The Analysis of a Friendly Fire Accident using a Systems Model of Accidents*

N.G. Leveson, Ph.D.; Massachusetts Institute of Technology; Cambridge, Massachusetts Polly Allen, Margaret-Anne Storey, Ph.D.; University of Victoria; Victoria, Canada

Keywords: accident analysis, accident models

Abstract

In another paper presented at this conference, Leveson describes a new accident model based on systems theory [2]. In this model, accidents are understood in terms of a lack of adequate control over safety at each level of the socio-technical control structure in which the accident occurred. In order to evaluate this model, we have applied it to the accidental shootdown in 1994 of two U.S. Army Black Hawk helicopters by two U.S. Air Force F-15s in the no-fly-zone over northern Iraq. Because of the complexity of the accident process and limitations in the length of this paper, only an incomplete description of the accident analysis can be provided. Examples taken from the complete analysis [1] are provided to show how the new accident model can be applied. The model has the potential for supporting new types of hazard analysis that better handle software, human decision-making, and organizational and social factors than current approaches.

Background

After the Persian Gulf War, Operation Provide Comfort (OPC) was created as a multinational humanitarian effort to relieve the suffering of hundreds of thousands of Kurdish refugees who fled into the hills of northern Iraq during the war. The goal of OPC was to ensure the security of relief workers assisting Kurdish refugees and to provide a safe haven for the resettlement of the refugees. In addition to the operations on the ground, a major portion of OPC's mission was to occupy the airspace over northern Iraq. To accomplish this task, a no-fly-zone (NFZ) was established that included all airspace within Iraq north of the 36th parallel. The coalition also established a security zone for the Kurds inside the NFZ, into which no Iraqi military could enter.

On April 14, 1994, two U.S. Air Force F-15's patrolling the NFZ shot down two U.S. Army Black Hawk helicopters carrying 26 people including 15 U.S. citizens and 11 others (British, French, and Turkish military officers as well as Kurdish citizens). Everyone was killed in one of the worst air-to-air friendly fire accidents involving U.S. aircraft in military history.

Both flights were flying under the control of an AWACS (Airborne Warning and Control Systems) aircraft, the most advanced system of its type in the world. The weather was clear, all the sophisticated electronic and technical systems appeared to be operational, and the people involved were all highly trained and experienced. After two years and hundreds of hours of extensive investigation by accident boards, autonomous Army and Air Force teams, investigative reporters, lawyers, and congressional committees and their staff, no single cause was identified. According to an Air Combat Command official who was familiar with the official investigations, over 130 different mistakes were identified as being involved in the shootdown [5].

Several analyses of the accident have been provided beyond the official investigation board report, most notably books by Scott Snook [4] and Laura Piper, the mother of one of the Army officers killed [3]. The GAO also wrote a report that evaluated the official accident reports [5]. Each of these sources gives different explanations of the accident, in some aspects significantly different, due to a focus on different factors involved. In this paper, we use a control-based accident model to try to separate fact from interpretations of those facts and to provide a more complete and independent analysis of the accident

^{*}This research was partially supported by NSF ITR Grant CCR-0085829 and a grant from the NASA Intelligent Systems (Human-Centered Computing) Program NCC2-1223

process. The goal of the model is not to determine blame but instead to more completely understand all the factors involved, particularly those that can be changed to prevent future accidents. In the next section, we provide a general description of the proximate events involved in the loss. Then a control-based model explaining these events is provided.

Some Proximate Events to the Loss

The Black Hawks (Eagle Flight) entered the NFZ through Gate 1, checked in with the AWACS controllers and flew to Zakhu, a town just inside the northeast corner of the security zone and forward headquarters for Army OPC ground operations. The AWACS surveillance officer labeled the flight on the radarscope track. The Black Hawk pilots did not change their IFF (Identity Friend of Foe) code from 42 (the code for all friendly fixed-wing aircraft flying in Turkey on that day) to 52 (the code for the NFZ). They also remained on the enroute radio frequency instead of changing to the frequency to be used in the NFZ. When the helicopters landed at Zakhu, their radar and IFF returns on the AWACS radarscopes faded. Thirty minutes later, Eagle Flight reported their departure from Zakhu to the AWACS and said they were enroute to Irbil (a town deep in the NFZ). The enroute controller reinitiated tracking of the helicopters.

Two F-15s were tasked that day to be the first aircraft in the NFZ and to 'sanitize' it (check for hostile aircraft) before other coalition aircraft entered the area. The F-15s reached their final checkpoint before entering the NFZ approximately an hour after the helicopters had entered. They turned on all combat systems, switched the IFF Mode I code from 42 to 52, and switched to the NFZ radio frequency. They reported their entry into the NFZ to the AWACS. At this point, the Black Hawks' radar and IFF contacts faded as the helicopters entered mountainous terrain. The computer continued to move the helicopter tracks on the radar display at the last known speed and direction, but the identifying H symbol (for helicopter) on the track was no longer displayed.

