National Transportation Safety Board

Washington, D.C. 20594

Safety Recommendation

Date: October 24, 2007

In reply refer to: A-07-70 through -86

Honorable W. Ralph Basham
Commissioner
U.S. Customs and Border Protection
Washington, D.C. 20229

The National Transportation Safety Board is an independent Federal agency charged by Congress with investigating transportation accidents, determining their probable cause, and making recommendations to prevent similar accidents from occurring. We are providing the following information to urge your organization to take action on the safety recommendations in this letter. The Safety Board is vitally interested in these recommendations because they are designed to prevent accidents and save lives.

This recommendation letter addresses deficiencies in the design, operation, and safety management of the unmanned aircraft system (UAS)[1] operated by the U.S. Customs and Border Protection (CBP), under the Department of Homeland Security, and deficiencies in the CBP's coordination with the air traffic control (ATC) facilities involved. These recommendations are derived from findings in the Safety Board's investigation of an April 25, 2006, accident involving an unmanned aircraft (UA) that crashed near Nogales, Arizona.

The Safety Board determined that the probable cause of the accident was the pilot's failure to use checklist procedures when switching operational control from pilot payload operator (PPO)-1 to PPO-2, which resulted in the fuel valve inadvertently being shut off and the subsequent total loss of engine power, and lack of a flight instructor in the ground control station (GCS), as required by the CBP's approval to allow the pilot to fly the Predator B. Factors associated with the accident were repeated and unresolved console lockups, inadequate maintenance procedures performed by the manufacturer, and the operator's inadequate surveillance of the UAS program. As a result of this investigation, the Board has issued 22 safety recommendations; 17 of which are addressed to the CBP. Information supporting these recommendations is discussed below.

[1] The UAS includes an unmanned aircraft, a ground control station, and related components.

Background

On April 25, 2006, about 0350 mountain standard time, a Predator B, a UA manufactured by General Atomics Aeronautical Systems, Inc. (GA-ASI), crashed approximately 10 nautical miles northwest of Nogales International Airport, Nogales, Arizona, within 100 yards of a house that was located in a sparsely populated residential area. There were no injuries to persons on the ground. The UA, which was unregistered and owned by the CBP and operated under contract with GA-ASI, sustained substantial damage. The public-use flight was operating in night visual meteorological conditions. An instrument flight rules flight plan had been filed and activated for the flight, which originated from the Libby Army Airfield (FHU),[2] Sierra Vista, Arizona.

According to GA-ASI, the Predator B is powered by a turboprop engine and has redundant, fault-tolerant avionics as well as the capability to be remotely piloted or fully autonomous. The wingspan of the Predator B is 66 feet, with a maximum weight of 10,000 pounds, maximum altitude ceiling of 50,000 feet, and a flight endurance in excess of 30 hours. The Predator B has the ability to fly at more than 220 knots. The UAS was designed as a long-endurance, high-altitude UA for use as a multi-mission system by a variety of customers.

The UAS was being operated by the CBP under a certificate of authorization (COA) issued by the Federal Aviation Administration (FAA) in April 2006. While the COA contains both security and safety information, the CBP has classified the entire document as security sensitive information. The Safety Board normally conducts transparent investigations in which facts and analytical conclusions (findings) that lead to safety recommendations are made public. At the CBP's request, the Board will not make public specific information contained in the COA. Therefore, certain safety issues will be discussed in this letter only in a general manner even though Board investigators have conducted a complete review of the relevant facts, including the COA, and a thorough analysis of those facts.

The Safety Board recognizes that the CBP was directed to initiate the Predator B program and to start flying in a very short time period. At the time of the accident, the UAS program was heavily dependent on contractors, primarily GA-ASI, for its safe operation. Since the accident, the CBP has performed a program review and developed policies, procedures, and training that provide much stronger operational control and safety oversight of its UAS program. The Board is strongly encouraged by the CBP's work in this regard and encourages the CBP's continued efforts to address all of the safety issues presented in this recommendation letter. The Board would appreciate a response from the CBP within 90 days addressing the actions it has taken or intends to take to implement these recommendations.

Unmanned Aircraft System Design and Inadvertent Engine Shutdown

The GCS at FHU, from which the accident flight was controlled, contains two nearly identical control consoles: PPO-1 and PPO-2 (see figure 1). During a routine CBP mission like the accident flight, the pilot (provided by GA-ASI) controls the UA from the PPO-1 console, and a payload operator (a U.S. Border Patrol agent) controls the camera mounted on the UA from the

---

[2] The accident flight was being piloted from a ground control station located at the airfield where the flight originated.

PPO-2 console. Although the aircraft control levers (flaps, condition lever, throttle, and speed lever) on PPO-1 and PPO-2 appear identical, they may have different functions depending on which console controls the UA. When PPO-1 controls the UA, the condition lever controls the engine via movement to one of three positions, as follows:

- Movement to the forward position opens the fuel valve to the engine;
- Movement to the middle position closes the fuel valve to the engine, which shuts down the engine; and
- Movement to the aft position causes the propeller to "feather."[3]

When the UA is controlled by PPO-1, the condition lever at the PPO-2 console controls the camera's iris setting. Moving the lever forward increases the camera's iris opening, moving the lever to the middle position locks the iris setting, and moving the lever aft decreases the opening. Typically, the lever is set in the middle position.

