RANGE SAFETY REVIEW QUESTIONS
FOR UNMANNED AIRCRAFT SYSTEMS (UAS)
Camp Roberts Ca, CIRPAS McMillan AF
Version 1, Sept 2010

1. INTRODUCTION TO REVIEW QUESTIONS

Range Safety is tasked to identify potential hazards on the range and ensure safeguards are put in place to reduce risk to an acceptable level, consistent with existing local policy guidance. If the operational risks of a specific program exceed specified levels even after implementation of reasonable safeguards, a waiver decision is required from the local Range Safety Officer.

The document will help ensure the local range Officer is fully advised and informed of all known risks. It also serves as a consistent approach to UAS program range safety reviews.

This document is focused on hazards that may result in the following consequences:

- UAS crashes which may result in death or injury, or damage to property.
- Failures that result in a fly-away condition of the UAS, resulting in the UAS leaving its assigned test area, or the Restricted Airspace R2504.
- Mid-air collision between UAS and manned aircraft causing death or injury to pilot, or damage to manned aircraft.

Each section provides questions, based on past experience and lessons learned from other programs.

Successful completion of this review process will result in confidence that:

- Key system vulnerabilities have been identified
- Safeguards have been verified to exist for these system vulnerabilities
- Safeguards are adequate, and
- Deficiencies or inadequacies of the proposed safeguards have been recognized

Note: Information is entered into the GREY colored boxes on the following pages.

1.2 <u>Control Measures and Risk Decisions.</u> *Control measures to reduce risks to an acceptable level are identified.*

Risks that are unacceptable in terms of severity and/or probability need to be controlled. The user must help identify specific strategies, tools, or safeguards to eliminate or reduce the risk to a level acceptable to the range.

According to MIL-STD-882, the desired order of precedence for implementing control measures is as follows:

- Design for minimum risk. Eliminate the hazard.
- Incorporate safety devices.
- Provide warning devices.
- Develop procedures and training.

1.2.1 <u>Design for Minimum Risk.</u>

The best way to control a hazard is to eliminate it by changing the design or adjusting the test and/or training requirements. If the hazard cannot be eliminated, design changes may reduce the risk to an acceptable level. Some examples of design or requirement changes, which may eliminate or reduce risk include:

- Including a highly reliable engine in the UAV design reduces the risk of loss of propulsion.
- Designing a series of tests with a gradual buildup in risk reduces the chance of sudden unexpected catastrophic failure.
- Confining test flights to an unpopulated area eliminates risk to people on the ground.
- Designing a low-level route that avoids populated areas reduces risk of ground casualties from system failures.
- Establishing policy to avoid icing conditions if the vehicle would be at risk in such conditions reduces the risk of icing induced loss of lift or loss of propulsion.

1.2.2 <u>Incorporate Safety Devices.</u>

If the hazard can not be eliminated through design change, fixed or automatic safety devices should be incorporated. Provisions for periodic functional checks for these safety devices should be instituted. Examples of safety devices include:

- Back-up battery in case of generator failure
- Redundant communications link in case of failure of the primary link
- Software “fly-home” routine in case of lost link
- Independent flight termination systems

1.2.3 <u>Provide Warning Devices.</u>

If the risk cannot be reduced adequately through design change or use of safety devices, warning devices that detect the hazardous condition and alert personnel of the hazard can be used. Procedures for functional checks of these warning devices should be incorporated. Examples of warning devices are:

- Engine performance safety data displays at the ground control station (i.e., overtemp alert)
- Strobe lights to make the UAV easier to see
- "Low fuel" warning lights
- Warning calls from air traffic control when the vehicle is approaching other traffic or hazard/flight boundaries

1.2.4 **Develop Procedures and Training.**

If it is impractical to eliminate hazards or reduce risk adequately through design changes or safety and warning devices, procedures and training can be used. Safety-critical procedures should be standardized and documented. Tasks and activities that are safety-critical may require certification of personnel proficiency. Examples of safety-related procedures and training include:

- Pre-flight checklists
- Published cautions and warnings
- Emergency procedures
- Specific operating limits
- Established operator qualification procedures
- Requirements for personal protective equipment in specific situations (i.e., hearing protection).

Note: Procedures and training should not be used as the only risk reduction methods for high risk hazards.

