Welcome to
ICAS, Programme Committee
Workshop
Oct, 4th 2005 in Mykonos
Security of Aircraft in the Future European Environment

Integrated Project in EC Sixth Framework Programme
DG Research AERONAUTICS & SPACE
1st call March 2003
contract n° AIP3-CT-2003-503521

Jack METTHEY
(Tjien-Khoen LIEM)
Marco BRUSATI (our EC/Project Officer)
12 Countries | 15 Large Firms | 10 SME | 6 Research centers
--- | --- | --- | ---
Finland | | | |
France | Airbus, Sagem, Thales Avionics, Rockwell-Collins MORS, EADS-CRC, SITA | IEEA, Miriad, ENERTEC | ONERA
Germany | Airbus, EADS-CRC Siemens | | BAM, Munich University of Technology (TUM)
Belgium | | CEDITI | |
Greece | | HAI | |
Ireland | | Airtel | |
Israel | | GS-3 | |
Italy | Galileo, Marconi, Teleavio | Cenciarini | |
Netherlands | | Ecorys | NLR
Portugal | | Skysoft | |
Spain | | | |
United Kingdom | BAE Systems | | University of Reading

*CORE TEAM*
### SAFEE Consortium
(31 partners, 12 countries)

<table>
<thead>
<tr>
<th>Country</th>
<th>Major Companies</th>
<th>SMEs</th>
<th>Research Institutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>Sagem, Thales Avionics, Airbus, Rockwell Collins, MORS, EDS-CRC, SITA</td>
<td>CEDITI</td>
<td></td>
</tr>
<tr>
<td>Finland</td>
<td>Environic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>Sagem, Thales Avionics, Airbus, Rockwell Collins, MORS, EDS-CRC, SITA</td>
<td>IEEA, Miriad, ENERTEC</td>
<td>ONERA</td>
</tr>
<tr>
<td>Germany</td>
<td>Airbus, EADS-CRC, Siemens</td>
<td></td>
<td>BAM, Munich University of Technology (TUM)</td>
</tr>
<tr>
<td>Greece</td>
<td>HAI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>Airtel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td></td>
<td>GS-3</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td>Galileo, Marconi, Teleavio</td>
<td>Cenciarini</td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td></td>
<td>Ecorys</td>
<td>NLR</td>
</tr>
<tr>
<td>Portugal</td>
<td></td>
<td>Skysoft</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
<td>ISDEFE</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>BAE Systems</td>
<td></td>
<td>Univ of Reading</td>
</tr>
</tbody>
</table>
Presentation of the SAFEE Programme

Started on February 1st, 2004
duration: 4 years

Budget: 36 M€
EC grant: 19,45 M€
The last defence against hostile actions

1 Intelligence & International cooperation
2 Airport periphery
3 Terminals
4 Aircraft parking lots
5 Aircraft in flight
Scope of SAFEE

Three origins of Threats

Crew & Passenger attacks

Outside Threats
« Currently Manpads
Out of SAFEE for the
Time being »

Cargo Hold Threats
Reminder: Broad Project Design

SUB-PROJECT 1: “ON-BOARD THREAT DETECTION SYSTEM”
Detection of abnormal events
Generation of Alert

SUB-PROJECT 2: “THREAT ASSESSMENT AND RESPONSE MANAGEMENT SYSTEM”
Consolidation and fusion of threat signals
Proposition of courses of actions

SUB-PROJECT 3: “FLIGHT PROTECTION against hostile attempts”

SUB-PROJECT 4: “DATA”, deals with this complete process for data only

SUB-PROJECT 5:
Legal and Regulatory issues
Threat Analysis
Operational Concept Description
Validation strategy, design, and evaluation
Training of end-users
Economic analysis
Technology Watch
Management of Users Club

SECURITY EVALUATION

AIRBUS DE « OTDS »
BAE Systems « TARMS »
SAGEM
THALES Avionics
EAS: Emergency Avoidance System
FRF Flight Reconfiguration Function

ICAS Programme Committee (Workshop Oct 4th, 2005)
Scope of SAFEE SP’s

- **Cyber/Hijack Attack**
  - SP4: Securing Data
  - Radar Tracking
  - Cargo
  - SP1: Threat Detection
  - SP3: Flight Reconfiguration
  - Trajectory

- **Hijack on Board**
  - Airground Datalink & Voice
  - SP2: TARMS
  - AOC
  - Ground Datalink

- **ATM environment**
  - SP1: Threat Detection
  - Cargo
  - SP3: Flight Reconfiguration
  - Trajectory
SP1