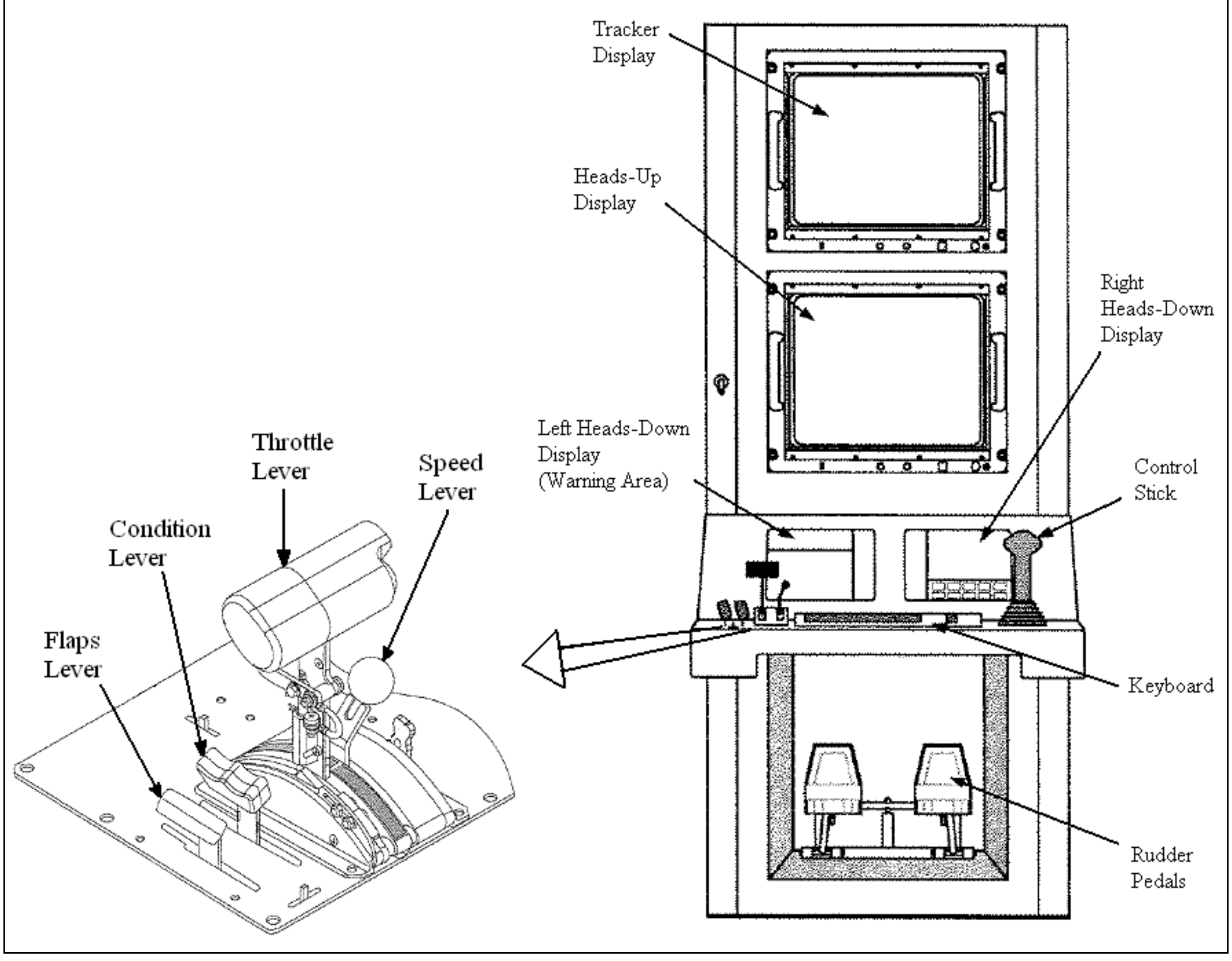

Figure 1. Diagram of a Control Console Installed at the CBP's Ground Control Station

[3] Feathering a propeller means adjusting the pitch of the blades so that the leading edge points into the wind, thus reducing the frontal area to a minimum and minimizing or stopping rotation of the blades, which reduces the drag caused by the propeller.

Operational control of the UA can be transferred from PPO-1 to PPO-2 in the event of a malfunction of PPO-1. Console lockup checklist procedures indicate that, before switching operational control between the two consoles, the pilot must match the control positions on PPO-2 to those on PPO-1 by moving the PPO-2 condition lever from the middle position to the forward position, which keeps the engine operating. The pilot[4] stated in a postaccident interview that, during the accident flight, the console at PPO-1 "locked up," which prompted him to switch control of the UA to PPO-2, as allowed by the system design. However, he did not consult the console lockup checklist. He stated that he did not position the PPO-2 levers to match the PPO-1 levers before the transfer of control, as defined in the console lockup checklist. As a result, the condition lever of PPO-2 was in the middle position when the transfer of control occurred, and the engine fuel shutoff valve was commanded to close when control of the UA was transferred from PPO-1 to PPO-2. Safety Board investigators later confirmed, through a review of parameters recorded during the event, that the condition lever of PPO-2 was in the fuel cutoff position when the switch from PPO-1 to PPO-2 occurred. As a result, fuel to the UA's engine was cut off, and its engine stopped operating.

