SESAR Solution #118 - Final SPR-INTEROP/OSED V3 - Part II - Safety Assessment Report

Topic:	**ATM Operations**
Edition Date:	**15 May 2018**
Edition:	**01.00.01**

SESAR JOINT UNDERTAKING

Authoring & Approval

Authors of the document

Name/Beneficiary	Position/Title	Date
[redacted] DSNA	[redacted]	
[redacted] DSNA		
[redacted] DSNA		28/02/2018

Reviewers internal to the project

Name/Beneficiary	Position/Title	Date
[redacted] /DSNA	[redacted]	03/05/2018

Approved for submission to the SJU By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date
[redacted] DSNA	[redacted]	15/05/2018

Rejected By - Representatives of beneficiaries involved in the project

Name/Beneficiary	Position/Title	Date

Document History

Edition	Date	Status	Author	Justification
01.00.00	28/02/2018	Draft	[redacted]	
01.00.01	15/05/2018	Final		

BASIC EXTENDED ATC PLANNING FUNCTION

Abstract

This document is the final version of the SAR for **Solution #118 - Basic EAP (Extended ATC Planning) function** at V3 level.

The basic EAP (*b*EAP) function concept describes an **automated tool supporting the basic communication** between the Local DCB position and the Controllers' Work Positions to be deployed in En-route operating environments of **Medium** and **High complexity**.

The basic EAP function is expected to facilitate the implementation of ATFCM measures to better match capacity to predicted demand and to reduce the complexity of traffic presentation in order to suit available capacity.

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This assessment allows definition of Safety Criteria for the change involved by the Solution and supports derivation of Safety Requirements so that the concept design is capable to meet the Safety Criteria.

The requirements from this document have been defined from

- The results of the VP687 validation exercise, focusing on initial EAP experimentation in French Reims ACC.
- The feedback from the experimentation/implementation project 4Me in French Reims ACC.

In addition, these requirements have been reviewed by bEAP operational and technical experts in order to ensure their realism (i.e. ability to be satisfied in a typical implementation in hardware, software, people and procedures) and testability (i.e. satisfaction can be demonstrated by direct means- e.g. testing- or, where applicable, indirectly through appropriate assurance processes).

All the assumptions made during the analysis have been logged.

Whenever it has not been possible to provide sufficient safety argument or evidence (given the level of maturity of the design or the means available within the Project in the current step), Safety Issues have been recorded.

2 Introduction

2.1 Background

In 2006, DSNA started to work on the concept of a complementary role to the existing Flow Manager to fill the gap between the ATFCM and the ATC. This concept was deemed to be much promising in terms of safety and capacity and moreover, the R&D work to be done was estimated compliant with the SESAR timeframe.

In 2013, the Integrated Network Management and extended ATC Planning concept (INAP) emerged from projects P04.02 and P07.02. This concept is introducing a new role, the Extended ATC Planning (EAP) role, which is intended to fill the current gap between ATFCM and ATC.

The safety and performance requirements developed in this SPR build upon the above-mentioned background information and on the work conducted within SESAR 1 in the project P04.07.08. This work allowed deriving operational requirements for a ***basic Extended ATC Planning*** concept, before the full Extended ATC Planning concept can be described and validated in SESAR 2020.

2.2 General Approach to Safety Assessment

This safety assessment is conducted as per the Safety Reference Material [1] which itself is based on a twofold approach:

- A success approach which is concerned with **the safety of the operations in the absence of failure** within the end-to-end system
- A conventional failure approach which addresses the **safety of the operations in the event of failures** within the end-to-end system.

Together, the two approaches lead to Safety Objectives and Safety Requirements which set the minimum positive and maximum negative, safety contributions of the system.

2.3 Scope of the Safety Assessment

This Safety Assessment includes:

- The setting of the Safety Criteria (SAC)
- The description of the key properties of the environment,
- The definition of the safety objectives (i.e. safety requirements at OSED level) from success and failure approach
- The definition of safety requirements at SPR level

The Safety Requirements defined herein are based on the activities performed in SESAR Project 4.7.8 and have been reviewed by bEAP concept experts. These safety requirements are consequently correct, complete and realistic.

Since the properties of the operational environment are crucial to the safety assessment, this assessment cannot be generic – it has to be specific to the Operational Environment defined in section 3.2 and consequently, the term 'specimen' safety assessment should be used.

2.4 Layout of the Document

Section 3 describes the basic Extended ATC Planning concept, defines the high level Safety Criteria and defines the safety objectives at the OSED level, i.e. operational safety requirements for basic Extended ATC Planning concept.

Section 4 describes an SPR-level Design of the bEAP system and ensures the existence of a complete and correct set of Safety Requirements so that the OSED-level specification is satisfied by the Safety Requirements

Section 5 is part of the Safety Assessment Report template but is not filled for the basic Extended ATC Planning concept.

Appendix A contains a consolidated list of safety objectives for the basic Extended ATC Planning

Appendix B derives the safety requirements on SPR-level model elements from the safety objectives

Appendix C presents the detailed causal analysis of each operational hazard

Appendix D provides a consolidated list of the Safety Requirements for the basic Extended ATC Planning

Appendix E states the assumptions, safety issues and limitations

3 Safety specifications at the OSED Level

3.1 Scope

This section addresses "how safe the system needs to be" through the following activities:

- Description of the key properties of the Operational Environment that are relevant to the safety assessment – section 3.2,
- Identification of the Airspace User requirements, in terms of benefits that the solution is intended to bring to the airspace users with a specific focus on the key requirements related to safety assessment – section 3.3,
- Identification of the pre-existing hazards that affect traffic in the relevant operational environment (aviation hazards) and the risks which basic Extended ATC Planning solution may reasonably be expected to mitigate to some degree and extent – section 3.4,
- Setting of the SAfety Criteria – section 3.5,
- Comprehensive determination of the operational services that are provided by the basic Extended ATC Planning solution to address the relevant pre-existing hazards and derivation of Safety Objectives - success approach, in order to mitigate the pre-existing risks under normal operational conditions – section 3.6,
- Assessment of the adequacy of the operational services provided by the basic Extended ATC Planning solution under abnormal conditions of the Operational Environment – section 3.7,
- Assessment of the adequacy of the operational services provided by the basic Extended ATC Planning solution in the case of internal failures and mitigations of the system-generated hazards (derivation of Safety Objectives -failure approach) – section 3.8,
- 3.9 assess the impact of the operational services provided by the basic Extended ATC Planning solution on the adjacent airspace
- Achievability of the Safety Criteria (i.e. how to make use of the Validation exercises in order to demonstrate that the Safety Criteria are achievable by the basic Extended ATC Planning solution) – section 3.10,
- Validation & verification of the safety specification – section 3.11

No formal safety plan has been produced for the basic Extended ATC Planning concept.

3.2 Basic EAP Solution Operational Environment and Key Properties

3.2.1 Introduction of bEAP solution

Operational Concept Elements in the scope of the Solution

The SESAR **Solution #118 - Basic EAP (Extended ATC Planning) function** is defined in the applicable version of EATMA (Dataset 18) as follows:

> **Solution #118 — Basic EAP (Extended ATC Planning) function**
>
> The basic Extended ATC Planner aims at bridging the gap between Air Traffic Flow and Capacity Management (ATFCM) and Air Traffic Control (ATC) providing real-time and fine-tuning measures to solve ATFCM hotspots and to perform early measures to alleviate complexity closest to ATC activities.
>
> The solution consists of an automated tool and associated procedures supporting the basic communication between the Local DCB position and the Controllers' Work Positions allowing the EAP and the ATC team in identifying, assessing and resolving local complexity situations. The basic EAP relies on a real time integrated process for managing the complexity of the traffic with capability to reduce traffic peaks through early implementation of fine-tuned solutions to solve workload imbalances at the local level, compatible with the short term timeframe of execution phase of the flights.

Operational improvement and expected benefits

The basic EAP (Extended ATC Planning) function introduces an **initial automated interface** together with the related procedures that will facilitate the communication between local DCB position and the Controllers' Work Positions through the provision of optimised solutions to solve workload imbalances compatible with the short term timeframe of execution phase of the flights.

The basic EAP concept introduces also a **new role**, the EAP role (Extended ATC Planning), which is intended to **fill the gap between ATFCM and ATC** as illustrated on Figure 1 below:

- The **EAP is not an additional staff**: it is a **role** covering a set of services/functions that can be assumed by different personnel of the ATSU (already existing actors, like TC or new actors like MSP or LTM);
- It is **highly recommended** that the EAP is holding or has held an **ATCO rating** in the concerned ATSU's airspace

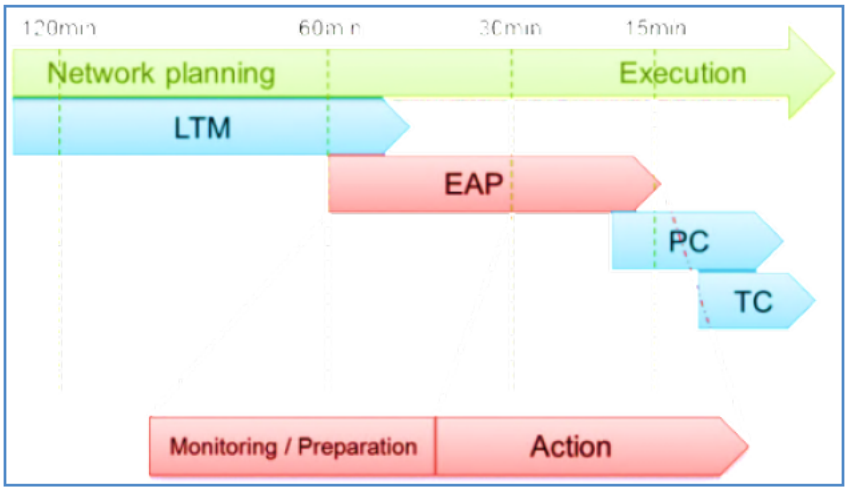


Figure 1: The EAP role fills the current gap between ATFCM and ATC

The main benefits expected from the basic EAP function are principally:

- To help providing a **better service to airspace users** through reduced delays, better punctuality, less ATFCM regulations, whilst maintaining or even increasing safety.
- To **increase the controllers' productivity** contributing thus to increase of the overall en-route capacity of the ACC.

In addition, the basic EAP concept can be considered as a **potential enhancement enabler** for the deployment of functionalities such as **Extended AMAN** or **Free Routing** operations, as it facilitates anticipation of potential extra workload linked to these concepts.

Key Feature and Capabilities under the scope of the Solution

The basic EAP function is part of the INAP (*Integrated Network management and extended ATC Planning*).

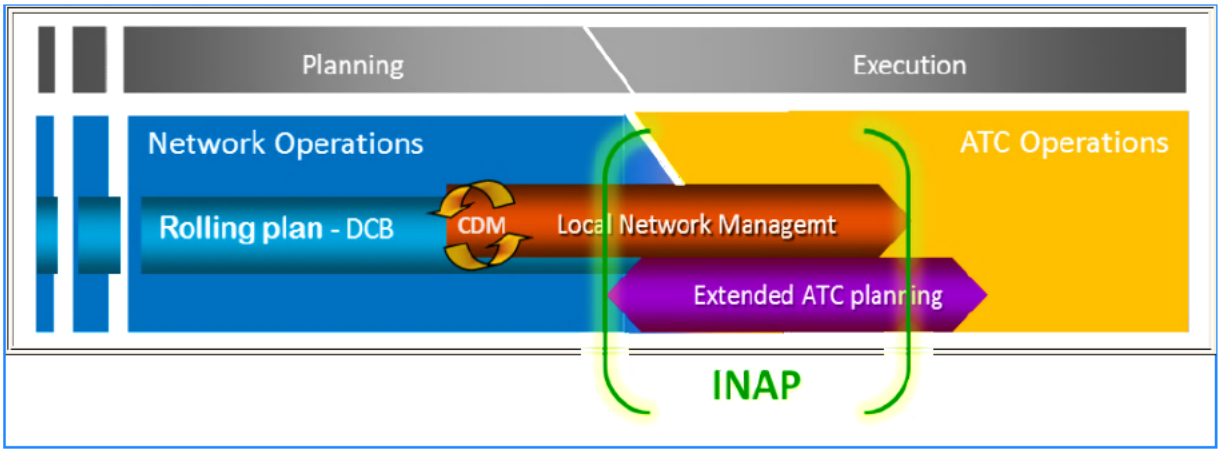


Figure 2: INAP horizon

As illustrated on Figure 2 above, the **tasks of the EAP role** are included in a timeframe **ranging from the short-term planning** (i.e. a few hours before flights entry time of the sector where a hotspot has been identified) **up to the execution phase of flights.**

The main responsibilities of the EAP role can be summarized as follows:

- In close coordination with the LTM (unless both roles are endorsed by a single actor), the EAP role is in charge to **monitor the hotspots evolution and elaborate the appropriate ATFCM measures** (STAM) to lower the sector team workload.

