The Hidden Human Factors in Unmanned Aerial Vehicles

Chris. W. Johnson, DPhil; Department of Computing Science, University of Glasgow, Scotland, UK.

Christine Shea, PhD; ESR Technology Ltd, Birchwood Park, Warrington, Cheshire, UK.

Keywords: UAV, UAS, accident analysis; organisational safety.

Abstract

In April 2006, an Unmanned Aerial Vehicle crashed near Nogales, Arizona. This incident is of interest because it triggered one of the most sustained studies into the causes of failure involving such a vehicle. The National Transportation Safety Board together with the US Customs and Border Protection agency under the Department of Homeland Security worked to identify lessons learned from this mishap. The crash at Nogales is also of interest because it illustrates an irony of Unmanned Aircraft Systems operations; the increasing reliance on autonomous and unmanned operations is increasing the importance of other aspects of human-system interaction in the cause of major incidents. The following pages illustrate this argument using an accident analysis technique, Events and Causal Factors charting, to identify the many different ways in which human factors contributed to the loss of this Predator B aircraft.

Introduction

The term Unmanned Aerial Vehicles (UAVs) refers to the airborne component of the wider Unmanned Aircraft Systems (UAS') that support the operation of a growing class of complex, safety-critical applications. Within the US military alone funding for UAS development has increased from $3 billion in the early 1990s to over $12 billion for 2004-2009 [1]. It has been estimated that the civil UAS market would reach €100 million (US $129.6 million) annually by 2010. This expenditure is intended to support a wide variety of surveillance and reconnaissance operations including the monitoring of forest fires, oil spills, contaminant clouds, algae bloom and border security.

The use of UAVs is typically intended to 'keep humans out of harm's way' – until things go wrong. As early as 2001 the UAV accident rate was considered significantly higher than that of manned aircraft [2]. However Nullmeyer et al note that even within common platforms, different analysts have attributed the same accident data to different causes [1]. Their review of Air Force Predator mishaps identified mechanical problems as a significant cause although it would seem that mechanical failures are decreasing with improvements in UAS [2]. In contrast, attention has begun to focus on human factors issues including shortfalls in individuals' skill and knowledge (checklist error, task mis-prioritization, lack of training for task attempted, and inadequate system knowledge), situation awareness (channelized attention), and crew coordination.

This paper illustrates the many different ways in which human intervention determines the success or failure of UAS operations. These include strategic, management decisions that help create the context for both the systems engineering and operations teams that monitor and control UAVs. They also include the regulatory framework that, in turn, influences every level of UAS operations. The complex nature of these applications can make it difficult to trace the different interactions between management and regulation, between operational staff and their support teams. It is for this reason that the following pages focus on a single accident involving a Predator Type B UAV. The intention is to focus on particular examples of the problems that can arise in the human factors of UAS operation in order to illustrate the more general issues that increasingly complicate the use of these safety-critical systems.

Overview of the Nogales Predator Mishap

In the early hours of 25th April, 2006, a Predator Type B UAV manufactured by General Atomics Aeronautical Systems, Inc. (GA-ASI), crashed northwest of Nogales International Airport, Arizona. Although it landed in a sparsely populated residential area, there were no injuries but there was substantial damage to the aircraft. The UAV was owned by the US Customs and Border Protection (CBP) agency but at the time of the crash was being operated under contract with GA-ASI. This commercial relationship is explained by the CBP's requirement to rapidly increase their use of unmanned surveillance aircraft to improve security along the United States' southern borders.

The Predator B is a turboprop aircraft with redundant, fault-tolerant avionics. It can be flown by a remote pilot or autonomously. It was designed as a long-endurance, high-altitude platform with a wingspan of 66 feet, a maximum weight of 10,000 pounds and a maximum speed above 220 knots. The National Transportation Safety Board (NTSB) coordinated the immediate investigation of the mishap [3]. They argued that the loss of the Predator was caused by the pilot's failure to use an appropriate checklist when switching control from one pilot payload operator position (PPO-1) to another (PPO-2). In making this change, he forgot to alter the position of the controls in the new position. This resulted in the fuel valve inadvertently being shut off, which in turn starved the engine. The decision to focus on this mishap is justified by the level of detail provided by the NTSB account. It is also motivated by the manner in which regulatory and organizational factors contributed to the context in which the operator 'error' was likely to jeopardize mission success.

