RISK ASSESSMENT OF NEWLY PROPOSED SYSTEMS TO IMPROVE IN-FLIGHT SECURITY

**L.J.P. Speijker*, C.J.M. de Jong*, M.K.H. Giesberts*,
O. Laviv**, D. Shumer**, Dr. D. Gaultier*****
*National Aerospace Laboratory NLR, **Athena GS-3, ***SAGEM Défense Sécurité**

Keywords*: in-flight, security, aircraft, risk and threat assessment*

Abstract

Aviation security concerns measures taken to counter acts of unlawful interference against civil aviation. The European Commission (EC) Project SAFEE (Security of Aircraft in the Future European Environment) aims to develop aircraft security systems designed to prevent and respond adequately to on-board threats [1, 2]. The main goal is to ensure a fully secure flight from departure to arrival destination whatever threats may occur. Among the key activities are the identification and analysis of in-flight threats. The SAFEE approach is to proactively anticipate these threats and to focus the system development on countering the threats with the highest risk. For this purpose, security occurrences are analyzed and a risk and threat assessment is performed. Based on the findings, the basic principles for the SAFEE operational concept and system architecture are defined. This paper introduces SAFEE and its risk and threat assessment process. Guidelines and recommendations for the execution of an aviation risk and threat assessment are given.

1 Introduction

Aviation security concerns measures taken to counter acts of unlawful interference against civil aviation. Since the events of September 11th, the aviation community has strengthened security, so as to counteract threats to air transport. In aviation, where the 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.

The 11th September event has shown that, by subduing the crew and passengers, hijackers can take control of a civil aircraft and use it as a guided weapon. 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. However, analysis of the 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 fully restores confidence of the 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.

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, we need to develop a tailor made, security oriented, Risk Assessment methodology and Process (RAP) for SAFEE, and to confront the challenges derived from this assignment: to identify the relevant targets and assets, to assess relevant threats, to identify vulnerabilities and loop holes, and to present potential consequences to the decision makers.

The events of September 11 have flagged the need to consider security oriented risk assessment as part of every overall system design and analysis. Historically, system and concept developers avoided explicit modeling of security risks because of challenges inherent in this effort, such as identifying relevant targets and threats; modeling threat, vulnerability, and consequence for a scenario; and presenting this information to regulators for decision making.

Over the years, risk assessments were focused on accident risks, natural hazard risks, business interruption risks, project risks, and financial risks. In these areas, those assessments were based on systematic processes and tools to understand and prioritize risks (especially those with catastrophic consequences) so that decision makers will be able to apply their resources to best use. However, the area of security risk did not receive its well deserved attention.

The distinction between security oriented risk assessments and safety oriented methodologies for risk assessment is needed 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.

Security assessments are commonly based upon analysis of Possible Modes of Hostile action scenarios (PMHAs), relying mainly on intelligence-based information, analysis of past events and activating "red teams" activities, trying to defeat the current security systems and procedures. Security assessments are then utilized into the security systems, by using a layered approach to security, also referred to as the "Security Circles" concept. After identification of a new PMHA (by intelligence or other means), the findings are immediately translated into new security countermeasures. Countermeasures are applied in a general manner, such that all threats receive the same level of importance (with no respect to threat impact and/or potentiality).

In this paper, we introduce a new security oriented risk assessment process, which might be used by regulatory authorities and decision makers to decide on the safe and secure introduction of new security systems/concepts. Section 2 presents some initiatives to improve air transport security, including the SAFEE concept. Section 3 describes the use of security incident/accident data to derive threat scenarios to be countered. Section 4 presents the SAFEE Risk Assessment Process (RAP). Section 5 contains the conclusions and recommendations.

2 Aviation security systems and procedures

2.1 International context
Aviation security procedures are well founded in international and national regulations, laws and procedures since at least the early 70s [3, 4, 5, 6, 7]. 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] and ERRIDS [9, 10]. 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 responsibilities with respect to in-flight security decision making are quite complex as, depending on threat level, different international and national organizations are involved in handling on-board threats. Responsibilities will also usually change as the threat level increases and in the case of very severe events (such as a hijacked aircraft being used as a guided missile) even military forces might become involved. This implies that it is not easy to fully oversee the impact and consequences of the introduction of new and advanced in-flight security measures on flight safety or the organizations itself.