  The *occupancy counts* which are illustrating instant load in a given sector, allow alleviating residual / reactional overloads on a small period of time.

- The EAP role has **to coordinate the STAM with the Planning Controller** (PC) from around 15' up to 30' before the flights enter the hotspot;

- The EAP role is then in charge **to monitor the STAM implementation** and their effect on hotspot status until the concerned flight has conformed to the measure (but not later than the entry of the flight in the on-loaded sector);

- Independently of ATFCM measures, the EAP role can **initiate short term actions on traffic**, in order to smooth the traffic for the next CWPs so as to facilitate anticipated resolution of conflicts and reduce the expected complexity;
  These actions have to be performed by the EAP role prior the traffic enters the concerned beneficiary sectors. These actions also have to be undertaken based on the most updated traffic situation and should fit with any other complementary ATFCM measures already in place.

The impact of basic Extended ATC Planning on the ATC team's side can be summarized as follows:

- With the introduction of the EAP role, the **Planning Controller becomes the interface between the EAP and the Tactical Controller** on the CWP:
  - The Planning Controller is in charge to **receive the requests** (proposed measures) from the EAP, and potentially **negotiate them with the EAP role** (via a CDM process supported by the EAP tool) according to the real time traffic conditions;
  - The Planning Controller is also in charge to **negotiate with downstream sectors** the changes of flights' delivery parameters, as foreseen by the EAP role in the proposed measures;
  - The Planning Controller has to **prepare as much as possible the actions of the Tactical Controller** related to the measures initiated/prepared by the EAP role;
  - The Planning Controller monitors **the implementation by the Tactical Controller of** the measures initiated/prepared by the EAP role ;
- **The Tactical Controller** of the Implementing Sector is directly impacted by EAP role's proposed measures.
  - The Tactical Controller takes the decision to **perform the actions requested by the Planning Controller** consequent to the measures proposed by the EAP role;
    For example, he might have to manage extra aircraft rerouted by the EAP role and accepted by the Planning Controller.

The EAP role addresses the same traffic as the LTM but in a different time horizon, and with a finer level of granularity (analysis is made on very few flights, and not a whole airspace volume): up to a few hours in advance for the EAP role whilst it is up to more than 5 hours in advance for the LTM (FMP).
It is worth noting that the basic cooperation between the two roles has been addressed through the validation exercise VP-687 but should be further investigated in SESAR2020.

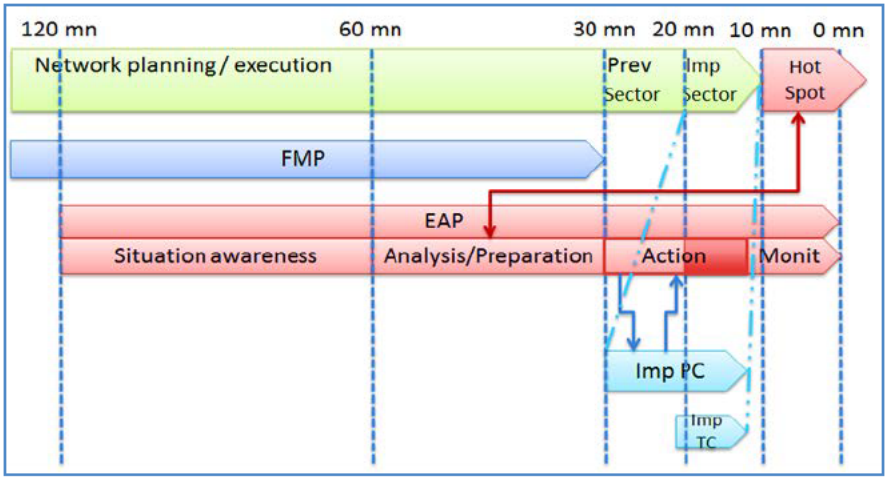


Figure 3: EAP role time horizon

To be more accurate regarding the EAP time horizon, the basic EAP concept developed in this SPR/INTEROP OSED relies on the following assumptions:

- He monitors hotspots up to one hour in advance;
- He is allowed to create *ad-hoc* hotspots in close coordination with the LTM up to one hour in in advance;
- He analyses the situation and prepares STAM up to one hour before flights enter the hotspot;
- He coordinates the STAM with the Planning Controller from around 15' up to 30' before the flights enter the hotspot;
- He monitors the STAM until the flights conformed to the measure (but no later than the entry of the flight in the on-loaded sector)
- Regarding the tools it is assumed that the EAP role will need to have a longer time horizon than one hour, not because of his own task but to be aware of what is the demand just after, and to facilitate coordination and task sharing with LTM.

3.2.2 Basic EAP Solution Operational Environment and Key Properties

The characteristics of the operational environment that are relevant for this safety assessment are recalled bellow. This operational environment is further described in the Part I of the bEAP SPR/OSED ([6]).

- **Airspace Structure and Boundaries**
  Managed airspace only
  Airspace includes segregated areas/FUA.
- **Types of Airspace – ICAO Classification**

No particular restriction in terms of Airspace classes

- **Airspace Users – Flight Rules**
  Concept applies to IFR, but environment allows all types of Airspace Users, including VFR.
- **Traffic Levels and complexity**
  The environment considered involves a high traffic density and complexity. Indeed, EAP concept is only required in environment of high traffic and high complexity in order to improve the ATFCM activities in this kind of environment.
- **ATM capabilities**
  - Ground:
    - IFPS,
    - ETFMS,
    - CHMI interface on LTM position
    - FDPS
    - Ground-ground interconnection
  - Airborne:
    - No specific requirement
- **Terrain Features - Obstacles**
  Not relevant
- **CNS Aids**
  Standard CNS capabilities
- **Separation Minima**
  Standard ICAO separation minima
- **Operational services**
  In the managed airspace being considered herein, the full set of ATM services are being provided:
  - ATS services (ATC separation assurance, Flight Information, Alerting)
  - ATFM service
  - Airspace Management service

3.3 Airspace Users Requirements

Airspace users requirements on the basic Extended ATC Planning are presented in the OSED section (see section 3 of [6]).

3.4 Relevant Pre-existing Hazards

This sub-section determines (from Guidance F.2.2 of Reference [2]), the relevant pre-existing hazards that the OFA 03.01.03 operational services have to mitigate in the relevant operational environment.

The main objective of the Extended ATC Planning is to continue the action of the LTM and to contribute to bridge the gap between Air Traffic Flow and Capacity Management (ATFCM) and Air Traffic Control (ATC).

The role of ATFM service in aviation Safety can be described as follows

By reducing traffic complexity (i.e. resolving traffic imbalance in terms of density & complexity) so as to provide ATCOs with manageable traffic, it reduces the number of potential conflicts or potential for airspace infringement to be managed simultaneously in the areas affected[1].

That implies that the ATFM service, and consequently bEAP concept contribute to the mitigation of the following hazards which pre-exist in the operational environment, before any form of de-confliction has taken place (extracted from SRM Guidance):

Hp#1 "Situation in which the intended trajectories of two or more aircraft are in conflict"

Hp#2 "Penetration of restricted airspace"

Considering the pre-existing hazards that are impacted by basic Extended ATC Planning concept, the relevant accident type for this concept is the **Mid-Air Collision**.

3.5 Safety Criteria

A high level validation Safety Target has been defined by the SESAR 1 Project B4.1 for the OFA05.03.04. This Safety Target is that *"Enhanced ATFCM Processes" shall decrease the annual number of accident and incident with ATM contribution of 1.89%"*.

The definition of Safety Criteria is the first step of the safety activities at solution level to ensure that this Safety Target will be reached. Safety Criteria are "high-level" criteria defined at the level of the Safety Barriers.

The steps to define the Safety Criteria are:

- Identification of the accident type impacted by the change
- Identification of the safety barriers and precursors of the relevant accident model impacted by the change and qualification of these impact (qualitative qualification or quantitative qualification)
- Definition of Safety Criteria at the level of the safety barriers

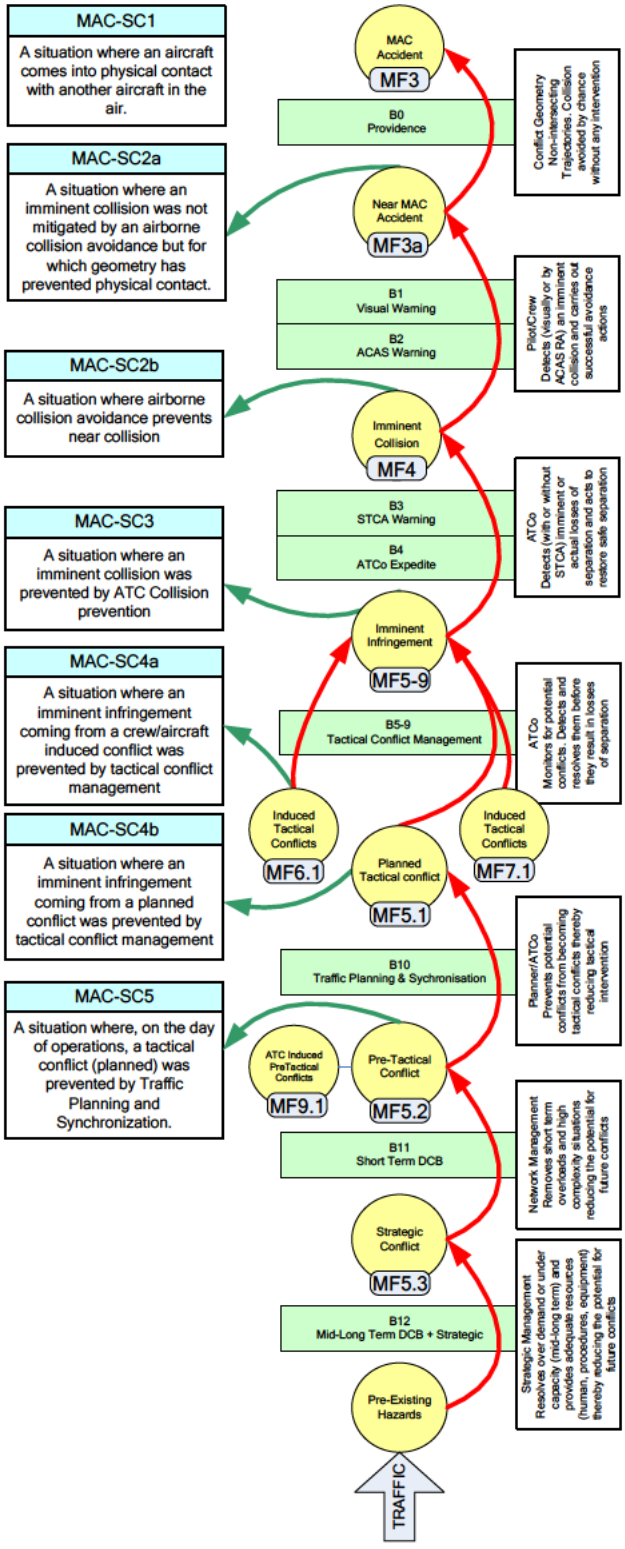
3.5.1 Identification of the accident type impacted by the change

Different type of accident can occur in ATM domain: Mid Air Collision, Runway Collision, Controlled Flight Into Terrain or Taxiway Accident. In order to avoid these accidents to occur several barriers are implemented at ATM level. Within the frame of SESAR WP16.6.1, barriers models have been defined for each kind of accident.

