Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

Executive summary

SAFEE - Security of Aircraft in the Future European Environment

Problem area
Aviation security concerns measures taken to counter acts of unlawful interference against civil aviation. Since the events of 11 September and also the London Mega Terror Plot in August 2006, the aviation community has strengthened security. A set of urgency measures were taken by authorities (e.g. Eurocontrol, ICAO, European Commission, ECAC, FAA/TSA) to increase security, both in airports and on-board aircraft. Analysis of the security measures demonstrated that little was done on-board (the focus was on cockpit door reinforcement, training of cabin crew, and sky marshals on board more flights). Hence, there might be a need to further increase on-board security.

Description of work
SAFEE aims to develop advanced aircraft security systems designed to prevent and respond adequately to in-flight threats. The main goal is to ensure a fully secured flight from departure to arrival destination. This is done through implementation of on-board threat detection systems and the provision of reliable threat information to the flight crew.
In this paper, we introduce SAFEE focusing on the SAFEE users (pilots, cabin crew, sky marshals) and their systems and technologies.

Results and conclusions
The SAFEE project has defined a set of potential targets for attacks, and identified detection tools and response actions to be developed and assessed. Depending on the threat level, different security procedures for the flight crew will apply. The SAFEE Operational Concept anticipates new interfaces for the pilot, cabin crew and security staff, on-board crew communication links, and air/ground communication links (with the European Regional Renegade Information Dissemination System. The SAFEE functionalities include:

- On-board threat detection
- Threat assessment and response management systems
- Emergency avoidance systems
- Flight reconfiguration
- Anti threat data links
- Secured voice and data communications.
- Secured open world (internet).
- Authentication of pilot/crew commands on-board aircraft.

Applicability
The SAFEE operational concept and systems are now validated with the NLR GRACE flight simulator. Results and recommendations are disseminated through the SAFEE Users Club, in which key aviation security representatives and air transport stakeholders participate.

Report no.
NLR-TP-2006-716

Author(s)
O. Laviv
L.J.P. Speijker

Report classification
Unclassified

Date
July 2007

Knowledge area(s)
Veiligheid (safety & security)

Descriptor(s)
in-flight security
aircraft systems
threat detection
risk assessment

This report is based on a presentation held at the 4th International Aviation Security Technology Symposium, Washington (U.S.A.), November 27 – December 1, 2006.

Nationaal Lucht- en Ruimtevaartlaboratorium, National Aerospace Laboratory NLR

Anthony Fokkerweg 2, 1059 CM Amsterdam,
P.O. Box 90502, 1006 BM Amsterdam, The Netherlands
Telephone +31 20 511 31 13, Fax +31 20 511 32 10, Web site: www.nlr.nl

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2006-716

SAFEE - Security of Aircraft in the Future European Environment

O. Laviv[1] and L.J.P. Speijker

[1] Athena GS-3

This report is based on a presentation held at the 4th International Aviation Security Technology Symposium, Washington (U.S.A.), November 27 – December 1, 2006.

This publication has been refereed by the Advisory Committee AIR TRANSPORT.

Customer	European Commission
Contract number	AIP3-CT-2003-503521
Owner	National Aerospace Laboratory NLR and partners
Division	Air Transport
Distribution	Unlimited
Classification of title	Unclassified
	September 2007

Approved by:

Author	Reviewer	Managing department

Summary

Since the events of September 11th (and, to some extent, also after the London Mega Terror Plot in August 2006), the aviation community has strengthened security, so as to counteract threats to air transport. However, analysis of the new security measures demonstrated that little was done on-board (the main focus was on cockpit door reinforcement, better training of cabin crew, and sky marshals on board more flights). Hence, there might still be a need to further increase on-board security. It is clear that a fresh approach needs to be adopted; an approach which will utilize new technologies in order to achieve the goal: create a safe, none burdening to the customer and economical security system which restores confidence of air passengers.

