IN-FLIGHT SECURITY ONBOARD COMMERCIAL AIRCRAFT: CRITICAL IMPROVEMENTS NEEDED

Lori J Brown
Western Michigan University, College of Aviation

Keywords: *In-flight, Wireless technologies, Communication Systems, Security, Aviation*

Abstract

The United States does not have a monopoly on threats to homeland security— or solutions needed to address them. The use of a hijacked aircraft as a weapon, and recent attempts to ignite incendiary devices onboard commercial aircraft requires new in-flight security strategies.
The goal of this study is to evaluate novel tools and approaches to confront homeland security issues. The study proposes to: 1.) Identify breakthrough technologies to mitigate the likelihood of individual radical and/or violent behavior, resulting in catastrophic airline casualties, and 2.) Understand whether wireless crew alert monitoring devices can provide discreet communication to the cockpit, and allow the pilots more time to land the airplane, in the event of a security breach or other compromising emergency in the cabin.

1.0 Introduction

The events of 11th September 2001 magnified the importance of crew security training, discreet communication devices, and the flight attendants' role as the last line of defence to the flight deck. While steps have been taken for airline pilots, who are now safely barricaded behind reinforced cockpit doors and in some cases- armed with guns, and air marshals are on a higher percentage of flights very little has changed for cabin crew since the 9/11 attacks.

Incidents and accidents have shown that flight attendants and Federal Air Marshalls (FAMS) require the ability to alert the flight deck discreetly of dangers, and thereby pre-warn the pilots of possible attempts to enter the cockpit or security breaches in the cabin. Discreet wireless communication devices could enhance security and improve effective communication between the cabin and flight deck [5].

The "Pilot/Fight Attendant Communication and Joint Training" study [3] sought to identify gaps that impede effective communication in a post-9/11 environment. This research examined the effectiveness of current communication and coordination between flight attendants and pilots [1]. As reported in the FAA, International Journal of Applied Aviation Studies [4], respondents included in the study represented 29 countries throughout the world. The countries of origin for the respondents airlines include; Australia, Austria, Belgium, Brussels, Canada, China, Finland, France, Germany, Greece, Hong Kong, Ireland, Italy, Japan, Mauritius, Mexico, New Zealand, Poland, Portugal, Romania, Slovakia, Spain, Switzerland, The Netherlands, Turkey, United States, United Arab Emirates, United Kingdom, and Venezuela. Significant gaps in crew resource management training, communication, and equipment used in-flight for flight attendants and pilots, were identified [3].

Flight attendant and pilot respondents [4] indicated that a discreet wireless communication device would enhance safety and security on-board. In the survey, 13% indicated a discreet wireless communication device would not enhance safety, 87% indicated a wireless communication device would improve communications and enhance safety. The study [4] also reports 58% of respondents did not find the current inter-phone system to be discreet, and 72% said they would be willing to wear a device to achieve wireless communication in-flight.

Focused research in this area, is currently ongoing in countries such as China, which are predicted to have major growth in aviation over the next twenty years [15].

2.0 Improved Communication needed between the Cabin and Flight Deck

Communication gaps have been cited as causation factors in fatal accidents, such as, Dryden [6], and Kegworth [11] (1989), ValuJet [13] (1996), and Helios [9] (2005). Most recently, the failed bombing attempt of Northwest Airlines flight 253 (2009) raised questions of gaps, which impeded communications between the cabin and flight deck. The US Federal Aviation Administrator (FAA) Randolph Babbitt, indicated that the pilots of Northwest Airlines Flight 253 were not alerted that a passenger had tried to ignite a bomb on the flight. The pilots stated they had a problem, only after landing in Detroit, Michigan [10].

Babbitt (2010) told a House subcommittee [10]:

There was a communication gap between the cabin and the flight deck crew, which left pilots unaware that there had been an alleged bombing attempt on-board. The flight deck crew reported they had someone who had attempted to set firecrackers off, so it didn't elevate to anyone — whether it was the cockpit or air traffic control — to anything of great seriousness at that point.

