SAFEE (Security of Aircraft in the Future European Environment)

FINAL PUBLISHABLE REPORT

Abstract

This Final report presents the SAFEE project (Security of Aircraft in the Future European Environment), co funded by EC (contract number AIP3-CT-2003-503521), started on February 1st, 2004 and finished on April 30th, 2008.

This 51 months project was an Integrated Project of 32 partners from 12 European countries.

SAFEE addressed security on board an aircraft as a response to several security related incidents in the past. All SAFEE studies were driven by investigating prevention of terrorism by direct human acts and by electronics means. Results on such field are quite sensitive and can't be disseminated without any control of the destination. In fact, dissemination was achieved by organising six User Club meetings with the participation of European experts dealing with Air Transport, Aeronautics and Security.

Documentation Tables

Programme	FP6-2002-AERO-1 & AERO-2; Priority 4: Aeronautics and Space – call March 03		
Project Acronym	**SAFEE**		
Contract Number	AIP3-CT-2003-503521	**Proposal Number**	503521
Project Co-ordinator	Sagem Défense Sécurité		

Document Title	**SAFEE_Final_Publishable_Report**		**Deliverable**	Final Report	
Document Id N°	SP0SAG_080109-1_E	**Version**	A1	**Date**	28/05/2008
Status	**Published as version A0 to ALL**				

Project Classification	**PUBLIC**

Filename	SP0SAG_080109-1_EA0_SAFEE_Final_report	
Document manager	Daniel GAULTIER	Sagem Défense Sécurité

Approval status		
Authors	**Responsible Partner Verification**	**Project Approval**
WP & SP Leaders	PMC Members	Coordinator
SAFEE partners	-	Daniel Gaultier

Revision table

Version	Date	Modified Pages	Modified Sections	Comments
A0	28/05/2008			**Published as version A0 to ALL**
A1	23/06/2010		Title	**Add “Publishable” in the title**

This document is classified as PUBLIC Information

Table of Contents

Table of Figures

1 EXECUTIVE SUMMARY

This Final report presents the SAFEE project (Security of Aircraft in the Future European Environment), co funded by EC (contract number AIP3-CT-2003-503521), started on February 1st, 2004 and finished on April 30th, 2008.

This 4 year project was an Integrated Project of 32 partners on 12 European countries.

SAFEE addressed security on board an aircraft as a response to several security related incidents in the past. All SAFEE studies were driven by investigating prevention of terrorism by direct human acts and by electronics means. Results on such field are quite sensitive and cannot be disseminated without any control of the destination. In fact, dissemination was achieved by organising 6 User Club meetings with the participation of European experts dealing with Air Transport, Aeronautics and Security.

This report covers:

- SAFEE Abstract
- SAFEE Project Objectives
    - SAFEE concepts of operations
    - SAFEE Systems
    - Validation of SAFEE Systems and Training
    - Evolution of Objectives of Original Proposal
    - Management of Activities
- Main Achievements in SPs
- Main conclusions reached
    - Legal Study
    - Threat assessment
    - Training
    - Economics
    - Operational conclusions
    - Impact of User Club members
- Recommendations for future researches

In some Annex are listed:

- Extract of glossary of terms definition,
- List of partners,
- Work packages breakdown of SAFEE
- List of publications

2 SAFEE PRESENTATION

The SAFEE IP was a large integrated project designed to restore full confidence in the air transport industry. The overall vision for SAFEE was the construction of advanced aircraft security systems designed to prevent on-board threats. The main goal of these systems is to ensure a fully secure flight from departure to arrival destination whatever the identified threats.

The baseline of the project was the assumption that upstream identification control and airport specific security measures have all been completed. The project focussed on the implementation of a wide spectrum of threat sensing systems, and the corresponding response actions against physical person(s) or electronic intruders. One of the key aspects of the project was an integrated information management system underpinned by a secure communication system.

For reaching these objectives SAFEE had 5 key activities (Sub-Projects):

SP1 - Onboard threat detection: an integrated threat detection system based on multiple sensor information has been specified, prototyped and evaluated.
SP2 - Threat Assessment and Response Management System: an urgency decision making tool
SP3 - Flight protection, which includes an Emergency Avoidance System and an automatic control of the aircraft for a safe return
SP4 - Data protection system securing all the data exchanges (in and out the aircraft).
SP5 - Security evaluation activities, including legal and regulatory issues about citizens' privacy and rights, economic analysis, and dissemination activities

The proponents were major European industrial actors of the Aeronautical sector associated with a high level research centre, several relevant SMEs and some specialised universities. A certain degree of confidentiality on proposed sensors and technologies was, for obvious reasons, imposed on the obtained results.

2.1 EVOLUTION OF OBJECTIVES OF ORIGINAL PROPOSAL

To monitor the evolution of the SAFEE objectives WP5.3 deployed a continuous survey on the evolution of the SAFEE subsystems development. Hence, the OCD evolved in order to track the evolution of the system and operational design. Finally a new task, WP5.3.5, has been created to demonstrate the structured modelling of requirements from the OCD. This set of requirements relates to the interfaces among the different subsystems developed in SAFEE. It also provides a clear view of the gaps that still remains to be fulfilled with further research, when comparing the needs addressed in the OCD and the actual performances of the systems according to the validation results.

A very interesting modification of the WP5.3 scope has been the collaboration that took place with the ERRIDS programme run by EUROCONTROL. The collaboration with ERRIDS was started during period 1 and several meetings with ERRIDS team aiming at a global common Operational Concept Definition were arranged.

In addition, to support the validation process based on E-OCVM, the Operational Concept has been systematically and formally analysed with the Objectiver tool in order to build a baseline model. This analysis consisted of a complete and structured inventory of goals and requirements used to trace design artefacts back to the requirements and to identify, for the sake of validation, potential discrepancies between requirements and implementation more easily.

3 SAFEE PROJECT OBJECTIVES

3.1 SAFEE CONCEPT OF OPERATIONS

The general goal of SAFEE was to develop a set of advanced on-board security functions in order to allow the crew to handle in-flight security incidents. SAFEE was to make a significant contribution towards the construction of an advanced on-board aircraft security system designed to operate during on-board threat scenarios. The functions improve the security in the aircraft by advanced detection and alerting capabilities. In combination with new security training concept the threat of a security breach is significantly reduced, limiting the impact of hostile actions, and enabling the aircraft to return safely to the ground.
This general goal was addressed in SAFEE through the implementation of 5 interconnected sub-projects that cover:

- Threat detection functions (access control, dangerous goods detection, automated surveillance)
- Automated threat assessment and response management assistance
- Countermeasures :
  - protection of the flight path,
  - data and voice communication protection
- Training. Pro-active security approach, improving detection, reaction and crew confidence.

The operational goals in SAFEE are:

- To identify a large set of threat scenarios including threats coming from persons, goods and materials, and attacks on data and communications.
- To identify weaknesses in current systems
- To produce and demonstrate technologies and systems allowing the detection of such threats with a high probability
- To produce alarms and propose actions to the on-board crew (and possibly the ground staff)
- To launch automatic actions such as data restoring, emergency avoidance of terrain impact, or clearing aircraft of terrain and obstacle hazards
- To test these systems on ground in realistic environments
- To assess the acceptability and deployment conditions of these systems
- To contribute to international standardisation and to operational procedures

The Operational Concept was further detailed in the Operational Concept Description (OCD) to ensure that the lower level objectives were understood on a project wide basis whilst defining a general strategy to address the specific needs of SAFEE. The OCD takes into account the ***Cockpit crew*** – as being instrumental in the handling and safety of the aircraft. The SAFEE concept recognises the commander as the most important decision-maker in the aircraft. Only in certain conditions (time constrains, or incapacitation) other security actors are allowed to take autonomous decisions. The pilots have also to be able to control the communication between the aircraft and the ground.. The ***Cabin Crew*** – due to the close contact with the persons in the aircraft the cabin crew is pivotal in the assessment of situations on board and reacting to them. With the introduction of the closed cockpit door concept the role of the cabin crew members in handling an incident has significantly changed. The crew is the first to face on-board threats, to deal with acts of unlawful interference (e.g. intolerable passenger behaviour), and to initiate actions. And the ***Sky marshal*** – when on board, the security officer needs to be in the loop when threats are detected.

In the decision making process on the ground, the g*overnment* - as final and decisive actor - has ultimate responsibility, i.e. governmental decision-making is instrumental in handling hijack and renegade situations. Military operations and Air Traffic Control (ATC) and Airline Operations Centre (AOC) are involved when such a threat occurs. Specific roles are therefore foreseen for these (ground-based) actors (Air Traffic Control, AOC, and authorities) when dealing with on-board threats. To support the actors on the ground, the SAFEE project cooperated with the development of new security decision support systems, such as ERRIDS "European Regional Renegade Information Dissemination System", which was proposed by Eurocontrol/NATO. The OCD defines potential SAFEE – ERRIDS interfaces that were developed during the project in co-ordination with Eurocontrol. Information on the threat assessment and response measures to the threat onboard the aircraft is considered essential information to the decision makers on the ground in order to take appropriate response measures. SAFEE introduced technology that would allow interfacing of the stakeholders, both on board as well as on the ground. ERRIDS was designed to take into account both available and emerging air-to-ground and ground-to-ground voice and data link systems. During the SAFEE project a trial was performed demonstrating how an ERRIDS-SAFEE interface and secure gateway could provide effective and timely data exchange between the stakeholders involved.

3.2 SAFEE SYSTEMS

In order to illustrate the developments within the SAFEE project, the next sections describe first the present situation for an aircraft in flight, and then compare this to a condition with the SAFEE security enhancements.

3.2.1 Present-day situation for an aircraft in flight

Erreur ! Source du renvoi introuvable. displays links between actors and systems in today's operational conditions.

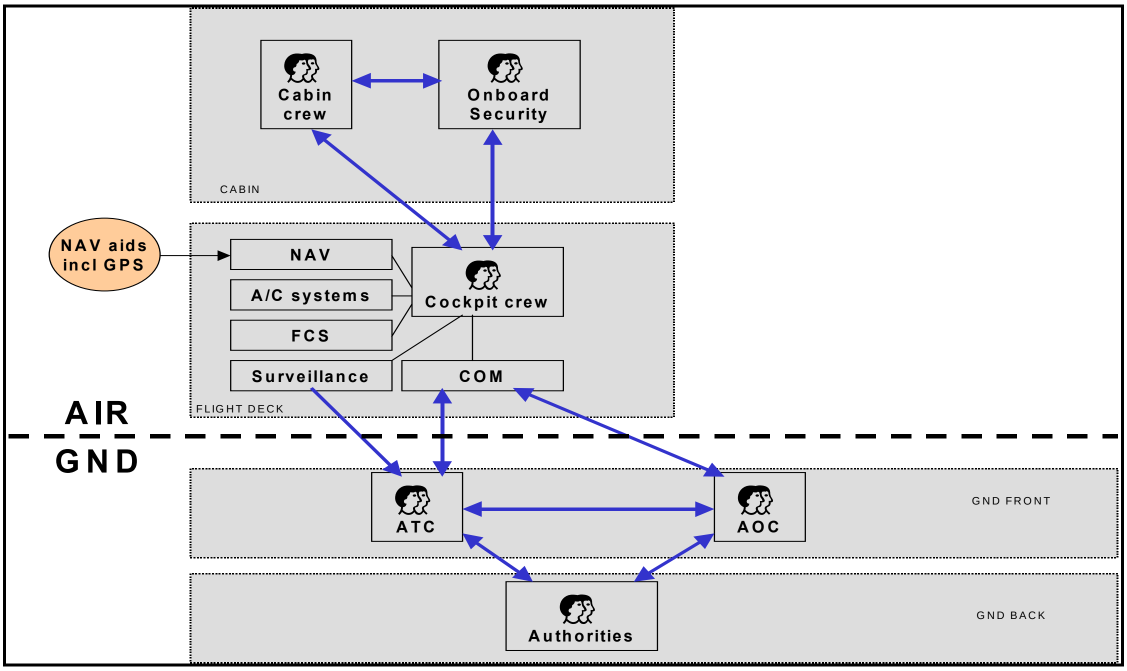

figure 1. Present On-board Systems and Data Flows

The aircraft flight crew communicates with ATC through surveillance (XPNDR, ADS-B) and communications systems (voice, CPDLC). The AOC may interface with the aircraft through voice (VHF or SATCOM) or through a data-link (ACARS, VDL).
Further relevant on-board systems in the process description are navigation systems (NAV), Automatic Flight Control Systems (AFCS, including auto-flight and engine thrust management), aircraft systems (hydraulic, electric, pneumatic). In case of security events on board both ATC as well as AOC will contact the following authorities whenever necessary:

- Airport authorities (fire-fighting, airside access control)
- Military (air force, special forces)
- Government (local/regional/national/international)

- Law enforcement

3.2.2 Flight with SAFEE functions

Within the SAFEE project, new security systems have been developed to detect, and provide a response to possible unlawful acts. These new systems interact with current aircraft systems as is illustrated in **Erreur ! Source du renvoi introuvable.**.

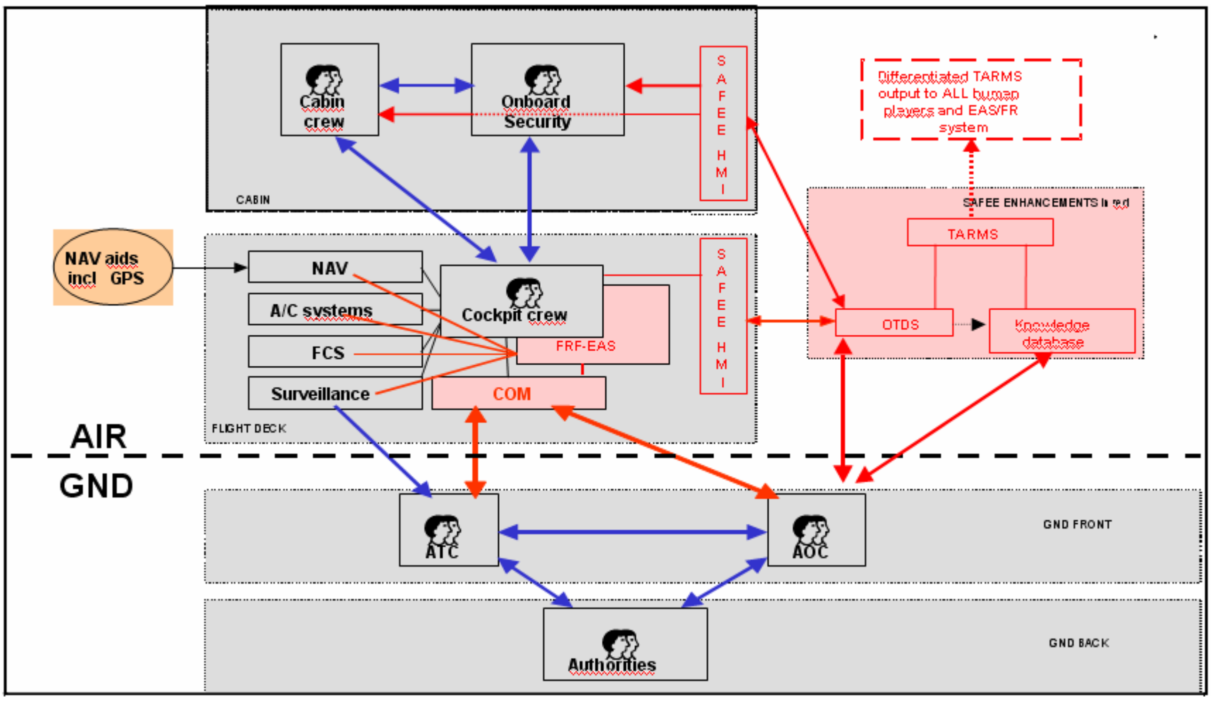

figure 2. SAFEE On-board Systems and Data Flows

In the figure 2, the on-board SAFEE functions (in red) are presented on a very abstract level, to show interoperability and interdependency with current systems and users. (The SAFEE HMI in the cabin is the paramount interface with the cabin crew).

The OTDS (Onboard Threat Detection System) aims at detecting unauthorized access, dangerous materials, or suspicious human activity. This is achieved by evaluating and correlating data from several kinds of sensors. The output of this system is an alert that is forwarded to the TARMS (Threat Assessment and Response Management). Only when a trigger level has been surpassed, information or an alert will be provided to the crew Using a combination of alerts generated by the OTDS and a dynamically derived knowledge base, TARMS determines first the threat situations, (with probabilities), followed by a recommendation of possible responses to deal with the perceived threats. Output is sent to the crew, and, only in very few cases, directly to ground actors for emergency reasons. When TARMS concludes that the cockpit crew is no longer in control of the aircraft, it will protect the flight path by initiating an automated maneuver through the EAS (Emergency Avoidance System). The EAS disables all unauthorized input to both the flight controls and. aircraft systems. This includes protection of electrical circuits, hydraulic systems and engine power. In addition to the EAS, a paper study has been performed to investigate a Flight Reconfiguration Function (FRF). This function would allow an automated landing at a secure airport in the case that both pilots are incapable of regaining control over the aircraft.

Finally, data flows between the aircraft and the ground and inside the aircraft are secured. An important requirement of secured data mobility is the detection of disrupted data, due to manipulation or consistency loss. All users of Internet Technology systems are ensured that the data they receive is reliable, and consistent. This will be in the future even more important then it is today since, with the SAFEE systems operational, the number of potential users of information will increase. Whereas currently only AOC and ATC are in contact with the aircraft, once SAFEE systems are deployed it might become standard that Authorities receive information via the commander on the detection of high level of threats, or will be alerted when an aircraft initiates autonomous flight maneuvers.

The SAFEE systems have interfaces for the pilot (in the cockpit), for the cabin crew and security staff (in the cabin), on-board crew communication links, and air/ground (voice and data) communication links. The SAFEE systems output (in flight) comprises:

- Alert/information/advice to the cockpit crew;
- Alert/information/advice to the cabin crew;
- Alert/information/advice to security staff;
- Commands to aircraft systems (only after authorisation of the pilot) or failed authenication of the cocpit crew);
- "Information"[1] to the ground when necessary (only after authorisation of the pilot).