Findings thus far in the CBP accident investigation and information about a similar U.S. Coast Guard event[5] demonstrate that the current design of the control consoles (that is, the dual functions assigned to a single lever) can cause an unsafe condition that can result in an unintended engine shutdown if proper procedures are not followed. The Safety Board is aware that, as a result of the accident, design changes were proposed for the GCS to inhibit transfer of control between PPO-1 and PPO-2 when the control levers are in disagreement (including the condition lever). However, Board investigators have been unable to assess the progress and outcome of these changes in preventing inadvertent engine shutdowns because the CBP and GA-ASI have not yet released the pertinent design details requested. Until the Board can obtain a more comprehensive understanding of this system change, concerns remain regarding the potential for inadvertent engine shutdown during the operation of the Predator B. Therefore, the Safety Board believes that the CBP should require GA-ASI to modify the UAS to ensure that inadvertent engine shutdowns do not occur.

Visual and Aural Alerting System

The accident pilot stated that, after switching to the PPO-2 console, he noticed that the UA was not maintaining altitude, but he did not know why. Engine data are usually presented on the PPO-1 console heads-up display when flight graphics are displayed, and those engine data turn red when the engine parameters fall below normal operating conditions. However, flight graphics such as engine data are not typically displayed on the PPO-2 console because the camera operator does not use them. The pilot stated later that, after the switch occurred, flight graphics (which includes engine data) were not displayed on the heads-up display.

[4] The accident pilot was a GA-ASI employee who held a commercial pilot certificate with single-engine land, multi-engine land, and instrument ratings. In addition, he held a certified flight instructor certificate with single-engine land, multi-engine land, and instrument ratings.

[5] In July 2004, the engine of a U.S. Coast Guard-operated GA-ASI Altair UA, which is very similar to the Predator B, inadvertently shut down after operating positions were switched and the fuel was cut off. In that incident, the crew was able to restart the engine.

Engine data and fault annunciations are also normally displayed and highlighted in the left heads-down display on the PPO-1 and PPO-2 consoles (see figure 1). However, a significant amount of information is presented in this display, including several highlighted warnings other than engine performance data that are not prioritized; therefore, it may be difficult to sort through information quickly in an emergency situation. Adding to this difficulty is the absence of a unique aural annunciation associated with the engine-out indication; only one tone is used for all fault conditions. Without an obvious indication of the engine-out condition, the pilot was unable to quickly evaluate the situation and recognize that the fuel had been cut off to the engine during the transfer to PPO-2.

The pilot also stated that it was difficult for him to assess if PPO-2 was also locked up, most likely because its heads-up display was blank and control inputs to the UA would not be readily apparent on the overhead tracking display. Postaccident evaluation of the telemetry data indicated that the PPO-2 console was not locked up and that, if the pilot had been able to quickly diagnose the engine failure, he should have been able to restart the engine.

The reasons for console lockups are varied, and, when a lockup occurs, the cues may not be readily apparent to the pilot. The system does not diagnose the nature, cause, or extent of a lockup and does not display a fault message to the pilot. Similar to a personal computer that slows down and freezes, the user is unaware of the extent of the problem or what functions are affected. In the event of a lockup, the pilot may become aware of the problem because some parameters are not updating as frequently as expected or all visual cues may freeze. The pilot may lose some or all situational awareness of the aircraft. Furthermore, the system does not adequately prioritize fault warnings to facilitate identification during an emergency situation. The Safety Board concludes that the CBP's UAS lacks adequate visual and aural indications for safety-critical fault conditions, such as an engine-out condition or console lockup. Therefore, the Safety Board believes that the CBP should require GA-ASI to modify the UAS to provide adequate visual and aural indications of safety-critical faults, such as engine-out conditions and console lockups, and present them in order of priority, based on the urgency for pilot awareness and response.

Unmanned Aircraft System Lost-Link Mission Profile

In the event of a lost data link between a GCS and UA, the UA is designed and programmed to fly a flightpath known as the lost-link mission profile, which is a predetermined autonomous flightpath, until the GCS operation can be restored and line-of-sight (LOS) data link transmissions can be reestablished.

A CBP contractor, Organizational Strategies, Inc. (OSI), developed several lost-link mission profiles for the accident UA. These profiles were submitted to the CBP and accepted as proposed by OSI. Each profile consisted of a series of altitudes and locations, which formed a loop, around which the UA would autonomously fly. If a data link cannot be reestablished, the UA cannot land, and it will eventually run out of fuel and crash at some location along the route. The specific details of the lost-link profiles and emergency procedures associated with their implementation are considered security sensitive.

