SAFE AUTOMATIC FLIGHT BACK AND LANDING OF AIRCRAFT (SOFIA)

Juan-Alberto Herrería, Jorge Bueno, Marcial Valmorisco
ISDEFE - Ingeniería de Sistemas para la Defensa de España

Keywords: *On-board Security, Flight Reconfiguration*

Abstract

SOFIA project is a response to the challenge of developing techniques enabling the safe and automatic return of an airplane to ground in the event of hostile actions. Activities in this sense was started in the framework of the SAFEE project, being SOFIA proposed as the continuation of the SAFEE works on Flight Reconfiguration Function (FRF). The FRF system takes the control of the aircraft and manages to safely return it to ground under a security emergency (e.g. hijacking), disabling the control and command of the aircraft from the cockpit. These mean to create and execute a new flight plan towards a secure airport and landing the aircraft at it. The flight plan can be generated in ground or in a military airplane and transmitted to the aircraft, or created autonomously at the own FRF system. SOFIA designs architectures for integrating the FRF system into several typologies of avionics for civil transport aircraft; develops one of this architectures; and finally validates, following the European Operational Concept Validation Methodology (E-OCVM), the FRF concept and the means to integrate it in the current Air Traffic Management (ATM) system.

1 Background

Europe is already researching in this area, taking benefit from the 6th Framework Programme sponsored by the European Commission (EC) [1]. Within such initiative several projects, participated by key European companies in the sector, are currently investigating in the FRF arena, e.g., the SAFEE and the SOFIA projects. These projects are the response to the EC concerns regarding the aviation security. Such concerns are derived from the results achieved by the Advisory Council for Aeronautics Research in Europe (ACARE) group. These results conforms the VISION 2020 and are presented in the ACARE Strategic Research Agenda (SRA2) [2]. The SOFIA outcomes rely in the SAFEE project results. Meanwhile the SAFEE project provides the aircraft with the capacity to detect the on-board hostile action and perform a diversion to take the aircraft up to a secure area, the SOFIA project controls the aircraft autonomously and lands it on a secure destination [3].

Furthermore, SAFEE has performed an initial design of the FRF function, which will be the basis for its development on the SOFIA project. Hence, as FRF is a system envisioned in the framework of the SAFEE project, SOFIA will develop FRF making it compatible with the SAFEE concept and systems carried out on it.

The FRF developed in the SOFIA project is the response from several leading European companies - Isdefe (coordinator), Deutsche Flugsicherung (DFS), GALILEO Avionica, Skysoft, Alenia SIA, THALES Avionics, Instytut Lotnictwa (IoA), Rheinmetall Defence Electronics (RDE) and Diamond Aircraft Industries - to the demand from the society of improving the security of the aircraft operation. And the improvement is gotten in an autonomous way, as requested in the ACARE SRA2 [2]. Furthermore, SOFIA project analyses the integration into the airspace of such airplane flown by the FRF and the requirements imposed to the ATC system, and assess the implications of this new development in the regulatory and certification frameworks.

2 Development Proposal

The main objective of the SOFIA project [3] is the validation of the Flight Reconfiguration Function system and the assessment of its integration into the airspace. SOFIA is mainly a technological project, but it also considers the operational and regulatory aspects are relevant enough. SOFIA dedicates an important effort in assessing the operational and regulatory issues related with the integration of the FRF system into the airspace. The operational assessment approach is not only a theoretical study but also practical since the validation exercises consider the interaction of FRF with the airspace.

Taking the fact of the clear symbiosis between the FRF system and the Unmanned Aerial Systems (UAS), SOFIA considers the UAS development and progresses as a constant reference in the project. This reference is not only present in the operational aspects, but also in the technological ones that enables the integration of the UAS into the airspace. For a few years, works are focused at the way to introduce UAS in non-segregated airspace, and in particular on the “sense and avoid” concept, that will allow to detect any other aircraft, to define and then to fly the appropriate trajectory permitting the collision avoidance.

