STPA Applied to SUAS use at Edwards AFB

Sarah Summers, Sarah Folse

Overview

- System Introduction
- Control Structure
- Accidents and Hazards
- Step 1 – Unsafe Control Actions
- Step 2 – Scenarios
- Key Safety Factors and Conclusion

System Introduction

Small Unmanned Aerial Systems

UAS Group	Maximum Takeoff Weight (lbs)	Nominal Operating Altitude (ft)	Speed (kn)
Group 1	0-20	< 1,200 AGL	100
Group 2	21-55	< 3,500 AGL	< 250
Group 3	56-1,320	< FL 180	
Group 4	> 1,320	< FL 180	Any Airspeed
Group 5		> FL 180	

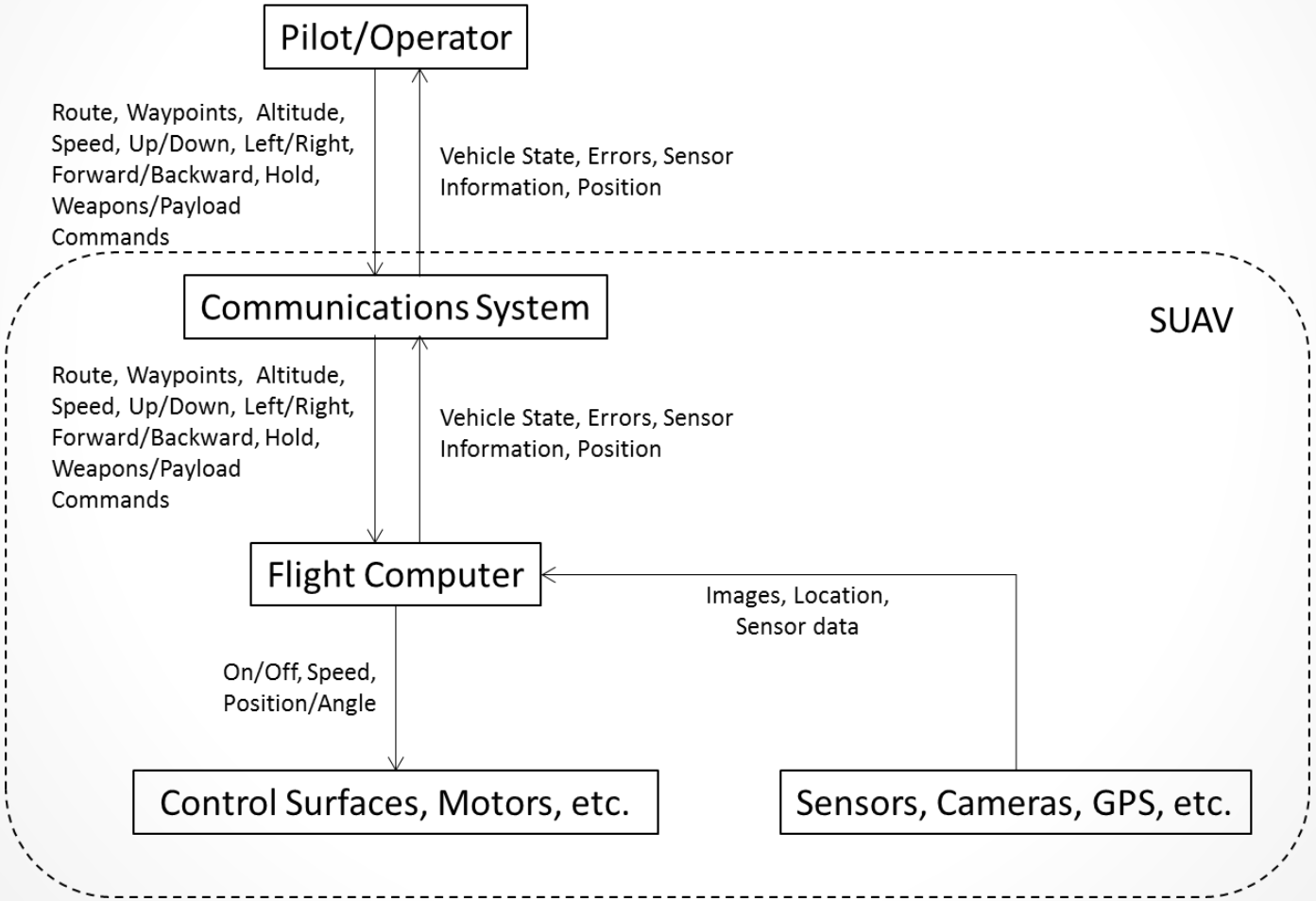
- Air Force Test Center: Emerging Technologies Combined Test Force
  - Focused on small UAV technologies & autonomy
- NASA & Air Force Research Laboratory Traveler UAV
  - To "prove" safe autonomous UAV operation
  - Supports FAA effort to define standards for autonomous UAV certification