The Safety Board's investigation reviewed the process for designing the lost-link profile and found that there was no standardized safety-based method for determining the routes for the lost-link flightpath and that inadequate consideration was given to ensuring the flightpath did not include flight over population centers, property, or other installations of value. Additionally, Board staff determined that the lost-link profile was quite complex and pilots were not aware of the actual initial flightpath of the UA in the lost-link mode or the possible consequences of an improper altitude setting in the lost-link mode. For example, one pilot entered the initial lost-link altitude at the start of the mission, as required, but did not modify the lost-link profile altitude as the aircraft was flown to an area beyond the takeoff zone. The new areas required a higher lost-link altitude value than the initial value input at takeoff. The pilot did not understand that a failure to modify this altitude setting would result in the UA flying at a lower altitude, which could potentially result in the UA flying below the approved altitude range, outside the temporary flight restriction (TFR). In addition, had the pilot correctly modified the altitude value for the lost-link mode, the UA would have remained at a higher altitude, which would have provided for a better opportunity to recover LOS control during lost-link operation.

Further, the Safety Board found that the lost-link procedure only provided for the UA to crash along the lost-link route. Future lost-link procedures should include provisions for the UA to proceed to a safe zone for a crash landing. The Safety Board concludes that a thorough review of the procedures for developing lost-link mission profiles and proper training of UA pilots on use of lost-link profiles during operation would minimize the potential safety impact to persons on the ground and optimize the ability to recover the data link. The Safety Board also concludes that the CBP should consider establishing a lost-link profile that would guide the UA to a safety zone for crash landing. Therefore, the Safety Board believes that the CBP should review its methods of developing lost-link mission profiles to ensure that lost-link mission profile routes minimize the potential safety impact to persons on the ground, optimize the ability to recover the data link, and, in the absence of data-link recovery, provide the capability to proceed to a safe zone for a crash landing. The Safety Board also believes that, following completion of the action requested in Safety Recommendation A-07-72, the CBP should require that pilots be trained concerning the expected performance and flightpath of the UA during a lost-link mission.

Loss of Essential Electrical Power and Engine Restart Capability

The Safety Board's investigation revealed that, after the console lockup and transfer of control to PPO-2, the engine shut down and the UA's functionality degraded quickly as it began to operate on battery power. On battery power, the UA automatically shuts down some systems to conserve electrical power. In this accident, the UA shut down several functions, including the satellite communication system and the transponder. At that point, the pilot likely had a blank heads-up display screen on PPO-2 and no visual cues to determine if he could control the UA from PPO-2. He initiated a procedure to send the UA to its lost-link mission profile. Analysis of recorded telemetry and radar data showed that the UA began flying the lost-link mission profile. However, with no engine power, the UA continued to descend below LOS communications, and further attempts to reestablish the data link with the UA were not successful. In addition, having shed electrical power to its transponder as a result of the loss of engine power, the aircraft could no longer be tracked by ATC.

The loss of the transponder resulted in ATC not being able to identify the UA, its position, or its altitude, thus creating an unsafe condition. The continuing operation of the transponder with mode C altitude data would have provided ATC with valuable information regarding the location of the UA. The Safety Board concludes that the CBP should consider the UA's transponder function to be essential to safe operation in the National Airspace System (NAS). Therefore, the Safety Board believes that the CBP should require that the UAS be modified to ensure that the transponder continues to provide beacon code and altitude information to ATC even if an engine shuts down in flight and that the pilot is provided a clear indication if transponder function is lost for any reason. Also, the Safety Board believes that the CBP should review all UAS functions and require necessary design changes to the UASs that the CBP operates to ensure that electrical power is available for an appropriate amount of time to all systems essential to UA control following loss of engine power.

Although the UAS is programmed to control certain functions without pilot-initiated commands, it is not programmed to autonomously control the position of the fuel shutoff valve and enable self-initiated engine restart after an inadvertent engine shutdown, entry into the lost-link mission profile, and descent below LOS control, such as occurred in this case. If the UA engine shuts down while operating in an area where LOS control can be lost, there is inadequate redundancy to restart the engine. Therefore, the Safety Board believes that CBP should develop a means of restarting the UA engine during the lost-link emergency mission profile that does not rely on LOS control, for example, through an autonomous capability in the UAS' control system or through use of control functions enabled via a backup satellite communication system available to the pilot on the ground.

Coordination with Air Traffic Control

Operators of aircraft are required to coordinate with ATC to allow for assured separation of aircraft operating in the NAS. Thus, the GA-ASI pilot, while piloting the UA, was required to coordinate with ATC to minimize the risk of collision with another aircraft. The UA was authorized to operate in temporarily restricted airspace defined by a TFR. Other aircraft were required to be in contact with ATC before operating in the TFR airspace, which extended along the southern U.S. border from 14,000 to 16,000 feet mean sea level. In this accident, the UA could not maintain altitude, breached the lower limit of the TFR, and was operating autonomously in unprotected airspace until it glided to the ground. The ATC transcript revealed that ATC contacted the pilot after it lost contact with the UA and after the UA transponder stopped working following engine shutdown. The pilot did not indicate that the UA had descended below the TFR altitude.