SOFIA follows a stepwise approach in its development, formed by four main interrelated steps, facilitating a clear continuation of the activities. The four steps defined in SOFIA are:

1. Assessment on the issues related with the operation of the FRF.
2. Design of the FRF system: functions, databases, components, interfaces…
3. Development of the FRF system for enabling the validation exercises.
4. Validation of the FRF system and its integration into the airspace.

2.1 STEP 1: Assessment of the operational issues

The main goal of this step is to define the future FRF environment, and thus prospects forthcoming avionics architectures considering in particular what can be expected for the features relevant to FRF, which are around Flight Control and Management and air-ground communication. Furthermore, the task studies the ATM environment that can be expected for the timeframe for the FRF implementation (initially 2025), in order to define, together with the modalities of the FRF, the integration into that environment and the procedures required for the management of FRF-controlled aircraft flying autonomously in the airspace. The task also assesses the avionics architectures where the FRF system will have to be integrated. This activity is quiet interesting for the project because the determined environment for the FRF deployment is the reference for the whole project in two key aspects: FRF functions and validation exercises.

Once the FRF environment is defined, the challenge of integrating the aircraft equipped with the FRF system into the airspace is afford. In the current situation, the aircraft are controlled by the pilot who interacts with the air traffic controller (ATCO). The ATCO can command the pilot to execute maneuvers (increase speed, change flight level, direct to a new waypoint…) that the pilot is in charge of executing. But when due to threats on-board the FRF becomes in control of the aircraft, the data link remains as the only possibility to communicate the controller with the FRF, by sending flight plans that the FRF will execute. But even this possibility can be disrupted. Then, the ATCO gets an aircraft flying its own flight plan, without any possibility of being commanded from the ground systems. In both events, new procedures are needed to guide the ATCO behavior. Such new procedures are proposed by the SOFIA project. SOFIA also introduces the need of a Ground Security Decision Station (GSDS) to manage these security events.

A special focus is given on the regulatory and certification issues to which FRF integration gives rise. At this point, the reference to the UAS progress reveals crucial, and thus it is used as a main source to propose the appropriate regulatory and certification framework for the FRF and the new procedures designed for its implementation. With respect to other projects dealing with future ATM environment and tackling the problem of integrating autonomously flying aircraft, the distinctive feature of SOFIA is to take account of the security-related circumstances under which the autonomous flights occur. In this scenario, two questions will be possessed when facing the FRF and the new ATC procedures to the regulatory and certification frameworks: How do the FRF and the procedures meet the frameworks? How could the frameworks be modified to enable the Flight Reconfiguration and the new ATC procedures operate by keeping the safety levels?

2.2 STEP 2: Design of the FRF System

Its main goal is to specify both the FRF system and its integration into the different avionics architectures that can be expected for the future, considering the three operations modes envisioned for the FRF:

- Flight Plan with Negotiation (FRF_N): the FRF executes a flight plan generated on ground and transmitted to the FRF via data link. FRF analyses the feasibility of the flight plan according to the aircraft conditions and performances. In case of agreement, the flight plan is executed. Otherwise, next mode is on.
- Flight Plan without Negotiation (FRF_WN): after negotiation is finished without agreement or communication disruption, FRF executes the flight plan elaborated by itself, without any control from ground.
- Military aircraft relay: this is an intermediate step between the two previous solutions. FRF receives a flight plan from a military aircraft and operates as in the FRF_N solution.

As most of the FRF implied automation modes are expected to be already present in future aircraft, SOFIA more specifically addresses the solutions allowing this automation and the associated mode transitions to be performed autonomously with no possibility for a malevolent onboard to intervene. This will lead SOFIA to focus especially on FRF interfaces to existing systems and HMI devices, and to perform specific in depth safety analyses to define an architecture that fits all of the needs and constraints. SOFIA in particular studies the autonomous flight re-planning function with the associated monitoring function, and the interfaces to available onboard surveillance systems which provides the means to detect various threats (equipment failure, terrain, traffic or weather hazard) and to autonomously make decisions about flight plan update. Especially for the detection of traffic threats, SOFIA will analyse and consider the most promising civil and military solutions under study in the UAS arena. It is remarkable the iterative process that will be run between the design activity and the regulatory, certification and safety assessments.

