This project has received funding from the European Union's Horizon 2020 Programme

RESEARCH PROJECT EASA.2020.C43

QUICK RECOVERY OF FLIGHT RECORDER DATA (wireless transmission)

Report D3

Technical investigation of the two selected solutions for wireless flight recorder data transmission

An Agency of the European Union

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Union Aviation Safety Agency (EASA). Neither the European Union nor EASA can be held responsible for them.

DELIVERABLE NUMBER AND TITLE:	QR-FRD D3 Technical investigation of the two selected solutions for wireless flight recorder data transmission
CONTRACT NUMBER:	EASA.2020.C43
CONTRACTOR / AUTHOR:	Collins Aerospace / Safran E&D / B. de Courville Consulting
IPR OWNER:	European Union Aviation Safety Agency
DISTRIBUTION:	Public

APPROVED BY:	MAIN AUTHORS	REVIEWERS	MANAGING DEPARTMENT
	Stéphane Lelièvre (Collins Aerospace) Eric Thomas (Collins Aerospace) Denis Delville (Safran E&D)		
		Emmanuel Isambert (EASA) Guillaume Aigoin (EASA)	

DATE: 28 August 2021

REPORT D3

Technical investigation of the two solutions for wireless flight recorder data transmission

Submitted to:

EASA

European Union Aviation Safety Agency

Cologne, Germany

Document Information	
Customer reference	EASA.2020.HVP.06
Project Title	Quick Recovery of Flight Recorder Data
Contract number	EASA.2020.C43
Consortium	Collins Aerospace / Safran E&D / B. de Courville Consulting
Task Number	03
Task Title	Technical investigation of the two solutions for wireless flight recorder data transmission
Deliverable Name	D3 - Technical investigation of the two solutions
Edition	01
Milestone Due Date	August 28, 2021
Dissemination Level	Public

Table of Contents

List of tables

List of figures

1 INTRODUCTION

1.1 QR-FRD Study Presentation

"*The overarching objective of the* Quick Recovery of Flight Recorder Data (QR-FRD) *study is to identify and assess technical solutions for the automatic wireless data transmission to quickly recover flight recorder data after an accident in a remote land area or an oceanic area for the purpose of faster understanding of the causal and contributory factors of an accident*" (EASA QR-FRD CFT,[Ref 18]).

The overall objectives of the project are to identify and to assess a series of candidate solutions for the wireless transmission of flight recorder data from commercial air transport aircraft in case of an accident (or a serious incident) in a remote land area or an oceanic area while considering thoroughly the challenges, constraints and limitations of each technical solution and the challenging conditions of an accident (or a serious incident). The evaluation of the candidate solutions will address the technical feasibility and maturity, the performance, the related constraints as well as the cost indicators in comparison to current flight data recorder installations.

The aircraft considered for the study are modern commercial air transport aircraft with a maximum take-off mass of over 27 tons, equipped with redundant combined flight data recorder (FDR) -cockpit voice recorder (CVR) capable of recording flight data, flight crew and flight deck audio, data link messages as well as, depending on the type certificate, flight crew – machine interface recordings (ICAO Annex 6 Part I, Section 6.3, [Ref 6]), and mandated to have a Flight Recorder Data Recovery (FRDR) means on-board.

A further investigation of the performance levels achievable will be carried out by developing several simulation exercises for two of the candidate solutions, applying representative operational conditions for aircraft accidents (and serious incidents) and aiming at analyzing the options for recovering the most useful data. In addition, the legal implications associated to the wireless transmission of flight recorder data, considering the existing data protection frameworks and the related ICAO Annex 13 provisions will be investigated.

The results of the feasibility project, together with the practical recommendations for the implementation of the candidate solutions, will be presented to a group of stakeholders involved in accident investigations and consolidated with the feedback received.

The activities undertaken within the QR-FRD study, and their respective documented outcomes are the following:

1. **Task 1 - Accident conditions relevant for wireless flight recorder data transmission:**
    - **Objective**: Identify and describe the technical and environmental factors which might affect the aircraft, its engines and its systems during the accident flight, and which need to be taken into account for maximizing the chances of successful wireless transmission of flight recorder data.
    - **Outcome**: A report (D1) of accident conditions which might affect the successful wireless transmission of flight recorder data (e.g. loss of power or equipment, excessive roll or pitch angles, in-flight fire, ditching …), and explaining the impact of such factors.
2. **Task 2 - Overview of technical solutions for automatic wireless transmission of flight recorder data:**
    - **Objective**: perform a screening of possible technical solutions for automatic wireless transmission of flight recorder data (flight data, audio and flight-crew interface recordings, data link messages…) in case of an accident (or serious incident) in a remote land area or an oceanic area.
    - **Outcome**: A solution overview report (D2) identifying the necessary technologies and capabilities of the communication infrastructure, as well as aspects not yet mature, and

discussing the potential effects of factors listed in D1 on the presented solutions. In addition, D2 will recommend the 2 most relevant technical solutions for further investigation to be performed under Task 3.

3. **Task 3 - Technical investigation of two technical solutions for automatic wireless transmission of flight recorder data:**
   - **Objective**: perform a technical investigation of the two most relevant technical solutions as identified in Task 2 and assess their performances for the automatic and wireless transmission of the data required to be recorded and retained by crash-protected flight recorders.
   - **Outcome**: A study report (D3) presenting technical solutions and detailing the two selected technical solutions (concept of operation, data transmission trigger logic (e.g. continuous or triggered), airborne functions and equipment, performance, communication infrastructure…).
4. **Task 4 – Assess challenges and limitations of two technical solutions:**
   - **Objective**: Assess the challenges and limitations of both technical solutions presented in Task 3 and comparison of their expected performance.
   - **Outcome**: An evaluation report (D4) of challenges and limitations addressing main technological enablers and their respective levels of maturity, reliability of main functions, impacts on flight crew procedures, ground handling and maintenance, as well as airline operations…
5. **Task 5 – First consultation of the stakeholder's group:**
   - **Objective**: Obtain the feedback of a group of stakeholders (accident investigation authorities, aviation regulators, operators of large commercial aircraft, associations of commercial pilots) on works performed under Tasks 1 to 4, with a view to incorporate this feedback into the analyses and assessments and to update the corresponding reports.
   - **Outcome**: A stakeholder feedback report (D5) containing the composition of the group of stakeholders, comments and questions raised by the stakeholders and replies as well as changes made to the different reports (D1 to D4).
6. **Task 6 – Simulation of technical solutions:**
   - **Objective**: Prepare an experimental set-up for the performance assessment of the two solutions investigated in Task 3, in particular for the comparison of the respective transmitted dataset (volume, accuracy, completeness, consistency) including reliability and robustness to factors identified in Task 1.
   - **Outcome**: A simulation report (D6) containing the detailed description of the performed simulations, as well as graphics showing the variation in performance when parameters (pitch and roll angles/rates, altitude, location of the aircraft…) are varied.
7. **Task 7 - Scenario-based study of legal aspects:**
   - **Objective**: Assess the legal aspects of data transmission over assets located on the territories of several countries or in space, in order to identify possible inconsistencies with ICAO Annex 13, legal uncertainties and risks for the protection of flight recorder data.
   - **Outcome**: A legal study report (D7) describing the legal framework applicable to the various assets of the communication infrastructure by which data will be transmitted or processed or recorded, scenarios of accidents in various places and with various setups, the potential issues for the protection and the transmission of data to the competent safety investigation authority, as well as proposals to ensure that the transmission service provider and the recipient of the flight recorder data are legally responsible for the preservation and the protection of transmitted flight recorder data.
8. **Task 8 – Second consultation of the stakeholder's group and additional simulation work:**

- **Objective**: Obtain the assessment of a group of stakeholders on the report resulting from Tasks 6 and 7, with a view to incorporate this feedback, to run where necessary complementary simulations and to update the simulation report.
- **Outcome**: A stakeholder feedback report (D8) containing the composition of the group of stakeholders, comments and questions raised by the stakeholders and replies as well as changes made to the different reports (D6 and D7), and possibly simulations and code.

9. **Task 9 – Conclusions and way forward:**
   - **Objective**: Conclude on the concept of automatic wireless transmission of flight recorder data in case of an accident and propose a way forward.
   - **Outcome**: A final report (D9) containing a general reflection on the works performed during the project, the feedback and recommendations received during the stakeholder meetings, the aspects of the concept of automatic wireless transmission of flight recorder data remaining to be explored or showing very challenging issues, a proposed approach for the development of compliance means and material in order to facilitate the performance demonstration to competent authorities, as well as practical recommendations to progress the maturity of this concept and prepare their implementation.

Figure 1 depicts the overall approach taken for the QR-FRD study and the relationship between the different deliverables.

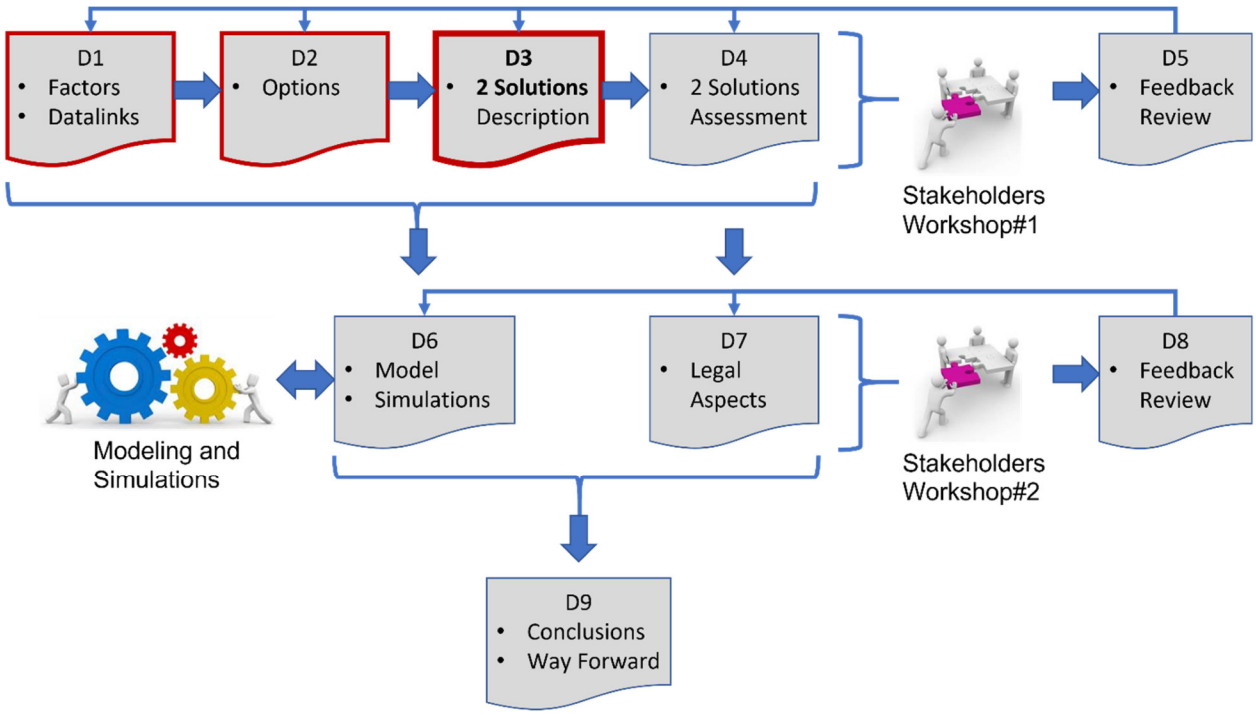

Figure 1: QR-FRD Study Approach and Deliverables Relationship

1.1 Scope of This Report

The present document corresponds to D3 as depicted Figure 1. It summarizes analysis and findings from Task 3 “Technical investigation of the 2 solutions” of the QR-FRD study.

It aims at:

1. describing two solutions for the wireless transmission of flight recorder data based on findings and conclusions from Task 2 “Overview of technical solutions for automatic wireless transmission of flight recorder data” and documented in D2 [Ref 2]
2. serving as inputs to activities undertaken within Task 4 (Assessment of the two solutions) and Task 6 (Modeling and Simulations) typically.

1.2 Organization of the Document

This document is part of Task 3 “Technical investigation of the 2 solutions” of the QR-FRD study, and is organized as follows:

Chapter 1, “INTRODUCTION”, (the present chapter), primarily provides background information on the initiation of QR-FRD studies and defines the scope of the present document.

Chapter 2, “REFERENCE DOCUMENTS”, provides the list of reference documents used for the drafting of the present document.

Chapter 3, “DEFINITIONS AND ACRONYMS”, provides definitions of terms and acronyms used in the present document

Chapter 4, “GENERIC SYSTEM OVERVIEW”, provides a description of a generic QR-FRD system in terms of functional architecture, and details its main functions and sub-functions, incl. compression, encryption and signature, as well as trigger logics. These descriptions cover both the airborne and ground-based segments.

Chapter 5, “SOLUTIONS PRESENTATION”, presents separately the two solutions in terms of hardware, functional specificities and concepts of operations.

“ANNEX A: FLIGHT DATA AND TRIGGER CONDITIONS USAGE” provides the list of parameters (flight data) per ED-112A and identifies their possible usage for the different trigger conditions discussed in Chapter 4.

“ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION” proposes formulas that could be used for the evaluation of trigger conditions.

“ANNEX C: FLIGHT WARNING SYSTEM” provides an overview of flight warning systems and alerts (cautions and warning) they cover.

“ANNEX D: ACCIDENTS CATEGORIES vs TRIGGER CONDITIONS ” cross references accident categories and related trigger conditions.

“ANNEX E: EU SAFETY OCCURENCES vs TRIGGER CONDITIONS” cross references incident reporting occurrences and related trigger conditions.

2 REFERENCE DOCUMENTS

[Ref 1] QR-FRD Study D1: “Accident conditions relevant for wireless flight recorder data transmission”, Ed 01, Aug 2021
[Ref 2] QR-FRD Study D2: “Overview of Technical Solutions for Automatic Wireless Transmission”, Ed 00, Nov 2021
[Ref 3] [R04] EUROCAE ED-112A, Minimum Operational Performance Specification for Crash Protected Airborne Recorder Systems, 2013
[Ref 4] [R05] EUROCAE ED-237, Minimum Aviation System Performance Specification for Criteria to Detect In-flight Aircraft Distress Events to Trigger Transmission of Flight Information, 2016
[Ref 5] [R03] ICAO Doc 10054-1, Manual on Location of Aircraft in Distress and Flight Recorder Data Recovery, 2019
[Ref 6] ICAO Annex 6 – Operation of Aircraft – Part I – International Commercial Air Transport – Aeroplanes, Ed. 11, July 2018
[Ref 7] ICAO Annex 11 – Air Traffic Services, Ed. 15, July 2018
[Ref 8] ICAO Annex 13 – Aircraft Accident and Incident Investigation, Ed. 12, July 2020
[Ref 9] EASA Certification Specification CS-25 – Large Aeroplanes, Jan. 2012, and amendments
[Ref 10] EASA Acceptable Means of Compliance (AMC) and Guidance Material (GM) Annex IV – Part CAT, Feb. 2016
[Ref 11] BEA, Technical Document, Triggered Transmission of Flight Data Working Group, March 2011
[Ref 12] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1018 - of 29 June 2015, “[…] occurrences in civil aviation to be mandatorily reported […]”
[Ref 13] ARINC-661, Cockpit Display System Interfaces To User Systems, Part 1 Avionics Interfaces, Basic Symbology, And Behavior, Sept. 2020
[Ref 14] ARINC-717-15, Flight Data Acquisition and Recording System, June 2011
[Ref 15] ARINC-767-1, Enhanced Airborne Flight Recorder, May 2009
[Ref 16] ARINC-841-3, Media Independent Aircraft Messaging (MIAM), Sept. 2016
[Ref 17] ISO/IEC 27040:2015 – Information technology – Security techniques – Storage security
[Ref 18] [R00] EN-EASA.2020.HPV.06, Quick Recovery of Flight Recorder Data Call for Tender

Other applicable documents:

EUROCONTROL, https://www.skybrary.aero/index.php/Emergency_or_Abnormal_Situation

3 DEFINITIONS AND ACRONYMS

Term	Definition
Abnormal Situation	A situation "*in which it is no longer possible to continue the flight using normal procedures but the safety of the aircraft or persons on board or on the ground is not in danger.*" (https://www.easa.europa.eu/sites/default/files/dfu/EASA_EHEST_HE_11.pdf) Could be assimilated to "*Alert phase: a situation wherein apprehension exists as to the safety of an aircraft and its occupants.*" as defined by ICAO Annex 12. However, this definition, along with the definition of "Distress phase" are from an air traffic controller perspective and are meant to manage search and rescue operations. The QR-FRD perspective, though maybe concurrent, is however different and aircraft oriented.
Aircraft	Equivalent to "*Aeroplane*" in the context of this study and defined as "*A power-driven heavier-than-air, deriving its lift in flight chiefly from aerodynamic reactions on surfaces which remain fixed under given conditions of flight*" (ICAO Annex 6, Part I) and "*of a maximum certificated take-off mass of over 27 000 kg and authorized to carry more than nineteen passengers*"
Chunk	Portion of a bulk of data, of a file, etc. to be processed (e.g. compressed and/or encrypted) and/or transmitted.
Distress Situation	"*A situation wherein there is a reasonable certainty that an aircraft and its occupants are threatened by grave and imminent danger and require immediate assistance*." (ICAO Annex 11, "Distress Phase") This situation usually triggers Search and Rescue operations.
Encryption	Process of encrypting (i.e. encoding) data with a cipher or ciphering methods. Cipher or the ciphering methods are the tools used to encode/decode the data. Encryption / decryption and ciphering / deciphering are often considered synonymous.
Flight recorder	"*Any type of recorder installed in the aircraft for the purpose of complementing accident/incident investigation.*" (ICAO Annex 6, Part I) Flight recorders addressed in the present document include: ● Flight data recorders ● Cockpit voice recorders ● Data link recorders ● Flight crew-machine interface recorders

Term	Definition
Flight recorder data	Any type of data recorded by the flight recorders that would be used for the purpose of complementing accident/incident investigation. Flight recorder data may include: ● Mandatory and optional flight parameters recorded by flight data recorders ● Audio recordings between the flight crew members and any other station ● Audio recordings of the acoustic environment of the cockpit ● Messages and information exchanged over data link ● Imagery from displays inside the cockpit and interactions of flight crew members with instruments and displays
Hash	Bit array of a fixed size (aka “hash value” or “digest”) resulting from a mathematical algorithm (cryptographic hash function). It is meant to be unique, as a fingerprint or a signature, for the set of data or message it results from, i.e. it is infeasible to find two different sets of data with the same hash value. A small change to the set of data will extensively change the hash value.
Historical flight recorder data	Flight recorder data that has been stored prior to the trigger condition for possible transmission.
Master caution	A caution alert typically provided by a Flight Warning Computer (FWC) as an “amber alert” to notify the flight crew of "*conditions that require immediate flight crew awareness and subsequent flight crew response*”. (Ref. EASA CS-25, §25.1322)
Master warning	A warning alert typically provided by a Flight Warning Computer (FWC) as a “red alert” to notify the flight crew of "*conditions that require immediate flight crew awareness and immediate flight crew response*”. (Ref. EASA CS-25, §25.1322)
Public key infrastructure	Set of roles, policies, procedures, hardware and software needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption. It provides a confirmation of the identity of parties involved in the communication as well as the validation of the information being transferred.
Real-time flight recorder data	Flight recorder data meant to be transmitted nearly instantaneously as they are collected, either by streaming (all along the flight) or after trigger (abnormal or distress situation is detected).

Term	Definition
Skybrary	A wiki set up by EUROCONTROL on flight operations, air traffic management (ATM) and aviation safety in general. It enables users to access the safety data made available on the websites of various aviation organizations - regulators, service providers, industry. As such, it is used in the study as a comprehensive and credible source of aviation safety information. The authors of the present report will nevertheless refer to original documents to the best extent possible.