Four threat levels of passenger disturbances were established by ICAO as definition, as to what is occurring on the aircraft [3]:

- Level 1 Disruptive behaviour,
- Level 2 Physically abusive behavior,
- Level 3 Life threatening behaviour, and
- Level 4 Attempted breach or actual breach of the flight crew compartment.

The overall target of any security system is to make the critical assets fully protected against anything that can inflict danger, damage, or threat to the asset or to its users. In air transport security, the wish could be to make the flight 100 % secure; when faced with reality, one must recognize that this will be very difficult to realize. Today, crews might need to use any means available up to and including deadly force, to e.g. prevent hijackers from gaining control over the aircraft. In case an aircraft is hijacked and used as a guided missile, military fighters are often expected to intercept the aircraft and ultimately shoot it down.

2.2 SAFEE Operational Concept & Systems

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 the air transportation system.
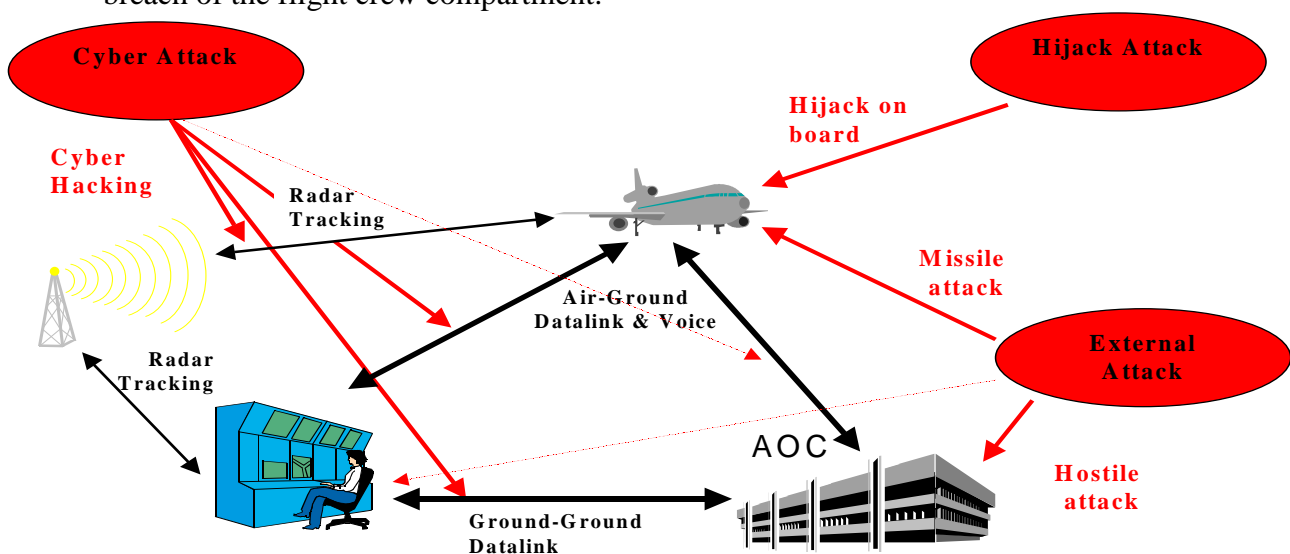

Figure 1 Overview of ATM Security Scope

Depending on the threat level, different security procedures for on-board actors apply. The *SAFEE Operational Concept* is in line with this, and 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 (DODF), Suspicious Behavior Function (SBDF), Access Control & 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.

A graphical representation of the whole SAFEE system, including the interfaces between the SAFEE systems, is shown in Figure 2.

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 [16].

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.