As part of FRF design, SOFIA includes thus a study focused on data bases with the aim of identifying FRF-related requirements and specifying, with respect to the databases foreseen for future aircraft, the modifications and new data fields that are required to fit FRF needs and the set of databases that enables the calculations to be performed by FRF:

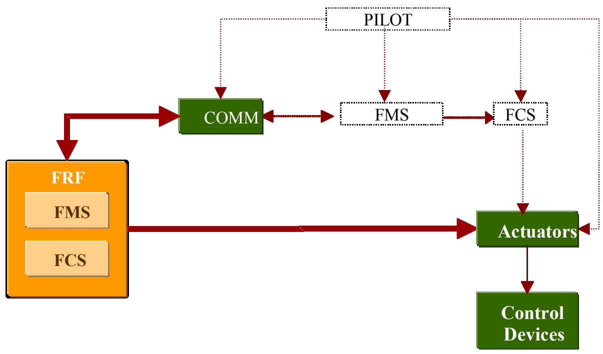

Fig. 1: FRF overall architecture

Also worthy of note is the innovation brought about by SOFIA at the ground side regarding the ATM procedures and tools, for which the impact of FRF related procedures and functions will be assessed. During the FRF design, a safety assessment is carried out. The main goal of this activity is to propose design requirements derived from the analysis of the preliminary design and the FRF integration into the airspace. Both safety assessments comprise the performance of a Functional Hazard Assessment (FHA) and a Preliminary System Safety Assessment (PSSA). EUROCONTROL EATMP SAM and SAE ARP 4761 are applied.

2.3 STEP 3: Development of the FRF System

Its main goal is to develop the FRF functions for their validation and set up the simulation environments that allow FRF functional validation to be performed according to the objectives and requirements set out in the SOFIA validation plan. The task includes the adaptation of already available platforms components and the development of appropriate new mock-ups components in order to get functional test beds ready for the carrying out of the FRF validation. Only the solutions FRF with Negotiation (FRF_N) and the FRF without Negotiation (FRF_WN) will be carried out.

Five validation platforms are used in the SOFIA project:

- ATENA, flight simulator developed by GALILEO Avionica.
- AIRLAB™ flight simulator developed by THALES Avionics.
- DFS ATC simulator.
- IoA´s I-23 Manager aircraft.
- Diamond Aircraft Industry Twin Star DA42 aircraft.

2.4 STEP 4: Validation of the FRF System and its integration into the Airspace

Its main goal is to perform the validation experiments envisaged for the SOFIA project to assess, first whether the design of the FRF system is capable of supporting the functionality required and second, the operation of FRF system integrated in the ATC procedures as proposed by SOFIA. The validation exercises follow a validation plan elaborated according to the E-OCVM.

The validation of FRF will be only made on the solutions FRF with Negotiation (FRF_N) and the FRF without Negotiation (FRF_WN). To carry out the validation, five experiments are proposed for SOFIA according to a stepwise strategy to feed back the development phase with validation results from a first set of validation exercises to refine the design and development of he FRF:

- A preliminary validation of the FRF functions will be carried out during the development phase. The ATENA simulator is linked to the DFS ATC simulator. This experiment is focused at refining the FRF functions, particularly the assessment of the FRF functions and its integration into the airspace. The options Flight re-planning with negotiation and Flight re-planning without negotiation modes will be assessed.
- A flight trial is executed during the development phase to refine the development process by using an aircraft provided by the IoA. This trial is focused at the assessment of the Flight re-planning without negotiation mode.
- A validation exercise is run in the THA AIRLAB™ simulator to assess the feasibility of the FRF solution for the commercial aircraft world.
- A flight trial by using an aircraft provided by DAI. This trial will be focused at the assessment of the Flight re-planning with negotiation mode thanks to the linkage to the DFS ATC facility.
- The SOFIA validation cycle is presented in the Figure 2. Such figure shows the linkages among the validation exercises, how they are used to refine the FRF versions developed in the project, and what validation platforms are used in each exercise.

