-(1,9) Specifications

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

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

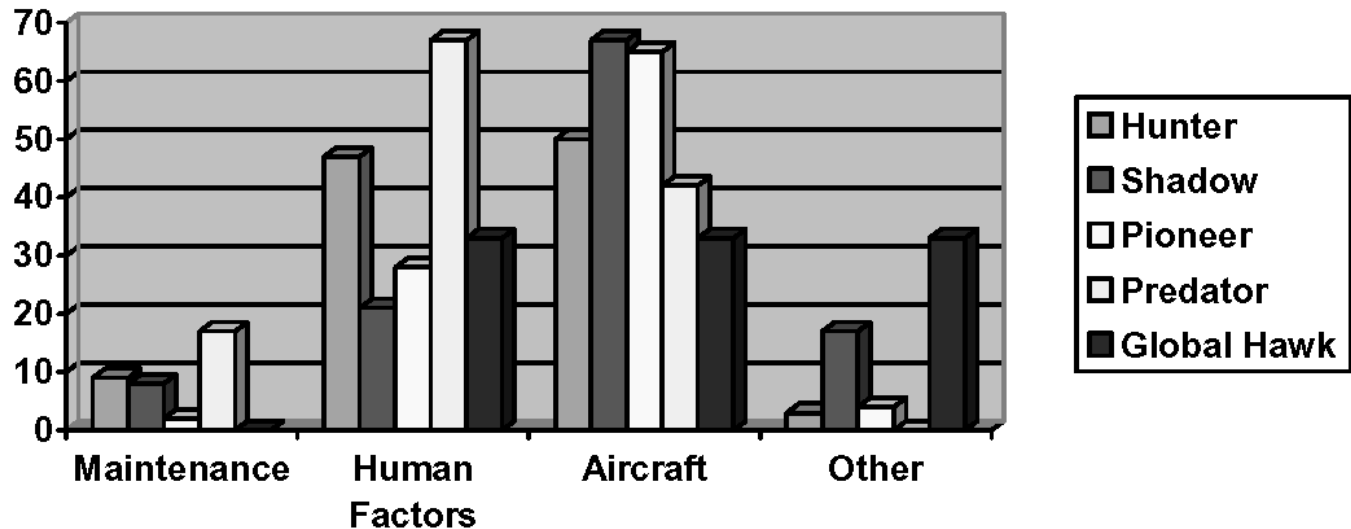
# US Air Force: Predator MQ1, MQ-9 (15)

---

- 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

# UAV Accidents

- Summary of causes of Military UAV accidents



Taken from: K. W. Williams, A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications, 2004.



# 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

---

	RQ-4A
Weight	26,750 lbs
Length	44.4 ft
Wingspan	116.2 ft
Ceiling	65,000 ft
Radius	5,400 nm
Endurance	32 hrs
Payload	1,950 lbs
Cruise Speed	345 kts
Aircraft Cost	\$20 M
System Cost	\$57 M