Therefore, this paper introduces the SAFEE aircraft systems. SAFEE aims to ensure a fully secured flight from departure to arrival destination. The SAFEE approach is to proactively anticipate in-flight threats and to focus the system development on countering threats with the highest risk. For this purpose, security occurrences have been analyzed and a risk and threat assessment has been performed [5]. Based on the findings, the developers of SAFEE have defined 11 basic threat scenarios which the system must counter. The countermeasures are based on subsystems that will identify threats in real time, recommend on (and execute) appropriate responses and increase survivability of the flight. The basic principles for the SAFEE operational concept and system architecture are now described. The SAFEE project has defined a set of potential targets for attacks, and identified detection tools and response actions to be developed and assessed. Depending on the threat level, different security procedures for on-board actors will apply. The SAFEE Operational Concept is in line with this, and anticipates security support for pilots, cabin crew, and security staff. The SAFEE system has interfaces for the pilot (in the cockpit), cabin crew and security staff (in the cabin), on-board crew communication links, and air/ground communication links. It is also possible that on-ground security staff may obtain real-time access individual sensor output or on-board threat level information through a data-link connection (ACARS or VDL). A foreseen air/ground data-link with the European Regional Renegade Information Dissemination System (ERRIDS) will be the main (secured) channel/gateway for uplink and downlink of threat information from the ground to the aircraft and vice versa. The SAFEE operational concept and systems are now being validated with the NLR GRACE flight simulator, which is also used for security training.

One should realize that, as terrorists are constantly developing new and improved abilities and Modes of Hostile Action, in addition to analyzing and utilizing aviation security data, it is important to include the use of intelligence-based information and/or opinion gathered from security experts.

List of acronyms

ACARS	Aircraft Communication Addressing and Reporting System
ACRF	Access Control and Registration
AOC	Airline Operations Centre
ATC	Air Traffic Control
ATDL	Anti Threat Data Link
ATM	Air Traffic Management
DB	Data Base
DODF	Dangerous Objects Detection Function
EADS	European Aeronautics Defence and Space company
EAS	Emergency Avoidance System
ECAC	European Civil Aviation Conference
ERRIDS	European Regional Renegade Information Dissemination System
ETDS	Electromagnetic Threat Detection System
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAA	Federal Aviation Administration
FRF	Flight Reconfiguration Function
GRACE	Generic Research Aircraft Cockpit Environment
ICAO	International Civil Aviation Organisation
JAR	Joint Aviation Requirements
NLR	Netherlands National Aerospace Laboratory
OPS	Operations
OTDS	On-board Threat Detection System
PMHA	Possible Modes of Hostile Action
PSA	Prohibited Security Area
RAP	Risk Assessment Process
SAFEE	Security of Aircraft in the Future European Environment (EU project)
SBDF	Suspicious Behaviour Detection Function
SME	Small or Medium sized Enterprise
TARMS	Threat Assessment and Response Management System
TSA	Transportation Security Administration
VDL	VHF Data Link
VHF	Very High Frequency

Contents

1 Introduction

Aviation security concerns measures taken to counter acts of unlawful interference against civil aviation. Since the events of September 11th (and, to some extent, also after the London Mega Terror Plot in August 2006), the aviation community has strengthened security, so as to counteract threats to air transport. The immediate drop in passengers following September 11th showed that public confidence in air transport was severely eroded for a significant period of time. A first set of urgency measures were taken by authorities (e.g. EUROCONTROL, ICAO, European Commission, ECAC, FAA/TSA) to increase security, both in airports and on-board aircraft. In aviation, where responsibilities and tasks are divided between several actors, implementing new security systems and procedures in a safe and secure way is not always easy, and depends strongly on adequate response and communication procedures.

Analysis of the new security measures demonstrated that little was done on-board (the main focus was on cockpit door reinforcement, better training of cabin crew, and sky marshals on board more flights). Hence, there might be a need to further increase on-board security. It is clear that a fresh approach needs to be adopted; an approach which will utilize new technologies in order to achieve the goal: create a safe, none burdening to the customer and economical security system which restores confidence of air passengers.

SAFEE aims to develop advanced aircraft security systems designed to prevent and respond adequately to in-flight threats. The main goal is to ensure a fully secured flight from departure to arrival destination. This is done through implementation of on-board threat detection systems and the provision of reliable threat information to the flight crew. In the decision making and response management process, air/ground exchange of threat level information (e.g. down-linking of aircraft voice/video information) is foreseen. In this process, SAFEE anticipates the use of the European Regional Renegade Information Dissemination System (ERRIDS), which is being developed under co-ordination of EUROCONTROL.

In this paper, we introduce the SAFEE project and its sub systems. The next Section presents some background. This is followed by an outline of the SAFEE approach and the Description of Work, focusing on the SAFEE users (pilots, cabin crew and sky marshals) and the SAFEE systems and technologies.