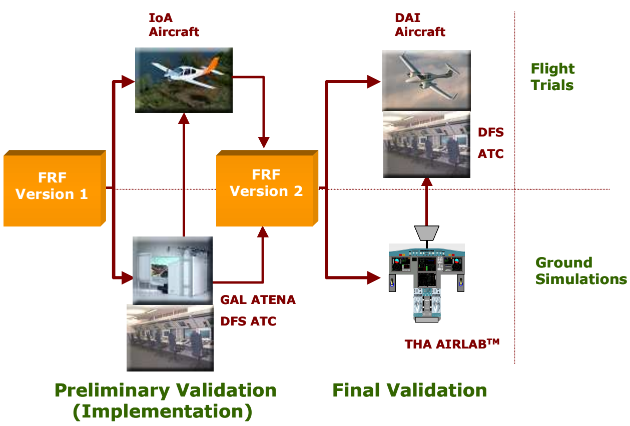

Fig. 2: SOFIA validation cycle

The validation objectives are those related to the demonstration of the FRF concept reliability in realistic environments: Issues relative to the appropriateness and feasibility of the FRF operational modes, evaluation of the impact on the ground segment (ATCO work load, flight plan creation on ground), cross checking and execution of the flight plan and landing of the aircraft by FRF that are to be assessed in SOFIA. The next list addresses a detailed relation of validation objectives to be achieved in SOFIA.

- Validation of the impact of the FRF system on ground:
  - Assessment of the reliability of the new ATC procedures and management in a FRF scenario.
  - Assessment on the reaction of the ATCO when FRF is activated and workload ATCO upon the different FRF operational modes.
- Validation of the FRF system on-board:
  - Creation of the flight plan by FRF on air.
  - Crosschecking by FRF of the flight plan received from ground.
  - Execution of the flight plan and landing of the aircraft by FRF.

3 SOFIA Current Status of Development

3.1 FRF Environment

In an emergency situation (e.g. a security crisis on-board as it is the case in SOFIA) the highest priority is to land the aircraft as quickly as possible. Therefore the flight to the selected aerodrome shall be as short as possible. The aircraft shall normally fly directly to the aerodrome. This part of the FRF flight will be the same for all the three FRF solutions introduced in the following paragraphs.

Solution 1: Autonomous Flight Re-planning

For the FRF, it is very easy to create a new flight plan to a special emergency aerodrome, because all necessary information is available on board. The information about the crisis on board, the status of the aircraft and databases about the airspace are part of the safety and security systems. Information about the conditions at the selected aerodrome could be available, e.g. via ATIS. En-route weather information could also be received via data link or on board weather radar. As all information is available a route to the airport can be calculated quickly. FRF can down link the route to the GSDS, so ATC can keep the surrounding controlled traffic away. GSDS can also inform the selected airport and security authorities. In case of data link problems the FRF aircraft flies to the aerodrome without information to/from GSDS. ATC monitors the flight and using predicting techniques (ATC tools) ATC can anticipate the possible aerodrome selected by the FRF system. Thus ATC can also inform that aerodrome and the authorities. This procedure is similar to today procedure for an aircraft with r/t failure. Therefore this solution is easy to work, clearly structured and the time to prepare is relatively short. This is the preferred solution for the controllers according to the outcomes from the workshop hold with them at the DFS.

Solution 2: Flight Re-planning with Negotiation

Due to the negotiation between the FRF system and the GSDS, the preparation phase in solution 2 is more time consuming. For the negotiation, data must be exchanged via data link. Depending on the technical equipment this data exchange may take longer. Additionally, during the negotiation phase two decisions must be taken. At first GSDS has to decide about the destination aerodrome (and the alternative); and secondly, the FRF system has to decide about the FPLN proposed by GSDS. Both decisions need extra time to compute. If the negotiation fails, the FRF uses the flight plan calculated by itself, reverting to Solution 1.

This information will be down linked to the GSDS through a secure data link. Regarding the premises made above, the aircraft will consume more time for the preparation phase than in Solution 1. Due to the decisions foreseen in the procedures, the structure of this solution is more complex. For the controllers this procedure is not as easy to work as Solution 1.