Small Unmanned Aerial Systems

UAS Group	Maximum Takeoff Weight (lbs)	Nominal Operating Altitude (ft)	Speed (kn)
Group 1	0-20	< 1,200 AGL	100
Group 2	21-55	< 3,500 AGL	< 250
Group 3	56-1,320	< FL 180	

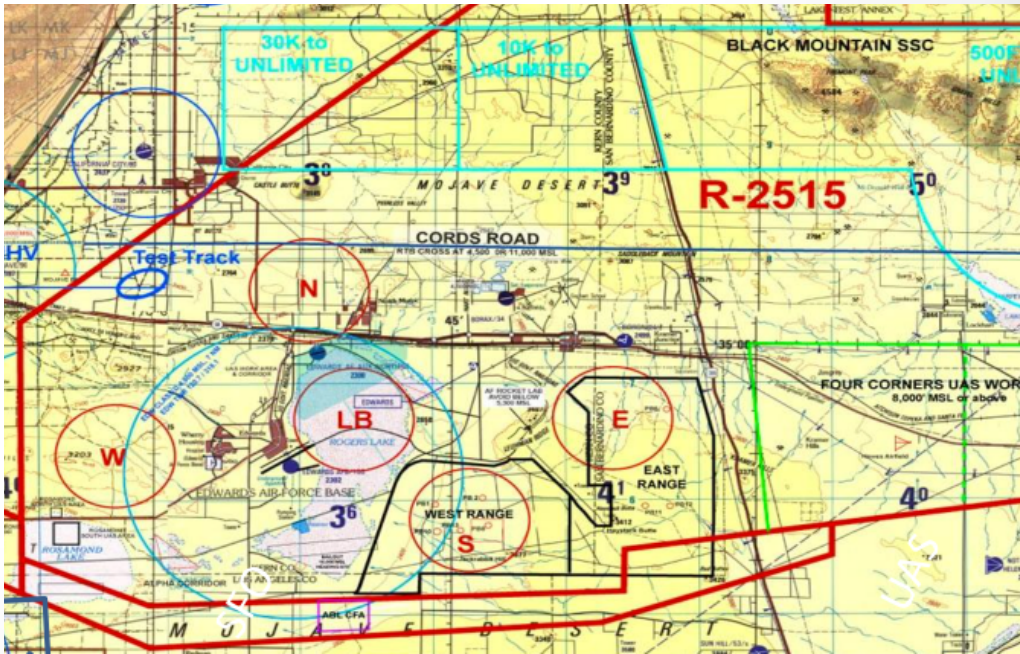
Non-Military

SUAS Safety Control Structure

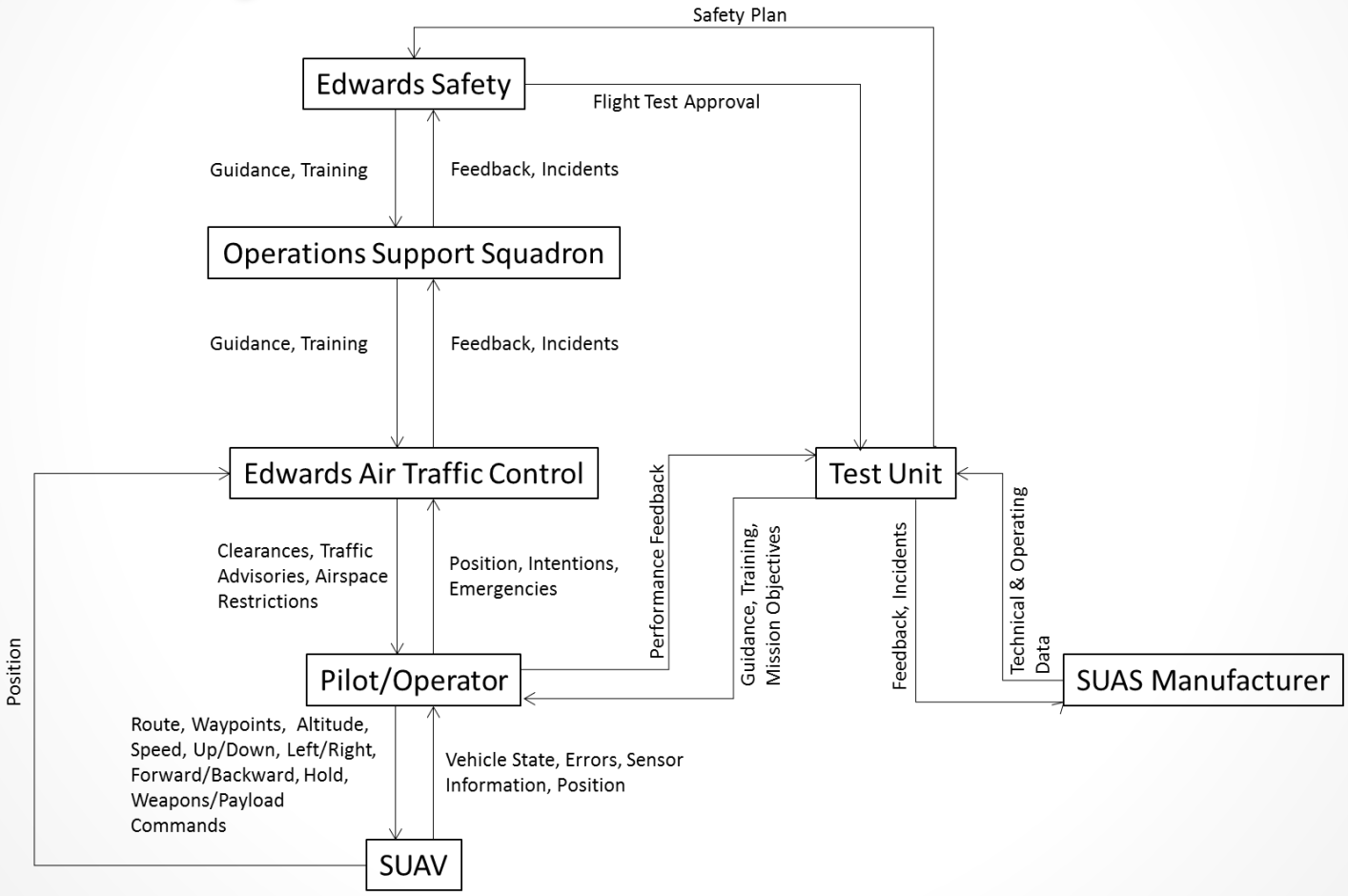


Edwards AFB

- Air Force Test Center
  - Manned, Unmanned DOD Aircraft in various stages of development
  - Personnel Drop Zones for Parachute Testing
  - Munitions, Airdrop, Sensor Testing
- NASA Armstrong Flight Research Center
  - Manned, Unmanned Aircraft in various stages of development
- Air Force Rocket Research Laboratory
  - Outdoor Rocket Testing
- Other Uses
  - Civil Aviation
  - RC Hobbyists
  - Small Arms Range



Edwards AFB (Simplified) Safety Control Structure



Accident and Hazard Definition

Accidents

A1. Aircraft (including both manned and unmanned systems) in the air are damaged or destroyed.

A2. Personnel on the ground are injured or killed.

A3. Structures on the ground are damaged or destroyed.

A4. Testing or flight operations are unable to be conducted.

Hazards – Air to Air

A1. *Aircraft (including both manned and unmanned systems) in the air are damaged or destroyed.*

H1. Collision of a manned and unmanned aircraft. [A1]

H2. Collision of two unmanned aircraft. [A1]

H3. Debris from an aircraft impacts another aircraft. [A1]

H4. Unmanned aircraft loses controlled flight capability. [A1]

Hazards – Air to Ground

A2. *Personnel on the ground are injured or killed.*

A3. *Structures on the ground are damaged or destroyed.*

H5. Collision of an unmanned aircraft with a person on the ground. [A2]

H6. Debris from an unmanned aircraft strikes a person on the ground. [A2]

H7. Collision of an unmanned aircraft with a structure on the ground. [A3]

H8. Debris from an unmanned aircraft strikes a structure on the ground. [A3]