1.3 Hazard Controls. *Control measures used in the hazard analysis are incorporated into range users test plan or procedure document.*

The range user must show that identified control measures are incorporated, understood, and documented. If required, test procedures and monitoring of the control measures must be certified and in place. If the control measures are not implemented, or the implementation is not effective or sufficient, the hazard is still present. If hazards still exist after all control measures are in place, the first step is to re-evaluate the hazard and control measures and verify that nothing was missed and no other solutions are available. Once this process has been established, documentation of all hazards, their respective control measures, and any remaining risks and recommendations must be presented to the appropriate level of authority for a wavier. The deciding authority will consider the benefits versus the risks to decide whether a waiver will be granted.

1.4 Supervision. *Follow-up evaluations of the control measures are planned in order to ensure effectiveness. Adjustments will be made before continuing with the test or operation.*

Independent review and approval of the documentation, hazard analysis, hazard controls, and test procedures and monitoring must take place prior to the test or operation. This monitoring of safety limits must take place on a continuing basis for each test and/or operation.

1.5 <u>Alternatives If the Risk Management Criteria Are Not Met.</u> *If normal risk management criteria are not met, the following alternatives may be exercised.*

- Range may re-evaluate the hazard analysis incorporating changes such as flight parameters, flight path, and new information from the user.
- Range may impose restriction to planned flight to control identified risk.
- Range may require additional control measures or safeguards to control identified risk.
- User can request a waiver from the Range Commander.
- User may not get permission to fly on this range.

NOTE

Other than in UAS Background Information section (2.0), please avoid describing programmable capabilities of the system without defining how that capability will be implemented. Any "if, can, may, or programmed to" statement should be followed with a description of how that function will be programmed.

For example, DO NOT state "The Sputnik MK2 autopilot is capable of flying to any programmed waypoint in case of lost link, where it can hold for a programmed amount of time after which it can be programmed to autoland at a predetermined location if desired."

Without adding something like this-

"For Camp Roberts operations, the Sputnik MK2 autopilot will be programmed to fly to the lost link point assigned by the CIRPAS Range Safety Officer where it will hold for 10 minutes in an attempt to regain local control. After 10 minutes it will fly to Lost link zone (or other assigned area) and attempt an autoland."

2.0 Vehicle <u>Performance.</u>

Please provide the following information on the UAS: (attach additional documents as necessary)

- Performance charts
- Max altitude
- Max endurance
- Max range
- Range vs. altitude (glide)
- Cruise speed
- Max speed
- Rate of climb, rate of descent
- Wind limits (all) for launch and recovery operations

2.1 Vehicle History and Reliability Data

A flight clearance is typically required for flight operations in the R2504 airspace. For DOD owned systems, a DOD issued flight clearance (or Safety of Flight (SOF) or Interim Flight Clearance (IFC)) is required. For non-DOD systems, a flight clearance issued by the aircraft manufacturer, or other competent authority is required-Or a Statement of Air worthiness.

1. Does the UAS currently have a flight clearance or FAA issued Certificate of Authorization (COA)? Issued by whom? If so, please provide a copy.

2. Vehicle history: How many flights (# of sorties, flight hours) has the UAS completed to date?

3. Is the UAS currently in use with the uniformed services? If so, provide details.

4. What is the heritage of the UAS (i.e. is it an evolution of another UAS system)?

5. Mishap history: How many crashes and failures have occurred? What has been the corrective action to ensure the failures do not occur again?

3. LOSS OF CONTROLABILITY

Vehicle loss of control can easily result in a mishap. If we can identify any potential causes of "loss of control" that may have been overlooked, safeguards can be applied, or test conditions can be restricted to reduce risk to an acceptable level.

3.1 Loss of Command Links.

1. Fully describe the command and control links, including equipment used, frequency, bandwidth, modulation, power output.

2. What happens when command link is lost? Will it climb to a specific altitude? Orbit? Can it land itself? What is the timing and sequence of events? Is there a time limit?

3. How does vehicle respond if link is never re-established?

4. How does the vehicle recognize that loss of command link has occurred?

5. How does the UAS operator in the ground control station recognize loss of command link has occurred?

6. Are there any identified Single Point or Common Mode failures in the Command and Control Links? If so, how are these mitigated?