In order to better assess the current status of air transport security and the future situation when SAFEE is used, the impact and potentiality of on-board threats shall be defined and assessed through a risk, vulnerability and threat assessment. Traditionally, such assessment is often based upon answering the following four questions:

- Why does the attacker want to perform certain Modes of Hostile Action (MHA)?
- Why use the MHA against a certain target or asset?
- If attacked, what might be the impact of the attack? How critical is the asset?
- What is the potentiality of the attack to succeed? What is the likelihood of the countermeasures to deny the attack?
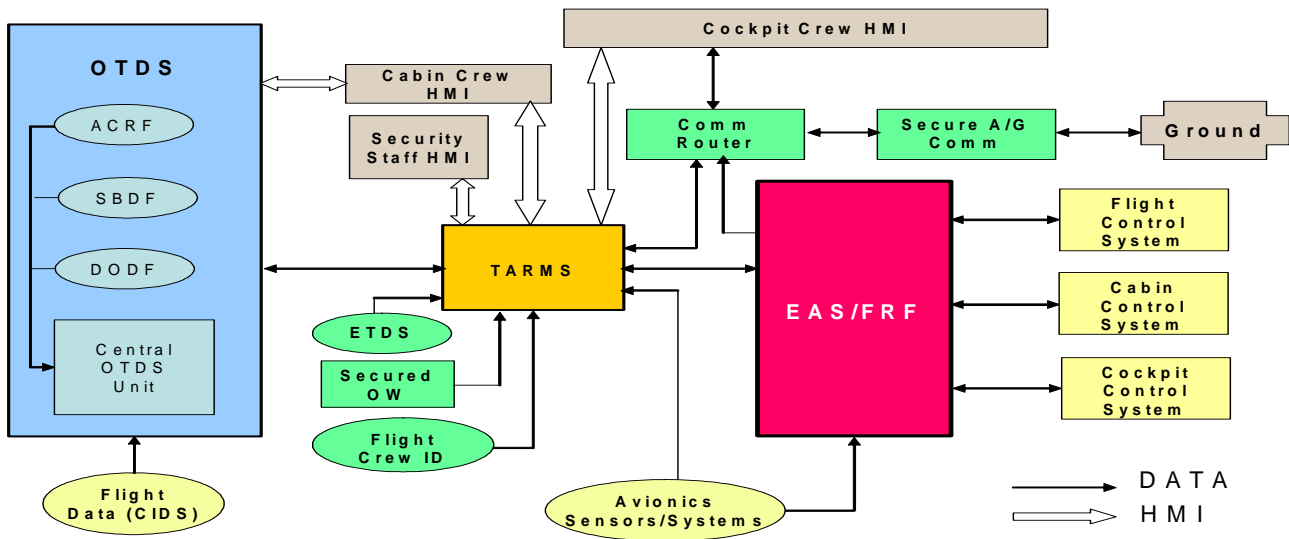
Figure 2 SAFEE on-board systems and data-flows

3 Analysis of aviation security occurrences

A wide range of aviation security incidents and accidents have occurred in the past, both during the flight and at the airport. An aviation security database helps to come up with a first assessment, based on incidents and accidents that occurred in the past, of the risk of threats occurring. Different security occurrences have been identified and analyzed:

- Terror/criminal acts – e.g. explosions, hijacks, and sabotage either in flight or at the airport.
- Unruly passenger behavior – disruptive or physically abusive behavior, and attempted breach of the cockpit door.
- Security breaches – the use of forbidden items in the cabin (found in baggage during security checks on the airport), people entering a forbidden airport area.

The NLR Air Transport Security database contains security occurrences (*e.g. hijacking, sabotage, unruly passengers, military action)* [11, 12, 13]. Data sources are: official ICAO reporting systems, insurance claims, regulator data, airline reporting systems, TSA data, Air Watch, and data from a security company.

GS-3 has selected, from its vast security database, the most relevant onboard terror incidents based upon the following sources: National Memorial Institute for the Prevention of Terrorism (MIPT), International Policy Institute for Counter Terrorism (ICT), Air safe web site; and information from open sources (e.g. internet), using special search tools dedicated for anti terror purposes.