Mapping Out the Context of the Nogales Mishap

Figure 1 uses a simple graphical formalism to map out the loss of the Predator. Events and Causal Factors (ECF) diagrams were originally developed by the US Department of Energy. It is important to stress, however, that this is only one of several different notations that might be used to provide a similar overview. Events are represented as rectangles. For example, the pilot's discovery that the PPO-1 console had locked-up, in turn, led him to transfer control to the second PPO-2 position. The prefix numbers in each event denote the page in the NTSB (2007) report where evidence is provided about these observations. Where an event is labelled 'Assum' then the analysts have introduced assumptions into their model which should be subject to further analysis as part of subsequent investigations. This initial transfer of control led to the fuel supply being cut. The PPO levers were used to perform different functions depending on whether PPO-1 or PPO-2 was being used to control the aircraft. If PPO-1 controls flight then the condition lever for PPO-2 controls the iris setting for the on-board camera. However, if control is transferred from PPO-1 to PPO-2 then this lever is used to open and close the fuel valve. It is, therefore, critical that pilots alter the position of these levers from the previous camera setting to an appropriate fuel valve position before moving flight control from PPO-1 to PPO-2.

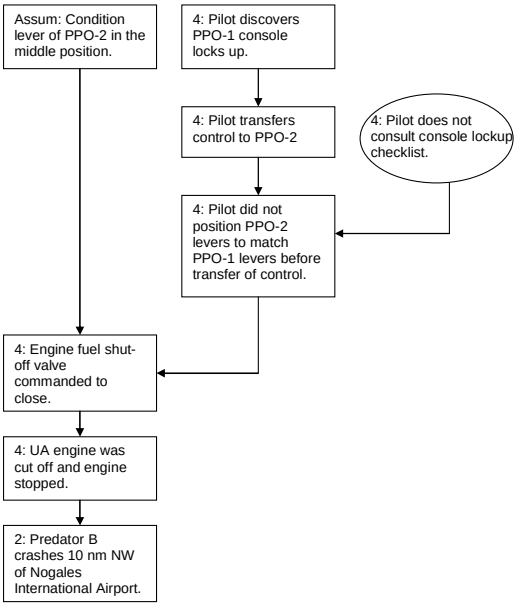

Figure 1: Preliminary Overview of UAV Crash

Figure 1 also includes the conditions that make particular events more likely. These are denoted by ovals. In this example, the pilot did not consult the procedural checklist associated with console failures and this contributed to his 'error' in not ensuring that the control levers had the same settings when they moved to PPO-2. Figure 1 only provides an initial overview of the immediate events surrounding the loss of the Predator. It does not explain the reasons the pilot failed to consult an appropriate checklist nor does it consider the factors that contributed to the failure of the PPO-1 console in the first place. These are important omissions; several of the previous studies in this

area have been content simply to identify the frequency of operator error or of maintenance failure in UAV incidents without taking the analysis any further. This results in forms of analysis that are often superficial and which fail to reflect the wider lessons that can be learned from those mishaps that have occurred. To avoid such a superficial analysis, Figure 2 extends the previous ECF diagram to consider the contributory factors that indirectly led to the problems with the PPO-1 control position. One important factor was a culture in which 'work arounds' were routinely accepted to enable safety-critical operations to continue. Previous papers have emphasised the hazards associated with long term acceptance of 'degraded modes of operation' [4]. Maintenance procedures were often poorly documented and so there was a lack of information about the corrective actions that were taken following nine previous 'lock up' failures in the three months before this incident. The high number of previous failures and the inadequate maintenance actions may also have reflected deeper problems in the risk assessment practices that were intended to guide the operation of the CBP UAS programme. As can be seen in figure, these diverse contributory factors can all be associated with the CBP's dual role both in operating the missions and in regulating the programme. Security considerations partly justify the FAA's delegation of regulatory responsibility through the CBP's certificate of authorisation. It can be argued that an independent regulator might have been more proactive in address the safety management concerns that are summarised in the contributory factors of Figure 2.