Two minutes after entering the NFZ, the lead F-15 picked up hits on its instruments indicating that it was getting radar returns from a low and slow-flying aircraft. The lead F-15 pilot alerted his wingman and then locked onto the contact and used the F-15's air-to-air interrogator to query the target's IFF code. If it was a coalition aircraft, it should have been squawking Mode I, code 52. The scope showed it was not. He reported the radar hits to the controllers in the AWACS, and he was told they had no radar contacts in that location.

The lead F-15 pilot then switched the interrogation to a second IFF mode (Mode IV) that all coalition aircraft should be squawking. For the first second, it showed the right symbol but for the rest of the interrogation (4 to 5 seconds) it said the target was not squawking Mode IV. The lead F-15 pilot then made a second contact call over the main radio, repeating the location, altitude, and heading of his target. The wing F-15 pilot replied that his equipment showed the target. This time the AWACS enroute controller responded that he had radar returns on this scope at the spot but did not indicate that this might be a friendly aircraft.

After making a second check of Modes I and IV and again receiving no response, the F-15 executed a visual identification pass to confirm that the target was hostile. He saw what he thought was an Iraqi helicopter. He pulled out his "goody book" with aircraft pictures in it, checked the silhouettes, and identified the helicopters as Hinds, a type of Russian helicopter flown by the Iraqis. The F-15 wing pilot also reported seeing two helicopters, but never confirmed that he had identified them as Iraqi aircraft.

The F-15 lead pilot called the AWACS and said they were preparing to engage enemy aircraft, cleared his wingman to shoot, and armed his missiles. He then did one final Mode I check, received a negative response, and pressed the button that released the missiles. The wingman fired at the other heliopter and both were destroyed.

Control-Based Model of the Loss

In Leveson's new systems accident model (see the accompanying paper at this conference) [2], accidents occur when external disturbances, component failures, and dysfunctional interactions among system

components are not adequately handled by a safety control structure that includes management functions. The most basic concept in the new model is not an event, but a constraint. The accident process is viewed as resulting from a lack of constraints imposed on the system design and operations. The process leading up to an accident (loss event) can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values.

Accidents are thus understood in terms of the inadequate enforcement of safety constraints at each level of the control structure. The first step in analyzing an accident using this model is to identify the hierarchical safety control structure. Then each level is examined to determine the inadequate control actions that failed to maintain the necessary safety constraint(s) at that level and the various explanations for the inadequate control based on the standard components of a control loop. Leveson has classified the factors that should be considered at each level [2], and we use that classification here to describe the accident process.

Description of the General Control Structure

Figure 1 shows the control structure involved in this accident, starting from the Joint Chiefs of Staff down to the aircraft involved in the accident. At the bottom, the pilots directly controlled the aircraft. The AWACS mission crew was responsible for tracking and controlling aircraft. The AWACS also carried an Airborne Command Element (ACE), who was responsible for ensuring that the larger OPC mission was completed. The ACE reported to a ground-based Mission Director. The Army headquarters (Military Coordination Center) Commander controlled the U.S. Black Hawk operations while the Combined Forces Air Component (CFAC) Commander was responsible for the conduct of OPC missions. The CFAC Commander had tactical control over all aircraft flying in the NFZ (including both Air Force fighters and Army helicopters), but operational control only over the Air Force fixed-wing aircraft.

In addition to the formal control channels, there were also communication channels, shown in Figure 1 as dashed lines, between the process components at each level of the hierarchy. Accidents in complex systems often involve not simply failures of individual components but dysfunctional interactions and communications among the components. Understanding why this accident occurred and learning how to prevent a reoccurrence requires understanding the role each of these elements played in the accident process as it unfolded.

After the basic control structure has been identified, the next step in analyzing an accident is to identify the safety constraints at each level of the structure and why they were inadequately enforced. The control flaw may involve inadequate or missing control actions due to inappropriate control algorithms, process models (models of the current state of the process and how it can change) used by the controllers and control algorithms that are inconsistent with the actual state of the controlled process, and inadequate coordination among controllers and decision makers. Additionally, ineffective control may result from flaws in the reference control channel (the communication channel from a controller to the process being controlled); flawed execution of the control action by the process actuator; or inadequate or missing feedback. Each of these factors is considered at each level of the control structure, starting from the bottom.

Physical Process Failures and Dysfunctional Interactions

Friendly fire is a well-known hazard, and a large number of controls were in place at each level of the control structure (hierarchy) shown in Figure 1 to prevent the hazard: Understanding the accident requires understanding why those controls were not effective in this instance. Because of space limitations, only some of the factors can be described in this paper, but a more complete analysis of the accident is available [1].

The physical process being controlled was air operations in the no-fly-zone. The hazard involved in the accident was mistaking a friendly aircraft for a hostile one and shooting at it (friendly fire). Each level will have a safety constraint required at that level to prevent the system hazard. The safety constraint at the physical process level in this example is that weapons must not be fired at friendly aircraft.