Solution 3: Mil. A/C Relay

Regarding the amount of time required and the complexity of the procedures, Solution 3 is the least preferred solution. Intercepting the FRF aircraft requires time. A specially equipped military aircraft must be informed and flown to intercept it. Then the military aircraft has to connect to the FRF aircraft and receive the status information. Based on this information the GSDS must calculate a new route to the emergency aerodrome. This information is to be transmitted via the military aircraft to the FRF flight. Then the FRF aircraft can start the flight plan. If the connection between the military aircraft and the FRF flight or the connection between the military aircraft and GSDS fails, the FRF system creates a flight plan and follows it to the emergency aerodrome. The interception of the FRF aircraft is time consuming and also the transmission of the data to GSDS via the military aircraft and back to the FRF aircraft is time consuming. Due to the integration of a third party (military aircraft) in the negotiation process the complexity of this solution is higher than in the other solutions.

Discussion on the solutions

Initially a combination between the three solutions was envisaged. The proposed stepwise approach started with solution 2, then solution 3 and, as a last back up, solution 1. This approach is very time consuming, very complex and not easy to work for all participating parties, particularly the Air Traffic Controllers (ATCo). Therefore in SOFIA a clear structured solution is preferred. This preferred solution could either be solution 1, solution 2, or solution 3. In solution 2 and solution 3 elements of solution 1 are integrated as back up procedures if failures occur during the normal procedure. So a combination of solution 2 and 1 or solution 3 and 1 is foreseen, not as a stepwise approach but as one solution. However the preferred solution according to the ATCo inputs is solution 1.

3.2 Certification and Regulation

SOFIA project has analysed the impact of the Flight Reconfiguration Function (FRF) in the certification and regulatory frameworks. SOFIA has kept several meetings with ICAO, EASA and EUROCONTROL.

The major demand regarding certification activities was detected on the air segment. Although the philosophy underlying the design of the FRF system shall pursue compliance with current regulatory framework, since the FRF system is a particularly innovative one, the existence of conflicts or gaps in current regulations is inevitable, and some changes in those regulations will be required in order to make possible the certification of the FRF system. Most conflicts detected in the current certification framework analysed stem from being the pilot out of the loop when the aircraft is under command of the FRF system. In particular, the main associated issues are the fact that there is no pilot to 1) take over control of the aircraft when a critical system fails, and 2) to monitor malfunctions or emergencies on-board so that the pilot can react to them. Requirements have been derived and became a valuable input for the design of the FRF system from all the analysed codes for the air segment.

On the ATC segment the certification issues are not so problematic, as ATC does not influence directly the FRF flight, only the configuration of already existing certified ATC systems has to be changed. Also the interface to the GSDS is based on existing technology.

On the ground segment the GSDS is the only relevant system that has to be certified. The responsibilities for the certification of the GSDS either the certification process are not defined. As the GSDS has the ability to influence the FRF flight directly it has to be regarded as a combination of air and ground segments. For regulatory issues, the procedures have to be confirmed by ICAO. All developed procedures have to be integrated into the ATM. Therefore the ANSPs procedures and documentations have to be updated with the FRF ones.

With regard to the regulatory issues of the air segment, as in the case of the certification issues, the main conflict with regulations stem from being the pilot out of the loop when the aircraft is under command of the FRF, since current regulatory framework assume, explicit or implicitly, that a pilot is on board to follow the prescribed procedures. Another important issue leading to conflicts with regulations is the loss of communications with ground when the aircraft is under command of the FRF system, since in this situation GSDS is not informed on the aircraft status and evolution of the crisis on-board, and no vital information can be up-linked to the aircraft when necessary. In addition, other aspects considered in the analysis of regulatory issues are Training, Aircraft Maintenance and Security. Regarding training new programmes dealing with '*security avionic systems*' should be developed. Analogously, procedures for handling these special systems should be developed for Aircraft Maintenance Organizations, based on requirements to be included in the regulatory framework.

3.3 FRF Design

In order to enable the implementation of the FRF the airplane avionics must be fly-by-wire. The design of the FRF has resulted in a set of eight (8) functions and three (3) databases (DB). The functions perform the actions assigned to the FRF to command and control the flight, and communicate with GSDS during the FRF flight of the airplane in emergency. The DB provides the data needed to enable the FRF to perform the calculations for the flight reconfiguration.