SAFEE systems input includes:

- Pre-flight data (loaded pre-flight into TARMS and OTDS,):
  - Passenger data;
  - Luggage data;
  - Cargo data;
  - Threat level update data;
  - Pre-Determined Indicators (PDI) data.
- In-flight data input:
  - Security sensor data;
  - Manual crew input to TARMS via HMI;
  - Aircraft systems input (e.g. position, time, etc…);
  - Updates of the pre-flight data.
- Input from other decision support systems (e.g. ERRIDS).

3.2.3 Flight deck integration

SAFEE will use the Electronic Flight Bag (EFB) as principle platform to manage the security functions developed in SAFEE. Using biometric access control, the crew can enter these functions to review data, to review and manage alerts and to manage information distribution both inside the aircraft as well as to stakeholders outside. Future applications might include functions that allow ground security staff to obtain real-time information via a security report sent by the captain.

3.3 VALIDATION OF SAFEE SYSTEMS AND TRAINING

3.3.1 Overview of the SAFEE Validation process

The SAFEE Validation Process was based on the Validation Guideline Handbook (VGH) proposed by the MAEVA project. As during the SAFEE initial steps, and thanks to the works performed by the CAATS project, the MAEVA VGH evolved to the European Operational Concept Validation Methodology (E-OCVM). SAFEE decided to take benefit of this improved methodology and adopted it for the validation work to be performed in the project. The application of the E-OCVM has enabled SAFEE to provide the necessary evidence to demonstrate how the solutions proposed by SAFEE are applied through implementation and application of an operational concept.

The validation process consisted of five steps which were supported through the validation experiments as described later in this section.

- Elaboration of an Operational Concept, performed in the WP5.3.1,
- Identification of the validation aims, objectives and hypothesis, performed in the WP5.3.2,

[1] Definition of such "Information" was defined within the ERRIDS-SAFEE collaboration work

- Elaboration of the Validation design-plan and preparation of the validation exercises, performed in the WP5.3.3,
- Execution of the validation exercises, performed in the corresponding WPs of SP1, SP2, SP3 and SP4,
- Evaluation of the Validation, performed in the WP5.3.4.

The development of an Operational Concept Description (OCD) ensures that the problems are understood whilst defining a general strategy to address the specific needs of SAFEE. The objectives pursued by the operational concept must be broken down into quantifiable elements to the level of system parameters that can be monitored in each Sub Project. This has led to the identification of the validation requirements needed to identify the validation technique(s) that are used and the precise configuration of the validation platform.

In order to better enable the linkage between the OCD elaborated and the systems actually developed, a new task, WP5.3.5 has been performed in the validation process. In this task system requirements have been derived from the OCD. This has enabled an easier comparison between the OCD and the real systems developed in the SAFEE project.

3.3.2 Operational Scenarios

One of the first steps in the validation process, as part of the OCD, was to define the operational scenarios. The security threat assessment indentified the following eleven of SAFEE scenarios related to in-flight threats.:

1. Mix up navigation to fly the aircraft into an object by remote "control" cyber attack.
2. Take control of the aircraft to destroy a target and the aircraft
3. Detonate a Weapon of Mass Destruction (nuclear, radiological, bomb, etc.) at a location to cause large scale casualties on the ground, destroy the aircraft and killing all on-board.
4. *Contaminate the occupants on-board with a biological compound. Killing after some days all on-board and all who had contact with the occupants.*
5. Detonate explosives on-board in order to kill all on-board and crash the aircraft.
6. Use of a chemical compound to kill all on-board and crash the aircraft.
7. Hamper the flight controls in order to crash the aircraft killing all on-board and destroy the aircraft.
8. *Use another aircraft to crash into the "target" aircraft, killing all on-board and destroy the aircraft.*
9. Hijack an aircraft in order to divert or negotiate.
10. Endanger the occupants with aggressive behavior or vandalism.
11. Hijacking the aircraft while taxiing on ground

After evaluation of these eleven operational scenarios it appeared that two scenarios are out of the scope of SAFEE technologies. These scenarios are number 4 (biological attack) and number 8 (use another aircraft to crash into the “target” aircraft). Consequently they have not been considered for assessment purposes. In addition it has to be noted that the threat of MANPADS is covered in other studies and as such ahs not been taken into account in SAFEE.

The remaining SAFEE operational scenarios are the basis for the design of the SAFEE sub-systems steering the implementation of the solutions to avoid or, at least minimize, the occurrence and impact of such scenarios. Based on the threats selected for assessment in SAFEE, operational scenarios were described for each of them.

The validation scenarios were also derived from the nine threat scenarios taking into consideration the remarks from the analysis performed in the risk assessment by security experts and end users. This analysis is included in the threat assessment of the current situation. The replication of the threat scenarios by the validation scenarios proved to be conditioned by the resources available for the validation exercises, the skill of the team working, and the performance of the validation platforms, tools and actors participating in the experiment.

3.3.3 On board Threat Detection System

The Onboard Threat Detection System (OTDS, developed in SP1) as an integrated means to detect upcoming threats onboard an aircraft has been integrally evaluated in an operational context. The following functions have been evaluated:

- Aircraft access control,
- Detection of suspicious personal behaviour, and
- Detection of dangerous materials.

For the detection of dangerous goods and materials, the corresponding trials have been conducted in a stand-alone demonstrator of an aircraft lavatory at EADS in Ottobrunn. The integrated evaluation facility then has been equipped with an alternate sensor, which provided the same signal characteristics to the integrated system as the original sensor, but could be triggered by a light source with a clear defined intensity instead of harmful substances.

The other evaluation campaigns have been conducted in a mock-up of an Airbus aircraft cabin (in Airbus Hamburg).

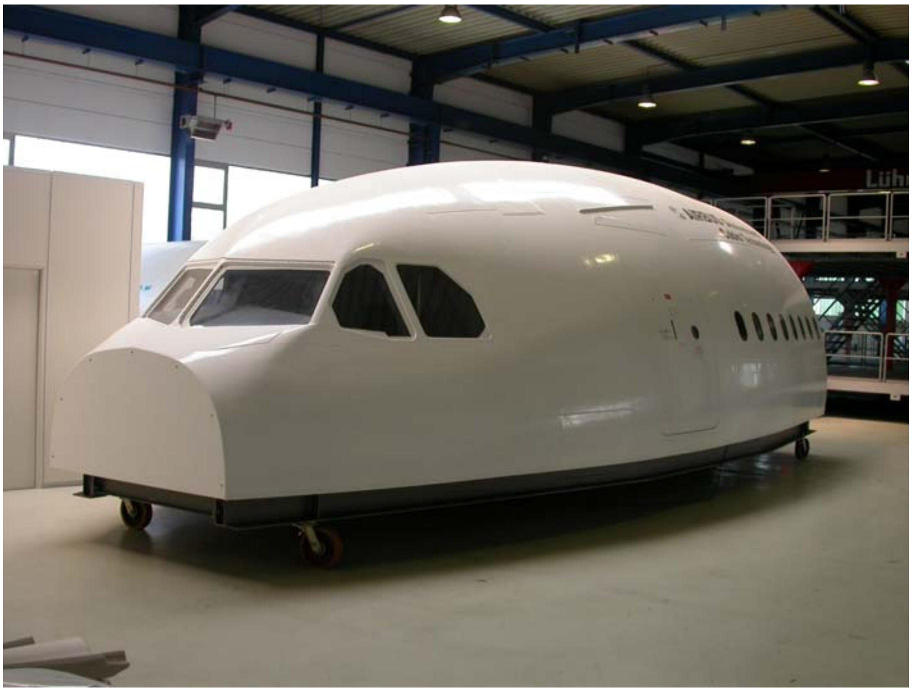

figure 3. Mock-up of an aircraft cabin (external view), used for OTDS evaluation

The entrance area of the fuselage mock-up had been equipped with

- Electronic boarding pass readers for passenger registration, and
- A video camera system for passenger authentication by biometric data,
- A detection system for dangerous goods and materials.

This has allowed the simulation of a complete boarding procedure with full application of the system prototype being developed.

The cabin area of the mock-up, which has been an imitation of an Airbus twin-aisle cabin, had a length of four seat rows in an economy class configuration. This has given capability to the partners to investigate the identification of seated passengers and behaviour detection of both, seated and walking passengers. The cabin area of the mock-up had been equipped as follows:

- Video system for person identification

- Video system for people tracking
- Video/audio system for behaviour detection

System architecture and component integration for all mentioned OTDS sub-systems has been done in accordance with the requirements worked out in the respective work packages. Moreover, results of the sub-system specification processes within the work packages have been considered for the demonstrator definition.

For the evaluation campaigns, scenarios had been developed that covered

- Attempts of unauthorised access to the aircraft,
- Attempts to smuggle dangerous objects onto the aircraft,
- Suspicious personal behaviour of passengers,
- Suspicious movement patterns of passengers.

The detection of suspicious behaviour or movement patterns has been evaluated for passenger behaviour and movements.

The results of the evaluation campaigns have been measurements of system efficiency, in particular with respect to detection capabilities, system performance figures, the rate of false alerts, and assessments of operational impacts. In addition, feedback provided by experts who participated to the evaluation campaigns has been recorded and evaluated.

3.3.4 Handling a crisis on the NLR GRACE simulator

Validation of TARMS (developed in SP2), and some of the Data Protection systems, has been performed at the NLR GRACE flight simulation laboratory in Amsterdam. The validation trials had five aims:

Aim 1: Validation of the usefulness of TARMS in assessing threats: is TARMS any better at threat assessment than crews currently are without the provision of TARMS on-board? The experiment aims to compare the threat assessments completed by the crews to the threat assessment made by TARMS in a given situation.

Aim 2: Validation of the response management module (RMM) in TARMS: given a certain threat assessment, does TARMS' RMM suggest appropriate courses of action? Are these different to the actions the crew would currently take without the provision of TARMS on-board?

Aim 3: Validation of the TARMS (cockpit and cabin) HMI: the experiment aims to gather subjective feedback and usability issues on the HMI.

Aim 4: Workload: the introduction of TARMS will add an extra element to the workload of the crew, but is it an increase that is considered acceptable and worthwhile?

Aim 5: Validation of the SAFEE-TARMS concept: is having a threat assessment and response management system on-board accepted in principle by the users?

To meet these aims, TARMS and some of the Data Protection systems were deployed in the Generic Research Aircraft Cockpit Environment (GRACE) simulator, for more information please see [ref], allowing the cockpit crew to interact with TARMS in a realistic situation. To allow the cabin crew to interact with TARMS a special room was prepared where a TARMS HMI was provided. A presentation of what was happening in the cabin was also displayed, whilst extra detail and explanations were given by a story teller. The cabin crew also had a headset and microphone to contact the cockpit crew whilst the cockpit was able to trigger a gong that gave the cabin crew a signal to contact the cockpit.

figure 4. NLR Flight/cockpit simulator (GRACE)

The systems deployed in GRACE were tested through scenarios developed to cover various security situations. Six scenarios were developed – see [ref] – of which five of these have been augmented with PDIs which could be detected by the SAFEE systems (OTDS and Data Protection systems), aircraft systems, and cabin crew as the scenario unfolds. The 5th scenario (The Inside Job) dealt with a threat that did not produce any PDIs during the flight. It was considered not useful to expose the flight crew to this threat for validation purposes.

The scenarios are:

Scenario	**Description**
Dr No	Hijacking attack in order to crash into target, using a medical diversion performed by "professionals".
Baby Boom	A female suicide bomber smuggling innocent liquids in order to assemble them into explosives.
Take My Breath Away	Chemical attack in multiple flights, simultaneously.
Chain of Events	2 unruly passengers.
The Inside Job	Attack using help from an insider
With Bare Hands	Group of unarmed, well-built hijackers

Each scenario contained:

- Rationale from a perpetrator's perspective, including assumptions about security processes and the specific attack they intend to carry out.
- Background information about the flight, the perpetrators, and any other passengers who become involved in the scenario.
- A storyboard and a timeline of actions made by the perpetrators, passengers, and crew as the story unfolded, including associated PDIs.

The scenarios have been validated by GIGN (Groupe d'Intervention de la Gendarmerie Nationale), the French Gendarmerie's elite counter-terrorism and hostage rescue unit.

For the VCAS validation – the main Data Protection system integrated into GRACE – a dedicated scenario dealing with a communication intrusion was developed where a disingenuous message was sent to the pilots asking them to cross a runway whilst an aircraft is landing.

The participants in the validation trials consisted of three-person crews; a pilot, a co-pilot and one cabin crew member, though in one experiment a crew with 2 cabin crew members was available. A total of 20 cockpit crew and 10 cabin crew members were involved. All flight crew were active pilots on Airbus, Boeing or Fokker aircraft. The experience of the pilots varied from trainee pilot up to very experienced. The crew members worked for well-established European airlines from 4 different countries.

All subjects were trained in security issues, the SAFEE concept of operations, and the use of the TARMS and its HMI. This training was performed just before the validation trials. For the pilots there was also a simulator familiarisation run to become accustomed to the Airbus A330 simulator. Especially for the Boeing and Fokker pilots there was a briefing about the specific Airbus features in the cockpit.

Each crew was present at NLR in Amsterdam for two days which included the training session and the validation trials. The half day training session covered; the SAFEE concept, the TARMS and a training run with TARMS in the GRACE simulator to enable each participant to have experience with the system prior to the validation trial.

For the validation trial each crew was involved in the five different scenarios. The pilots were situated in the cockpit simulator and the cabin crew member in an adjacent room throughout each scenario. Each of the scenarios could be conducted with or without the use of the TARMS system and each crew completed one scenario without TARMS. Over the course of the trial all five scenarios were conducted at least once without TARMS. Each scenario was divided into blocks. At the end of each block the crew filled in a questionnaire detailing their assessment of the current threat situation on board, the suggested response, their interaction with the TARMS system and their communication with the other crew members. At the end of the experiments the crew filled in an electronic questionnaire dedicated to HMI issues. Finally the crew was debriefed in a classroom setting where they were able to give their final feedback and comments.

At the end of each experimental scenario the participants returned to the debrief room for a quick discussion about the scenario and received a briefing on the next scenario in the trial. After all five scenarios had been completed each participant filled in a separate questionnaire about the TARMS HMI. Each of the different types of questionnaires was designed to capture data to answer the questions posed by the aims. The results of which are described in section 4.2.6. The 2 day trials finished with a final debrief session.

3.3.5 Flight Protection

3.3.5.1 SP3 Flight protection: Objectives of the intended systems

Flight Protection constitutes an important element of the responses envisioned in SAFEE for hostile attempts countering. It includes two main components, the Emergency Avoidance System (EAS) and the Flight Reconfiguration Function (FRF). Both are set in motion in response to TARMS requests and remain under the control of TARMS during operation.

The Emergency Avoidance System (EAS) provides protection against

- Controlled flight into terrain, obstacles or areas prohibited for security reasons,
- Malicious or inappropriate actions on cockpit systems (function referred to as Function protection or FP).

Avoidance of terrain, obstacles and PSA (Prohibited Security Areas) implies that EAS has the capability to take control of aircraft flight so as to guide it, independently of any action from the part of those present in the cockpit, on a safe and conflict free trajectory. This feature is used to enable the further important functionality of commanding, also in an autonomous manner, a flight path when the cockpit crew is incapacitated. For this function, EAS is supposed to receive navigation targets from the TARMS.

The Flight Reconfiguration Function (FRF) supplements the EAS function by providing autonomous flight re-planning for a safe return to the most suitable airfield, and the subsequent guidance to control the aircraft according to the plan, the guidance being performed up to the landing phase, which is also performed autonomously.

3.3.5.2 SP3 Flight protection: Objectives of the work

SP3 includes two sub projects, SP3.1 and SP3.2, which address EAS and FRP respectively.

The objectives of SP3.1 are mainly

- To produce a preliminary specification of what would be the intended EAS system in the near future, taking into account the appropriate safety-related considerations and requirements, as well as the integration constraints associated with the implementation of such a system into avionics
- And to get from the users – mainly pilots – a feedback on the EAS requirements with regards to the most critical aspects on the basis of evaluation experiments performed with pilots.

The experimentation stage implies the development of a simulation environment allowing the EAS functions to be performed in a sufficiently realistic manner in front of users. Given these objectives, the SP3.1 Work Packages have been organized in accordance with the logic of the approach dubbed as “mini-V” cycle that is used to amend the classical “Waterfall” development approach when an experimental validation stage is introduced early in the requirements development process.

Unlike to EAS, investigation regarding the FRF in SP3.2 takes essentially the form of an assessment performed from a high level perspective, with the goal of considering and identifying all the responses that can be provided as flight reconfiguration functions in case of security threat. The overall objective is to lay the foundations of a further long-term objective project. The aim is to perform a technical system analysis that identifies the impacts and implications of threat reduction measures and actions based on forced flight deviation functions able to safely re-route and land threatened aircraft on a secure airport. Given the challenge implied in these functions, the analysis includes also consideration of safety requirements.

3.3.5.3 SP3 Flight protection: Objectives of the experimentation stage

The modification of the aircraft and its avionics in order to implement EAS functions is likely to modify the interaction between the aircraft and the users (mainly pilots) in normal operation and should be acceptable by them. SP3 includes an assessment phase specifically focussed on the EAS (Emergency Avoidance System). This forms indeed part of a concept validation process that aims to spark off reaction of users – especially airlines pilots – by putting them in front of an animated form of the concept subject to validation. The main objective from the experiments is to get a feedback on the requirements produced at the analysis stage. Work objectives include therefore the realization of a software mock-up for the EAS and the adaptation of the associated simulation environment (the latter being built on an existing flight simulation platform) which implements, from the requirements applicable to the future final product, those deemed to require special scrutiny prior further work towards realization of that product may be envisaged.

This overall simulation objective implies the definition of features and functions that the EAS mock-up and the operating platform need to implement, in order to allow the evaluation to focus on the pilot acceptability of a concept where, in some cases, the pilot is deprived of the control of aircraft while keeping some responsibilities in the development of the situation. Part of the objectives of the SP3 work was to establish detailed evaluation strategy and plan, in coherence with the guidelines and recommendations expected from SP5.