These data sources use different classifications for security occurrences and also describe these occurrences with different levels of detail. An interesting finding is the apparent lack of statistical trends over the years (see Figure 3).
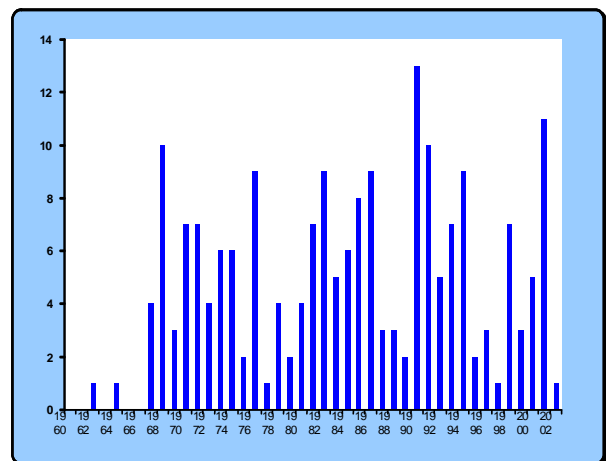

Figure 3 Example number of major occurrences [12]

The aviation security databases have been used to identify and analyze threats related to current practice flight operations. One of the outcomes is a list of threat scenarios that have been used by terrorists to invade through the security systems, exploiting the vulnerabilities inherent in those systems. After assembling this threat scenarios list, it has been 'tested' against a variety of examples of security occurrences and information gathered through brainstorm sessions with security experts and operational experts. It appears that a full list of in-flight security occurrences can be related to one (or more) of eleven identified scenarios which are used within the threat assessment process (for confidentiality reasons it is not possible to describe these scenarios in detail in this paper).

4 Risk assessment process

4.1 Concept of building a validation case

The concept of Validation Case Building is well embedded in the European Operational Concept Validation Methodology (E-OCVM) for providing the argument for introduction of ATM systems/concepts [19]. Since 2005, E-OCVM is required to be used in all new EC and Eurocontrol projects dealing with validation of ATM systems. It requires construction of a Safety Case, Business Case and Human Factors case. In this context, EUROCONTROL has recently also started the development of a Security Case Methodology [10]. Such analysis considers:

- Security impact of bringing a new security system/concept into operation.
- Decommissioning of existing systems which will be replaced.
- Staff training, clearance level and qualification.
- Abnormal modes of operation.
- How to validate all the assumptions.

A Security Case will proof the security concept of a new system/concept against security objectives and targets. As such it will deal with the outcome of the threat assessment and

vulnerability analysis of a new system/concept, in line of defense for security against all potential attacks (threat scenarios). The aim is to provide answers to the questions:

- What is being assessed?
- How secure should it be?
- Is the design secure?
- Is the implementation secure?

An important part of building such Security Case is the execution of a threat assessment. In principle, there are two ways to support the introduction of new security systems, namely by showing that the risk of threats to occur:

- does not increase with the introduction of the proposed security system/concept (a relative assessment);
- does not exceed some pre-defined risk requirement (an absolute assessment).

4.2 Risk and threat assessment principles

The first step in preventing or minimizing the damage caused by terror attacks is assessment of the risks to the security system. It provides the foundation for selection and implementation of countermeasures to reduce the risk associated with existing or new threats.

Assessing threats requires a different approach than other risks: terrorist attacks and sabotage events do not follow a 'natural' or 'predictable' pattern, and thus shall be dealt with in another way than safety related incidents/accidents. Traditionally, risks are measured as function of event frequency and probability that all safeguards fail. However, to assess the risk of a security occurrence, we have to address threat (posed by the attacker) and vulnerability (lack of safeguarding of a system against threats).

