APPENDIX G

NMSU PSL TAAC Operational Safety Assessment (OSA) Guidance

NMSU PSL TAAC has demonstrated that a collision of the ADS Aerostar UAS with another aircraft, parachutists, other civil airspace users, and injury to persons and/or property along the designated flight path, is extremely improbable by taking a collective view of the total infrastructure available for flight operations. The hazards associated with the Model Aerostar UAS operations at NMSU PSL TAAC are based on prior system knowledge, hazard analysis, past experience, and lessons learned.

The format used to identify the hazards has not been formalized but the potential hazards have been identified. Examples of NMSU PSL TAAC documents that may identify hazards include hazard lists (see information contained herein), hazard analysis, and portions of TAAC USOVP procedures manual. NMSU PSL TAAC guidance material has enabled TAAC safety personnel to identify potential system hazards and review existing hazard controls.

The particular Model Aerostar UAS system configuration (platform, GCS, controls/communications) have been addressed, but not limited to, features and characteristics, equipment installations, use of checklists (pre-flight, in-flight, post-flight), prescribing operating limitations and conditions, ground observations, use of chase plane, etc. The objective is to show the extremely improbable case by demonstrating that the total system, taken together, can provide a minimum level of safety for operations conducted under provisions of a COA.

FAA Order 8040.4, dated 6/26/98, establishes the safety risk management policy and prescribes procedures for implementing safety risk management as a decision-making tool within the FAA. The objective of this policy is to formalize a common sense approach to risk management and safety risk analysis/assessment in the FAA decision-making process. It contains principles for safety risk assessment/risk characterization, tasks to analyze risk reduction benefits/costs, product life cycle, mishap, etc. The TAAC uses this as a guide and has established an appropriate safety risk management committee that supports the NMSU PSL TAAC safety risk management activities.

RISK ASSESSMENT MATRIX

	Severity			
Likelihood	**Catastrophic**	**Critical**	**Marginal**	**Negligible**
Frequent	High	High	Serious	Medium
Probable	High	High	Serious	Medium
Occasional	High	Serious	Medium	Low
Remote	Serious	Medium	Medium	Low
Improbable	Medium	Medium	Medium	Low

The following hazard severity categories and probability levels have been adopted by NMSU PSL TAAC using criteria and guidelines contained in the Range Commanders Council (Range Safety Group) Supplement to Document 323-99, Range Safety Criteria for Unmanned Air Vehicles, as follows:

RANGE SAFETY CRITERIA HAZARD SEVERITY CATEGORY GUIDELINES:

Description	Level	Effect on People	Effect on Property	Environmental Effects
Catastrophic	I	death, permanent disability	greater than $ 1million	severe (hazardous)
Critical	II	severe injury, permanent partial disability, hospitalization for 5 or more people	$ 200,000 to $ 1 million	major
Marginal	III	minor injury, 1 or more lost workdays	$ 10,000 to $ 200,000	minor
Negligible	IV	less than minor injury	less than $ 10,000	less than minor (no effect)

RANGE SAFETY CRITERIA HAZARD PROBABILITY LEVEL GUIDELINES:

Description	Level	Incidents Per 100,000 Flight Hrs	Individual Exposure Rate	Fleet or Inventory Exposure Rate
Frequent	A	100 or more	likely to occur frequently	continuously experienced
Probable	B	10 to 99	will occur several times in the life of an item	will occur frequently
Occasional	C	1 to 9.9	likely to occur sometime in the life of an item	will occur several times
Remote	D	0.1 to 0.99 `	unlikely but possible to occur in the life of an item	unlikely but can reasonably be expected to occur
Improbable	E	less than 0.1	so unlikely, it can be assumed occurrence will not be experienced	unlikely to occur, but possible

The following information has been used as a guide for the assessment of the ADS Aerostar. These are generic hazard conditions and vehicle failure modes which can lead to loss of the UA, a midair collision, serious injury, and/or death. The background information summarized in these tables is based on mishap data as well as UAS hazard analyses, not necessarily that of the Aerostar.