7. What is the processing time (i.e. lag time) of the Command and Control links?

3.2 Return Home Modes (NOT lost-link).

1. Some UAS will self-detect a in-flight failure/discrepancy and automatically abort the mission and return. Does this vehicle have an automatic "return home" feature (sometimes also called "reversion mode" or "Preprogrammed Emergency Mission")?

2. What conditions will cause the vehicle to go into "return home" mode?

3. What does the vehicle do once it arrives at the "return home" point? Will it climb to a specific altitude? Orbit? Can it land itself? What is the timing and sequence of events?

3.3 Selection of Lost Link, Return Home (i.e. Emergency) Locations.

1. Can the "emergency" point be any location, or just the takeoff point? How many "emergency" locations can the UAS have?

2. Is the "emergency" point pre-programmed, or can it be updated in flight?

3. Is the UAS required to fly direct to the "emergency" location or can it fly a programmed route (intermediate waypoint(s)) to its assigned location? Are altitude limits defined? What happens if the altitude limits are exceeded?

4. How are the "emergency" positions entered? What safeguards prevent erroneous position input?

3.4 Backup Communications Links.

1. Is there a backup command transmitter and receiver? Is the backup link on the same frequency as the primary?

2. Does the backup transmitter have the same or more "effective radiated power"?

3.5 Link Analysis.

1. Has RF link analysis been performed to verify both primary and backup transmitters can communicate with the vehicle at the furthest point in its planned operation?

2. Does link analysis address all RF links?

- Uplinks from primary and backup ground stations
- Secondary uplinks from each ground station
- Downlinks to primary and backup ground stations
- Flight Termination Link (if equipped)

3. What is the maximum range for each link?

4. How do you determine if the primary and backup transmitters are radiating specified output power?

5. How do you determine if the vehicle primary and backup command and control receivers (and FTS receivers, if equipped) are operating at specified sensitivity?

6. Are there any nulls in the command transmitter antenna pattern? If so, describe.

7. Are there areas of RF masking due to location of antennas on the UAS relative to their position and to ground station antennas?

8. What is the link susceptibility to multipath? What is the system response if multipath is experienced?

3.6 Loss of Vehicle Position Information.

1. Fully describe the navigation system of the UAS, including backup navigation sources if applicable.

2. What are the sources of vehicle navigation position information to the UAS operator?

3. Are there redundant sources so the UAS operator can tell if there is a discrepancy?

4. How with the UAS respond in a denial of GPS environment? What happens if GPS is not recovered? What happens if the GPS stops reporting (locks up) or keeps reporting the same

position information? Does your navigation system take into account GPS Dilution of Precision (DOP) in using GPS data for navigation?

5. If the UAS operator loses primary position information, is control also lost?

6. Does the UAS operator have access to any external sources of position information that could serve as a backup (radar, IFF, binoculars)?

7. How does the vehicle autopilot respond to loss of primary internal navigation source? Is there a backup? What are the indications in the ground station to the UAS operator?

3.7 Loss of Flight Reference Data.

1. Fully describe the inertial flight data system of the UAS, including backup sources if applicable.

2. What are the on-board sources of position, attitude, heading, altitude, and airspeed information to the UAS operator and/or autopilot?

3. How does the vehicle autopilot respond to loss of primary attitude source? Is there a backup? What are the indications to the UAS operator?

4. Is there a DR (dead reckoning) mode if GPS or inertial navigation is unavailable or degraded?

3.8 Unresponsive Flight Controls.

1. What will happen if a servo or flight control sticks or becomes unresponsive? How does the autopilot respond? Is there a backup? How quickly will the UAS operator recognize this?

2. What happens if the throttle is stuck? How will the UAS operator recognize this condition? Is there a recovery procedure?

3.9 Loss of Propulsion.

1. What happens to the vehicle when propulsion stops? Will the UAS immediately depart controlled flight or can it glide for some distance?

2. Will sufficient velocity and electrical power remain for “controlled ditch” or “dead stick landing”?

3. Can the engine be restarted, turned off or turned on in flight?

4. Is the propulsion system affected by environmental conditions (temperature, icing, dust, etc.)? What are the limits? Are the limits and failure modes confirmed by test data? Are limits considered in test plan?

5. How is fuel volume (or battery charge) and utilization monitored during flight?

3.10 Loss of Electrical Power.

1. What happens when primary electrical power is lost?

2. Is there a separate battery bus? What does battery bus power? Does automatic system load shedding occur if power is reduced? Are there "essential busses" for reduced power operations?