Onboard Threat Detection System (OTDS)
Leader: AIRBUS HAMBURG
SAFEE SP1 Objectives

Detection of threats coming from
- Persons (passengers, crew, personnel) or
- Dangerous goods and materials

by
- Access control for persons, luggage and cargo,
- Detection of suspicious behaviour

Once
- Access control for persons
- Cargo and luggage registration
- Dangerous goods and materials detection

Warning/Alert

Continuously
- Detection of unauthorised action
- Detection of suspicious behaviour

Warning/Alert

Access to sensitive area

Leaving sensitive area
Scope of SAFEE SP1: Onboard Threat Detection System (OTDS)

Cabin Area
- Detection of suspicious behaviour

Cockpit Access Area
- Access control for persons (in SP4 validation)
- Detection of dangerous goods and materials

Cargo Area
- Detection of dangerous goods and materials
- Cargo and luggage registration

Aircraft Entrance Area
- Access control for persons
- Detection of dangerous goods and materials

To be prototyped
To be specified only
OTDS Schematics

Electronic Pass Readers
Video System Entrance Area
Goods and Material Detectors
Electronic Tag Readers
Goods and Material Detectors
Video System Cockpit Door
Crew Data Base
Video System Cabin
Audio System Cabin

Person Registration
Cabin Access Control
Cargo Registration
Dangerous Goods Detection
Cockpit Access Control
Behaviour Detection

Threat Detection
by
Data Evaluation
and Correlation

Alerts:
Unauthorized Access,
Weapon, Attack,
Unruly Passenger,
etc.
SP2 - TARMS

Threat Assessment and Response Management System
Leader: BAE Systems (Bristol)
What is TARMS?

- **Threat Assessment and Response Management System**

- Decision-support tool to enable end-users to:
  
  1) Assess threat levels
  
  2) Choose appropriate responses
What does TARMS Do?

Step 1: Assimilates all information available to decision makers

Background & Context Information
- Intelligence from security agencies
- Information from Pre-Board checks
- Databases of current Terrorists/Criminals and Unruly Pax
- Knowledge bases of current terrorist activity
- Prior Knowledge, about the Flight
  - Destination
  - Passengers
  - Luggage/Cargo
  - The Prevailing Security Situation
  - etc

Ground Based Agencies
  e.g. ATC/ AOC

OTDS
Sensor System

‘Live’ (Real time) Data
Detected Alerts derived from SP1(on-a/c sensors)
What does TARMS Do?

Step 2: Analyses information using models based on expert knowledge

Fuses ‘live’ data from various sensors with background and context information.

Uses a threat model based on expert knowledge to place ‘live’ data in context of background information.

TARMS

Ground Based Agencies e.g. ATC/ AOC

Background and Context Information

OTDS

Sensor System

Live Alert (Real Time) Sensor Data

Threat Assessment

Expert Knowledge Model

Threats

Makes judgements about the current threat levels.
What does TARMS Do?

Step 3: Analyses Possible Courses of Action

- Ground Based Agencies e.g. ATC/ AOC

Background and Context Information

TARMS

- OTDS
  - Sensor System
  - Live Alert (Real Time) Sensor Data

- Expert Knowledge Model
  - Threat Assessment
  - Response Management

Courses of action are also based on expert knowledge

Response Management Process determines best courses of action based on type & level of threat and current situation

---

SAFEE Consortium
SAGEM DS/ Daniel GAULTIER

ICAS Programme Committee (Workshop Oct 4th, 2005)
What does TARMS Do?

Step 4: Presents information & advice to the decision-maker

- Alerts the decision-maker to the candidate threats
- Presents evidence to support the threat assessment

**TARMS**

- Threat Assessment
- Response Management

**OTDS**

- Sensor System
- Live Alert (Real Time) Sensor Data

**Background and Context Information**

- Ground Based Agencies e.g. ATC/ AOC

**ACTORS**

- Pilot
- Security Staff
- Cabin Crew

**USERS**

- Pilot
- EAS

**Threats**

- Provides decision-maker with the option to re-examine data or request more data
- Presents proposed courses of action associated with each threat
TARMS ‘Knowledge Models’