3.4 DATA PROTECTION

The objective of Data Protection (Sub project 4) was to protect communications and data that are daily used for exploitation of aircraft in an hostile fashion that may lead to a dramatic situation like direct or indirect control of the aircraft by hijackers or use of false data that can endanger the flight safety.

Data Protection Systems aims at working on security aspects around DATA in the aircraft. Main interest is to detect attacks to on-board related data, pre-assess, and then act to protect the data which are critical for flight safety

Authentication in cockpit command will prevent an attempt to get control of the aircraft command by unauthorised person.

Authentication in air traffic control operation will prevent the false air controllers, as it has been seen in some previous case.

Authentication in Air traffic / Navigation / Operation and maintenance data will prevent the use of false data by crew or airline that may endanger the flight safety.

Aircraft / ground communication has a limited transfer rate and availability that makes impossible a complete physical separation of the operational network and the on-board passenger network which is expected in the future. SAFEE have to define efficient firewall between open world and avionics.

Another main objective of Data Protection Systems is to set up a first protection against jamming of radio navigation of communication means. Today, jamming could be performed either from the ground or from the aircraft interior with very simple and light device that could be hidden in PC (Personnel Computer) or in mobile phone box. Electromagnetic jamming alone will not enable to lead in most case to a dramatic situation. Nevertheless, it is a very efficient accompanying action.

3.5 MANAGEMENT OF ACTIVITIES

SAFEE partners have signed a consortium agreement describing the management of the project. A Steering Committee (SC) composed of all partners having equal right of vote is in charge of controlling the financial management by the coordinator and of voting modifications of funding proposed by the PMC (Project management committee). The PMC was composed of the SPs leaders and was chaired by the coordinator (Sagem Défense Sécurité). PMC was composed of Airbus Deutschland & France, BAE systems, Thales Avionics, Sagem Défense Sécurité and NLR.

A management quality plan was produced and applied by all partners. A collaborative private secured platform “AGORA SAFEE” was used to exchange and store all information. An-other collaborative private secured platform was settled within the User Club members’ community, as part of the dissemination of objectives and results of SAFEE.

SAFEE description of work was detailed at the beginning of each period (1 year). The work was described in tasks included in each work package (WP), driven by a Task leader and WP leader. The management of the tasks and WP were reviewed within Sub Project Management meetings (SPnMTm). Before each SPnMTm, technical meetings were driven by tasks leaders and WP leaders. The scheduling of the SPnMTm meeting is in line with the PMC meetings every 4 months to prepare these meetings. In the middle of these PMC dates, audio PMC meetings of 1 ½ hour with the PMC members permitted to review the on-going actions and to decide when necessary. All meetings had a calling notice with a foreseen agenda in order to allow all attendees to prepare themselves. All meetings had a minutes of meeting document with a list of actions.

4 MAIN ACHIEVEMENTS

4.1 THREAT DETECTION ACHIEVEMENT

The objective of the *Onboard Threat Detection System* (OTDS) task was to specify and develop a prototype. The system is intended to support TARMS (Threat Assessment and Response Management System) by providing an early and automatic detection of threats that are emerging on board of an aircraft. It comprises following functions:

- Control of access to the aircraft,
- Detection of suspicious personal behaviour, and
- Detection of dangerous goods and materials.

The availability of these functions will significantly improve the security and, at the same time, the efficiency of air transportation. This will be achieved by prevention of unauthorised access to the aircraft on ground and by early detection of threatening events in the cabin when the aircraft is in flight. Thereby, the system will contribute to ensure public confidence in the air transportation system.

The development of the Onboard Threat Detection System has been undertaken within five strongly interconnected work packages:

1. Definition of the overall threat detection concept
2. Prototype development for the access control function
3. Prototype development for the suspicious behaviour detection function
4. Prototype development for the dangerous goods detection function
5. Overall system integration and evaluation

The development cycle started with the definition of the overall concept, in which all partners of the team were involved. Then the three functions were developed in parallel, with mutual exchange of information between development teams, for sub-system prototyping. At the end, all sub-system prototypes were integrated and commonly evaluated in an operational context.

4.1.1 Definition of the overall threat detection concept

At the beginning of the work, the overall threat detection concept was defined. This concept comprises two parts:

- The functional requirements for the Onboard Threat Detection System, consisting of several interconnected sub-systems, and the integration of and interfaces between these sub-systems, and
- The operational concept for the Onboard Threat Detection System.

The functional requirements of the overall threat detection concept were derived from the threat scenarios that were established for system evaluation (in sub-project 5). These scenarios provided some information on the threats to be detected and the detailed threat characteristics. On the basis of this information, suitable detection algorithms were identified and sensor types were selected. The overall threat detection concept also clearly defines the system boundaries for the sub-systems, their interfaces and the data correlation in between them.

The operational concept describes the use of the threat detection system from the aircraft operator's point of view. It covers the development of procedures to be applied and an anticipation of operational impacts to be expected.

4.1.2 Prototype development for the access control function

For the implementation and integration of an access control sub-system prototype, several technologies were considered and appropriate development steps were undertaken:

- Face recognition algorithms: Different algorithms were tested on a stand-alone prototype before the final implementation and testing in the OTDS evaluation facility. The most promising were selected and further improved during the development phase, also taking into account the specific constraints and environmental conditions of the evaluation facility.
- RFID (Radio Frequency Identification) technology: The specific integration constraints of the OTDS evaluation facility were investigated, and operational issues influencing the technology selection were

discussed. As a result, the best suited RFID chip technology was selected out of two candidate technologies, which already had been defined in the initial phase of the project. The appropriate reading device was implemented in the evaluation facility, and a corresponding enrolment station for the generation of the boarding passes was set up.

- Video cameras: Several types of cameras that are available off-the-shelf were evaluated and the most promising were chosen for the detection of personal behaviour and for the face recognition. An appropriate software interface was implemented to allow the integration of the selected type of camera with the detection and recognition algorithms developed in the SAFEE project.
- Image pre-processing: Several pre-processing algorithms to get usable images for face recognition out of high contrast video pictures were evaluated. The best suited were selected, implemented and further improved. After installation in the evaluation facility, they were adapted to the specific environmental conditions in the mock-up.

4.1.3 Prototype development for the suspicious behaviour detection function

Following steps were taken for the implementation and integration of the sub-system for the detection of suspicious personal behaviour:

- To facilitate the detection of suspicious behaviour patterns, suitable indicators for this kind of behaviour were derived from appropriate threat scenarios. These *Pre-Determined Indicators* (PDIs) were validated and further broken down into measurable *Low-Level Features* (LLF). Quantified measures for the automatic detection of LLFs were specified and validated.
- The scenarios and PDIs defined within the SAFEE project were investigated for their applicability for the evaluation campaigns. According to the results of this investigation, more detailed scenarios were defined, which address the main points of the scenarios and, at the same time, consider the options and constraints of the evaluation facility.
- Definitions of basic behaviour detection principles were completed and appropriate detection algorithms were implemented in the sub-system prototype.
- An analysis and evaluation of different sensors with respect to the efficiency of sensing and aircraft integration constraints was conducted. According to the results, sensor installations and connections for the evaluation facility were specified.

Remark : The work performed within the suspicious behaviour detection work package led to the nomination of the BAE team for the BAE internal Chairman’s Award.

4.1.4 Prototype development for the dangerous goods detection function

For the implementation and integration of a sub-system prototype for the detection of dangerous goods, several technologies were considered and appropriate development steps were undertaken:

- Various detection technologies and sensor types were concluding investigated and evaluated. Besides the detection efficiency, particular focus was on the operational specifics and the constraints for the installation on board of an aircraft.
- Particular attention was paid to the evaluation of technologies for liquid explosives detection. Promising sensors for this kind of detection were selected and integrated in a stand-alone prototype of an aircraft lavatory, where their capabilities could be demonstrated.

  Note : For the integrated OTDS evaluation facility, the demonstration of the detection of real explosives was not possible for safety reasons. Therefore, an alternate sensor, providing the same signal characteristics as the explosives detector, was integrated in the evaluation facility and linked with the overall system. This allowed to demonstrate how the detection of suspicious substances interfaces with the scenario recognition implemented in the central OTDS unit.

Remark : The achievements of the dangerous goods detection work package resulted in the win of an internal innovation price for the involved team of EADS.

4.1.5 Overall system integration and evaluation

The overall integration of all sub-systems of the Onboard Threat Detection System allowed to run evaluation campaigns that addressed two aspects:

- The assessment of capabilities concerning sensor based person identification, personal behaviour detection, person movement tracking and detection of dangerous substances, and

- The system's capability to recognize complex threat scenarios that have been pre-defined by security experts.

The evaluation campaigns were conducted according to a specified evaluation plan, and their results were concluded in a final report.

4.2 THREAT ASSESSMENT AND RESPONSE ACHIEVEMENT

The design and development of the Threat Assessment and Response Management System (TARMS) required to undertake the following tasks:

1. User and System requirements capture
2. Expert knowledge elicitation
3. Bayesian network and Response Management model construction
4. Design and Implementation of TARMS
5. Validation scenario construction
6. Validation Trials

4.2.1 User and System requirements capture

It was decided, at the start of the project, to use a rigorous methodology to elicit end user's needs, and then transforming them into requirements. The decision to use a rigorous methodology was made because TARMS is considered to be at the core of SAFEE. It was mandatory to guarantee that any event that could be correlated to a potential threat should be identified, and when a threat is confirmed, suggesting a reasonable set of responses.

For the end users' needs elicitation a classical way of interviewing stakeholders was used. A long list of stakeholders was identified, and for each stakeholder, in each country of the TARMS partners, a 2-hour interview was conducted. Each interview pattern was the same for the different kinds of stakeholders. An interesting by-product of this work was the different meaning of the notion of threat. The different meanings are not contradictory but rather complementary or totally independent.

Starting from the contents of the interviews (50 people have been interviewed in total) the Objectiver methodology was used to build a number of different models where concepts such as goal, sub-goal, functional requirement and constraint, risk, contradiction, anti-goal, obstacle are represented graphically. These graphical models are used because they can identify inconsistencies between the goals of stakeholders, and incompleteness' in the knowledge captured. After the models were built they were frequently updated in order to solve conflicts and remove inconsistencies. They were also validated both by the stakeholders who were interviewed but also by the TARMS partners. The final result of the Work Package was a set of requirements documents, the first representing the stakeholders wishes, the second the system requirements, to be used in the design and implementation of TARMS. Also this work has shown that the use of a rigorous methodology is the correct way to build a stable basis for future developments.

4.2.2 Expert knowledge elicitation

The aim of the knowledge elicitation task was to capture knowledge from security experts and to store it in a knowledge base. The knowledge base would then be used to create the models to perform threat assessment and response management. The task was broken down into three main phases.

i- The first was the development of the Knowledge Elicitation Plan which described which elicitation methods were to be used, what knowledge would be captured, and how it was to be stored.

ii- The second phase was the development of the Knowledge Acquisition Tool (KAT). This software tool was designed to complement the interview process providing visualisation and data storage.

iii- The third phase was the generation of the Knowledge Base through expert interviews. The knowledge base was built up over many interviews. The interview process also known as the Knowledge Acquisition Process (KAP) Process is comprised of 5 stages.

  - The first stage involves informal interviews with experts without the use of the Knowledge Acquisition Tool. The aim is to elicit variables relevant to the domain, e.g. what behaviours could be observed on a plane.
  - The second stage rationalises the results of the first stage. This involves removing redundant information, merging equivalent variables, and separating variables with the same name that represented different concepts. Each variable is given a rigid definition.

- The third stage of the process uses the KAT to elicit the relationship between the knowledge variables, i.e. how a particular behaviour contributes towards a threat. This phase uses the same experts as the first stage.
- The fourth stage elicits probability estimates associated with each link.

The fifth stage updates the knowledge base and generates a Bayesian network automatically.

The results of using the Knowledge Acquisition Process for the SAFEE project are described in more detail in [TEHOSS].

Four of the SAFEE partners used the KAP and KAT to interview 20 subject matter experts. On the whole, users and interviewers have been positive regarding use of the KAP and KAT. However, the resulting knowledge base is incomplete because experts could not afford to spend the time required to complete the process.

The methodology of the knowledge elicitation (i.e. the interview process and the functionality embodied in the KAT) was shown to be very successful. The majority of experts stated that the most beneficial aspect of the process was experimenting with the automatically generated Bayesian network. Once the experts understood the primary goal of the interview process (that is, generation of a Bayesian network for threat assessment) and saw their knowledge embodied in a network, they had greater confidence in the previous stages. Many of the experts became willing to spend more time in the interview, which was used to validate the Bayesian network by running scenarios through it and noting the expert's comments.

4.2.3 Threat Assessment and Response Management model construction

The aim of this task was to take the knowledge base provided by the Knowledge Elicitation task and to construct models that would perform threat assessment and response management. The task itself was broken down into two subtasks - the development of the TA models and the development of the RM models.

i- Threat Assessment (TA) model construction

The TA model constriction subtask worked closely with the Knowledge Elicitation task and placed requirements detailing what type of knowledge should be captured and how it should be stored. This allowed the Bayesian network threat assessment models to be generated automatically from the knowledgebase. Overall, nearly 20 Bayesian networks have been constructed, each based on the opinions of a different domain expert. The intention was to fuse all of these models into a single model that would be used within TARMS. Unfortunately, the limited availability of many experts meant that only nine of the models were complete (see IX2.7.1.3a). The fused model resulting from these was not adequate for use in TARMS. In consequence, a single expert's model was selected for use in TARMS. This model performs well against the scenarios created independently by GS_3.

The decision to use Bayesian networks for threat assessment was a good choice for SAFEE. The graphical representation allows experts to see how their knowledge is being used and understand the behaviour of the Bayesian network (at a high level). A single model captures the possibility that a single passenger is planning to execute several threats (for example, a hijack or a bomb-on-board threat), allowing evidence for one threat to 'explain away' evidence for another threat. By incorporating models of benign behaviours that may look suspicious the Bayesian network can differentiate between a variety of situations making it very suitable for the SAFEE domain.

ii- Response Management (RM) model construction

The RM model construction subtask developed a model to suggest appropriate actions for the cockpit and cabin crew in the event of a threat being detected. BAE developed a simple rule-based model and it was populated with actions relating to specific threats and PDIs. The actions were derived from a number of brainstorming sessions and interview transcripts, and were validated by a team of domain experts gathered by GS_3. The model was executed in TARMS by a Response Management component which suggested responses for the most severe threat detected by the Threat Assessment module.

The simple rule base was a good model in that it implemented common security methodologies. However, the implementation was not able to take into account the context of the threat situation, so it sometimes suggested responses that could not be performed. As multiple threats arose, the system would repeatedly suggest responses that the crew had already done or had decided not to do. Some of these 'silly' mistakes could be rectified by further refinement of the system.

The crew were sceptical of some of the responses, highlighting the need for training and customisation of the system for each airline and regulatory authority. Many pilots disliked the concept of an automated system for response management, and it became clear that a detailed study of the operational issues raised by a TARMS-like system is imperative if such a system will ever meet the needs of the aviation industry and be accepted by all the stakeholders (pilots, cabin crew, ground staff, regulatory authorities, airports and airlines, passengers, etc.).

4.2.4 Design and Implementation of TARMS

Erreur ! Source du renvoi introuvable.5 shows the architectural decomposition of TARMS and clearly identifies three major modules: the User Management, the Threat Assessment and the Response Management.

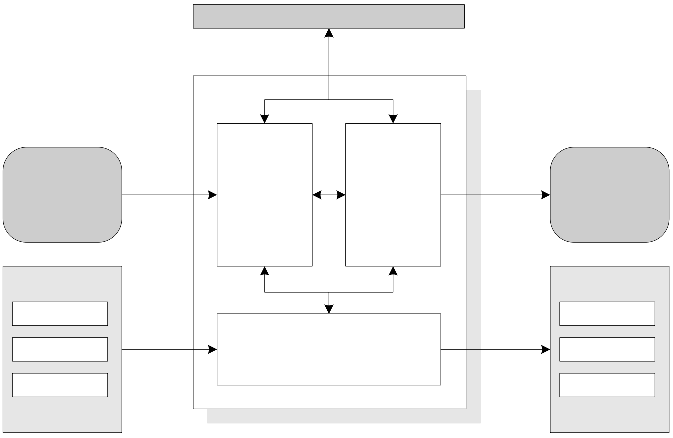

figure 5. TARMS High-Level Architecture

The User Management Module (UMM) is responsible for receiving observations inputs and providing suggestions of actions from/to the users of the system. Different users have different profiles, workloads and roles inside an aircraft and this must be taken into account when designing a user interface. The UMM must be capable of making the bridge between these different user interfaces and the other modules of TARMS.

The Threat Assessment Module (TAM) aims to discover hidden relationships between different security input data received from onboard sensor systems, users and from ground intelligence agencies, and make useful inferences about potential threats arising from inside the aircraft. The approach to the design of the TAM is to use probabilistic models in the form of Bayesian graph networks. A probabilistic approach has a number of advantages: the model can be conditioned on evidence (i.e. observations), summarised predictions can be made and information can be predicted or removed from the model.

The Response Management Module (RMM) is the component that allows TARMS to provide suggestions to users and to activate aircraft systems, in order to reduce the threat level of the flight. The approach to the design of the RMM was to use a simple rule-based mechanism implemented in Prolog which mimicked a security methodology outlined by Athena GS$_{3.}$ The model provides a simple mapping from threats and critical PDIs to a list of responses, thereby making it easy for experts to validate its functionality.

The design of a software framework to support the TARMS objectives created a significant number of challenges. One important goal was not to restrict TARMS to interact with a specific set of external systems, i.e., it should be possible to interface TARMS with any external sensor/actuator system which complied with some basic requirements. This guided TARMS' design to be as scalable and modular as possible. Another important goal was that TARMS should provide responses to threats in a timely fashion. The usage of novel reasoning technologies in the TAM and RMM created some problems and uncertainty in the performance of such system. The possibility of distributing modules among different resources was the solution proposed to mitigate this problem.