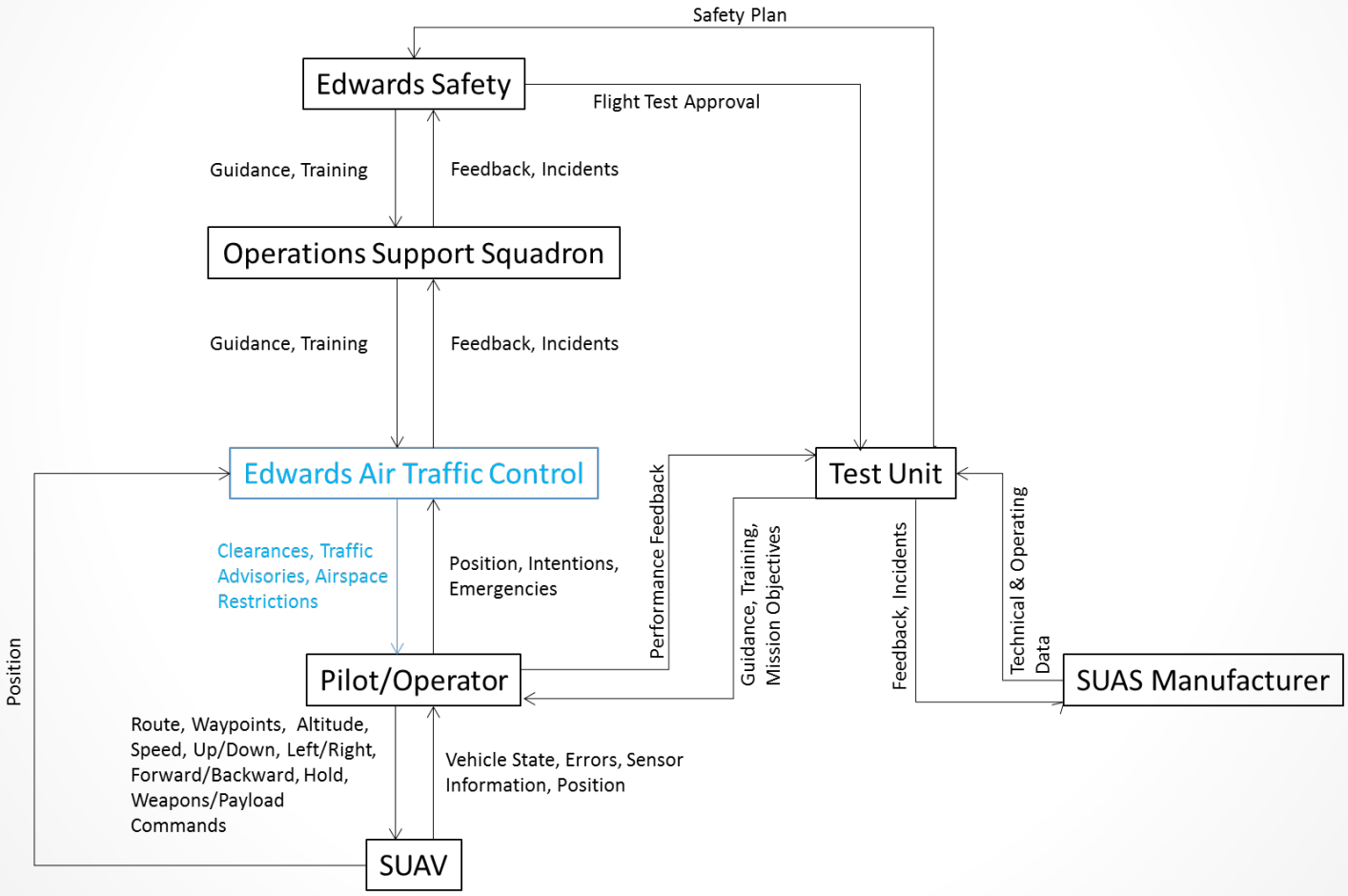
Hazards - Efficiency

A4. *Testing or flight operations are unable to be conducted.*

H9. Unmanned aircraft testing unnecessarily interferes with flight operations. [A4]