Considering the pre-existing hazards that are impacted by the bEAP concept, the relevant accident type for this solution is the **Mid-Air Collision**.

The barrier model of the Mid-Air Collision is the following:

[1] According to ICAO Doc 9854 « Global ATM Operational Concept » **Error! Reference source not found.** "the strategic conflict management is the first layer of conflict management and is achieved through the airspace organization and management, demand and capacity balancing and traffic synchronization components"



Severity Class Scheme for Mid-air Collision
AIM MAC BARRIER MODEL (TMA&ER)

Figure 4: Mid Air Collision Barrier Model

The main barriers of this model are:

- "**Mid / Long Term Demand and Capacity Balancing + Strategic Planning**". This barrier consists in:
    - Performing the mid/long term demand and capacity balancing : forecast of long / medium term traffic demand and implementation of measure to balance capacity and demand
    - Performing the strategic planning in accordance with the demand forecast: airspace design, sector design, and definition of capacity threshold…
- "**Short Term Demand and Capacity Balancing**": This barrier consists in:
    - Identification of demand and capacity imbalance situation (i.e. cases where demand exceeds the capacity) based on occupancy count, entry count, complexity estimation…
    - Resolution of demand/capacity imbalance situation by implementation of DCB measures: sectorisation, STAM, regulation…

  This barrier is implemented by the network manager and by the local traffic manager (LTM)
- "**Tactical planning barrier**: **traffic planning and synchronisation**" : This barrier consists in :
    - Checking and coordinating entry conditions
    - Identifying the planned conflicts in the AOR and informing the TC
    - Checking and coordinating the exit conditions
    - Synchronizing the traffic

  This barrier is implemented by the Planning Controller.
- "**Tactical conflict resolution barrier**: **tactical conflict management**": This barrier consists in managing the tactical conflicts and consequently maintaining the separation between aircrafts or with restricted areas. This barrier includes:
    - Management of planned conflict (conflict detected by the PC),
    - Management of ATC induced conflict (conflict induced by the ATCO when solving another conflict or when dealing with a situation of bad weather / restricted area activation),
    - Management of crew/aircraft induced conflict (conflict induced by a failure of the pilot or the aircraft)

  This barrier is implemented by the Tactical Controller (for detection and resolution of the conflict) and the crew (for execution of the clearance)
- "**ATC collision prevention barrier: ATCO expedite and STCA warning**": This barrier includes the management of imminent collision situations detected by the pilot or by the short term conflict alert (STCA). This barrier is implemented by the Tactical Controller (for detection and resolution of the conflict) and the crew (for execution of the clearance).

- "**Airborne collision avoidance barrier: ACAS Warning / Visual Warning**": This barrier includes the management of imminent infringement situations detected by the pilot or by collision avoidance system (TCAS/ACAS). This barrier is implemented by the crew.

The main precursors (conditions, events, and sequences that precede and lead up to the mid-air collision) of this model are

- Strategic conflict
- Pre-tactical conflict
- ATC induced pre-tactical conflict: conflict induced by the Planning Controller within the frame of its activities.
- Planned Tactical conflict
- ATC induced tactical conflict: conflict induced by the Tactical Controller within the frame of its activities.
- Pilot induced tactical conflict: manoeuver performed by the aircraft or the pilot leading to a deviation and potentially to a conflict
- Imminent Infringement
- Imminent Collision

All these barriers and precursors contribute to "Mid Air Collision". These barriers and precursors are further developed in low-level barriers in a more detailed model (see [2]).

The impact of the bEAP concept on these barriers and the definition of the associated Safety Criteria are presented in the following section

3.5.2 Identification of barriers and precursors impacted and definition of Safety Criteria

The bEAP concept sits between the "**Short Term Demand and Capacity Balancing**" (B11 barrier) and the "**Tactical planning barrier**: **traffic planning and synchronisation**" (-B10 barrier).

The bEAP concept by helping the LTP and bridging gap between the LTM and the ATCO enhance the efficiency of the "**Short Term Demand and Capacity Balancing**" and "**Traffic planning and synchronisation**" (see B11 & B10 barriers from MAC En Route accident incident model). More particularly:

- Thanks to a higher number of STAMs on Intruders, unforeseen Hotspots due to Intruders will be more easily managed
- By reducing the number of flights in conflicts in a TFV through STAMs, the resulting traffic Complexity will decrease
- EAP deals with better predictions than LTM and this will improve the relevance of the STAM.
- The resulting ATC workload will then be smoothed

It does not appear feasible to determine (or at least assume) in what proportion the introduction of bEAP (in complement/refinement of current Regulations) impacts this barrier. Meanwhile, as a cumulative effect of enhancing the two barriers, the En-Route sectors' capacity is increased (i.e.

more traffic can be managed, as a result of reduced sector capacity buffer enabled by the better management of traffic imbalance) whilst keeping the same safety level (i.e. the same yearly probability of MAC accident).

Consequently the following Safety Criteria (SAC) is for bEAP concept (with regards to Baseline 1):

SAC#1: With bEAP introduction, the number of "planned" conflicts in En Route sectors shall not increase despite the increase in traffic (ER sector capacity) enabled by DCB EAP measures

3.6 Mitigation of the Pre-existing Risks – Normal Operations

3.6.1 Operational Services to Address the Pre-existing Hazards

The bEAP concept introduces a new operational service between the Demand and Capacity Balancing (DCB) and the En Route ATC planning. The table below introduces this service and indicates the pre-existing aviation hazards to which it contribute to mitigate, in order to highlight its contributing role to aviation safety.

ID	Service Objective	Pre-existing Hazards [Hp xx]
EAP	Perform Extended ATC Planning	**Hp#1** **Hp#2**

Table 1: ATM and Pre-existing Hazards

3.6.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations

Two different use cases are defined for the basic EAP concept within the OSED section of this SPR:

- **Use Case 1**: Implementation of DCB EAP measure (i.e. STAM or decomplexification measure) required by the LTM. Within this use case, the EAP receive a request of DCB EAP measure from the LTM and is in charge of the implementation of the appropriate DCB EAP measure (i.e. STAM or decomplexification measure) to meet the request from the LTM.

- **Use Case 2**: Implementation of decomplexification measure at EAP level (with no LTP supervision). Within this use case, the EAP is not triggered by the LTM. EAP identify a hotspot within its area of responsibility and within the time-horizon under its responsibility. He is then in charge of the implementation of the appropriate decomplexification measure to solve the hotspot.

These two use cases are described in the bEAP OSED (see section 3 of [6]).

Table 2 highlights for each of these use cases the main operational requirements on the EAP, i.e. the operational safety objectives. References **1.X** are associated to use case 1 and references **2.X** are associated to use case 2.

Ref	Phase of Flight / Operational Service	Achieved by / Safety Objective [SO xx]
1.1	EAP shall receive and analyse request of DCB EAP measure from the LTM	SO_EAP_001
1.2	EAP prepare the appropriate DCB EAP measures	SO_EAP_003
1.3	EAP shall coordinate the implementation of DCB EAP measures with ATCO	SO_EAP_004
1.4	EAP shall monitor the implementation of DCB EAP measure	SO_EAP_005
2.1	EAP shall identify situations requesting a decomplexification measure	SO_EAP_002
2.2	EAP prepare the appropriate decomplexification measures	SO_EAP_003
2.3	EAP shall coordinate the implementation of decomplexification measures with ATCO	SO_EAP_004
2.4	EAP shall monitor the implementation of decomplexification measures	SO_EAP_005

Table 2: bEAP Solution Operational Services & Safety Objectives (success approach)

ID	Description
SO_EAP_001	EAP shall receive and analyse request of DCB EAP measure from the LTM
SO_EAP_002	EAP shall identify situations requesting a de-complexification measure
SO_EAP_003	EAP shall prepare appropriate DCB EAP measures
SO_EAP_004	EAP shall coordinate the implementation of DCB EAP measures with ATCO
SO_EAP_005	EAP shall monitor the implementation of DCB EAP measures

Table 3: List of Safety Objectives (success approach) for Normal Operations

3.6.3 Analysis of the Concept for a Typical Flight

Not relevant: basic EAP is not working on a specific flight but on traffic flows.

3.7 Basic EAP Solution Operations under Abnormal Conditions

The purpose of this section is to assess the ability of the Solution to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the Solution System, that might be encountered relatively infrequently.

3.7.1 Identification of Abnormal Conditions

The following list of abnormal conditions has been identified for the basic EAP solution:

- ABN1. Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud …)
- ABN2. Severe weather conditions
- ABN3. Unplanned limitation in capacity (ATC ground system failures, unforeseen sector closure/regrouping)
- ABN4. NOP failure (all FMPs & CFMU)
- ABN5. Aircraft emergency

3.7.2 Potential Mitigations of Abnormal Conditions

The Table 4 below assesses, for each abnormal condition, the immediate effect on EAP operations and identifies the possible mitigations of the safety consequence of the operational effect with a reference to the existing safety objectives (as per Table 3) or to new safety objective describe in Table 5.

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
ABN1	Unforeseen airspace closure (e.g. Volcanic Ash, nuclear cloud …)	Unforeseen airspace closure can cause new hotspots, which might turn the existing DCB EAP measures insufficient or inefficient. Worst consequences are that a series of DCB EAP measures designed to deal with an overload situation in replacement of regulation cannot be implemented and is too late to restore regulation. LTM remains responsible for the monitoring of short term ATFCM at ATSU level. LTM detects the demand and capacity imbalance and defines appropriate ATFCM measures. The situation can also be detected by the EAP through monitoring of the situation (	Short term: None (ATC deals with the imbalance in the affected sectors) Longer term: Restrictive regulation
ABN2	Severe weather conditions	Severe weather condition can cause aircraft to no execute flight and then create new hotspots. In	Short term: None (ATC deals with the imbalance in the

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
		consequence, the existing DCB EAP measures can be insufficient or inefficient. Worst consequences are that a series of DCB EAP measures designed to deal with an overload situation in replacement of regulation cannot be implemented and is too late to restore regulation. LTM remains responsible for the monitoring of short term ATFCM at ATSU level. LTM detects the demand and capacity imbalance and defines appropriate ATFCM measures. The situation can also be detected by the EAP through monitoring of the situation (	affected sectors) Longer term: Restrictive regulation
ABN3	Unplanned limitation in capacity (ATC ground system failures, unforeseen sector closure/regrouping)	In case of unplanned limitation in capacity, the DCB EAP measures proposed by the EAP will probably be insufficient to maintain an acceptable level of ATCO workload. LTM remains responsible for the monitoring of short term ATFCM at ATSU level. LTM detects the demand and capacity imbalance and defines appropriate ATFCM measures. The situation can also be detected by the EAP through monitoring of the situation (	Short term: None (ATC deals with the imbalance in the affected sectors) Longer term: Restrictive regulation
ABN4	NOP failure	LTM And EAP are not able to assess the demand and to identify possible hotspots. Management of this event is not different with EAP than without. LTM remains responsible for the monitoring of short term ATFCM at	Restrictive regulation

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
		ATSU level. LTM detects the situation and defines appropriate ATFCM actions to ensure that workload will remain acceptable.	
ABN5	Aircraft emergency	This event is managed tactically by the ACTO as in current operation without EAP. DCB EAP measures proposed by the EAP are considered of lower propriety by the ATCO (**SO_EAP_006**). In case the aircraft in emergency is an aircraft impacted by a DCB EAP measure, the situation is detected by the EAP through monitoring of the implementation (**SO_EAP_005**) and new measures are proposed by the EAP.	Tactical management of the aircraft by the ATCO DCB EAP measure have lower priority than management of tactical situation (**SO_EAP_006**)

Table 4: Additional Safety Objectives (success approach) for Abnormal Conditions

ID	Description
SO_EAP_006	ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation.