2 Background

Aviation security procedures are well founded in international and national regulations, laws and procedures since at least the early 70s. However, the '9/11' hijackings have shown that it is not always possible to prevent the occurrence of extremely severe events. This has led to adaptations of the aviation security standards, recommended practices and regulations, and has increased security research and development. The two main European aviation security research programs are SAFEE [1, 2, 4] and ERRIDS [3]. Whereas SAFEE focuses on the construction of an *aircraft* decision support system, the EUROCONTROL driven ERRIDS (*European Regional Renegade Information Dissemination System*) focuses on exchange of threat and incident information between ground organizations involved in handling renegades. The main goal of these systems is to ensure a fully secure flight from departure to arrival destination whatever the identified threats are.

The proponents of the SAFEE project are major European industrial actors of the Aeronautical sector associated with high level research centers, several relevant Small Medium Enterprises (SMEs) and some specialized universities. Among the 31 partners are the co-ordinator Sagem Defense Sécurité, Airbus, Thales Avionics (France); Siemens, EADS (Germany); BAE Systems, University of Reading (UK); National Aerospace Laboratory NLR, Ecorys, SITA (the Netherlands); Athena GS3 (Israel); Galileo Avionica, Selex, Teleavio (Italy); to name a few.

The project characteristics are:

Title:	Security of Aircraft in the Future European Environment
Acronym:	SAFEE
Customer:	European Commission
Scientific Officer:	Mr. Marco Brusati
Contract No.:	AIP3-CT-2003-503521
Total Cost:	36 M€
EC Contribution:	19 M€
Starting Date:	01/02/2004
Duration:	48 months
Web-site:	http://www.safee.reading.ac.uk

3 Description of Work

SAFEE project main purpose is to develop systems that will be able to address an on-board situation in the case that all preceding measures have failed. The SAFEE objective is to strengthen the last line of defense. The SAFEE approach is that waiting for new types of threats and incidents to occur and then improve security is not the right way forward. The aim shall be to proactively anticipate threats and to focus the system development on countering those threats with the highest risk. In order to identify threats, and the risks resulting from those threats, SAFEE has developed and applied a tailor made, security oriented, Risk Assessment methodology and Process (RAP), and then designed an operational concept and system requirements following challenges derived from this outcome of the risk assessment.

The project baseline is past experience, which has demonstrated that hostile persons may go through the different airport controls and security measures, access an aircraft, and even initiate hostile actions. There is therefore a need to secure the aircraft itself as the last barrier to attacks. The project is focused on the implementation of onboard threat detection systems and the provision of reliable threat information to the flight crew. In the decision making and response management process, secured air/ground exchange of threat level information is foreseen. In Figure 1 the ATM security environment and the main threats to it are depicted. On-board threats include hijacking, sabotage of the aircraft systems, bringing explosives on-board, use of biological and chemical agents, hampering of the flight controls. Not all these threats are easily detected with the current state of security systems. As long as certain threats can't be detected by the ground security and certainly not on board, there is a high potentiality of a successful attack. In the wake of the September 11th terrorist attacks, several technologies have been developed and new procedures have been implemented to improve the security in air transport.

Potential danger can be found in several areas of the Air Traffic Management (ATM) environment. SAFEE does not address all identified areas where improvement may be implemented; the project aims to strengthen the last line of defence by implementing technology to deal with on-board security issues. Within SAFEE only a number of topics are handled. The SAFEE project has defined a set of potential targets for attacks, and identified detection tools and response actions to be developed and assessed. The JAR-OPS security requirements for commercial air transportation (Ref. 6, Subpart S - Security) prescribe that the cabin crew notifies the flight crew in case of suspicious activity or security breaches in the cabin. SAFEE is in line with this, as it aims to develop new on-board security systems to support the commander, who -at present - has the end-authority for dealing with threats on-board the aircraft (up to and including emergency declaration). However, note that SAFEE also *investigates* the situation where the cabin crew has some authority to deal with threats (*low-level only*) in the cabin.

