APPENDIX D

NMSU PSL TAAC Internal Guidance UAS Airworthiness

Composite System

- The UAS will not present or create a hazard to other aircraft in flight or persons and/or property on the ground.
- The air vehicle structure and flight critical systems shall be designed, built, and tested to minimize the risk of failures.
- Probable failures or combination of failures of the UAS (air vehicle, ground control station, command/control & communications) must not result in unacceptable conditions.
- For a UAS, each item of equipment, each subsystem, and each installation will be examined separately and in relationship to other systems and installations to determine if the aircraft is dependent upon its function for continued safe flight and landing.

Air Vehicle Element

- The air vehicle structure, primary flight controls system, other systems/equipment (i.e., electrical, hydraulics, avionics, software, etc) including the power-plant installation, will have features which provide for the safe functioning of the air vehicle, in the event of a system(s) malfunction or failure. The UAS software (air vehicle and ground control station) should be verified and validated.

- Provisions shall be provided for a failure detection apparatus (preflight and in-flight built-in-tests). Adequate procedures for the safe operation of the vehicle following a system failure and/or automatic recovery shall also be implemented. Potential errors by the operator(s) of the vehicle must be considered during the system design.

- For the UAV flight demonstration, a properly functioning and appropriate flight recovery system (FRS) shall be considered. The FRS must be capable of terminating flight without undue hazard to other aircraft, human life, and/or property on the ground. The FRS shall be used during the following conditions:

  - UA loses the ability to respond in accordance to direction from the UA pilot (i.e., lost command and control link)
  - UA can no longer maintain safe operations due to hardware/software problems (i.e., structural damage, loss of power, corrupted flight management system (FMS), etc
  - Any other unsafe condition that exists to human life and/or property

  - The FRS will function independently of the aircraft's propulsion system and flight controls system. An automatic preprogrammed course of action and/or a non-explosive system shall be considered as the preferred approach.

Note:
Execution of a pre-programmed flight routine must consider the following i.e., to loiter for a designated amount of time until control/communications is re-established; to land at a pre-designated UAV qualified airport; or to execute a spiraling or mush-type maneuver into a pre-designated crash site. Regardless of the type used, the FRS should be capable of being activated by the operator of the vehicle and/or autonomously (i.e., fail-safe). Appropriate contingency procedures shall also be established governing the time duration that should transpire between when the anomaly occurs and when the FRS is engaged.

Note:
The Aerostar UA does not use a parachute as a flight recovery system (FRS). The system incorporates a set of procedures and software to address the safety factors for a FRS. It utilizes two programmable files as part of its "Return Home" (RH) program. The internal pilot, during flight, can update one while the other is designated as the RH program. The program includes way points, altitudes, routes, and speeds. As necessary, the internal pilot can switch between the two RH programs and is able to select, program and/or change emergency landing site before or during the flight. This enables locations to be pre-selected and pre-programmed into the Aerostar's onboard memory. Additionally, NMSU PSL TAAC has a launch and recovery system (LRS) which is mobile and performs several functions including a tertiary back-up in the event that both bays of the ground control system experience a failure. The LRS is able to travel to the UA location while in the return home mode to re-acquire vehicle control through an improved communications with the UA as required.

Ground Control Element

The ground control station (GCS) provides the Human-Machine Interface (HMI) for operating the UAS. The nominal function of the GCS shall be to: monitor the health of flight and mission critical systems; facilitate communications with ATC; and provide positive control of the UAV by the operator.

- The GCS shall include displays, enunciators (visual + audio), and computer equipment necessary to ensure safe control of the vehicle's flight path
- The GCS shall provide an equivalent level of safety with respect to detect, see, and avoid capabilities of a manned aircraft in the same category/class.
- Other equipment installed in the GCS not essential to safety, must be considered acceptable on a no hazard basis.
- The GCS shall be configured to ensure the operator is informed of any degraded mode of operations due to failure, including cases in which there is an automatic switching to an alternate or degraded mode of operation.
- The control station shall include a diagnostic and monitoring capability for the status of the air vehicle. Real time, direct communications and surveillance, and data transmission capability may be provided in the absence of failure.
- For operations in the controlled airspace, direct communications with FAA air traffic control (ATC) shall be incorporated into the control station system design.
- The GCS shall protect the pilot-in-command (PIC) from fire, smoke, or other harmful or potentially incapacitating hazards. The GCS shall also protect the PIC from interruptions while they are performing their crew duties.
- The GCS shall be equipped with instruments that will enable the flight crew to control the flight path of the air vehicle, carry out any required procedural maneuvers, and observe the operating limitations of the aircraft in the expected operating conditions (a minimum equipment list (MEL) shall be established for the UAS).