The usage of JADE[2], a JAVA agent-based framework, was adopted to cope with the aforementioned requirements. JADE provides a distributed environment where agents implementing components of the software can be deployed seamlessly across several computing platforms. Also, the addition of new sensors and user interfaces can be accomplished by adding new agents to the system which would support the specific interface with those external systems. JADE also provides agent communication protocols between agents using standard

[2] http://jade.tilab.com/

technologies, such as Ethernet protocols, providing TARMS the required modularity. All the architectural and detailed design was described using the UML notation. However, UML fails to represent correctly the proactive behaviour of an agent-based approach. For this purpose, a few steps from an agent-oriented development process (PASSI) were adopted. PASSI[3] is a process for specifying and implementing multi-agent systems using UML. PASSI may be considered a use case driven process, as it begins by describing the system's requirements through use cases, and proceeds by identifying roles and building agents to fulfil these use cases. It contains a few steps that address agent social behaviour modelling, in other words, the way that agents interact and cooperate with each other, and some steps/models to address and specify details regarding inter-agent communication.

The implementation was in the JAVA language on top of the JADE framework. The system is highly customisable and modular. The communication with other systems inside GRACE uses the NLR's Ethernet libraries encapsulated in JAVA classes. The threat assessment module uses NETICA's JAVA classes and the response management module developed by BAE was seamlessly integrated in the whole TARMS application.

4.2.5 TARMS Validation scenario construction

The aim of this task was to construct possible scenarios to test the TARMS system as part of the validation and testing of the system. A panel of experts which consisted of aviation security specialists, terrorism consultants, flight crew, pilots, a sky marshal, psychologist, Red Team specialist, explosives expert and former intelligence agents were assembled to create those scripts. The panel was acquainted with SAFEE goals in general, the SAFEE identified threats, the task of the specific Work Package and the specific use of the scenarios in the project.

The panel of experts' objective was not only to make the scenarios as realistic as possible, relying on possible modes of hostile actions (PMHA) relevant information and appropriate security systems and procedures, but also to attempt to derive the scenarios from the OTDS sensor systems in order to keep the scenarios "TARMS oriented" as required to test the TARMS system as part of the validation and testing of the system in WP2.6. The panel was also asked to base the scenarios on the SAFEE threats (focusing on hijacker for demands/use as a missile, explosives, chemical weapon or unruly) and to highlight, while focusing on human behaviour, the expected PDI's the system should be able to identify.

The experts initiated their work by identifying which of the SAFEE threats will be exploited in the scenarios, and which of the scenarios will be used to test the TARMS system.
The mission as was presented for the panel of experts:

- To create 6 realistic scenarios to be used for TARMS validation activities in SAFEE
- The scenarios must be based upon actual procedures
- The scenarios may utilize any apparent security loopholes

The panel then developed full scenarios during think tank meeting (total of 10 meetings) describing:

- Detailed flight Information including information on the a/c and basic identification of the actors participating in the validation exercise.
- Background information, including a description of the perpetrators, their goal and objectives, as well as pre-flight security information.
- The scenario description, containing a minute by minute textual description of the activities occurring prior to the flight, and during the flight, and the actors allocation which display the perpetrators and other actors allocation.

For the final check, the six completed scenarios were presented in GIGN (the French Gendarmerie's elite counter-terrorism and hostage rescue unit) headquarters before a selected group of different European In-flight Security Officers during a special conference. All the scenarios gained extensive approval from the participants.
During the process it was recognized and stressed that the actual information presented in the scenarios should be deleted (or classified) in order to prevent any possible misuse.

4.2.6 TARMS Validation Trials

Validation (and training) has been done at NLR. NLR's GRACE simulator was used to simulate handling of crises by onboard users e.g. captain, first officer and cabin crew. In September and November 2007, the TARMS validation experiments on were completed. A total of 30 crew members in 10 teams drawn from several airlines were exposed to six validation scenarios. These scenarios include the threat information, the so-called PDIs (Pre

[3] Cossentino M., and Potts C. PASSI: a Process for Specifying and Implementing Multi-Agent Systems Using UML

Determined Indicators) which would be detected by SAFEE systems (OTDS and data protection systems), aircraft systems, and cabin crew as the scenario unfolds. The scenarios have been divided into blocks. At the end of each block the crew filled in a questionnaire detailing their assessment of the current threat situation on board, the suggested response, their interaction with the TARMS system and their communication with the other crew members. At the end of the experiments the crew filled in an electronic questionnaire dedicated to HMI issues. Finally the crew was debriefed in a classroom setting where they were able to give their final feedback and comments.
The results of the experiments showed that for the aims described in section 3.3.4:

- Aim 1: No evidence was found to support the hypothesis that posits that crew with TARMS can make 'better' threat assessments than crew without TARMS. Though one interesting result was found was that crew provided a significantly higher threat assessment for the Unruly passenger than any other threat! This is possibly due to crews seeing this threat much more often than the other threats.
- Aim 2: TARMS does suggest different courses of action to a threat than a crew does without TARMS, and while the participants agreed that most of the recommendations were sensible, the majority of participants commented on the need for these recommendations to be customised to airline company procedures.
- Aim 3: The validation of the HMI showed that the majority of ratings provided by the participants were positive. The issues that were raised though focused mainly on the flexibility and alignment with airline company procedures.
- Aim 4: Feedback from participants showed some concern about the increased workload required to operate TARMS. It is believed though that increased training and the development of TARMS related policies and procedures would increase the effectiveness and efficiency of TARMS and mitigate some of the workload concerns.
- Aim 5: The main impression was that TARMS and the SAFEE concept are interesting and have great potential for enhancing the security on-board an aircraft. However, in its current state many participants had reservations about the value of having TARMS on board the aircraft, and in particular about the response management aspect of TARMS. Participants felt that the strength of the system is in the detection of PDIs rather than in their interpretation and decision making.

4.3 FLIGHT PROTECTION ACHIEVEMENT

The design and development of the flight protection system required to undertake the following tasks:

1. Emergency Avoidance System (EAS) analysis
2. EAS mock-up and simulation environment
3. EAS experimentations
4. Prohibited Security Area Data Base (PSA DB) experimentation
5. Flight Reconfiguration Function (FRF) analysis

4.3.1 EAS analysis phase

The analysis phase of the work on EAS (SP3.1) resulted in the drawing up of high level requirements applicable to the EAS to fulfil the needs defined at SAFEE level. These requirements comprise two main parts, the Functional baseline and the Allocated baseline.

- The Functional baseline has been established as a result of a thorough analysis of the needs and possible responses that shall be considered in case of security threat. It defines the different modes of operation of the EAS and identifies the main functional components of the system while specifying the interfaces within these components as well as the relationships with other systems, mainly avionics on one side (including cockpit crew HMI), and TARMS on the other side.

- The Allocated baseline defines the integration of EAS into a generic avionics architecture. It establishes the distribution of the EAS functional components over the avionics systems taking account of the design features generally used for these systems to get the required resistance to failures. It defines also the "connection points" – i.e. switches – that allow EAS to take the control of the flight.

A further valuable output of the analysis phase is constituted by the outcome of the work done on safety and human factors issues, which produced, as a result of appropriate analyses, the requirements that need to be fulfilled to fight the hazards that could result from system failures and/or pilot errors. The work was conducted in close collaboration with the allocated baseline elaboration, and produced the results that can be expected from the classical analyses performed in the course of avionics system design, i.e. Functional Hazard Analysis and Preliminary System Safety Assessment.

In addition, in the light of the findings unveiled in the course of the analyses, the task produced some valuable recommendations which are about functional extension of the EAS, disengagement logic of the EAS and improvements to be considered for the fulfilment of safety requirements.

4.3.2 EAS mock-up and simulation environment

The software mock-up developed for experimental validation and evaluation purposes provides a representative model for the key components and features of the EAS. The mock-up includes a simplified implementation of TARMS, restricted to the minimum required to allow EAS to function. Moreover, the EAS mock-up works into a flight simulation environment derived from an existing simulation platform that was modified and adapted for the purpose.

The EAS functions made available for experimentation include:

- Operation according to the modes defined for the “In-flight” phase of aircraft flight. All the modes of operation defined for EAS, according to which protection and autonomous flight controls is provided or not (depending on TARMS request) are implemented, except the mode corresponding to the case of aircraft staying on ground, which is not relevant given the evaluation objectives.
- Conflict detection and avoidance trajectory computation. The implementation of these functions considers terrain only and combines actual TAWS software with dedicated software set up for SP31.
- Aircraft guidance under EAS control. The guidance of the aircraft performed in avoidance and autonomous flight modes is ensured by means of a control law specifically developed for the purpose.
- Display and Control Management. The information display that is deemed necessary for pilot awareness includes the mode into which EAS is entered, and the navigation targets followed by the guidance function. Further information for awareness is provided via the standard means included in the flight simulation environment, including mainly the terrain hazard display, furnished by the TAWS and displayed on ND (Navigation Display), and the terrain profile ahead of the current aircraft position displayed on the VD (Vertical [Situation] display). Moreover, prealerting information is provided through the standard TAWS messages, displayed on PFD (Primary Flight Display), and aural announces (Terrain ahead, Pull up, etc).
- Recovery procedure. This function uses a software checklist, displaying a set of items to be cleared successively, to inform pilot of the checks and actions he has to perform before the aircraft control is given back to him.
- Function Protection, which inhibits, depending on EAS mode, selected parts of the cockpit controls so as to illustrate the concept advocated in SAFEE with regards to the protection of avionics systems against malevolent actions.

For the aspects relating to aircraft flight and information display in the cockpit, the degree of fidelity to what would be implemented in the final product is deemed to be at the appropriate level given the evaluation objectives. The Function protection and the Recovery procedure were however implemented for the purpose of illustrating the concepts involved and sparking off comments and suggestions. They are not intended to prefigure the form that could be required for the final product.

4.3.3 EAS experimentation

Two categories of tests have been formally performed and reported. Validation tests have been conducted firstly to check that the EAS mock-up works in accordance with its intended function. Then, evaluation experiments carried out with the involvement of professional pilots provided further feedback from those who are a priori the most involved in the use of the system.

The interest of the tests performed in the frame of Validation is to give a further light on how EAS works, providing, in the execution domain where assessment is easier, the impact of what has been specified in the requirements domain, which otherwise could be felt somewhat abstract and difficult to follow. According to the methodology defined for SAFEE, the validation strategy involves tests classified in Validation Exercises. Each Validation exercise, also called Use Case, has experimental objectives relating to particular EAS requirements or features that the corresponding test scenario aims to exercise. A Use Case defines a class of behaviours that can be obtained experimentally and assessed, and involves the definition of initial conditions test procedures including sequence of actions to be performed and observations to be made during the experiments. The produced report records the results of the validation tests, gives details of the procedures performed, and includes records of the observations.

The experimentation performed in the frame of Evaluation consisted of a series of 15 trial days with the involvement of pilots who have various flying experience in different aircraft types. The simulation scenario run for these trials corresponds to the sequence of events of a generic hijacking scenario, which involves EAS-protected flight phases, CFIT (Controlled Flight into Terrain) attempts followed by avoidance manoeuvres, recovery phases and phases of flights performed under the automatic control of EAS to follow navigation targets provided by TARMS. Feedback and comments from pilots have been collected with the help of questionnaires. The analysis performed on the outcome of the evaluation trials is organized so as to address the following aspects:

- Efficiency of the protection against CFITs
- Quality of the flight realized under EAS control during avoidance and just after
- Recovery procedure
- Pilot workload, situation awareness and training aspects
- Acceptability of the EAS concept as response to security threat.

4.3.4 EAS PSA DB experimentation

In the course of the work, the concept of Prohibited Security Area Data Base (PSA DB), which stems from the aim of providing protection against penetration into prohibited area in case of hijacking, appeared to be a topic of great interest with regard to the objectives addressed in SAFEE. This motivated the carrying out of research specifically focussed on the issue, which includes an experimental assessment phase involving competencies in Air Traffic Control and/or aircraft piloting.

The mock-up developed in this context consists of a stand alone application software running on a PC and providing management and display functions for all relevant flight-related data, which goes beyond the strict needs of PSA DB as this includes also information about Navigation aids, terrain elevation, cartographic data, obstacles, and intended flight plan(s). The functions featured by the software allow users to import data from external sources and then to get various displays with the aim of assessing flight situation against conflict areas.

Experimentation of the EAS PSA DB software mock-up followed an approach similar to the one used for EAS validation, with a strategy based on aims and exercises defined so as to be in accordance with the guidelines and requirements set out. The formal evaluation campaign was carried out in Israel with the involvement of people having competencies either in Air Traffic Control or in aircraft control (or both), which allowed valuable comments and suggestions to be gained about the implementation of the concept in future systems for security crisis management.

4.3.5 FRF analysis

In line with the work plan set up, the results of the work done on FRF correspond to what can be expected from the activity performed at early stages of the aircraft systems development process. Schematically, such an activity deals with the design of functions and the drawing up of different levels of requirements for the intended aircraft function. The resulting outcome of the process applied to the FRF includes therefore the following.

- A thorough analysis of the security threats addressed in SAFEE resulted in the identification of a set of possible responses in terms of trajectory determination (flight planning) and flight control functions, considering different degrees of air-ground interaction. These responses have been assessed against applicable constraints considering aspects such as Human factors, feasibility, safety, corruptibility and technology. Built from this assessment the SSS (System Segment Specification) of the FRF has been produced, which freezes the FRF role and functions, and provides the related applicable high level requirements covering the following domains: functional, operational, performance, environment, technological, interfaces, human factors, safety, and quality assurance. In addition, recommendations that accompany this SSS has been produced as further information for system installation in aircraft.

- The step that logically follows the specification at system level proceeded with refinement of FRF operational scenarios (including interaction with other SAFEE systems as well as with the involved avionics components). As a result, a SSDD (System Segment Design Document) has been produced, which allocates the SSS requirements to the sub systems involved and provides derived requirements for

  - security-related aspects, as a result of the refinement process,
  - and for safety-related aspects, which result from the FHA (Functional Hazard Assessment).

  A further output at this stage is about the impact of FRF introduction in existing avionics and takes the form of recommendations for the upgrades that are required to enable such integration.

- According to guidelines in force for safety-critical avionics systems (such as ARP 4761), safety analyses were conducted proactively and in parallel with the development of requirements for FRF functions and architecture. These analyses drew on a review of relevant parts – given the FRF purpose of providing automatic guidance – of applicable standards and regulations. The main results of the safety analyses are made up of the FHA (Functional Hazard Assessment), which identifies functional failure modes classified in function of the severity of their effects, and the PSSA (Preliminary System Safety Assessment), which provides lower level safety requirements and show the evidence that safety targets can be met by the proposed FRF architecture. The PSSA is based on two complementary assessment methods, which are FTA (Fault Tree Analysis) and the FMEA (Failure Modes and Effects Analysis). A further result of safety analyses was produced by Operational Expert Hazard Brainstorming sessions, which were added to the work plan in the course of the task and correspond to a best practice of the safety assessments carried out by ANSP. The valuable feedback provided by these brainstorming sessions on operational issues of FRF within ATM takes the form of recommendations for the improvement of FRF services.

- The last stage of the work on FRF addressed acceptability issues and provided recommendations to update the management of existing avionics systems and databases, as well as the air traffic rules and procedures, in relationship with FRF operation. Acceptability assessment includes the feedback provided, via a questionnaire designed for the purpose, by relevant stakeholders (pilots, airlines, air traffic control, etc.), which can be utilised as a form to capture end-user requirements and expectations towards the FRF system. The results of the questionnaire-based assessment forms part of the report produced at the end, which includes a synthesis of the overall work done on FRF while providing the main conclusions and recommendations for the whole product life-cycle of the intended system, from specification to withdrawal.

4.4 DATA SECURITY ACHIEVEMENTS

The objective was to protect communications and data that are daily used for exploitation of aircraft in a hostile fashion that may lead to a dramatic situation like direct or indirect control of the aircraft by hijackers or use of false data that can endanger the flight safety.

The design and development of the data protection systems required to undertake the following tasks:

1. Electromagnetic attack protection and back-up line
2. Data link protection
3. Voice communications protection
4. Open world protection
5. Cockpit protection

4.4.1 Electromagnetic Attack & Back-Up Link

An Anti-Threat Data Link System (ATDL) has been studied and developed. The Risk Analysis results show that the current safety of commercial flight is high, but there are several situations where this safety is not enough. The future trend is to guarantee the totally safety, and this requires the protection of the current communications systems.

The main idea was the development of system highly integrated among the different radio transceiver; this have lead to develop a centralized controller in order to manage the different radio-link; the information about the jammer situation should be send by the new detection system and by each available radio-link.

The theoretical results, relevant to the anti-jam techniques, have been applied to the VHF/UHF transceiver to realize a radio system that fulfils the SAFEE requirements.

In addition to these theoretical results, the implementation of the ATDL experimental mock-up using the frequency hopping technique and the demonstration of the functionality of such transceiver system, realize the final assessment of this SAFEE Work Package.

4.4.2 Securing Data link

Through the task "Securing Data link" the functional specifications of the experimental mock-up were defined. The Mock-up is actually composed of three independent mock-ups that correspond to the ACARS, ATN and IP domain.

The IPSEC-over-VDL2 feasibility has been validated in a scenario that closely looks like an operating one (i.e. with an actual VDL2 system).
The combined use of IPSEC and X.509 certificates demonstrated their robustness against eavesdropping, reply and impersonation threats. Moreover, the future passage from IPv4 to IPv6 for aeronautical applications makes this solution feasible for integration with future, wide-band data links.
The limited bandwidth of VDL2 channel made this integration critical, in terms of throughput and air-interface timers.