In order to come up with the new SAFEE risk assessment methodology, several systematic risk assessment methodologies, utilized by Airbus, NLR and GS-3 (all members of the SAFEE Consortium) have been analyzed [11, 14, 15, 16, 17]. Material from Eurocontrol and ICAO [4, 5, 9, 10] has also been analyzed,

because SAFEE aims to be consistent with regulatory requirements and best practices. The diagram[1] represents a relationship between Risk, Vulnerability, Threat and Assets; the concepts upon which the SAFEE risk assessment methodology has been built.
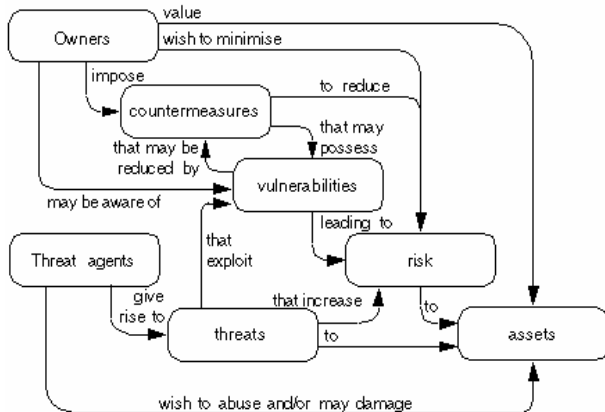

Figure 4 Security concepts and risk relationships [14]

The risk of loss of an asset is linked to vulnerabilities it possesses, which are exploited by threats. The assessment consists of defining assets, determining vulnerabilities and threats, so that we are able to assess the risk (i.e. threat) level. Countermeasures may be specified to lower the risk, and will be expressed in the form of Security Design Objectives. Note that threats considered as such are malevolent actions (aggressions). This differs from the Mehari model [14], where threats of misuse or dysfunction are also considered.

4.3 Risk Assessment Methodology

The SAFEE risk assessment methodology is used for assessment of the risk related to in-flight threats, and consists of 4 consecutive phases comprising fourteen tasks (Figure 5).

The risk assessment aims to identify potential threats, to determine timely means to safeguard against these threats, and to prioritize them according to a risk level. The outcome of a threat assessment shall always be accompanied by a proof that safety is not jeopardized.
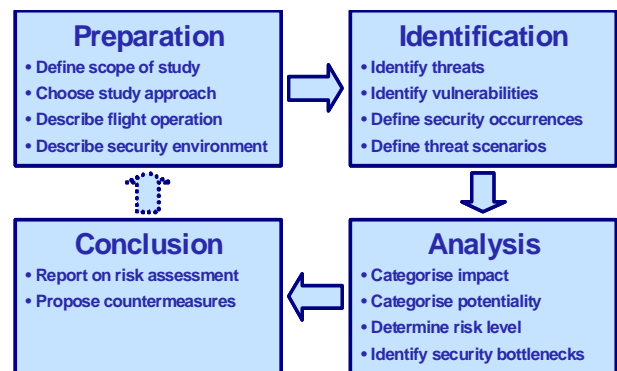
------

[1] Common Criteria, Chapter 4 from Part 1 [14]

Figure 5 Four phases of risk assessment [11]

The goal of the **preparation phase** is to understand the 'problem', i.e. to sketch the operation and its security environment, to explain the (user's) need for performing the operation, and to determine a way to investigate the problem. The preparation phase identifies assets and vulnerabilities to be protected and provides a sufficient description of the operational environment of these assets.
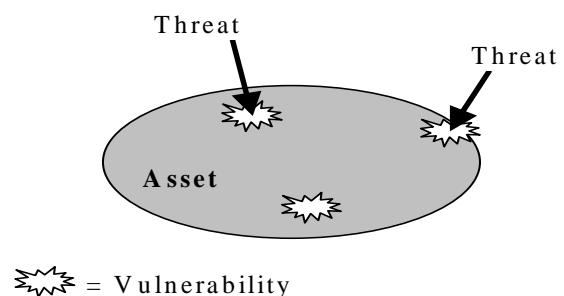

Figure 6 Assets, vulnerabilities and threats [11]

Threats existing in the operational environment need to be identified and understood. This is done in the **identification phase**. The individual threats are structured into threat scenarios. A scenario is defined as a sequence of modes and events leading to a security occurrence (a security-related accident or incident). Modes indicate states of for instance systems, human operators, or the aircraft; events signify changes between these modes.