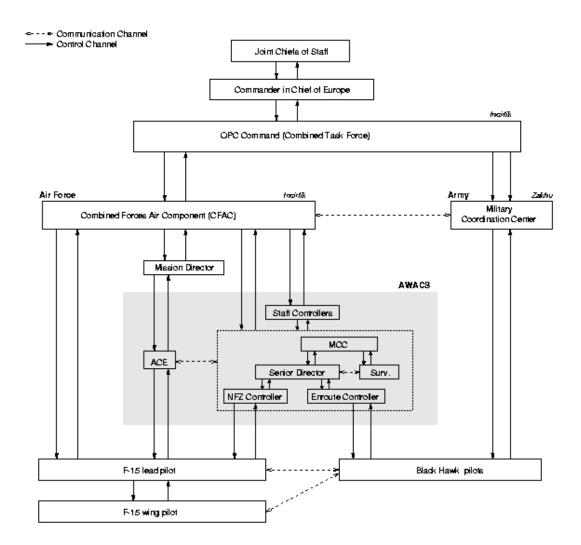


Figure 1 - Hierarchical Control Structure

All the physical components worked exactly as intended, except perhaps for the IFF system. The fact that the Mode IV IFF gave an intermittent response has never been completely explained. There were, however, several dysfunctional interactions and communication inadequacies among the correctly operating aircraft equipment:

- The Black Hawks and F-15s were on different radio frequencies and thus could not speak to each other or hear the transmission between others involved in the incident, e.g., the radio transmissions between the two F-15 pilots and between the lead F-15 pilot and personnel onboard the AWACS. Looking only at this level, it appears that the Black Hawk pilots were at fault in not changing to the NFZ frequency, but an examination of the higher levels of control (later) points to a different conclusion.
- Even if they had been on the same frequency, the Air Force fighter aircraft were equipped with the latest anti-jamming HAVE-QUICK II radios while the Army helicopters were not. The only way the F-15 and Black Hawk pilots could have communicated would have been if the F-15 pilots switched to non-HAVE QUICK mode. The procedures the F-15 pilots were given to follow did not tell them to do so.
- The Black Hawks were not squawking the required IFF code for those flying within the NFZ. Although the official accident investigation report concluded that the reason the F-15s received no

response to their Mode IV IFF query was that the Black Hawks were squawking the wrong code, the GAO reported that according to an Air Force analysis of the IFF system, the F-15s should have received a Mode IV response regardless of the code squawked by the targets. This Air Force analysis was inconclusive with respect to the reason the Mode IV IFF response was never received.

One reason for these dysfunctional interactions lies in the *asynchronous evolution* of the Army and Air Force technology, leaving the different services with largely incompatible radios. In addition, environmental factors, such as the hilly terrain, disrupted communications that depended on line-of-sight transmissions.

The Controllers of the Aircraft and Weapons (the Pilots)

The pilots control the aircraft systems, including the activation of weapons. The safety constraints that must be enforced at this level of the socio-technical control structure are that the F-15 pilots must know who is in the NFZ and whether they should be there or not, i.e., they must be able to accurately identify the status of all other aircraft in the NFZ at all times. They must also follow the rules of engagement (ROE), which specify the procedures the pilots must follow before firing weapons at any targets. The OPC ROE were devised by the OPC Commander, based on guidelines created by the Joint Chiefs of Staff. They were purposely conservative because of the many multinational participants in OPC and the potential for friendly fire accidents. The ROE were designed to slow down any military confrontation, thus preventing the type of friendly fire accidents that had been common during Operation Desert Storm.

<u>Dysfunctional Interactions</u>: The most obvious dysfunctional interaction is that the F-15 pilots fired missiles at the friendly Black Hawk helicopters. Communication problems between the pilots of the aircraft were related to dysfunctional interactions in the physical process (incompatible radio frequencies, IFF codes, and anti-jamming technology) resulting in the ends of the communication channels not matching and information not being transmitted along the channel. Communication between the physical process controllers was also hindered by a *minimum communication* policy that led to abbreviated phraseology in communication and a reluctance to clarify potential miscommunications.

<u>Flawed or Inadequate Control Actions</u>: The accounts of and explanations for the unsafe control actions of the Air Force differ greatly among those who have written about the accident. Analysis is complicated by the fact that any statements the pilots made after the accident were likely to have been influenced by the fact that they were being investigated on charges of negligent homicide. Also, in the excitement of the moment, the lead pilot did not make the required radio call to his wingman requesting the turn on of the HUD tape, and he forgot to turn on his own tape. Therefore, evidence about certain aspects of what occurred and what was observed is limited to pilot testimony during the post-accident investigations and trials.

• **Black Hawk Pilots**: The Army helicopters entered the NFZ before it had been "sanitized" by the Air Force fighters, despite the fact that the Aircraft Control Order (ACO) specified that a fighter sweep of the area must precede any entry of allied aircraft. However, because of the frequent trips of Eagle Flight helicopters to Zakhu, an official exception had been made to this policy. The fighter pilots had not been informed about this exception.