- **Ground Based Agencies**
  - e.g. ATC/ AOC

- **Background and Context Information**

**TARMS**

- **OTDS Sensor System**
  - Processed Sensor Data

- **Threat Assessment**
  - Expert Knowledge Model

- **Response Management**
  - Expert Knowledge Model

**Cabin Anti-Threat Manoeuvres**

**USERS**
- Pilot
- Security Staff
- Cabin Crew

**ACTORS**
- Pilot
- EAS

**Flight Anti-Threat Manoeuvres**
SP3 – FRF/EAS

Leader THALES Avionics
Proposed response:
After original pilot is inoperative, the Flight Reconfiguration Function (FRF) takes over the A/C flight controls
Emergency Collision Avoidance System (EAS) Description

- Flight controlled by the pilot
- Collision detection Alert
- Automatic avoidance
The ultimate step: Flight Reconfiguration Function

- Extension of EAS concept

- Long term, advanced research study
SP4 DATA

Leader: SAGEM Défense Sécurité
SP4 Objectives

- To protect communications and data that are daily used for exploitation of aircraft in an hostile environment

- SP4 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.
Security layers

Certified Avionics
Avionics Security node
AF Network
AF Network Security node
AL Network
AL Network Security node
Open Network
Open Network Security node
outside aircraft

OPEN WORLD
SP5 Security Evaluation

Leader: NLR
SP5 Objectives

- To identify and analyse legal and regulatory issues relevant for the introduction of the new SAFEE systems
- To analyse and evaluate the security of flight operations (with and without the SAFEE systems) through a threat assessment
- To develop a validation strategy and experiment design plan, and to evaluate the overall SAFEE system validation results
- To provide training to the potential end-users of the SAFEE systems, using a validated real-time flight simulation environment
- To perform an economic analysis of the SAFEE systems and measures
- To study international security improvements, and to evaluate their potential to support the further improvement of the SAFEE systems
Legal and regulatory issues

- Review, analysis and evaluation of relevant existing aviation legal and regulatory requirements and (both international & national documents):
  - ICAO Documents
  - EU Documents
  - ECAC Documents
  - ACARE Document
  - EASA (JAA) Documents
  - FAA Documents
  - IATA Documents
  - EU state members’ documents
Who is responsible?
Legal and regulatory issues

<table>
<thead>
<tr>
<th>Aircraft</th>
<th>Parking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boarding</td>
<td>Taxi Out</td>
</tr>
<tr>
<td>People</td>
<td>Check In</td>
</tr>
<tr>
<td>Airport</td>
<td>Airline</td>
</tr>
</tbody>
</table>
Responsibilities and liabilities

- The novelty of SAFEE creates new perspective of pilot in command authority.
- The current basic rule is that the pilot in command has the ultimate authority regarding the operation of the aircraft.

- However, SAFEE EAS creates for the first time a situation when the aircraft is not controlled by the pilot in command.
  - Who is responsible then?
  - Is there a need for re-evaluation of the pilot in command’s legal status?

- Post 9/11 two developments occurred on board: (1) increased enforcement of locked cockpit doors and (2) much wider deployment of Sky Marshals.
- Therefore, is the pilot in command responsible/liable for the combat activity of the sky marshal or a new envisaged “flight security officer”? 
Human Rights Issues

- SAFEE operational concept requires information processing of passengers, crew members, airline and airport employees, by:

  - Monitoring – on board cameras and sensors
  - Recording of information (pre flight and during the flight)
  - Gathering Intelligence information
  - Use of “black list” of suspected passengers and industry employees
  - Information collected during ground passengers screening
  - Pre flight data collection (PNR) and passengers profiling
Human Rights Issues

- However, these elements most probably will entail a departure from what is universally considered as "privacy".

- The EC has already recognized this problem in Reg. (EC) 2320/2002, dealing with civil aviation security – stating that the fundamental rights of the EU Charter have to be respected. This regulation also emphasises the principals of proportionality.

- Possible direction for legal solution is shown in the 2004 agreement between the EU and the USA authorizing EU airlines to transmit Passenger Name Records (PNR) to the US Department of Homeland Security. The agreement stresses that the necessary balance has to be maintained between security concerns and privacy concerns.
Direction for Possible Solutions

The primary objective of International civil aviation security is - to assure protection and safety of the passengers and crew. An inherent dilemma: How to assure maximum security with minimum breach of human rights

- This dilemma between security & human rights will continue to exist, i.e.:
  - The world community will have to accept that when one enters the aircraft some rights will have to be sacrificed to secure civil aviation
  - This not a too expensive price - when we consider what is at stake
SAFEE Impact on Regulatory Bodies

- At Airlines level
  - improvement of current security manuals

- At National level (for instance in France)
  - improvement of current regulations: new amendments in Security Programme for each international airport (different controls at the SC/P)
  - introduction of new regulations: renewal of the CNIL regulations