Table 1: Definitions

Acronym	Definition
AC	Alternating Current
ACAS	Airborne Collision Avoidance System
ACD	Aircraft Control Domain
ACMS	Aircraft Condition Monitoring System
ADFR	Automatic Deployable Flight Recorder
ADPCM	Adaptive Differential Pulse-Code Modulation
AES	Advanced Encryption Standard
AIA	Accident Investigation Authorities (aka SIA in Europe)
AISD	Airline Information Service Domain
aka	also known as
ANP	Actual Navigation Performance
ANSP	Air Navigation Service Providers
APU	Auxiliary Power Unit
ATN/IPS	Aeronautical Telecommunications Network/Internet Protocol Suite
AVC	Advanced Video Coding
CA	Certificate Authority
CDS	Cockpit Display System
CG	Center of Gravity
CNN	Convolution Neural Network
CRC	Cyclic Redundancy Check
CSP	Communications Service Provider
CSR	Certificate Signing Request
CVR	Cockpit Voice Recorder
DC	Direct Current

Acronym	Definition
DLR	Data Link Recorder
DME	Distance Measuring Equipment
DSP	Datalink Service Provider
DTLS	Datagram Transport Layer Security
ECAM	Electronic Centralized Aircraft Monitoring
EFIS	Electronic Flight Instrument System
EGT	Exhaust Gas Temperature
EPE	Estimated Position Error
EPR	Engine Pressure Ratio
EPU	Estimated Position Uncertainty
EUROCAE	European Organization of Civil Aviation Equipment
FB	Functional Block
FCMIR	Flight Crew-Machine Interface Recorder
FDAU	Flight Data Acquisition Unit
FDIU	Flight Data Interface Unit
FDR	Flight Data Recorder
FMS	Flight Management System
FWC	Flight Warning Computer
FWS	Flight Warning System
GBAS	Ground-Based Augmentation System
GCAS	Ground Collision Avoidance System
GLS	GBAS Landing System
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
HMI	Human-Machine Interface
HTTPS	Hypertext Transfer Protocol Secure
ICAO	International Civil Aviation Organization
IAN	Integrated Approach Navigation
ILS	Instrument Landing System
IRNAV	Integrated Area Navigation
ITU	International Telecommunication Union
JPEG	Joint Photographic Expert Group
LZMA	Lempel-Ziv Markov chain Algorithm

Acronym	Definition
LZSS	Lempel-Ziv-Storer-Szymaski
MEL	Minimum Equipment List
MELP	Mixed Excitation Linear Prediction
MLS	Microwave Landing System
MPEG-4	Moving Pictures Expert Group 4
N_1	(Engine) Fan Speed
N_2	(Engine) Intermediate/High Pressure Spool Speed
N_3	(Engine) High Pressure Spool Speed
NA	Not Applicable
NSA	National Security Agency
OFDM	Operational Flight Data Monitoring
P2P	Point-to-Point
PIESD	Passenger Information and Entertainment Service Domain
PKI	Public Key Infrastructure
PTT	Push-to-Talk
QR-FRD	Quick Recovery of Flight Recorder Data
RAAS	Runway Awareness and Advisory System
RAR	Roshal Archive
ROPS	Runway Overrun Prevention System
RSA	Rivest-Shamir-Adleman
SATCOM	Satellite Communications
SDAC	System Data Acquisition Concentrator
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIA	Safety Investigation Authority
SMS	Safety Management System
TAWS	Terrain Avoidance and Warning System
TCAS	Traffic Collision Avoidance System
UA	User Application
VPN	Virtual Private Network

Table 2: Acronyms

4 GENERIC SYSTEM OVERVIEW

4.1 Overall System Architecture

Figure 1 provides an overview of the end-to-end QR-FRD system architecture, based on functional blocks (FB) discussed in D2 [Ref 2]. It basically consists of an airborne segment covering FB1 (Data Collection), FB2 (Start Condition Detection) and a first part of FB3 (Data Transport), a possible space segment covering an intermediate part of FB3 (i.e. SATCOM), and a ground segment covering the final part of FB3, as well as FB4 (Off-Aircraft Storage) and FB6 (Data Recovery). As can be seen, it is meant to securely transmit flight recorder data for two main end-users:

- Accident Investigation Authorities (AIA), which will use the data to analyze the events and conditions that led to the serious incident or accident they are investigating.
- The operator (or contracted organization), which will use the data for mandatory periodic quality inspection of the recordings and for possible additional data for Operational Flight Data Monitoring (OFDM). The operator may also use this data to investigate incidents not subject to ICAO Annex 13 [Ref 8], in the framework of its Safety Management System (SMS). This use of flight data and audio recordings is permitted and framed in Air OPS rules, Part-CAT, CAT.GEN.MPA.195 point (f) [Ref 10].

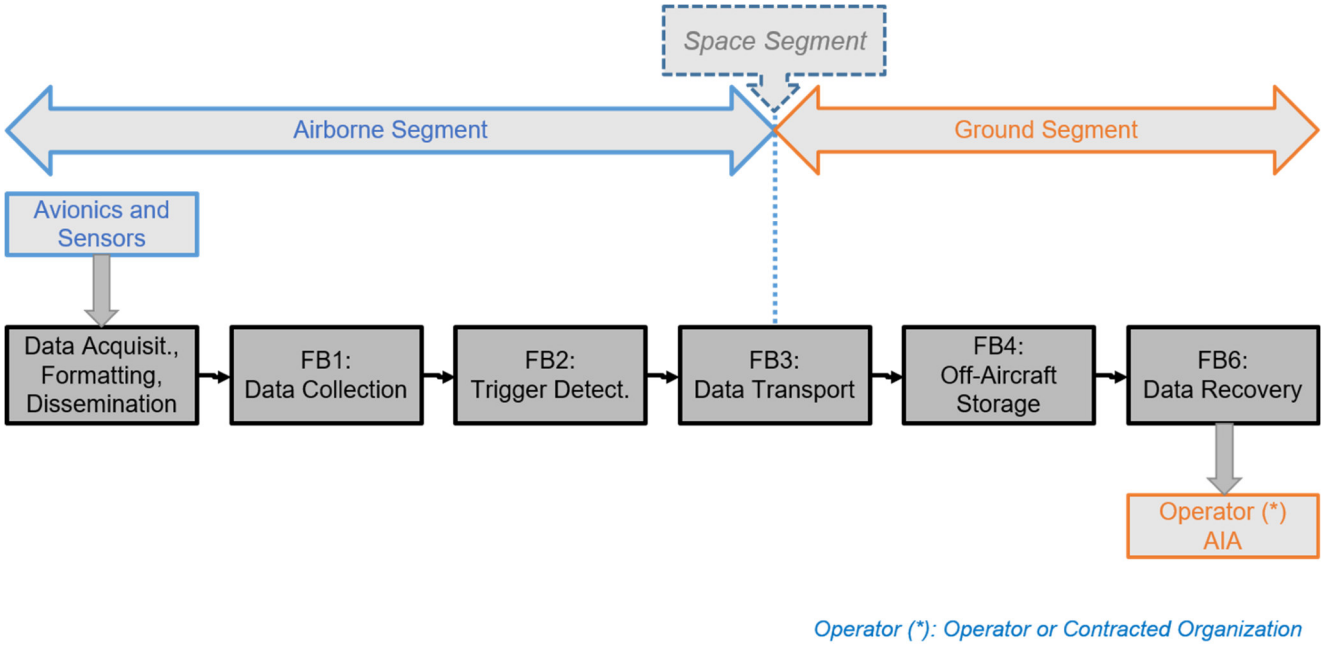

Figure 2 : QR-FRD overall end-to-end system architecture

The airborne and ground segments system functional architectures are further detailed in the following sections.

4.2 Airborne Segment Description

4.2.1 System Architecture

Figure 2 depicts a high-level system architecture for the airborne segment. Two main capabilities are respectively responsible for:

1. The acquisition, conditioning and possible management of signals and data provided by different sources (avionics and sensors), as well as the dissemination of resulting flight recorder data towards conventional flight recorders on the one hand, and towards the core QR-FRD capability on the other hand.
2. The collection and possible buffering of the flight recorder data, as well as their transmission after trigger detection using the different data link means available on board at the time of the transmission.

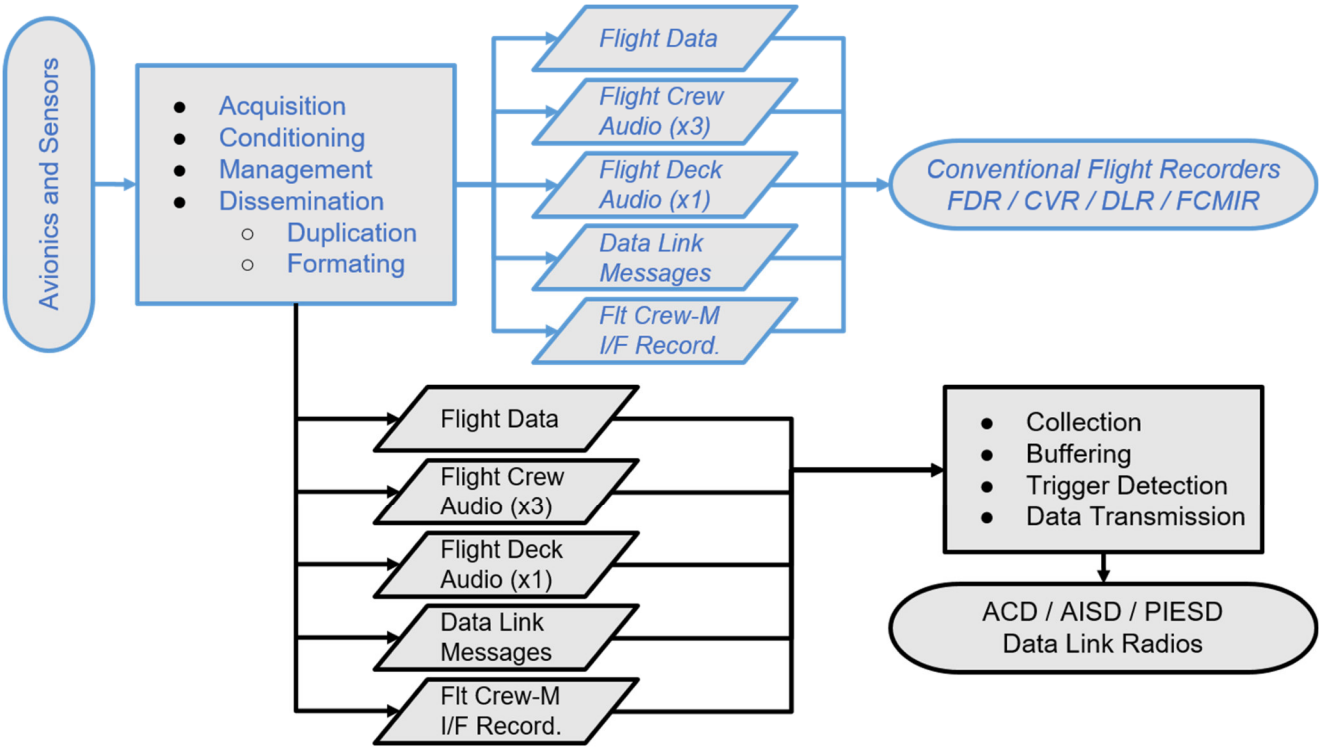

Figure 3 : Airborne segment high level system architecture

Note: The term “conventional flight recorders" (i.e. Flight Data Recorder (FDR), Cockpit Voice Recorder (CVR), Data Link Recorder (DLR) and Flight Crew-Machine Interface Recorder (FCMIR)), is used irrespectively of the actual implementation of the recorders. Indeed, these can be physically integrated (e.g. Combined FDR/CVR that would also act as crash-protected flight recorders hosting the DLR and/or FCMIR recording functions), be fixed or automatically deployable (i.e. ADFR) as proposed as an alternative for QR-FRD.

Note: For the sake of simplification, continuous transmission (stream) can also be seen as a triggered transmission, the trigger or start condition being “as soon as powered on” or “as soon as the

conventional flight recorders start recording". In such a case, only real-time flight recorder data would be transmitted, historical flight recorder data being inexistent[1].

Note: The data link media that are selected for the proposed solutions will be detailed later in the document. These can be part of the Aircraft Control Domain (ACD), Airline Information Service Domain (AISD) and Passenger Information and Entertainment Service Domain (PIESD) as discussed in D2 [Ref 2].

Note: The two threads of flight recorder data may be formatted slightly differently, especially for audio. Provided the quality complies with requirements defined in ED-112A [Ref 3], a digital audio format, as considered by aircraft manufacturers[2], could be used for the QR-FRD solution. All flight recorder data inputs to the core QR-FRD capability would then be digital.

Figure 3 depicts a high-level functional architecture for the core QR-FRD capability in the airborne segment, and lists main functions and sub-functions identified in D2 [Ref 2]:

- Collection: function in charge of interfacing with flight recorder data inputs and gathering the data after digitization of audio signals typically if necessary, as well as time stamping the data for synchronization at storage and/or recovery.
- Buffering: function in charge of conditioning the chunks of data in view of their transmission. As discussed in D2 [Ref 2], the flight recorder data can be merged in the same chunk or left separated by type, possibly compressed with lossless compression techniques, signed, encrypted and stored for immediate transmission (continuous streaming) or on condition (triggered) transmission.
- Trigger Detection: function in charge of monitoring flight recorder data, typically flight data, and evaluating distress or abnormal situations events to trigger the transmission of flight recorder data and cancel it once the situation is back to normal.
- Data Transmission: function in charge of establishing, if required/not available, a secured point-to-point connection with the flight recorder data repository on the ground (or using an already existing secured communication pipe provided it meets the performance requirements), managing the transfer of data (buffered chunks) as well as managing the data link media available for the transmission of the flight recorder data.

[1] Buffered flight recorder data prior to the "trigger", i.e. stored historical flight recorder data, should be inexistant in the "continuous transmission" case, which is not the case for "triggered transmission". However, real-time flight recorder data sent for transmission will be temporarily stored during periods when connectivity is lost. This will be managed at transmission level.
[2] Aircraft manufacturers and equipment manufacturers are considering fully digital audio solutions, i.e. for which digital audio would directly feed recorders.

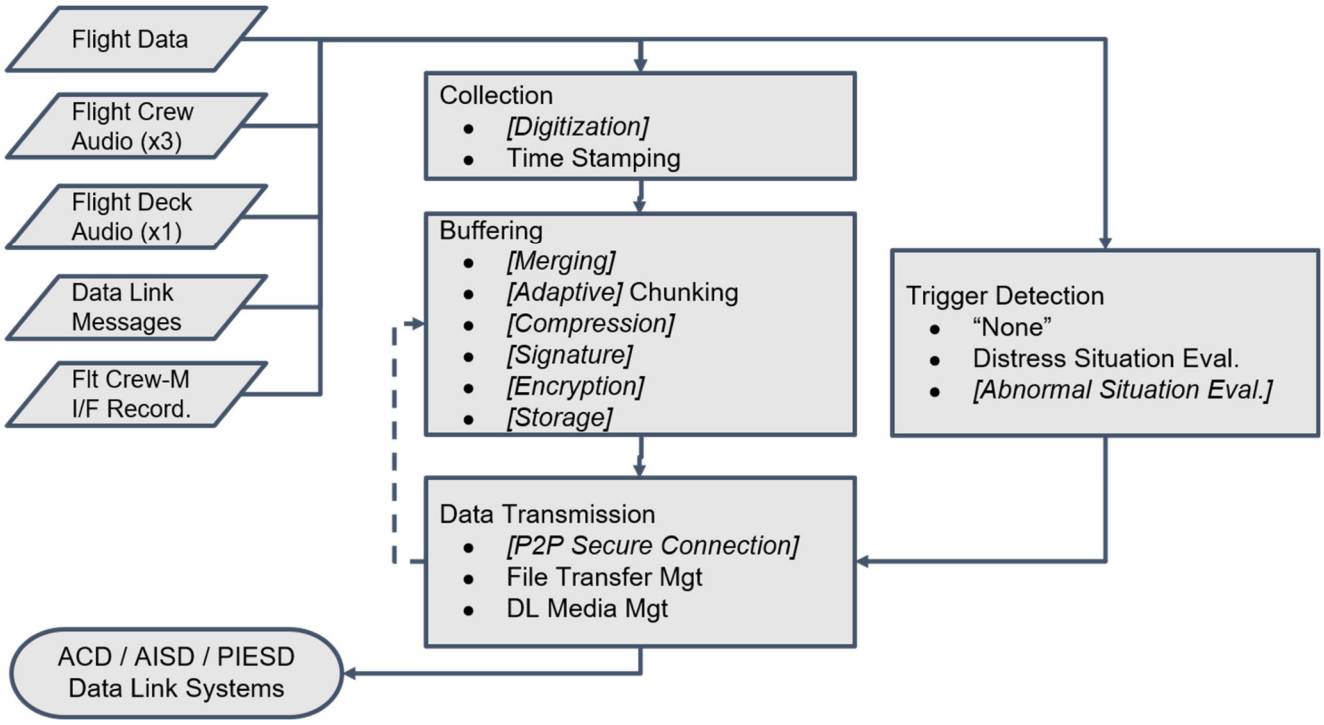

Figure 4 : Airborne QR-FRD capability high level functional architecture

Note: The sub-functions are not sorted in a definitive order of data processing. The arrangement may depend on the options being selected for implementation. For instance, separate data chunks could be compressed and then encrypted before being merged. Some sub-functions may not be implemented at all, e.g. Merging or Signature, though this latter is recommended.

Note: The size of the chunks is presently undetermined. As discussed in D2 [Ref 2], a trade-off needs to be made between the efficiency of compression for instance, the latency introduced by the processing time for encryption and signature, as well as the probability of their successful transmission. Depending on the sophistication of the Data Transmission function and Data Link Media Management sub-function in particular, the size of the chunks could be adaptive, i.e. larger when transmission conditions are close to nominal and smaller when the available bandwidth is limited.

Note: Latency introduced by the different processing between the time the data is collected and the time it is actually transmitted (i.e. reaches the ground, not necessarily its final destination) successfully will be an issue to be investigated during further activities of the study (typically, modeling and simulation. The overall latency will indeed be a matter of processes applied to the data (e.g. chunking, merging, encryption…) as well as transmission performance (e.g. encapsulation, handshakes, acknowledgements…).

Note: Though discussed in D2 [Ref 2], triggering transmission of flight recorder data from the ground is not considered in the proposed solutions. Also, manual activation of the transmissions by the flight crew for other purposes than testing or quality inspection of the recordings is not addressed in the present document.

Note: The present version of the document considers triggers for the initiation of the whole set of flight recorder data, both real-time and historical. Depending on the prioritization scheme selected to cope with available bandwidth, flight recorder data may be sent by data types, e.g. flight data first and audio

when possible, as discussed in D2 [Ref 2]. Alternative transmission schemes for which specific data types would be transmitted on specific conditions (e.g. flight phase) for instance will be investigated later in the study as time permits.

4.2.2 Core Sub-Functions Description

4.2.2.1 Digitization

This sub-function is intended to digitize non-digital flight recorder data that serve as inputs to the core QR-FRD capability, i.e. flight crew audio channels as well as the flight deck audio channel (aka cockpit environment audio).

Minimum requirements for digitization of flight crew audio channels and the flight deck audio channel are provided in ED-112A [Ref 3].

Flight data are expected to be provided using digital formats defined in ARINC 717 [Ref 8] or ARINC 767 [Ref 9].

Data link messages are expected to be provided using digital formats defined in ARINC 767 [Ref 9].

Flight crew-machine interface recorders are not standardized yet. It is nevertheless assumed Flight crew-machine interface recordings would be provided using digital formats possibly defined in ARINC 767 [Ref 9].

4.2.2.2 Time Stamping

This sub-function is intended to time stamp the flight recorder data at their reception by the collecting function for future processing, e.g. chunking, merging, resynchronization…

Minimum requirements for time stamping of flight recorder data can be found in ED-112A [Ref 3].

4.2.2.3 Merging

This sub-function is intended to merge the different flight recorder data into a single chunk ensuring their recovery will be consistent timewise.

As discussed in D2 [Ref 2], AIA may prefer analyzing smaller amounts of time correlated flight recorder data of multiple types, e.g. flight data and both flight crew and flight deck audio, rather than a larger amount of a single type, e.g. flight data only.

When not merged, data threads may be processed individually (e.g. different compression techniques, or different levels of encryption), and their transmission prioritized per data type (cf. D2 [Ref 2]). In that case, juxtaposition and resynchronization will be necessary at the data recovery stage by the investigators based on timestamps.

4.2.2.4 Chunking

This sub-function is intended to split the bulk of collected data into chunks the size of which may be fixed a priori (e.g. equivalent to 4 seconds time intervals) or dependent on transmission conditions (adaptive chunking, e.g. based on the available or negotiated bandwidth), which could vary over time, or dependent on the transmission scheme, i.e. continuous or triggered.

Further analysis based on modeling and simulations will help in the determination of the most efficient chunk size as there will be a trade-off between efficiency of compression and encryption should they be used, and probability of successful transmission (cf. D2 [Ref 2]).

An alternative can be to record the data into chunks of different sizes concurrently and have them later transmitted with a “try and adapt” scheme, starting with the largest size and considering using the smaller size(s) for retransmitting data in case of failure.

Note: The concepts of chunking and merging assume all data merged withing the same chunk have the same lifetime, i.e. once prepared for transmission, the bulk of data will not have to be modified, e.g. more recent data replacing some of those already present in the bulk. Such operation would indeed require “de-processing” (i.e. decrypting and decompressing) the bulk of data first, replacing the data and “re-processing” (i.e. compressing and encrypting) the bulk.

Note: The size of the chunk will, depending on implementation, influence (i.e. possibly delay) the transmission of real-time flight recorder data that would be slightly postponed during communication failures or transmission of a chunk of historical flight recorder data.

4.2.2.5 Compression

This sub-function is intended to reduce the size of the chunks prior to their storage and/or transmission.