TAAC System Safety Areas of Interest for Aerostar (for all phases of flight), but not limited to:

- engine failure
- pilot induced error
- failure of chase plane to observe
- failure of UAS security protection
- failure of communication equipment
- malfunction/failure of sense & avoid
- malfunction of flight recovery system
- loss of GCS capabilities (full or partial)
- flight beyond authorized containment area
- loss of navigation capabilities (full or partial)

- loss of electrical power (GCS and/or platform)
- failure of command & control (uplink and/or downlink)
- natural ice/lightning/electromagnetic/other environmental hazards

TAAC established guidelines of hazard conditions for COA application:

Hazardous Condition	Cause	Severity	Mitigations	Likelihood
Loss of Propulsion	(1) engine failure	critical	Reduce engine MTBF	remote
	(2) fuel starvation	critical	preflight/inflight check	remote
	(3) stuck throttle	critical	preflight check	remote
	(4) icing/weather	critical	survey planned route	remote
Loss of Lift	(1) structural failure	catastrophic	preflight/maint check	remote
	(2) icing/weather	critical	survey planned route	remote
Loss of Flight Control Surfaces	(1) stuck servo	critical	preflight controls check	remote
	(2) autopilot failure	critical	preflight system operation	remote
	(3) computer failure	critical	preflight system operation	remote
	(4) software error	critical	preflight system operation	remote
	(5) icing / damage to control surface	critical	limit flight operations	remote
Aircraft Structural Failure	(1) exceeding limit loads permanent deformation	critical	install accelerometer and limit maneuvers	remote
	(2) exceeding ultimate structural loads	critical	install accelerometer and limit maneuvers	remote
Loss of Control Link	(1) radio frequency interference	critical	call ATC	remote
	(2) flight beyond horizon	critical	lost link procedures	remote
	(3) antenna masking	critical	limit maneuvers	remote
	(4) loss of GCS	critical	USOVP procedures	remote
	(5) software interrupt between GCS & and air vehicle	marginal	continue flight safe orbit	remote
	(6) atmospheric attenuation	marginal	continue flight safe orbit	remote
	(7) inadvertent deactivation of autopilot	marginal	continue flight safe orbit	remote
	(8) loss of satellite link	critical	lost link procedures	remote
Loss of Heading/ Attitude/Position Information	(1) heading/attitude system failure	critical	preflight check of navigation system	remote
	(2) navigation failure	critical	dead reckoning capability	remote
Loss of Voice Communications Link	(1) loss communication with observer/spotter	critical	backup personnel & communication equipment	remote

Hazardous Condition	Cause	Severity	Mitigations	Likelihood
Latency of Flight Control Commands	(1) control link through satellite	critical	verification process per USOVP procedures	remote
	(2) pilot induced oscillation	critical	provide structural overload protection	remote
Loss of UAS Electrical Power	(1) generator failure	critical	reduce generator MTBF	remote
	(2) backup battery failure	critical	USOVP procedures	remote
	(3) excessive load from payload	critical	weight limits in AFM	remote
Loss of Ground Control Station (GCS)	(1) loss of GCS power	critical	USOVP procedures	remote
	(2) GCS transmitter/ receiver/antenna failure	critical	USOVP procedures	remote
	(3) GCS computer failure	critical	USOVP procedures	remote
	(4) GCS battery failure	critical	USOVP procedures	remote
Altitude Error	(1) incorrect barometric setting	critical	preflight checklist	remote
	(2) inadequate alert for altitude deviation	critical	backup comm. capability	remote
Navigation Error	(1) navigation system failure	critical	preflight check & onboard monitoring	remote
	(2) navigation system discrepancy (INS vs GPS)	negligible	INS not installed	improbable
	(3) map display inaccuracy	critical	preflight check	remote
Loss of Link "Fly Home" Mode	(1) mission planning error for loss of link mode	catastrophic	USOVP training & procedures	remote
Failure to See & Avoid	(1) no capability	critical	use of chase aircraft	remote
	(2) autonomous operation	critical	use of chase aircraft	remote
Not Observed by Other Aircraft	(1) strobe/position lights inadequate or fail	critical	preflight check	remote
	(2) TCAS failure	negligible	equipment not installed	remote
	(3) ATC/UAV operator Communication link failure	marginal	backup communication capability	remote
Mission Planning Error	(1) flight below minimum en-route altitude	critical	training & locking flight critical commands	remote
	(2) undetected man-made Obstacles (towers, cables, etc)	critical	preflight planning	remote