Step 1 Analysis: Unsafe Control Actions

UCAs for the Air Traffic Controller

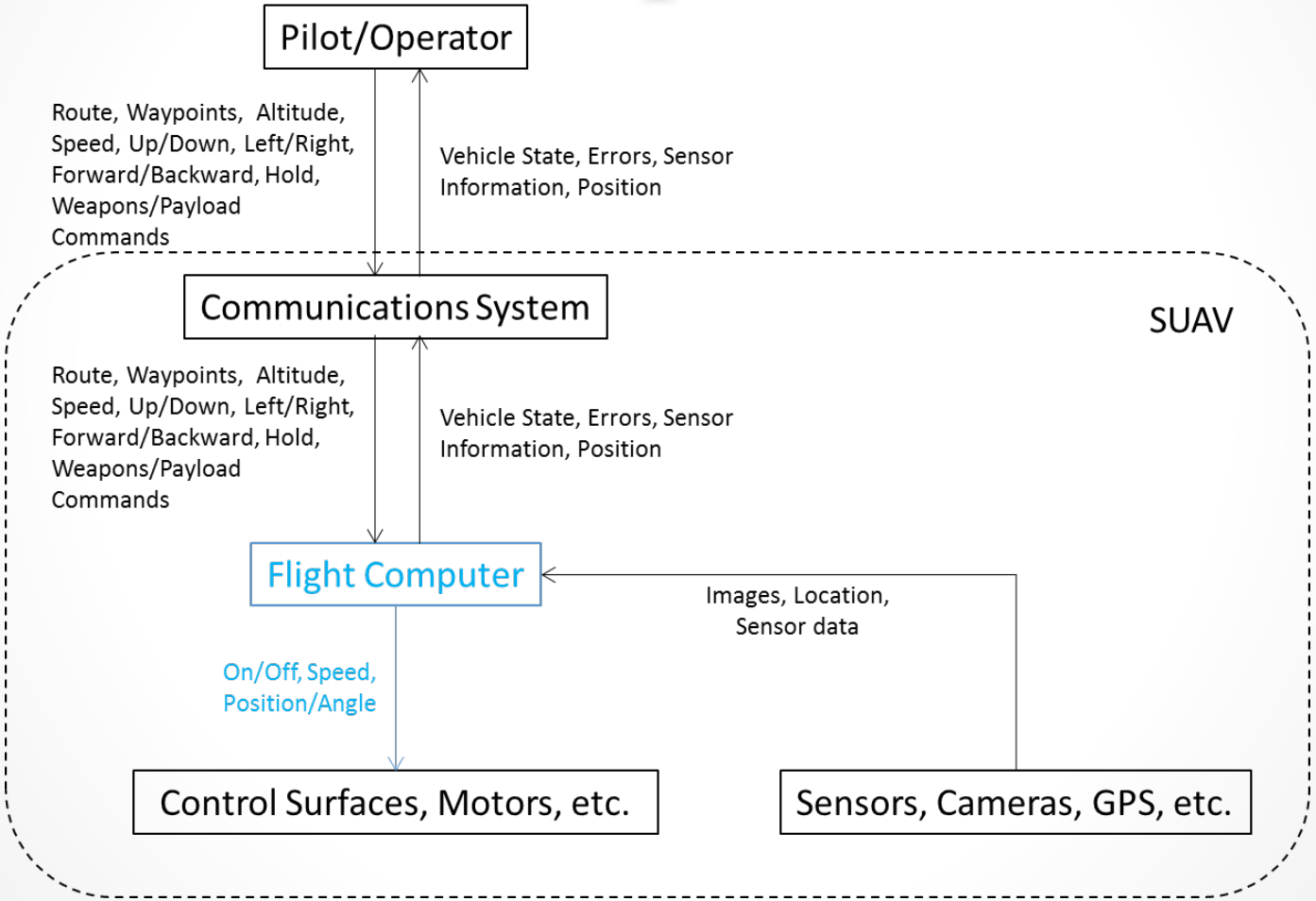


UCAs for the Air Traffic Controller

Control Action / UCA	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Takeoff Clearance	…when it is clear of safe to takeoff [H9].	…while another aircraft is in the way [H1, H2]. …while personnel in the area [H5].	…before landing aircraft clears the runway [H1, H2]. …before personnel are clear [H5].	Provided & not rescinded when conditions are no longer safe to takeoff [H1, H2, H5].
Landing Clearance	…when the aircraft is low on fuel [H4].	…while another aircraft is on the runway [H1, H2]. …while personnel in the area [H5].	…before landing aircraft clears the runway [H1, H2]. …before personnel are clear [H5].	Provided & not rescinded when conditions are no longer safe to land [H1, H2, H5].
Airspace Clearance	…when airspace is clear/safe [H9].	…when airspace is not clear/safe [H1, H2].	No Hazard	Provided & not rescinded when the airspace is no longer safe [H1, H2].
Traffic Advisories	…when another aircraft is nearby/moving towards the SUAS [H1, H2].	…when an aircraft is not in the vicinity & causes testing to stop [H9]	…provides too late for corrective action [H1, H2].	Provided & not rescinded when encroaching aircraft is no longer a factor [H9].
Airspace Restrictions	…when the airspace is unsafe [H1, H2, H7].	…when the airspace is clear/safe/unrestricted [H9].	No Hazard	…not rescinded when restriction is no longer valid [H9].

H1. Collision of a manned and unmanned aircraft.
H2. Collision of two unmanned aircraft.
H4. Unmanned aircraft loses controlled flight capability.
H5. Collision of an unmanned aircraft with a person on the ground.
H9. Unmanned aircraft testing unnecessarily interferes with flight operations. [A4]