At that point, the pilot or ATC should have declared an emergency to initiate a process to provide for better surveillance of the UA, if possible, and for ATC to advise other aircraft at risk for a collision. Had an emergency been declared, controllers in adjacent facilities as well as pilots operating in the area would be alert to a missing aircraft and apply additional vigilance to assist in locating it.

Also, the Safety Board investigation revealed that the CBP did not initiate, nor did FAA offer support, in early coordination with the Western Area Defense Sector (WADS).[6] Timely coordination with WADS may have provided time-critical altitude information with height-finding radar capability when the transponder and altitude encoder quit operating.

Further, any changes to the lost-link profiles developed by the CBP and contained in the COA were supposed to have been shared with the FAA and ATC, to allow coordination between the operator and ATC in the event of a lost-link emergency. However, the investigation revealed that the CBP developed subsequent changes to the profiles contained in the COA but did not share these revised and/or new lost-link profiles with ATC.

The Safety Board concludes that the lack of advance planning between the CBP and ATC to define responsibilities in the event of a UAS emergency creates a hazard for users of the NAS. Although there was no in-flight collision and no one on the ground was injured in this accident, the Board is concerned about the potential for loss of life or more extensive property damage in the future stemming from such hazards. Therefore, the Safety Board believes that the CBP should participate in periodic operational reviews between the UAS operations team and local ATC facilities, with specific emphasis on face-to face coordination between the working-level controller and UA pilot(s), to clearly define responsibilities and actions required for standard and nonstandard UA operations. These operational reviews should include, but not be limited to, discussion on lost-link profiles and procedures, the potential for unique emergency situations and methods to mitigate them, platform-specific aircraft characteristics, and airspace management procedures.

Recording of Communications Between Unmanned Aircraft Pilots, Air Traffic Controllers, and Other Unmanned Aircraft System Assets

Aviation safety investigators have long recognized the value of cockpit voice recorders and recordings of ATC radio communications in accurately determining the facts of an accident or incident and have used that information to improve the safety of aircraft operations. During the investigation of this UA accident, Safety Board investigators found that routine radio communications between the UA pilot and ATC controllers were recorded by ATC and did provide valuable information. However, after radar contact was lost and the search for the UA ensued, additional communications by the UA pilot with ATC and other assets[7] involved in supporting the UA operation were conducted by telephone. The telephone conversations were not recorded. The lack of such recordings hampered the investigation because Board investigators could not evaluate the effectiveness of the communications between the UA pilot, ATC controllers, and other assets.

Further, the communications between UA pilots and other personnel within the GCS are not recorded. The value that cockpit voice recordings provide to accident investigations is well known. Recorded conversations between UA pilots located in the GCS as well as conversations

[6] WADS is an Air National Guard unit; its headquarters are located in Washington State. It protects skies in the western United States by detecting, identifying, tracking, and, if necessary, scrambling fighters to intercept unknown or threatening airborne objects.

[7] Assets include WADS and the Air Marine Operations Center, which is a communications center for the CBP.

with additional mission support personnel stationed in the nearby mobile GCS[8] would be of equal value. Therefore, the Safety Board believes that the CBP should require that all conversations, including telephone conversations, between UA pilots and ATC, other UA pilots, and other assets that provide operational support to UA operations, be recorded and retained to support accident investigations.

Maintenance, Troubleshooting, and Minimum Equipment Lists

A review of UAS maintenance processes and records revealed several deficiencies, some of which were a factor in this accident. Deficiencies that could result in a decreased level of safety were also identified even though they were not considered to be a factor in this accident. The first link in the chain of events that led to the accident involved a fault in the GCS, which caused PPO-1 to lock up. Review of a computer logbook kept in the GCS showed 9 lockups in a 3-month period before the accident, including 2 on the day of the accident before takeoff and another on April 19, 2006, 6 days before the accident.[9] Review of a maintenance logbook revealed no entries describing any corrective action to address the control console lockup that occurred 6 days earlier. The CBP and GA-ASI accepted the repeated console lockups as routine, correcting the fault by cycling the power to the system, without identifying the source of the lockups and rectifying the problems before further flight.

Because the source of the lockup events had not been traced to any particular component or element in the system, the full impact that lockups could have on the UAS' function was likely not fully understood. As a result, the failure to eliminate repetitive lockups invited the possibility of a more severe consequence to UA operation the next time a lockup occurred. Further, although system redundancy is provided by the ability to manually switch to backup systems, such as the PPO-2 console or the mobile GCS, continued reliance on backup systems to mitigate repeated failures reduces safety margins, diminishes the functional capability of the UAS, and, in some cases, may increase pilot workload.

Investigators also noted that there did not appear to be any process by which the UAS could be functionally tested and returned to service in a reliable manner. For example, if the console was rebooted and was functional following a lockup, the vehicle could be launched without further verification of UAS capability. Further, to address the last lockup that occurred before the launch of the accident flight, the main processor circuit board was switched between the two consoles. Switching main processor circuit boards between consoles may be an appropriate interim troubleshooting step in an attempt to isolate the problem; however, it should not be used as a corrective action to clear a UA for launch, as occurred in this case, because it may simply transfer an unresolved problem to the backup console.