4.4.3 Voice Communications Authentication System - VCAS

During the risk analysis performed on the Voice Communications, several counter-measures were defined to reduce the identified risks to an acceptable level. A functional specification was produced to define the set of counter-measures that were selected and specify the mock-up functions that are required to support such counter-measures. The purpose of the mock-up is to evaluate the counter-measures' efficiency and compatibility with the aircraft environment and operations.
The counter-measure to reduce the risks level associated to the Voice Communication domains identified during the risk analysis and to be implemented in the mock-up consists in the voice authentication.
It has to be considered that in a near future, a new generation of radio will appear. The update process of currently used VHF radios has begun and will lead to a more developed data system surrounding air-ground communications. Indeed, there will be less voice communications and most of the time; data link will be used to obtain clearances and information.
Meanwhile, voice communications will be used mostly for emergency messages: one more reason to guarantee to the receiver the authenticated property of these messages. This is founded by the results of the validation trials.

4.4.4 Open World

Based on the ARINC 763 standard, the new "Open World" domain is realised outside of the avionics/aircraft control domain.

The Open World domain is centralising the aircraft information, making data links available with the certified avionics domain and with the aircraft external communication links, thus creating security holes endangering the flight safety. The Open World is using COTS server machines wired all together through Ethernet networks and capable to host software applications not dedicated to aircraft environment and sometimes just purchased from traditional COTS retailers.

4.4.5 Securing the cockpit

The aim of this task is to analyse the detection of the attempt of an unauthorised person to take the direct or indirect control of the aircraft in the cockpit.

This task will not try to create an authentication means to control avionics equipment, mainly because it will add an unacceptable unwanted event on safety: “false reject of the pilot authentication”.

Therefore, this task will mainly try to find out the correct way to identify people in the cockpit area, triggered by the ground (or TARMS) after an event such as:

- Trajectory modification according to the flight plan,
- No response on the radio,

- Sending transponder code 7500 (hijacking code),
- TARMS request.

This task aims at searching the best biometrics authentication technologies to be used in the cockpit.

- A mock up of an identification system will be defined and developed. It will integrate authentication sensor with fingerprint processing and will be coupled with cockpit photo snapshots or short video sequence in order to insure that pilots are not under constraint. These data will be sent to the ground through the data link secured (see §4.4.2) or through the specific back-up connection studied (see §4.4.1).
- Functional and ergonomic test in laboratory shall be finally performed.
- Finally, the mock-up was integrated with the TARMS at the NLR for the general integration and assessment.

4.5 TRANSVERSE ACHIEVEMENT

In addition to specific work on specific domains (refer to § 4.1 to 4.4), SAFEE aims were to perform transverse work valid for all the SAFEE domains. It required undertaking the following tasks:

1. Legal analysis
2. Risk assessment
3. Validation strategy
4. Training
5. Economic study
6. Technology watch
7. Users involvement

4.5.1 Legal Achievements

The legal research group provided overall conclusive synthesis on Aviation Legal and Regulatory Documentation (and their Relevance to SAFEE), as well as legal recommendations to SAFEE with respect to international security standards and guidelines. The work included Review of all relevant legal requirements (in EU and European States, as well as international and American regulations), analysis of legal conflicts between SAFEE and current regulations, and analysis of SAFEE sub-systems legal implications to provide SAFEE with Final recommendations.

4.5.2 Risk Assessment Achievements

Three security risk assessment methodology utilized in SAFEE was based on existing methodologies from partners Airbus, NLR and GS-3. A review showed that all three methods had potential, and in the end the NLR proposed Risk Assessment Process (RAP) was used to assess impact and potentiality of the 11 threat scenarios using expert opinion from aviation security specialists. The risk assessment methodology in SAFEE performed in SAFEE was of a qualitative nature.

The methodology proposed by NLR was successfully used to assess the security risk of current practice flight operations. The assessment resulted in a ranking of the risk related to eleven threat scenarios. SAFEE has published the Security Risk Assessment Model in several professional conferences and forums.

4.5.3 Validation Achievements

The aim of the "Security Evaluation" is to provide all the necessary means and knowledge to enhance the overall SAFEE system developments. To this aim the validation task served as a supportive platform assisting the developments in the sub-projects and to assure the coherence between them. This required close cooperation within the SAFEE as well as communication with stakeholders relevant to the aviation security issue and potential end-users of the SAFEE systems via User Club meetings (refer to §4.5.7). In order to ascertain cohesion it was elaborated the overall SAFEE Operational Concept Description (OCD) definition, based on operational procedures and guidelines for the different actors. A further important step was to thoroughly analyse and evaluate in-flight threats and threat scenarios with respect to their impact and potentiality (through a "risk assessment"). This allowed the definition of responses to counteract the different threats imposed by terrorists, to be used to enhance the SAFEE system development

After the completion of the SAFEE OCD and system requirements and specifications an important activity was to develop an overall validation strategy, which was followed by experiment design plan and evaluation method.

Subsequently, an overall SAFEE validation strategy and design plan was established. This was used as basis for the integration and validation activities carried out within the four technological areas:

- Validation of the Onboard cabin Threat Detection System ;
- Validation of the Threat Assessment and Response Management System ;
- Validation of the Flight Protection System ;
- Validation of the secured Data Links technology.

Apart from the evaluation in the validation exercises SAFEE project results were assessed by a security assessment of the aviation security system, when the SAFEE systems and operational procedures are in use. The results of this assessment showed that the technology developed in SAFEE has significant potential to improve the security situation on-board an aircraft. Although it became clear that technology alone cannot provide a complete solution without the support of procedures and human interaction.

4.5.4 Training Achievements:

The objectives of the SAFEE Training work package were:

- To provide a Blueprint of training required for operational training once SAFEE may be in operation;
- To enhance/ease understanding of the stakeholder communities on the intentions and results of the SAFEE project;
- To provide practical training to the stakeholder community (this includes preparation of the flight crew to their contribution of validation). This involved a 3 step training program starting with a Web-based training module to be performed at home, a classroom seminar and to end with a simulator training session to improve also the skills needed for SAFEE operations.
- SAFEE training seminar and practical training provided the following:
  - Understanding of the systems and procedures in SAFEE concept
  - Knowledge of capabilities, functions and usability of SAFEE systems
  - The ability to activate TARMS functions and screens
  - The ability to make security based decisions using a pro-active security mindset in combination with advanced information network.

These objectives have been met, first by analysing the training needs, followed by designing and developing the training modules and finally by delivery of training to a range of stakeholders (air crew, cabin crew, IFALPA representatives, airline managers and representatives),

The training analysis outlined the impact of the SAFEE systems on operational procedures and where it might enhance the ICAO regulations. SAFEE introduces new technology, new concepts and new procedures. Given SAFEE systems and procedures, additional training is needed in order to fill in the gap between the current level and what SAFEE considers a required proficiency level. As the first integrated security oriented system on-board, it is important that the crew knowledge regarding security will be complemented and upgraded to be able to benefit from the increased security level offered by the application of new technology. Relevant stakeholders should be acquainted with the new system, the new concept and general characteristics. It was suggested to supply a simple awareness program designed to introduce the system's ability to the different stakeholders.

For end-users, SAFEE requires a higher level of crew training regarding new knowledge, skills and attitudes regarding the different threats the system is able to detect, the ability to analyse the threats, the passenger's behaviour and PDI's; the ability to recognise concealed weapon or an item that can easily turn into weapon; the correct way of interacting with the passenger in order to verify or refute the threat; and even basic submission techniques and more. In order to assure a high level of understanding and knowledge, the training will be delivered using hands-on drills and practices, videos, live demo's, simulations and simulators. Training materials used should be stimulating to refrain from training complacency.

Based on these requirements, SAFEE dedicated training was designed and materials were developed. This involved a three level approach where classroom seminar type training was augmented with a dedicated computer based training (CBT) program and hands-on training using the NLR GRACE simulator.

The overall training program, as actually delivered, proved to be a very powerful tool for providing an overall understanding of the SAFEE concept and systems –a top down approach, and a user point of view oriented understanding of the system – a bottom up approach.

4.5.5 Economic achievements

In the SAFEE study an economic analysis of the SAFEE measures has been carried out. In this analysis, it has been assessed whether the introduction, either mandatory of voluntary, would be cost-beneficial for the airline industry and society as a whole.

Apart from the economic analysis of the SAFEE systems for airline industry and society, an airline decision model has been developed that allows individual airlines to assess the feasibility of investments in the SAFEE systems themselves. This model is based on advanced financial engineering techniques.

4.5.6 Technology Watch Achievements

In the first 18 months, the Technology Watch group has conducted thorough research on existing and developing technologies that might be used in SAFEE. Afterwards, the technology watch provided an overview of the latest developments in the field of technology and threats that were relevant to SAFEE research. On the SAFEE secured website (AGORA) a dedicated watch room was developed that was weekly updated with information from outside the project. The technology watch provided reports on security equipment and developments in detection and protection technology..

4.5.7 User Club achievements

During the course of the SAFEE project six User Club meetings were organised. The user club meetings were instrumental element in the dissemination of SAFEE developments. The plenary User Club meetings were used to brief larger audiences on the developments in SAFEE and to collect feed-back. In smaller dedicated thematic users group meetings were organised to allow more detailed discussions and workshops. The input from end-users and stakeholders was valued as important input for the guidance of the system developments. User group members on occasion also provided individual contributions to SAFEE using their expert knowledge for assessments and validation. Part of the user group members were trained for participation in the TARMS validation trails. All user club meetings were documented in a corresponding deliverable.

5 MAIN CONCLUSIONS REACHED

5.1 DATA SECURITY

5.1.1 Electromagnetic Attack & Back –Up link

SAFEE had increased the knowledge of antennas response when they are working in strong electromagnetic fields environments.

The theoretical results for Anti-Threat Data Link System, relevant to the anti-jam techniques, have been applied to the VHF/UHF transceiver to realize a radio system that fulfils the SAFEE requirements.

5.1.2 Voice Communication Authentication System - VCAS

The main conclusions of these works are:

- Technical viability of the system was demonstrated, which shows also the stand-alone property of the system that doesn't have any impact on Airborne and ground communication architecture.
- The pilots like the idea behind the VCAS. They see the voice communication authentication information as valuable and useful information.

5.1.3 Open World - Biometric Database

The developed systems on the mock-up are useful and enough reactive.

- The protection of OW application is mandatory.
- Users think that biometrics-based OW authentication is more secure and easy to use than classical pin-code procedures.

User's concentrated on evaluating impacts on aircraft operation, so they proposed improvements about some functions.

- Identification of crewmembers before requesting access to the cockpit

The feedback about the identification of crewmembers before requesting access to the cockpit is very positive.
The developed biometry system could favourably replace the current keypad, but with a terminal dedicated to request access to the cockpit.

- Authentication of the crewmembers when they are boarding.

This SAFEE top level requirement is performed during an upload session.
The main constraints of the system are linked to the process inherent to the biometry: upload and database management. A further step of development should focus on this process, in order to make it more flexible and adaptable to airlines operation.
The proposed improvement is to perform upload on a dedicated terminal. This should allow mitigating the constraints linked to the unique terminal used for upload and identification as implemented in the SAFEE experimental mock-up.
Note: The process to perform the authentication of a crewmember that is rejected because of his temporary bad fingerprint should be also reviewed in the frame of this development step.

- Erasure of the local data base

The crewmembers agree with the local database erasure to prevent access to their personal data, when they leave the aircraft.
In the mock-up, the erasure function is automatically performed after each flight, when the aircraft arrives at the gate, even if the same crewmembers are in charge of the next flight (short range/domestic flights).
So it is expected to redefine the erasure function with additional conditions.

- Re-authentication of the cockpit crew

The used technologies (biometry and video analysis) seem to be mature enough to assess if the cockpit is secure.
Nevertheless, further developments are needed to work on integration and HMI in close contact with airlines for reducing as much as possible the operational constraints and for successfully integrate the system in the cockpit environment.
Moreover, as the results of this system are used to determine if a hijacking has occurred, high reliability will be one of the key success factor, as well as the transmitted information to the ground. Regarding this last point, the sent data should have to be as intuitive as possible and should be elaborated with the end-users.

5.2 LEGAL STUDY

An analysis identified at first step three new main topics which required special legal attention:

- The Apparent breach of human rights, by heavily monitoring and recording/saving passengers various activities during check in process and especially on board the aircraft. The due balance should be analyzed.
- Such supervision, while monitoring and putting on record wide range of personal details and real time behaviour, could easily give evidential ground for proving some unlawful acts which are not related to security. Questions of privileges and immunities should be discussed.
- EAS -Emergency Avoidance System could in some situations take over full control of the aircraft while totally neutralizing the pilot in command. Significant questions of responsibilities and liabilities are raised.

Current security regulatory norms do not provide adequate solutions for the above mentioned legal conflicts

Based on further research in SAFEE the following additional issues where identified:

The traditional authority of the Aircraft Commander (PIC):

- PIC's full authority has been eroded through the years, basically due to technical developments and security needs. This erosion was not comprehensibly addressed by the international aviation lawmakers.
- Once PIC authority is diminished, his responsibility is diminished respectively.
- SAFEE's approach as implemented in EAS system is quite revolutionary, especially if on some stages (due to security reasons) we totally neutralize the PIC from any theoretical option to re-takeover the control. The existing global regulatory regime does not face such situation and should be reframed.
- Until that update, and certainly following it, EAS shall have essential implications on basic legal issues related to PIC, such as authorities, responsibilities and liabilities.

The applicable laws during all stages of the flight:

- Any aviation law question is likely to raise an international air law question and not only a municipal law question, since most areas of air law are nowadays covered by international agreements and conventions.
- Thus, every individual question concerning the various elements participating in, and connected with, the flight operation, as well as in relation to the position of the aircraft as it progresses along the flight route, will have to be scrutinized under this complex amalgam of norms, whether they originate from international law, or from the applicable individual municipal law, or laws.

The legal regime applicable to encryption:

- Although encryption is referred to within global aviation legislation, it is done symbolically and not in a manner of any prohibition and/or limitation to be imposed. Encryption as it is cannot be legally treated as a "stand alone" component, but as part of other product/s, as long as it does not diminish the level of safety.
- The aviation industry does not welcome encryption in its systems, unless there is a good cause to do so. Yet, terrorism activities and hacking are explicitly mentioned as legitimate causes, as well as keeping human rights, such as privacy issues within encryption context.
- Encryption should legally be dealt with, then, like any other avionic product. It should be safe and reliable. Its complicacy is an issue for the manufacturers to tackle, according to existing norms of Product Liability4

[4] See 3.6.4 above.

The liability regime applicable to aircraft manufacturers:

- The Rules of Product Liability Law will apply to SAFEE as to any other product. Thus, each manufacturer of any individual component of the SAFEE system will be liable for any injury, or damage, resulting from a defective product it has manufactured.
- In Europe the 1985 EC Directive, coupled with individual national liability systems, will most probably create a no-fault regime, so, in general, it can be stated that claimants against SAFEE manufacturers will not have to prove fault.

5.3 THREAT ASSESSMENT

Direct assessment of the SAFEE systems proved to be challenging due to unavailability of system performance data at the time of the assessment. An alternative approach was introduced to assess the potential security benefits of the SAFEE functions in which operational system performance parameters were determined and used as reference. The results from the assessment of the SAFEE functions showed that, in general, TARMS is expected to contribute significantly to the reduction of the security risk in all the threat scenarios. The EAS is rated to be significant in the reduction of the security risk in 9/11 scenarios.. Furthermore, the communication protection functions are deemed to be useful for countering communication attacks. The experts indicated that, from their expectations, the OTDS functions might need additional evolvement in order to have important security benefits.

5.4 TRAINING

During the SAFEE training analysis phase it was recognised that current crew security training can be upgraded with increased pro-active knowledge and skills. Especially regarding the possible on-board threats, passenger behaviour analysis using PDI's, interaction with passengers, countermeasures and under threat communication techniques among the crew. It was indicated by the trainees that extended security training would enable them to better understand and react towards on-board threat situations.

The SAFEE training analysis process proved to be an instrumental tool for creating the basics for the future SAFEE operational concept and procedures for end-users using SAFEE systems. By providing a description of the overall operational concept and a specific end-users perspective, the training activity (using a SAFEE classroom and simulating sessions) also played an important role in introducing the SAFEE concept to high level stakeholders and decision makers.

The following lessons learned could be distilled from the training evaluation:

- SAFEE systems and procedures will have an impact on the airline operation. Airline SOPs therefore may require to be adjusted.
- The SAFEE training provided the flight crew with background and system knowledge to enabled them to understand the reasoning and possible implications of the SAFEE functions. Based on the training pilots were able to assess the TARMS recommendations and to select the correct response related to resolving the threat situation.
- Analysis showed that the human factor is critical in the final assessment of an potential threat situation. Consequently it proved valuable to train the cabin crew in knowledge and skills needed to handle the various suggestions TARMS may provide. As a result of the training, the cabin crew understood the reasoning and possible implication of each suggestion on the threat situation.
- Early training activities for novel systems and procedures proved to be an excellent means for dissemination of project intentions as well as receiving early feedback on the system design & procedural aspects operation under realistic operating conditions.
- Due to its intuitive design the TARMS related procedures and systems prove relatively easy to learn.
- There proved to be a considerable variation in the way aircrews make use of the SAFEE functions. In order to ensure a common (airline-wide) approach, more consideration needs to be given to these individual approaches. Training may have to adapt to the personality profiles of the crew. Further study is required.
- Training needs, design and development should be developed by a single training-specific team.

- Seminar training should be delivered by the training-specific team. A particular operational training can be performed, but with guidance and assistance of the training-specific team to ensure commonality of the full training program.
- By representing the end user's perspective (performing end-user analysis), the training team should be involved from early stages of the project, in the creation of the end user's operational concept. In addition, the training system-prototypes may (apart from the test training) also be valuable for early and quick engineering prototyping and in eliciting user requirements.
- Training (delivery) management requires a specific project activity, with a budget and an assigned training manager to cover the different logistics needed in order to handle end-user's training activity, This includes organising seminars, inviting different stakeholders and invite end-users for simulator training.
- More pro-active approach towards security is needed by all operational stakeholders. Both in flight as during the airport passenger handling and screening. Training would serve as the first place to adapt the knowledge skills and attitudes needed for an effective operation of SAFEE systems and procedures. The SAFEE systems will need and provide more and different form of information compared to current situation. To assure correct operation training will be needed.