Table 5: List of Safety Objectives (success approach) for Abnormal Operations

3.8 Mitigation of System-generated Risks (failure approach)

This section concerns bEAP operations in the case of internal failures of the bEAP system. Before any conclusion can be reached concerning the adequacy of the safety specification of these operations, at the OSED level, it is necessary to assess the possible adverse effects that failures internal to the end-to-end bEAP System might have upon the provision of the relevant operational services described in section 3.6.1and to derive safety objectives (failure approach) to mitigate against these effects.

3.8.1 Identification and Analysis of System-generated Hazards

The system-generated hazards have been identified from the above description of the bEAP operations and by considering, for each safety objective (from the success approach above), what

would happen if the objectives were not satisfied. Then the different failures leading to similar operational effects have been consolidated into operational hazards.

For each system-generated hazard, the following assessment has been conducted

- Assessment of immediate operational effect
- Assessment of possible mitigations of the safety consequence of the operational effect with a reference to existing or new safety objectives (functionality and performance).
- Assessment of the severity of the most probable effect from hazard occurrence as per the relevant Severity Classification Scheme(s) from Guidance E.2 of Reference [2].

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
Hz_EAP_ 001	No detection of need for a DCB EAP measure	SO_EAP_01 SO_EAP_02	The need of a DCB EAP measure is not detected neither by the LTM nor the EAP. Considering the time-horizon of the EAP, it is not possible to implement a less restrictive ATFCM measure (e.g. regulation) to solve the hotspot. Sector associated to the complex situation or hotspot will face imbalance which might impact the traffic planning & synchronization tasks (increase of workload of the Planning Controller).	Tactical conflict management	SC-4b
Hz_EAP_ 002	DCB EAP measure not implemented	SO_EAP_03 SO_EAP_04	The DCB EAP measure requested in order to solve a hotspot or reduce the complexity in a sector is not implemented. The complex situation or hotspot will not be resolved as expected. Considering the time-horizon of the EAP, it is not possible to implement a less restrictive ATFCM measure (e.g. regulation) to solve the hotspot. Sector associated to the complex situation or hotspot will face imbalance which might impact the traffic planning & synchronization tasks (increase of workload of the Planning Controller). Absence of implementation of an EAP measure is normally detected through monitoring by EAP	Tactical conflict management	SC-4b

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
			(SO_EAP_005).		
Hz_EAP_ 003	DCB EAP measure inefficient	SO_EAP_03	The DCB EAP measure requested in order to solve a hotspot or reduce the complexity in a sector is implemented but does not sufficiently reduce the complexity. Sector associated to the complex situation or hotspot will face imbalance which might impact the traffic planning & synchronization tasks (task of the Planning Controller).	Tactical conflict management	SC-4b
Hz_EAP_ 004	DCB EAP measure with contrary effect on the target sector	SO_EAP_03	A DCB EAP measure is wrongly defined & agreed or wrongly implemented (e.g. too late) to the extent that not only it will not resolve the complex situation or hotspot but even it makes it more severe. As the DCB EAP measure was required because the targeted sector was already being exposed to a significant complexity or hotspot, the complexity might be so high that even the tactical conflict management tasks may be compromised	ATC collision prevention (STCA warning and ATCO expedite)	SC-3
Hz_EAP_ 005	DCB EAP measure generating imbalance in other sectors	SO_EAP_03	The DCB EAP measure requested in order to solve a hotspot or reduce the complexity in a sector is implemented but it generates a demand and capacity imbalance in another sector (e.g. due to	Tactical conflict management	SC-4b

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
			the limited/local view of the EAP). No effect for the implementing sector: complexity is solved in this sector. On-loaded sector will face imbalance which might impact the traffic planning & synchronization tasks (increase of workload of the Planning Controller).		
Hz_EAP_ 006	DCB EAP measure generating excessive workload in implementing sector	SO_EAP_04	The implementation of the EAP DCB measure generates extra-workload on the implementing sector. In any, case the implementation of an EAP DCB measure need to be considered of lower priority by the ATCO, in comparison to the management of the tactical situation (SO_EAP_006). The extra workload might compromise the traffic planning & synchronization tasks in the implementing sector.	Tactical conflict management	SC-4b

Table 6: System-Generated Hazards and Analysis

3.8.2 Derivation of Safety Objectives (integrity/reliability)

This section derives Safety Objectives (addressing integrity/reliability) to limit the frequency with which the above bEAP System-generated hazards could be allowed to occur using the relevant Rick Classification Scheme(s) from Guidance E.3 of Reference [2] and SO mathematical calculation guidance in Guidance E.4 of Reference [2].

Integrity Safety Objectives are expressed as maximum frequency of occurrence for each hazard. They are directly derived from the severity of the hazard, using the following formula (extracted from P16.6.1 guidance document: [2]):

$$SO = \frac{MTFoO_{relevant\_severity\_class}}{N \times IM}$$

where:

- $MTFoO_{relevant\_severity\_class}$ stands for the Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard's effect as defined in document [2], expressed per flight hour. More particularly for MAC hazards, relevant values are
  - 1e-4 per flight hour for severity class MAC-SC3
  - 1e-2 per flight hour for severity class MAC-SC4b
- N is the overall number of operational hazards for a given severity class at a given barrier as obtained from document [2]. More particularly for MAC hazards, relevant values are:
  - 25 hazards for severity class MAC-SC3
  - 30 hazards for severity class MAC-SC4b
- IM is the Impact Modification factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard. This factor is not used for our analysis and considered as equal to 1.

When necessary, safety objectives are converted from [per flight*hour] into [per sector operational hour] using the following formula.

$$SO_{PerSOH} = SO_{PerFH} * X$$

Where

- X is the average number of flight hour controlled per sector hour. It is assumed that 6 flight hours are controlled per sector hour in high complexity. This figure is extracted from ED-161 and is a result from combining a sector capacity with average flight time in sector related to medium-density operations, e.g., 60 flights per hour sector capacity with an average 6 minute flight length in sector, or another example could be 45 flights per hour sector capacity with an 8 minute average flight length.
- An important factor in these traffic numbers is that average sector length and throughput are dependent elements, being that sector design factors will balance increasing sector throughput requirements (based on demand) with smaller sectors, and therefore shorter

average flight lengths within the sector. If a local implementation differs from these figures, safety objectives per flight hour shall be considered and a new conversion with appropriate figures need to be performed

Hazard ID	Safety Objectives
FHz_EAP_001	SO_EAP_101: The frequency of occurrence of a lack of detection of need for a DCB EAP measure shall not be greater than 2.0x10-3 per sector ops hour
Hz_EAP_002	SO_EAP_102: The frequency of occurrence of a DCB EAP measure not implemented shall not be greater than 2.0x10-3 per sector ops hour
Hz_EAP_003	SO_EAP_103: The frequency of occurrence of a DCB EAP measure inefficient shall not be greater than 2.0x10-3 per sector ops hour
Hz_EAP_004	SO_EAP_104: The frequency of occurrence of a DCB EAP measure with contrary effect on the target sector shall not be greater than 2.4x10-5 per sector ops hour
Hz_EAP_005	SO_EAP_105: The frequency of occurrence of a DCB EAP measure generating imbalance in other sectors shall not be greater than 2.0x10-3 per sector ops hour
Hz_EAP_006	SO_EAP_106: The frequency of occurrence of a DCB EAP measure generating excessive workload in implementing sector shall not be greater than 2.0x10-3 per sector ops hour

Table 7: Safety Objectives (integrity/reliability)

3.9 Impacts of basic EAP Solution operations on adjacent airspace or on neighbouring ATM Systems

EAP operates at local level. Any DCB EAP measure that would require coordination with adjacent ATSU would be managed by the LTM.

3.10 Achievability of the Safety Criteria

Safety Objectives are defined in section 3.6 to 3.9 in order to meet the bEAP Safety Criteria defined in section 3.5.

The safety objectives of this section have been defined in regard to:

- The results of the VP687 validation exercise (see Validation Report [7]). In particular, this exercise focused on the evaluation of following safety benefits
  - Reduction of ATCO and LTM actors workload due to better coordination and mutual situational awareness,
  - Reduction of unforeseen ATCO overloads thanks to the monitoring of Intruders.

- The feedback from the experimentation/implementation project 4Me in French Reims ACC.

The content of this section has also been reviewed by bEAP concept experts.

3.11. Validation & Verification of the Safety Specification

Consolidated list of Safety Objectives is provided in Appendix A. The process by which these safety objectives were derived is presented in previous section 3.6 to 3.9.

4 Safe Design at SPR Level

4.1 Scope

This section addresses the following activities:

- Description of the SPR-level model of the end-to-end system supporting the bEAP solution - section 4.2
- Derivation, from the Safety Objectives (Functionality and Performance) of section 3, of Safety Requirements for the SPR-level design – section 4.2.2
- Analysis of the operation of the SPR-level design under normal operational conditions – section 4.3
- Analysis of the operation of the SPR-level design under abnormal conditions of the Operational Environment - section 4.4
- Assessment of the adequacy of the SPR-level design in the case of internal failures and mitigation of the System-generated hazards - section 4.5
- justification that the SAfety Criteria are capable of being satisfied in a typical implementation - section 4.6
- Realism of the SPR-level design - section 4.7
- Validation & verification of the Specification - section 4.8

4.2 Basic EAP Solution SPR-level Model

The SPR-level Model in this context is a high-level architectural representation of the bEAP System design that is entirely independent of the eventual physical implementation of the design. The SPR-level Model describes the main human tasks, machine functions and airspace design. In order to avoid unnecessary complexity, human-machine interfaces are not shown explicitly on the model – rather they are implicit between human actors and machine-based functions.

4.2.1 Description of SPR-level Model

The SPR-level model is provided on the figure below. Details about the different components of this model are provided in the sections below.

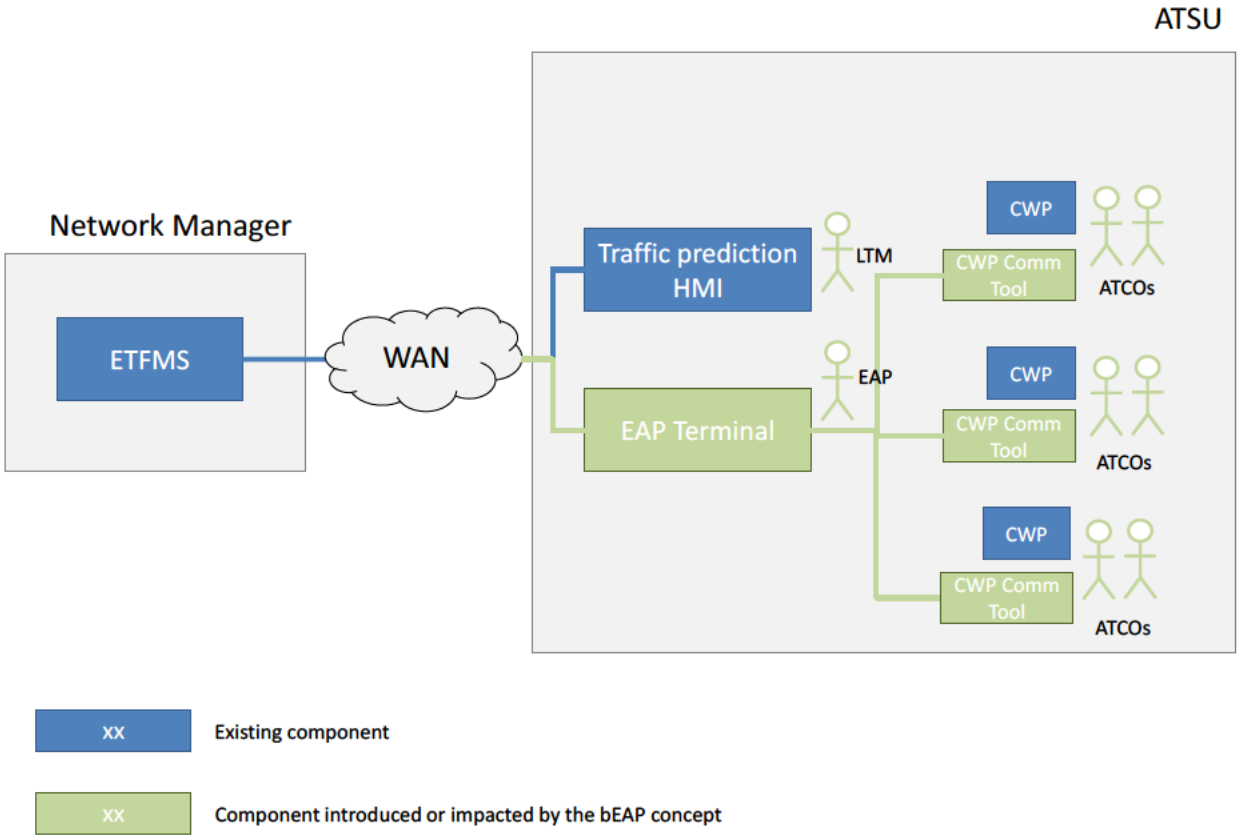


Figure 5: bEAP Solution SPR-level Model

4.2.1.1 Aircraft Elements

No aircraft element is presented on the SPR level model, considering that the bEAP concept has no impact on these elements: exchanges between ATCO and pilots are performed as per current operation within bEAP concept.