[8] The mobile GCS is a smaller, second GCS available on site, from which the UA can be controlled. It can serve as a backup to PPO-1 or PPO-2, if needed.

[9] The Safety Board was recently made aware of a second CBP Predator B incident that occurred on November 17, 2006. The CBP advised that, while flying a new Predator B UA on an experimental mission in a restricted area, a console lockup occurred and the pilot commanded the UA to return to the departure airport. During landing, the UA's camera interface malfunctioned, which altered the camera view. As a result, the pilot inadvertently steered the UA off the side of the runway. The UA sustained minor damage.

Typically, complex systems require in-depth troubleshooting, repair, and verification procedures for return to service. Neither the CBP nor its contractors had a documented maintenance program that ensured that maintenance tasks were performed correctly and that comprehensive root-cause analyses and corrective action procedures were required when failures, such as console lockups, occurred repeatedly. As a result, maintenance actions could not be relied upon to be effective or repeatable, which is a critical factor in ensuring airworthiness.

The Safety Board notes that the primary purpose of aircraft maintenance programs is to ensure that an aircraft is in safe condition and properly maintained for its intended operation. The Board's investigation revealed that the accident UA was dispatched with unresolved system deficiencies that caused the GCS to lock up as it had done on previous missions. Investigators found that the CBP had no effective mechanism in place to ensure such deficiencies were permanently resolved before further flight and to maintain the continued airworthiness of these UASs. Therefore, the Safety Board believes that the CBP should identify and correct the causes of the console lockups. Also, the Safety Board believes that the CBP should implement a documented maintenance and inspection program that identifies, tracks, and resolves the root cause of systemic deficiencies and that includes steps for in-depth troubleshooting, repair, and verification of functionality before returning aircraft to service.

Further, because the CBP UA operation is considered public use, the FAA is not responsible for overseeing many aspects of the CBP's UAS program.[10] The CBP must fulfill the roles of the regulator (which normally conducts oversight of operators) as well as the operator of its UASs; thus, the CBP must not only establish an effective maintenance program plan for its UA operation but also must monitor its implementation. Although the CBP had delegated many aspects of the Predator B operation to its contractor, GA-ASI, the CBP had insufficient infrastructure in place to oversee GA-ASI in its role to provide continued airworthiness and maintenance of its UASs. The Safety Board's investigation revealed that the CBP staff overseeing the maintenance work done by GA-ASI on the CBP's UASs did not possess expertise in areas such as engineering and maintenance, which are necessary to effectively evaluate the adequacy of and compliance with maintenance program goals. Therefore, the Safety Board believes that the CBP should require that aviation engineering and maintenance experts oversee the definition of maintenance tasks, establishment of inspection criteria, and the implementation of such programs. The CBP also should ensure oversight of contractor(s) implementing such programs.

The investigation also revealed that the CBP lacked a plan to manage the potential risks associated with operating a UAS with inoperative components. For example, review of maintenance records revealed that the satellite communication control function of PPO-2 was inoperative due to an unresolved component problem. Operating without such an important function should have been carefully evaluated against predefined guidelines or mandates using a minimum equipment list (MEL) and dispatch deviations guide.[11] These documents are

[10] The FAA has limited oversight authority over public-use aircraft operations.

[11] An MEL is typically developed by an airframe manufacturer and approved by an industry flight operations evaluation board. The MEL allows operators to safely dispatch an aircraft with an inoperative component or system. The dispatch deviations guide provides procedures for maintenance crewmembers to follow to correctly disable the component or system and label the associated item in the cockpit to make flight crews aware of the inoperative item.

developed with careful thought about how the operation or flight may be affected if certain components fail. However, the CBP's system lacked an MEL and dispatch deviations guide that could have been used to determine if an acceptable level of safety or reliability could have been achieved for the flight. An MEL and dispatch deviations program would provide a standardized process to guide maintenance personnel to determine if a UA should be dispatched with an inoperative component. MELs and dispatch deviation guides also remove the option to operate with certain inoperative components or without alternate plans to safely and reliably complete a mission. Without such specific guidance, UAs may be dispatched with known inoperative components that could result in unintended consequences, especially if other critical components fail unexpectedly in flight.

The development of an MEL and dispatch deviation guide would also provide a source of information to define spare-parts requirements. The investigation also disclosed that spare parts were virtually nonexistent at the facility. Although neither the lack of a MEL nor the lack of spare parts was a factor in this accident, these findings highlight a weakness in the operation of the UAS. Therefore, the Safety Board believes that the CBP should develop MELs and dispatch deviation guides for its UAS operations. In addition, the Safety Board believes that the CBP should assess the spare-parts requirements for its UAS operations to ensure the availability of parts critical to UA launch, as defined by the MEL requirements.