5.5 ECONOMICS ASSESSMENT

The results show that many of the SAFEE measures bring about benefits in terms of improved security. These benefits have been expressed in monetary terms. These benefits accrue to the airline industry, but also to society as a whole, and stem from a reduction of future damage as a result of accidents / incidents invoked by unlawful events. The order of magnitude of these benefits varies significantly among SAFEE functions, as some functions address a typical single threat, while other functions address a larger set of threats, and would thus prevent more security events in future.

The results of the economic analysis indicate as well that some of the SAFEE measures are not cost-beneficial under the current (indicative) costs estimates. However, some of these measures bring about operational benefits that might from an airline perspective be more important than the benefits of improved security, as these operational benefits could be considered more tangible. The benefits from better reaction regarding unruly passengers are an example in this respect, as well as the benefits from improving turnaround times as a result of more rapid counting of passengers.

Finally, a set of sensitivity analyses have been carried out, to overcome the issue that there are still many uncertainties surrounding the systems that influence the outcomes of the economic analysis. These sensitivity analyses address the influence of key factors and assumptions on the outcome of the economic analysis, and cover for instance an analysis of the maximum costs the systems may costs to still be cost-beneficial.

5.6 OPERATIONAL CONCLUSIONS

5.6.1 OTDS conclusions

5.6.1.1 *Access control function*

The access control function was successfully tested. The reading devices for the electronic boarding passes worked perfectly, and the involved experts were impressed by the high reliability of the face recognition system.

However, it must be noted that the system had to be adjusted to cope with the adverse lighting conditions at the OTDS evaluation facility. In daily operation, even more adverse and, in addition, rapidly changing lighting conditions have to be considered. To cope with this, the robustness of the system will have to be improved. This concerns both, the camera technology and the software algorithms for image pre-processing and evaluation.

In the same way cultural aspects, which could not be extensively considered in the evaluation campaigns in SAFEE, could impact the face recognition function. Even if the system was proven to be robust against effects of wearing glasses or large hats, there is other specific clothing like veils that make the recognition of a human face completely impossible. This is an issue that cannot be solved technically, but requires adequate operational procedures.

5.6.1.2 Suspicious behaviour detection function

The sub-system for the detection of suspicious personal behaviour worked fine for some pre-defined behaviour patterns. Single PDIs like nervousness and aggressiveness could be successfully detected, and the system was also capable to detect complex scenarios that comprised a sequence of several PDIs.

However, as for the access control function, the reliability of the system strongly on environmental conditions, in particular on the lighting conditions. More than that, even the definition of suspicious behaviour is currently not fully completed and validated. Particularly, cultural aspects need to be better considered when aiming at the development of a system that can be used in daily operation.

5.6.1.3 Dangerous goods detection function

The sub-system for the onboard detection of dangerous goods was successfully tested for specific substances. A stand-alone prototype has shown the performance of the developed sub-system and how it could be integrated in the lavatory compartment of an aircraft.

The basic issue with the detection of dangerous substances is that for each substance specific sensors and environmental conditions are required. This makes the installation and operation of such a system on board an aircraft more complicated. One option to overcome this issue is a careful selection and combination of several types of sensors. The progressing development of effective and small sensor types supports this approach.

5.6.1.4 Overall system

It was appreciated by the involved experts that the three basic functions

- Access control,
- Suspicious behaviour detection, and
- Dangerous goods detection

were implemented in terms of dedicated sub-systems, which are interconnected, but could also be implemented independent of each other. This will allow implementing individual functions according to their technical maturity and to specific needs of an aircraft operator.

Concluding it must be noted that the OTDS, as it was implemented, was far from being industrialised. However, the basic feasibility of the implemented functions could be proven, and needs for further improvements of both, hardware and software algorithms could be identified.

5.6.2 TARMS conclusions

The TARMS study has successfully built a prototype decision-support system for use by teams of on-board actors when managing a threat situation. This prototype has been fully evaluated by 10 teams of 3 persons (pilot, co-pilot, cabin crew) using 6 threat scenarios. Detailed conclusions now follow.

Through consultation with a range of stakeholders, a set of requirements for an information management and decision-aiding system to support pilots and cabin crew in security related situations has been captured. The Objectiver tool was used to great success as a means of storing and representing the stakeholder’s needs and system requirements.

Using these requirements, we have designed and built a prototype system that can make threat assessments based on outputs from onboard and ground based sensor systems. These outputs (e.g. signs of nervousness) could be provided from human reports or from sensor-based systems. The prototype was constructed using an object-orientated agent based design, built around the successful use of JADE and PASSI.

The prototype is able to provide estimates of threat for the 4 key threats as highlighted by security experts. These 4 threats are Hijack for use as a missile, Hijack for demands, Bomber on board and Unruly Passenger. This threat information, along with advice in the form of possible responses to mitigate the threat, is presented to the pilots and cabin crew via an HMI. In the case of the pilots, the HMI is accessed via the Electronic Flight Bag (EFB). The threat assessment and responses are based on knowledge captured from experts and embedded within inference models of Bayesian Networks and a Rule-based expert system.

The prototype TARMS system was successfully integrated into the GRACE simulator where it was tested against 6 scenarios developed through consultation with domain experts and validated by GIGN. Although there was a debate at the start of the project as to the benefit of using GRACE to validate what is essentially a cabin based system, the success of the trials and the quality of comments provided by the pilots showed that the use of GRACE was the correct choice.

Extensive validation trials were conducted with pilots and cabin crew as the participants. The results showed that:

- TARMS increased the crew's awareness of the threat situation, although it had no effect on the crew's perception of the likelihood of the threat.
- The participants highlighted the ability of TARMS to provide a common picture of the situation to all the different users. Though TARMS cannot replace the voice communication between the cockpit and the cabin crew, the common picture provided by TARMS does allow the communications to be concise and focused which is very beneficial during a threat situation.
- Participants felt that the strength of the system was in its detection of PDIs rather than in its interpretation and decision making. Many participants had reservations about the value of having TARMS on board the aircraft in its current state, and in particular about the response management aspect of TARMS.
- Overall the main impression from the validation trials was that TARMS and the SAFEE concept are interesting and have great potential for enhancing the security on-board an aircraft. The majority of experiment participants stated that there was value in having a security based system such as TARMS on board the aircraft.

Integration with other SAFEE sub-systems was performed. The validation trials showed that the integration of TARMS with systems like the VCAS and the Authentication systems provided additional value to the experiment participants especially allowing them a greater understanding of the SAFEE concept as a whole. This shows that further integration with the other SAFEE systems would be beneficial.

Interfaces with other sub-systems have been proposed. as TARMS is not stand-alone system and is considered at the heart of the SAFEE concept. TARMS was not integrated with the OTDS which means that two of the key questions posed at the start of the project remain unanswered 'Should the users provide input into TARMS?' and 'Can an OTDS-like system provide the quality of input needed by a TARMS-like system?' As these questions still remain, conclusions about the full impact of TARMS on the crew workload and the quality of the TARMS responses including predictions about false alarms cannot be made.

It is clear that TARMS and SAFEE are part of a larger security concept with ground systems and governmental organisations in the loop. The trials with ERRIDS demonstrated that sending information about an on-board threat to the ground stakeholders can save a lot of valuable time. TARMS can play the central role in the aircraft as the system where all information is brought together. From TARMS this information can be injected into the ground-based information management networks. In a similar way, TARMS can receive information from the ground and distribute it to the actors on-board.

These conclusions have shown that TARMS could provide benefit in improving the security onboard an aircraft though further research must be conducted into the Response Management aspect of TARMS in order for the users to fully trust the decision that are being suggested. The trials have also shown the benefit in providing users with aspects of the SAFEE concept as a whole, which suggests that further integration with the remaining SAFEE systems, and with relevant ground-based systems, should be a priority for any further work.

5.6.3 EAS & FRF conclusions

5.6.3.1 EAS

The experimental evaluation of EAS proved to be successful since, in line with the expectations that motivated the construction of the work plan, it produces valuable feedback on the concepts and requirements envisioned at the analysis stage. Positive aspects are mainly:

- The results of the experiment indicate that EAS protection against CFIT (Controlled Flight into Terrain) works well, in the sense that the objective of clearing conflicts is met, and allows claiming that EAS has the potential of saving lives.
- The results indicate also that EAS may be acceptable, even if automatic engagement by TARMS is questionable and was questioned by airline company pilots. The engagement and disengagement philosophy shall be clarified by considering the matter from a higher-level perspective that brings TARMS and EAS together.

Besides, other valuable outcome concerning the functions and features of the EAS brings about several suggestions for improvement. These improvements are about:

- The recovery procedure, which will require special attention according to the comments received on the simplified form implemented in the mock-up.
- The trajectory in avoidance needs to be made even safer, thanks to increased safety margins and better alignment with current flying practices.
- Information display when EAS is engaged and/or active. The topic proved to be – to some extent – controversial and requires further investigation.
- The avoidance triggering logic has been lead to work at the bounds of its capacity, which gives rise to an important feedback on TARMS in terms of threat assessment and response modes management.

Further conclusions have been drawn from the experimentation which concern the evaluation process itself. It appears that for the aspects such as Flight trajectory, pilot workload and situation awareness, the evaluation suffered from some lacks in the simulation environment with respect to what would be required to apprehend correctly these aspects. Issues to be solved in the future have been identified as follows:

- Recording means should be installed on the simulator for better and more objective assessment of the A/C status and trajectory.
- Additional simulation effort could reduce confidence intervals and improve statistical significance of the results obtained in the frame of SAFEE.
- The measurement of instantaneous workload under stress induced by exceptional demands such as hijacking is an open human factor issue. Existing workload measurement methods allowing the separation of the stress component, such as NASA's Task Load indeX, are only valid for post run global evaluation. Two research directions are possible:
    - The development of instantaneous indicators allowing the separation of workload and stress.
    - The control of the level of induced stress through experimental conditions.
- Finally, an integrated experiment with TARMS and EAS working together could be very useful to clarify the engagement and disengagement conditions that could be accepted by the crew.

5.6.3.2 EAS PSA DB

Despite of the limitations of the testing environment used for the assessment of the EAS PSA DB – which stems from the involvement of a stand alone mock-up not connected to neither EAS nor TARMS – the EAS PSA DB evaluation trials proved to be successful and yielded new insights into issues relating to the use of such a concept.

The evaluators brought two complementary viewpoints, the pilots viewpoint and the ATC controllers viewpoint. In both cases there is an agreement on the fact that, in general, the PSA DB has the potential of being useful in case of security-related crisis situation for the avoidance of prohibited areas. The improvement suggestions gained from the assessment are mainly about:

- General ergonomics of the displays which tend in particular to be cluttered with too much information shown;
- Geometrical shapes to be considered for the prohibited airspace areas

Further suggestions from pilots concern the display logics for it to be better in accordance with EAS and TARMS modes while providing information on pilots demands in normal situations. Besides, the controllers' viewpoint provides a feedback that can be turned into requirements that need to be considered further to fulfil the needs of crisis management on ground.

5.6.3.3 FRF

Regarding the Flight Reconfiguration Function, SAFEE allowed the European aeronautical industry to do a valuable groundwork in a domain that poses great challenges due to the fact that the intended function of the system consists of taking full control of the aircraft.

All airspace users (ANSP, Airlines and States) will have to participate to the deployment of such system, as it has big impact on ATM when engaged.

The study showed that the enabling basic technology is either already available or will be available in the short term. The most salient issues will relate to safety concerns (resistance to failures), which require specific care in the case of FRF since system operation is assumed to occur with no involvement of any reliable person onboard.

Given, the anticipated technical complexity of the required upgrades to host FRF, the retrofit of existing aircrafts with FRF poses serious questions about economical viability. Forward fitting proves to be the only reasonable way to proceed.

Regarding acceptability, it appears that even if most of the users called on to express their opinion accept to say that the FRF will decrease terrorist risk, many manifested reluctance in accepting it as proposed. This psychological obstacle needs to be addressed in further studies with proper consideration of the identified concerns.

5.6.4 DATA PROTECTION

5.6.4.1 Open World

For going towards the realisation of the final product, additional investigation should address the following areas:

- Physical integration of the fingerprint sensors in the OW terminals.
  For easier operation, the fingerprint sensors must be physically integrated into the OW terminals, for example: external fingerprint sensors are not acceptable for maintainers.
- Study the possibility of the integration of WP4.4 data in airline cards.
  Flying personnel have already their company badge, adding a new badge for crewmembers identification /authentication is embarrassing; the personnel should have the possibility to use their existing badge to operate with the developed system.
  The adaptation or the modification of airline badges must be examined, but it is foreseen the interoperation of the badges by various systems will require some standardisation agreements. Additionally, this standardisation is also expected to allow maintainers to work on aircraft from different airlines with the same personal card.
- Integration of digital certificates in the badges.
  In order to give the possibility to OW user to sign digitally their actions inside the OW applications, digital certificates must be integrated in the badges. To provide this functionality, the following points must be studied:
  - Generation of certificates in the enrolment phase (organisational procedure)
  - Technical integration and the protection of the certificates in the badge
  - Adaptation of the current system for using digital signature
  - Revocation and renewing of certificates (with aircraft constraints)
- Impacts on system architecture.
  The identification /authentication process of the crewmembers relies on an authentication server.
  In the frame of SAFEE, this function should be part of the TARMS (the central system security sub-system), but alternate solutions should be analysed to implement the authentication function on aircraft already in operation, taking into account the various constraints such as weight, volume, and security criteria...

Finally, the work already started in SAFEE should be pursued with architecture choices and final specification definition for implementation details and security assessment.
Moreover, due consideration should be given to certification needs.

5.6.4.2 Securing the Cockpit

The evaluation of the experimental mock-up proved to be successful despite of the impacts of the late availability of the mock-up. So, the mock-up was not operated with different settings (such as time to present the finger for re-authentication…).
These different settings should be experimented for getting the best operational behaviour of the system.

For going towards the realisation of the final product, additional investigation should address areas that are today open:

- The physical integration of the fingerprint sensors (in the instrument panel) and cameras (in the cockpit) requires dedicated equipment to be developed, with specific features such as shapes, cables or external coating.
- The principle of pilots authentication (authenticate one individual at one seat) adopted in the framework of SAFEE could be rethought. Indeed it should be more flexible to just verify if the person who presents his/her finger is authorized to be in the cockpit. The operational constraints should be decreased in this way (presence of a third man, presence of a cabin crew during a toilet visit of a pilot, etc.).
- The confirmation process by a human of a possible hijacking should be deeply investigated. The transmitted results of the re-authentication have to be studied in close contact with the competent national/international authorities and end-users.
- The cameras in the cockpit should also be considered for monitoring the overall cockpit situation, if they are powered on continuously and if images are transmitted the ground. This requires additional analysis with the competent national/international authorities and requires also agreements with the cockpit crew.

Other areas of further investigation are identified in the Final Assessment report as they relate to the same topics such as system architecture, standardized badge content and digitally-signed badges.

Finally, the work already started in SAFEE should be pursued with final specification definition for implementation details and security assessment.
Moreover, due consideration should be given to certification needs.

6 RECOMMENDATIONS FOR FUTURE RESEARCH

6.1 ONBOARD THREAT DETECTION

Since the feasibility of the OTDS functions could be basically proven, future research and development should concentrate on these aspects:

- The robustness of the system and its sub-systems against adverse environmental conditions has to be improved. This concerns mainly robustness against lighting conditions, which severely impact performance and reliability of both, the access control system and the suspicious behaviour detection system. But also the audio part of the behaviour detection system has to become more robust against surrounding noise.
- The reliability of the access control function and the function for the detection of suspicious behaviour has to be ensured for all kinds of personal or cultural specifics.
- Both, system hardware and software implementations need to be modified to meet requirements for the onboard installation and system qualification.
- The modularisation of all implemented functions should be increased to improve scalability and customisation capabilities.

Another aspect that needs to be considered is the integration of the OTDS with other onboard systems. This concerns legacy systems (e.g. cabin management systems) as well as other SAFEE systems (e.g. TARMS). In particular, the borderline between threat detection (OTDS) and threat assessment (TARMS) could never be satisfactorily defined. Since most of the information generated by the threat assessment module of the TARMS is already made available by the threat detection functions of the OTDS, it is recommended to adapt the OTDS in such a way that the alert messages can be directly used by the response management module of the TARMS.

6.2 THREAT ASSESSMENT AND RESPONSE MANAGEMENT SYSTEM

The Conclusions from the trials have indicated that users are very interested in the concept of a TARMS like system providing decision support to them in the early detection of possible airborne threat, thus allowing them the opportunity to take actions to prevent that threat occurring, The trials elicited the users' responses to different aspects of the system and this leads to the following recommendations.

1. Initiate a consultation with the user community (e.g. airlines and other stakeholders) to determine what form of decision-support system would now be required. This would include firstly assessing the benefits offered by the current TARMS functions e.g. the PDI (as provided by the OTDS), the collaborative working environment, and the expert-based Threat Assessment and Response Management. This should then lead to a more detailed specification of the information requirements, the collaborative decision-making processes and the user interfaces. One key recommendation is to create an additional facility to explain the reasons behind the advice provided on possible Threats and appropriate Responses.

2. Assuming the Threat Assessment (and Response Management) are considered beneficial, perform a further analysis to identify the value of sources of expertise, and then develop advanced methods for eliciting and representing this expert knowledge. This could include defining a common language to describe threats and responses with their consequences. Validation of the elicited knowledge will be a key step.

3. TARMS made various assumptions about provision of PDIs from the OTDS system. Although SP1 demonstrated some important capabilities in automatic detection of some PDIs, the majority of the required PDIs remain difficult to detect automatically. An assessment needs to be made of which systems are likely to be developed to maturity in the next 5 years, and significant work should then be instigated to accelerate the development of these systems. For the remaining PDIs, the alternative of humans providing the information (e.g. via PDAs) should be investigated.

4. TARMS identified a number of interfaces to other SAFEE subsystems (e.g. the VCAS system) and demonstrated these as part of its trials programme. A priority for any future integration project should be to define these interfaces in greater detail in the context of an overall system requirement. It is also recommended that a Technical Management Committee (TMC) be set up as a means of managing the integration of the different sub-systems. This TMC will have a mandate to enforce a system engineering

process including a standard development environment plus a rapid prototyping approach to which all the sub-projects must adhere.