Other potential control flaws include not changing to the appropriate IFF Mode I signal nor to the radio frequency to be used in the area. Even if they had been on the same frequency, however, they would have been unable to communicate with the F-15s because of the different anti-jamming technology of the radios. The Commander of OPC had testified after the accident that the use by the Black Hawks of the enroute radio frequency rather than the NFZ frequency had been briefed to him as a safety measure because the Black Hawk helicopters were not equipped with HAVE QUICK technology. The ACO required the F-15s to use non-HAVE QUICK mode when talking to various other types of aircraft that also did not have the new technology, but did not include Black Hawks in the list. The control problem appears, therefore, to be at the higher levels that allowed the use of the enroute frequency as a safety measure but did not ensure that this measure would be effective by coordinating it with the F-15 procedures specified in the ACO. The Piper account of the accident also contains reference to

helicopter pilots testimony that six months before the shootdown, in October, 1993, they had complained that the fighter aircraft were using their radar to lock onto the Black Hawks an unacceptable number of times. They had argued that there was an urgent need for the Black Hawks to be able to communicate with the fixed-wing aircraft, but nothing was changed until after the accident, when new radios were installed in the Black Hawks.

- Lead F-15 Pilot: The lead F-15 pilot did not perform a proper visual identification, misidentified the Black Hawks as Iraqi, and did not make a second pass to confirm the visual identification. He also did not report to the ACE (as required by the ACO and the ROE) that he had encountered an unidentified aircraft and did not wait for the ACE to approve the release of the missiles. Indeed, he acted very quickly, without giving those above him in the control structure (who were responsible for controlling the engagement) time to act. The Combined Task Force Commander partially attributed the F-15 pilots' urgency to engage the targets to the fact that F-16s would have entered the NFZ soon, potentially allowing the F-16 pilots to get credit for the downing of an enemy aircraft. In addition, Snook argues that this was a rare opportunity for peacetime pilots to engage in combat. An additional factor was that when the lead pilot called out that he had visually identified two Iraqi helicopters, he asked the wing pilot to confirm the identification. The wingman called out "tally two" on his radio, which the lead pilot took as confirmation, but which the wing pilot later testified only meant he saw two helicopters. The lead pilot did not wait for a positive identification from the wingman before starting the engagement and did not question the vague response when he got it.
- Wing F-15 Pilot: The wing pilot did not make a positive identification of the helicopters, did not tell the lead pilot that he had not identified the helicopters, and continued the engagement despite that fact.

<u>Reasons for Flawed Control Actions and Dysfunctional Interactions</u>: Once the inadequate or missing control actions are identified, the factors identified in Leveson's classification can be used to identify the reasons behind the flawed control to learn how to prevent future accidents.

• *Inaccurate Mental Models:* There were many inconsistencies between the mental models of the Air Force pilots and the actual process state. First, they had an ineffective model of what a Black Hawk helicopter looked like. There are several explanations for this, including poor visual recognition training and the fact that the Black Hawks, which had extra wing-mounted fuel tanks for this mission, resembled the Russian helicopters flown by the Iraqis (but which were also flown by U.S. allies in the area). None of the pictures of Black Hawks on which the F-15 pilots had been trained had these wingmounted fuel tanks. Additional factors include the speeds at which the F-15 pilots do their visual identification passes and the angle at which the pilots passed over their targets. Pilots are taught to recognize many different types of aircraft at high speeds using "beer shots", which are blurry pictures that resemble how the pilot might see those aircraft while in flight. The Air Force pilots, however, received very little training in the recognition of Army helicopters, which they rarely encountered because of the different altitudes at which they flew. All the helicopter photos they did see during training, which were provided by the Army, were taken from the ground, a perspective from which it was common for Army personnel to view helicopters but not useful for a fighter pilot in flight above them. Air Force visual recognition training and procedures were changed after this accident.

The F-15 pilots also had an inaccurate model of the current airspace occupants, based on the information they had received about who would be in the airspace that day. They assumed and had been told repeatedly and by almost everyone involved that there would be and were no friendly helicopters in the NFZ at that time.

The F-15 pilots may have also had a misunderstanding about (incorrect model of) the ROE and what procedures were required when they detected an unidentified aircraft. The accident report says that the ROE were reduced in briefings and in individual crew member's understandings to a simplified form. This simplification led to some pilots not being aware of specific considerations required prior to engagement, including identification difficulties, the need to give defectors safe conduct, and the possibility of an aircraft being in distress and the crew being unaware of their position.

The Black Hawk control actions can also be linked to incorrect mental models, i.e., they were unaware there were separate IFF codes for flying inside and outside the NFZ and that they were supposed to change radio frequencies inside the NFZ. They had also been told that the ACO restriction on the entry of allied aircraft into the NFZ before the fighter sweep did not apply to them.