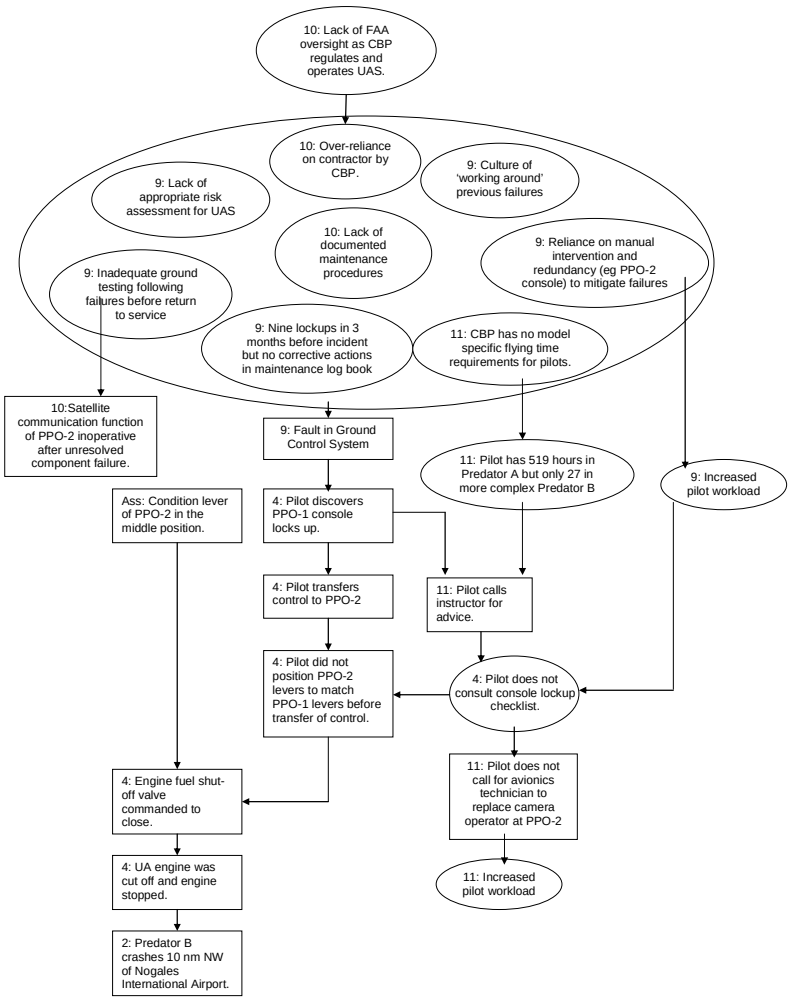

Figure 2: Contextual Factors Leading to the PPO-1 'Lock-Up' and the Initial Pilot 'Error'

Figure 2 also provides a high-level overview of the factors that contributed to the failure to follow a recommended checklist when the PPO-1 control position locked-up. In this case, specific links are drawn from the more general cluster of contributory factors. The CBP did not set specific flying time requirements for particular models of UAV. At the time of the accident, the sole pilot in charge of the ground control system had only 27 hours of

experience on the Predator B. This arguably was insufficient for him to be familiar with detailed emergency procedures even though he had more than 500 hours on the simpler Predator A. This argument provides an indirect explanation for the failure to use an emergency check-list. Given his lack of experience with the platform, the pilot contacted an instructor over the telephone. He may have assumed that this was sufficient given that he was already operating under higher levels of workload as he struggled to find a work-around from the failure to PPO-1.