4.2.1.2 Ground Elements

- **ETFMS** provides short term prediction of the traffic over the full area under NMOC responsibility (including occupancy count, traffic count, flight profile, flight details). The ETFMS data are made available in real time to local users at ATSU level via a traffic prediction HMI.
- **Traffic prediction HMI** is an HMI used by LTM and EAP to :
  - Monitor the prediction of traffic
  - Detect the demand and capacity imbalance
  - Identify the hotspots

  Different instance of "Traffic prediction HMI" can be deployed in a same ATSU if needed, in case of different persons assuming the role of EAP and LTM. C-HMI from Eurocontrol can be a possible Traffic prediction HMI.
- **EAP Terminal** is a tool supporting the EAP to

- Monitor the prediction of traffic (in complement to the "Traffic Prediction HMI"
- Prepare of the DCB EAP measure
- Coordinate the implementation of the DCB EAP measure

- **CWP Communication tool** is a tool supporting the ATCO for the communication with the EAP regarding the proposed DCB EAP measure
- **LTM** is in charge to:
  - Monitor the Demand and Capacity Imbalance at ATSU level
  - Identify hotspot at ATSU level
  - Identification appropriate ATFCM measure to solve the hotspot, including possibly DCB EAM measure
  - Provide request of DCB EAP measure to the EAP
  - Coordinate with adjacent FMP if necessary
- **EAP** is in charge to:
  - Receive request of DCB EAP measure from the LTM
  - Analyse the request DCB EAP measure from the LTM through the Traffic prediction HMI
  - Identify situation requesting a decomplexification measure through the Traffic prediction HMI
  - Prepare appropriate DCB EAP measure through the EAP terminal
  - Coordinate the implementation of the DCB EAP measure with the ATCO through the EAP terminal
  - Monitor the implementation of the DCB EAP measure through the EAP terminal and Traffic prediction HMI
- **ATCOs** are in charge to perform their normal operations. In addition, within the bEAP concept, they are in charge to:
  - Analyse the request of DCB EAP measure from the EAP
  - Answer regarding the request of DCB EAP measures through the ATCO Communication Tool
  - Implement the DCB EAM measures

  In any case, the DCB EAP measures proposed by the EAP are considered of lower priority by the ATCO in comparison to the management of the tactical situation.

Note 1: LTM and EAP are presented as two distinct persons on this figure. However, the LTM and EAP roles can be assumed by the same person.

Note 2: Only one EAP is presented on this figure. However, in case of large and complex ACC, several EAP can work at the same in the same ACC, with distinct EAP area of responsibility.

4.2.1.3 External Entities

Not relevant

4.2.2 Derivation of Safety Requirements (Functionality and Performance – success approach)

The bEAP OSED (see section 3 of [6]) includes an analysis of bEAP operation, encompassing two operational scenarios:

- Operational scenario 1: STAM or decomplexification measure required by the LTM (local network level)
- Operational scenario 2: Decomplexification measure at EAP level (no LTM supervision)

The operation within each scenario has been described and subsequently has been formalized by decomposing the operations into a set of Use Cases. Those Use Cases can be traced to the Safety Objectives (success) as follows:

ID	Use Case	Achieved by / Safety Objective [SO xx]
UC 1.1	Analysis of the LTM request	SO_EAP_001
UC 1.2	Preparation of the LTM request	SO_EAP_003
UC 1.3	Coordination of the LTM request	SO_EAP_004
UC 1.4	Implementation of the LTM request	SO_EAP_005
UC 2.1	Analysis of the decomplexification measure	SO_EAP_002
UC 2.2	Preparation of the decomplexification measure	SO_EAP_003
UC 2.3	Coordination of the decomplexification measure	SO_EAP_004
UC 2.4	Implementation of a decomplexification measure	SO_EAP_005

Table 8: bEAP Solution Operational Services & Safety Objectives (success approach)

In the OSED (see section 3 of [6]), each Use Case has been analysed in detail in terms of Actors, Pre-conditions, Post-conditions and Flows.

This safety assessment derives SPR-level requirements by undertaking in next section 4.3 an analysis of the SPR-level model covering all the Safety Objectives (and consequently all the use cases).

4.3 Analysis of the SPR-level Model – Normal Operational Conditions

This section is concerned with ensuring that the SPR-level design is complete, correct and internally coherent with respect to the Safety Requirements (success approach) derived for the normal operating conditions that were used to develop the corresponding Safety Objectives (success approach) in section 3.6.2.

Table 16 in Appendix B presents the mapping between the Safety Objective (Functionality and Performance) identified in section 3 and the elements of the SPR-level model. In addition, it present the Safety Requirements derived on the elements of the SPR-level model.

The Table 9 below presents the Safety Requirements derived from this mapping.

ID	Safety Requirement (functionality & performance)	Safety Objective
SR_EAP_001	LTM shall provide request of EAP DCB measure to the EAP	SO_EAP_001
SR_EAP_002	The EAP shall analyse and monitor the predicted occupancy count on all TFV in the EAP area of responsibility within a timeframe of one hour	SO_EAP_001 & SO_EAP_002
SR_EAP_003	The EAP shall analyse and monitor the traffic count on all TFV in the EAP area of responsibility within a timeframe of one hour.	SO_EAP_001 & SO_EAP_002
SR_EAP_004	The EAP shall analyse and monitor filed, regulated or current ATFCM flight profiles on all TFV in the EAP area of responsibility, within a timeframe of one hour	SO_EAP_001 & SO_EAP_002
SR_EAP_005	The EAP shall be able to consult ATFCM relevant flight details within its area of responsibility	SO_EAP_001 & SO_EAP_002
SR_EAP_006	The EAP shall be able to identify and monitor the predicted intruders (types 1, 2 & 3) on all potential TFV in the EAP area of responsibility within a timeframe of one hour.	SO_EAP_001 & SO_EAP_002
SR_EAP_007	The EAP shall be provided with an appropriate air situation display dedicated to his/her tasks	SO_EAP_001 & SO_EAP_002
SR_EAP_008	EAP shall answer LTM if a request of EAP DCB measure is considered as no more valid	SO_EAP_001
SR_EAP_009	The EAP shall assess ATCO workload on all TFV in the EAP area of responsibility within a timeframe of one hour.	SO_EAP_002

ID	Safety Requirement (functionality & performance)	Safety Objective
SR_EAP_010	The EAP shall be able to create of a local hotspot from a given flights list through the EAP terminal	SO_EAP_002
SR_EAP_011	The EAP shall hold (or having held) an ATCO rating	SO_EAP_002
SR_EAP_012	The EAP shall be able to create and prepare DCB EAP measures through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility	SO_EAP_003
SR_EAP_013	The EAP shall be able to create a STAM through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility	SO_EAP_003
SR_EAP_014	The EAP shall be able to create a de-complexification measure through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility	SO_EAP_003
SR_EAP_015	EAP shall be able to highlight urgent or late DCB EAP measures through EAP terminal	SO_EAP_003
SR_EAP_016	The EAP shall inform the FMP in case of inability to identify a solution that satisfy the LTM request	SO_EAP_003
SR_EAP_017	The EAP shall be able to propose a DCB EAP Measure to Implementing sector through EAP terminal	SO_EAP_004
SR_EAP_018	ATCO of implementing sector shall receive propositions of DCB EAP measures from the EAP through the CWP Communication tool	SO_EAP_004
SR_EAP_019	Proposition of DCB EAP measures relating to flight not yet known by the ATC system of the implementing sector shall not be displayed on the CWP Communication tool	SO_EAP_004
SR_EAP_020	ATCO shall be informed through specific stimuli on the CWP Communication tool in case of urgent or late DCB EAP measure.	SO_EAP_004
SR_EAP_021	ATCO of implementing sector shall analyse the proposition of DCB EAP measure from the EAP	SO_EAP_004
SR_EAP_022	ATCO of implementing sector shall coordinate the proposed DCB EAP measure with adjacent sector if necessary	SO_EAP_004
SR_EAP_023	ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation.	SO_EAP_004

ID	Safety Requirement (functionality & performance)	Safety Objective
SR_EAP_024	ATCO of implementing sector shall answer to the EAP regarding the proposed DCB EAP measure through CWP Communication tool	SO_EAP_004
SR_EAP_025	The EAP shall be informed of the answer from the implementing sector (accepted, rejected or implemented) regarding a DCB EAP measure, through the EAP Terminal	SO_EAP_004 & SO_EAP_005
SR_EAP_026	The EAP shall be able to send a reminder regarding a DCB measure via the EAP terminal	SO_EAP_004
SR_EAP_027	The EAP shall be able to edit a DCB EAP measure through EAP terminal when needed	SO_EAP_004
SR_EAP_028	The EAP shall be able to inform Off-Loaded sector and all On-Loaded sector(s) inside the ATSU, of every STAMs accepted or implemented through EAP terminal	SO_EAP_004
SR_EAP_029	ATCO of Off-Loaded sector and all On-Loaded shall be informed of accepted or implemented STAM impacting their sector, through the CWP Communication tool	SO_EAP_004
SR_EAP_030	ATCO of implementing sector shall inform the EAP though CWP communication tool when a proposition of DCB EAP measure has been correctly implemented	SO_EAP_004
SR_EAP_031	The EAP shall be able to monitor DCB EAP measures under the EAP area of responsibility	SO_EAP_005
SR_EAP_032	The EAP should be able to access to operational history of past DCB EAP measures of the day, through EAP Terminal	SO_EAP_005

Table 9: Derivation of Safety Requirements (functionality and performance) from Safety Objectives

4.4 Analysis of the SPR-level Model – Abnormal Operational Conditions

This section is concerned with ensuring that the SPR-level Design is complete, correct and internally coherent with respect to the Safety Requirements (Functionality and Performance) derived for the abnormal operating conditions that were used to derive the corresponding Safety Objectives (success approach) in section 3.6.2.

The analysis of the consequences of abnormal conditions on bEAP operations has been performed in section 3.7 where the abnormal conditions have been identified and for each abnormal condition the

operational effects have been assessed in order to identify the appropriate mitigation of the risk associated to those effects, based on the bEAP specification. The mitigations were of three types:

- Mitigations already existing in the Baseline operations (continuing to be available with the introduction of the Concept); no additional safety requirement need to be derived;
- Safety Objectives (functionality & performance) already identified within Normal operational conditions (i.e. SO_EAP_005 regarding monitoring of the implementation of DCB EAP measures); the related Safety Requirements are identified at section 4.3 above;
- New Safety Objectives derived for abnormal operational conditions in section 3.7.2; dedicated Safety Requirements are derived in this section. Only one new safety objective has been identified from the analysis of the abnormal operational conditions: SO_EAP_006 ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation.