As discussed in D2 [Ref 2], lossless compression is recommended if compression is used.

Also, different compression algorithms may be applied on the different data types to increase efficiency. Nevertheless, there will again be a trade-off between the amount of data to be compressed, the expected compression ratio and the acceptable processing duration.

Such a trade-off will require further analysis, especially for flight crew and/or flight deck audio. Indeed, it may be worth considering a better digitization technique (cf. §4.2.2.1) than the sampling rates and resolution meant for CVR, associated with lossy compression algorithms, as this may result in less storage space still allowing higher audio quality at recovery level.

ICAO Doc 10054-1 [Ref 5] recommends the use of 3-bit adaptive differential pulse-code modulation (ADPCM) algorithms should lossy compression be considered for cockpit environment audio (cf. D2 [Ref 2]).

Commonly used lossless compression algorithms include Lempel-Ziv-Storer-Szymaski (LZSS) used by RAR (Roshal Archive) for instance, Lempel-Ziv Markov chain Algorithm (LZMA) used by ZIP[3] for instance and DEFLATE as proposed for message compression in ARINC 841 [Ref 11] for instance.

H.264[4], HVEC[5] and JPEG[6] (Joint Photographic Expert Group) are well known methods to compress video and images. Neural network-based algorithms, e.g. convolution neural network (CNN) algorithms, are being developed that would improve video compression performance, i.e. ratio and speed, by a factor 2.

It is recommended to use state-of-the-art lossless and non-proprietary formats and algorithms for the actual implementation of the solution.

[3] ZIP is not an acronym, and would have been suggested to its designer, Phil Katz, as “zip” means “moving at high speed”.

[4] H.264 is a video compression standard defined by International Telecommunication Union (ITU), and also known as Moving Pictures Expert Group 4 (MPEG-4) Advanced Video Coding (AVC).

[5] HVEC (High Efficiency Video Coding), aka H.265 and MPEG-H Part2, is a video compression standard defined by ISO/CEI 23008-2 and IUT-T H.265

[6] JPEG uses a lossy form of compression based on the discrete cosine transform (DCT). Nevertheless, a lossless mode exists in the standard but is not widely supported.

Note: Snapshots of cockpit displays rather than pictures / videos taken from a distance as for AIR may be considered for FCMIR. Use of vector files[7] or ARINC 661 records[8] could be used to reduce the amount of data to be recorded. The latter option needs further analysis, possibly in a follow-on study, to identify what additional information the investigators would require to rebuild the actual displays.

The following table provides typical figures on the performance of compression algorithms found in literature.

Lossless data compression ratio	2:1 (binary data) – 5:1 (text data)
JPEG compression ratio	>= 10:1
Compression rate (64-bit, 2.4 GHz processor)[9]	1 – 25 Mbyte/s

Table 3: Compression algorithms performance figures

A chunk comprising a 4-second recording of flight data, flight crew and cockpit audio, data link messages, but no images, would roughly represent 59 kbyte (cf. D2 [Ref 2]). That amount of data could be compressed to approx. 17 kbyte in less than 3 milliseconds (assuming a mean 3.6:1 compression ratio and a mean 8 Mbyte/s compression processing time).

4.2.2.6 Encryption

This sub-function is primarily intended to ensure confidentiality, i.e. guarantee the flight recorder data cannot be read by unauthorized personnel/applications, if intercepted during their transmission or once stored on the ground.

Encryption requires a keying mechanism to encrypt the data using a ciphering method. Typical implementations rely on symmetric ciphering, meaning that the same key is used to encrypt and decrypt the data.

Using the same key for all chunks being transmitted nevertheless exposes to the risk of compromising the key (risk of “collision”). A more secure solution would consist in encrypting the data with a random key and encrypting this temporary key with a public key (generated by an additional asymmetric ciphering mechanism). The associated private key, kept securely on the ground, would allow to decrypt the encrypted temporary symmetric key transmitted together with the encrypted chunk and finally allow access to the data. The private/public key pair can be managed on the ground and the public key loaded on the aircraft as part of the configuration. Such process can be controlled by the airline as discussed in the concept of operations later in the present document (cf. §5.1.1).

Note: Key pairs are usually kept for a limited period of time (typically one year[10]) to limit the security risk hence requiring the need to periodically update the airborne side with the new public key. Automatic

[7] Vector files are images that are built by mathematical formulas that establish points on a grid. Because they can infinitely adjust in size without losing resolution, vector files are more versatile and compact than raster files (bitmaps). A typical vector file format is pdf (portable document format).

[8] ARINC 661 [Ref 13] defines an overall architecture along with many sub-components to facilitate the creation of interactive displays: a rendering machine dedicated to presenting graphical information known as the Cockpit Display System (CDS), its associated logic which is handled by the User Application (UA) and the link between these two pillars, the Runtime Protocol, which carries events that are generated through user interaction to the UA and brings requests to display new data back to the CDS. The contents of the displays are defined by using a finite set of components called the widget library.

[9] Hardware compression can be 10 times faster than software compression.

[10] Aircraft certificate lifetime could be longer. A 3-year period is being discussed.

secure processes exist to distribute a public key and simplify the process. This nevertheless requires specific maintenance task.

Advanced Encryption Standard (AES) based on the Rijndael algorithm and Twofish are two of the most common symmetric encryption algorithms, Twofish being up to 3 times faster. Nevertheless, use of AES has been approved by the National Security Agency (NSA) to secure government files.

The Rivest-Shamir-Adleman (RSA) is the most widely used asymmetric encryption algorithm, typically for email encryption, signatures and secured websites, but is too slow to encrypt large amounts of data.

Elliptic Curve Digital Signature Algorithm (ECDSA), now also used in aviation may be an option. It is recommended to use state-of-the-art and non-proprietary algorithms for the actual implementation of the solution.

The following table provides typical figures on the performance of the AES encryption algorithm found in literature.

Encryption expansion ratio	0.15 %
Encryption rate (64-bit, 2.4 GHz processor)	10 -100 Mbyte/s

Table 4 : AES encryption algorithms performance figures

A chunk comprising a 4-second recording of flight data, flight crew and cockpit audio, data link messages, but no images, which would roughly represent 17 kbyte once compressed (cf. §4.2.2.5), would be encrypted in less than a millisecond (assuming a mean 48 Mbyte/s encryption processing time).

4.2.2.7 Signature

This sub-function is primarily intended to ensure authenticity, i.e. guarantee that the flight recorder data, once recovered, were actually transmitted by a QR-FRD equipped aircraft. It also ensures that the flight recorder data have not been modified since they have been signed.

Signature typically operates in three steps:

1. Compute a hash value using a secure hash algorithm on the data to be signed
2. Encrypt the hash value using a private key
3. Add the certificate including the public key associated with the private key used to encrypt the signature

Verifying the signature will consist in performing the reciprocal operations:

1. Verify that the certificate is valid, typically by using a Public Key Infrastructure (PKI)
2. Recalculate the hash value on the signed data
3. Check the hash value matches with the decrypted signature (the decryption being performed using the public key of the certificate)

As was mentioned for encryption (cf. §4.2.2.6), key pairs have a limited lifetime to maintain the security of the solution. Therefore, it might be required to periodically update these keys, using a process such as a Certificate Signing Request (CSR). CSR would consist in having the airborne system generating a key pair and submitting a secure request over wireless communication media to a ground server and get a signed key (certificate) from a Certificate Authority (CA). CSR allows to maintain the private key on the airborne side and never disclose it as only the public part is sent to ground as part of the CSR.

The CSR ground server and associated CA should be managed by a trusted entity ensuring that only approved operators / systems can obtain a signed certificate. The use of a Public Key Infrastructure (PKI) deployed with the CA will allow the ground user of the signed data to verify that the airborne certificate (private key part) used to sign the data has been authorized and is valid.

A simpler solution would consist in fusing (programming) the private key used for signature during the equipment production and distributing the equipment associated public key. The drawbacks of this solution include the use the same key for the equipment lifetime and the necessity to archive the unique public key for each and every equipment, which is not necessary with a PKI implementation.

RSA (also used for encryption, cf. §4.2.2.6) and Secure Hash Algorithm (SHA), (and SHA-256 that produces a 256-bit long hash value in particular,) are the two most popular methods used for signature.

The following table provides typical figures on the performance of signature algorithms found in literature.

Signature size (SHA-256)	256 bits (32 bytes)
Signature size (RSA)	1024 bits (128 bytes)
Signature rate (64-bit, 2.4 GHz processor)	50 -100 Mbyte/s

Table 5 : Signature algorithms performance figures

A chunk comprising a 4-second recording of flight data, flight crew and cockpit audio, data link messages, but no images, which would roughly represent 17 kbyte once compressed (cf. §4.2.2.5) and encrypted (cf. §4.2.2.6), would be signed in less than a millisecond (assuming a mean 70 Mbyte/s signature processing time).

4.2.2.8 Storage

This sub-function is intended to retain the chunk(s) prepared for transmission. The depth of the storage space will depend on the transmission strategy, i.e. continuous streaming of real-time flight recorder data or triggered transmission of both real-time and historical data.

A minimum of 20 minutes history is expected (cf. ICAO Doc 10054-1 [Ref 5]). This can be achieved with a cyclic buffer where the oldest data are replaced by the most recent ones, though storage space is not an issue nowadays. D2 [Ref 2] provides rough estimates of the amounts of data generated at destination of the different flight recorders during 25 hours for flight data, flight crew audio, flight deck audio and data link messages, as well as the last 2 hours of flight crew-machine interface recordings. This would lead to approximately 3 Gbyte of uncompressed, not encrypted and not signed flight recorder data (10 times less if only 20 minutes of history is considered).

4.2.2.9 Distress Situation Evaluation

This sub-function is intended to monitor and evaluate conditions that would trigger (and stop) the transmission of flight recorder data after a distress situation is detected. ED-237 [Ref 4] defines those distress situations as:

- "*Unusual attitude*": basically, extreme values of roll angle, roll angle rate, pitch angle and/or pitch angle rate
- "*Unusual speed*" and acceleration: basically, extreme values of vertical speed and/or normal and lateral accelerations, as well as stall warning or inappropriate speed for the flight situation
- Near CFIT: unintentional flight into the ground, a mountain, a body of water or an obstacle, typically, all activations of Terrain Avoidance and Warning System (TAWS) "hard" alerts (e.g. "Pull Up")

- **"***Total loss of thrust/propulsion on all engines*": basically, conditions and/or engine performance parameters indicating a loss of thrust

Most of the parameters necessary for the distress situation evaluation, if not all, are part of flight data listed in ED-112A [Ref 3]. A matrix in ANNEX A: FLIGHT DATA AND TRIGGER CONDITIONS USAGE identifies the parameters used for the evaluation of each distress condition.

Note: BEA Tech Doc [Ref 6] defines additional distress situations:

- "***Control command inputs***": excessive or inappropriate roll command and use of rudder[11]
- Possible collision with other traffic: ACAS resolution advisory
- "***Cabin depressurization***": cabin altitude warning

The last two situations are considered in §4.2.2.10 addressing abnormal situations.

BEA Tech Doc [Ref 6] provides algorithms for determining distress conditions, combining the different parameters along with respective thresholds. These latter will of course need to be tuned to the aircraft type. Generic formulas based on BEA's algorithms are provided in ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION.

4.2.2.10 Abnormal Situation Evaluation

This sub-function is intended to monitor and evaluate conditions that would trigger (and stop) the transmission of flight recorder data after an abnormal situation is detected. Indeed, as identified in D1 [Ref 1] and discussed in D2 [Ref 2], early detection of conditions that could ultimately lead to a distress situation would allow more time to transmit historical flight recorder data before transmission conditions degrade. Also, as discussed in D2, this may be an alternative for continuous transmission on flight recorder data, i.e. start streaming real-time data only once an abnormal condition is detected.

The Commission Implementing Regulation (EU) 2015/1018 [Ref 12] lays down a list classifying occurrences in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation.

Its Annex I (Occurrences Related To The Operation Of The Aircraft) and III (Occurrences Related To Air Navigation Services And Facilities) are structured in such a way that the pertinent occurrences are linked with categories of activities during which they are normally observed, according to experience, in order to facilitate the reporting of those occurrences. As such, they were considered within the QR-FRD study as a relevant taxonomy for incident, serious incidents (and accident, the difference between an accident and a serious incident lying only in the result (cf. ICAO Annex 13 [Ref 8]).

"ANNEX E: EU SAFETY OCCURENCES vs TRIGGER CONDITIONS" provides a table, based on those 2 annexes, that tentatively associates trigger conditions and "triggering systems", to occurrences relevant for the scope of the QR-FRD study. Over 60 different occurrences are listed and can be further grouped as the following abnormal situations:

1. Cabin depressurization: basically, prolonged abnormal value of cabin pressure altitude, loss of cabin pressure alert
2. Fire on board the aircraft: basically, prolonged fire on board alert
3. Aircraft system failure or malfunction: basically, abnormal engine parameters, engine alerts (vibrations, over temperature…), electrical bus failures indications, abnormal values of hydraulic pressure, computers failures, etc…

[11] Excessive or inappropriate control command inputs by the flight crew were detected few seconds before aircraft loss when analyzing the BEA's database. These likely result from excessive reaction from the crew to regain control of the flight, and as such too late to trigger transmission of data. Nevertheless, they could be used considering refinement of the formulas to detect flight crew incapacitation (cf. §4.2.2.10) for instance.

4. Low fuel or fuel system anomaly: basically, abnormal values of fuel quantities for the flight situation, conditions that would lead to either fuel exhaustion or fuel starvation
5. Near MAC (NMAC): Flight situations that could lead to a collision hazard with other traffic: basically, Airborne Collision Avoidance System (ACAS) alerts
6. Possible penetration of severe weather (or atmospheric) conditions: basically, weather alerts (severe wind shear, severe turbulence…)
7. Deviation from planned flight path: basically, abnormal values of cross track error or estimated time of arrival, abnormal re-planning, etc...
8. Flight crew incapacitation: basically, lack of voice communications or interactions with flight instruments for an abnormal period of time, signs of abnormal health status (both physiological state and a behavioral state of the flight crew member(s)), etc...

Except for the last two abnormal conditions, most of the parameters necessary for the abnormal situation evaluation are part of flight data listed in ED-112A [Ref 3]. A matrix in ANNEX A: FLIGHT DATA AND TRIGGER CONDITIONS USAGE identifies the parameters that can possibly be used for the evaluation of each abnormal condition, and Generic formulas that will need further refinement are provided in ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION.

Note: CS-25.1322 “Flight Crew Alerting” [Ref 9] provides recommendations for developing alerting systems and displays (visual, aural, haptic…) of warning alerts and caution alerts. The flight crew alerting system is expected to use a consistent philosophy for alerting conditions, urgency and prioritization, and presentation. As such, a flight crew alerting system acts as a “concentrator” of alerts provided by sensors and avionic computers generating a master caution or a master warning output to be displayed depending on the time-criticality and severity of the alert. These alerts are meant to provide the flight crew with awareness of a non-normal condition and include but are not limited to predictive and reactive windshear warnings, terrain awareness warnings (TAWS), airborne collision avoidance system resolution advisories (ACAS II), overspeed warnings and low energy warnings. “ANNEX C: FLIGHT WARNING SYSTEM” provides details on the architecture and lists “red warning” and “amber caution” alerts. It may be recommended to rather use the flight warning computer outputs, i.e. caution and warning information, as triggers instead of performing similar computations.

Advanced QR-FRD solutions may need to monitor other flight recorder data than flight data, e.g. flight deck audio or flight crew-machine interface recordings to monitor the flight crew activity (e.g. absence of aural communication, absence of (or abnormal) actions on control panels…), or be connected to specific avionics computers, e.g. Flight Management System (FMS), and future flight crew health monitoring systems. For the last two abnormal conditions, there is no guarantee a solution can be found with current systems.

Note: QR-FRD solutions are not standardized yet. Nevertheless, several classes of solutions could be considered depending on their sophistication and the conditions they are able to evaluate. These classes of solutions could for instance include:

- Continuous transmission only
- Triggered transmission on distress condition only, based on flight data only
- Triggered transmission on abnormal condition only, based on flight data only
- Triggered transmission on abnormal condition and distress condition, based on flight data only
- Triggered transmission on abnormal condition only, based on flight data and other information from various sources
- Triggered transmission on abnormal and distress conditions, based on flight data and other information from various sources

4.2.2.11 Point-to-Point Secure Connection

This sub-function is intended to manage the airborne side of the secure connection between the QR-FRD capability on board the aircraft and the QR-FRD repository on the ground (at the operator facility or contracted service).

This can be achieved by the establishment of a Virtual Private Network (VPN), or the use of secure transmission protocols (e.g. Hypertext Transfer Protocol Secure (HTTPS) or Secure File Transfer Protocol (SFTP)). These will add another layer of data protection (typically encryption, and mechanisms to ensure authenticity and integrity) meant to avoid man-in-the-middle attacks.

Trend in aviation is to use web-technologies, e.g. HTTPS and Quick UDP (User Datagram Protocol) Internet Connections (QUIC). It is recommended to use state-of-the-art and non-proprietary formats and algorithms for the actual implementation of the solution.

Encapsulation overhead	48 bytes

Table 6 : VPN encapsulation performance figures

Note: Aeronautical Telecommunications Network/Internet Protocol Suite (ATN/IPS) identified in D2 [Ref 2] as a candidate solution in the future (though originally meant for air traffic service communications) will provide Datagram Transport Layer Security (DTLS) for security with an option for cryptography. Use of ANT/IPS could then be considered, assuming air navigation service providers (ANSP) and airlines will then have secured pipes, avoiding need for other point-to-point secured connections (e.g. VPN). Rationalization of the number of point-to-point connections is indeed an issue.

4.2.2.12 File Transfer Management

This sub-function is intended to manage the transfer of files (chunks readily prepared by previous sub-functions) from the aircraft at the destination of the ground. This includes:

- Selecting the file to be transmitted
- Monitoring the transfer status
- Managing retries in case of transmission failure
- Providing feedback on the transmission performance to other sub-functions

Note: The last two bullets (managing retries and providing feedback) are dependent on the sophistication of the system, protocols used between the different transmission layers (as well as between the associated hosting equipment), and strategies set in place. They can possibly be used to adapt the size of the files (chunks) to be transmitted (cf. §4.2.2.4).

Data link characteristics are detailed in D1 [Ref 1]. Throughput values range from a couple of kbit/s to several Mbit/s depending on the media being used. A chunk comprising 4 seconds recordings of flight data, flight crew and cockpit audio, data link messages, but no images, which would roughly represent 17 kbyte once compressed (cf. §4.2.2.5), encrypted (cf. §4.2.2.6) and signed (cf. §4.2.2.7), would be transmitted in less than half a second (assuming a mean 500 kbit/s transmission data rate). This nevertheless means that approx.10% of the throughput for that media would be dedicated to QR-FRD transmissions when downlinking a 4-second chunk once every 4 seconds. The transmission of images providing from flight crew-machine interface recordings needs to be thoroughly investigated. Indeed, even if compressed, the transmission of the whole set of flight recorder data might take longer than the time it takes to collect it, i.e. longer than 4 seconds.

4.2.2.13 Data Link Media Management

This sub-function is intended to manage the data link media (radios and dedicated routers as necessary) on board the aircraft that are selected for the transmission of the flight recorder data. This includes:

Selection of the media to be used for the transmission (should there be more than one made available for the QR-FRD capability)

- Establishing connection with the ground counterpart
- Reconnecting in case of disruption
- Monitoring the media performance / quality of service
- Providing feedback on the transmission performance to other sub-functions
- Possibly, preempting a media to allocate the whole bandwidth for the sole purpose of QR-FRD transmissions

Note: The last but one bullet (providing feedback) is dependent on the sophistication of the system, protocols used between the different transmission layers (as well as between the associated hosting equipment), and strategies set in place. It can possibly be used to adapt the size of the files (chunks) to be transmitted (cf. §4.2.2.4).

Note: As discussed in D2 [Ref 2], the media bandwidth may be shared among aircraft in vicinity. Allocating more/full bandwidth to the aircraft triggering QR-FRD transmissions may be considered provided the Communication Service Provider (CSP) provides the associated Quality of Service (QoS), e.g. “distress transmission” / “high priority transmission”[12]. This will likely require discussions / negotiations with the selected CSP offering the service.

Note: When considering triggered transmissions, there will still be the need to periodically have a message transmitted and acknowledged (heartbeat) during the flight to ensure the communication pathway is operational should a trigger condition be detected.