UCAs for the SUAS Flight Computer



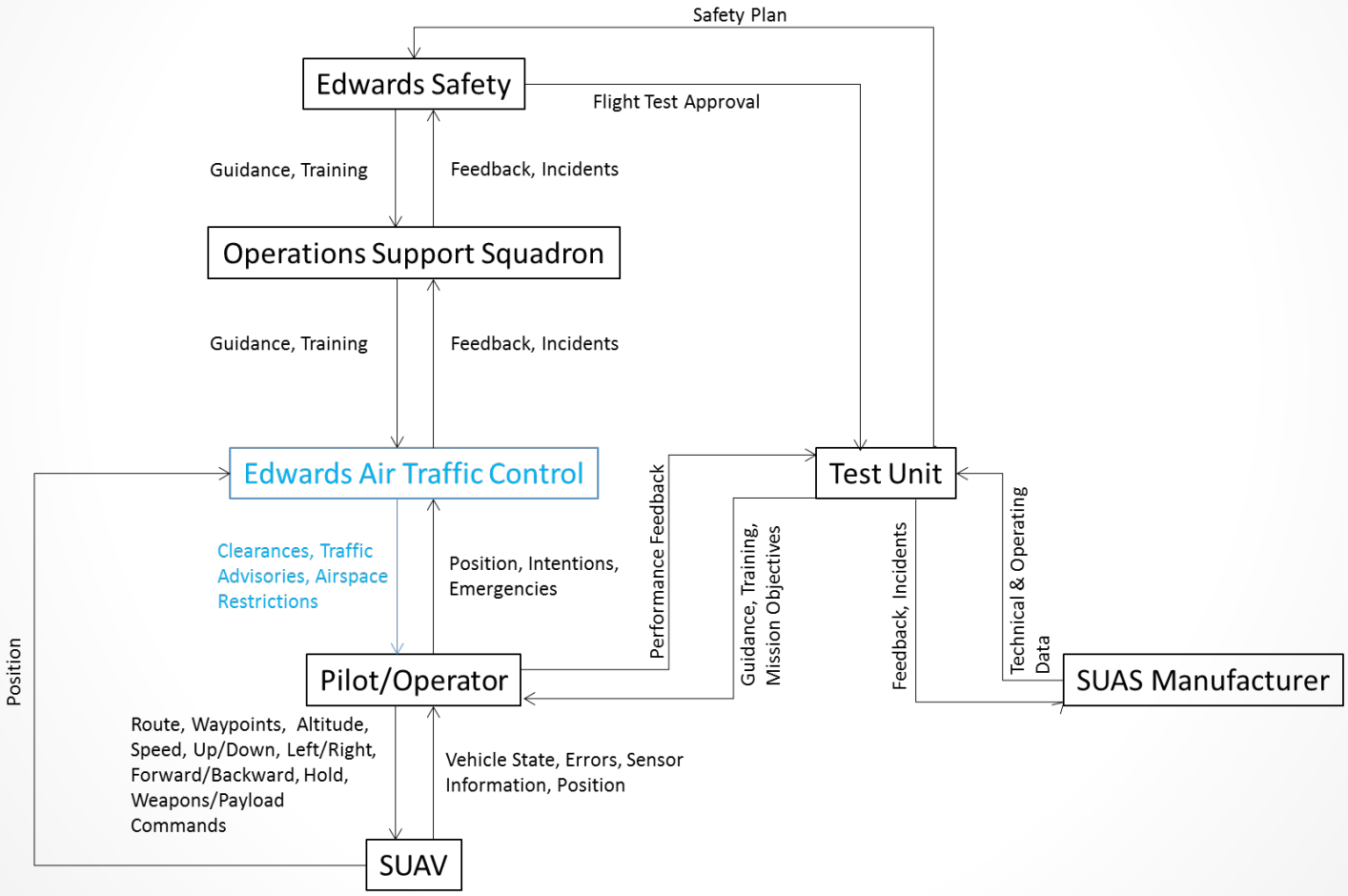
UCAs for the SUAS Flight Computer

Control Action / UCA	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Control Surface Servo Command	…when SUAS needs to maneuver [H4].	…when SUAS should not maneuver [H4].	…in incorrect order with other control commands [H4].	…stopped before aircraft reaches correct attitude [H4]. …continues after correct attitude attained [H4].
Throttle Increase Command	…when SUAS needs to accelerate [H4].	…when aircraft needs to decelerate or maintain airspeed [H4].	…in incorrect order with other control commands [H4].	…stopped before aircraft reaches correct airspeed [H4]. …continues after correct airspeed attained [H4].
Throttle Decrease Command	…when SUAS needs to decelerate [H4].	…when aircraft needs to accelerate or maintain airspeed [H4].	…in incorrect order with other control commands [H4].	…stopped before aircraft reaches correct airspeed [H4]. …continues after correct airspeed attained [H4].

H4. Unmanned aircraft loses controlled flight capability.

Step 2 Analysis: Scenarios

UCAs for the Air Traffic Controller



UCAs for the Air Traffic Controller

Control Action / UCA	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Takeoff Clearance	…when it is clear of safe to takeoff [H9].	…while another aircraft is in the way [H1, H2]. …while personnel in the area [H5].	…before landing aircraft clears the runway [H1, H2]. …before personnel are clear [H5].	Provided & not rescinded when conditions are no longer safe to takeoff [H1, H2, H5].
Landing Clearance	…when the aircraft is low on fuel [H4].	…while another aircraft is on the runway [H1, H2]. …while personnel in the area [H5].	…before landing aircraft clears the runway [H1, H2]. …before personnel are clear [H5].	Provided & not rescinded when conditions are no longer safe to land [H1, H2, H5].
Airspace Clearance	…when airspace is clear/safe [H9].	…when airspace is not clear/safe [H1, H2].	No Hazard	Provided & not rescinded when the airspace is no longer safe [H1, H2].
Traffic Advisories	…when another aircraft is nearby/moving towards the SUAS [H1, H2].	…when an aircraft is not in the vicinity & causes testing to stop [H9]	…provides too late for corrective action [H1, H2].	Provided & not rescinded when encroaching aircraft is no longer a factor [H9].
Airspace Restrictions	…when the airspace is unsafe [H1, H2, H7].	…when the airspace is clear/safe/unrestricted [H9].	No Hazard	…not rescinded when restriction is no longer valid [H9].