• Feedback from the Controlled Process: The F-15 pilots received ambiguous feedback from their visual identification pass. At the speeds and altitudes they were travelling, it is unlikely they would have detected the unique Black Hawk markings that identified them as friendly. The mountainous terrain in which they were flying limited their ability to perform an adequate identification pass. The feedback from the wingman to the lead F-15 pilot was also ambiguous and apparently misinterpreted by the lead pilot. The minimum communication policy may have again come into play here. Snook suggests that the expectations of what the pilots expected to hear resulted in a filtering of the inputs. This is a well-known problem in airline pilots communications with controllers; the use of well-established phraseology is meant to reduce it. But the calls by the wing pilot were non-standard. In fact, Piper notes that in pilot training bases and programs that train pilots to fly fighter aircraft since the shootdown, these radio calls are used as examples of "the poorest radio communications possibly ever given by pilots during a combat intercept" [3].

Controllers of the F-15 and Black Hawk Pilots

The AWACS mission crew were responsible for identifying, tracking, and controlling all aircraft enroute to and from the NFZ; for coordinating air refueling; for providing airborne threat warning and control in the NFZ; and for providing surveillance, detection, and identification of all unknown aircraft. The ACE was responsible for controlling combat operations and for ensuring that the ROE were enforced.

The general safety constraint involved in the accident at this level was to prevent misidentification of aircraft by the pilots and any friendly fire that might result. There were, however, many controllers with confused and overlapping responsibilities for enforcing different aspects of this general constraint. The overlaps and boundary areas in the controlled processes led to serious control coordination problems among those responsible for controlling aircraft in the NFZ.

<u>Context in Which Decisions and Actions Took Place</u>: At the time of the shootdown, shrinking defense budgets were leading to base closings and cuts in the size of the military. At the same time as this downsizing, a changing political climate, brought about by the fall of the Soviet Union, demanded significant U.S. military involvement in a series of military operations. The military (including the AWACS crews) were working at a greater pace than they had ever experienced, and this was leading to poor morale, inadequate training, and high personnel turnover.

AWACS crews are stationed and trained at Tinker Air Force Base in Oklahoma and then deployed to locations around the world for rotations lasting approximately 30 days. Although all but one of the AWACS controllers on the day of the accident had served previously in the Iraqi NFZ, this was their first day working together and, except for the surveillance officer, the first day of their current rotation. Due to last minute orders, the team got only minimal training together, including one simulator session instead of the two full sessions required prior to deploying. In the only session they did have, some of the members of the team were missing and one was later replaced. In addition, the information in the simulator session was not current (for example, the maps were out of date as was the ROE provided) and did not include a listing of Black Hawks as friendly participants.

The OPC leadership recognized the potential for some distance to develop between stateside training and continuously evolving practice in the NFZ. Therefore, they had permanent *staff* or *instructor* personnel fly with each new AWACS crew on their maiden flight in Turkey. This "shadow" crew of experts was onboard the day of the accident to answer any questions the new crew might have about local procedures and to alert them as to how things were *really* done in the NFZ.

<u>Dysfunctional Interactions Among the Controllers</u>: Control of aircraft was supposed to be handed off from the enroute controller to the NFZ controller when the aircraft entered the NFZ. This handoff did not occur

for the Black Hawks, and the NFZ controller was not made aware of the Black Hawks' flight within the NFZ. Snook explains this as resulting from a computer terminal failure that interfered with communication between the NFZ and enroute controllers. But this explanation does not gibe with the fact that the *normal* procedure was for the enroute controller to continue controlling helicopters, without handing them off to the NFZ controller, even when the enroute and NFZ controllers were seated in their usual places next to each other. There may usually have been more informal interaction about aircraft in the area when they were seated next to each other, but there is no guarantee that such interaction would have occurred even with a different seating arrangement. Note that the helicopters had been dropped from the radar screens and the enroute controller did not know where the helicopters were: He thought they were close to the boundary of the NFZ and was unaware they had gone deep within it.

The interaction between the surveillance officer and the senior weapons director with respect to tracking the helicopter flight on the radar screen involved several dysfunctional interactions. For example, the surveillance officer put an attention arrow on the senior director's radar scope in an attempt to query him about the lost helicopter symbol that was floating, at one point, unattached to any track. The senior director did not respond to the attention arrow, and it automatically dropped off the screen after 60 seconds. The helicopter symbol (H) dropped off the radar screen when the radar and IFF returns from the Black Hawks faded and did not return until just before the engagement, removing any visual reminder to the AWACS crew that there were Black Hawks inside the NFZ.

During his court martial for negligent homicide, the senior director argued that his radar scope did not identify the helicopters as friendly and that therefore he was not responsible. When asked why the Black Hawk identification was dropped from the radar scope, he gave two reasons. First, since it was no longer attached to any active signal, they assumed that the helicopter had landed somewhere. Second, because the symbol displayed on their scopes was being relayed in real time through a JTIDS¹ downlink to commanders on the ground, they were very concerned about not sending out an inaccurate picture of the NFZ. "Even if we suspended it, it would not be an accurate picture, because we wouldn't know for sure if that is where he landed. Or if he landed several minutes earlier, and where that would be. So, the most accurate thing for us to do at the time was to drop the symbology [*sic*]."