5. Through a joint trial with the ERRIDS project, TARMS has demonstrated how its on-board system could collaborate with a ground-based system. It is our belief that any future project must consider the full integration of the on-board system within a system-wide information management network. Technology, architecture solutions, data and information models and rules of operation (i.e. roles of the users) should all be investigated. This should all then be demonstrated and validated in a large crisis management exercise with the operational users in the loop.

6.3 FLIGHT PROTECTION

Flight Protection addressed two important protection systems aimed at safeguarding aircraft flight against hostile attempts onboard.

6.3.1 Emergency Avoidance System

For the EAS, the work done in SAFEE corresponds to the initial cycle of an incremental development process. It comprised an analysis stage that produced an initial requirements baseline, followed by a prototyping and experimentation stage that was introduced to get further insight into requirements from end users perspective.

The results of the experimentation phase ensured the identification of the refinement and improvement areas that need to be brought into requirements specification to fully meet users expectations. The first objective of the study to be carried out as a follow-up study to SAFEE will be to establish an updated requirements baseline thanks to a further iteration cycle involving new experiments. A particularly salient point of the study will be to give even more weight to the consideration of security aspects – i.e. protection against malevolent actions – so as to have an approach appropriately focussed on the intended operational scenarios. This will inevitably lead to TARMS being included in the scope of the investigation, with the possibility of reconsidering the functional boundaries between EAS and TARMS regarding the detection and management of operational modes. A further consequence will concern the test environment, which will have to be more realistic and provide a more global operation environment.

In addition to the topics deriving from the experimentation results, further investigation shall address the left open areas. These areas of investigation include:

- The Function Protection which requires an in depth study
- The auto land extension suggested at the design stage to close gaps left in the operational use of the original functional scope.
- The on ground phase of operation, which shall be addressed to get a fully operational product.
- Further validation work that includes consideration of PSA (Prohibited Security Areas) and obstacles, in addition to terrain, is required to finalize the avoidance function.
- Compliance with the JAA/EASA regulatory framework, which is required to demonstrate that the EAS system complies with all safety regulations regarding its interface design and hence can achieve certified status.

Finally, the implementation-related work already started in SAFEE – through the ground elements that the analysis stage could bring about – shall be pursued with the aim of paving the way towards the realization of the final product. To be beneficial, such follow-on work shall concentrate on a well-defined implementation target (avionics architecture) and address the specification of the EAS components at a level sufficiently detailed, including extensive consideration not only of safety and human factors aspects, but consideration of certification needs as well.

6.3.2 Flight Reconfiguration Function

Regarding the FRF, SAFEE established the foundations of a system providing the ultimate protection function able to safely re-route and land threatened aircraft on a secure airport. The groundwork carried out in SAFEE has already allowed a follow-up study to be started in the form of the ongoing SOFIA (Safe Automatic Flight Back and Landing of Aircraft) project of the 6th Framework Programme (3-year duration from 2006 to 2009). SOFIA includes a requirements refinement stage followed by a trial phase with the whole aimed at performing a first iteration on requirements based on experimental validation. Further consideration is also to be given to the different aspects that affect acceptability. It can however be anticipated that, from technical perspective, the introduction of FRF will be facilitated by the strengthening trend towards the use of more automation in aircraft operation, which becomes all the more acceptable as the automatism behaves subliminally, i.e. in perfect synergy with operators and users expectations.

6.4 DATA PROTECTION

All the SAFEE knowledge of securing information and data will have to extended the sharing information from the on board A/C and the ground.

A net-centric operation is proposed by SESAR where the ATM network is considered as a series of nodes, including the aircraft, providing or consuming information [SESAR / Deliverable D3]. Aircraft operators with operational control centre facilities will share information via their applications while the individual user will be able to do the same via applications running on any suitable personal device. The support provided by the ATM network will in all cases be tailored to the needs of the user concerned.

Solutions have been proposed to implement SWIM[5] (including the management of its security and its safety), which is a corner stone of the future European ATM System. The **SWIM** environment will shift the ATM architecture paradigm from message exchange to information publishing/using/contributing where the definition of the data and associated services are crucial.

The architecture work has investigated and identified a number of principles and recommendations for the future architecture development within the SESAR Development Phase. Key among these is to make use of:

- An Enterprise Architecture (EA) framework which will ensure better alignment between the Information Technology systems and the Air Traffic Management business;
- Service Oriented Architecture (SOA) techniques, which clearly distinguish the ATM services, those have to be provided, from the underlying supporting services and the physical assets that will need to be deployed. SOA techniques will provide the mechanism to organise and utilise distributed capabilities that may be under the control of different ownership domains. They define a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

In

and **Erreur ! Source du renvoi introuvable.** a high level overview of the SWIM architecture is given [SESAR / Deliverable D3].

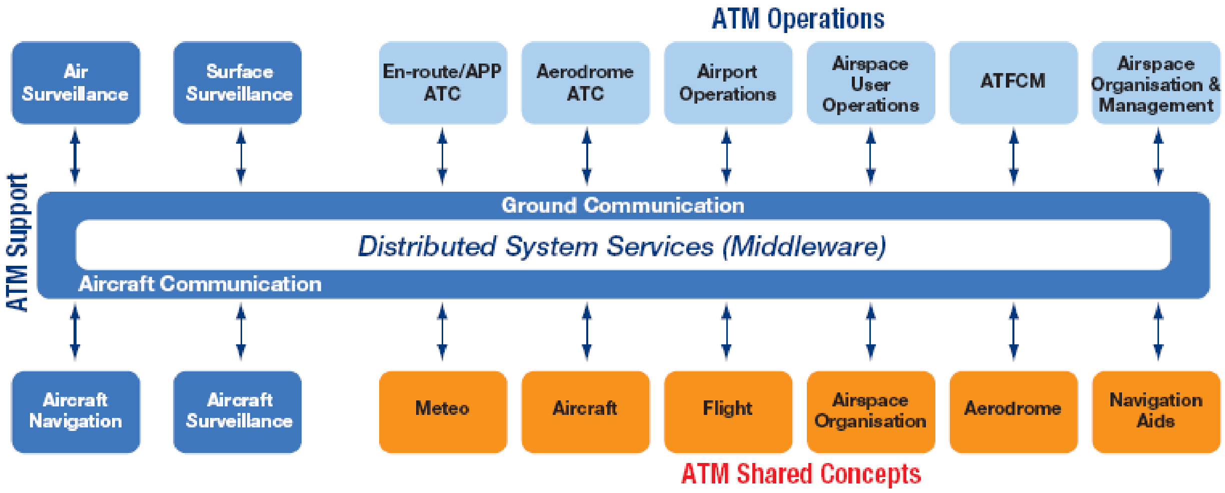

figure 6. High level European ATM System 2020 logical architecture

[5] SWIM = System Wide Information Management

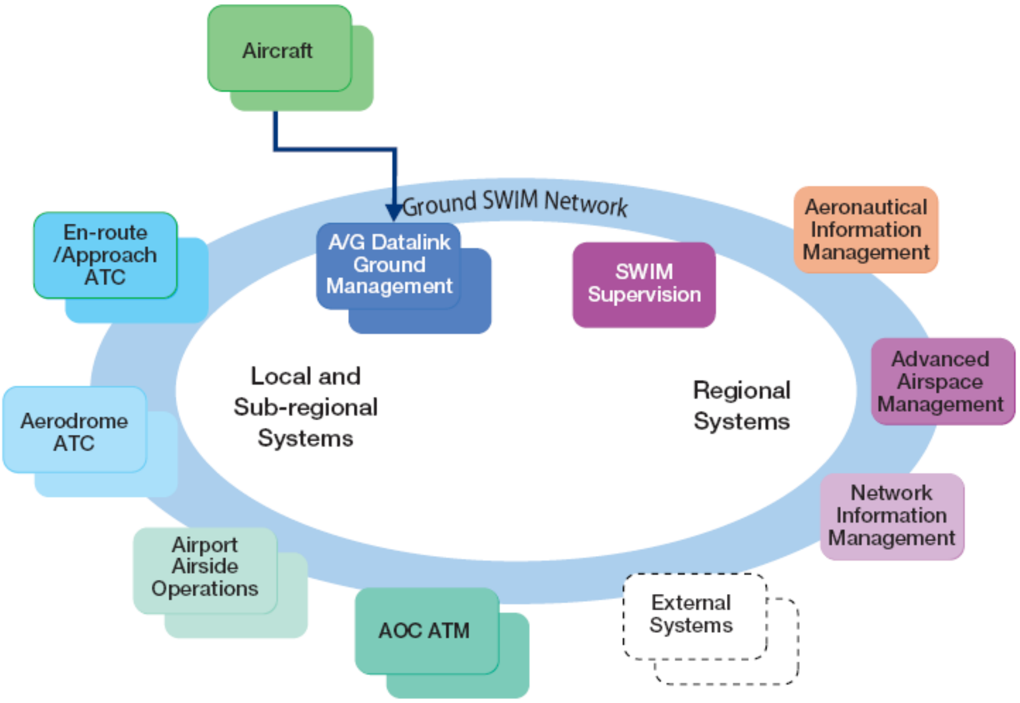

figure 7. High level European ATM system 2020 technical architecture

SWIM is supported by a set of architectural elements (so-called SWIM architecture) allowing exchange of data and ATM services across the whole European ATM System. SWIM is based on the interconnection of various automation systems. The SWIM architecture aims at providing specific value added information management services: the SWIM services. They will:

- Support flexible and modular sharing of information, as opposed to closely coupled interfaces;
- Provide transparent access to ATM services likely to be geographically distributed;
- Ensure the overall consistency.

SWIM services will need to comply with potentially stringent Quality of Service (QoS) parameters, such as integrity, availability, latency, etc. Not all users will have permission to access all data within a domain because of operational, commercial or security reasons. SWIM integrates Air-Ground and Ground-Ground data and ATM services exchange.
It is clear that TARMS and SAFEE are part of a larger security concept with ground systems or actors in the loop. ERRIDS is set-up as an information dissemination system for exchange of information related to security threats. Under SESAR a net-centric operation is proposed, implemented by the SWIM architecture. In both the ERRIDS network and the SWIM architecture the aircraft is a node. The trials with **ERRIDS** have demonstrated that sending information about an on-board threat to the ground players can save a lot of valuable time. TARMS can play the central role in the aircraft as the system where all information is brought together. From TARMS this information can be injected into the information management networks. In the same way TARMS can receive information from the ground and spread it to the actors on-board.

6.5 REQUIREMENTS AND VALIDATION

The validation process in SAFEE has been performed in accordance with the E-OCVM methodology. This has,
- first, enabled a correct organisation of the validation process and a clear approach to the validation objectives to be assess by the exercises;
- second, facilitated the coherence and cohesion in the definition of the validation experimental plans in the four sub-projects;
- third, provided an easy methodology to carry out the validation process and to present it and the results to the external community.

The experience of applying the E-OCVM in SAFEE has been successful, as it has facilitated the organisation of the validation process and its presentation to the external community.

During the validation process, the development of an overall validation scenario revealed an important support in the definition of the validation scenarios. Though initially difficult to define, such scenario enabled the transfer from the operational scenarios to the particular validation scenarios performed in the validation exercises.

The validation process in SAFEE has only focused in the performance of the systems. This is a gap to be solved in next projects, especially in large ones, where the validation has to be linked also to other characteristics related to the system and its impact in the environment. In particular, SAFEE systems are also related to security, safety and economical aspects. Though all of them have been assessed in the SAFEE project, such assessments have been done without any connection to the validation process. This is to be avoided in next projects as the validation has to be seen as an overall process affecting several aspects, not only the performances.

For this reason, it is recommended that future projects consider the validation as an integrated process to assess performance, security, safety, economical, human factors, and environmental aspects depending on the scope of the systems developed. To achieve this aim, the E-OCVM and the outcomes from projects like CAATS II reveals key.

Finally, and as a general remark, it is important the participation of the authors of the project validation methodology in the design and performance of the validation exercises to be performed in the project, specially when the number of exercises is high. This is the only way to keep the coherence and relation among the validation exercises along the project and to facilitate their presentation to the external community.

6.5.1 Security risk assessment

Security risks assessment techniques need to be further improved to be able to validate the security risk of systems and operations in conditions where limited information is available on effectiveness of functions. The approach should allow an assessment of the systems even when limited operational data is available of the intended security systems.

6.5.2 Legal issues

Privacy issues remain a challenge that will need constant attention. Especially in the area of surveillance of passengers and crew sensitive situations might occur. Close cooperation with responsible legal entities is needed to further develop these technologies.

In the field of data protection global standardisation might be needed on legal issues in order to allow these technologies to be used on a world-wide scale.

From a point of view of automated flight functions the position of the captain as the commander of the aircraft and most responsible entity for the safety of the flight need to be taken into account in future developments.

6.5.3 Security Training

From a training point of view it was concluded that training should be integral part of the system development. It was determined that training can even be a valuable tool for the assessment of systems and the capture of (additional) improvements and feed-back. The intensive use of systems in combination with procedures in simulated operational conditions proved to be a unique asset for the collection of user feed-back.

As an example: following the SAFEE training sessions in the NLR GRACE simulator it was recognised that the future TARMS operational procedures might be improved by incorporating the training results. Partially this was based on individual or company preferences but also more generic improvements were identified.

Training made also clear that the human factor in the handling of a crisis is of paramount importance. Technology alone cannot provide complete identification assessment and response to a threat.

7 ACKNOWLEDGEMENTS – POINT OF CONTACT

The SAFEE consortium wants to thank the European Commission for having given the opportunity to carry out such research on Security with their contribution to the funding.

The SAFEE consortium thanks our EC Project Officer Marco Brusati with the 3 Reviewers, [Steve Zerkowitz (only during the first 1 ½ year), Professor Yurdanur Tulunay and Jean Grossin] for their participation to our management meetings, to the assessment sessions and for their valuable comments.

For any complementary information contact could be done via:

EC Officer Dr. Marco Brusati

Fax : **+32 2 296 67 57**

E-mail **marco.brusati@cec.eu.int**

And

http://www.safee.reading.ac.uk/.

8 ANNEX/ EXTRACT OF GLOSSARY OF TERMS DEFINITION

Acceptance

Acknowledgement by the certification authority that the submission of data, argument, or claim of equivalence satisfies applicable requirements (derived from CAST discussions).

Agreement

Acknowledgement by the certification authority that a plan or proposal relating to, or supporting, an application for approval of a system or a requirement, is an acceptable statement of intent with respect to applicable requirements.

Anomalous behaviour

Behaviour that is inconsistent with specified requirements.

Applicant

A person or organisation seeking approval from the certification authority.

Application

The act of putting to a special use or purpose

Approval

Acceptance and/or the formal act of approving.

Certification

Legal recognition by the certification authority that a product, service, organisation or person complies with the requirements. Such certification comprises the activity of technically checking the product, service, organisation or person and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval or other documents as required by national laws and procedures. In particular, certification of a product involves: (a) the process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety; (b) the process of assessing an individual product to ensure that it conforms with the certified type design; (c) the issuance of a certificate required by national laws to declare that compliance or conformity has been found with standards in accordance with items (a) or (b) above.

This process includes validation and verification of a function according to regulatory and functional requirements containing qualified components.

Certification Authority

Organisation or person responsible for granting approval on behalf of the nation of manufacture.

Database

A set of data, part or the whole of another set of data, consisting of at least one file that is sufficient for a given purpose or for a given data processing system.

Demonstration

A method of proof of performance by observation

Function

The appropriate or assigned duties, responsibilities, missions, or tasks of an individual, office, or organization

Guidelines

Recommended procedures for complying with regulations

Implementation

The act of creating a physical reality from a specification

Integration

1) The act of causing elements of an item to function together.
2) The act of gathering a number of separate functions within a single implementation.

Network

A term used to refer to one or more physical communications links used for the same purpose.

Object Code

A low-level representation of the computer program not usually in a form directly usable by the target computer but in a form which includes relocation information in addition to the processor instruction information.

Operating System (O/S)

The same as Executive Software.
The OS refers to the software kernel only which services the underlying hardware platform.

Qualification

The process of demonstrating whether a system or component is suitable for operational use **[near IEEE]** and fulfilled the safety requirements.

Realisation

Realisation consists of all further Design and Implementation activities proceeding from a Specification. No particular level of abstraction of such a Specification is assumed unless implied by the context.

Requirement

An identifiable element of a function specification that can be validated and against which an implementation can be verified.

Risk

The frequency (probability) of an occurrence and the associated level of hazard.

Safety

1) This is the attribute of dependability with regard to the non occurrence of failures of given criticality level. In a quantified way, it is the conditional probability that the system has not fallen into a category of failures till the time ***t***, given that it was operational at time ***0***.
2) The state in which risk is lower than the boundary risk. The boundary risk is the upper limit of acceptable risk. It is specific for a technical process or state.

Security

This is the attribute of dependability with regard to the prevention of unlawful acts.

Service

Service means the functions that the application can use for operation.

Simulation

All the elements (executables, configuration files, test sets) defining a functional model which can be handled by a user.

Simulator

A device, computer program or system used during verification, that accepts the same inputs and produces the same output as a given system.

Standard

A rule or basis of comparison used to provide both guidance in and assessment of the performance of a given activity or the content of a specified data item.

System

1) Any group of components, modules or sub-systems describing an operational entity **[ARINC 651]**.

2) A collection of hardware and software components organised to accomplish a specific function or set of functions. **[DO-178B]**
3) A term used to refer to collection of interconnected entities which perform a particular aircraft related role e.g. the control of Cabin Pressure.
4) A combination of inter-related items arranged to perform a specific function (WATOG).

System architecture
The structure of the hardware and the software selected to implement the system requirements.

Task
1) Any kind of activity.
2) The basic unit of work from the standpoint of a control program. **[DO178-B]**

Test
A quantitative procedure to prove performance using stated objective criteria with pass or fail results.

Testing
The process of exercising a system or system component to verify that it satisfies specified requirements and to detect errors.

Test procedure
Detailed instructions for the set-up and execution of a given set of test cases, and instructions for the evaluation of results of executing the test cases.