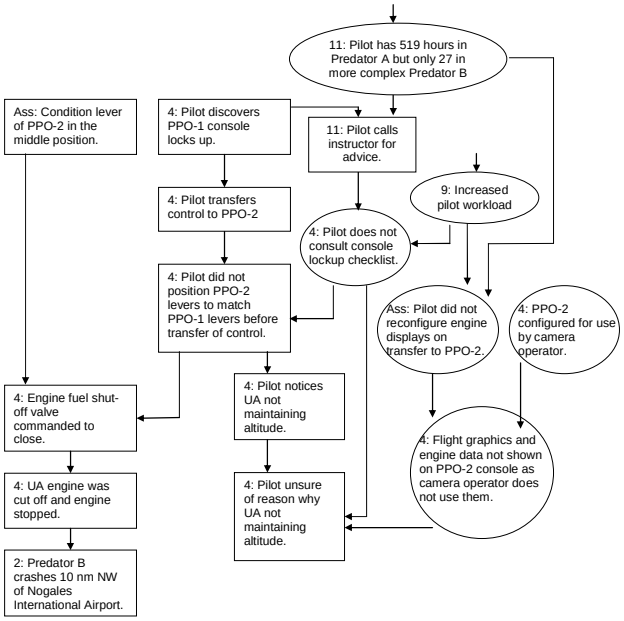

Figure 3: Recovery Problems after Initial Problems Noticed

The opening sections of this paper described how the Predator Type B can be flow either autonomously or under direct control from the ground based pilot. One of the benefits of using this mixed approach is the flexibility that is provided by enabling operators to intervene and respond during degraded modes of operation. It is for this reason that Figure 3 focuses on the attempts by the two-person ground control team to both diagnose and then resolve the immediate problem that arose when the transfer of working positions triggered fuel starvation to the UAV's engines. In particular, the bottom right contributory factors denote that the PPO-2 displays remained configured for the camera operator. This may have prevented the pilot from observing the engine monitoring data that was indicating a fuel starvation problem. The reason for this was that under normal operation the camera operator would have no need for the engine data. The high operational workload involved in the transfer of positions following the 'lock up' of PPO-1 and the failure to use a recommended checklist also help to explain the failure to successfully reconfigure the displays as the pilot began operations from PPO-2. Equally, research in interface design has shown that detailed development decisions in the Human-Machine Interface (HMI) for UAS applications contributed to the pilots problems. Similar systems have been developed to automatically configure displays whenever there is a change in controller position. If this had been available at the time of this Predator mishap then the pilot need not have been required to explicitly reconfigure the PPO-2 display to present essential engine management data.

Figure 4 continues this analysis of the HMI issues that contributed to the Nogales UAS mishap. It records the observation that engine data and fault annunciations were presented on the left heads down display areas for both PPO-1 and PPO-2. However, this information was integrated with a mass of other parameters and that this may have contributed to the pilot's uncertainty over the cause of the UAV's loss of altitude. There was no unique aural alert for the loss of thrust. The reliance on non-specific alerts removed an additional cue that might have prompted the crew to look in this area of their displays. The problems of information presentation and filtering combined with the high workload, noted in previous sections, to undermine the situation awareness of the pilot as they struggled to understand the UAV's loss of altitude. This was compounded by a concern that PPO-2 might also lock-up following the failure of the pilot's initial work station. This was a significant concern given that previous failures had been resolved by swapping the circuit cards between the work stations – increasing the chance of future

problems with the secondary control position. The PPO-2 head-up display was not being updated as the pilot struggled to diagnose the underlying causes of the problems with the Predator.