The purpose of the **analysis phase** is to estimate the risks associated with the threat scenarios. As risk is characterized as the combination of the severity of the outcome of

an event and its likelihood of occurrence, the impact and potentiality of the threat scenarios needs to be assessed and evaluated.

Finally, **conclusion and recommendations** need to be drawn from the risks as evaluated in the analysis phase. Here, it will be necessary to understand the risks and to translate them into security objectives or requirements for the operational environment. When it is determined that risk levels are (too) high, countermeasures will need to be defined that reduce either the impact of the consequence of a threat, or the potentiality of its occurrence.

4.4 Risk Level Determination

The purpose of the analysis phase is to **determine the risk levels associated to the threat scenarios**. Risk is defined as the combination of the gravity of an event, and the likelihood of its occurrence. The gravity of a threat scenario is expressed by the impact of the consequences of the scenario. The likelihood of a threat scenario is expressed by the potentiality of its consequences. Several aspects appear relevant when estimating the potentiality of a scenario, for instance:

- The level of skills and knowledge required by the perpetrators.
- The availability of required means, such as weapons and electronic devices.
- The opportunity that the security environment offers to place the attack.
- The expected potential gains, for instance in money or media attention.
- The chance to be caught and punished.

Initial impact and potentiality metrics for classification of a threat scenario are given in Appendix A. The consequences of a threat scenario must be assessed according to all metrics, i.e. a total of 15 metric items will need to be assessed through use of expert opinion, incident/ accident data analysis and/or intelligence. Note that the potentiality class has been split into two separate classes, based on the motivation and possibility for an attack.

After this classification process, which involves assessment of all the consequences for all metric items, the threat scenarios are ranked according to the impact and potentiality results. In this ranking process, the scenarios with high attack motivation and high attack possibility are ranked with the highest potentiality. Since different estimated effects will be applicable to a threat scenario, mathematics might be used to translate the impact metrics and potentiality metrics into one impact ranking and one potentiality ranking.

When impact and potentiality rankings for the threat scenarios have been determined, the risk level of the security occurrences follows from a risk level matrix (see Table 1). Such matrix is based on the notion that security occurrences with a large impact should have a low potentiality, and consequences with a high potentiality should have little impact.

Table 1: SAFEE risk level matrix (proposed)

Impact Potentiality	Strong (4)	Medium (3)	Weak (2)	No impact (1)
Probable (A)	4A	3A	2A	1A
Possible (B)	4B	3B	2B	1B
Unlikely (C)	4C	3C	2C	1C

Acceptability of threats and risk is a sensitive issue, which needs to be decided through a political process rather than in engineering. The proposed risk level table will therefore need to be backed up by regulators. Security system and/or operational objectives and requirements are to be established if the risk level is higher than deemed acceptable.

4.5 Security objectives and requirements

It might be necessary to define countermeasures that reduce either severity of the consequence of an individual threat, or the likelihood of its occurrence. The security objectives should be consistent with the stated operational aim or product purpose of the

system, and any knowledge about its physical environment. The need for defining a set of security objectives was already recognized by regulatory entities in the wake of the 9/11 events. ICAO has made amendments to Annex 17 of the Chicago Convention, which identify additional areas of concern, clarify aviation security objectives in a changing environment, and recommend changes to authority delegation, information sharing and response mechanisms. EUROCONTROL suggests that, as part of the security case, a set of security objectives must be developed against which a new security system will be assessed. The security objectives are based upon the consequences that can be accepted by the regulators, the security experts, and the public.

The purpose of determining security objectives is to address all of the security concerns and to declare which security aspects are either addressed directly by the system or by its environment. This categorization is based on a process incorporating database research, overall security policy, risk assessment and risk level acceptance decisions. Security objectives are needed for two reasons:
- Enforce security policies – once approved, security objectives may serve as leverage to enforce the security policy due to the fact that the security objectives were determined as a result of prior analyses.
- Counter risks – the main objective of security systems is to counter risks, and the best way of checking that the system meets its objectives, is to check it against predetermined objectives.