- At European level
  - direct impact (improvement?) of Doc. 30 Part II of ECAC

- At World level
  - improvement of Annex 17 of ICAO
Threat Assessment Methodology

**Preparation**
- Define scope of study
- Choose study approach
- Describe flight operation
- Describe security environment

**Identification**
- Identify threats
- Identify vulnerabilities
- Define security occurrences
- Define threat scenarios

**Conclusion**
- Report on risk assessment
- Propose countermeasures

**Analysis**
- Categorise impact
- Categorise potentiality
- Determine risk level
- Identify security bottlenecks
How to validate?
(flight simulators; also for training)

Involvement of end-users!
NLR GRACE Simulator
AFT Station
Who is expected to finance?
Costs and benefits of security measures

Heads of cost
1. Aircraft physical damage
2. Possible loss of resale value
3. Aircraft loss of use
4. Passenger/crew death/injury
5. Loss of cargo, baggage
6. Third party damage
7. Airline costs of delay
8. Suspension of activities
9. Passenger delay
10. Airport closure
11. Airspace closure
12. Site contamination & clearance
13. Search & rescue
14. Airline immediate response
15. Cost of investigation
16. Cost of insurance
17. Loss of reputation & income
18. Loss of company value
19. Wider economic damage

Airline (industry)

Other actors in society
Who will support design of SAFEE systems?

Managing the end-users club

SAFEE PRES_ICAS_051004_V4

Plan for SAFEE User Club

The User Club is being created at the outset of the project. This is because we would like to schedule a meeting early in the lifetime of the project to gather information from individuals like yourself on the issues to be examined. The User Club will be jointly run by BAE SYSTEMS in the UK and the Netherlands National Aerospace Laboratory NLR.

The User Club has the following objectives:

- Annual meetings for communication of SAFEE project results
- Emphasis on broader communication — you will be relevant to the project
- Direct communication of SAFEE results to those unable to attend the meetings

Contact Details

If you would like to become a member of the User Club, please enter your contact details in the space provided below. The first meeting is planned for early 2004 and we will issue invitations and further details of this event in the near future.

Please complete the following details:

Name
Company
Address
Telephone
Email

Please return the completed form to the SAFEE project member who sent you this invitation, or to safety-userclub@baesystems.com.

The success of the SAFEE User Club relies on the assistance of individuals such as yourself. We would encourage you to purchase and we would welcome your contribution. Please remember, there is no commitment whatsoever at this, or any other stage.

Security

Due to the sensitive nature of this project and the associated information, which may be generated through the SAFEE User Club, please read and note that the User Club of the project will be by invitation only and by approval of the SAFEE Project team.

Please note that any personal details you provide will be held in confidence and not passed onto any other parties who are not directly involved with the SAFEE project.

Affiliate User Club Meeting, l’Aéro-Club de France, Paris, June 7&8th, 2004

Plenary User Club Meeting, NLR, Amsterdam, November 25&26th, 2004

Plenary User Club Meeting, Musée Air & Espace Le Bourget, June 14th 2005
If you are dealing with this « security approach » you can join SAFEE User Club

So feel free to contact SAFEE Coordinator (daniel.gaultier@sagem-ds.com)

Next meetings
- Plenary meeting in May 2006
- Affiliate meeting in November 2006
Collaboration
SAFEE / ERRIDS

European Regional Renegade Information Dissemination System (ERRIDS)
SAFEE-ERRIDS NEXT STEP

SAFEE
Cockpit and Cabin protection
Airborne security applications

ERRIDS
Core Network

AOC
ATC N
ATC N

Mil ATC
Air Def N

NGA

Pol N
Airport

Intel N
Europol

Existing Links e.g. ACARS/SATCOM

Air-ground encryption key management

Integrated Intelligence Analysis

COSEC
Secure A-G communications
ADS Surveillance

Integrated Incident Management

Overall secure network management

ATC N

Mil ATC

Air DEF N

NGA

Pol N
Airport

Intel N
Europol

Existing Links e.g. ACARS/SATCOM

Air-ground encryption key management

Integrated Intelligence Analysis

COSEC
Secure A-G communications
ADS Surveillance

Integrated Incident Management

Overall secure network management

SAFEE Consortium
SAGEM DS/ Daniel GAULTIER

ICAS Programme Committee (Workshop Oct 4th, 2005)
Thanks for your attention and your foreseen comments
Welcome on board
Line up
Set « Trust »
And Take off