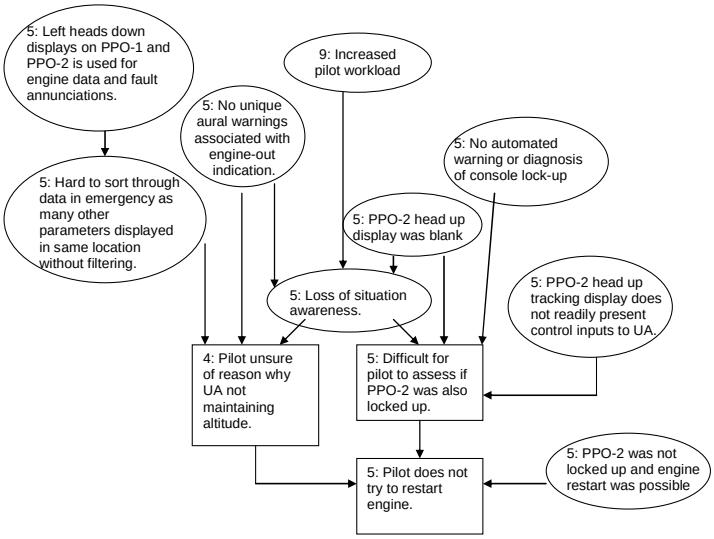

Figure 4: HMI Issues Connected to Recovery Problems

The pilot's problems were compounded by the immediate consequences of the loss in altitude once fuel had been cut to the engines of the UAV. Once direct data communications with the aircraft have been cut, the UAV follows a pre-programmed, autonomous flight-path known as the 'Lost Link Mission Profile'. This is intended to provide pilots and technicians with an interval of time during which they can take steps to restore the line of sight data link to the UAV. Figure 5 summarises the problems in tracing the vehicle's movements on the lost link profile.

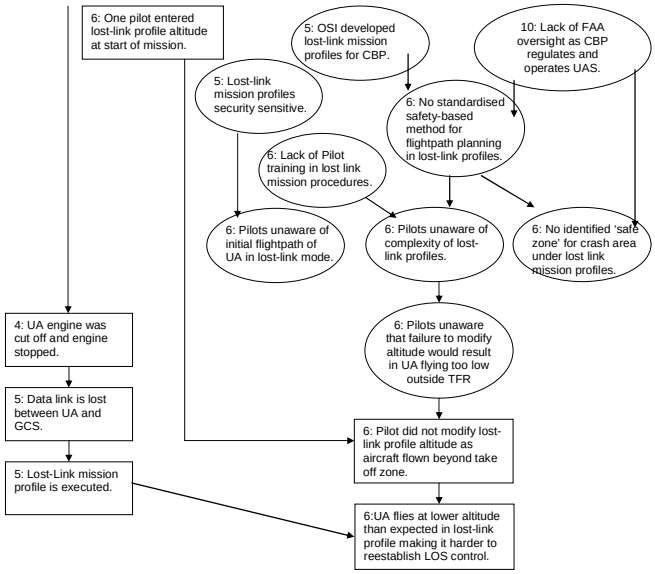

Figure 5: Lost-Link Mission Profile Issues

As can be seen, one of the pilots is responsible for programming the lost link altitude at the start of the mission. The exact nature of this route is considered to be security sensitive by the CBP. However, this creates a number of problems given the lack of external regulatory oversight that might otherwise be expected for such a critical routing. There was no standardised form of risk assessment to consider the possible consequences and likelihood of collision

with ground obstacles, including conurbations, during the planning of lost link profiles. Subsequent investigations concluded that the profiles did not adequately identify 'safe zones' where a UAV could ditch as it followed the lost link manoeuvres. These factors were compounded by the pilots' lack of experience and expertise in tracing the probable course of a UAV as it followed one of these profiles. They were, typically, unaware of the complex set of trajectories that were used to help re-establish data ink communications. This in turn may explain why the pilot in this accident failed to understand the importance of modifying the lost link altitude setting if the UAV was operated away from the original mission area. This was important if the vehicle was to have sufficient altitude to avoid descending outside temporary flight restriction (TFR) airspace. The term TFR is used to describe an area in which other aircraft can only enter if they explicitly contact Air Traffic Controllers; the intention is to minimise any potential conflicts with unmanned or autonomous vehicles. This accident illustrates how the regulations and procedures governing the air traffic management of UAVs are in a state of flux – it seems clear that many of the assumptions that govern the operation of existing airspace can have dangerous consequences with this new generation of systems. The loss of altitude had further consequences, not only did it lead to an incursion beyond the TFR but it also created further problems as attempts were made to re-establish data link communications.