Security objectives aim at either protecting the asset **before** an attack (e.g. deterrent or preventive measures), or by reducing the effect of an attack **after** it has arose (e.g. protective, palliative or recovery measures). In order to produce security objectives, experts should review the newly proposed security system together with the assessed risk level (the outcome of the threat assessment) and define a

qualitative scale for definition of the objective. E.g. because hijacking was ranked as bearing a high risk, reinforced cockpit doors accompanied with tight security procedures were introduced. The security objective for this could be that the number of times the door is opened not in accordance with the security procedures should be zero. A similar objective could be derived from a requirements demand that the cockpit door must be locked from the time the cabin doors were closed until they are open again. The security objective then can be that every time the door is opened during flight, possible hijack countermeasures are implemented fully. Every time the door was opened and the countermeasures were not enforced by the crew, it will be reported as a failure of the security system.

5 Conclusions and recommendations

This paper introduces SAFEE and its risk and threat assessment process. 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 is performed. Based on the findings, the basic principles for the SAFEE operational concept and system architecture have been defined. Guidelines and recommendations for execution of an aviation risk and threat assessment have been given.

Risk Assessment Process (RAP)
A comprehensive Risk Assessment Process is the essential primary component of any security system. The identification and grading of the risks –according to their potential impact or potentiality – are essential for developing the best corresponding countermeasure and design. During this study study, it was decided that the SAFEE RAP uses a *qualitative approach*, which is based on a *relative assessment* of the risks related to the SAFEE Operational Concept Description with the current situation.

It is important that the decisions upon acceptable/unacceptable risk level are taken by the regulators and are not changed during the risk assessment itself. The regulators might use conclusions and recommendations of the security experts to adapt the aviation security requirements and objectives, when it appears to be necessary – there will be more information to use at the end of the process. Even the lowest risk, as long it poses some level of risk, must be considered and carefully analyzed. In this decision making process one should realize that flight safety must not be jeopardized by introduction of new security procedures.

Security incident/accident analysis
Aviation security databases have been explored to come up with a first assessment of the risk of each of eleven defined SAFEE in-flight threat scenarios to occur. Two databases were used: the air transport security database of NLR (with 20000 occurrences) and the aviation terror database of GS-3. Past occurrences are often used to stimulate the security effort and not as only source for evaluating the threat potential.

The role of intelligence
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.

Further work and co-operation
The SAFEE team uses the Risk Assessment Process (RAP) to evaluate the SAFEE system design. SAFEE participants are working in the EUROCAE Working Group 72 'Aeronautical Systems Security' towards a Handbook for Civil Airborne Systems Security Assessment. The authors also acknowledge the co-operation of SAFEE with the Eurocontrol ATM Security Domain, which is responsible for the ERRIDS.

6 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] ICAO Annex 17 to the Convention on International Civil Aviation 'Security–Safeguarding International Civil Aviation against acts of unlawful interference', (up to and including amendment 11), July 2006

[4] ICAO DOC 8973; Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, 6th Edition, 2006 (restricted).

[5] ICAO DOC 9811; Manual on the implementation of the security provisions of Annex 6 (Aircraft Operation) (restricted);

[6] ECAC Doc No. 30, ECAC Policy Statement in the field of Civil Aviation Facilitation 9th Edition/July 2003 (amended by DGCA/122), including additional Annexes K and L (2005) and M (2006) (Restricted).

[7] Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security – Inter-institutional declaration (*Official Journal L 355, 30/12/2002 P. 0001 - 0022).*

[8] European Commission Single European Sky (SES) Committee Regulation on common requirements for the provision of Air Navigation Services, 2006.

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

[10] EUROCONTROL Security case methodology.