<u>Flawed or Inadequate Control Actions:</u> There were myriad inadequate control actions in this accident, involving each of the controllers in the AWACS. The NFZ controller did not monitor the course of the Black Hawks in the NFZ and did not alert the F-15 pilots before they fired that the helicopters they were targeting were friendly. None of the controllers warned the F-15 pilots at any time that there were friendly helicopters in the area. The accident investigation board found that because Army helicopter activities were not normally known at the time of the fighter pilots' daily morning briefings, normal procedures were for the AWACS crews to receive real-time information about their activities from the helicopter crews and to relay that information to the other aircraft in the area. This established procedure obviously was not followed on this occasion.

The enroute controller never told the Black Hawk pilots to change to the NFZ frequency and did not hand off control of the Black Hawks to the NFZ controller. The established practice of not handling off the helicopters had probably evolved over time as a more efficient way of handling traffic. Because the helicopters usually only flew at the very border of the NFZ and spent very little time there, the overhead of handing them off twice was probably considered inefficient by the AWACS crews. As a result, the procedures used had changed over time to the more efficient procedure of keeping them under the control of the enroute controller. Complicating this was a lack of written guidance or training regarding the control of helicopters within the NFZ. In the absence of such guidance or procedures, the AWACS crews adapted their normal practices for fixed-wing aircraft as best they could to apply them to helicopters.

The shadow crews were supposed to be monitoring the activities of this first time crew, but they did not appear to be doing their job. One was in the galley "taking a break" while the other went back to the crew rest area, read a book, and took a nap.

¹ JTIDS, or *Joint Tactical Information Distribution System*, provides ground commanders with a real-time downlink from the AWACS of the current situation.

Finally, the ACE did not provide any control commands to the F-15s with respect to following the ROE and firing on the friendly helicopters.

Reasons for the Flawed Control:

- *Inadequate control algorithms*: This level of the accident provides an interesting example of the difference between specified procedures and accepted practice, the adaptation of procedures over time, and migration toward the boundaries of safe behavior. Accepted practice appeared to be safe until the day that the helicopters' behavior differed from normal, i.e., they stayed longer in the NFZ and ventured beyond a few miles inside the boundaries. The established procedures no longer assured safety under these conditions. A complicating factor in the accident was the universal misunderstanding of each of the controllers' responsibilities with respect to tracking Army helicopters.
- *Inaccurate Mental Models*: Most of the people involved in the control of the F-15s were unaware of the presence of the Black Hawks in the NFZ that day, the lone exception perhaps being the enroute controller who knew they were there but apparently thought they were far from their actual location deep within the NFZ. The enroute controller thought the helicopters would stay at the boundary. When the Black Hawk pilots originally reported their takeoff from Zakhu, they contacted the enroute controller and said they were bound for *LIMA*. The enroute controller was not aware of what city the call sign *LIMA* referred to and did not look this information up. After the accident, he went searching for the document defining the call signs and finally found it back in the surveillance section of the AWACS aircraft. Clearly, tracking helicopters using call signs was not a common practice or the charts would have been closer at hand. Other members of the crew also had inaccurate models of their responsibilities, as described in the next bullet.

Finally, the ACE expected that the F-15 pilots would ask him for guidance in any situation involving a potentially hostile aircraft, as required by the ROE. The F-15 pilots did not seem to understand the ROE in this regard.

• Coordination Among Multiple Controllers: As mentioned earlier, control coordination problems are pervasive in this accident due to overlapping control responsibilities and confusion about responsibilities in the boundary areas of the controlled process. Most notably, the helicopters usually operated close to the boundary of the NFZ, resulting in confusion over who was or should be controlling them.

Coordination problems also existed between the activities of the AWACS surveillance personnel and the other controllers. During the investigation of the accident, the surveillance crew said their responsibility was south of the 36th parallel and the other controllers were responsible for tracking and identifying all aircraft north of the 36th parallel. The other controllers suggested that surveillance was responsible for tracking and identifying all unknown aircraft, regardless of location. In fact, Air Force regulations said that surveillance had tracking responsibility for unknown and unidentified tracks throughout the NFZ. It is not possible, again because of threat of court martial, to piece out exactly what was the problem here, including perhaps simply a normal migration of accepted operations from specified operations. At the least, it is clear there was confusion about who was in control of what.

There was also confusion about who was responsible for the engagement of unidentified aircraft: the ACE or the pilots. The rules of engagement stated that the ACE was responsible, but some pilots believed they had authority when an imminent threat was involved. It is difficult to argue, however, that the slow, low-flying Black Hawks posed a serious threat to the F-15s. One expert later commented that even if they had been Iraqi Hinds, "a Hind is only a threat to an F-15 if the F-15 is parked almost stationary directly in front of it and says 'Kill me'. Other than that, it's probably not very vulnerable."

One possible explanation for the lack of coordination among controllers at this level of the hierarchical control structure is that, as noted above, the group was never trained as a team. Another explanation for all the coordination problems involved in this accident is the fact that the helicopters and fixed-

wing aircraft had separate control structures that only joined fairly high up in the hierarchy (the OPC Commander). Coupling that with the communication problems between the components at each level of the control hierarchy, e.g., between the Army Military Coordination Center and the Air Force Combined Forces Air Component headquarters, the reasons for the problems becomes clear. Even if the roles of everyone in such a structure are well-defined originally, local adaptation to more efficient procedures and asynchronous evolution of the different parts of the control structure are very likely to create dysfunctionalities as time passes.