Unmanned Aircraft System Pilot Training and Emergency Procedures Training

The CBP's training records showed that the GA-ASI accident pilot was experienced in flying Predator A UASs (519 hours); however, he had logged only 27 hours in a Predator B UAS. This is significant because the Predator B has a different engine and more complex engine controls than the Predator A. For example, the control console for the Predator A does not have a condition lever, the positioning of which caused the engine to be inadvertently shut down in this accident. The Safety Board's investigation revealed that the CBP's pilot experience requirements were general: 200 manned aircraft time and 200 hours of UAS time. No model-specific flight time requirements exist for UASs. A syllabus from the accident pilot's training showed that the syllabus referenced emergency procedures, but neither the syllabus nor the pilot's flying training record specified which emergency procedures were reviewed or practiced in training.

Interviews with the pilot and others present during the emergency indicated the pilot's initial response to the console lockup was to call, via cell phone, the instructor pilot who was located in a building across the ramp. Interviews also revealed that there was confusion in the GCS and that the pilot did not follow the console lockup checklist procedure although it was available at the console. For example, because this was a single-pilot operation, the flight manual called for an avionics technician to replace the CBP camera operator at the PPO-2 console to assist the pilot in performing appropriate portions of the console lockup checklist procedure. Though an avionics technician was present, the pilot moved to PPO-2 and did not request the assistance of the sensor operator.

As previously discussed, the pilot did not correctly transfer control from the PPO-1 console to the PPO-2 console. In addition, the COA outlined operational emergency procedures to notify and coordinate with ATC in response to an emergency. The investigation found that the pilot did not perform many of the defined actions.

Based on the accident pilot's response to the emergency, the Safety Board concludes that the pilot was not proficient in the performance of emergency procedures. Therefore, the Safety Board believes that the CBP should revise its pilot training program to ensure pilot proficiency in executing emergency procedures.

Unmanned Aircraft System Safety Risk Management

During its investigation, the Safety Board evaluated the CBP's safety control plans, which include equipment design features, operational procedures, pilot training and proficiency, and maintenance. Overall, investigators found that, although the CBP had implemented some operational safety controls, these controls did not prevent a console lockup from leading to an accident. Also, given the frequency of Predator B UAS console lockups, the occurrence of the two lockup-induced engine shutdowns, and previously noted deficiencies with the system's human interface, the Board is concerned that a single pilot may not be adequate to ensure safe operation of the UAS.

For example, flight testing of remotely piloted vehicles at various flight test ranges commonly requires two pilots as well as a range safety officer and a flight safety officer.[12] Although UA operations such as those conducted by the CBP are generally routine and a single pilot may be able to adequately manage the routine operations, an emergency or unusual operational situation may quickly overload a single pilot, as was demonstrated in this accident. Therefore, the Safety Board believes the CBP should require that a backup pilot or another person who can provide an equivalent level of safety as a backup pilot be readily available during the operation of a UAS.

Additionally, given the widespread nature of the deficiencies uncovered by the Safety Board's investigation, the Board is concerned that additional potential shortcomings could still exist in the CBP's safety control plan for its UASs. The CBP indicated to Board investigators that it did not use a system safety process,[13] to evaluate the potential safety risks of its UA operation or as part of its most recent postaccident program review. Because the CBP did not require GA-ASI to perform a comprehensive system safety assessment on its Predator B UAS, the Board is concerned that hazards arising from equipment malfunctions may not have been thoroughly evaluated and appropriate safety requirements and controls put in place, such as design safety objectives,[14] cautions and warnings, irregular and emergency operating procedures, and safety-critical maintenance tasks and inspections. This further supports the Board's concerns that additional, unmitigated safety risks may exist in the CBP's UA operation.

---

[12] Typically, a range safety (or range control) officer coordinates the range functions, including ATC, radar, cameras, etc.; a flight safety officer ensures that the aircraft stays over the range or that it has flight recovery or termination capability. The flight safety officer operates independently from the other UAS team members. If the operator (in the case of this accident, the CBP) has a proven track record, it need not send a range safety officer, but the operator must be in direct communication and coordinate with range safety staff.

[13] As noted by the FAA System Safety Handbook, a system safety process is one that proactively identifies, assesses, and eliminates or controls safety-related hazards to acceptable levels to achieve accident prevention.

[14] For manned civil aircraft operating in the NAS, the qualitative design safety objective is that a logical and acceptable inverse relationship exists between the probability and the severity of each failure condition. FAA Advisory Circular 25.1309-1A defines a failure as a loss of function or a malfunction of a system or a part thereof and a failure condition as the effects on the airplane and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operational or environmental conditions.

Given the ineffective and inadequate safety controls discovered in this investigation, the Safety Board is concerned that the CBP operation may lack an effective plan to control safety risks in the future. The Safety Board concludes that the CBP must develop an operational safety plan using a methodical system safety process. This process could help the CBP address the widespread deficiencies noted in this investigation as well as other presently unmitigated safety risks. It also could ensure development of a suitable monitoring program that tracks and analyzes malfunctions and incidents and incorporates lessons learned from other operators of similar UASs. This monitoring program could ensure that the safety plan remains effective throughout the UAS' lifecycle. Therefore, the Safety Board believes that the CBP should develop a safety plan, which ensures that hazards to the NAS and persons on the ground introduced by its UAS operation are identified and that necessary actions are taken to mitigate the corresponding safety risks to the public over the life of the program. The plan should include, as a minimum, design requirements, emergency procedures, and maintenance program requirements to minimize the safety impact of UAS malfunctions in flight, continuous monitoring of the CBP's UA operation, analysis of malfunctions and incidents, and lessons learned from other operators of similar UAS designs.