Unsafe Action Applied

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if **another aircraft is in the airspace without informing ATC** and **does not show up on ATC radar control system**. May be due to…	Aircraft is designed to minimize radar return and is not broadcasting Mode C/ADS-B/IFF
	ATC radar control system is inoperative and the aircraft does not appear on the controller's displays.
	Terrain masking due to location and altitude in comparison to the radar coverage.
	ATC communications are busy, and the controller missed a call **requesting access to the airspace**.
	ATC communication system is inoperative.
	The aircraft is experiencing some problem with communication (outside system scope)
	Spin zones are in use, but the aircraft did not inform ATC they had begun their maneuver.

Unsafe Action Applied

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if an **aircraft that was in the airspace hasn't left yet after informing ATC** and **does not show up on ATC radar control system**. May be due to…

Aircraft is designed to minimize radar return and is not broadcasting Mode C/ADS-B/IFF.
ATC radar control system is inoperative and the aircraft does not appear on the controller's displays.
Terrain masking due to location and altitude in comparison to the radar coverage.
ATC communications are busy, and the controller missed a call requesting an extension in the airspace.
ATC communication system is inoperative.
The aircraft is experiencing some problem with communication (outside system scope)
Aircraft announced they were descending/ascending, but delayed without notifying ATC.

Unsafe Action Applied

<table>
<tr><td rowspan="2">ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if ATC thought that UAV was entering a different airspace and gave them a clearance for that airspace, which may be due to…</td><td>Communications between the pilot and ATC are unclear</td></tr>
<tr><td>UAV is too small to be visible on radar & not broadcasting Mode C/ADS-B/IFF</td></tr>
</table>

Unsafe Action Applied

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if	**The AFRL Rocket Test Facility did not properly notify ATC regarding a rocket test.**
ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if	**The small arms range is active, but did not notify ATC.**

Unsafe Results

<table>
<tr><td rowspan="4">ATC gives an airspace clearance but the UAV doesn't enter airspace (hand-off between controllers happens, so ATC assumes UAV is in new airspace). This could happen because…</td><td rowspan="3">Communication from ATC not received by pilot, so pilot is unaware to enter the airspace. This can be due to</td><td>ATC and UAV pilot transmitting on different frequencies</td></tr>
<tr><td>ATC or UAV communications equipment inoperative</td></tr>
<tr><td>The airspace clearance transmission was "stepped on" by another transmission</td></tr>
<tr><td colspan="2">The UAV itself is incapable of entering the airspace</td></tr>
<tr><td colspan="2">The UAV pilot receives conflicting clearance from another air traffic controller, which he/she follows</td></tr>
</table>

Unsafe Results

<table>
<tr><td rowspan="4">ATC gives an airspace clearance, but the UAV goes outside of this boundary. This could happen because…</td><td rowspan="3">UAV Pilot believes that the vehicle is still within the boundary because…</td><td colspan="2">The boundary is unclear, due to map updates, etc.</td></tr>
<tr><td rowspan="2">The position of the UAV is unclear</td><td>Poor sensor feedback from vehicle to operator</td></tr>
<tr><td>No sensor feedback from vehicle to operator</td></tr>
<tr><td colspan="3">UAV malfunctions and pilot is incapable of keeping the vehicle in the airspace</td></tr>
</table>

Requirements from Step 2 Analysis

- Aircraft shall not enter a controlled airspace without broadcasting their location through Mode C, ADS-B, or IFF.
- Aircraft shall not enter a controlled airspace without verbal confirmation from the controller.
- In areas where terrain masking may occur, the controller shall maintain awareness of aircraft that have requested access to the airspace.
- When spin zones are in use, the controller shall not consider the area clear or safe.
- Controllers shall not approve requests for access to zones other than those that they are controlling.
- Controllers shall confirm that an aircraft has exited the zone via both voice communications and radar confirmation.
- Controllers shall monitor radar returns of aircraft that are ascending/descending to ensure minimum separation requirements.

Requirements from Step 2 Analysis

- Controllers shall confirm that there are no rocket tests ongoing.
- Controllers shall confirm that the small arms range is inactive.
- UAS operator shall read back airspace clearance to controller.
- UAS operator shall immediately notify the losing controller if the UAV is incapable of exiting the old airspace.
- **Wing safety shall ensure that the UAV software is updated with new airspace boundaries when they are changed.**
- **UAS operator shall immediately inform the controller if the UAV position becomes unclear.**
- **UAS operator shall immediately inform the controller in the event of a UAV malfunction.**
- **UAS operations shall, when possible, be conducted well away from the boundaries of the airspace.**

Recommendations and Conclusion

Key Safety Factors

- ATC knowledge of the SUAV location
- Communication between the SUAS operator and ATC
- Communication between ATC and other people in the airspace
- SUAS process model for autonomous operations

Questions?