- *Feedback from Controlled Process*: Signals to the AWACS controllers from the Black Hawks were inconsistent due to line-of-sight limitations and the mountainous terrain in which the Black Hawks were flying. The helicopters used the terrain to mask themselves from air defense radars, but this terrain masking also caused the radar returns from the Black Hawks to the AWACS (and to the fighters) to fade at various times. The squawking of the wrong Mode I signal did not help. Neither did the failure of the F-15 pilot to follow the ROE and report the unidentified aircraft to the ACE.
- *Time Lags*: Important time lags contributed to the accident such as the delay of radio reports from the Black Hawk helicopters due to radio signal transmission problems and their inability to use their backup TACSAT radios until they had landed.

An unusual time lag occurred where the time delay was in the controller and not in one of the other parts of the control loop. The F-15 pilots responded faster than the controllers in the AWACS and on the ground were able to issue appropriate control instructions with regard to the engagement (as was required by the ROE). Snook attributes the fast reaction to the overlearned defensive responses taught to fighter pilots during training and both Snook and the GAO report mention the rivalry with the F-16 pilots and the desire of the lead F-15 pilot to shoot down an enemy aircraft. Additional or alternative explanations are also possible. Like the explanation for any human actions, it is not possible to get a definitive answer. Even in this case where the F-15 pilots survived the accident, there are many reasons to discount their own explanations, not the least of which is that they were facing the possibility of being charged with negligent homicide and spending many years in jail. The explanations a week later during the official investigations to determine whether they should be court martialed.

Military Coordination Center, Combined Forces Air Component, and CTF Commander

Fully understanding the behavior at any level of the socio-technical control structure requires understanding how and why the control at the next higher level allowed or contributed to the inadequate control at the current level. The MCC had operational control over the Army helicopters while the CFAC had operational control and tactical control over *all* aircraft in the NFZ. The Combined Task Force Commander (who was above both groups) had ultimate responsibility for the coordination of fixed-wing aircraft flights with Army helicopters.

There were many safety constraints violated at this level of the control structure, and several people were investigated for potential court martial and received official letters of reprimand. The safety constraints violated include: (1) procedures must be instituted that delegate appropriate responsibility, specify tasks, and provide effective training to all those responsible for tracking aircraft and conducting combat operations; (2) procedures must be consistent or at least complementary for everyone involved in NFZ airspace operations; (3) performance must be monitored (feedback) to ensure that safety-critical activities are being carried out correctly and that local adaptations have not moved operations beyond safe limits; (4) equipment and procedures must be coordinated between the Air Force and Army to make sure that communication channels are effective and that asynchronous evolution has not occurred; (5) accurate information about scheduled flights must be provided to the pilots and the AWACS crews.

Dysfunctional Interactions among Controllers: The weekly helicopter flight schedules the MCC provided to the CFAC staff were not complete enough for planning purposes. While the Air Force could plan their

missions in advance, Army helicopter missions had to be flexible and react to daily needs. Daily Situation Reports (SITREPS) updated the advance information, but did not contain complex flight details and arrived too late to be part of the next days' ATO (Air Tasking Order). In addition, there were no procedures in place to get the SITREPS from the Army Military Coordination Center to the Air Force CFAC. Finally, no MCC representative was assigned to the CFAC for scheduling purposes, and no MCC helicopter detachment representatives had attended the CFAC weekly scheduling meeting for the past three to four months.

After the OPC mission had changed in September, 1991, the original organizational structure of the CTF was modified but the operations plan was not. In particular, the position of the person who was in charge of communication and coordination between the MCC and CFAC was eliminated without instituting an alternative communication channel. This is another example of asynchronous evolution; in this case, there was a structural change without a corresponding change in the operations plan.

<u>Flawed or Inadequate Control Actions</u>: There were many flawed or missing control actions at this level, including:

- The Black Hawk pilots were allowed to enter the NFZ before the fighter sweep and the F-15 pilots and AWACS crews were not informed about this exception to the policy.
- F-15 pilots were not told to use non-HAVE QUICK radio mode for helicopters.
- Helicopter flight plans were not distributed to F-15 pilots (but were to F-16 pilots)
- Inadequate training was provided on the ROE for new rotators as well as inadequate discipline enforced on fighter pilots.
- Inadequate training was provided to the F-15 pilots on visual identification
- Inadequate simulator and spin-up training was provided to the AWACS crews.
- Handoff procedures were never established for helicopters. In fact, no procedures were established for AWACS handling of helicopters in the NFZ.
- Inadequate procedures were specified or enforced for how the shadow crew would instruct the new crews.
- The rules and procedures established for the operation did not provide adequate control over unsafe and undisciplined F-15 pilot behavior. So many flight discipline incidents had occurred leading to close calls that a group safety meeting had been called a week before the shootdown to discuss it. That fix obviously was not effective. But the fact that there were a lot of close calls indicates serious safety problems existed and were not handled.
- Equipment and procedures were not coordinated between the Air Force and the Army to make sure communication channels were effective and that asynchronous evolution had not occurred.
- Performance was not monitored to ensure that safety-critical activities were being carried out correctly and that local adaptations had not moved operations beyond safe limits. Control was not established to prevent unsafe adaptations.
- After the OPC mission changed in September, 1991, operational plans were not updated.