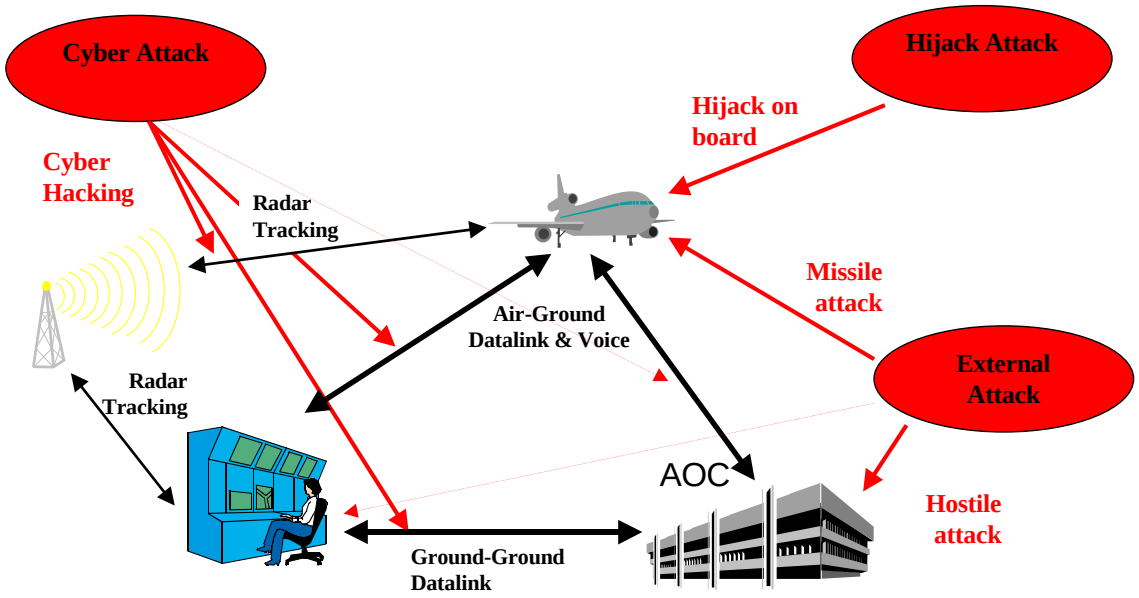

Figure 1 Overview of SAFEE Security Scope

The *SAFEE Operational Concept* anticipates security support for:

- *Pilots* – will have a modified cockpit and new equipment available for use when a threat occurs. After an attack emergency procedures will be applied.
- *Cabin Crew* – might be the first to detect acts of unlawful interference. Trained cabin crew, supported by passenger and cargo information, might be able to prevent escalation of low level threats into more severe incidents.
- *Sky marshal* – is well trained to respond to severe on-board threats, and to decide (together with the pilots) how to react in the first minutes of an attack. SAFEE also considers the possibility that there is no sky marshal on board.

The following functionalities are foreseen:

- On-board Threat Detection System (OTDS), with three functionalities:
  - Dangerous Objects Detection Function (DODF),
  - Suspicious Behavior Detection Function (SBDF),
  - Access Control and Registration (ACRF).
- Threat Assessment and Response Management System (TARMS).
- Emergency Avoidance System (EAS).
- Flight Reconfiguration Function (FRF).
- Anti Threat Data Link (ATDL).
- Electromagnetic Threat Detection System (ETDS).
- Secured voice & data communications.
- Secured open world (internet on-board).
- Authentication of pilot/crew commands.

The SAFEE systems output comprises:

- Alert / information to the cockpit crew;
- Alert / information to the cabin crew;
- Alert / information to security staff;
- Commands to the aircraft systems;
- Information to ground when necessary.

SAFEE systems input includes:

- Pre-flight data: passenger data, luggage data, cargo data, threat level data.
- Pre-flight Terrain, Obstacles, Prohibited for Security Areas (PSA) data.
- In-flight data: OTDS alerts, crew input, aircraft systems input (e.g. position), sensor data, updates of pre-flight data.
- Input from ground network systems (ERRIDS).
- Potential collision alerts (from EAS).

The SAFEE system has interfaces for the pilot (in the cockpit), cabin crew and security staff (in the cabin), on-board crew communication links, and air/ground communication links.It is also possible that on-ground security staff may obtain real-time access individual sensor output through a data-link connection (ACARS or VDL). The foreseen air/ground data-link with the ERRIDS will be the main (secured) channel/gateway for uplink and downlink of threat information from the ground to the aircraft and vice versa. Information on the status of control of the aircraft and its predicted flight path is essential to the national authorities and other decision makers. The key subsystems are introduced in the following.