Hazardous Condition	Cause	Severity	Mitigations	Likelihood
Operator Error	(1) outside weather / wind limits	marginal	flight under marginal conditions avoided	improbable
	(2) internal pilot / external pilot handoff errors	critical	USOVP procedures	remote
Inadequate Operator Response	(1) failure to recognize flight critical situation	critical	USOVP training & procedures	remote
	(2) flight-critical information missing, erroneous, or ambiguous	critical	USOVP training & procedures	remote
Incorrect Inputs of Flight Critical Parameters	(1) operator entry errors	critical	verification process per USOVP procedures	remote
Operator Fatigue	(1) inadequate crew rest	major	AFM limitations	remote
	(2) task saturation	major	AFM limitations	remote
Software Paths to Unsafe State	(1) unexpected reboot	major	preflight check	remote
	(2) inadequate software safety process	major	failsafe modes and manual override	remote

Preliminary Safety Risk Hazard Assessment

The preliminary hazard analysis/safety assessment has taken into consideration the airworthiness of the Aerostar UAV, the pre-flight reviews (Independent Safety Review and Flight Readiness Review) that are a part of each mission, pre-flight briefing and post-flight critique, operating procedures, see and avoid procedures, volume of air traffic operations within the affected airspace, and, in the UA operating airspace, general weather conditions, density of population on the surface underlying the UA flight areas, and ATC and public awareness. The following are salient facts that provide details of the Hazard Analysis/Safety Assessment.

1. Airworthiness – The ADS Aerostar UAS has been evaluated with respect to MIL-HDBK-516 airworthiness certification criteria. In addition, historical data from the manufacturer (ADS) and the number of flight hours (in excess of 17,500), are positive indicators of the Aerostar UAS capability to operate safely and in conformance to the criteria/guidelines for its intended operation in the NAS by NMSU PSL TAAC. The Aerostar is presently being flown in a number of countries and has more than 30,000 hours of flight time with three accidents in its history; 8000 flight hours with the DH290 engine version (same as PMA263's Aerostar) and 22,000 flight hours with the Zanzottera 498 engine version (5000 hours with engine version 3) with no critical failures. There were three crashes; one electrical failure due to incorrect maintenance (DH290 engine version), and two engine failures during the engine version testing (from DH290 to Zanzottera). The subsequent corrective actions included changes to the maintenance procedures and Zanzottera engine version 3 (modified fuel map, crankcase and pistons.

2. Pre-flight Reviews – Prior to the beginning of any mission (series of flights to achieve the planned objectives), there are two separate committee reviews to ensure that safety is maintained. The first is an Independent Safety Review (ISR), which includes individuals who are not involved directly in the NMSU PSL TAAC UAS programs and activities. These individuals participating in the ISR are primarily from the White Sands Missile Range, Holloman AFB, and other military installations and civil organizations that are

knowledgeable of aviation criteria and safety standards. UAS flight operations are not performed until identified safety issues and concerns are resolved to the ISR group's satisfaction. The second review is by the Flight Readiness Review (FRR) committee, which is conducted shortly before the beginning of flight operations. The FRR is conducted primarily by NMSU PSL TAAC personnel who are involved in the UAS operations; however, the process always involves others that are not directly involved in the UAS operation. Similar to the ISR, no UAS flights will occur until deficiencies identified during the FRR have been corrected.

3. Pre-flight Briefing and Post-flight Critique - Before each flight, all personnel involved in the flight operation of the UAS meet together for a briefing on the mission plan, operating procedures, contingency procedures, and to ensure all personnel are knowledgeable of the intended flight operation procedures and understand their respective roles and responsibilities. At the conclusion of each flight, a post-flight critique is performed to evaluate the total operation with emphasis on identifying any deficiencies or problems and areas of improvement. Any identified deficiencies or problems will be corrected prior to the next flight.