4.3 Ground Segment Description

4.3.1 System Architecture

Figure 4 depicts a high-level functional architecture for the QR-FRD capability in the ground-based segment, and lists main functions and sub-functions identified in D2 [Ref 2]:

- Data Reception: ground-based counterpart of the airborne Data Transmission function, the function is in charge of the completion of the secured point-to-point connection with the airborne QR-FRD capability and successful reception of the transmitted files.
- Off-aircraft Storage: function in charge of securely storing and retaining / deleting flight recorder data in the dedicated repository.
- Data Recovery: largely a ground-based counterpart of the airborne Buffering function, the function is in charge of reconditioning the chunks of data in view of their exploitation, as well as managing access to the flight recorder data for authorized organizations, namely the Accident Investigation Authorities (AIA) for accident investigation purposes and the operator (or contracted organization) for quality inspection of the recordings primarily. Compressed and encrypted chunks will have to be decrypted and decompressed, and authenticity as well as integrity checking (typically an AIA concern) will be enabled with signature. The chunks will be

[12] However, flight recorder data will always be of lower priority than flight crew / ATC communications that are required for safe flight and landing.

reassembled into larger files covering long portions of the flight to be analyzed, and the files possibly split per data type if originally merged.

Note: As of today, some AIAs have in their labs the ground equipment and software to perform by themselves the downloading of the stored files, their decompression and their decoding into usable data. When considering QR-FRD, they will probably want to be able to decrypt, check authenticity, decompress, etc. by themselves and they will want to get the software to be able to perform these operations in their labs. This matters for their independence and credibility. Through advanced agreement, the AIA not having such laboratory equipment may ask major AIAs to do the job for them in the framework of Annex 13 investigations.

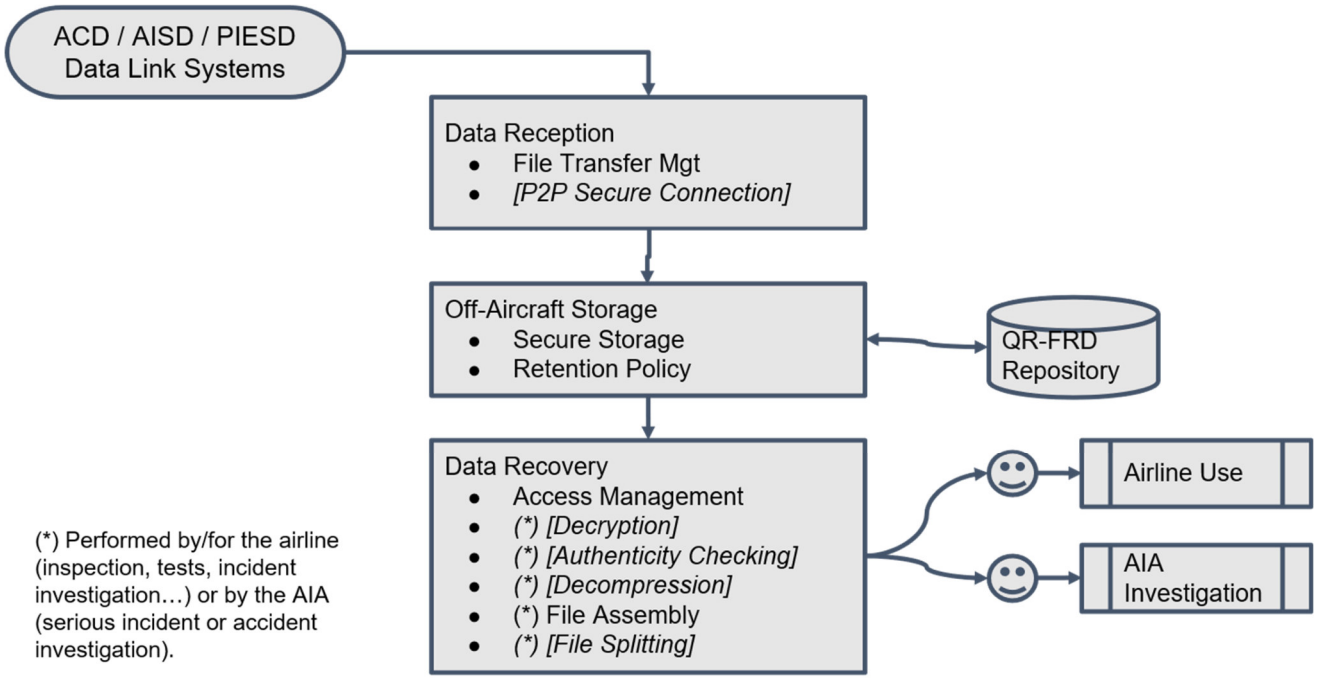

Figure 5 : Ground-based QR-FRD capability high level functional architecture

Note: The sub-functions are not sorted in a definitive order of data processing. The presence and arrangement will be highly dependent on the airborne counterparts selected for implementation.

4.3.2 Sub-Functions Descriptions

4.3.2.1 File Transfer Management

This sub-function is the ground-based counterpart of the airborne homonymic sub-function (cf. §4.2.2.12). It is intended to manage the transfer of files (chunks) received from the aircraft. This includes:

- Reception of the chunks
- Interrupted transfer and erroneous transfer management

4.3.2.2 Point-to-Point Secure Connection

This sub-function is the ground-based counterpart of the airborne homonymic sub-function (cf. §4.2.2.11). It is intended to manage the ground-based side of the secure connection between the QR-FRD capability on board the aircraft and the QR-FRD repository on the ground (at the operator facility or contracted service).

4.3.2.3 Secure Storage

This sub-function is intended to securely store and retain the flight recorder data in the dedicated QR-FRD repository. Secure data storage involves protecting storage resources and the data stored on them (either on-premises or in external data centers or "the cloud"[13]) from accidental or deliberate damage or destruction and from unauthorized users and uses. This can be achieved using redundant and secure servers owned by the operator, or a cloud-based storage owned / outsourced by a contracted organization (using redundant array of independent disks (RAID) technology and multi-site servers for instance). ISO/IEC 27040 [Ref 17] defines best practices that set the minimum expectations for storage security.

4.3.2.4 Retention Policy

This sub-function is intended to definitively delete the data securely stored (cf. §4.3.2.3) according to a retention policy (typically, 60 days after its reception in case of an accident as discussed in D2 [Ref 2]). It may be recommended that this feature be automatic.

AMC/GM Annex IV Part CAT [Ref 10] CAT.GEN.MPA.195(a) to (f) provide recommendations for the handling of flight recorder recordings, incl. preservation of recorded data for investigation, use for inspection and checks of flight recorders recordings, use of CVR recordings for maintaining or improving safety as well as use of FDR data and CVR recordings for a flight data monitoring (FDM) program. The procedures related to the handling of CVR recordings may have to be adapted to the handling of flight crew and flight deck audio recordings in order to fulfil the privacy requirements (e.g. deletion to the extent possible of parts of the recordings that contain information with privacy contents).

Note: Flight crews may activate the bulk erase function once at the gate to modify the CVR recordings in such a way they can no longer be retrieved using normal replay or copying techniques (cf. ED-112A [Ref 3]). This prevents the operator from accessing the audio recordings. Nevertheless, accident investigations authorities are still able to retrieve the data using non-normal replay techniques. This feature needs to be adapted to the QR-FRD case. Access denial for the operator to audio recordings could be achieved by the access management function (cf. §4.3.2.5) or data protection management (e.g. encryption key management) for instance.

4.3.2.5 Access Management

This sub-function is intended to manage access to the QR-FRD repository for authorized organizations/personnel only.

Access[14] could for instance be provided to Accident Investigation Authorities (AIA) for a specific flight, possibly tagged "serious incident" or "accident", and to an operator only for its flights/aircraft.

4.3.2.6 Authenticity Checking

This sub-function is intended to enable verification of the authenticity (along with the integrity) of the data based on their signature (cf. §4.2.2.7).

The organization wanting to check the authenticity of the data will have to be provided with the means (e.g. password and/or public key) associated with the signature.

[13] Using cloud-based solutions may have serious consequences on data access and protection. Although Annex 13 protects investigation data, storing it in extra-territorial clouds may undermine data privacy and protection (cf. US Cloud Act). This issue will be assessed in later in the study (D4 / D7).

[14] Remote or on-site access feature should leverage a strong access control policy. This access control is the ultimate safeguard before accessing flight recorder data, while not in the core business of an operator. The attack surface should be considered and security information and event management, including insider threat mitigation, set in place.

4.3.2.7 Decryption

This sub-function is the ground-based counterpart of the airborne Encryption sub-function (cf. §4.2.2.6). It is intended to decrypt the encrypted chunks and enable their subsequent processing.

The organization wanting to decrypt the data will have to be provided with the means (e.g. private key) associated with the one(s) used for encryption.

4.3.2.8 Decompression

This sub-function is the ground-based counterpart of the airborne Compression sub-function (cf. §4.2.2.5). It is intended to decompress the compressed chunks and enable their subsequent processing.

The organization wanting to decompress the data will have to be provided with the means (e.g. algorithm) associated with the one(s) used for compression.

4.3.2.9 File Assembly

This sub-function is the ground-based counterpart of the airborne Chunking sub-function (cf. §4.2.2.4). It is intended to assemble the decrypted and decompressed chunks into a larger file, e.g. covering large portions of the flight if not its entirety, and enable its subsequent analysis.

4.3.2.10 File Splitting

This sub-function is the ground-based counterpart of the airborne Merging sub-function (cf. §4.2.2.3). It is intended to split the assembled files (cf. §4.3.2.9) containing merged flight recorder data into separate files only containing a single type of flight recorder data and enable their subsequent analysis with the tools as of today.

5 SOLUTIONS PRESENTATION

The functional allocation for the two solutions discussed in D2 [Ref 2] is depicted in Figure 5.

Solution #1, “AISD-based”, is articulated around an AISD router for the airborne functions, and around communication and datalink service providers, the airline (or contracted organization) and the accident investigation authority for the ground-based functions.

Solution #2 is articulated around FDAU/FDIU and ACMS units as well as an AIDS router for the “FDAU/FDIU&ACMS-based” airborne functions, and, similarly to Solution #1, around communication and datalink service providers, the airline (or contracted organization) and the accident investigation authority for the ground-based functions.

As such, the two solutions are very close from a system / hardware perspective.

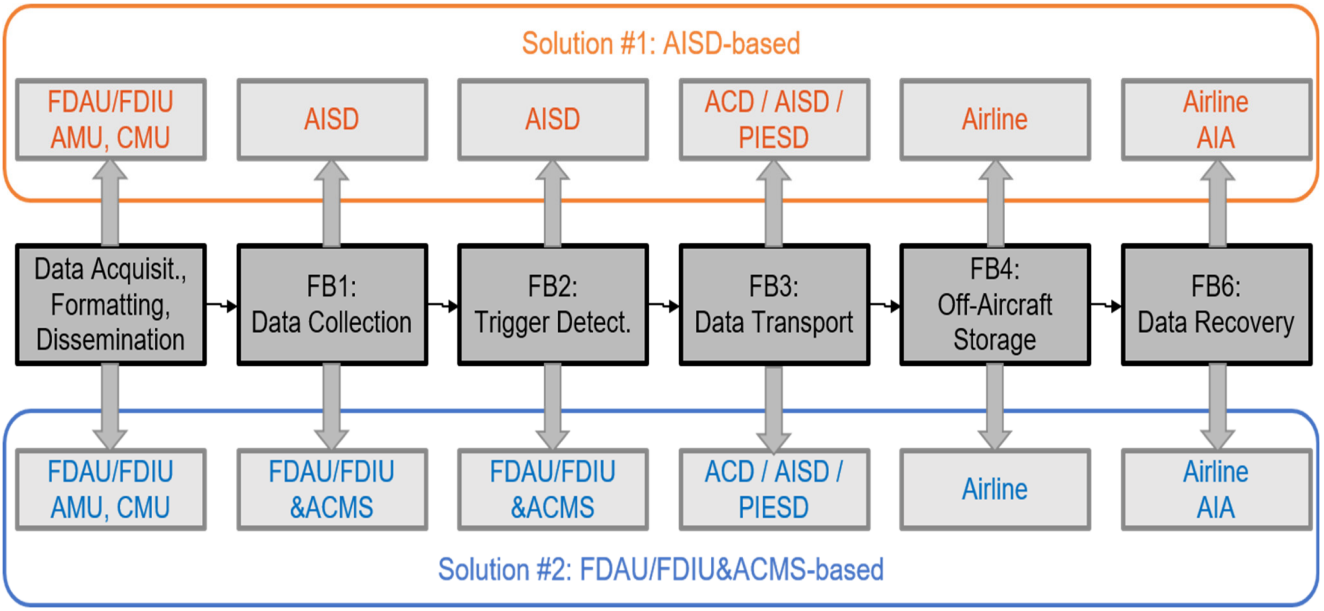

Figure 6 : Solution #1 (AISD-based) and Solution #2 (FDAU/FDIU&ACMS) functional allocations

Nevertheless, several options (features), were identified in D2, and further described in the present document (cf. §4). The proposed distribution of the selected options across two “software” solutions is summarized in the following table:

Option / Feature	Software Solution#1	Software Solution#2	Comment
Transmission mode	Continuous (streaming)	Triggered	
Merging	TBD	Yes	
Chunking	Fixed	Adaptive	Cf. Note 1

Compression	Yes	Yes	
Signature	Yes	Yes	
Encryption	Yes (audio)	Global	Cf. Note 2
Storage	Limited	20 minutes minimum[15]	
P2P Secure Connection	https / sftp	VPN	Cf. Note 3
Datalink Media Mgt	PIESD (Cell + Satcom)	PIESD (Satcom)	TBC by survey

Table 7 : Options for Software Solutions #1 and #2

Note 1: At the time of the drafting of the present document, it is unclear how efficient adaptive chunking could be performed. Modeling and simulations will provide insight on criteria or parameters such as situation, influence of the size of the chunk on transmission success, datalink performance, etc…

Note 2: If Merging is considered in the Continuous transmission case, it should occur after encryption, since the latter would only concern the audio data type.

For the sake of simplification, “software” Solution #1 is associated to “hardware” Solution #1, and “software” Solution #2 to “hardware” Solution #2. The resulting Solution #1 and #2 are detailed in the following sections. Nothing prohibits associating “software” and “hardware” solutions differently.

Note 3: Establishment of a VPN will require handshakes that will delay the transmission of flight recorder data. This may impact significantly triggered transmissions should the VPN be set up right after the trigger condition is detected. It may be recommended to open a VPN upfront or use an already existing VPN. A time diagram is provided §5.1.2.4 below for illustration.

[15] As mentioned in D2 [Ref 2], there is no technical limitation to the size of the buffer. CVR and DLR have a minimum recording duration of 2 hours. The two cases (20 minutes and 2 hours) will be considered during the simulation activities undertaken within Task 6 of the QR-FRD study.

5.1 Solution #1: AISD-based

5.1.1 Hardware architecture

The hardware architecture for Solution #1 is depicted Figure 6.

Note: For the sake of consistency, flight crew-machine interface recorders (FCMIR) and associated inputs not being standardized at the time this version of the document was drafted, it is assumed a "Flight Crew Interface Acquisition Unit" will collect flight crew-machine interface recordings and feed them to the FCMIR function (standalone or hosted by one of the other mandatory crash-protected flight recorders).

The numerous digital and analog sources are acquired and processed by their respective acquisition and management units, namely, Flight Data Acquisition Unit (FDAU), Audio Management Unit (AMU), Communication Management Unit (CMU), and possibly Flight Crew Interface Acquisition Unit (cf. note above). These duplicate their outputs and feed, on the one hand, their respective recorder, i.e. Flight Data Recorder (FDR), Cockpit Voice Recorder (CVR), Data Link Recorder (DLR) that can typically be hosted by the CVR, and Flight Crew-Machine Interface Recorder (FCMIR) likely hosted by either FDR, CVR or a combination of both. On the other hand, they also feed the Airline Information Service Domain (AISD) router with flight data, flight crew audio and flight deck audio, data link messages and flight crew-machine interface recordings as described in §4.2.1

As depicted in Figure 6, the AISD router hosts the major part of the airborne QR-FRD functions. It nevertheless interfaces with the different data link radios either directly or via their respective domain router[16], i.e. Aircraft Cockpit Domain (ACD) router, actually the CMU, and the Passenger Information and Entertainment Service Domain (PIESD) router[17].

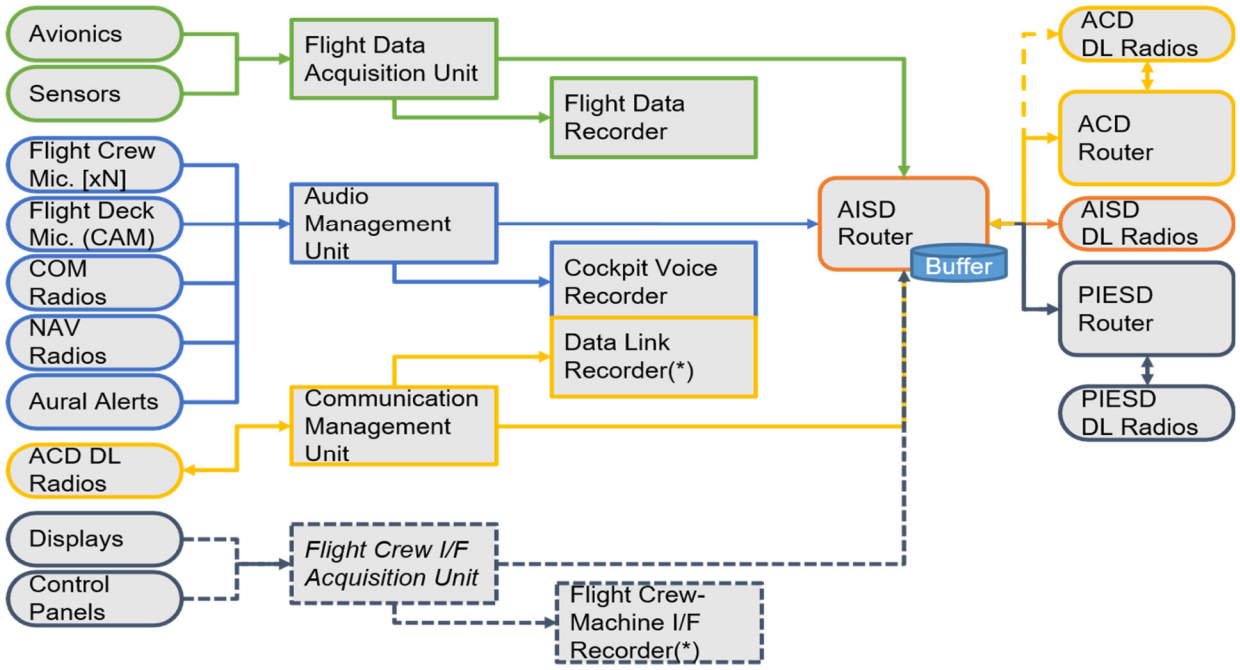

Figure 7 : Solution #1 (AISD-based) airborne system architecture

[16] The different domains are usually protected if not segregated using "firewalls" managing the exchanges between the routers.
[17] Provisions exist for instance in ARINC-791 (Mark I Aviation Ku-band and Ka-band Satellite Communication System) to allow a direct connection to the PIESD SATCOM.

Note: Power supply buses are not depicted in Figure 7 not to clutter the figure, focusing on flight recorder data flow-down between the different units. The issues related to the power supplies will be addressed in the assessment of the solution during Task 4 activities.

5.1.2 Operational Concept

5.1.2.1 Cryptographic Keys Management

Providing data confidentiality, Integrity and Authentication requires using cryptographic techniques based on the usage of Cryptographic Keys. This applies to both the security of communication channels or the encryption/signature of the data itself. These will be managed by a Public Key Infrastructure (PKI).

PKI features the possibility to perform an on-line enrollment with a Certificate Authority (CA). This avoids the need to manually load certificate on airborne device. Each device will have to follow the following steps[18]:

- Locally create a public/private key pair. The private key will be kept inside the device reducing compromising risk
- Create a Certificate Signing Request (CSR) including the public key and signed with the private key
- Post the CSR to a ground server using a communication media. The requestor will have to authenticate to the ground server.
- If the CSR is accepted, the CSR will be signed by the CA creating a valid certificate
- The remote device will regularly request ground server for its certificate
- Before the device certificate expires, the remote device will automatically submit a re-enrollment request to the ground server reducing drastically the maintenance

The QR-FRD has several objectives requiring the use of keys. As such, it is a possibility to have an independent infrastructure to serve each of them. A typical use case would be to have an independent management of the keys to digitally sign the recorded data from the one used to secure the air-ground communication (e.g. VPN or HTTPS communication). They could also be managed by different entities since they do not address the same objective.

Some keys could be managed by the airline including for example the ones used to secure the communication channel or to encrypt the QR-FRD data.

Figure 7 depicts the relationships between main actors (Aircraft, Communication Service Provider (CSP), Datalink Service Provider (DSP), Airline, AIA and PKI) involved with the QR-FRD capability, which shall be interconnected by secure communication channels.