Therefore the National Transportation Safety Board recommends that the U.S. Customs and Border Protection:

> Require General Atomics Aeronautical Systems, Inc., to modify the unmanned aircraft system to ensure that inadvertent engine shutdowns do not occur. (A-07-70)
>
> Require General Atomics Aeronautical Systems, Inc., to modify the unmanned aircraft system to provide adequate visual and aural indications of safety-critical faults, such as engine-out conditions and console lockups, and present them in order of priority, based on the urgency for pilot awareness and response. (A-07-71)
>
> Review the U.S. Customs and Border Protection's methods of developing lost-link mission profiles to ensure that lost-link mission profile routes minimize the potential safety impact to persons on the ground, optimize the ability to recover the data link, and, in the absence of data-link recovery, provide the capability to proceed to a safe zone for a crash landing. (A-07-72)
>
> Following completion of the action requested in Safety Recommendation A-07-72, require that pilots be trained concerning the expected performance and flightpath of the unmanned aircraft during a lost-link mission. (A-07-73)
>
> Require that the unmanned aircraft system be modified to ensure that the transponder continues to provide beacon code and altitude information to air traffic control even if an engine shuts down in flight and that the pilot is provided a clear indication if transponder function is lost for any reason. (A-07-74)

Review all unmanned aircraft system (UAS) functions and require necessary design changes to the UASs that the U.S. Customs and Border Protection operates to ensure that electrical power is available for an appropriate amount of time to all systems essential to unmanned aircraft control following loss of engine power. (A-07-75)

Develop a means of restarting the unmanned aircraft (UA) engine during the lost-link emergency mission profile that does not rely on line-of-sight control, for example, through an autonomous capability in the unmanned aircraft system's control system or through use of control functions enabled via a backup satellite communication system available to the pilot on the ground. (A-07-76)

Participate in periodic operational reviews between the unmanned aircraft system operations team and local air traffic control facilities, with specific emphasis on face-to-face coordination between the working-level controller and unmanned aircraft (UA) pilot(s), to clearly define responsibilities and actions required for standard and nonstandard UA operations. These operational reviews should include, but not be limited to, discussion on lost-link profiles and procedures, the potential for unique emergency situations and methods to mitigate them, platform-specific aircraft characteristics, and airspace management procedures. (A-07-77)

Require that all conversations, including telephone conversations, between unmanned aircraft (UA) pilots and air traffic control, other UA pilots, and other assets that provide operational support to UA operations, be recorded and retained to support accident investigations. (A-07-78)

Identify and correct the causes of the console lockups. (A-07-79)

Implement a documented maintenance and inspection program that identifies, tracks, and resolves the root cause of systemic deficiencies and that includes steps for in-depth troubleshooting, repair, and verification of functionality before returning aircraft to service. (A-07-80)

Require that aviation engineering and maintenance experts oversee the definition of maintenance tasks, establishment of inspection criteria, and the implementation of such programs. Also, ensure oversight of contractor(s) implementing such programs. (A-07-81)

Develop minimum equipment lists and dispatch deviation guides for the U.S. Customs and Border Protection's unmanned aircraft system operations. (A-07-82)

Assess the spare-parts requirements for U.S. Customs and Border Protection's unmanned aircraft operations to ensure the availability of parts critical to unmanned aircraft launch, as defined by the minimum equipment list requirements. (A-07-83)

> Revise U.S. Customs and Border Protection’s pilot training program to ensure pilot proficiency in executing emergency procedures. (A-07-84)

> Require that a backup pilot or another person who can provide an equivalent level of safety as a backup pilot be readily available during the operation of an unmanned aircraft system. (A-07-85)

> Develop a safety plan, which ensures that hazards to the National Airspace System and persons on the ground introduced by the U.S. Customs and Border Protection’s (CBP) unmanned aircraft system (UAS) operation are identified and that necessary actions are taken to mitigate the corresponding safety risks to the public over the life of the program. The plan should include, as a minimum, design requirements, emergency procedures, and maintenance program requirements to minimize the safety impact of UAS malfunctions in flight, continuous monitoring of the CBP’s unmanned aircraft operation, analysis of malfunctions and incidents, and lessons learned from other operators of similar UAS designs. (A-07-86)

The Safety Board also issued five safety recommendations to the Federal Aviation Administration. In your response to the recommendations in this letter, please refer to Safety Recommendations A-07-70 through -86. If you need additional information, you may call (202) 314-6177.

Chairman ROSENKER, Vice Chairman SUMWALT, and Members HERSMAN, HIGGINS, and CHEALANDER concurred with these recommendations.

[*Original Signed*]

By: Mark V. Rosenker
Chairman