Reasons for the Flawed Control:

• *Inaccurate Mental Models*: The Commander of the Combined Task Force thought that the appropriate control and coordination was occurring. His mental model was supported by the feedback he received flying as a regular passenger on board the Army helicopter flights, where it was his perception that the AWACS was monitoring their flight effectively. He was also an active F-16 pilot who attended the F-16 briefings. At these briefings, he observed that Black Hawk flight schedules were part of the daily ATOs received by the F-16 pilots and assumed that all squadrons were receiving the same information. However, the head of the F-16 squadron with which the Commander flew had gone out of his way to procure the Black Hawk flight information because the F-16s sometimes flew low-level missions where they might encounter the low-flying Army helicopters. The leader of the F-15 squadron did not take a similar initiative because F-15s never flew similar low-level missions. Clearly others also were under the impression that the ATOs provided to the F-15 and Black Hawk pilots were consistent, that

required information had been distributed to everyone, that official procedures were understood and being followed, etc.

- *Coordination Among Multiple Controllers*: There were clearly problems with overlapping and boundary areas of control between the Army and the Air Force. Coordination problems between the services are legendary and were not handled adequately here.
- *Feedback from the Controlled Process*: As noted, the Commander of the Combined Forces used his own experience as an F-16 pilot to create his mental model of what information was available to all pilots, which turned out to be misleading. Because formal feedback and auditing procedures were not established, the Commander had only informal and misleading information available. The lack of feedback kept the higher levels of control in this safety control structure unaware of problems existing at lower levels. OPC had operated accident-free for over three years at the time of the shootdown. During that time, local adaptations to compensate for inadequate control from above had managed to mask the ongoing problems until a situation occurred where local adaptations did not work. A lack of awareness at the highest levels of command of the severity of the coordination, communication, and other problems is a key factor in this accident.

US Commander in Chief, Europe

The CTF Commander, General Pilkington, had made several unsuccessful requests to the Commander of the 17th Air force to have an experienced F-15 pilot on flying status assigned to the CTF staff (feedback). According to General Pilkington, the 17th Air Force Commander told him that the available number of F-15 slots was limited and one could not be spared for OPC (incorrect control decision). As part of the corrective actions following the shootdown, an F-15 pilot was assigned to the CTF staff.

Conclusions

When looking only at the proximate events and the behavior of the immediate participants in the accidental shootdown, the reasons for this accident appear to be gross mistakes by the operators (pilots and AWACS crew). While there certainly were mistakes made at these levels, a more complete picture of the safety control structure in place paints a very different explanation including: inconsistent, missing, or inaccurate information; incompatible technology; inadequate coordination; overlapping areas of control and confusion about who was responsible for what; a migration toward more efficient operational procedures over time without any controls and checks on the potential adaptations; inadequate training; and in general a control structure that did not effectively enforce the safety constraints. A systems model of accidents provides a more complete understanding of the reasons for the accident than simply looking at the chain of events.

References

- 1. Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.
- 2. Nancy Leveson. A New Foundation for System Safety. International Conference of the System Safety Society, Denver, 2002.
- 3. Joan L. Piper. *Chain of Events: The Government Cover-Up of the Black Hawk Incident and the Friendly Fire Death of Lt. Laura Piper.* Brasseys Inc., 2001.
- 4. Scott A. Snook. Friendly Fire. Princeton University Press, 2000.
- U.S. Government Accounting Office, Office of Special Investigations. Operation Provide Comfort: Review of Air Force Investigation of Black Hawk Fratricide Incident (GAO/OSI-9804). U.S. Government Printing Office, Washington D.C., 1997.

Biography

N. G. Leveson, Ph.D., Professor, Department of Aeronautics and Astronautics, MIT, 77 Massachusetts Avenue, Cambridge, MA 02139, USA, telephone - (617) 258-0505, facsimile - (617) 253-7397, e-mail - leveson@mit.edu.

Dr. Leveson teaches and conducts research in system safety, system engineering, and software engineering. She is a member of the NAE and serves on numerous NASA, DOD, and other governmental committees.

P. Allen, Dept. of Computer Science, University of Victoria, Canada, email - allenp@uvic.edu Polly Allen is a graduate student in the Dept. of Computer Science at the University of Victoria.

M-A. Storey, Ph.D., Professor, Dept. of Computer Science, University of Victoria, Canada, telephone – (250) 721-8796, email – <u>mstorey@csr.uvic.ca.</u>

Dr. Storey teaches and conducts research on software engineering and software visualization.