Security measures in the architecture should include:

- Secure communication channels to protect confidentiality, integrity and availability of data communications
- Resilience of each asset to peripheral attacks
- Fail-secure degraded modes
- Security elements and measures, incl. cryptographic key management and security audits

[18] The steps listed below describe a simple and common process, that will need further refinement when implementing the PKI, especially when addressing possibilities an airline could tamper the data before distributing it to AIA. Several organizations among which the Trust Framework Study Group (TSFG) at ICAO, EUROCONTROL (European Aviation Common PKI (EACP)), FAA as well as third parties (SITA, Airbus…) are currently working on PKI management. Aircraft identity certificate management… are documented in ICAO Doc 10095 and ARINC 842.

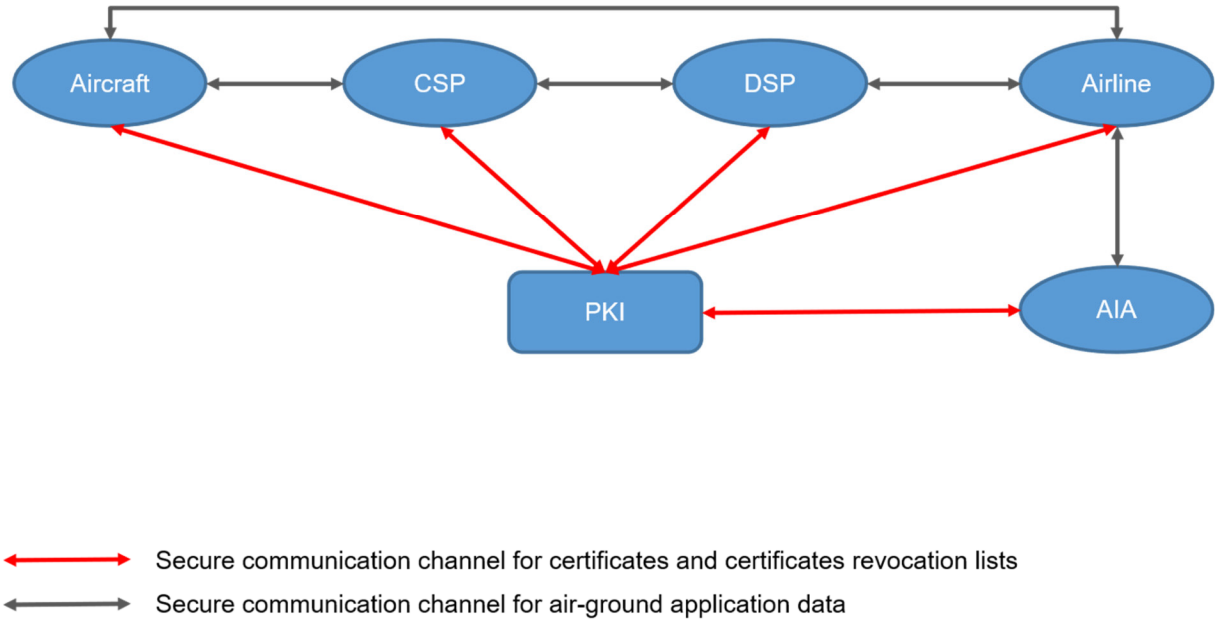

Figure 8 : Secure data transmission architecture among main actors

It is recommended when generating the PKI to make sure that the method is reproducible and iterated so missing, deleted and/or locally aborted sessions leave traces and break evidence chains.

5.1.2.2 Data Collection

Flight recorder data are processed by the Data Collection as follows:

1. Digitization: digitization will concern the up to four audio inputs (captain, first officer, passenger address, and cockpit environment) unless these are already digital as foreseen in the future.
2. Time Stamping: the different data are time stamped at the time they are collected.
3. Chunking: all data collected within the same time window (e.g. 4 seconds TBC) are recorded in the same chunk of flight recorder data records.
4. Compression: the flight recorder data records are compressed, using the same lossless compression technique or dedicated compression techniques depending on their data type to increase compression efficiency.
5. Encryption: the compressed audio records are encrypted for privacy purposes, and the related public key (cf. §5.1.2.1) is appended to the records.
6. Merging: the different flight recorder data records, compressed and possibly encrypted, are merged in a single “archive”.
7. Signature: the “archive” of flight recorder data is signed, and the related hash value and certificate (cf. §5.1.2.1) are appended to the “archive” for integrity and authenticity purposes.
8. Storage: storage of the archive will be quite limited in nominal transmission conditions, and the archive prepared to be readily available for continuous transmission of flight recorder data.

The processing flow and resulting outcomes is illustrated in Figure 8.

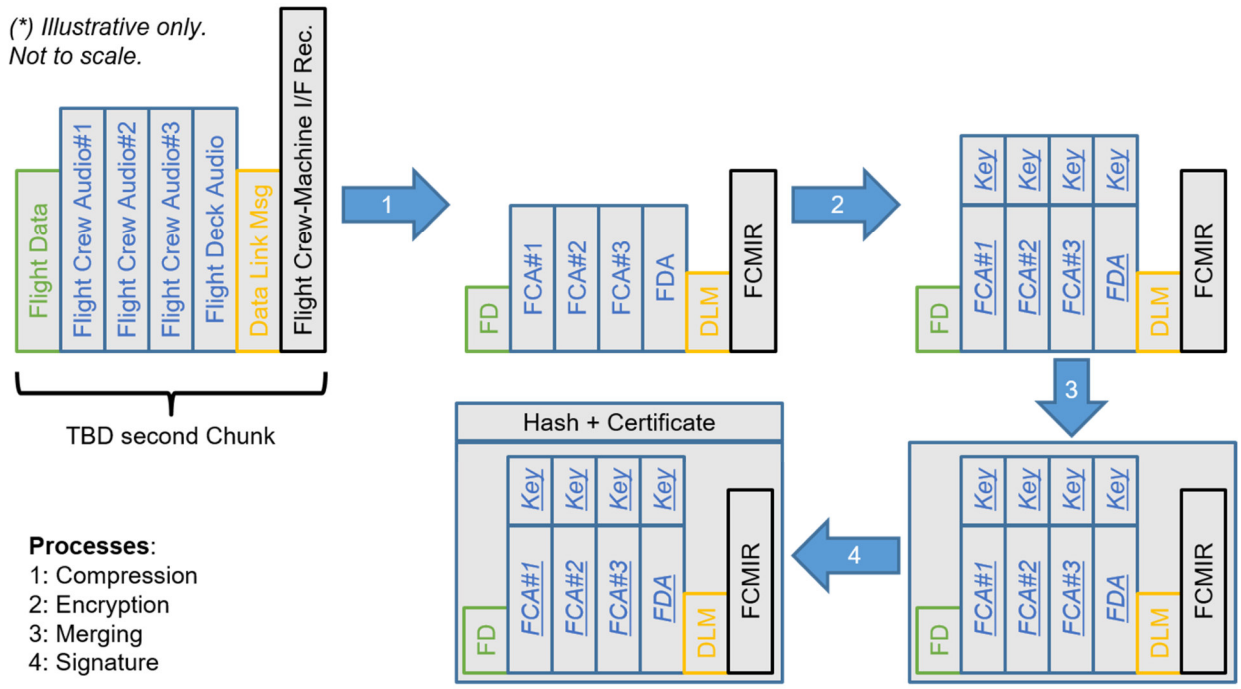

Figure 9 : Solution #1: Processing flow

Encrypting not only audio records but the whole set of flight recorder data would result in a slightly different and more conventional organization and outcome, as illustrated in Figure 9. This alternate processing flow would then be:

1. Digitization
2. Time Stamping
3. Chunking
4. Merging: the different flight recorder data records are merged in a single “archive” of a specific duration chunk.
5. Compression: the “archive” flight recorder data records is compressed using a single lossless compression technique.
6. Signature: the “archive” of flight recorder data is signed, and the related hash value and certificate (cf. §5.1.2.1) are appended to the “archive” for integrity and authenticity purposes.
7. Encryption: the signed “archive” of flight recorder data is encrypted for privacy purposes, and the related public key (cf. §5.1.2.1) is appended to the “archive”.
8. Storage

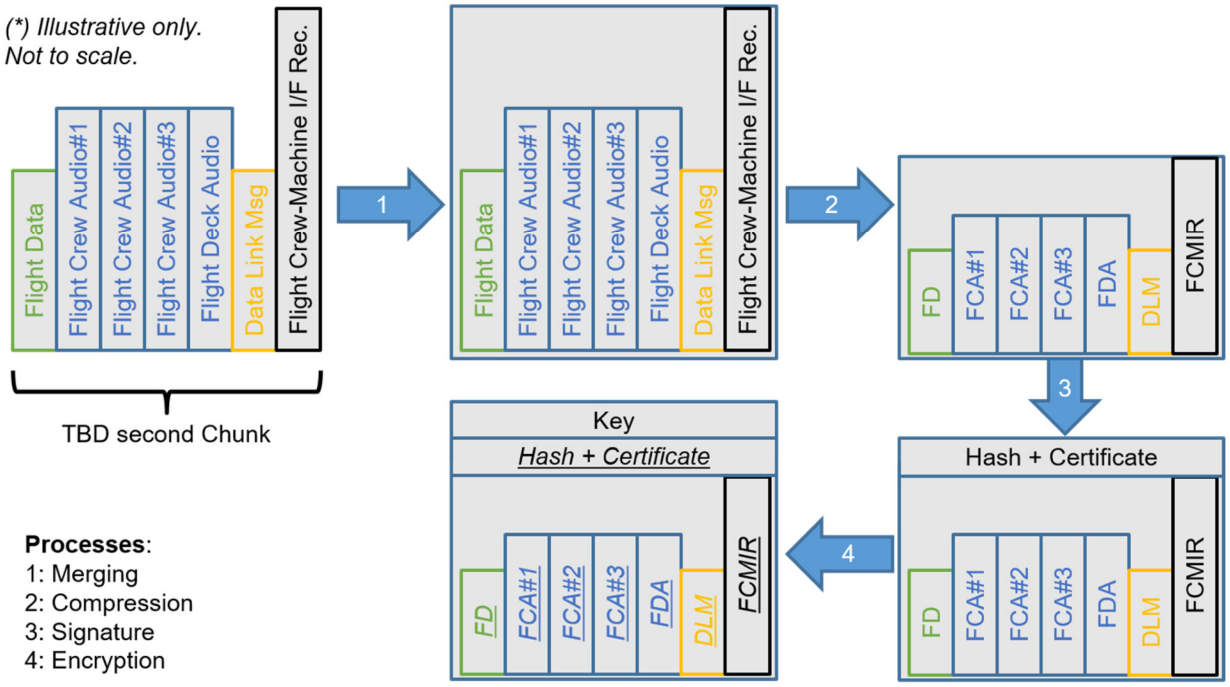

Figure 10 : Solution #1: Processing flow (alternative)

5.1.2.3 Trigger Detection

Continuous transmission of flight recorder data does not require triggers such as those discussed in §4.2.2.9 and §4.2.2.10 to be detected.

As discussed in D2 [Ref 2], transmission of flight recorder data is meant to start as soon as flight recorders start recording, if not as soon as the aircraft is powered on.

5.1.2.4 Data Transport

Continuous transmission of flight recorder data starting while the aircraft is still at the gate as recommended (cf. §5.1.2.3) will benefit from terrestrial high bandwidth communication media, typically AISD or PIESD cellular telephony (4G at the time this version of the document was drafted). Once airborne, it is likely the system will switch to high bandwidth satellite communication media, typically PIESD SATCOM.

Secure point-to-point (P2P) communications at destination of the large airline servers or a contracted organization (incl. DSP) for smaller airlines not owning secured servers themselves, using CSP/DSP services and assets to transport the data over the air and over ground networks. The overall system (incl. actors and assets (routers, servers…) is depicted Figure 10.

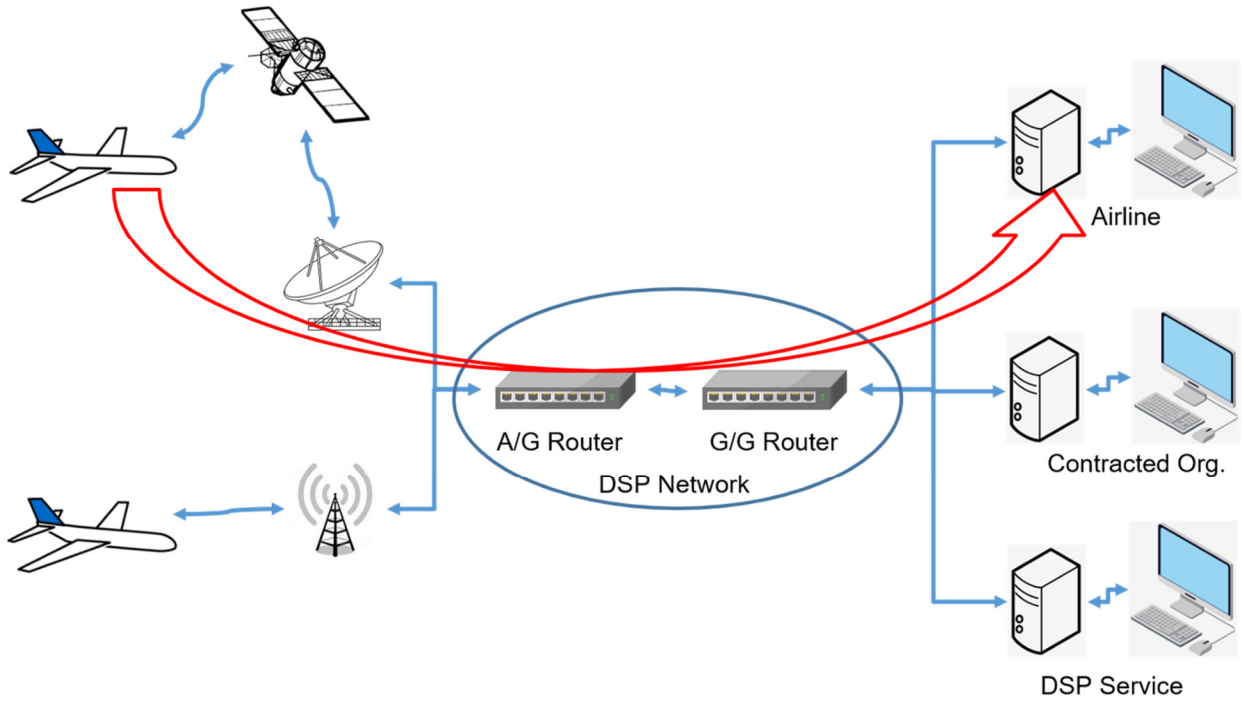

Figure 11 : Overall end-to-end system and secure point-to-point connection (example)

The secured P2P connection, “pipe”, between the AISD router and the destination server is established during the initiation of the QR-FRD capability while the aircraft is still at the gate using Internet Protocols (e.g. https/sftp). The multi-link routers being aware of the availability of the different media will use the most appropriate one, i.e. cellular if the terrestrial infrastructure exists at the airfield, SATCOM otherwise.

Figure 11 depicts point-to-point exchanges necessary to establish a secure end-to-end data exchange. Mains steps are:

1. Subnetwork establishment with log-on and secure connection establishment
2. Mobile link establishment and ground networks binding
3. Secure link establishment between end systems

Each of these steps will require a number of exchanges between the different entities hence a time budget allocated to each of these exchanges. Use of an already existing end-to-end secure connection will hence be valuable.

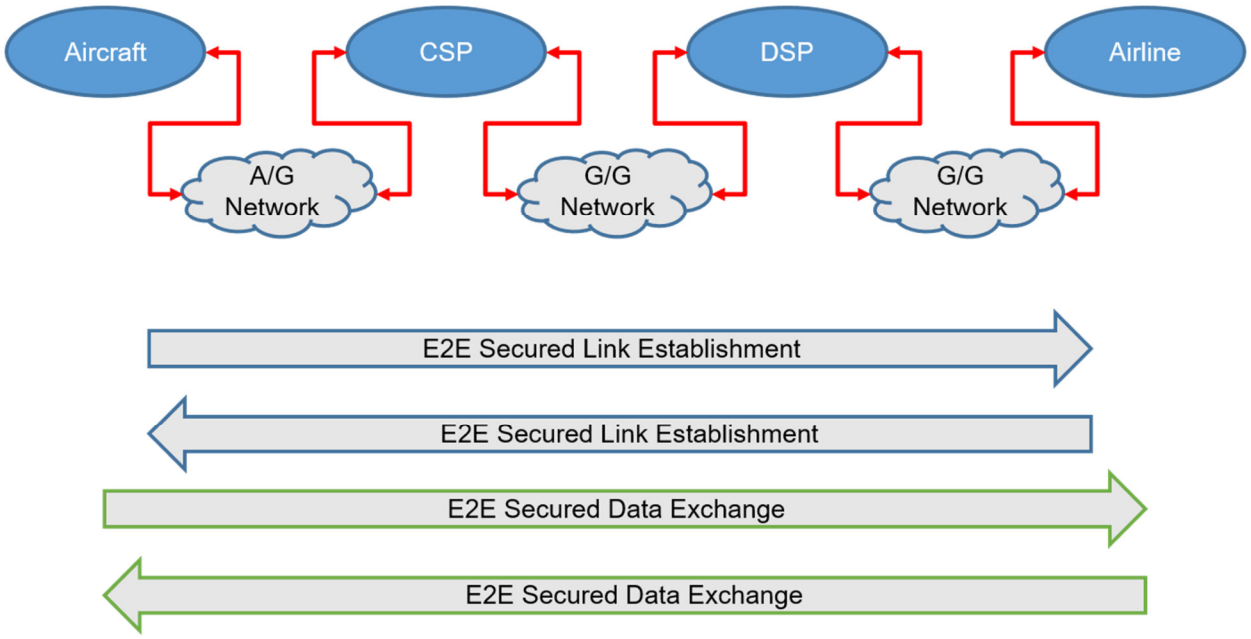

Figure 12 : : End-to-end secured link establishment and data exchange

Once the end-to-end secure connection is available, the AISD router will continuously route the prepared flight data recorder "archives" as soon as they are made available by the Data Collection function depending on a set of criteria (air/ground, availability…), directly to radios or through the PIESD router, depending on the installation.

Note: Common AISD file transfers occur one at the time, i.e. the next file is pushed for transmission once the previous transfer is successful. This will influence the size of the chunk (hence "archive") or necessitate more sophisticated preemption mechanisms in the AISD router / PIESD router /Radio chain.

Note: Should transmission conditions deteriorate and bandwidth become too limited to be shared with other applications, the AISD router may decide to increase the priority of the QR-FRD capability or halt applications of lesser priority in order to regain acceptable bandwidth.

5.1.2.5 *Off-Aircraft Storage*

The airline will store the flight recorder data as received in its own secured information infrastructure, or have it stored by contracted services (e.g. those of its DSP) likely on a secure cloud infrastructure.

The airline will define and set up necessary retention policies in place.

5.1.2.6 *Data Recovery*

The airline (or its contracted organization) will be able to recover flight data and audio recordings recorded during nominal flights for its own purposes (e.g. quality inspection and possible additional data for OFDM). Policies[19] will prevent doing so after accidents without being authorized by the investigation authorities.

After a serious incident or an accident, investigation authorities will be granted access to the flight recorder data.

[19] Policies will outline in writing the required processes and procedures adopted across the involved organizations (airline, contracted organization, accident investigation authorities…) in order to manage access rights and retrieval, retention and destruction of flight recorder data, depending on whether the flights were completed nominally or not.

It is likely a portal, along with necessary tools and credential validation, will be set in place to allow pilots to deny/allow access to all audio recordings after nominal flights to the airline (cf. §4.3.2.4). However, the accident investigation authorities will always be able to recover the audio files of a flight (using special software, key or equipment as necessary) if they have to.

Note: It is likely the designated AIA will want to process the raw flight recorder data themselves (i.e. perform the required decryption, decompression, integrity checks …) rather than getting pre-processed data from the airline. In such case, they will be provided with the necessary cryptographic keys.

5.1.3 Specificities

Specificities for Solution #1 include:

- Data linked cryptographic key management.
- Additional protection mechanisms (encryption and other) on top of each “archive”.
- Flight recorder data are stored on redundant and likely distributed servers (“virtual flight recorders”)

5.1.4 Performance Expectations

As the results from the SATCOM service providers survey cannot be communicated, a range of values is given for information in the following table.

Parameter	Min	Max
Antenna directionality (azimuth / hemisphere)	360°	360°
Typical handover duration (ms)	0	500
Worst case handover duration (seconds)	150	300
Best reception cone (from zenith)	0-45°	0-60°
Degraded reception cone (from zenith)	45° - 70°	60° - 75°
No reception cone (from zenith)	above 70°	above 75°
Reconnection duration (seconds)	4	30
Upstream throughput (Mbps)	10	50
Latency (ms)	50	1000

Table 8 : SATCOM characteristics ranges

It can be expected ”100%” of the flight recorder data be transmitted before the aircraft faces a distress situation, that ratio decreasing when excessive roll and/or pitch angles are reached, to the point of not being transmitted with extreme bank angles close to collision with the surface (provided physical integrity of the QR-FRD system components). Simulations undertaken within Task 6 will provide more accurate values in different flight conditions.