Air traffic controllers did not divert the aircraft to a remote location, "nor did the cockpit get very excited about it," Babbitt said [10]. When the aircraft was on the ground, pilots and airport personnel became aware of the bomb. Minutes and seconds lost in communication gaps, are valuable to communicate with ground operations, warn other aircraft in the air, or land the aircraft.

Resolving in-flight security threats of this type, typically involves four main stages: [12]

- Identifying the threat and notifying affected agencies
- Sharing pertinent information and collaboratively assessing the severity of the threat
- Deciding on and carrying out the appropriate in-flight response, such as initiating a diversion
- If necessary, completing the law enforcement response when the flight has landed

Options for response to an in-flight security threat include either (1) ordering the aircraft to divert from its flight plan by denying it access to U.S. airspace or requiring it to land at a U.S. airport different from its intended destination, or (2) launching military fighter jets to monitor or intercept the aircraft [12]. Although only a small percentage of in-flight security threats are serious enough to divert aircraft from its original destination, it is imperative that correct information relayed in a timely manner.

Crew communications and coordination are critical as they relate to the survival of all onboard and the overall control of the aircraft, and is the primary point of failure during live situational scenarios.

A device that is discreet, or as small and innocuous as possible, could allow all crew members to carry on their person the ability to communicate from anywhere in the aircraft. Each personal device must have capability for encrypted, bidirectional communications.

The International Transport Workers Federation and the Association of Fight Attendants has called for security of the system through use of dedicated hardware components that are accessible only to authorized personnel such as crew members and, potentially, any active law enforcement officers who may have presented credentials to the crew prior to the flight. The hands-free concept will allow crew members under both general emergency (e.g., medical crises, emergency evacuations) and security threat conditions to use their hands to protect themselves, the cockpit, other crew members, passengers, and the aircraft while continuing to coordinate and communicate with the cockpit, the ground, and the rest of the crew. A device possessing such characteristics must be wireless.

Currently, the only communication device available for the flight attendants, air marshals, and the flight deck crew, is the aircraft interphone. The interphone, typically used for public announcements and normal communication between the cabin and flight deck, is usually located in the forward or aft cabin [1, 8]. This isolated location, may limit the flight attendants' ability to reach the interphone, especially during busier phases of flight [5]. Aircraft interphones have been proven easily rendered inoperative (9/11 attacks and Operation Atlas [8, 7]. If the current system is disabled, the flight attendants would not be able to alert the pilots without alarming the hijackers or causing panic in the cabin. These minutes and seconds are very crucial, the pilots need as much warning as possible of a security breach, to attempt to land the airplane. The Association of Professional Flight Attendants [1] "strongly supports the need for hands-free wireless communication devices, which is not available through the current aircraft interphone systems, now mandated". Flight attendants spend much of their time in aircraft aisles away from interphones located in service galleys and near their jump seats. "A flight attendant who suspects a security breach and is working in the cabin could potentially be half the distance of the aircraft away from notifying the flight crew of the threat" [1].

3.0 Research Goals

The goal of this research is to evaluate novel tools and approaches to confront homeland security issues. The study proposes to: 1.) Identify breakthrough technologies to mitigate the likelihood of individual radical and/or violent behavior, resulting in catastrophic airline casualties, and 2.) Understand whether the Crew Alert Monitoring System can provide discreet communication to the cockpit, and allow the pilots more time to land the airplane, in the event of a security breach or other compromising emergency in the cabin, and 3.) Identify any radio interference and possible operational issues with crew and passengers in ground tests onboard transport aircraft.

4.0 Technology Considered

STG Aerospace of U.K. has developed a wireless, discreet cabin alert system to enable the crewmembers to alert the flight deck of a security breach [2, 5]. The system provides the flight crew with an audible alert, coupled with a visible cockpit annunciation signal. The signal will indicate an alert, while giving a "zonal" location. The system also includes a door intercom to provide the additional audio communication between the cabin and the flight deck sides of the cockpit door [2, 5].

The purpose of this system is to provide the following functionality [2, 5]:

1. When a person authorized to access the cockpit seeks entry, the existing visual identification through the cockpit door, coupled with a new audio intercom confirmation that the door area is clear.
2. In the event of an attack on a cabin crewmember, or other security breach in the cabin, a system is provided to enable the cabin crew to alert the flight crew of the emergency event, this will be achieved by using discreet wireless “Panic Buttons” provided to the crewmembers.