Backup Slides

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if another **aircraft is in the airspace without informing ATC** and **does not show up on ATC radar control system**. May be due to…

- Aircraft is designed to minimize radar return and is not broadcasting Mode C/ADS-B/IFF
- ATC radar control system is inoperative and the aircraft does not appear on the controller's displays.
- Terrain masking due to location and altitude in comparison to the radar coverage.

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if **another aircraft is in the airspace without informing ATC** and **does not show up on ATC radar control system**. May be due to…

- ATC communications are busy, and the controller missed a call requesting access to the airspace.
- ATC communication system is inoperative.
- The aircraft is experiencing some problem with communication (outside of the scope of this system)

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if **another aircraft is in the airspace without informing ATC** and **does not show up on ATC radar control system**. May be due to…

- Spin zones are in use, but the aircraft did not inform ATC they had begun their maneuver.
- A controller from a different zone approved the airspace request and did not inform the controller controlling the zone.

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if an **aircraft that was in the airspace hasn't left yet after informing ATC** and **does not show up on ATC radar control system**. May be due to…

- Aircraft is designed to minimize radar return and is not broadcasting Mode C/ADS-B/IFF.
- ATC radar control system is inoperative and the aircraft does not appear on the controller's displays.
- Terrain masking due to location and altitude in comparison to the radar coverage.

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if an **aircraft that was in the airspace hasn't left yet after informing ATC** and **does not show up on ATC radar control system**. May be due to…

- ATC communications are busy, and the controller missed a call **requesting an extension in the airspace.**
- ATC communication system is inoperative.
- The aircraft is experiencing some problem with communication (outside of the scope of this system).

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if an **aircraft that was in the airspace hasn't left yet after informing ATC** and **does not show up on ATC radar control system**. May be due to…

- Aircraft announced they were descending/ascending, but delayed without notifying ATC.

Unsafe Action Applied

UCA: *"ATC provides airspace clearance when airspace is not clear/safe [H1, H2]."*

ATC believes that the airspace is clear/safe (Process Model Flaw), which could happen if ATC thought that UAV was entering a different airspace and gave them a clearance for that airspace, which may be due to…

- Communications between the pilot and ATC are unclear
- UAV is too small to be visible on radar & not broadcasting Mode C/ADS-B/IFF

Unsafe Results

ATC provides proper airspace clearance, but unsafe actions result.

ATC gives an airspace clearance but the UAV doesn't enter airspace (hand-off between controllers happens, so ATC assumes UAV is in new airspace). Communication from ATC not received by pilot, so pilot is unaware to enter the airspace. This can be due to

- ATC and UAV pilot transmitting on different frequencies
- ATC or UAV communications equipment inoperative
- The airspace clearance transmission was "stepped on" by another transmission

Unsafe Results

ATC provides proper airspace clearance, but unsafe actions result.

ATC gives an airspace clearance but the UAV doesn't enter airspace (hand-off between controllers happens, so ATC assumes UAV is in new airspace). This can also be due to

- The UAV itself is incapable of entering the airspace
- The UAV pilot receives conflicting clearance from another air traffic controller, which he/she follows

Unsafe Results

ATC provides proper airspace clearance, but unsafe actions result.

ATC gives an airspace clearance but the UAV doesn't enter airspace (hand-off between controllers happens, so ATC assumes UAV is in new airspace). This can also be due to

- The UAV itself is incapable of entering the airspace
- The UAV pilot receives conflicting clearance from another air traffic controller, which he/she follows

Unsafe Results

ATC provides proper airspace clearance, but unsafe actions result.

ATC gives an airspace clearance, but the UAV goes outside of this boundary. This may happen if the UAV Pilot believes that the vehicle is still within the boundary because…

- The boundary is unclear, due to map updates, etc.
- The position of the UAV is unclear
  - Poor sensor feedback from vehicle to operator
  - No sensor feedback from vehicle to operator

Unsafe Results

ATC provides proper airspace clearance, but unsafe actions result.

ATC gives an airspace clearance but the UAV doesn't enter airspace (hand-off between controllers happens, so ATC assumes UAV is in new airspace). Communication from ATC not received by pilot, so pilot is unaware to enter the airspace. This can be due to

- ATC and UAV pilot transmitting on different frequencies
- ATC or UAV communications equipment inoperative
- The airspace clearance transmission was "stepped on" by another transmission

Unsafe Results

ATC provides proper airspace clearance, but unsafe actions result.

ATC gives an airspace clearance, but the UAV goes outside of this boundary. This may happen if the UAV Pilot believes that the vehicle is still within the boundary because…

- UAV malfunctions and pilot is incapable of keeping the vehicle in the airspace