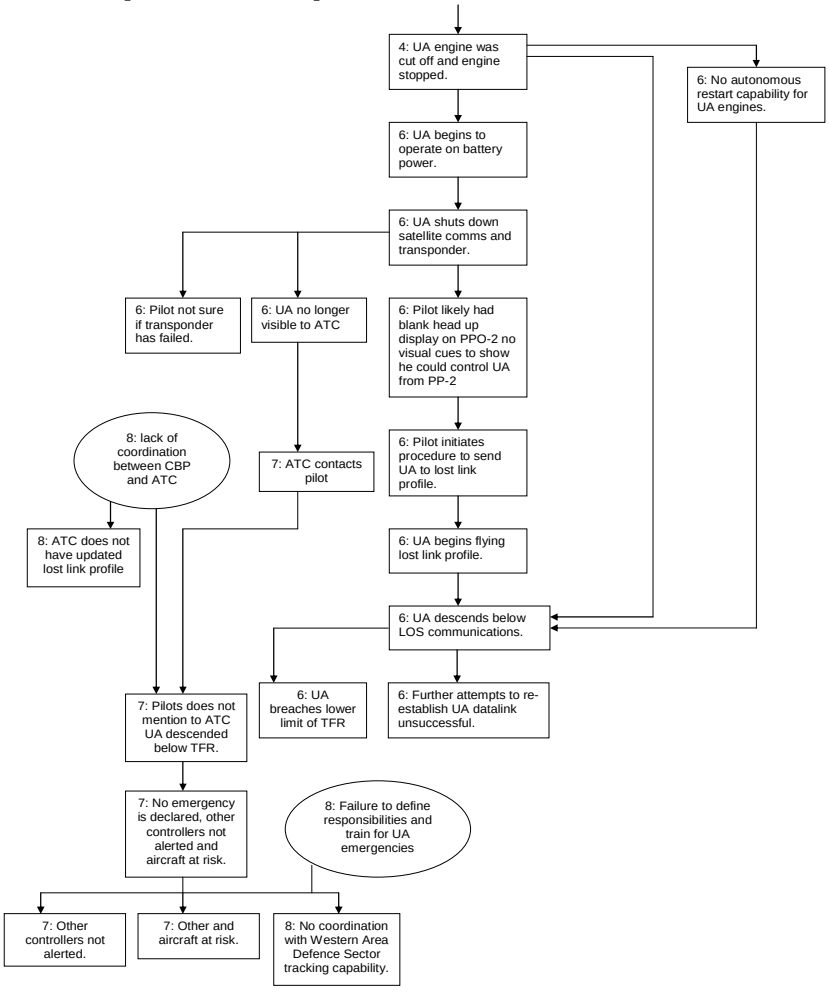

Figure 6: Loss of Electrical Power and Engine Restart Capability

Figure 6 summarises the knock-on effects that exacerbated the initial problems created by the loss of engine power to the Predator. This ECF diagram extends the previous analysis to consider the interaction between the pilot and other stakeholders, including local Air Traffic Management. After the Predator lost engine power, it began to rely on battery reserves. This triggered the UAV to shut down satellite communications, increasing the importance of re-establishing the line of sight data links. The aircraft also responded to the loss of engine power by disabling the transponder that Air Traffic Management systems used to track the UAV. The pilot could not immediately see

whether or not the transponder was still working. Fortunately, Air Traffic Management staff contacted the pilot to determine whether or not he could explain the sudden loss of contact with the Predator. This and subsequent interactions between the ATM and CBP staff were compromised by a number of long standing problems. In particular, ATM staff were not provided with detailed information about the lost link profiles used by the UAVs. It is unclear whether this lack of communication was justified by security concerns or was the result of underlying problems in inter-agency coordination. In either case, the pilot failed to inform the ATC officer that the aircraft might have descended below the TFR and out of controlled airspace. The lack of coordination and of regular exercises for emergencies involving UAV platforms may also explain why the pilot and his co-workers did not seek assistance from the Western Area Defence Sector which had a range of systems for tracking the UAV in the minutes before it came down in a residential area.

Conclusions and Further Work

In April 2006, an Unmanned Aerial Vehicle crashed near Nogales, Arizona. This incident is of interest because it triggered one of the most sustained studies into the causes of failure involving a UAS. The National Transportation Safety Board together with the US Customs and Border Protection agency under the Department of Homeland Security worked to identify lessons learned from this mishap. The crash at Nogales is also of interest because it illustrates an irony of UAV operations; the increasing reliance on autonomous and unmanned operations is increasing the importance of other aspects of human-system interaction in the cause of major incidents. This paper has used an accident analysis technique, Events and Causal Factors charting, to identify the many different ways in which human factors contributed to the loss of this Predator B aircraft.