3. The communication and alerts recorded onto the cockpit flight recorder can be relayed from the flight deck to: the relevant Security Operations Center; Air Traffic Control National Hostage; Rescue Team and local crisis response teams; Local Airport Emergency Responders; and Military responders. This technology will allow effective communication, while keeping the cost and weight to a minimum to meet the economic constraints of U.S. Airlines, as well as other potential users [5].

4.1 Crew Alert Monitoring Device (CAMS)

The Crew Alert Monitoring device (CAMS), a wireless device that is an ultra secure cabin alert and monitoring system, using small donut shaped alarm units held on person of each cabin crew, or FAMS, which, when activated, sends an alarm signal to the cockpit, effectively warning them of trouble, and the expectation of escalation of that trouble to the cockpit. The signal also tells the cockpit where in the aircraft the alarm was triggered, and therefore an indication of the time, which may be available to them to undertake appropriate actions before attempts at intrusions to the cockpit. The system also provides a means of voice communication between cabin crew and pilot at the cockpit door, and combined with the use of the door peephole provides the pilots with a good means of monitoring if anyone wishing entry to the cockpit is under stress and possible coercion. The system is aircraft specific, extremely secure, has 'designed in' safeguards against inadvertent activation, and meets all the needs of those most closely affected - the pilots, cabin crew and passengers.

The system also includes a flight deck door intercom to provide the additional audio communication between the cabin and the flight deck sides of the cockpit door as recommended in the NPRM. The audio link will be combined with the currently installed video or door viewer, whichever is installed [2, 5].

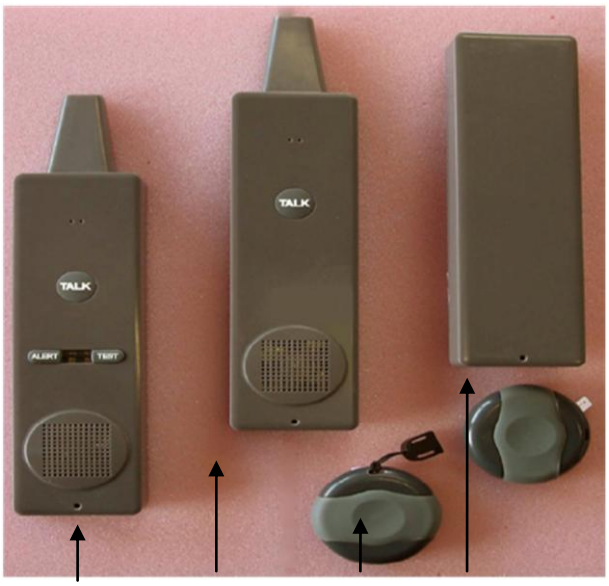

Fig. 1 Crew Alert Monitoring System (CAMS)

The system consists of four parts (Fig. 1):Panic Button, System Module, Relay Module. And Intercom.

4.1.1 Description of device

1. A CAMS panic button is to be carried by crewmembers to provide discreet alert.

2. A CAMS System Module (CSM) placed in the cockpit by the entry door, providing audio communications to the intercom along with audible and visual alerts when a panic button has been activated.

3. CAMS Relay Modules (CRM) to act as wireless transceivers for propagation of the alert signal through the aircraft. The designs of these will mimic that of the
CAMS System Module, but will be installed out of sight in the cabin ceiling area.

4. A CAMS Intercom unit for outside the cockpit door area, to provide audio confirmation. This is coupled with the existing visual confirmation provide by video or through the door viewing device. The CAMS system will have a specific aircraft ID to stop interference between adjacent aircraft systems on the ground. There will be 2048 possible IDs available, allocated at installation. This means that the probability of two aircraft having the same *specific* ID is over four million to one and the probability of one having an incident or test while the other aircraft is close enough is a multiple of that figure [2, 5].

4.1.2 Radio Frequency Performance Testing

The CAMS uses a 2.4GHz spread-spectrum radio transmission to send a signal from the panic buttons worn by the cabin crew. The same radio channel is used to signal the panic button location from the receiver points in the cabin roof to the control panel in the cockpit. This section addresses an investigation of the technical capability of the CAMS system and its ability to provide useful and reliable information in an operational environment.