5.1.5 Limitations and Open Points

- Additional protection mechanisms (encryption and other) on top of each “archive”. Security analysis in D4/D7will tell if they are really needed
- Flight recorder data not stored on a dedicated removeable hard disk without specific intervention[20]. Analysis in D4/D7 will tell if this is an issue should physical requisition be necessary and if special policies need to be set in place.
- The organization in charge of processing and analyzing the data stored on the ground (especially AIA) should be provided with means to check if the entire received dataset is being made available. This is to avoid possible dissimulation of parts of the archive received following an accident or serious

[20] Since the flight recorder data will be stored on multiple servers likely spread in different locations, it will be impossible for investigators to get hold of the physical supports used to store the data of a specific flight without a dedicated intervention, e.g. having the requested data copied to a removable hard disk.

incident (pretending a transmission issue for instance). An option could be that the QR-FRD solution manufacturer receives the data files still encrypted instead of the operator or the AIA, and provides a copy of the data files if requested by an AIA.

5.2 Solution #2: FDAU/FDIU&ACMS and AISD router systems

5.2.1 Hardware architecture

The hardware architecture for Solution #2 is depicted Figure 12.

Note: This architecture is assumed in the context of new aircraft types for which a Combined Flight Recorder will record all data types, i.e. flight data, flight crew and flight deck audio, data link messages as well as flight crew-machine interface records. It is nevertheless also applicable in the context of legacy flight recorders (DFDR and CVR).

Note: When this document is written, the flight crew-machine interface records are not yet standardized. So in this solution, this flight crew-machine interface record data are considered as a provision. In this architecture, it is assumed the need for a unit for acquisition and formatting of these interface messages. This assumption has to be confirmed.

The onboard solution is articulated around two onboard systems:

1. FDAU/FDIU&ACMS system that will be in charge of:
   - Collecting of the various flight recorder data, compressing of these data, authenticating the data, encrypting them, and storing in a buffer.
   - Evaluating the trigger condition
2. Communication system, including the different communication routers and radios, performing the transmission of flight recorder data once triggered

The ground architecture is common with solution 1 and is not provided in the following figure.

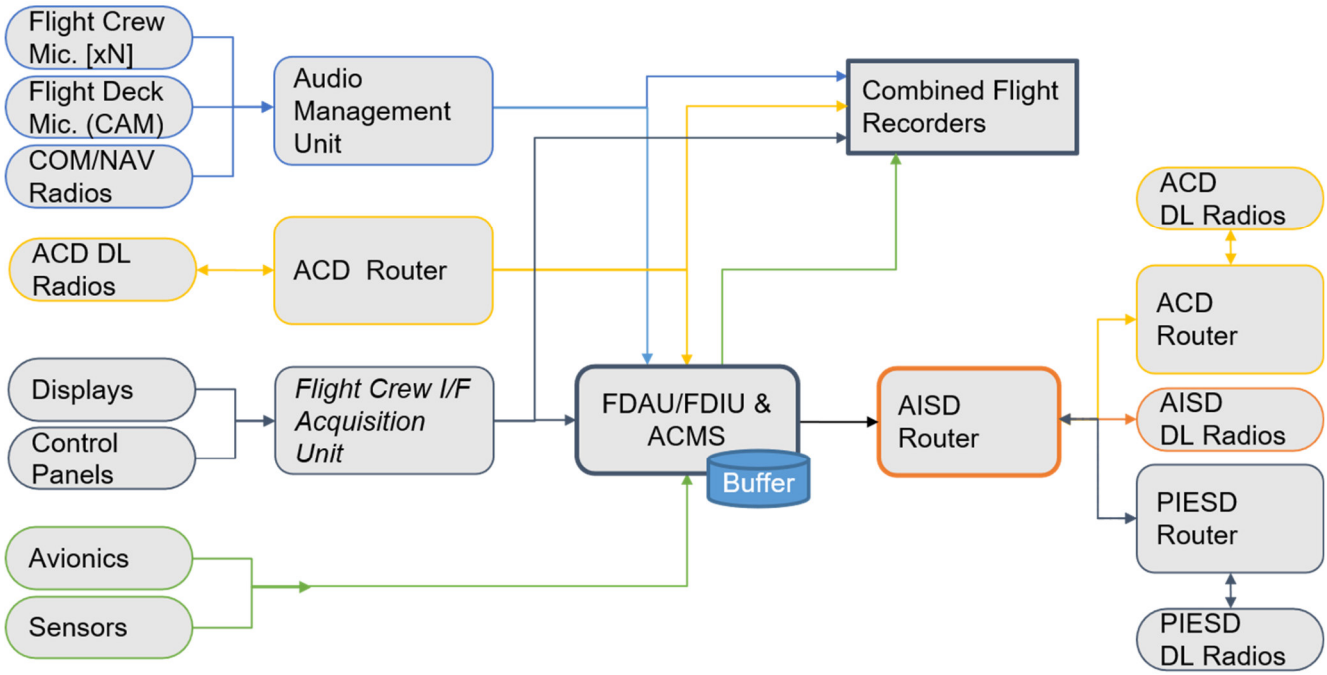

Figure 13: Solution #2 (FDAU/FDIU&ACMS-based) airborne system architecture

Note: Power supply buses are not depicted in Figure 13 not to clutter the figure, focusing on flight recorder data flow-down between the different units. The issues related to the power supplies will be addressed in the assessment of the solution during Task 4 activities.

5.2.2 Operational Concept

5.2.2.1 Cryptographic Keys Management

The following figure describes the relationships between main actors (OEM/System Provider, Airline, AIA and PKI provider) involved with the QR-FRD capability, which are actors in the cybersecurity objectives.

The characteristic of solution 2 is to secure the storage of flight recorder data: the flight recorder data is encrypted during storage in the onboard buffer. They will remain encrypted during transmission and in ground storage.

In addition, flight recorder data is authenticated when writing to the buffer. Authentication is given by a digital signature. This signature ensures that the data cannot be modified (mistakenly or maliciously). This signature guarantees that the data that will be analyzed are those recorded onboard.

The assurance of this guarantee of authenticity between the various partners (OEM, System provider, airlines, AIA) is assumed by the use of a PKI. This PKI can be managed by a third party.

Security measures in the architecture should include:

- Storage of the flight recorder data in a secure mode (signed and encrypted)
- High protections of the keys (and other assets)
- Security elements and measures, incl. cryptographic key management and security audits

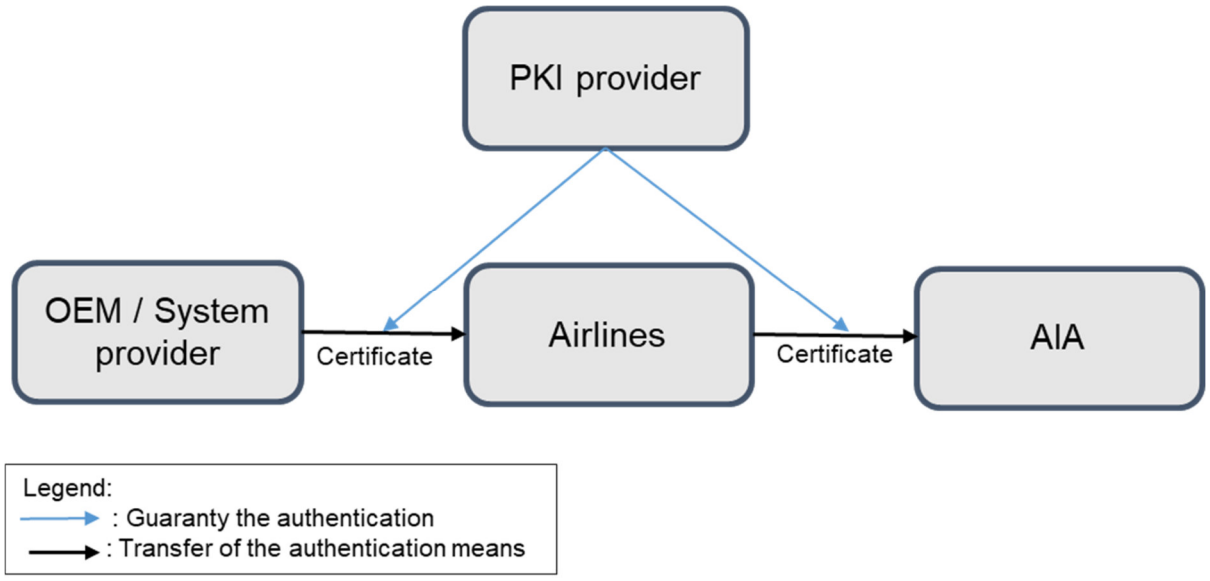

Figure 14: Cyber security main actors

Signature keys management

For the digital signature, the sequence is the following:

1. Each FDIMU/FDAMU&ACMS unit is programed in factory by a unique private key (RSA or equivalent). The unit is design with the constraint that this private key cannot be read out. Following the initialization of the unit in the factory, all copy of this private key is erased. This action can be done also by EOM on aircraft delivery, eventually on maintenance operation[21].
2. The associated public key is also stored inside the unit under certificate form. The transformation of public key to certificate uses the PKI service, which guaranty the identity
3. On flight, when a "record" is generated and compressed, it is also digitally signed, using the internal private key and the certificate
4. When it is received on ground, the signature can be checked, based on certificate and PKI, which guaranty the origin of the data

RSA/SHA256 algorithm may be a good candidate for signature.

Note: If required by future security analyses, this private key can be updated cyclically:

- Maintenance operation (based on data loading)
- Online operation (CSR protocol cf. §5.1.2.1)

Encryption key management

For this solution 2, data encryption is proposed for all recorder data[22]. The advantage of this choice is to ensure confidentiality, all time (even if the FDIU/FDAU or ACMS box is unplugged, and recorded data inside the "buffer" recovered by unauthorized people)

In this proposal, confidentiality is ensured by a symmetric ciphering.

In accordance with usual practice, the encryption key will be generated randomly. It is transmitted (encrypted) at the start of each file.

AES 128 algorithm may be a good candidate for the encryption.

5.2.2.2 Data Collection

The data collection is performed by the FDAU/FDIU&ACMS system. This function addresses the following data:

- The DFDR data (88-parameter data flow)
- The CVR data (4 audio signals)
- The ATC data link messages
- The FCMIR messages.

Note: When this document is written, the FCMIR data are not yet standardized, it is mentioned in this section as a provision to be implemented when it will be specified.

The data collection function is sequenced as following:

[21] This section is about the private key, for digital signature purpose, and not for encryption. If the unit is replaced, the signature identifies the new unit. There is no security issue. The only consideration is in case of "serious incident/accident" to inform the AIA what is the onboard unit serial number.

[22] The data encryption addresses the "buffer storage", not the "protected flight recorders storage". The protected flight recorder storage is compliant with ED 112A (and future ED 112B). In addition, the choice "encryption" or "no encryption" can be configured by the operator.

1. Acquisition: The FDR data are acquired: data, voice, data link and FCMIR. (If not yet digitalized, the audio signals are digitized inside the unit, in accordance with the performance requested by the ED-112A document [Ref 3]).
2. Chunking: all data collected within the same time window (e.g. 4 seconds TBC) are recorded in the same chunk of flight recorder data records (note this 4 seconds value can be enlarged if the compression performance is not sufficient).
3. Time Stamping: the different records are time stamped at the time of the beginning of collection.
4. Compression: The flight recorder data records are compressed, using dedicated compression techniques depending on their data type to increase compression efficiency.
5. Signature: the "archive" files of flight recorder data are signed, and the related digital signature (cf. §5.1.2.1) are appended to the "archive" for integrity and authenticity purposes.
6. Encryption: The authenticated "archive" files are encrypted for privacy purposes, and the related symmetric key, already encrypted (cf. §5.1.2.1) is appended to the records.
7. Storage: the encrypted authenticated "archive" files are stored in a buffer, using a FIFO policy (when the buffer is full, the oldest files are removed first). The size of the buffer is not critical. As a minimum, the data corresponding to the last 20 minutes are guaranteed to be memorized and to be possibly retrieved. This duration can reach 2 hours, to obtain the minimum retention time of crash recorders.

Note: As a proposal, and with the objective to reduce the volume of data to be transmitted, 3 audio signals could be merged. The pilot audio, the first officer audio and the ATC audio could be merged into a single signal, reducing the volume of data to be transferred. In that case, the CVR data are reduced to only the cabin and cockpit ambiance audio signal and the communication audio signal. This concatenation could be associated with the identification of the microphone, the source of the recorded speech. This identification would also be recorded with the speech. This proposal has to be confirmed with the AIA experts[23].

Note: In case of ARINC 767 flight data recorder configuration, the FDIU/FDAU is able to generate the same data frame than the one recorded in the flight recorder.

Note: The initial EASA request was about the transfer of the complete content of the crash recorders, i.e. 25 hours of recording. These requirements lead to such a data volume that it is not possible to find a technical solution. Following the investigation confirmed by ICAO Doc 10054-1 [Ref 5] §3.4.3.4, it seems that 20 minutes of historical data is a minimum expectation. For the first issue of this document, a buffer of minimum 20 minutes, maximum 2 hours, is taken, but it can evolve during the project, in case of new technologies becoming available.

For temporary storage in the buffer, each type of data will be recorded individually, in a separate type of record: DFDR, CVR, DLR and FCMIR. This strategy is chosen for the following reason:

- To adapt the compression algorithm to the data type, and so expect a better compression rate (less volume to transfer, better efficiency expected)
- The possibility to adapt the priority of the data type to be transmitted (referring to the data priority described in ARINC 861 document)

Note: As all acquisitions are done in the same unit, by process, data, voices, DL data and FCMIR are synchronized. Nevertheless, a "timestamp" is added to help the recovery process on ground.

[23] Indeed, accident investigation authorities are concerned with possible superposition of voice signals, difference between audio levels and settings… Investigators also use "noise" for their spectral analysis.

5.2.2.3 Trigger Detection

The trigger detection function is performed by the ACMS system. ACMS unit includes software engine to perform these detections.

In accordance with sections §4.2.2.9 and §4.2.2.10, the two types of triggers may be designed and implemented for this purpose: “Distress situation” trigger and “Abnormal situation” trigger.

The ACMS unit offers a great flexibility to define algorithm, including parameter switching, check constraints, frequency of evaluation, etc. These algorithms are reprogrammable by field loadable software (FLS), without heavy maintenance procedure, whenever an update is requested.

Note: During the first part of the project, the BEA flight data referenced in their technical document [Ref 11] have been tested, using the described triggers. The results, provided by the document, were confirmed. These trigger conditions are a good starting point but should be adapted to detect as early as possible the “distress condition” duration and, consequently more time to transmit data.

The “trigger detection” function is sequenced as following:

1. Acquisition of the aircraft parameters, identified as necessary
2. Pre-condition of aircraft parameters (Management of validity, switching process, filtering management)
3. Evaluation of conditions
4. Confirmation of conditions (based on duration)
5. Management of trigger (activation, deactivation on condition or timeout)

It is proposed the “distress trigger” to be a discrete signal, activated by the ACMS unit, used internally and by the communication system (AISD router and other)

An additional human-machine interface (HMI) command enables maintenance operator to trig a flight recorder data transmission, for regular quality check and maintenance purpose.

Note: The use of the FDR data is bound to ICAO Annex 13 and EU 996/2010, in all cases, even following spurious alerts or other non-relevant events.

5.2.2.4 Data Transport

This function is segregated between the two systems, FDIU/FDAU & ACMS system and the AISD Router:

- The FDIU/FDAU&ACMS system, which provided the files to be transferred to the ground
- The AISD router, which is responsible of the file transfer, the routing, the flow control and the acknowledge management.

When the “distress condition” is detected, the AISD router switches in distress mode, aborting the usual communication, and open an “emergency” link with a ground server.

Then, as fast as possible, the buffer content is transmitted. The buffer data are transmitted, in LIFO order (the last data added in the buffer, the first transmitted). The real time data (i.e. the data generated during the transmission of the buffer) is added on the fly into the transmission flow.

The “Data transport” function is sequenced as following:

1) On trigger, the AISD router (and other communication routers) closed all communication with ground.

2) The AISD router opens a VPN with the ground server, which is dedicated for the ground storage of the flight recorder data.

3) The AISD router reads the flight recorder data files, on the FDAU/FDIU&ACMS system, and send them using the available link. In accordance with the bandwidth allowed, several strategies can be implemented (refer to a following paragraph)

4) At each "time window" delay, new record files are generated, with updated recorder data, and must be transferred to the data stream as a priority.

5) If the trigger is deactivated, the AISD router stops the transmission, closes the VPN and restart the commercial activity.

For the transmission policy, several sequences are possible, in accordance with the available bandwidth (refer to ICAO Doc 10054-1 [Ref 5] and ARINC Project Paper 681 Draft 4)). The transmission priorities could be (cf. D2 [Ref 2]):

1) (Highest priority) DFDR parameters –Real time

2) CVR CAM – Real time

3) DFDR parameters – Historical

4) CVR Crew microphones – Real time

5) CVR (all) – Historical

6) Data link – Real time

7) Data Link – Historical

8) (Lowest priority) FCMIR data

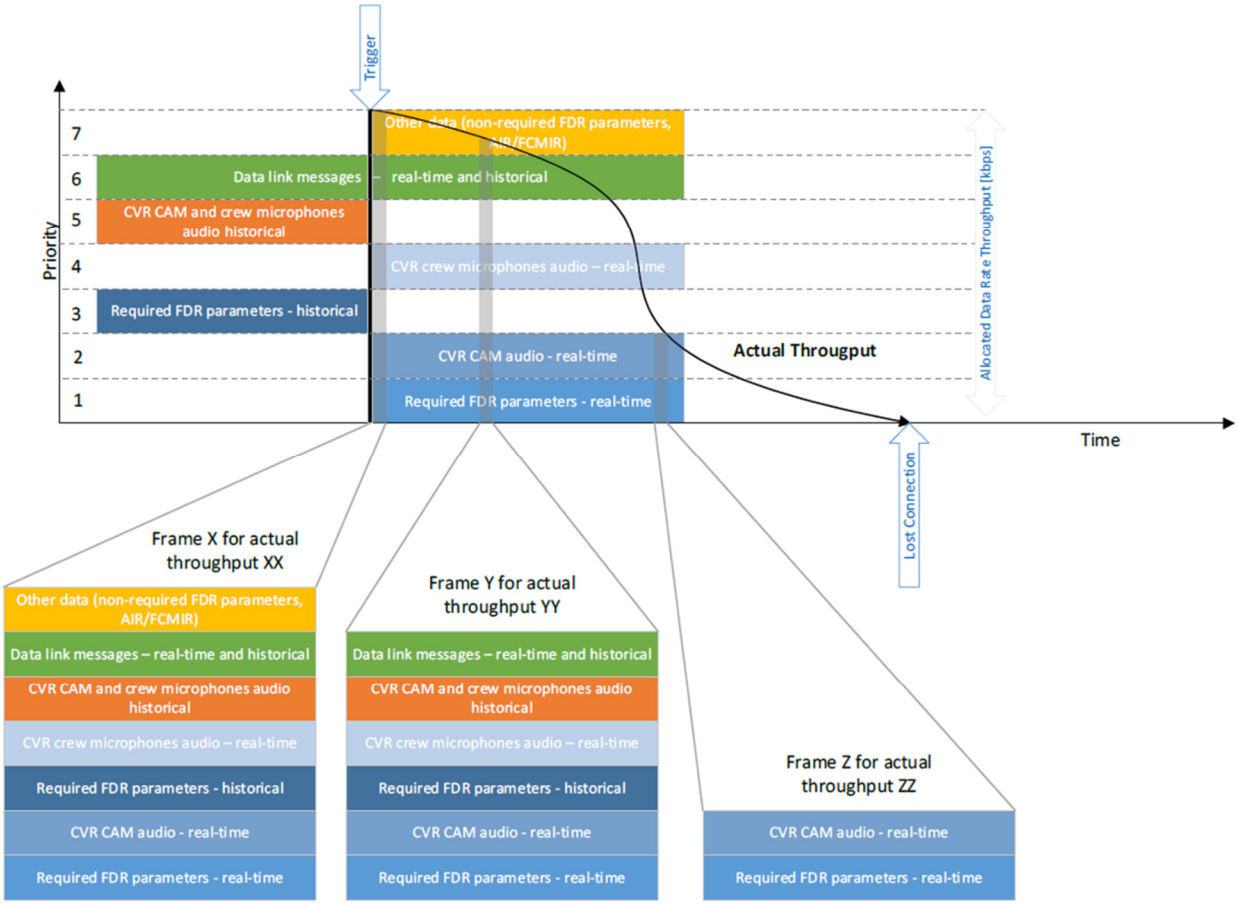

Figure 15: Example priority scheme as bandwidth diminishes (source ARINC Paper 681)

5.2.2.5 Off-Aircraft Storage

Same as for Solution #1 (cf. §5.1.2.5), except for the amount of data.

5.2.2.6 Data Recovery

Incident / Accident: Same as solution #1 (cf. §5.1.2.6).