3. Are all flight essential systems on an essential bus?

4. Is there a battery power available time limit associated with loss of electrical power? How long?

5. If equipped with a backup battery, how is it checked prior to takeoff?

6. Safety backup system battery lifetime is a critical issue. How do you know how much emergency battery power is left? Is battery usage data available on telemetry? Is a battery use log kept?

3.11 Ground Control Station.

1. What is the source of electrical power for the ground control station? Is there an un-interruptable backup power source?

2. What happens if electrical power is lost?

3. Do backup command transmitter and emergency systems have adequate protection from loss of electrical power?

4. If power to the ground station is lost, does it affect how flight information is calculated? Do all flight parameters get reset to zero?

4. FLIGHT TERMINATION SYSTEM

A major concern for Range Safety is containment of the UAS within its assigned range test area. Range Safety must ensure that the UAS system does not enter into a ‘fly-away’ condition. This section should describe those features of the UAS which will prevent a fly-away condition.

4.1 Deadman Switch / Kill Switch / Failsafe.

A Deadman Switch / Kill Switch / Failsafe timer is typically circuitry that is incorporated into the UAS that will cause the UAS to stop flying, typically by stopping propulsion. The Deadman/Failsafe functionality can be programmed to occur automatically, based upon a hardware failure, such as loss of heartbeat or software failure. In some cases it can also be controlled from the ground. The CloudCap/Piccollo tach/deadman interface board is one example of this technology.

1. Has a Deadman switch, kill switch or some other failsafe mode been incorporated into the UAS design?

2. Describe how this function has been incorporated into the UAS design.

3. When the function is activated, describe what happens to the UAS. What is the timing and sequence of events?

4.2 Prevention of Fly-Away Conditions

1. Describe any systems installed in the UAS designed to prevent a fly-away condition.

2. What failures could cause a fly-away condition and how are these mitigated?

4.3 Parachute.

1. If the UAS has a parachute system, at what altitude will the chute deploy and what is the impact and drift rate?

2. What is the rate of descent at max weight?

3. Are there altitude, airspeed, or attitude limits on deploying the parachute?

4. Does the engine have to shut off prior to the deployment of the parachute, and what happens if the engine fails to shutdown? Can the propeller cut the parachute shroud line?

4.4 Independent/Standalone FTS Function.

1. Is an Independent/Standalone FTS system installed? Describe its architecture.

2. Describe the operation of the FTS. What is the timing and sequence of events?

3. Does the FTS operate on an independent battery circuit? Does the FTS activate if the battery fails (i.e., fails “safe”)?

4. If there is a separate FTS Transmitter, does its coverage equal or exceed the command transmitter coverage? Does the coverage meet or exceed the maximum range the UAS will fly?

5. Is there a “fail safe” mode that comes into play if a FTS command is not received? What conditions cause it to activate? What happens (engine shut off, flight controls to “turn” or “tumble”)?

5. QUESTIONS ABOUT AIRSPACE AND AIRFIELD OPERATIONS

5.1 Airspace.

1. Will test procedures require exclusive airspace? If not, how will risk to other aircraft be minimized?

2. If shared, is UAV airspace use compatible or incompatible with any type aircraft or type mission?

3. What are the weather minimums for this type vehicle? Can the UAS fly in clouds or IFR conditions?

7. MISCELLANIOUS

7.1 Ground Safety

1. For systems that do not utilize wheeled takeoff and/or landings, what are the ground safety arcs for your launch and recovery operations? The ground safety arcs are those areas that are free from personnel, except system operators if required, during launch and recovery operations. Please provide a diagram of these safety arcs for both launch and recovery operations.

7.2 Mishaps

1. Is there a mishap plan?

2. What are the procedures in the event of a mishap?

7.3 Tracking Systems.

1. What do you have? Can it be shared?

7.4 Is RAS displayed on GCS Map?

1. RAS and ROZ **MUST** be displayed on GCS.

7.5 Camera.

1. Do you have a forward looking camera on board? Camera must be on board for non-line of sight.

8.0 Line of Sight.

1. All non proven UAS must be flown within visual line of sight until CIRPAS personnel give safety approval to fly non line of sight.