On Board Threat Detection (OTDS)

The aim of the development of an On-board Threat Detection System (OTDS) is to provide means for automatically detecting upcoming threats on board of an aircraft and for alerting the cabin crew and other on-board systems in case of a detected threat. The OTDS goal is to identify a large scale of threat scenarios including threats emerging from different origins such as individuals or certain goods and materials. For the reliable detection of threats at an acceptable rate of false alert, information gained from multiple sensors needs to be evaluated and correlated. Among those sensors are video cameras and microphones (for face recognition, evaluation of voice or speech characteristics, and analysis of gait peculiarities, extraordinary motion patterns and gestures), chemical ‘sniffers’ and detection systems (for detecting weapons, explosives, chemical agents).

Threat Assessment and Response Management System (TARMS)

One of SAFEE's most innovative sub systems is the operational Threat Assessment and Response Management System (TARMS). The TARMS is assessing the overall threat level to the aircraft at any given time, by processing a large amounts of information, gathered from different sources / actors, such as the threat information obtained from on-board sensors, off-board intelligence, passenger background files, behaviour models and the expected threat scenarios. TARMS, therefore is comparing observations with expectation models, and then finally recommend the appropriate response action. TARMS will use this information to generate a prioritised menu of courses of action for actors that are feasible, safe and conform to relevant governmental policy. The decision support tool is able to analyze evident as well as hidden relationships between different input variables, work with uncertain inputs and make useful inferences in the presence of this uncertainty and missing information. The use of a probabilistic framework and probabilistic graph models (such as Bayesian networks) allow disparate sources of information to be fused. TARMS engineering takes into consideration different end users, depending on the level of the threat (cabin crew, air marshals, pilots, ground security, ATC) and links together all the actors, for the first time.

Flight Survivability

The SAFEE Flight Survivability sub systems are activated in the event that the pilot is incapacitated by a terrorist action, or perpetrators have gained access to the flight controls, and aim to prevent ‘9/11’ like scenarios where the aircraft itself is used as a weapon. SAFEE Emergency Avoidance System (EAS) ultimately foresees automatically take control of the aircraft and the generation of a manoeuvre to avoid ground or manmade structure collision. In the case of a crisis situation, the EAS is a temporary measure, as it does not propose a definitive solution to the situation. Automatic return to an airfield with all the pilot controls disabled is the final complement to EAS. SAFEE is also assuming that flight plan, suitable for a normal "no threat situation" might not be suitable when the flight risk exceeds a certain thresh hold. Therefore, EAS is connected to a so-called Prohibited Security Areas Database (PSA DB). The PSA DB is flight area information (terrain elevation data, obstacles data, and PSA data) in a hierarchical manner, based on unique risk assessment process (SAFEE RAP), developed within the SAFEE framework. When a threat is detected and processed on board and the EAS is engaged, an authorized flight area (in a non threat flight condition) can become prohibited. The area to be avoided can be a a society symbol (government institute, cultural symbol), a high risk facility (such as a nuclear power plant or a chemical industrial facility), a major sport event (the Olympic Stadium, the Superbowl), et cetera. The prohibited areas need to be established by the appropriate authorities, in a national and international level field.

Secure Communications and Data Protection

Some attempts to take over the control of an aircraft by false Air Traffic Control messages have been already detected, and the taking over of remote computers by hackers has been achieved successfully on many occasions. Securing data transfer outside the aircraft and inside the aircraft is therefore a major issue and SAFFE provide communication services that meet both safety and security requirements and increasing communications' throughput. The communication between the "open world" and the avionics of the aircraft makes it potentially very sensitive to a cyber attack by a hacker located in the aircraft or on ground. SAFEE therefore is taking advantage of the most recent progress on data encryption and of firewalls, allowing attacks detection, to report and to restore initial critical data when necessary.