We have seen how the pilot failed to use an approved procedure when responding to a 'lock up' in the PPO-1 console. In consequence, a control lever on the alternate PPO-2 workstation was left in a position that was appropriate for its previous use as a camera console but which was interpreted as a command to close the engine fuel valve when the pilot designated PPO-2 as the new flight control interface. Although the use of an approved checklist or procedure might have helped the pilot to identify the need to reset the PPO-2 control levers, it is important not to ignore the systemic causes of this incident. In particular, the lack of adequate maintenance management systems meant that little attempt had been made to resolve previous incidents in which the control systems had frozen. Instead, operators began to form a culture of 'making do' or of finding 'work arounds' to degraded modes of operation. This included the swapping of 'failed' circuit boards between the PPO-1 and PPO-2 positions. In such circumstances, it was highly likely that these ad hoc strategies would eventually fail to ensure safe and successful operation of the UAV platform.

We have also seen how human intervention played a critical role in emergency response even after the Predator went into fully autonomous flight. The lack of coordination and emergency planning between the CBP, Air Traffic Management and organisations including the Western Area Defence Sector was exposed in the minutes after contact was lost. Not only was it difficult for ATM personnel to identify the risks of possible incursions as the UAV strayed beyond the TFR zone, the pilot had insufficient knowledge about the lost link profile that he could not provide the detail that they needed. This mishap revealed a pressing need for safety management structures to be used beyond the design phases involved in UAV construction. It revealed the importance of adequate incident reporting and of accurate maintenance logs during operational service. It also illustrated the need for structured risk assessment techniques to inform detailed mission planning, in particular to guide the identification of 'crash zones' within lost link profiles.

We would argue that further work needs to focus on two key areas – degraded modes of operation and contingency planning. 'Degraded modes of operation' describes failures of critical components that can gradually erode safety margins but which need not prevent an application from being used to achieve its intended function. In other words, operators can find 'work arounds' that get the job done but which may also threaten the safety of operators and the general public. In contrast, contingency operations refer to the response that organisations plan for the total failure of a safety-critical control system. It can be argued that because UAV's do not carry aircrew, there has been a temptation to find work-arounds that would never be allowed within other areas of aviation. The 'hot swapping' of a failed circuit board between operational avionics systems is not recommended practice in most airlines but has been described in several UAV incidents. Similarly, it might be argued that an undue level of complacency has also

undermined contingency planning within these operations. Too little thought is often given to the coordination that is needed when large, unmanned or autonomous flying vehicles unintentionally stray from controlled airspace.

References

1. R.T. Nullmeyer, G.A. Montijo, R. Herz, R. Leonik, Birds of Prey: Training Solutions to Human Factors Issues, The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC), 2007.

2 K.W. Williams, A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications. (December 2004), DOT/FAA/AM-04/24, Office of Aerospace Medicine.

3 NTSB, Safety recommendation A-07-70 through -86: Loss of a Type—B Predator 10 nautical miles northwest of Nogales International Airport, Nogales, Arizona, April 25, 2006. Washington DC, USA, October 2007.

4. C.W. Johnson and C. Shea, The Contribution of Degraded Modes of Operation as a Cause of Incidents and Accidents in Air Traffic Management. In Proceedings of the 2007 International Systems Safety Society Conference, Baltimore, USA, 2007.

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.

Christine Shea, M Ed, PhD, ESR Technology Ltd, Whittle House, Birchwood Park, Warrington, Cheshire, WA3 6FW. E-mail - christine.shea@esrtechnology.com

Christine Shea is a principal consultant in safety and risk management with ESR Technology. Her work involves the management of risk in complex, safety-critical domains including aviation, rail, the petroleum industry and health care. Her research interests include the management and organisation of work in safety critical domains, safety culture, the development and implementation of incident reporting systems and human error.