Training
Training refers to the acquisition of knowledge, skills, and competencies as a result of teaching.

Validation
The determination that the requirements for a product are sufficiently correct and complete

Verification
The evaluation of an implementation of requirements to determine that they have been met

Version
Items that have the same specification, but are implemented differently are called versions.

ACRONYM	MEANING
A/C	Aircraft
ACARE	Advisory Council for Aeronautics Research in Europe
ACARS	Aircraft Communication Addressing and Reporting System
ACRF	Access Control and Registration Function
AOC	Airline Operation Communication
APC	Airline Passengers Communication
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATDL	Anti-Threat Data Link
ATM	Air Traffic Management
ATN	Aeronautical Telecommunications Network
ATS	Air Traffic Services
CAATS	Cooperative Approach to Air Traffic Services
CFIT	Controlled Flight Into Terrain
COTS	Commercial Off The Shelf
DODF	Dangerous Objects Detection Function
EAS	Emergency Avoidance System
EASYII	Enhanced Anti-jam SYstem II
ECAC	European Civil Aviation Conference
E-OCVM	European Operational Concept Validation Methodology
ERRIDS	European Regional Renegade Information Dissemination System
ETDS	Electromagnetic Threat Detection System
FAA	Federal Aviation Administration
FRF	Flight Reconfiguration Function
HMI	Human Machine Interface
ICAO	International Civil Aviation Organization
IED	Improvised Explosive Device
IP	Internet Protocol
IPSEC	Internet Protocol Security
LLF	Low-level Feature
MAEVA	Master ATM European validation Plan
NATO	North Atlantic Treaty Organisation
OTDS	Onboard Threat Detection System
OTDS	On-board Threat Detection System
PAX	Passengers
PDI	Pre-Determined Indicator
PIN	Personal Identifier Number
PSA DB	Prohibited Security Area Database
RFID	Radio Frequency Identification
RMM	Response Management Module
SAFEE	Security of Aircraft in the Future European Environment
SATCOM	SATellite COMmunications
SBDF	Suspicious Behaviour Detection Function
SP	Sub Project
SWIM	System Wide Information Management

ACRONYM	MEANING
TAM	Threat Assessment Module
TARMS	Threat Assessment and Response Management System
VCAS	Voice Communication Authentication System
VPN	Virtual Private Network
WAN	Wide Area Network
WP	Work Package

9 ANNEX/ LIST OF PARTNERS

Participant				Country	Date	
Role	**No.**	**Name**	**Short Name**		**Enter project**	**Exit project**
CO	1	SAGEM Défense Sécurité	SAG	FR	01/02/2004	30/04/2008
CR	2	Airbus – France	AIF	FR	01/02/2004	01/02/2008
CR	3	Airbus Deutschland GmbH	A-D	DE	01/02/2004	01/02/2008
CR	4	BAE SYSTEMS (Operations) Ltd.	BAE	UK	01/02/2004	30/04/2008
CR	5	THALES Avionics SA	THA	FR	01/02/2004	01/02/2008
CR	6	Stichting Nationaal Lucht- en Ruimtevaartlaboratorium (NLR)	NLR	NL	01/02/2004	30/04/2008
CR	7	ATHENA Global Security Services Solutions (GS3)	Gs3	IL	01/02/2004	01/02/2008
CR	8	Selex Communications S.p.A.	SEL	IT	01/02/2004	01/02/2008
CR	9	SITA Information Networking Computing B.V	SIT	FR	01/02/2004	01/02/2008
CR	10	EADS Innovation Works FRANCE	EAF	FR	01/02/2004	01/02/2008
CR	11	EADS CCR GERMANY	EAD	DE	01/02/2004	01/02/2008
CR	12	Ingenieria de Sistemas para la Defensa de España, S.A.(ISDEFE)	ISD	SP	01/02/2004	01/02/2008
CR	13	Galileo Avionica SpA (a Finmeccanica Company)	GAL	IT	01/02/2004	01/02/2008
CR	14	Bundesanstalt für Materialforschung und -prüfung (BAM)	BAM	DE	01/02/2004	01/02/2008
CR	15	Hellenic Aerospace Industry (HAI)	HAI	GR	01/02/2004	01/02/2008
CR	16	Airtel ATN Limited (AIRTEL)	AIR	IRL	01/02/2004	01/02/2008
CR	17	Office National d'Etudes et de Recherches Aérospatiales (ONERA)	ONE	FR	01/02/2004	01/02/2008
CR	18	SKYSOFT	SKY	PT	01/02/2004	01/02/2008
CR	19	Siemens Gebäudesicherheit GmbH (SIEMENS)	SGS	DE	01/02/2004	01/02/2008
CR	20	ROCKWELL-COLLINS FRANCE	RCF	FR	01/02/2004	01/02/2008
CR	21	SODIELEC	SOD	FR	01/02/2004	01/02/2008
CR	22	CENCIARINI	CEN	IT	01/02/2004	01/02/2008
CR	23	Informatique Electromagnétisme Electronique Analyse numérique (IEEA)	IEE	FR	01/02/2004	01/02/2008
CR	24	Environics Oy	EOY	FI	01/02/2004	01/02/2008
~~CR~~	~~25~~	~~Miriad Technologies~~ (bankruptcy)	~~MIR~~	~~FR~~	01/02/2004	01/02/2006
CR	26	ECORYS Nederland BV	ECO	NL	01/02/2004	01/02/2008
CR	27	RESPECT IT	RES	BE	01/02/2007	01/02/2008
CR	28	Technische Universität München	TUM	DE	01/02/2004	01/02/2008
CR	29	University of Reading	UoR	UK	01/02/2004	01/02/2008
CR	30	CEDITI => RESPECT IT	CED	BE	01/02/2004	01/02/2007
CR	31	THALES SVS	SVS	FR	01/02/2004	01/02/2008
CR	32	SIA SpA	SIA	IT	01/02/2004	01/02/2008

10 ANNEX/ WORKPACKAGES BREAKDOWN OF SAFEE

SAFEE was structured in 5 Sub projects (SP) each of which having their own work package (WP) structure.

- SP1 OTDS: Onboard Threat Detection System (leader Airbus Deutschland)
  - WP 1.1: Overall Concept Definition (leader Airbus Deutschland)
  - WP 1.2: Access Control and Registration (leader Rockwell Collins)
  - WP 1.3: Person Movement and Behaviour Detection (leader Rockwell Collins)
  - WP 1.4: Detection of Dangerous Goods and Materials(leader EADS Deutschland)
  - WP 1.5: Integration and Evaluation (leader Airbus Deutschland)

- SP2 TARMS: Threat Assessment and Response management System (leader BAE systems)
  - WP 2.1: Requirements (leader ONERA)
  - WP 2.2: System Specification (leader Skysoft)
  - WP 2.3: TARMS System Development (leader BAE systems)
  - WP 2.4: Database Construction (leader BAE systems)
  - WP 2.5: System Integration (leader NLR)
  - WP 2.6: Validation and Training (leader NLR)
  - WP 2.7: Technological assessment (leader ONERA)

- SP3 Flight protection (leader Thales Avionics)
  - SP3.1: Emergency avoidance system
    - WP 3.1.1: Environment (leader ISDEFE)
    - WP 3.1.2: Implication of threat/requirements (leader GALILEO)
    - WP 3.1.3: Safety Aspects (leader ISDEFE)
    - WP 3.1.4: System architecture and specification (leader Thales Avionics)
    - WP 3.1.5: Development of the experimental mock ups (leader Thales Avionics)
    - WP 3.1.6: EAS Test bed development (leader Thales Avionics)
    - WP 3.1.7: EAS Integration & validation (leader Thales Avionics)
    - WP 3.1.8: Evaluation & Assessment
  - SP3.2 Flight Reconfiguration (leader SIA)
    - WP 3.2.1: Flight reconfiguration potential solutions (leader GALILEO)
    - WP 3.2.2 Flight reconfiguration safety & human factor (leader ISDEFE)
    - WP 3.2.3 Flight reconfiguration system architecture and specifications (leader Thales Avionics)
    - WP 3.2.4 Flight reconfiguration acceptability & confidentiality (leader HAI)
    - WP 3.2.5 Flight reconfiguration recommendations (leader Thales Avionics)

- SP4 Data Security (lead SAGEM Défense Sécurité)
  - WP 4.0: Critical Data Identification (leader AIRBUS France)

  - WP 4.1: Electromagnetic attack & back up link (leader SELEX)
  - WP 4.2: Securing Data Links (leader SITA)
  - WP 4.3: Securing Voice Communications (leader SODIELEC)
  - WP 4.4: Securing the Open World (leader SAGEM)
  - WP 4.5: Securing the cockpit command (leader SAGEM)

- SP5 Security Evaluation
  - WP5.1: Legal and regulatory issues (leader GS3)
  - WP5.2: Security/risk analysis (leader NLR)
  - WP5.3: Validation strategy, design and evaluation (leader ISDEFE)
  - WP5.4: Training (leader NLR)
  - WP5.5: Economic analysis (leader ECORYS)
  - WP5.6: Technology Watch (leader GS3)
  - WP5.7: End-Users Club (leader BAE)

11 ANNEX/ DISSEMINATION

11.1 SAFEE PARTICIPATION IN EXTERNAL MEETINGS

Event	Article /Presentation	Venue and Date
ASAS TEN-T Workshop	SAFEE presentation	Toulouse 19&20 April 04
Communicating European Research	SAFEE presentation	Brussels 11&12 May 04
MAEVA Dissemination Forum	No presentation	Palma deMallorca, 13-14/05/2004
IMG3 Brussels	SAFEE presentation	Brussels 19 May 04
BALPA Security meeting	SAFEE/SP2 presentation	London 2 June 2004
ARINC Working group	SAFEE presentation	21-23 September 04
ERRIDS User Group	SAFEE presentation	28 Sept 04
ARINC SEC group	SERA Risk Assessment Methodology presentation (without any SAFEE result)	Toulouse, 16th to 19th November 2004
EUROCAE	SAFEE presentation	19 Janvier 05
AAAF seminar	TARMS presentation	Toulouse 27 January 05
ICAO-OACI AVSEC Seminar	SAFEE presentation	10-12 January 05
CAATS Workshop	SAFEE Validation process	Budapest 20-21/01/2005
Public Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against Terrorism	SAFEE presentation	Brussels 29 November 2005
Violence in the Skies	Security Of Aircraft in the Future European Environment (SAFEE)	16-17th March 2005 Heathrow
EUROCONTROL SAMTF	SAFEE SP3 Safety Assessment presentation	Brussels, 22-24/03/2005
The Ergonomics Society Conference	Security Of Aircraft in the Future European Environment (SAFEE)	Hatfield University, UK. April 5th –7th, 2005.
The Security Session of the 22nd International Aircraft Cabin Safety Symposium.	Security Of Aircraft in the Future European Environment (SAFEE)	Brussels, Belgium. 21-23 June 2005.
Air Transport Security Seminar	Principle of OTDS	Lübeck, 23 June 2005
ECAC Security Workshop	Discussion of OTDS related issues	Brussels, 10 October 2005
ERRIDS	ERRIDS Stakeholders	15 February in Maastrich
CAATS Workshop	Only participation/ No presentation	Lanzarote 16th and 17th of February 2006
EU Security	European Conf. on Security Research in Vienna	20-21 February Vienna
EUROCAE	Eurocae WG 72	13-15 March In Malakoff (Paris)
JRC	Meeting with JRC	April 6th In ISPRA
ECAC	Meeting with Urs Haldimann head of Security Forum	20 April in ECAC (Neuilly)
ECAC Aircraft Security Workshop	Presentation of SAFEE in ECAC Aircraft Security Workshop	4 May Prague

France-Russie Workshop	Presentation of SAFEE	May 3, 4 &5in Moscow
IFALPA Meeting	Scope of SAFEE SP1 Discussion with IFALPA Security Working Group	17 May 2006, Bruxelles
EASA	Meeting with P Goudou & Yves Morier	23 May Cologne/Köln
EUROCAE	Eurocae WG 72	1-2 June Eurocontrol, Brussels
AERODAYS	EU Aerodays	19-29 June Vienna
Removv workshop June 6th	Regulation Modeling and their Validation and Verification	June 6th
ERRIDS	ERRIDS Stakeholders	4 July in Brussels
EASTI	Meeting on Training with EASTI in Brussels	26 July Brussels
SESAR	SESAR Stakeholder	12 September Geneva
TEHOSS 2006	SP31 - EAS PSA DB SP2 TARMS SAFEE Presentation	9-13 October 2006, Istanbul Turkey
SAGAS/AVSEC	SAGAS/AVSEC meeting 28	18 Octobre 06 Brussels
SAGAS/AVSEC	SAGAS/AVSEC meeting 2ç	30 Nov 2006 Brussels
PAPS n°3	PAPS Preparation	7 December Sagem,Paris
Seminar	The Violence in the Skies	23-25 January '07 Bangkok
Aviation Security Asia Conference	Aviation Security Asia Conference,	29-31 January '07 Singapore
Sky marshals Workshop	6 x Threats scenarios	GIGN Versailles/ March 21st
Security Incident Management workshop	SAFEE	Eurocontrol, Brussels - June 26th, 2007
TRANSEC WORLD EXPO	SAFEE Flyers	June 27/2 , 2007
Monterey workshop 2007	Applying the SAFEE requirements methodology to securising the airport	Monterey from the 10th to 14th of September
SOFIA workshop	SAFEE	Sept 13th
AVSEC World 2007	SAFEE Flyers	Vancouver, Canada, on October 30, 2007
JERE	SAFEE	Munich Airport October 24
Meeting chaired by Sophie in ´t Veld, ALDE MEP with others MEPs: Prof Yurdanur Tulunay (EC Reviewer) Marco Brusati (EC) Linda van Renssen, assistant Sophie in ´t Veld Jorgo Chatzimarkakis, ALDE MEP Sarah Ludford, ALDE MEP Stavros Lambrinidis, PSE MEP Philip Bradbourn, EPP-ED MEP Carlos Coelho, EPP-ED MEP Miriam Schoeps, assistant Alexander Alvaro Peter Hustinx, EDPS Kees Bos, Dutch newsagency ANP	SAFEE/"Human Rights"	Brussels European Parliament February 27th,2008

11.2 SAFEE USER CLUBS

- Affiliate User Club Meeting, l'Aéro-Club de France, Paris, 7-8 th June 2004
- Plenary User Club Meeting, NLR, Amsterdam, 25-26 th November 2004
- Affiliate User Club Meeting, Le Bourget Airshow, 14 th June 2005
- Affiliate Meeting, at International Airport Geneva, 30-31 th May 2006
- Plenary Meeting, at NLR Amsterdam, 7-8th December 2006
- Affiliate User Club Meeting, Le Bourget Airshow, 20-21 th June 2007

11.3 PRESS COVERAGE

May 2004	Interview of NLR/ECORYS with Magazine "Holland Airports"
17 May 2004	Le Soir Le Cediti veille sur les airs
July 2006	Der Spiegel
August 2006	Reuters Agency
September 2006	Agence France Presse
September 2006	NLR_ Article in Dutch Magazine Elsevier
10 September 2006	The Sunday Times: One page article covering all of SAFEE
06 Oct 2006	CNN.COM by Dana Rosenblatt
16 October 2006	The Engineer: Cover story
Friday 19th, 2007	Air & Cosmos
16 January 2007	SAFEE in The Washington Post
January 2007	Paper in IEEE news letter
June 2007	Le Bourget 2007 SAFEE in Sciences & Vie June 2007 Special Security Paris Airshow
February 2008	SAFEE in German press February 2008
February 2008	SAFEE in Dutch press February 2008

11.4 PUBLICATIONS / CONFERENCES

1. The Ergonomics Society Conference April 5th –7th, 2005: Security Of Aircraft in the Future European Environment (SAFEE) Hatfield University, UK.. Tim Hughes & Catherine Neary (BAE)
2. EUROCON 2005: Baysean Network Based Multi Stream Fusion for Automated Online Video Surveillance (8 June 2005, conference paper , TUM team)
3. The Security Session of the 22nd International Aircraft Cabin Safety Symposium. 21-23 June 2005: Security Of Aircraft in the Future European Environment (SAFEE) Brussels, Belgium. . Tim Hughes (BAE)
4. ICIP 2005: Video Based online Behavior Detection using Probabilities multi stream fusion Paper and Poster session (13 September 2005, conference paper "TUM Team")
5. European Aircraft Cabin Safety Symposium, 9 June 2006 : "An on-board security system and the interaction with cabin crew" presented by Arjan Lemmers and Tanja Bos
6. Goal-oriented Analysis of Regulations - Robert Darimont (CEDITI, Belgium), Michel Lemoine (ONERA, France) in Proc. Of REMO2V'2006, International workshop on Regulations Modelling and their Validation & Verification, June 2006, Luxemburg

7. ICAS Sept 2006 Hamburg : SAFEE/Risk Assessment Methodology (Lennaert Speijker)
8. Technical presentation at TEHOSS 2006 in Istanbul (09/10/06):Presentation of SAFEE; PSA Database & 'The Construction of Bayesian Networks to Provide decision Support for Security Operatives'.
9. ICT 6th annual conference on global terrorism workshop on "Threat Assessment as a Tool in Counter-Terrorism" 13 September 2006,Israel
10. Safety of Flight Conference, 25 October 2006: UoR presentation
11. 4th International Aviation Security Technology Symposium; Washington D, 27 November - 1 December 2006
12. Security Requirements for Civil Aviation with UML and Goal Orientation - - Robert Darimont (Respect-IT, Belgium), Michel Lemoine (ONERA, France) in Proc. of REFSQ'07 (Requirements Engineering: Foundation of Software Quality), June 2007, June 2007, Trondheim, Norway
13. Security of the Airport According to the RE-TARMS methodology, Robert Darimont (Respect-IT, Belgium), Michel Lemoine (ONERA, France), Monterey Workshop sponsored by NPS of Monterey, August 2007, Monterey, USA
14. ICME07: Suspicious Behavior Detection in Public Transport by Fusion of Low level video descriptors /Paper and Poster session (TUM Team)