Test/Quality inspection: Same as solution #1 (cf. §5.1.2.6).

Cryptographic keys management: different from Solution #1 counter part of §5.2.2.1

On request, the airline can provide the flight recorder data to the AIA, under two formats:

- Decoded (the un-cypher action may be under the Airline responsibility)
- Or encoded, with the "encoding symmetric key" (or means to get it)

As all files are digitally signed, AIA is able to validate the record origin (the aircraft ident) and the record time, even if the files are decoded by the Airlines.

5.2.3 Specificities

The specificities of solution 2 are the following:

- Onboard acquisition of the data, ensured on a DAL C computer, which guarantees the integrity and the synchronization of the different flight recorder data, based on development process, tests and guarantied quality assurance.
- Centralization of the acquisition of all data, which ensures:
  - Synchronization of the "data", even in case of loss of time reference.
  - Reduced latency for the buffer storage
- Use of a digital signature, which guarantees the origin of the recorded data
- Use of encryption to guarantee the non-divulgation of the recorded data (and especially the CVR data)
- Transmission on condition only, which reduces the volume of transferred data, and so the recurring price of the function

5.2.4 Performance Expectations

The following performances are expected:

- Evaluates triggers at frequencies above 1 Hz (according to the receive frequencies of the aircraft parameters), to start the transmission instead
- Reliability of the calculation of triggers (taking into account the validation of aircraft parameters)
- Reduced recurring cost of the function

5.2.5 Limitations and Open Points

One limitation has been identified, for solution 2:

- There is no theoretical guarantee that all requested data will be transmitted. The transmission time, and therefore the volume of data transmitted, will depend on the performance of the triggers and the bandwidth.

The following open points have been identified for this solution 2:

- What will be the best compression algorithms, for each data types?
- What will be the optimum size of the files to be transferred? Then the corresponding parameter: What will be the best “acquisition time windows” (refer to “chunking”)?
- The most important open point is the definition of the “distress trigger” (or “abnormal trigger”) algorithms.

The results of the modeling and simulations activities undertaken in task 6 should provide answers to the open points listed above.

Also, the organization in charge of processing and analyzing the data stored on the ground (especially AIA) should be provided with means to check if the entire received dataset is being made available. This is to avoid possible dissimulation of parts of the archive received following an accident or serious incident (pretending a transmission issue for instance). An option could be that the QR-FRD solution manufacturer receives the data files still encrypted instead of the operator or the AIA and provides a copy of the data files if requested by an AIA.

6 ANNEX A: FLIGHT DATA AND TRIGGER CONDITIONS USAGE

Table 8 below tentatively sets relationship between flight data (parameters) listed in ED-112A [Ref 3] and their possible use for the evaluation of trigger conditions, both for distress and abnormal situations (cf. §4.2.2.9 and §4.2.2.10 respectively).

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
1a Time	X[24]	X	X	X	X	X	X	X	X	X	X	X
2 Pressure altitude	-	X	-	-	-	-	-	?	X	X	-	-
3 Indicated / Calibrated airspeed	-	X	-	-	-	-	-	-	-	X	-	-
4 Heading	-	-	-	-	-	-	-	-	-	-	-	-
5 Normal acceleration	-	-	-	-	-	-	-	-	-	X	-	-
6 Pitch attitude	X	-	-	-	-	-	-	-	-	-	-	-
7 Roll attitude	X	-	-	-	-	-	-	-	-	-	-	-
8 Manual radio PTT and CVR/FDR syncho refer.	-	-	-	-	-	-	-	-	-	-	-	X
9 Engine thrust/power	-	-	-		-	-	-	-	-	-	-	-

[24] Time is necessary for each trigger condition evaluation with hysteresis at activation and deactivation at least (cf. formulas is ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION). It may also be needed to compute derivatives (e.g. rates of variation) when the parameter is not recorded.

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
9a Parameters for engine thrust determination 9b Cockpit thrust/power lever position				X -								
10 Flaps 10a Trailing edge flap position 10b Cockpit control selection	-	-	-	-	-	-	-	-	-	-	-	-
11 Slats 11a Leading edge slat position 11b Cockpit control selection	-	-	-	-	-	-	-	-	-	-	-	-
12 Thrust reverse status	-	-	-	-	-	-	-	-	-	-	-	-
13 Ground spoiler and speed brake 13a Ground spoiler position 13b Ground spoiler selection 13c Speed brake position	-	-	-	-	-	-	-	-	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
13d Speed brake selection												
14 Total or Outside Air Temperature	-	-	-	-	-	-	-	-	-	X	-	-
15 Autopilot/Autothrottle/AFCS mode and engagement status	-	-	-	-	-	-	-	-	-	-	X	-
16 Normal acceleration	-	X	-	-	-	-	-	-	-	X	-	-
17 Lateral acceleration	-	X	-	-	-	-	-	-	-	X	-	-
18 Primary flight control surface / pilot input 18a pitch axis 18b roll axis 18c yaw axis	-	-	-	-	-	-	-	-	-	-	-	-
19 Pitch trim surface position	-	-	-	-	-	-	-	-	-	-	-	-
20 Radio altitude	-	X	X	-	-	-	-	-	-	X	-	X

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
21 Vertical beam deviation 21a ILS/GPS/GLS glide path 21b MLS elevation 21c IRNAV/IAN vertical deviation	-	-	-	-	-	-	-	-	-	-	X	-
22 Horizontal beam deviation 22a ILS/GPS/GLS localizer 22b MLS azimuth 22c IRNAV/IAN lateral deviation	-	-	-	-	-	-	-	-	-	-	X	-
23 Marker beacon passage	-	-	-	-	-	-	-	-	-	-	-	-
24 Warnings	-	-	X	-	-	X	-	-	-	X	-	-
25 Each navigation receiver frequency selection	-	-	-	-	-	-	-	-	-	-	-	X
26 DME 1 and 2 distances 26a Distance to runway threshold (GLS)	-	-	-	-	-	-	-	-	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
26b Distance to missed approach point (IRNAV/IAN)												
27 Air – ground status	-	-	-	-	-	-	-	-	-	-	-	-
28 GPWS/TAWS/GCAS status 28a Selection of terrain display mode 28b Terrain alerts (cautions, warnings, advisories) 28c On/off switch position	-	-	X	-	-	-	-	-	-	-	-	-
29 Angle of attack	-	-	-	-	-	-	-	-	-	-	-	X
30 Low pressure warning 30a Hydraulic pressure 30b Pneumatic pressure	-	-	-	-	-	-	 X X	-	-	-	-	-
31 Ground speed	-	-	-	-	-	-	-	-	-	-	-	-
32 Landing gear	-	-	-	-	-	-	-	-	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
32a Landing gear position 32b Landing gear selector position												
33 Navigation data 33a Drift angle 33b Wind speed 33c Wind direction 33d Latitude / Longitude 33e GPS correction in use	-	-	-	-	-	-	-	-	-	 X X X X -	 X	-
34 Brakes 34a Left and right brake pressure 34b Left and right pedal position	-	-	-	-	-	-	-	-	-	-	-	-
35 Additional engine parameters 35a EPR	-	-	 -	-	-	-	 X	 -	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
35b N_1			X[25]				X	-				
35c Indicated vibration level			-				X	-				
35d N_2			-				X	-				
35e EGT			-				X	-				
35f Fuel flow			-				X	X				
35g Fuel cut-off lever position			-				-	-				
35h N_3			-				X	-				
35i Engine fuel metering valve position			-				-	-				
36 TCAS/ACAS status	-	-	-	-	-	-	-	-	X	-	-	-
37 Windshear warning	-	-	-	-	-	-	-	-	-	X	-	-
38 Selected barometric setting	-	-	-	-	-	-	-	-	-	-	-	X
39 Selected altitude	-	-	-	-	-	-	-	-	-	-	-	X

[25] N1 is used in “Near CFIT” trigger formulas in §ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION.

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
40 Selected speed	-	-	-	-	-	-	-	-	-	-	-	X
41 Selected Mach	-	-	-	-	-	-	-	-	-	-	-	X
42 Selected vertical speed	-	-	-	-	-	-	-	-	-	-	-	X
43 Selected heading	-	-	-	-	-	-	-	-	-	-	-	X
44 Selected flight path 44a Course / Desired Track 44b Path angle 44c Final approach path (IRNAV/IAN)	-	-	-	-	-	-	-	-	-	-	-	X
45 Selected decision height	-	-	-	-	-	-	-	-	-	-	-	X
46 EFIS display format	-	-	-	-	-	-	-	-	-	-	-	X
47 Multi-function/Engine/Alerts display format	-	-	-	-	-	-	-	-	-	-	-	X
48 AC electrical bus status	-	-	-	-	-	-	X	-	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
49 DC electrical bus status	-	-	-	-	-	-	X	-	-	-	-	-
50 Engine bleed valve position	-	-	-	-	-	-	-	-	-	-	-	-
51 APU bleed valve position	-	-	-	-	-	-	-	-	-	-	-	-
52 Computer failure	-	-	-	-	-	-	X	-	-	-	-	-
53 Engine thrust command	-	-	-	-	-	-	-	-	-	-	-	X
54 Engine thrust target	-	-	-	-	-	-	-	-	-	-	-	-
55 Computed center of gravity	-	-	-	-	-	-	-	-	-	-	-	-
56 Fuel quantity in CG trim tank	-	-	-	-	-	-	-	X	-	-	-	-
57 Head up display in used	-	-	-	-	-	-	-	-	-	-	-	-
58 Para visual display on	-	-	-	-	-	-	-	-	-	-	-	-
59 Operational stall protection, stick shaker and pusher activation	-	X	-	-	-	-	-	-	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
60 Primary navigation system reference	-	-	-	-	-	-	-	-	-	-	-	-
61 Ice detection	-	-	-	-	-	-	-	-	-	X	-	-
62 Engine warning: each engine vibration	-	-	-	-	-	-	X	-	-	-	-	-
63 Engine warning: each engine over temperature	-	-	-	-	-	-	X	-	-	-	-	-
64 Engine warning: each engine oil pressure low	-	-	-	-	-	-	X	-	-	-	-	-
65 Engine warning: each engine over speed	-	-	-	-	-	-	X	-	-	-	-	-
66 Yaw trim surface position	-	-	-	-	-	-	-	-	-	-	-	-
67 Roll trim surface position	-	-	-	-	-	-	-	-	-	-	-	-
68 Yaw or sideslip angle	-	-	-	-	-	-	-	-	-	-	-	-
69 De-icing and/or anti-icing systems selection	-	-	-	-	-	-	-	-	-	-	-	-
70 Hydraulic Pressure (each system)	-	-	-	-	-	-	X	-	-	-	-	-

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
71 Loss of cabin pressure	-	-	-	-	X	-	-	-	-	-	-	-
72 Cockpit trim control input position: pitch	-	-	-	-	-	-	-	-	-	-	-	X
73 Cockpit trim control input position: roll	-	-	-	-	-	-	-	-	-	-	-	X
74 Cockpit trim control input position: yaw	-	-	-	-	-	-	-	-	-	-	-	X
75 All cockpit flight control input forces[26]	-	-	-	-	-	-	-	-	-	-	-	-
76 Event marker	-	-	-	-	-	-	-	-	-	-	-	-
77 Date	-	-	-	-	-	-	-	-	-	-	-	-
78 ANP or EPE or EPU	-	-	-	-	-	-	-	-	-	-	X	-
79 Cabin pressure altitude	-	-	-	-	X	-	-	-	-	-	-	-
80 Aircraft computed weight	-	-	-	-	-	-	-	-	-	-	-	-

[26] This parameter may not be recorded on aircraft with fly-by-wire flight control systems (ED-112A [Ref 3]).

Parameter	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	Near MAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
81 Flight director command 81a Left flight director pitch command 81b Left flight director roll command 81c Right flight director pitch command 81d Right flight director roll command	-	-	-	-	-	-		-	-	-	-	-
82 Vertical speed	-	X	-	-	-	-		-	-	X	-	X

Table 9: Parameters and possible usage for triggers evaluation

7 ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION

This section proposes a set of generic formulas for the evaluation of triggers related to distress situations (cf. §4.2.2.9) and abnormal situations (cf. §4.2.2.10). These latter will have to be refined in a follow-on study. Both will have to be tuned to the aircraft type and actual equipage.

This section also identifies possible needs for data/information that are not part of flight data (parameters listed in ANNEX A: FLIGHT DATA AND TRIGGER CONDITIONS USAGE) or could be alternatives to flight data.

Note: Formulas for the evaluation of triggers related to distress conditions are based on those provided in BEA Tech Doc [Ref 11]. Constants proposed in BEA Tech Doc [Ref 6] are provided for illustration.

Note: Special conditions (e.g. en route, above transition altitude, N minutes after take-off, N minutes before arrival, etc.) are provided when the criteria needs to be evaluated only during specific phases of flight not to generate nuisance triggers. Information necessary to calculate the special conditions may not be part of flight data. If applicable to several criteria, these special conditions may be computed separately from the evaluation of the different criteria.

Note: It is recommended to use warning and possibly caution alerts originating from dedicated equipment (e.g. Enhanced Ground Proximity Warning System (EGPWS), Traffic Collision Avoidance System (TCAS), Flight Warning Computer (FWC)) whenever possible rather than duplicating their alerting logic for triggering transmissions.

Distress Situation	**Unusual Attitude**
Criteria	***Excessive roll angle and roll angle rate***
Equation	{ |Roll_attitude#7| > ROLL_ATT_MAX2 } OR { |Roll_attitude#7| > ROLL_ATT_MAX1 AND |Calculated_roll_rate| > ROLL_RATE_MAX }
Configuration Constants (BEA)	ROLL_ATT_MAX2 = 50° ROLL_ATT_MAX1 = 45° ROLL_RATE_MAX = 10°/s
Confirmation Time (BEA)	2 sec
Special Conditions	TBD
Criteria	***Excessive pitch angle and pitch angle rate***

Distress Situation	Unusual Attitude
Equation	{ Pitch_attitude#6 > PITCH_ATT_MAX2 } OR { Pitch_attitude#6 < PITCH_ATT_MIN2 } OR { Pitch_attitude#6 > PITCH_ATT_MAX1 AND Calculated_pitch_rate > PITCH_RATE_MAX } OR { Pitch_attitude#6 < PITCH_ATT_MIN1 AND Calculated_pitch_rate < PITCH_RATE_MIN }
Configuration Constants (BEA)	PITCH_ATT_MAX2 = 30° PITCH_ATT_MAX1 = 20° PITCH_RATE_MAX = 3°/s PITCH_ATT_MIN2 = -20° PITCH_ATT_MIN1 = -15° PITCH_RATE_MIN = -3°/s
Confirmation Time (BEA)	2 sec
Special Conditions	TBD

Table 10: Formulas for distress situation triggers: Unusual attitude

Note: Calculated_roll_rate and Calculated_pitch_rate are derived from Roll_attitude#7 and Pitch_attitude#6 respectively.

Distress Situation	Unusual Speed
Criteria	***Excessive vertical speed***
Equation	{ |Vertical_speed#82| > VERT_SPEED_MAX }
Configuration Constants (BEA)	VERT_SPEED_MAX = 9000 ft/min
Confirmation Time (BEA)	2 sec
Criteria	***Excessive normal and lateral accelerations***
Equation	{ Normall_acceleration#16 > NORM_ACC_MAX } OR { Normal_acceleration#16 < NORM_ACC_MIN } OR { |Lateral_acceleration#17| > LAT_ACC_MAX }

Configuration Constants (BEA)	NORM_ACC_MAX = 2.6 g NORM_ACC_MIN = -1.1 g LAT_ACC_MAX = 0.25 g
Confirmation Time (BEA)	2 sec
Special Conditions	TBD
Criteria	***Stall warning***
Equation	{ Stall_warning#N = TRUE }
Configuration Constants (BEA)	N/A
Confirmation Time (BEA)	1 sec
Criteria	***Inappropriate speed for the flight situation***
Equation	{ Calibrated_air_spd#3 < CAL_AIR_SPD_MIN } OR { Indicated_air_spd#3 > IND_AIR_SPD_MAX } OR { Overspeed_warning#N = TRUE AND Pressure_altitude#2 < PRESS_ALT_MIN }
Configuration Constants (BEA)	CAL_AIR_SPD_MIN = 100 kt IND_AIR_SPD_MAX = 400 kt PRESS_ALT_MIN = 15,000 ft
Confirmation Time (BEA)	2 sec
Special Conditions	TBD

Table 11: Formulas for distress situation triggers: Unusual speed

Distress Situation	**Near CFIT**
Criteria	***Terrain Avoidance and Warning System (TAWS) alerts***
Equation	{ TAWS_alert#28| = TRUE }
Configuration Constants (BEA)	N/A

Confirmation Time (BEA)	1 sec
Special Conditions	TBD
Criteria	***Inappropriate altitude for the flight situation:*** ***Poor altitude gain after take-off***
Equation	{ Radio_Altitude#7 > RADIO_ALT_MIN } AND { Radio_Altitude#7 < RADIO_ALT_MAX } AND { Engine1_N1#35 > ENG_FAN_SPD_MAX AND Engine2_N1#35 > ENG_FAN_SPD_MAX }
Configuration Constants (BEA)	RADIO_ALT_MIN = 40 ft RADIO_ALT_MAX = 100 ft ENG_FAN_SPD_MAX = 80%
Confirmation Time (BEA)	10 sec
Special Conditions	TBD

Table 12: Formulas for distress situation triggers: Collision with the surface

Distress Situation	**Total loss of thrust/propulsion on all engines**
Criteria	***Engine performance parameters indicating a loss of thrust***
Equation	For each engine: { Engine_Thrust#9 < ENG_THRUST_MIN }
Configuration Constants	ENG_THRUST_MIN = TBD
Confirmation Time	TBD sec
Special Conditions	TBD

Table 13: Formulas for distress situation triggers: Total loss of thrust on all engines

Abnormal Situation	**Cabin depressurization**
Criteria	***Loss of cabin pressure alert***
Equation	{ Loss_Cabin_Pressure#71 = TRUE }
Configuration Constants	N/A
Confirmation Time	10 sec (BEA)
Special Conditions	TBD
Criteria	***Abnormal value of cabin pressure altitude***
Equation	{ Cabin_Pressure_Altitude #79 > CAB_PRES_ALT_MAX }
Configuration Constants	CAB_PRES_ALT_MAX = 10,000 ft (TBC)
Confirmation Time	5 (TBC) min
Special Conditions	TBD

Table 14: Formulas for abnormal situation triggers: Cabin depressurization

Abnormal Situation	**Fire on board the aircraft**
Criteria	***Fire on board alert***
Equation	{ Warnings#24 = FIRE_ALERT } OR { Warnings#24 = SMOKE_ALERT }
Configuration Constants	N/A
Confirmation Time	2 (TBC) minutes[27]
Special Conditions	TBD

[27] The authors propose that "quite long" duration due to sensors reliability issues.

Table 15: Formulas for abnormal situation triggers: Fire on board the aircraft

Abnormal Situation	**Aircraft system failure or malfunction**
Criteria	***Abnormal engine parameters***
Equation	For each engine: { Engine_Pressure_Ratio#35 > ENG_PRESS_RATIO_MAX } OR { Engine_Indicated_Vibration_Level #35 > ENG_VIBR_LEVEL_MAX }
Configuration Constants	ENG_PRESS_RATIO_MAX = TBD ENG_VIBR_LEVEL_MAX = TBD
Confirmation Time	TBD sec
Special Conditions	TBD
Criteria	***Engine alerts***
Equation	For each engine: { Engine_Vibration_Warning#62 = TRUE } OR { Engine_Overtemperature_Warning#63 = TRUE } OR { Engine_Oil_Pressure_Low_Warning#64 = TRUE } OR { Engine_Overspeed_Warning#65 = TRUE }
Configuration Constants	NA
Confirmation Time	TBD min
Special Conditions	TBD
Criteria	***Low pressure warning***
Equation	{ Low_Hydraulic_Pressure_Warning#30 = TRUE } OR { Low_Pneumatic_Pressure_Warning#30 = TRUE }
Configuration Constants	NA
Confirmation Time	TBD min

Special Conditions	TBD
Criteria	***Electrical bus failure indications***
Equation	{ AC_Electrical_Bus_Status#48 = FAIL } OR { DC_Electrical_Bus_Status#49 = FAIL }
Configuration Constants	NA
Confirmation Time	TBD min
Special Conditions	TBD
Criteria	***Computer failure***
Equation	{ Computer_Failure#52 = TRUE }
Configuration Constants	NA
Confirmation Time	TBD min
Special Conditions	TBD

Table 16: Formulas for abnormal situation triggers: Aircraft component failure or malfunction

Abnormal Situation	**Low fuel or fuel system anomaly**
Criteria	***Abnormal values of fuel quantities for the flight situation***
Equation	{ Fuel_Quantity_CG_Trim_Tank#56 < FUEL_QTY_CG_TANK_MIN }
Configuration Constants	FUEL_QTY_CG_TANK_MIN
Confirmation Time	TBD sec
Special Conditions	TBD
Criteria	***Fuel Exhaustion***
Equation	TBD

Configuration Constants	TBD
Confirmation Time	TBD
Special Conditions	TBD
Criteria	***Fuel Starvation***
Equation	TBD
Configuration Constants	TBD
Confirmation Time	TBD
Special Conditions	TBD

Table 17: Formulas for abnormal situation triggers: Shortage of fuel

Abnormal Situation	**NMAC**
Criteria	***Airborne Collision Avoidance System (ACAS) alerts***
Equation	{ TCAS_ACAS_Status#36 = ACAS_RA }
Configuration Constants	ACAS_RA
Confirmation Time	1 sec (BEA)[28]
Special Conditions	TBD

Table 18: Formulas for abnormal situation triggers: Flight situations that could lead to collision with other traffic

Abnormal Situation	**Possible penetration of severe weather**
Criteria	***Wind shear alert***

[28] This duration looks inappropriate to consortium members. To be discussed/refined.