Ref	Abnormal Conditions / SO (*Functionality and Performance*)	Mitigations (SR 0xx and/or A 0xx)
1	ANB5: Aircraft emergency SO_EAP_006 ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation	One safety requirement is already derived in section 4.3, in relation to SO_EAP_004 SR_EAP_023: ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation

Table 10: Safety Requirements or Assumptions to mitigate abnormal conditions

In conclusion, no safety requirement additional to those already identified or defined in previous sections, has been derived in relation to the mitigation of the effects of abnormal conditions.

4.5 Design Analysis – Case of Internal System Failures

Since the consequences of the identified system-generated hazards have been derived and analysed at the OSED level in the FHA process (see section 3.8 above), this part of the safety assessment focuses on the causes of those hazards, i.e. the PSSA process. It is performed in the following steps:

- Identification, for each system-generated hazard, of the failures of the SPR model elements that could cause the hazard;
- Derivation of mitigations to reduce the likelihood that specific failures would propagate up to the Hazard (i.e. operational level) - these mitigations are either identified as Safety Requirements that have been already been derived in the previous safety assessment steps, or captured as additional Safety Requirements (Functionality and Performance);

- Setting of safety integrity/reliability Safety Requirements to limit the frequency with which each identified hardware failure could be allowed to occur, such that the residual risk is within the specified numeric values as per section 3.8.2 above;

4.5.1 Causal Analysis

The detailed analysis of internal system failure is presented in Appendix C.

For each hazard, this table present:

- The possible failure of SPR level element that could contribute to the hazard. For each hazard, the possible contribution of following SPR level elements is considered:
  - LTM
  - EAP
  - ATCO
  - ETFMS
  - EAP Terminal (Hardware)
  - "EAP Terminal (Software)"
  - CWP Communication tool (Hardware)
  - CWP Communication tool (Software)
- The preventive mitigations (i.e. to reduce the likelihood that the causes would propagate up to the Hazard) that is associated to each cause. These mitigations are either identified as Safety Requirements that have been already been derived in previous steps and/or within the OSED/SPR, or captured as additional Safety Requirements (Functionality and Performance).

4.5.2 Safety Requirements derived from cause analysis

Table 11 and Table 12 respectively collect the additional Functional/Performance Safety Requirements and Integrity Safety Requirements derived within the failure approach for bEAP.

ID	Safety Requirement	Derived from
SR_EAP_033	Training of EAP shall ensure their qualification is adequate to identify the predicted traffic situation that requires decomplexification measure.	HZ_EAP_01
SR_EAP_035	EAP shall be informed of a loss of connection between EAP Terminal and ETFMS	HZ_EAP_02"
SR_EAP_036	Training of EAP shall ensure their qualification is adequate to propose feasible DCB EAP measure to the ATCO (e.g. feasibility due to aircraft performance...)	HZ_EAP_01
SR_EAP_037	In case of absence of answer from the ATCO regarding a	HZ_EAP_02

ID	Safety Requirement	Derived from
	DCB EAP measure after a significant period, EAP shall be informed of the rejection of the measure through the EAP terminal.	
SR_EAP_039	Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure that are inefficient or that have contrary effects (generate imbalance in the target sector or in others sectors)	HZ_EAP_02
SR_EAP_040	The EAP shall be able to request the refresh of the traffic prediction data on the EAP Terminal	"HZ_EAP_03
SR_EAP_041	Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure which are too difficult/workload demanding to implement	HZ_EAP_04
SR_EAP_042	LTM shall provide the request of DCB EAP measure to the EAP sufficiently in advance to allow him to analyse, prepare and implement the measure.	HZ_EAP_05"
SR_EAP_043	EAP shall provide the DCB EAP measure to the ATCO sufficiently in advance to allow them to analyse and implement the measure.	"HZ_EAP_03

Table 11: Safety Requirements (Functional and Performance) to mitigate internal failure

ID	Safety Requirement	Derived from
SR_EAP_034	The continuity failure of the EAP Terminal shall not occur more frequently than 1e-3 per sector ops hour	"HZ_EAP_01
SR_EAP_038	The continuity failure of the CWP Communication tool shall not occur more frequently than 1e-3 per sector ops hour	HZ_EAP_02

Table 12: Safety Requirements (Integrity) to mitigate internal failure

4.6 Achievability of the SAfety Criteria

Safety requirements are defined in section 4.2 to 4.5 in order to meet the bEAP Safety Criteria defined in section 3.5.

The safety requirements of this section have been defined in regard to:

- The results of the VP687 validation exercise (see Validation Report [7]). In particular, this exercise focused on the evaluation of following safety benefits

- Reduction of ATCO and LTM actors workload due to better coordination and mutual situational awareness,
- Reduction of unforeseen ATCO overloads thanks to the monitoring of Intruders.

- The feedback from the experimentation/implementation project 4Me in French Reims ACC.

The content of this section has also been reviewed by bEAP concept experts.

4.7 Realism of the SPR-level Design

The development and safety analysis of the SPR-level design would be seriously undermined if it were found in the subsequent Implementation phase that the Safety Requirements were either not 'testable' or impossible to satisfy, and / or that some of the assumptions were in fact incorrect.

The achievability and testability of the safety requirements and assumption from this document is ensures through the review of the present document by operational and technical experts.

4.8 Validation & Verification of the Safe Design at SPR Level

Consolidated list of Safety Requirements is provided in Appendix D. The process by which these safety objectives were derived is presented in previous section 4.2 to 4.5.

5 Detailed Safe Design at Physical Level

No applicable for bEAP concept

6 Acronyms and Terminology

Acronym	Definition
ACC	Area Control Centre
ACT	Flight Activated by ATC systems and processed by ETFMS
AMAN	Arrival Manager
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATFCM	Air Traffic Flow and Capacity Management
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATSU	Air Traffic Service Unit
*b*EAP	*basic* Extended ATC Planning
CHMI	CFMU Human Machine Interface
CNS	Communication Navigation and Surveillance
CR	Change Request
CTO	Controlled Time Over
CWP	Controller Working Position
DCB	Demand and Capacity Balancing
dDCB	Dynamic Demand and Capacity Balancing
EAP	Extended ATC Planning role or Extended ATC Planning
EAP Area	Extended ATC Planning Area
EATMA	European ATM Architecture
ETFMS	Enhanced Tactical Flow Management System operated by NMOC
FDPS	Flight Data Processing System
FMP	Flow Management Position
FRA	Fixed Routing Airspace
HMI	Human Machine Interface
INAP	Integrated Network management and extended ATC Planning
INTEROP	Interoperability Requirements
IRS	Interface Requirements Specification

Acronym	Definition
KPA	Key Performance Area
LTM	Local Traffic Manager
MSP	Multi Sector Planner
NM	Network Management or Network Manager
NMOC	Network Management Operation Centre
OI	Operational Improvement
OSED	Operational Service and Environment Definition
PC	Planning Controller
SAC	Safety Criteria
SAR	Safety Assessment Report
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SPR	Safety and Performance Requirements
STAM	Short Term ATFCM Measures
SWIM	System Wide Information Model
TC	Tactical Controller also termed Executive Control
TS	Technical Specification
TFV	Traffic volume
UAC	Upper Area Control Centre

Table 13: Acronyms and terminology

7 References

Safety

[1] SESAR, Safety Reference Material, Edition 4.0, April 2016

[2] SESAR, Guidance to Apply the Safety Reference Material, Edition 3.0, April 2016

[3] SESAR Safety Assessment Plan Template

[4] SESAR, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015

[5] SESAR, Resilience Engineering Guidance, May 2016

[6] SESAR Solution#118 – SPR/INTEROP/OSED V3 - Basic Extended ATC Planning - Edition 01.00.01, 15/05/2018

[7] SESAR Solution#118 – Validation Report V3 - Basic Extended ATC Planning Edition 01.00.00, 28/02/2018

Appendix A Safety Objectives

Following tables lists the safety objectives derived from the safety assessment at OSED level (cf. section 3)

- Safety objectives referenced as
-

A.1 Safety Objectives (Functionality and Performance)

ID	Description
SO_EAP_001	EAP shall receive and analyse request of DCB EAP measure from the LTM
SO_EAP_002	EAP shall identify situations requesting a de-complexification measure
SO_EAP_003	EAP shall prepare appropriate DCB EAP measures
SO_EAP_004	EAP shall coordinate the implementation of DCB EAP measures with ATCO
SO_EAP_005	EAP shall monitor the implementation of DCB EAP measures
SO_EAP_006	ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation.

Table 14: List of functional and performance safety objectives

A.2 Safety Objectives (Integrity)

ID	Description
SO_EAP_101	The frequency of occurrence of a lack of detection of need for a DCB EAP measure shall not be greater than 2.0x10-3 per sector ops hour
SO_EAP_102	The frequency of occurrence of a DCB EAP measure not implemented shall not be greater than 2.0x10-3 per sector ops hour
SO_EAP_103	The frequency of occurrence of a DCB EAP measure inefficient shall not be greater than 2.0x10-3 per sector ops hour
SO_EAP_104	The frequency of occurrence of a DCB EAP measure with contrary effect on the target sector shall not be greater than 2.4x10-5 per sector ops hour
SO_EAP_105	The frequency of occurrence of a DCB EAP measure generating imbalance in other sectors shall not be greater than 2.0x10-3 per sector ops

	hour
SO_EAP_106	The frequency of occurrence of a DCB EAP measure generating excessive workload in implementing sector shall not be greater than 2.0x10-3 per sector ops hour

Table 15: List of integrity safety objectives

Appendix B Derivation of Safety Requirements (Functionality and Performance) – Normal operation

Table 16 below present the mapping between the Safety Objective (Functionality and Performance) identified in section 3 and the elements of the SPR-level model.

In addition, it present the Safety Requirements derived on the elements of the SPR-level model.

Safety Objectives	Maps on to	Requirement
SO_EAP_001: EAP shall receive and analyse request of DCB EAP measure from the LTM	LTM	**SR_EAP_001**: LTM shall provide request of EAP DCB measure to the EAP
	EAP	**SR_EAP_002**: The EAP shall analyse and monitor the predicted occupancy count on all TFV in the EAP area of responsibility within a timeframe of one hour
	EAP	**SR_EAP_003**: The EAP shall analyse and monitor the traffic count on all TFV in the EAP area of responsibility within a timeframe of one hour.
	EAP	**SR_EAP_004**: The EAP shall analyse and monitor filed, regulated or current ATFCM flight profiles on all TFV in the EAP area of responsibility, within a timeframe of one hour
	EAP	**SR_EAP_005**: The EAP shall be able to consult ATFCM relevant flight details within its area of responsibility
	EAP	**SR_EAP_006**: The EAP shall be able to identify and monitor the predicted intruders (types 1, 2 & 3) on all potential TFV in the EAP area of responsibility within a timeframe of one hour.