4. Operating Procedures – Operating procedures are designed to achieve the safest operation possible. Flight operations in the vicinity of the airport, except during takeoffs and landings, will be performed at altitudes above the traffic patterns for the airport and away from normal approach courses that manned aircraft use at the airport. All flight operations will be consistent with 14 CFR 91 criteria.

5. See-and-Avoid Criteria – Direct visual observation of the UA will be maintained at all times, either through the use of visual observer(s) on the surface or onboard a chase aircraft. The visual observer will operate within the stated FAA permissible distance parameters. Since the visual observer can see above and below as well as behind the UA, the actual safety factor is greater than that capable of a pilot in a manned aircraft.

6. Volume of Air Traffic - The volume of air traffic at the airports of intended operations is normally light. The volume of air traffic in the UA flight airspace (17,500 MSL and below in Class E and G airspace) is light with brief periods of moderate air traffic. Most of the air traffic in this airspace consists of high-altitude en route traffic in Class A airspace, mostly at FL280 and above. The WSMR restricted areas act as a buffer for most of the UA airspace.

7. Weather Conditions – Inherently, the weather conditions in the UA flight airspace consist of clear skies with unlimited visibility. No UA flights will be performed in marginal weather conditions.

8. Population Density – The UA flight operations airspace is located in the Southwest section of New Mexico. This is a very sparsely populated area; one of the least populated in the entire United States. With the exception of the City of Las Cruces, there are no other cities in this area. Several small towns are situated throughout this large area with many miles of uninhabited or very small number of persons residing between these small towns.

9. ATC/Public Awareness – Advanced coordination will be performed with Albuquerque Air Route Traffic Control Center (ARTCC) at least seven days in advance of any flights. In addition, military airspace users that commonly fly within the airspace that will be used for UA operations will be coordinated in advance. Public awareness of the UA flights is accomplished through announcement materials being made available to pilots through the local Fixed Base Operators (FBOs) and the various airport managers. In addition, all pilots will have an opportunity to know about the UA flight activity by receiving information that is contained in the Notice to Airmen (NOTAM) that will be issued for each UA flight.

Determination – Consistent with NMSU PSL TAAC's knowledge of what is required to achieve safe UA flight operations, commitment to ensure safety is maintained, and coupled with the analysis/assessment defined in the above factors, NMSU PSL TAAC has determined that injury to persons or property along the UA flight path is "extremely improbable."

NMSU PSL TAAC safety personnel have implemented the following measures for the Aerostar S/N 617 and S/N 618, i.e., design changes to minimize risk, incorporated safety and warning devices, developed series of procedures & training, and selected routes confined to unpopulated areas:

- Provided pre-flight checklists
- Provided emergency procedures
- Provided "low fuel" indicator warning lights
- Specified operating limitations & conditions
- Established operator qualification procedures
- Provided containment and verification procedures
- Tested return home mechanism (including software)
- Provided a back-up battery for the UA in case of generator failure
- Installed and required strobe lights to make the vehicle easier to see
- Provided software and procedures for "fly-home" routine in case of lost link
- Provided a back-up battery for the unmanned multi-application system (UMAS)
- Confined flights to unpopulated areas to eliminate risk to people on the ground
- Provided a redundant communications link in case of failure of the primary link
- Warning calls are provided by ATC when the vehicle is approaching other traffic or hazard/flight boundaries
- Installed a more reliable engine as an upgrade to reduce the risk of loss of propulsion
- Engine performance safety data displayed at the ground control station (GCS) (e.g., over-temperature alert)

Aeronautics Defense Systems (ADS) Operational Safety Assessment (OSA):

Aeronautics Defense Systems (ADS) has provided the following BQR Reliability Engineering Ltd. Documents (1) Aerostar UAS Reliability, Availability, Maintenance, Safety (RAMS) Report, BQR Document No. 1477 dated Oct 15, 2006 (Appendix I), (2) Aerostar UAS Failure Modes and End Effect Criticality (FMECA), BQR Report No. 1475 dated Oct 11, 2006 (Appendix J), and (3) Aerostar Fault Tree Analysis (FTA) Report, BQR Document No. 1476 dated Oct 11, 2006 (Appendix K).