Equation	{ Windshear_Warning#37 = TRUE }
Configuration Constants	N/A
Confirmation Time	TBD sec
Special Conditions	TBD
Criteria	***Turbulence alert***
Equation	{ TBD = TRUE }
Configuration Constants	N/A
Confirmation Time	TBD sec
Special Conditions	TBD

Table 19: Formulas for abnormal situation triggers: Flight situations that could lead to penetration of adverse weather

Note: Additional weather alerts or analysis related to thunderstorms for instance will require further studies. Weather radar image processing for instance does not seem practical. The QR-FRD capability is likely to evolve based on onboard weather detection capabilities evolutions.

Abnormal Situation	**Deviation from planned flight path**
Criteria	***Abnormal values of cross-track error or estimated time of arrival***
Equation	**Note**: This is a placeholder as the formulation would need further investigations. It is not certain the ANP_EPE-EPU#78 parameter would be sufficient. It is likely FMS inputs would be necessary. TBD
Configuration Constants	TBD
Confirmation Time	TBD
Special Conditions	TBD

Table 20: Formulas for abnormal situation triggers: Deviation from planned flight path

Abnormal Situation	Flight crew incapacitation
Criteria	**Note**: This is a placeholder as the criteria definition and formulation would need further investigations. R&D projects are tackling the topic. The QR-FRD study and deliverable could be revisited based on the outcomes of these projects.
Equation	TBD
Configuration Constants	TBD
Confirmation Time	TBD
Special Conditions	TBD

Table 21: Formulas for abnormal situation triggers: Flight crew incapacitation

8 ANNEX C: FLIGHT WARNING SYSTEM

A simplified flight warning system architecture is depicted Figure 16 for illustration purposes. Actual system installations are dual-redundant.

The Flight Warning Computer (FWC) presents failures and status information on electronic centralized aircraft monitoring (ECAM) display units. It also gives the visual (Master Warning and Master Caution) and aural (alarm sound and synthetic voice call outs) triggers to the flight crew.

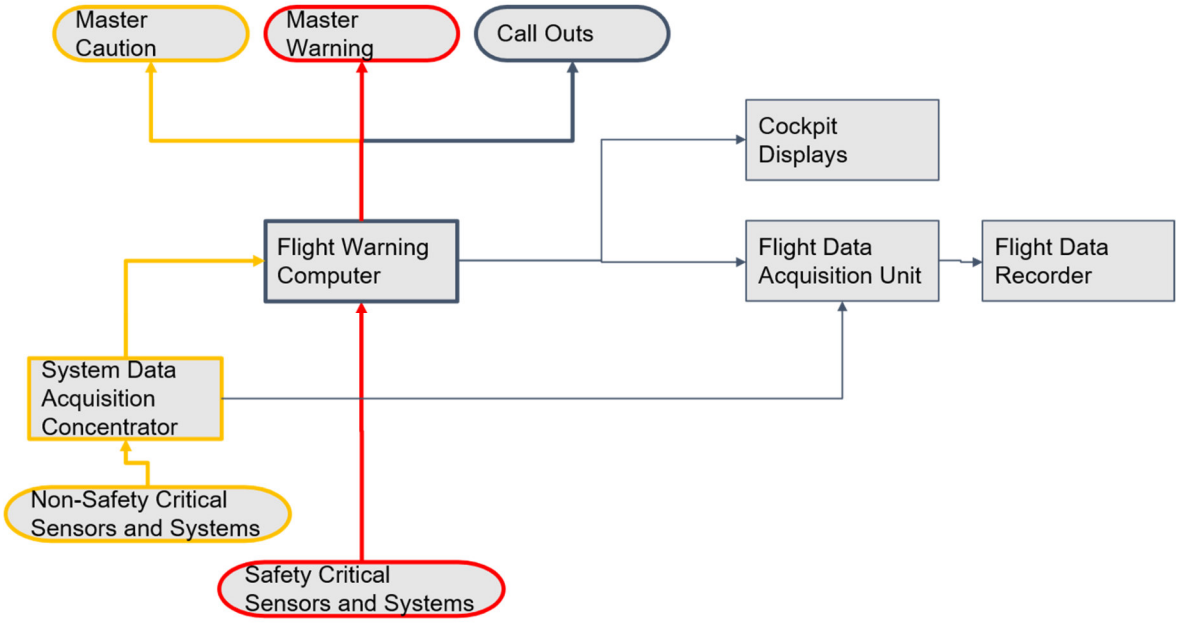

Figure 16: Simplified Flight Warning System (FWS) system architecture

The FWC typically generates alert messages, aural alerts, and synthetic voice messages for data it acquires:

- Directly from safety critical sensors and systems to generate “red” warnings alerts. These latter require immediate corrective action from the flight crew being made aware of dangerous aircraft configurations (e.g. flap/slat/trim settings), limit flight conditions (e.g. stall, overspeed…) or system failures altering the safety of the flight (e.g. engine fire, cabin depressurization…)
- Through the System Data Acquisition Concentrator (SDAC) for non-safety critical sensors and systems to generate “amber” caution alerts. These latter do not require immediate action from the flight crew being made aware of system failures with no direct consequence on the safety of the flight (e.g. hydraulic system failure…). However, these caution alerts should be considered by the flight crew without delay, time and situation permitting, to prevent any further degradation of the affected system.

Besides the master caution and master warning lights, as well as call outs, the FWC also generates alert messages displayed on cockpit displays (ECAM display).

The SDAC and FWC, among other avionics systems, feed the Flight Data Acquisition Unit (FDAU) with parameters, incl alerts, to be recorded by the Flight Data Recorder (FDR).

The FWC manages alerts depending on flight phases and flight conditions and observes priority levels for warning alerts and caution alerts, warning alerts having priority over caution alerts.

- “Red” warning alerts would typically include (ref. miscellaneous aircraft ATA-31 Indicating and Reporting Systems documents): ACAS warnings (TCAS RA)
- Stall warning
- Windshear warning
- Overspeed alert
- Fire alerts
- TAWS warnings
- Cabin pressure warnings
- FWC warnings (auto-pilot, engine oil pressure, …)

“Amber” caution alerts would typically include (ref. miscellaneous aircraft ATA-31 Indicating and Reporting Systems documents):

- TAWS cautions
- ACAS cautions
- FWC cautions (altitude, speed, auto-throttle, flaps, gear…)

9 ANNEX D: ACCIDENTS CATEGORIES vs TRIGGER CONDITIONS

In continuity of the matrix provided in D1 [Ref 1], "Accident categories (CICTT) and possible factors affecting wireless transmission", the table below presents a possible relationship between accident categories (2010-2019) and the trigger conditions defined in §4.2.2.9 and §4.2.2.10).

Accident Categories (CCICTT)	Unusual Attitude	Unusual speed	Near CFIT	Total Loss of thrust/propulsion	Cabin depressurization	Fire on board the aircraft	Aircraft system failure or malfunction	Low fuel or fuel system anomaly	NMAC	Possible penetration of severe weather	Deviation from planned flight path	Flight crew incapacitation
CFIT (Controlled Flight Into Terrain)			X								(X)	(X)
F-NI (Fire/Smoke – Non Impact)						X						
FUEL (Fuel related)								X				
ICE (Icing)										X		
LOC-I (Loss of Control - In flight)	X	X	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)
MAC (Mid-Air Collision)									X			
SCF-NP (System/Component Failure – Non Power plant)							X					
SCF-PP (System/Component Failure – Power plant)				X			(X)					
WSTRW (Windshear or Thunderstorm)										X[29]		

Table 22: Relationship between accident categories and trigger conditions

Note: LOC-I (Loss of Control - In flight) may result from all other accident categories listed in the table (cf. D1 [Ref 1]).

[29] Partially. A trigger condition for Windshear is exists, but not for Thunderstorm per se. It is indeed difficult to evaluate as discussed in "ANNEX B: FORMULAS FOR TRIGGER CONDITIONS EVALUATION". Further study will be necessary to address trigger conditions for Thunderstorm, using side effects for instance or advanced weather radar alerts.

10 ANNEX E: EU SAFETY OCCURENCES vs TRIGGER CONDITIONS

The Commission Implementing Regulation (EU) 2015/1018 [Ref 12] lays down a list classifying occurrences in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation.

Its Annex I (Occurrences Related To The Operation Of The Aircraft) and III (Occurrences Related To Air Navigation Services And Facilities) are structured in such a way that the pertinent occurrences are linked with categories of activities during which they are normally observed, according to experience, in order to facilitate the reporting of those occurrences. As such, they were considered within the QR-FRD study as a relevant taxonomy for incident, serious incidents (and accident, the difference between an accident and a serious incident lying only in the result (cf. ICAO Annex 13 [Ref 8]).

The following table, based on those annexes, tentatively associates trigger conditions and "triggering systems", to occurrences relevant for the scope of the QR-FRD study.

Occurrence	Identified Trigger	D3
OCCURRENCES RELATED TO THE OPERATION OF THE AIRCRAFT (Annex I)		
1. AIR OPERATIONS		
1.1. Flight preparation		
(1) Use of incorrect data or erroneous entries into equipment used for navigation or performance calculations which has or could have endangered the aircraft, its occupants or any other person.	NA	NA
(2) Carriage or attempted carriage of dangerous goods in contravention of applicable legislations including incorrect labelling, packaging and handling of dangerous goods.	NA	NA
1.2. Aircraft preparation		
(1) Incorrect fuel type or contaminated fuel.	NA	NA
(2) Missing, incorrect or inadequate De-icing/Anti-icing treatment.	NA	NA
1.3. Take-off and landing		
(1) Taxiway or runway excursion.	RAAS/ROPS[30]	Near CFIT
(2) Actual or potential taxiway or runway incursion.	RAAS/ROPS	NA
(3) Final Approach and Take-off Area (FATO) incursion.	RAAS	NA
(4) Any rejected take-off.	NA	NA
(5) Inability to achieve required or expected performance during take-off, go-around or landing.	TAWS (GPWS)	Unusual attitude and/or speed
(6) Actual or attempted take-off, approach or landing with incorrect configuration setting.	FWC (TO Conf) TAWS (EGPWS)	Near CFIT
(7) Tail, blade/wingtip or nacelle strike during take-off or landing.	None	Near CFIT
(8) Approach continued against air operator stabilized approach criteria.	TAWS (EGPWS) RAAS/ROPS	Near CFIT
(9) Continuation of an instrument approach below published minimums with inadequate visual references.	None	NA
(10) Precautionary or forced landing.	None	NA
(11) Short and long landing.	None	NA
(12) Hard landing.	NA	NA
1.4. Any phase of flight		
(1) Loss of control.	FWC TAWS (GPWS) BEA Algo	Unusual attitude and/or speed
(2) Aircraft upset, exceeding normal pitch attitude, bank angle or airspeed inappropriate for the conditions.	FWC TAWS (GPWS) BEA Algo	Unusual attitude and/or speed
(3) Level bust.	None	-

[30] Runway Awareness and Advisory System (RAAS) and Runway Overrun Prevention System (ROPS) are optional onboard aircraft.

Occurrence	Identified Trigger	D3
(4) Activation of any flight envelope protection, including stall warning, stick shaker, stick pusher and automatic protections.	FWC TAWS (GPWS) BEA Algo	Unusual attitude and/or speed
(5) Unintentional deviation from intended or assigned track of the lowest of twice the required navigation performance or 10 nautical miles.	None	Deviation from flight path
(6) Exceedance of aircraft flight manual limitation.	FWC TAWS (GPWS) BEA Algo	Unusual attitude and/or speed
(7) Operation with incorrect altimeter setting.	None	-
(8) Jet blast or rotor and prop wash occurrences which have or could have endangered the aircraft, its occupants or any other person.	NA	NA
(9) Misinterpretation of automation mode or of any flight deck information provided to the flight crew which has or could have endangered the aircraft, its occupants or any other person.	None	-
1.5. Other types of occurrences		
(1) Unintentional release of cargo or other externally carried equipment.	NA	NA
(2) Loss of situational awareness (including environmental, mode and system awareness, spatial disorientation, and time horizon).	None	-
(3) Any occurrence where the human performance has directly contributed to or could have contributed to an accident or a serious incident.	None	Flight crew incapacitation
2. TECHNICAL OCCURRENCES		
2.1. Structure and systems		
(1) Loss of any part of the aircraft structure in flight.	None	-
(2) Loss of a system.	FWC	Aircraft system failure
(3) Loss of redundancy of a system.	FWC	Aircraft system failure
(4) Leakage of any fluid which resulted in a fire hazard or possible hazardous contamination of aircraft structure, systems or equipment, or which has or could have endangered the aircraft, its occupants or any other person.	None	-
(5) Fuel system malfunctions or defects, which had an effect on fuel supply and/or distribution.	FWC	Low fuel or fuel system anomaly
(6) Malfunction or defect of any indication system when this results in misleading indications to the crew.	None	-
(7) Abnormal functioning of flight controls such as asymmetric or stuck/jammed flight controls (for example: lift (flaps/slats), drag (spoilers), attitude control (ailerons, elevators, rudder) devices).	FWC	Aircraft system malfunction
2.2. Propulsion (including engines, propellers and rotor systems) and auxiliary power units (APUs)		
(1) Failure or significant malfunction of any part or controlling of a propeller, rotor or powerplant.	FWC	Total loss of thrust/propulsion
(2) Damage to or failure of main/tail rotor or transmission and/or equivalent systems.	NA	NA
(3) Flameout, in-flight shutdown of any engine or APU when required (for example: ETOPS (Extended range Twin engine aircraft Operations), MEL (Minimum Equipment List)).	None	-
(4) Engine operating limitation exceedance, including overspeed or inability to control the speed of any high-speed rotating component (for example: APU, air starter, air cycle machine, air turbine motor, propeller or rotor).	FWC	Aircraft system malfunction
(5) Failure or malfunction of any part of an engine, powerplant, APU or transmission resulting in any one or more of the following: (a) thrust-reversing system failing to operate as commanded; (b) inability to control power, thrust or rpm (revolutions per minute); (c) non-containment of components/debris.	None	Aircraft system malfunction

Occurrence	Identified Trigger	D3
3. INTERACTION WITH AIR NAVIGATION SERVICES (ANS) AND AIR TRAFFIC MANAGEMENT (ATM)		
(1) Unsafe ATC (Air Traffic Control) clearance.	None	-
(2) Prolonged loss of communication with ATS (Air Traffic Service) or ATM Unit.	None	-
(3) Conflicting instructions from different ATS Units potentially leading to a loss of separation.	None	-
(4) Misinterpretation of radio-communication which has or could have endangered the aircraft, its occupants or any other person.	None	-
(5) Intentional deviation from ATC instruction which has or could have endangered the aircraft, its occupants or any other person.	None	-
4. EMERGENCIES AND OTHER CRITICAL SITUATIONS		
(1) Any event leading to the declaration of an emergency ('Mayday' or 'PAN call').	XPDR (7700 squawk)	-
(2) Any burning, melting, smoke, fumes, arcing, overheating, fire or explosion.	FWC	Fire on board the aircraft
(3) Contaminated air in the cockpit or in the passenger compartment which has or could have endangered the aircraft, its occupants or any other person.	None	-
(4) Failure to apply the correct non-normal or emergency procedure by the flight or cabin crew to deal with an emergency.	None	-
(5) Use of any emergency equipment or non-normal procedure affecting in-flight or landing performance.	None	-
(6) Failure of any emergency or rescue system or equipment which has or could have endangered the aircraft, its occupants or any other person.	None	-
(7) Uncontrollable cabin pressure.	FWC	Cabin depressurization
(8) Critically low fuel quantity or fuel quantity at destination below required final reserve fuel.	FWC	Low fuel or fuel system anomaly
(9) Any use of crew oxygen system by the crew.	None	-
(10) Incapacitation of any member of the flight or cabin crew that results in the reduction below the minimum certified crew complement.	None (PHM)	Flight crew incapacitation
(11) Crew fatigue impacting or potentially impacting their ability to perform safely their flight duties.	None (PHM)	Flight crew incapacitation
5. EXTERNAL ENVIRONMENT AND METEOROLOGY		
(1) A collision or a near collision on the ground or in the air, with another aircraft, terrain or obstacle[31].	TAWS ACAS	Near CFIT or NMAC
(2) ACAS RA (Airborne Collision Avoidance System, Resolution Advisory).	ACAS	NMAC
(3) Activation of genuine ground collision system such as GPWS (Ground Proximity Warning System)/TAWS (Terrain Awareness and Warning System) 'warning'.	TAWS (GPWS)	Near CFIT
(4) Wildlife strike including bird strike.	None	-
(5) Foreign object damage/debris (FOD).	None	-
(6) Unexpected encounter of poor runway surface conditions.	None	-
(7) Wake-turbulence encounters.	None	-
(8) Interference with the aircraft by firearms, fireworks, flying kites, laser illumination, high powered lights, lasers, Remotely Piloted Aircraft Systems, model aircraft or by similar means.	None[32]	-
(9) A lightning strike which resulted in damage to the aircraft or loss or malfunction of any aircraft system.	FWC	Aircraft system malfunction/failure
(10) A hail encounter which resulted in damage to the aircraft or loss or malfunction of any aircraft system.	FWC	Aircraft system malfunction/failure

[31] Obstacle includes vehicle.

[32] Assuming RPAS means small drones equipped with electronic conspicuity devices at most. IFR capable ones would be transponder equipped.

Occurrence	Identified Trigger	D3
(11) Severe turbulence encounter or any encounter resulting in injury to occupants or deemed to require a 'turbulence check' of the aircraft.	BEA calc (Normal accelerations)	Penetration of severe weather
(12) A significant wind shear or thunderstorm encounter which has or could have endangered the aircraft, its occupants or any other person.	PWS (<2,500 ft)	Penetration of severe weather
(13) Icing encounter resulting in handling difficulties, damage to the aircraft or loss or malfunction of any aircraft system.	None	Penetration of severe weather
(14) Volcanic ash encounter.	None	-
6. SECURITY		
(1) Bomb threat or hijack.	Out of Scope	-
(2) Difficulty in controlling intoxicated, violent or unruly passengers.	Out of Scope	-
(3) Discovery of a stowaway.	Out of Scope	-
OCCURRENCES RELATED TO AIR NAVIGATION SERVICES AND FACILITIES (Annex III)		
1. AIRCRAFT-RELATED OCCURRENCES		
(1) A collision or a near collision on the ground or in the air, between an aircraft and another aircraft, terrain or obstacle[33], including near-controlled flight into terrain (near CFIT).	ACAS TAWS	NMAC Near CFIT
(2) Separation minima infringement[34].	ACAS	NMAC
(3) Inadequate separation[35].	ACAS	NMAC
(4) ACAS RAs.	ACAS	NMAC
(5) Wildlife strike including bird strike.	None	-
(6) Taxiway or runway excursion.	ROPS	Near CFIT
(7) Actual or potential taxiway or runway incursion.	RAAS	Out of scope
(8) Final Approach and Take-off Area (FATO) incursion.	NA	Out of Scope
(9) Aircraft deviation from ATC clearance.	None	Deviation from flight path
(10) Aircraft deviation from applicable air traffic management (ATM) regulation: (a) aircraft deviation from applicable published ATM procedures; (b) airspace infringement including unauthorized penetration of airspace; (c) deviation from aircraft ATM-related equipment carriage and operations, as mandated by applicable regulations.	None	-
(11) Call sign confusion related occurrences.	None	-
2. DEGRADATION OR TOTAL LOSS OF SERVICES OR FUNCTIONS		
3. OTHER OCCURRENCES		

Table 23: Relationship between occurrences and trigger conditions

[33] Obstacle includes vehicle.
[34] This refers to a situation in which prescribed separation minima were not maintained between aircraft or between aircraft and airspace to which separation minima is prescribed.
[35] In the absence of prescribed separation minima, a situation in which aircraft were perceived to pass too close to each other for pilots to ensure safe separation.

---- end of document ----

European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3
50668 Cologne
Germany

Mail EASA.research@easa.europa.eu
Web www.easa.europa.eu

An Agency of the European Union