# Global Hawk: Accident of Note

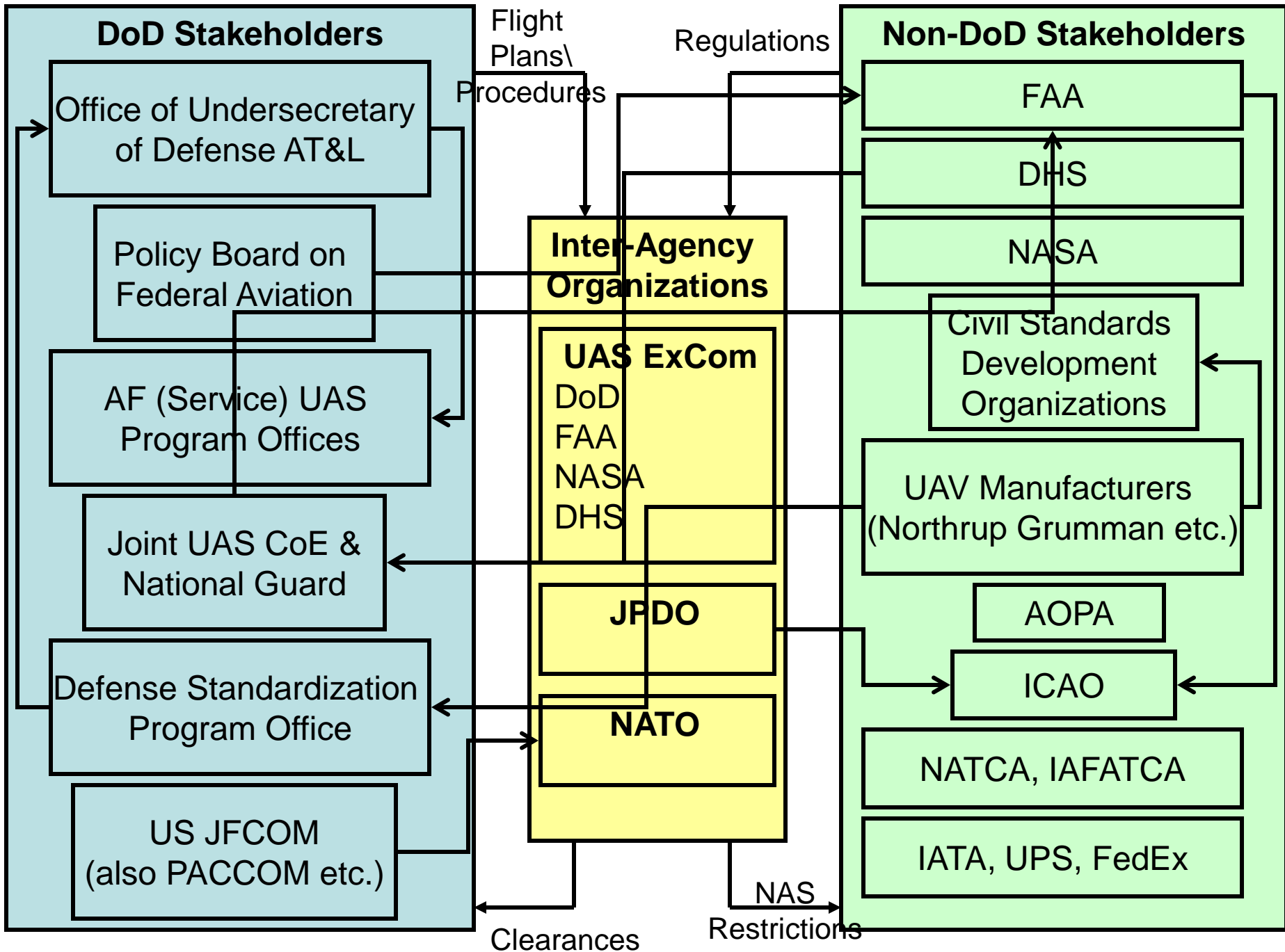
---

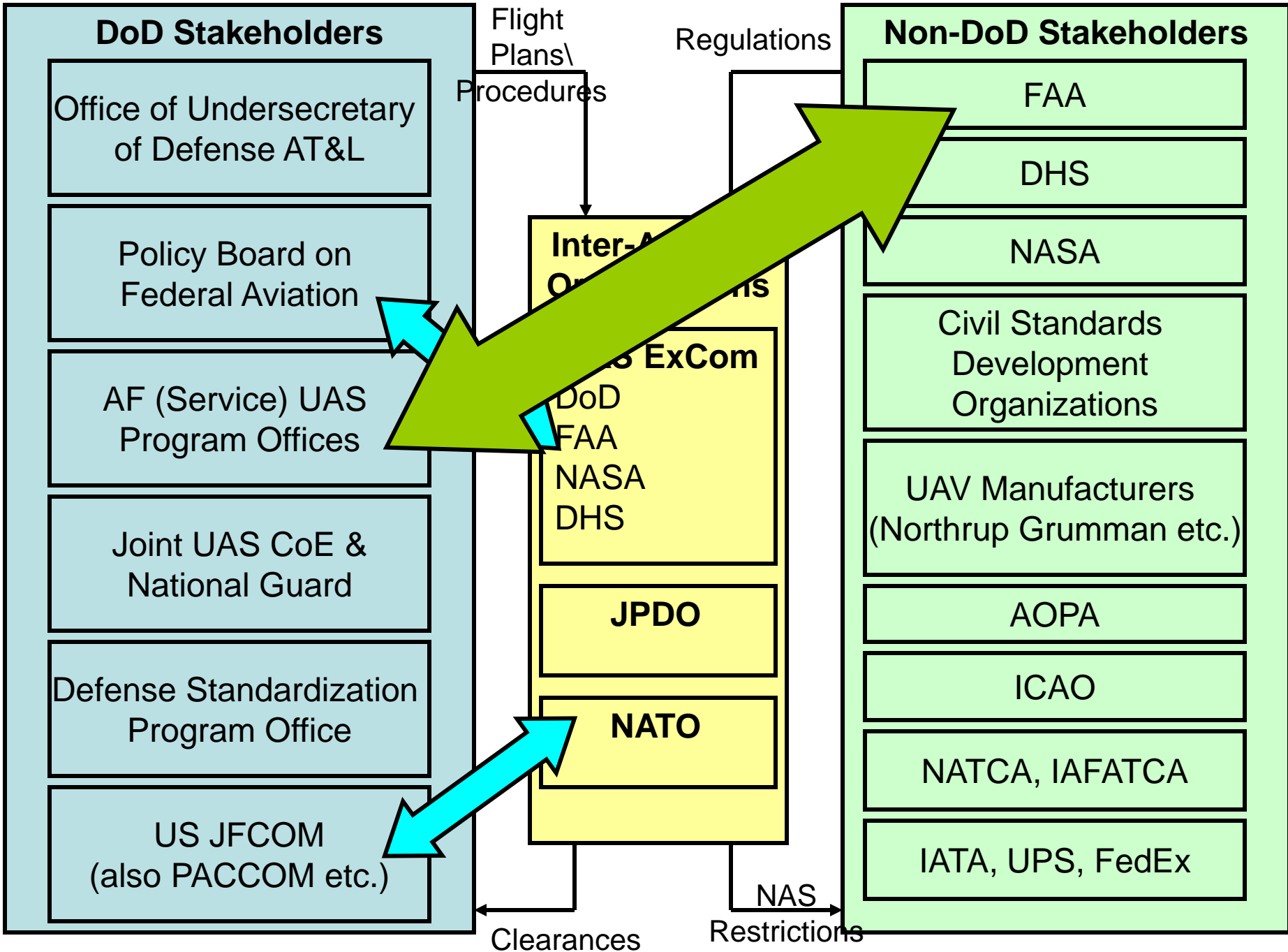
- Pilot and crew actions pre-programmed
  - Mission planning process begins 270 days a priori
  - Mission planners become actively involved 90 days prior to flight
  - Takes 3-5 weeks to write a flight plan
  - Validation takes 10 days, starts 18 days a priori to flight
- Aircraft suffered from inflight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