Command & Control

- The command and control linking system shall consist of: (l) receiving vehicle status and navigation information and (2) transmitting commands to the aircraft.

- The command and control system, at any time during the flight regime, shall be comprised of two or more separate links that are dedicated solely to performing the above two functions.

Note: These individual links will use appropriate radio or satellite communications technology, depending upon whether the UA is within line-of-site (LOS) or over-the-horizon (OTH) from the ground control station (GCS). *At the present time, Aerostar UAS flights conducted by NMSU PAL TAAC have been limited to LOS operations only.*

- All transmission of any signal between the UA and GCS shall adhere to the rules and policies established by the Federal Communications Commission (FCC).

- When operating in the national and international airspace systems, the UAS shall be equipped throughout the flight operation with a command and control link that provides real-time monitoring and control capability by the operator in command.

- During autonomous control or a preprogrammed automated flight profile that does not require human intervention for normal operations, the flight management system shall allow the operator to continuously monitor the aircraft's flight course and altitude.

- The aircraft shall have an over-ride provision for the immediate transfer from autonomous control to operator control of the vehicle.

- Losing the capability to either receive information from the vehicle or transmit commands to the aircraft constitutes loss of the command and control link.

Note: The appropriate precautions should be made to ensure that any transfer from LOS communications to OTH communications, and vice versa, occurs without losing the command and control link. To ensure a smooth transition from LOS communications to OTH communications, the OTH link should be established prior to the LOS signal-to-noise ratio falling below a certain level, or prior to the UA traveling beyond the maximum LOS range (i.e., link is expected to be lost). *At the present time, Aerostar UAS flights conducted by NMSU PAL TAAC have been limited to LOS operations only.*

- In the event of failure of any on-board flight management system hardware and/or software, the UA shall have the capability to be recovered or redirected. This capability shall be separate from, and in addition to, any flight recovery system (FRS) that may be installed on the UAS. It is noted that the Aerostar is equipped with a robust unmanned multi-application system (UMAS) that has a separate independent power source (battery). To date, no failure of the UMAS has occurred on the Aerostar.

Note: Another means to limit loss of the command and control link is to limit the UA ability to exceed a certain bank angle. This constraint, in essence, prohibits the UA structure from blocking the command and control signal from the onboard antenna. Because the command/control link may be used to govern/direct the UA, it is essential that the link/message sent be properly protected to reduce the likelihood that an outside source could take over control of the vehicle. Additionally, each UA should be uniquely identified so as to ensure that another command and control link, from a different UA GCS cannot inadvertently uplink commands to a UA flying within the proximity of the transmitted signal.

System Safety Design & Analysis

The following fail-safe design concept principles or techniques have been reviewed and noted by safety personnel at NMSU PSL TAAC in order to ensure a safe design: .

- Integrity and quality, including life limits, to ensure intended functions and prevent failures.

- Redundancy or backup systems to enable continued function after any single (or other defined number of) failures e.g., flight control system, control & command, vehicle hydraulic system, etc.
- Isolation of systems, components, and elements so that the failure of one does not cause the failure of another.
- Reliability so that multiple, independent failures are unlikely to occur during the same flight.
- Failure warnings or indications to provide detection.
- Procedures for use after failure detection, to enable continued safe flight and landing by specifying corrective action.
- Procedures to check a component's condition.
- Failure limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.
- Failure path to control and direct the effects of a failure in a way that limits its safety impact.
- Margins or factors of safety to allow for any undefined or unforeseeable adverse conditions.
- Tolerances that consider adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation, and maintenance.

General Guidelines (but not limited to)

Evaluation of the air vehicle and ground control station systems and equipment need to consider the following:

- Determine if systems and equipment are essential to safe operations or not essential to safe operations.

- Determine that operations of installed equipment have no unacceptable adverse effects (verify by applicable flight and/or ground checks).

- Determine that failure or malfunction of the installed equipment does not result in unacceptable hazards (i.e., a hazard could result from loss of equipment or systems essential to safe operations when the minimum required functions are lost).