A number of radio frequency measurements and tests of the equipment are to be made as part of this research program [5].

The purpose of these tests is:

1. To validate the operation of the CAMS system in an aircraft cabin
2. To investigate the operational safety margin in normal use (i.e. how much excess signal strength is provided when body shadowing etc. is present)
3. To confirm, via analysis and ground test, non-interference with the aircraft communications and navigation systems
4. To investigate the potential for harmful interference from the aircraft and passenger electronic devices
5. To investigate the performance differences between a lightly-loaded and heavily occupied cabin

4.1.3 Analytical Approach

The radio measurement tests will be carried out in two environments, a test aircraft, and the cabin simulator. The test aircraft is representative of a large passenger aircraft with operational communications and navigational aids, but necessarily will not be available for long periods with different patterns of passenger seating. The cabin simulator gives considerable flexibility for changing the loading of the cabin section and investigating the effects of local shadowing (masking) of the radio signal as the position where the panic buttons are worn are altered [8].

4.1.4 Aircraft tests

A CAMS system will be temporarily installed in a test aircraft. A series of tests to examine coverage will be defined in a test plan and approved by the aircraft operator before the test. This will include test items such as [2, 5]:

1. Confirmation of operation in all zones of the aircraft
2. Mapping the accuracy of zone identification dependent on position of the initiating panic button in the aircraft, different positions of the panic button on the wearer.
3. Using a modified CAMS cockpit unit to indicate the signal strength received by the CAMS sensors

4. Operation of communication devices and navigational instrument when operating the CAMS system to detect potential interference.

4.1.5 Analysis of interference

The potential for the CAMS system to generate interference to aircraft systems will be studied using the guidelines laid out in RTCA DO-294B Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDS) on Aircraft and RTCA DO-307 - Aircraft Design and Certification for Portable Electronic Device (PED) Tolerance [2].

In addition, the potential for a T-PED or other device to interfere with the operation of the CAMS system will be investigated.

A report will be produced outlining the results of the interference investigation and any further tests will be defined for running on the aircraft simulator [2].

4.1.6 Aircraft simulator tests

A second CAMS system will be installed in the aircraft simulator and used for the behavioral experiments. The Behavioral (human) Factors of this study are as follows:

- Identify how discreet the traditional means of communication between the cabin and the cockpit is;
- Identify how discreet the CAMS communication between the cabin and the cockpit is;
- Identify the amount of time lapse between the trigger event (security breach) and effective communications from the cabin to the flight deck, when using the intercom method.
- Identify the amount of time lapse between the trigger event (security breach) and effective communications from the cabin to the flight deck, when using the CAMS communication method.
- Identify effectiveness of door entry procedures: The first will involve the traditional interphone method and a second method would involve visual identification of the door area, coupled with an audio confirmation procedure. Through a viewing device installed in the flight deck door, one person on the flight deck would view the door area and identify the person seeking access. Then a crewmember would provide audio confirmation that the door area is clear while viewing the outside door area. For example, before providing audio confirmation to the flight deck, the crewmember would assure that no passengers are standing near the door area, and. that no passenger is in any forward lavatory.
- Test security levels 1-5 and procedures for use

In addition to the behavioral experiments, a series of tests will be run to examine any change in operation with different cabin occupant loading. The aircraft simulator represents a portion of a single-aisle cabin, and consequently the results of tests can be compared and verified against a single (e.g. front) section of the main aircraft tests [2,5].

RF tests in the aircraft simulator include items such as [2]:

1. Investigation of the signal strength margin fully loaded and lightly loaded with passengers
2. Investigation of the ability to interfere with the CAMS system using a T-PED such as a wireless laptop connection
3. Investigation of the ability to interfere with the CAMS system using a purpose-built interferer [2].
4.

5.0 Conclusions and Future Work

In this paper, we provided an overview of our proposed framework for the use of RFID and human factors methodologies for data collection to evaluate the use of wireless communication devices onboard commercial aircraft.

The results of the aircraft and simulator tests will be analyzed and written into a report to summarize the suitability of the CAMS system in a true operational environment.