Risk Assessment to further Improve In-Flight Security

The SAFEE approach is to proactively anticipate in-flight threats and to focus the system development on countering the threats with the highest risk. For this purpose, security occurrences have been analyzed and a risk and threat assessment has been performed [5]. Historically, system and concept developers avoided explicit modeling of security risks. Over the years, risk assessments were focused on accident risks, natural hazard risks, business interruption risks, project risks, and financial risks. However, the area of security risk did not receive its well deserved attention and it should be noted that there exists a clear distinction between security oriented risk assessments and safety oriented methodologies for risk assessment due to the different nature of the risk element. Safety related incidents/accidents are un-intentional occurrences, while security related occurrences often are intentional acts of unlawful interference where perpetrators are constantly seeking to exploit the vulnerabilities of the air transportation system to perform a certain threat scenario. In security related risk assessment, the vulnerability element is therefore to be included via a metric of the likelihood that various types of safeguarding against a scenario will fail. The aim is to identify potential threats, to determine timely means to safeguard against these threats, and to prioritize them according to a risk level. In SAFEE, we have introduced a new security oriented risk assessment process, which might be used by decision makers to decide on the safe and secure introduction of new security systems/concepts : the SAFEE Risk Assessment Process (RAP) [5]. A wide range of aviation security incidents and accidents (from the NLR Air Transport Security database, official ICAO reporting systems, insurance claims, regulator data, airline reporting systems, and research centers) was analyzed in the process, including terror/criminal acts – e.g. explosions, hijacks, and sabotage either in flight or at the airport, unruly passenger behavior and Security breaches – the use of forbidden items in the cabin. The aviation security databases have been used to identify and analyze threats related to current practice flight operations. The outcome of the risk assessment has been used to focus the operational concept and supporting SAFEE technologies on the most relevant in-flight threats.

4 Conclusions and recommendations

Since the events of September 11th (and, to some extent, also after the London Mega Terror Plot in August 2006), the aviation community has strengthened security, so as to counteract threats to air transport. However, analysis of the new security measures demonstrated that little was done on-board (the main focus was on cockpit door reinforcement, better training of cabin crew, and sky marshals on board more flights). Hence, there might still be a need to further increase on-board security. It is clear that a fresh approach needs to be adopted; an approach which will utilize new technologies in order to achieve the goal: create a safe, none burdening to the customer and economical security system which restores confidence of air passengers.

Therefore, this paper has introduced the SAFEE aircraft systems. SAFEE aims to ensure a fully secured flight from departure to arrival destination. The SAFEE approach is to proactively anticipate in-flight threats and to focus the system development on countering threats with the highest risk. For this purpose, security occurrences have been analyzed and a risk and threat assessment has been performed [5]. Based on the findings, the developers of SAFEE have defined 11 basic threat scenarios which the system must counter. The counter-measures are based on subsystems that will identify threats in real time, recommend on (and execute) appropriate responses and increase survivability of the flight. The basic principles for the SAFEE operational concept and system architecture have been described. The SAFEE project has defined a set of potential targets for attacks, and identified detection tools and response actions to be developed and assessed. Depending on the threat level, different security procedures for on-board actors will apply. The SAFEE Operational Concept is in line with this, and anticipates security support for pilots, cabin crew, and security staff. The SAFEE system has interfaces for the pilot (in the cockpit), cabin crew and security staff (in the cabin), on-board crew communication links, and air/ground communication links. It is also possible that on-ground security staff may obtain real-time access individual sensor output or on-board threat level information through a data-link connection (ACARS or VDL). A foreseen air/ground data-link with the European Regional Renegade Information Dissemination System (ERRIDS) will be the main (secured) channel/gateway for uplink and downlink of threat information from the ground to the aircraft and vice versa. The SAFEE operational concept and systems are now being validated with the NLR GRACE flight simulator, which is also used for security training.

One should realize that, as terrorists are constantly developing new and improved abilities and Modes of Hostile Action, in addition to analyzing and utilizing aviation security data, it is important to include the use of intelligence-based information and/or opinion gathered from security experts.

5 References

[1] SAFEE Synopsis. http://www.safee.reading.ac.uk/.

[2] O. Einav, O. Laviv. SAFEE: a European solution for airborne security, Aviation Security International, p. 24-27, June 2005.

[3] EUROCONTROL ERRIDS European Regional Renegade Information Dissemination System.

[4] A.J.J. Lemmers, T.J.J. Bos, L.J.P. Speijker. An on-board security system and the interaction with cabin crew, European Aircraft Cabin Safety Symposium, 7 -9 June 2006, Prague, Czech Republic.

[5] L.J.P. Speijker, C.J.M. de Jong, M.K.H. Giesberts, O. Laviv, D. Shumer, D. Gaultier. Risk assessment of newly proposed concepts to improve in-flight security, International Congress of the Aeronautical Sciences, 3 - 8 September 2006, Hamburg, Germany.

[6] Joint Aviation Authorities (JAA). JAR-OPS 1: Joint Aviation Requirements for Commercial Air Transportation (aeroplanes) (including Amendment 13), May 2007.