The FRF functions are described hereafter:

The **Decision Centre Function (DCF)** shall manage the different FRF capabilities. It shall act like an event controller. It performs the FRF initialization (including built in test), modes management and systems interface management (including update of databases). The modes management deals with the four FRF modes: START, IDLE, ARMED and ACTIVE, described herebelow:

- START: power up of the system.
- IDLE: usual mode during the normal of operation of the airplane in absence of security emergencies or threats.
- ARMED: the FRF primary functionality is to calculate a new flight plan that flies the aircraft to a safe landing.
- ACTIVE: the FRF executes the flight plan calculated when in ARMED mode and prepares the aircraft for landing

The **Health Monitoring System Interface (HMS)** gathers data from systems critical to the operation of the FRF, and performs corrective actions in case of failure in order to ensure continuity of the FRF service. If a failure is critical enough not to be recoverable, the FRF will notify to ground (GSDS) with the condition that forced this disengagement. This will give the GSDS the opportunity to consider the best course of action for the given situation.

The **Route Planning and Static Flight Monitoring (RPL)** generates a suitable flight plan to a secure landing airfield. It takes into account the external airfield selection criteria and authorizations and the information coming from the FRF databases regarding commercial routes and airports, terrain, restricted area and military airports, static and dynamic Prohibited Security Areas and weather,

The **Guidance and Leg Management (GLM)** monitors the flight of the aircraft along the route continuously evaluating the displacements from the desired path and providing inputs to the autopilot for guidance. It also performs all the operations of leg change and connection.

The **Route Re-planning (RRP)** performs any type of amendment to the flying plan during its execution due to external constraints (e.g., traffic, weather…). Procedures similar to the **(RPL)** shall be applicable.

The **Dynamic Flight Monitoring (DFM)** consists of different subfunctions that shall be activated during the FRF flight of the airplane:

- **A/C Performance Monitoring**, in order to provide all the necessary information (fuel consumption, timing information etc.) to FRF to perform a check along the selected path,
- **Resolving of conflicts with static obstacles**, e.g. terrain and PSAs,
- **Resolving of conflicts with air traffic**, performing automatically the TCAS procedures,
- **Resolving of conflicts with bad weather condition**

The **External Communication (COM)** produces the information to be exchanged between FRF and the GSDS: FRF Mode, FMS acceptance/rejection of the GSDS flight plan, Selected airfield to land, Selected flight path, Modified Flight Path and Health Data.

The **Display Management (DSM)** provides the interface between FRF and Display Function. As a general philosophy, in order to respond to the terrorist attack on board, a solution that prevents hijackers to know the real state of the aircraft (engines, trajectory etc) is preferred, only displaying the FRF mode.

Several airplane systems are interfaced by the FRF. Hence, navigation and surveillance sources, guidance systems and control systems are interfaced by the FRF. TARMS and EAS are security systems developed in SAFEE project.

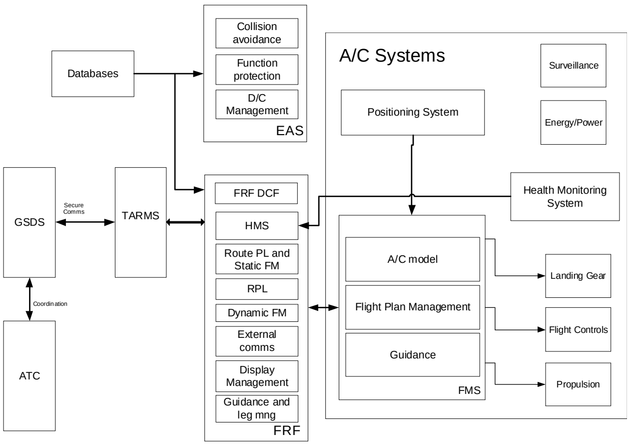

Fig. 3: FRF interfaces

The FRF databases are described hereafter.

The **Static and Dynamic Data Base** stores static data as terrain, obstacles, Prohibited for Security Areas (PSA), civil and military aerodromes and their characteristics to deal with threats, restricted areas, and dynamic data as FPLN and airport selected, weather data,etc.