# Accident and Hazard

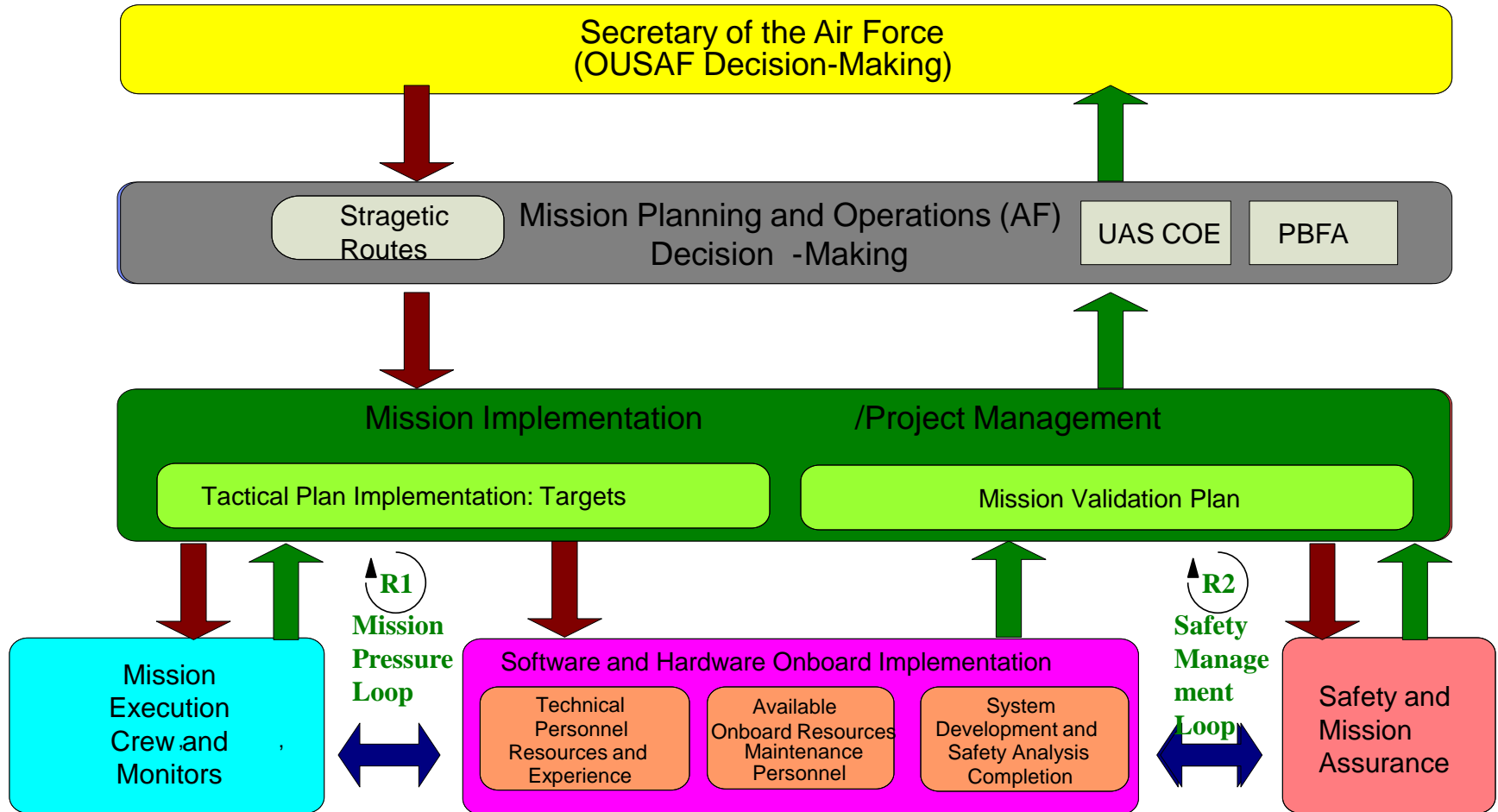
---

- 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.