[11] C.J.M. de Jong, M.K.H. Giesberts, L.J.P. Speijker; Threat Assessment Methodology, National Aerospace Laboratory NLR, CR-2004-435;

[12] M.K.H. Giesberts, B.A. van Doorn, L.J.P. Speijker, G.W.H. van Es; Aviation Security Database, National Aerospace Laboratory NLR, CR-2005-063.

[13] B.A. van Doorn, M.K.H. Giesberts; Review and analysis of security occurrences, National Aerospace Laboratory NLR, CR-2005-387.

[14] MEHARI, Commision Methods, Club de la Securite des Systemes d'Information Francais, Clusif, Version 2, August 2000.

[15] Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031.

[16] G. Gobbo. SERA Risk Analysis and Vulnerability Identification Methodology, Airbus, SAFEE 40AIF_ 040308-1_T02, March 2004.

[17] O. Laviv, D. Shumer. Security Risk Assessment - a Methodology, Athena GS-3, October 2005.

[18] A. Lemmers, T. Bos, L.J.P. Speijker. An on-board security system and the interaction with cabin crew, European Aircraft Cabin Symposium, Prague 2006.

[19] EUROCONTROL Air Traffic Management Programme (EATMP); European Operational Concept Validation Methodology (E-OCVM).

Appendix A   Initial impact and potentiality metrics

	Potentiality level		
Risk factor	**Probable** (A)	**Possible** (B)	**Unlikely** (C)
Possibility			
Required skills	No special skills required	Requires some Knowledge or skills	Requires expert knowledge or skills
Required means	No special means required or the required means are easy to obtain	Required means can be made available with difficulty	Required means are difficult to obtain and/or to apply
effectiveness of the existing security countermeasures	Security countermeasures are not effective or ill-fitting the threat	Security countermeasures are limited or have low level of effectiveness on the threat	Security countermeasures are very effective on the specific threat
Defender's current intelligence information	No information about intention to attack	General information with no specific target	Specific information about time and place of attack
Time opportunity	Attack can be placed (almost) at any moment in time; time does not play a role in the attack	Time plays some role in the attack	Time plays a crucial role; a successful attack can only be placed at a few moments in time
Motivation level			
Financial profit for each one of the different parties involved: – The planner – The attacker or his family – The collaborator	All the parties involved or at least one of the parties involved will receive a large sum of money (above ten thousands dollars)	All the parties involved or at least one of the parties involved will receive only a fair sum of money (few thousands of dollars)	All the parties involved or at least one of the parties involved will receive negligible sum or no money at all (few hundreds of dollars)
Receiving Media attention and coverage	World coverage with vast attention	Regional coverage and fair attention	Very small coverage and attention
Glorification of the attacker or organization by : The people which the attack was directed at. The attacker's supporting environment The attacker's followers	Receiving world wide recognition as being very courageous and fearless	Limited recognition as being very courageous and fearless	no change in recognition
Impunity of the attack's planner	Small chance of being caught	Fair chance of being caught	High chance of being caught
Impunity of the attacker	Small chance of being caught	Fair chance of being caught	High chance of being caught

Effect on …	Impact class			
	Strong (4)	**Medium** (3)	**Weak** (2)	**No impact** (1)
Human life	Multiple Fatalities	Few fatalities	Minor injuries	No effect
Aircraft and infrastructure	Loss of aircraft Damage to infrastructure on the ground	Aircraft unusable for limited time	Minor damage	No effect
Air traffic control and overall security operation	Transportation impossible for a significant time and/or in a large region Disorganisation of ground services New developments and major changes of security countermeasures and operation	Re-routing of some aircraft Flight interrupt Limited security upgrade and operational improvement	Slight delays in flight schedules Minor changes in the security operation	No effect
Global – political and/or economical and/or military tension	Dramatic political change and/or full military campaign and/or dramatic economical drop	Long-term Political pressure and/or Limited Military operation and/ or Long-term economical change	Short-term or minor political pressure and/or minor military movements and/or short-term economical change	No effect
Public confidence in aviation	Dramatic and extensive loss of confidence in air traffic	Long term loss of confidence in air traffic	Short term loss of confidence in air traffic	No effect