Safety Objectives	Maps on to	Requirement
	EAP	**SR_EAP_007**: The EAP shall be provided with an appropriate air situation display dedicated to his/her tasks
	EAP	**SR_EAP_008**: EAP shall answer LTM if a request of EAP DCB measure is considered as no more valid
SO_EAP_002: EAP shall identify situations requesting a decomplexification measure	EAP	**SR_EAP_009**: The EAP shall assess ATCO workload on all TFV in the EAP area of responsibility within a timeframe of one hour.
	EAP	**SR_EAP_002**: The EAP shall analyse and monitor the predicted occupancy count on all TFV in the EAP area of responsibility within a timeframe of one hour
	EAP	**SR_EAP_003**: The EAP shall analyse and monitor the traffic count on all TFV in the EAP area of responsibility within a timeframe of one hour.
	EAP	**SR_EAP_004**: The EAP shall analyse and monitor filed, regulated or current ATFCM flight profiles on all TFV in the EAP area of responsibility, within a timeframe of one hour
	EAP	**SR_EAP_005**: The EAP shall be able to consult ATFCM relevant flight details within its area of responsibility
	EAP	**SR_EAP_006**: The EAP shall be able to identify and monitor the predicted intruders (types 1, 2 & 3) on all potential TFV in the EAP area of responsibility within a timeframe of one hour.
	EAP	**SR_EAP_007**: The EAP shall be provided with an appropriate air situation display dedicated to his/her tasks

Safety Objectives	Maps on to	Requirement
	EAP, EAP Terminal	**SR_EAP_010**: The EAP shall be able to create of a local hotspot from a given flights list through the EAP terminal
	EAP	**SR_EAP_11**: The EAP shall hold (or having held) an ATCO rating
SO_EAP_003: EAP shall prepare appropriate DCB EAP measures	EAP, EAP Terminal	**SR_EAP_12**: The EAP shall be able to create and prepare DCB EAP measures through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility
	EAP, EAP Terminal	**SR_EAP_13**: The EAP shall be able to create a STAM through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility
	EAP, EAP Terminal	**SR_EAP_14**: The EAP shall be able to create a decomplexification measure through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility
	EAP, EAP Terminal	**SR_EAP_15**: The EAP shall be able to highlight urgent or late DCB EAP measures through EAP terminal
	EAP	**SR_EAP_16**: The EAP shall inform the FMP in case of inability to identify a solution that satisfy the LTM request
SO_EAP_004: EAP shall coordinate the implementation of DCB EAP measures with ATCO	EAP, EAP Terminal	**SR_EAP_17**: The EAP shall be able to propose a DCB EAP Measure to Implementing sector through EAP terminal
	ATCO,	**SR_EAP_18**: ATCO of implementing sector shall receive propositions of DCB EAP

Safety Objectives	Maps on to	Requirement
	CWP Comm tool	measures from the EAP through the CWP Communication tool
	ATCO, CWP Comm tool	**SR_EAP_19**: Proposition of DCB EAP measures relating to flight not yet known by the ATC system of the implementing sector shall not be displayed on the CWP Communication tool
	ATCO, CWP Comm tool	**SR_EAP_20**: ATCO shall be informed through specific stimuli on the CWP Communication tool in case of urgent or late DCB EAP measure.
	ATCO	**SR_EAP_21**: ATCO of implementing sector shall analyse the proposition of DCB EAP measure from the EAP
	ATCO	**SR_EAP_22**: ATCO of implementing sector shall coordinate the proposed DCB EAP measure with adjacent sector if necessary
	ATCO,	**SR_EAP_23**:
	ATCO, CWP Comm tool	**SR_EAP_24**: ATCO of implementing sector shall answer to the EAP regarding the proposed DCB EAP measure through CWP Communication tool
	EAP, EAP Terminal	**SR_EAP_25**: The EAP shall be informed of the answer from the implementing sector (accepted, rejected or implemented) regarding a DCB EAP measure, through the EAP Terminal

Safety Objectives	Maps on to	Requirement
	EAP, EAP Terminal	**SR_EAP_26**: The EAP shall be able to send a reminder regarding a DCB measure via the EAP terminal
	EAP, EAP Terminal	**SR_EAP_27**: The EAP shall be able to edit a DCB EAP measure through EAP terminal when needed
	EAP, EAP Terminal	**SR_EAP_28**: The EAP shall be able to inform Off-Loaded sector and all On-Loaded sector(s) inside the ATSU, of every STAMs accepted or implemented through EAP terminal
	ATCO, CWP Comm tool	**SR_EAP_29**: ATCO of Off-Loaded sector and all On-Loaded shall be informed of accepted or implemented STAM impacting their sector, through the CWP Communication tool
	ATCO, CWP Comm tool	**SR_EAP_30**: ATCO of implementing sector shall inform the EAP though CWP communication tool when a proposition of DCB EAP measure has been correctly implemented
SO_EAP_003: EAP shall prepare appropriate DCB EAP measures	EAP,	**SR_EAP_31**: The EAP shall be able to monitor DCB EAP measures under the EAP area of responsibility
	EAP, EAP Terminal	**SR_EAP_32**: The EAP should be able to access to operational history of past DCB EAP measures of the day, through EAP Terminal
	EAP,	**SR_EAP_27**: The EAP shall be able to edit a DCB EAP measure through EAP

Safety Objectives	Maps on to	Requirement
	EAP Terminal	terminal when needed
SO_EAP_006: ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation.	ATCO	**SR_EAP_23**:

Table 16: Mapping of Safety Objectives to SPR-level Model Elements

Appendix C Detailed Cause Analysis

Following table presents the detailed cause analysis of the bEAP hazards. For each hazard, it presents

- The possible SPR model element contributing to the hazard
- The mitigation means that are defined in order to prevent the failure of the SPR model element and the associated safety requirements or assumptions

HAZARD		CAUSE ANALYSIS		
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
HZ_EAP_01	No detection of need for a DCB EAP measure	LTM	LTM does not identify a hotspot	This cause is not impacted by the bEAP concept. No mitigation defined.
		EAP	EAP unable to identify a DCB EAP measure to solve the demand and capacity imbalance	EAP are not in charge of identification of need of STAM. LTM remain responsible for this task. EAP are in charge of identification of need of decomplexification measure. Following mitigations prevent inability of EAP to identify the need of decomplexification measure: SR_EAP_033: Training of EAP shall ensure their qualification is adequate to identify the predicted traffic situation that requires decomplexification measure. SR_EAP_011: The EAP shall hold (or having held) an ATCO rating. Requirement already identified within success approach
		ATCO	No cause on ATCO role for this hazard: ATCO are not in charge of identification of need of DCB EAP measure	-

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		ETFMS	Loss of connection from ETFMS	ETFMS is out of scope of the bEAP system. Following assumption is defined A_001: It is assumed that continuity of service of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions In addition, following requirement is defined to inform EAP of loss of connection with ETFMS SR_EAP_035: EAP shall be informed of a loss of connection between EAP Terminal and ETFMS
		EAP Terminal (Hardware)	EAP Terminal unavailable (hardware failure)	Following quantitative safety requirements is identification to ensure that hardware continuity failure of EAP Terminal will remain acceptable: SR_EAP_034: The continuity failure of the EAP Terminal shall not occur more frequently than 1e-3 per sector ops hour
		EAP Terminal (Software)	EAP Terminal unavailable (software failure)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_001: A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards
		CWP Commn tool	No cause on CWP Comm tool for this hazard: ATCO are not in charge of identification of need of DCB EAP measure	-
HZ_EAP_02	DCB EAP measure not implemented	LTM	LTM provides the request of DCB EAP measure to the EAP lately	Following mitigation is defined to ensure that EAP will have sufficient time to prepare and implement the DCB EAP measure SR_EAP_042: LTM shall provide the request of DCB EAP measure to the EAP sufficiently in advance to allow him to analyse, prepare and implement the measure.

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		EAP	DCB EAP measure proposed by the EAP is not feasible	Following mitigations prevent inability of EAP to identify the need of decomplexification measure: SR_EAP_036: Training of EAP shall ensure their qualification is adequate to propose feasible DCB EAP measure to the ATCO (e.g. feasibility due to aircraft performance...) SR_EAP_011: The EAP shall hold (or having held) an ATCO rating. Requirement already identified within success approach
		ATCO	ATCO is not able to implement the DCB EAP measure proposed by the ATCO	Following mitigation is defined to ensure that ATCO will have sufficient time to implement the DCB EAP measure: SR_EAP_043 : EAP shall provide the DCB EAP measure to the ATCO sufficiently in advance to allow them to analyse and implement the measure. Following mitigations are defined to inform the EAP in case of inability to implement a DCB EAP measure: SR_EAP_024: ATCO of implementing sector shall answer to the EAP regarding the proposed DCB EAP measure through CWP Communication tool SR_EAP_037: In case of absence of answer from the ATCO regarding a DCB EAP measure after a significant period, EAP shall be informed of the rejection of the measure through the EAP terminal.
		ETFMS	No cause on ETFM for this hazard. ETFMS is not involved in the implementation of the DCB EAP measures	-

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		EAP Terminal (Hardware)	EAP Terminal unavailable (hardware failure)	Following quantitative safety requirements is identification to ensure that hardware continuity failure of EAP Terminal will remain acceptable (equi-repartition of the safety objective on EAP Terminal and CWP communication tool): SR_EAP_034: The continuity failure of the EAP Terminal shall not occur more frequently than 1e-3 per sector ops hour
		EAP Terminal (Software)	EAP Terminal unavailable (software failure)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_001: A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards
		CWP Commn tool (Hardware)	CWP Communication tool (hardware failure)	Following quantitative safety requirements is identification to ensure that hardware continuity failure of EAP Terminal will remain acceptable (equi-repartition of the safety objective on EAP Terminal and CWP communication tool): SR_EAP_038: The continuity failure of the CWP Communication tool shall not occur more frequently than 1e-3 per sector ops hour
		CWP Commn tool (Software)	CWP Communication tool (software failure)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_002: A SWAL need to be allocated to the CWP Communication Tool considering is possible contribution to the bEAP hazards
HZ_EAP_03	DCB EAP measure inefficient	LTM	No cause on LTM role for this hazard: LTM is not in charge of the preparation or implementation of the DCB	-

HAZARD		CAUSE ANALYSIS		
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
			EAP measure	
		EAP	DCB EAP measure prepared and proposed by the EAP is inefficient	Following mitigations prevent EAP to propose inefficient measure or measure with negative aspects on target sector or others sectors: SR_EAP_039: Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure that are inefficient or that have contrary effects SR_EAP_011: The EAP shall hold (or having held) an ATCO rating. Requirement already identified within success approach
		ATCO	No cause on ATCO role for this hazard: ATCO are not in charge of preparation of the DCB EAP measure	-
		ETFMS	Inaccurate traffic prediction data provided by the ETFMS leading EAP to prepare inappropriate DCB EAP measure	ETFMS is out of scope of the bEAP system. Following assumption is defined A_002: It is assumed that integrity of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions.
		ETFMS	Loss of connection with ETFMS leading to display of out of date prediction data	Following requirements are defined to inform EAP of loss of connection with ETFMS: SR_EAP_040: EAP shall be informed of a loss of connection between EAP Terminal and ETFMS The EAP shall be able to request the refresh of the traffic prediction data on the EAP Terminal

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		EAP Terminal (Hardware)	Hardware failure of EAP Terminal cannot contribute to this hazard (only to unavailability of the EAP Terminal)	-
		EAP Terminal (Software)	Inaccurate traffic prediction data provided by the EAP Terminal leading EAP to prepare inappropriate DCB EAP measure	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_001: A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards
		CWP Commn tool (Hardware)	Hardware failure of CWP Communication tool cannot contribute to this hazard (only to unavailability of the tool)	-
		CWP Commn tool (Software)	Software failure of the CWP Communication tool leading to display of inappropriate DCB EAP measure (measure different from the one prepared by the EAP)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_002: A SWAL need to be allocated to the CWP Communication Tool considering is possible contribution to the bEAP hazards
HZ_EAP_04	DCB EAP measure with contrary effect on the target sector	LTM	No cause on LTM role for this hazard: LTM is not in charge of the preparation or implementation of the DCB EAP measure	-

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		EAP	DCB EAP measure prepared and proposed by the EAP has contrary effect on the target sector	Following mitigations prevent EAP to propose inefficient measure or measure with negative aspects on target sector or others sectors: SR_EAP_039: Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure that are inefficient or that have contrary effects SR_EAP_011: The EAP shall hold (or having held) an ATCO rating. Requirement already identified within success approach
		ATCO	No cause on ATCO role for this hazard: ATCO are not in charge of preparation of the DCB EAP measure	-
		ETFMS	Inaccurate traffic prediction data provided by the ETFMS leading EAP to prepare inappropriate DCB EAP measure	ETFMS is out of scope of the bEAP system. Following assumption is defined A_002: It is assumed that integrity of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions.
		ETFMS	Loss of connection with ETFMS leading to display of out of date prediction data	Following requirements are defined to inform EAP of loss of connection with ETFMS: SR_EAP_040: EAP shall be informed of a loss of connection between EAP Terminal and ETFMS The EAP shall be able to request the refresh of the traffic prediction data on the EAP Terminal
		EAP Terminal (Hardware)	Hardware failure of EAP Terminal cannot contribute to this hazard (only to unavailability of the EAP	-