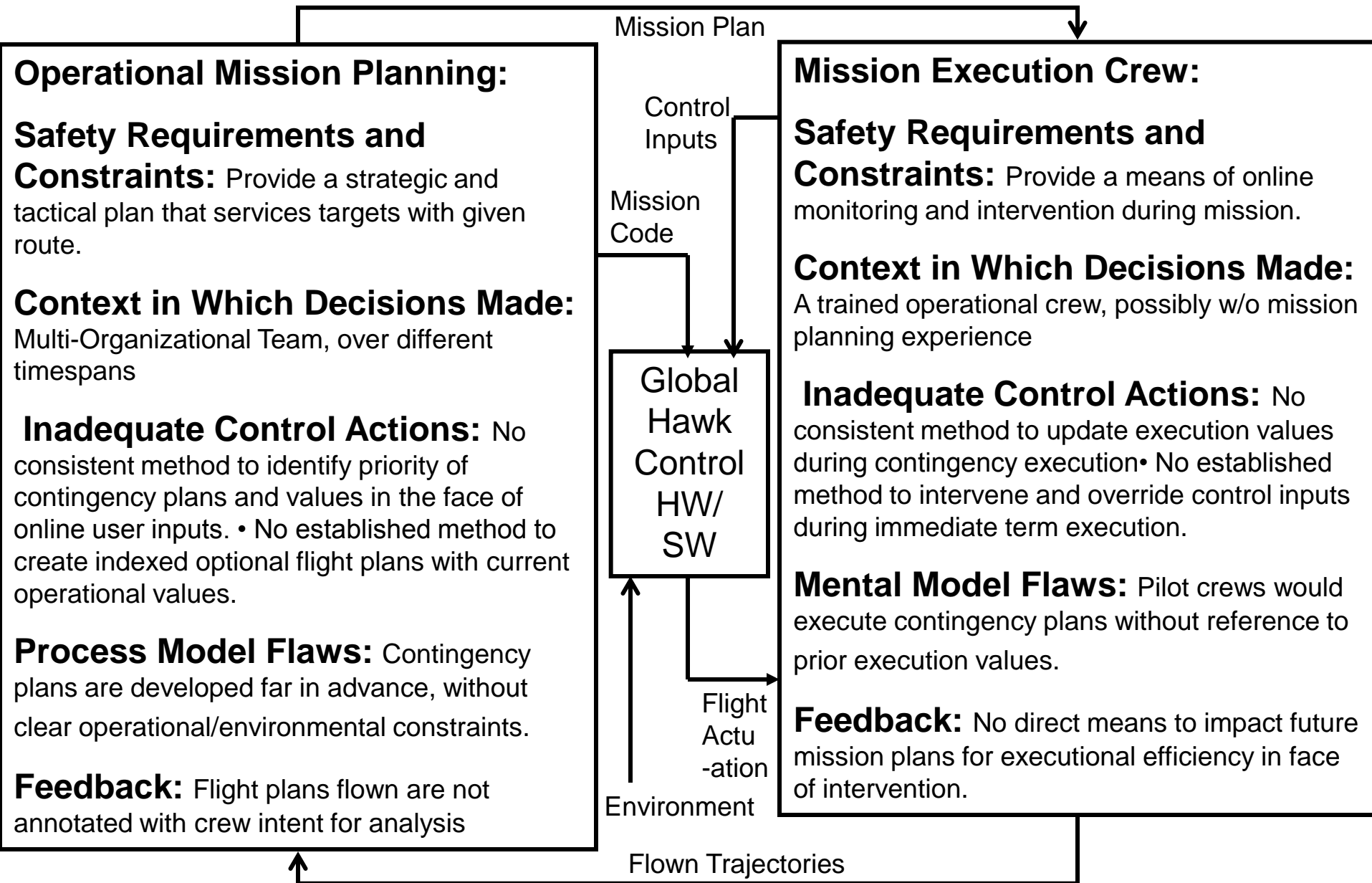


# Mission Planning System Dynamics





# Detailed Control Structure



# 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


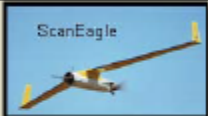


# Overview

---

- 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)

DoD UAS Groups

UAS Groups	Maximum Weight (lbs) (MGTOU)	Normal Operating Altitude (ft)	Speed (kts)	Representative UAS
Group 1	0 – 20	<1200 AGL	100	Raven (RQ-11), WASP 
Group 2	21 – 55	<3500 AGL	< 250	ScanEagle 
Group 3	< 1320	< FL 180		Shadow (RQ-7B), Tier II / STUAS 
Group 4	>1320		> FL 180	Any Airspeed
Group 5		Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N) 		