The **Aircraft Performance Database,** needed to perform the guidance function.

The **Navigation Data Base**, with Jeppessen plus airliner specific data.

3.4 FRF Safety Assessment

Safety is a requirement "society" poses on the air transport. Although air travel is one of the safest forms of transportation, an increase in the number of accidents will not be accepted, not even in a context of growing traffic or emerging threats, such as for instance related to security. Hence the challenge to industry and regulatory agencies is to make an already safe system even safer.

The FRF provides a solution to a situation with a potentially catastrophic ending caused by the presence of a security threat. When a hijacking (or similar threat) occurs on-board an aircraft, the probability of losing the aircraft increases considerably, therefore any action taken to mitigate this possible end result will significantly improve safety. From this point of view, it might not be necessary to design a system to the same level of safety as it is required for current on-board aircraft systems, however the inadvertent activation of the FRF shall be strongly prevented.

The issue of making sure that the FRF is only activated when it should becomes then crucial. It can be demonstrated that the inadvertent activation of the FRF can be dealt with a moderate increase of workload by flight crews and will never have catastrophic consequences. Nevertheless, having a lot of spurious FRFs will not be acceptable by pilots or airlines and will not be sustainable by the ATS. Therefore requirements are necessary to keep this number small enough.

Since the expected number of FRF like scenarios is still to be better assessed, conservative estimates have been performed when imposing safety requirements on the FRF functionalities. Clear show stoppers have not been identified although equipment redundancy and additional design effort might be necessary to reach some of the targets.

While the FRF is in operation there are two main modes that have been assessed throughout this work. The following two paragraphs discuss the feasibility of the functionalities proposed in the different modes from a safety point of view.

In the ARMED mode, a number of failures in this functional area could endanger the success of the FRF mission, not only during the calculation of the first FLPN but also in the hypothetical case that the FRF has to recalculate the flight plan and choose a new destination due to unanticipated events (e.g. conflict with traffic, change of threat, weather, etc).

In the ACTIVE mode, safety requirements necessary to guarantee a safe landing without pilot-in-the-loop are also quite rigorous. This includes not only those functions associated to actions performed to configure the airplane for landing but also functions intended to resolve conflicts found on the way to the chosen destination (like traffic or weather).

The following paragraphs discuss the feasibility of the different scenarios from a safety point of view.

Scenario 2: Solution 1 with datalink where the FRF autonomously chooses a 4D route.

A large proportion of the safety requirements derived seem feasible for this scenario. Clear show stoppers (safety requirements that definitely cannot be identified) have not been identified. Nevertheless, a number of safety requirements may be very difficult or costly to achieve:

- Information regarding the state of the airport, its runways, its navigation equipment and suitability of weather conditions for landing are of critical importance for the '*blind*' landings to be performed by the FRFs. This poses challenging requirements on availability and quality of the information provided to the FRF at the holding as well as the information provided by ATIS when the FRF is approaching a certain airport and runway. In case of late information that the selected approach and landing can for whatever reason not be performed safely, the FRF has to re-plan a runway, airport, approach and possibly even a holding. This process has neither been defined nor assessed in the present work.
- A general issue is the selection of a set of suitable airports where FRFs should land. These airports on the one hand, should be quiet, such that procedures necessary for clearing approaches, runways and their neighbourhoods are feasible. On the other hand, the navigation equipment of these airports needs to be of very high quality and availability as safe landing of an FRF critically depends on it. Such equipment may be relatively costly for such airports.
- Another general issue is that when overflying cities, nuclear reactors or generally areas where one would not want to have security challenged flights such as FRFs is considered as a severe situation (severity class 2) in itself, this poses challenging requirements to onboard and ground databases regarding the corresponding information.

Scenario 3: Solution 2 where the destination airport is negotiated with ATC

The general situation is that the safety requirements for scenario 3 are equally or less difficult to achieve than for scenario 2. This is intuitively clear, as the selected airport and route have been assessed and confirmed by ATC in the negotiation process between FRF and ATC. Nevertheless, the difficult safety requirements for scenario 2 are generally still a challenge.