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
			Terminal)	
		EAP Terminal (Software)	Inaccurate traffic prediction data provided by the EAP Terminal leading EAP to prepare inappropriate DCB EAP measure	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_001: A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards
		CWP Commn tool (Hardware)	Hardware failure of CWP Communication tool cannot contribute to this hazard (only to unavailability of the tool)	-
		CWP Commn tool (Software)	Software failure of the CWP Communication tool leading to display of inappropriate DCB EAP measure (measure different from the one prepared by the EAP)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_002: A SWAL need to be allocated to the CWP Communication Tool considering is possible contribution to the bEAP hazards
HZ_EAP_05	DCB EAP measure generating imbalance in other sectors	LTM	No cause on LTM role for this hazard: LTM is not in charge of the preparation or implementation of the DCB EAP measure	-

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		EAP	DCB EAP measure prepared and proposed by the EAP generates imbalance in others sectors	Following mitigations prevent EAP to propose inefficient measure or measure with negative aspects on target sector or others sectors: SR_EAP_039: Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure that are inefficient or that have contrary effects (generate imbalance in the target sector or in others sectors) SR_EAP_011: The EAP shall hold (or having held) an ATCO rating. Requirement already identified within success approach
		ATCO	No cause on ATCO role for this hazard: ATCO are not in charge of preparation of the DCB EAP measure	-
		ETFMS	Inaccurate traffic prediction data provided by the ETFMS leading EAP to prepare inappropriate DCB EAP measure	ETFMS is out of scope of the bEAP system. Following assumption is defined A_002: It is assumed that integrity of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions.
		ETFMS	Loss of connection with ETFMS leading to display of out of date prediction data	Following requirements are defined to inform EAP of loss of connection with ETFMS: SR_EAP_040: EAP shall be informed of a loss of connection between EAP Terminal and ETFMS The EAP shall be able to request the refresh of the traffic prediction data on the EAP Terminal
		EAP Terminal (Hardware)	Hardware failure of EAP Terminal cannot contribute to this hazard (only to unavailability of the EAP	-

HAZARD			CAUSE ANALYSIS	
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
			Terminal)	
		EAP Terminal (Software)	Inaccurate traffic prediction data provided by the EAP Terminal leading EAP to prepare inappropriate DCB EAP measure	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_001: A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards
		CWP Commn tool (Hardware)	Hardware failure of CWP Communication tool cannot contribute to this hazard (only to unavailability of the tool)	-
		CWP Commn tool (Software)	Software failure of the CWP Communication tool leading to display of inappropriate DCB EAP measure (measure different from the one prepared by the EAP)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_002: A SWAL need to be allocated to the CWP Communication Tool considering is possible contribution to the bEAP hazards
HZ_EAP_06	DCB EAP measure generating excessive workload in implementing sector	LTM	No cause on LTM role for this hazard: LTM is not in charge of the preparation or implementation of the DCB EAP measure	-

HAZARD		CAUSE ANALYSIS		
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		EAP	DCB EAP measure prepared and proposed by the EAP generates excessive workload in the implementing sector	Following mitigations prevent EAP to propose inefficient measure or measure with negative aspects on target sector or others sectors: SR_EAP_039: Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure which are too difficult/workload demanding to implement SR_EAP_011: The EAP shall hold (or having held) an ATCO rating. Requirement already identified within success approach
		ATCO	No cause on ATCO role for this hazard: ATCO are not in charge of preparation of the DCB EAP measure	-
		ETFMS	Inaccurate traffic prediction data provided by the ETFMS leading EAP to prepare inappropriate DCB EAP measure	ETFMS is out of scope of the bEAP system. Following assumption is defined A_002: It is assumed that integrity of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions.
		EAP Terminal (Hardware)	Hardware failure of EAP Terminal cannot contribute to this hazard (only to unavailability of the EAP Terminal)	-
		EAP Terminal (Software)	Inaccurate traffic prediction data provided by the EAP Terminal leading EAP to prepare inappropriate DCB EAP measure	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_001: A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards

HAZARD		CAUSE ANALYSIS		
HZ ID	**Hazard description**	**SPR model element**	**Cause description**	**Mitigations / Safety Requirements**
		CWP Commn tool (Hardware)	Hardware failure of CWP Communication tool cannot contribute to this hazard (only to unavailability of the tool)	-
		CWP Commn tool (Software)	Software failure of the CWP Communication tool leading to display of inappropriate DCB EAP measure (measure different from the one prepared by the EAP)	No SWAL assessment is performed in this document. This allocation depends on local architecture and is to be performed locally by ANSP. Following issue is defined: I_002: A SWAL need to be allocated to the CWP Communication Tool considering is possible contribution to the bEAP hazards

Table 17: bEAP concept – Detailed cause analysis

Appendix D Consolidated List of Safety Requirements

Following tables lists the safety requirements derived from the safety assessment at SPR level (cf. section 4)

D.1 Safety Requirements (Functionality and Performance)

ID	Description
SR_EAP_001	LTM shall provide request of EAP DCB measure to the EAP
SR_EAP_002	The EAP shall analyze and monitor the predicted occupancy count on all TFV in the EAP area of responsibility within a timeframe of one hour
SR_EAP_003	The EAP shall analyze and monitor the traffic count on all TFV in the EAP area of responsibility within a timeframe of one hour.
SR_EAP_004	The EAP shall analyze and monitor filed, regulated or current ATFCM flight profiles on all TFV in the EAP area of responsibility, within a timeframe of one hour
SR_EAP_005	The EAP shall be able to consult ATFCM relevant flight details within its area of responsibility
SR_EAP_006	The EAP shall be able to identify and monitor the predicted intruders (types 1, 2 & 3) on all potential TFV in the EAP area of responsibility within a timeframe of one hour.
SR_EAP_007	The EAP shall be provided with an appropriate air situation display dedicated to his/her tasks
SR_EAP_008	EAP shall answer LTM if a request of EAP DCB measure is considered as no more valid
SR_EAP_009	The EAP shall assess ATCO workload on all TFV in the EAP area of responsibility within a timeframe of one hour.
SR_EAP_010	The EAP shall be able to create of a local hotspot from a given flights list through the EAP terminal
SR_EAP_011	The EAP shall hold (or having held) an ATCO rating
SR_EAP_012	The EAP shall be able to create and prepare DCB EAP measures through EAP terminal in order to

ID	Description
	solve a given hotspot inside the EAP area of responsibility
SR_EAP_013	The EAP shall be able to create a STAM through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility
SR_EAP_014	The EAP shall be able to create a decomplexification measure through EAP terminal in order to solve a given hotspot inside the EAP area of responsibility
SR_EAP_015	EAP shall be able to highlight urgent or late DCB EAP measures through EAP terminal
SR_EAP_016	The EAP shall inform the FMP in case of inability to identify a solution that satisfy the LTM request
SR_EAP_017	The EAP shall be able to propose a DCB EAP Measure to Implementing sector through EAP terminal
SR_EAP_018	ATCO of implementing sector shall receive propositions of DCB EAP measures from the EAP through the CWP Communication tool
SR_EAP_019	Proposition of DCB EAP measures relating to flight not yet known by the ATC system of the implementing sector shall not be displayed on the CWP Communication tool
SR_EAP_020	ATCO shall be informed through specific stimuli on the CWP Communication tool in case of urgent or late DCB EAP measure.
SR_EAP_021	ATCO of implementing sector shall analyse the proposition of DCB EAP measure from the EAP
SR_EAP_022	ATCO of implementing sector shall coordinate the proposed DCB EAP measure with adjacent sector if necessary
SR_EAP_023	ATCO shall consider the proposition of DCB EAP measures of lower priority in comparison to management of the tactical situation.
SR_EAP_024	ATCO of implementing sector shall answer to the EAP regarding the proposed DCB EAP measure

ID	Description
	through CWP Communication tool
SR_EAP_025	The EAP shall be informed of the answer from the implementing sector (accepted, rejected or implemented) regarding a DCB EAP measure, through the EAP Terminal
SR_EAP_026	The EAP shall be able to send a reminder regarding a DCB measure via the EAP terminal
SR_EAP_027	The EAP shall be able to edit a DCB EAP measure through EAP terminal when needed
SR_EAP_028	The EAP shall be able to inform Off-Loaded sector and all On-Loaded sector(s) inside the ATSU, of every STAMs accepted or implemented through EAP terminal
SR_EAP_029	ATCO of Off-Loaded sector and all On-Loaded shall be informed of accepted or implemented STAM impacting their sector, through the CWP Communication tool
SR_EAP_030	ATCO of implementing sector shall inform the EAP though CWP communication tool when a proposition of DCB EAP measure has been correctly implemented
SR_EAP_031	The EAP shall be able to monitor DCB EAP measures under the EAP area of responsibility
SR_EAP_032	The EAP should be able to access to operational history of past DCB EAP measures of the day, through EAP Terminal
SR_EAP_033	Training of EAP shall ensure their qualification is adequate to identify the predicted traffic situation that requires decomplexification measure.
SR_EAP_035	EAP shall be informed of a loss of connection between EAP Terminal and ETFMS
SR_EAP_036	Training of EAP shall ensure their qualification is adequate to propose feasible DCB EAP measure to the ATCO (e.g. feasibility due to aircraft performance...)

ID	Description
SR_EAP_037	In case of absence of answer from the ATCO regarding a DCB EAP measure after a significant period, EAP shall be informed of the rejection of the measure through the EAP terminal.
SR_EAP_039	Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure that are inefficient or that have contrary effects (generate imbalance in the target sector or in others sectors)
SR_EAP_040	The EAP shall be able to request the refresh of the traffic prediction data on the EAP Terminal
SR_EAP_041	Training of EAP shall ensure their qualification is adequate to prevent the design of DCB measure which are too difficult/workload demanding to implement
SR_EAP_042	LTM shall provide the request of DCB EAP measure to the EAP sufficiently in advance to allow him to analyse, prepare and implement the measure.
SR_EAP_043	EAP shall provide the DCB EAP measure to the ATCO sufficiently in advance to allow them to analyse and implement the measure.

Table 18: List of functional and performance safety requirements

D.2 Safety Requirements (Integrity)

ID	Description
SR_EAP_034	The continuity failure of the EAP Terminal shall not occur more frequently than 1e-3 per sector ops hour
SR_EAP_038	The continuity failure of the CWP Communication tool shall not occur more frequently than 1e-3 per sector ops hour

Table 19: List of integrity safety requirements

Appendix E Assumptions, Safety Issues & Limitations

E.1 Assumptions log

The following Assumptions were necessarily raised in deriving the above Functional and Performance Safety Requirements:

Ref	Assumption	Validation
A001	It is assumed that continuity of service of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions	To be validated through review by NM experts
A002	It is assumed that integrity of ETFMS is sufficient to allow LTM and EAP to assessment prediction of traffic in safe conditions.	To be validated through review by NM experts

Table 20: Assumptions log

E.2 Safety Issues log

The following Safety Issues were necessarily raised during the safety assessment:

Ref	Safety issue	Resolution
I001	A SWAL need to be allocated to the EAP Terminal considering is possible contribution to the bEAP hazards	To be addressed during local implementation
I002	A SWAL need to be allocated to the CWP Communication Tool considering is possible contribution to the bEAP hazards	To be addressed during local implementation

Table 21: Safety Issues log

E.3 Operational Limitations log

No operational limitation is identified

-END OF DOCUMENT-