BQR Fault Tree Analysis (FTA):

The FTA used a top-down approach and was based on the end effects that were previously defined in the FMECA. The FTA was divided in three parts: (1) ground roll and take-off, (2) flight, and (3) final approach and landing. The purpose of the analysis was to identify all possible combinations of the end effect (with high severity), that define the system failure modes which can result in a safety hazard and possible system loss of the Aerostar. The analysis substantiates the final probability of a critical loss of control of the Aerostar that is lower than 10-6. Human errors were also considered in the analysis as relevant factors.

BQR Failure Modes and End Effect Criticality (FMECA):

The FMECA covers the failure modes effect and criticality analysis for the Aerostar UAS that includes the UAV, mission control station (MCS), and the communication modules. The purpose of the FMECA is to assess the high risk items and was prepared to analyze potential failure modes of each component and to evaluate their effect on the system overall performance. The failure modes were classified according to their severity. See report for classifications of severity and criticality, and the end effects.

BQR Reliability, Availability, Maintenance, Safety (RAMS):

The RAMS report contains final results and recommendations on safety. The purpose of the RAMS analysis is to examine the Aerostar UAS that includes the UAV, mission control station (MCS), and the control & communication functions in order to satisfy that the system can fly over settled area safely with a

very low probability of creating an unsafe condition. The Aerostar UAS loss of control as the critical failure mode has a probability of 0.94 x 10e-06 per operational hour, which is considered within acceptable limits. The Aerostar UAS was analyzed as follows:

- UAV
  - Fuselage
  - Engine
  - Electrical
  - Fuel Tank
  - Avionics
  - Optics
- Mission Control Station (MCS)
  - Internal Pilot (IP)
  - Mission Commander (MC)
  - Payload Operator (PO)
  - External Pilot (EP)
- Communication
  - Air Communication
    - Main Channel
    - Secondary Channel
  - Ground Communication
    - Main Channel
    - Secondary Channel

It is noted in the RAMS report that the FMECA analysis included all system critical components and all failure modes of those components were considered. The probability of every failure was propagated to the system level, and used to create a criticality matrix of the system that included the probability and the severity of each and every single failure. The FMECA analysis considered two system level failures: (1) fail, but UAV is able to return safely, and (2) UAV loss of control.

The mean time between failures (MTBF) of the Aerostar system is calculated as follows:

- MTBF for the UAV = 1,107 hours
- MTBF for the MCS = 1,204 hours
- MTBF for the Comm = 39,094 hours

The mean time between critical failures (MTBCF), in this case, a failure which will end the UAV mission and covers the UAV, MCS, and communications modules is computed at 3683 hours.

The following failures of the Aerostar UAV were considered as safety related failures that can lead to UAV loss of control:

- During Take-off
  - Avionics failure
  - Foreign object damage
  - Engine shutdown after take-off
  - Permanent communication lost
  - Flaps, elevator servo jammed in extreme angle
  - Failure in front wheel servo (stuck in max angle)
  - Exceptional and unwanted command from the external pilot's box (CBX)
  - Front wheel or one of the main wheels are fractured or disconnected from UAV
  - Deviations from the centerline during the ground roll as the result of human error

- During Flight
  - Human error
  - Avionics failure
  - Permanent communication lost
  - Flaps, elevator servo jammed in extreme angle
  - Engine shutdown (out of range for gliding to safe landing)
  - Fire due to shortage in main electrical harness or in one of the electrical components

- During Landing
  - Human error
  - Foreign object damage
  - Serious avionics failure
  - Permanent communication lost
  - Exceptional weather conditions
  - No fuel (depending on landing status)
  - Flaps, elevator servo jammed in extreme angle
  - Engine shutdown prior to approaching threshold
  - Failure in front wheel servo (stuck in max angle)
  - Exceptional and unwanted command from the external pilot's box (CBX)
  - Front wheel or one of the main wheels are fractured or disconnected from UAV