The results of the human factors test will be analyzed to determine [2, 5]:

1.) The efficacy of the current interphone system, and new technologies for communications between the cabin and flight deck

2.) Determine whether the Crew Alert Monitoring System can provide discreet communication to the cockpit from the cabin; and allow the pilots more time to safely land the airplane, in the event of a security breach or other compromising emergency in the cabin.

3.) Evaluate various placements for the device on the crewmembers person (e.g. watch style, embedded in uniform, wrist or neck lanyard, FAM pocket, etc).

4.) Evaluate various placements in the aircraft (e.g. discreetly located on serving cart, jumpseat, or galley area).

5.) Evaluate the time lapse between the trigger event (security breach) and communications from the cabin to the flight deck, when using the intercom method.

Our future work will provide an in-depth security assessment and performance analysis of wireless communication devices, to compliment the breadth and depth of homeland security efforts. These data will support the US Transportation Security Administration Authorization Act (H.R. 2200, sec. 235), which directs the Assistant Secretary of the US to: (1) prepare a report that assesses technologies and includes standards for the use of wireless devices to enhance aircraft security and communication between cabin crew and pilot crewmembers, embarked federal air marshals, and authorized law enforcement officials [15]. This act will require-not later than one year after the date of enactment, the US Assistant Secretary, in consultation with the Advisory Committee established under section 44946 of title 49, United States Code, shall prepare a report that assesses technologies and includes standards for the use of wireless devices to enhance transportation security on aircraft for the purpose of ensuring communication between and among cabin crew and pilot crewmembers, embarked Federal air marshals, and authorized law enforcement officials, as appropriate.

References

[1] Air Safety Week. Modified cockpit security measures proposed. *ASW*, 2007.

[2] Braithwaite S, and STG Aerospace, *Commercial in confidence, CAMS system description. STG Aerospace, 2008.*

[3] Brown L, and Niehaus J. Pilot/flight attendant communication to improve aviation safety. *Proceedings of the Flight Safety Foundation, Corporate Aviation Safety Symposium*. Orlando, Florida, 2009.

[4] Brown L, and Rantz B. The efficacy of flight attendant/pilot communication, in a post-9/11 environment: viewed from both sides of the fortress door. (in press) *International Journal of Applied Aviation Studies, (IJAAS),* Federal Aviation Administration, Summer 2010.

[5] Brown L. The evaluation of wireless communication devices. *International Journal of Aviation Technology and Engineering*. 2010.

[6] Dryden. Commission of inquiry into the air ontario crash. *Moshansky*. Toronto, Canada, 1992.

[7] Fleisher L. Terror response is tested 'OPERATION ATLAS'. *Boston Globe*, June 5th, 2005.

[8] Federal Aviation Administration. Communication and coordination between flight crew members and flight attendants. *Advisory Circular No. 120-48*. 1992.

[9] Greece. Aircraft accident report. Helios airways flight HCY522, Boeing 737-31S. AAIBSB, Accident investigation report, 2006. Retrieved from: http://www.skybrary.aero/bookshelf/books/1170.pdf

[10] House of Transportation and Infrastructure Committee Aviation Subcommittee Representatives. *The agency's call to action on airline safety and pilot training. Congress, Feb. 04, 2010*.

[11] Kegworth Great Britain. *Report 4/1990, on the accident of boeing 737-400*. *The Department of Transport, Air Accidents Investigation Branch*. United Kingdom, 1989. http://www.aaib.gov.uk/publications/formal_reports/4_1990_g_obme.cfm.

[12] Seidenstat P, and Splane, F. (Eds.) Onboard security. *Protecting Airline Passengers in the Age of Terrorism*. Greenwood Publishing, 2009.

[13] ValuJet. In-flight fire and impact with Terrain *Aircraft Accident Report***,** Flight 592. 1996.

[14] Western Michigan University. *Grant spurs groundbreaking aviation research*. 2010. www.wmich.edu/wmu/news/2010/04/069.shtml

[15] 111th Congress, US transportation security information act, H.R. 2200, section 235. *House report on cabin crew communication.* 111-123, Library of Congress, GPO, 2010.

Copyright Statement

Lori.brown@wmich.edu