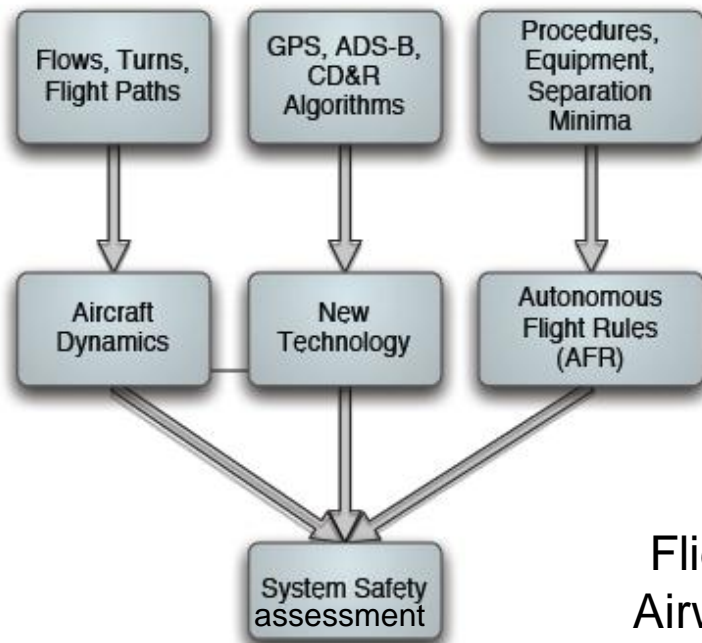
What about:

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

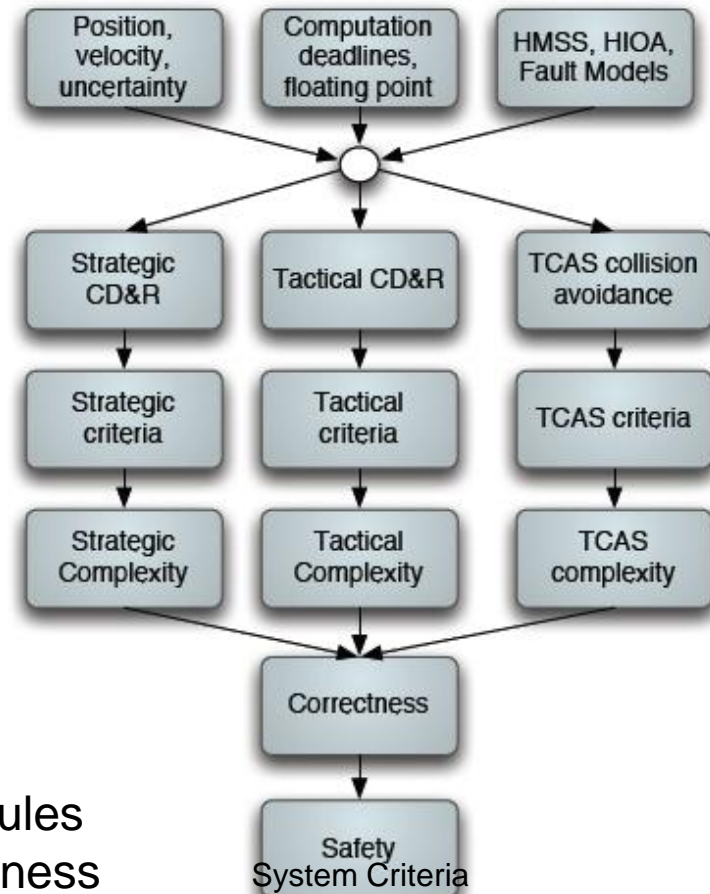
Understand assumptions, rationale, implications to enable cross-comparison

# 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



# 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](mailto:Natasha.Neogi@nianet.org)