Scenario 1: Solution 1 without datalink, where the FRF autonomously chooses a 4D route

Scenario 1 generally seems very difficult to achieve in a manner satisfying safety objectives and requirements. A crucial point on top of the aforementioned requirements, which here are even more difficult to achieve, is that the FRF blindly chooses a destiny airport and approach and is then completely dependent on ATIS for information to confirm that the actual state of the runway, navigation equipments, weather, etcetera allow a safe landing. It seems very difficult to have ATIS contain all necessary information of sufficient quality in a sufficiently timely manner, also because the FRF does not inform about the airport and route it has selected. For the latter reason, these FRFs also pose a considerable challenge to ATC.

The work is not complete, even after the safety assessment has been defined and turned over to the system developers responsible for leading the implementation of the FRF. The implementation activities should be continuously monitored to ensure that action is being accomplished, any roadblocks to implementation are removed and the plan accommodates any newly identified gaps.

This safety enhancement process is best accomplished in a step-wise fashion to move to the next level of maturity. Once the initial action plan has been completed, the process should be repeated in order to identify the next safety enhancement actions to implement.

4 Summary and Conclusions

The FRF system is proposed as countermeasure to terrorist, hostile actions that aims to use the aircraft as a mean to affect asserts on ground. The affection can be implemented in different ways: crashing the aircraft, using it to propagate biological or chemical agents, or to multiply the effects of the explosion of a mass destruction weapon on-board the aircraft. As a response to this challenge, SOFIA project [3] develops the FRF system that enables the safe, automatic and autonomous return to ground of an airplane in the event of hostile actions. To carry out this action, the FRF disables the control and command of the aircraft from the cockpit, creates and executes a new flight plan towards a secure airport and lands the aircraft at it. Regarding the generation of the flight plan to be executed by the FRF, several options are considered in the SOFIA project: The flight plan can be generated in ground (ATC) or in a military airplane and transmitted to the aircraft, or created autonomously at the own FRF system. Additionally, the SOFIA project investigates the integration of such solution into different airspace environments: current ATM, ASAS/ADS-B, automation of ground functions, airspace with/without radar coverage, CDM, 4D trajectory negotiation. Finally, SOFIA project also analyses the impact of the regulatory and certification frameworks into the FRF system and vice-versa, first, to constrain the FRF design to such frameworks and second, to propose new procedures and standards to facilitate the technological development.

The FRF system developed in the SOFIA project proposes a solution to one of the biggest challenges of the future aviation: to make the aircraft more secure by themselves. But it also introduces some interesting questions that will have to be solved before these systems starts to operate, in order to guarantee the security introduced by them. Additionally to the technological development, SOFIA aims to provide answers to the following open questions:

- Who is responsible of the management and upgrading of the FRF database, including the PSA and airports?
- Who is responsible of uploading and upgrading the FRF database into the airplanes?
- Who is responsible of the designation of the airports capable of dealing with the foreseen threats? And furthermore,
- Who is responsible of designating to what airport an FRF aircraft is to be deviated?
- Who is responsible of the aircraft when it is flown by the FRF system: the airliner, the FRF manufacturer, the nation of the airliner, the nation of the airspace, the nation of the destination airport, EUROCONTROL, the EC, the EDA?
- What is the responsibility of the ATC system, and particularly of the ATCOs, when dealing with an FRF airplane?
- Who is responsible on ground of generating the new flight plan for the FRF aircraft?

References

[1] EC, FP6-2005-AERO-1 Aeronautics and Space Research Work Programme, 01-04-2005.

[2] ACARE, Strategic Research Agenda (SRA) Version 2, October 2004, 2001.

[3] SOFIA consortium, SOFIA Annex I Description of Work, 06/07/2006.

[4] SOFIA consortium, SOFIA D1.2 Definition of the FRF Procedures, 25/04/2007

[5] SOFIA consortium, SOFIA D1.3 Regulatory and Certification Issues, 19/11/2007

[6] SOFIA consortium, SOFIA D2.2.2 FRF Final System Safety Assessment (aircraft and airspace levels), 30/05/2008

[7] SOFIA consortium, SOFIA D.2.3 FRF Functions Design), 12/12/2007

Copyright Statement