INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

# SESAR Solution PJ.02-W2-21.1 SPR/INTEROP-OSED for V3 - Part II - Safety Assessment Report (SAR)

| | |
|---|---|
| **Deliverable ID:** | **D6.1.002** |
| **Dissemination Level:** | **PU** |
| **Project Acronym:** | **AART** |
| **Grant:** | **874477** |
| **Call:** | **H2020-IBA-SESAR-2019-1** |
| **Topic:** | **Airport Airside and Runway Throughput** |
| **Consortium Coordinator:** | **Eurocontrol** |
| **Edition Date:** | **24 May 2023** |
| **Edition:** | **00.01.02** |
| **Template Edition:** | **00.00.04** |

## Authoring & Approval

### Authors of the document

| Beneficiary | Date |
|---|---|
| ENAIRE | 12/12/2022 |

### Reviewers internal to the project

| Beneficiary | Date |
|---|---|
| DFS | 21/02/2023 |
| LEONARDO | 20/02/2023 |
| Indra | 22/02/2023 |
| ENAIRE | 27/02/2023 |

### Reviewers external to the project

| Beneficiary | Date |
|---|---|
| PJ19 Safety Team | 22/02/2023 |

### Approved for submission to the S3JU By - Representatives of all beneficiaries involved in the project

| Beneficiary | Date |
|---|---|
| DFS | 28/02/2023 |
| LEONARDO | 28/02/2023 |
| Indra | 28/02/2023 |
| ENAIRE | 28/02/2023 |

### Rejected By - Representatives of beneficiaries involved in the project

| Beneficiary | Date |
|---|---|
| | |
| | |

## Document History

| Edition | Date | Status | Beneficiary | Justification |
|---|---|---|---|---|
| 00.00.01 | 12/12/2022 | Draft | ENAIRE | Initial Draft |
| 00.00.02 | 05/02/2022 | Version for internal review | ENAIRE | Version for internal review |
| 00.00.03 | 22/02/2022 | Version including internal reviews | ENAIRE, LEONARDO, DFS, Indra | Version including comments from LEONARDO, DFS, INDRA and ENAIRE |
| 00.00.04 | 22/02/2022 | Version for external review | ENAIRE | Version for external review |
| 00.01.00 | 28/02/2022 | Final Version | ENAIRE | Submitted Version |
| 00.01.01 | 04/05/2023 | Update | ENAIRE | Version considering SJU reviews and Maturity Gate comments. |
| 00.01.02 | 22/05/2023 | Final Version | DFS | Version for submission with updated references to updated data package documents |

# AART

AIRPORT AIRSIDE AND RUNWAY THROUGHPUT

This **PJ.02-W2-21.1 Safety Assessment Report for V3** is part of a project that has received funding from the SESAR3 Joint Undertaking under grant agreement No 874477 under European Union's Horizon 2020 research and innovation programme.

## Abstract

The purpose of this Safety Assessment Report for Solution **PJ.02-W2-21.1 — Extended Airport Safety Nets for Controllers at A-SMGCS Airports** is to analyse the analysed solution from a safety perspective, identifying and evaluating the risks that it generates, and finding mitigation measures to minimize or eliminate their impact on aviation. With this aim, a series of Safety Requirements, both at ATS service level (SRS) and at refined design level (rSRD), are being established.

# Table of Contents

# List of Tables

## List of Figures

# 1 Executive Summary

Safety is enhanced for airport operations as Support Tools for controllers at A-SMGCS Airports detect potential and actual conflicting situations, incursions and non-conformance to procedures or ATC clearances, involving mobiles (and stationary traffic) on runways, taxiways and in the apron/stand/gate area as well as unauthorised/unidentified traffic. Controllers are provided in all cases with the appropriate predictive indications and alerts.

This document contains the Specimen Safety Assessment for a typical application of the PJ.02-W2-21.1 Solution in operations. The Safety Assessment Report (SAR) represents Part II of the SPR-INTEROP/OSED document and presents the assurance that the Safety Requirements for the V1-V3 phases are complete, correct, and realistic, thereby providing all material to adequately inform the PJ.02-W2-21.1 Solution SPR-INTEROP/OSED and TS/IRS.

Solution PJ.02-W2-21.1 builds on the work performed in SESAR 1 Solution #02 (Operational Improvement OI AO-0104-A) and SESAR 2020 Wave 1 Solution PJ.03b-01 (Operational Improvement OI AO-0104-B). This solution PJ.02-W2-21.1, which develops enhanced airport safety nets for controllers at A-SMGCS Airports, includes safety assessment activities to support the Design and Validation activities of the solution.

# 2 Introduction

## 2.1 Background

ICAO, EUROCONTROL, European Commission and other international organizations have developed specific programmes to prevent ground accidents. As a first example, Doc 9476 of ICAO includes that traffic on the airport surface should be controlled according to “seen and be seen” principle. Besides, A-SMGCS has been established at ICAO (Doc. 9830), EUROCAE (Doc ED.87) and EUROCONTROL A-SMGCS Specification.

Nevertheless, further improvements of the Airport Safety Nets and their extension to cover the whole airport movement area are needed.

Solution PJ.02-W2-21.1 updates and extends the Airport Safety Nets Conflicting ATC Clearances (CATC) and Conformance Monitoring Alerts for Controllers (CMAC) to cover the entire airport surface.

Based on airport surveillance data and electronic environment integrating ATC clearances, taxi-routes and local procedures the Safety Support Tools for controllers upgrade the Advanced Surface Movement Guidance and Control System (A-SMGCS) to detect potential and actual conflicting situations, incursions and non-conformance to procedures or ATC clearances, involving mobiles (and stationary traffic) on runways, taxiways and in the apron/stand/gate area as well as unauthorised/unidentified traffic.

The solution targets traffic Safety on the entire movement area on medium, large, and very large airports and during take-off and landing.

Appropriate predictive indications and alerts are provided to controllers in all cases, increasing situational awareness and giving automated support to avoid hazardous situations. This is expected to raise benefits in Safety and Human Performance.

| SESAR Solution ID | SESAR Solution Title | OI Steps ID | OI Steps Title | Enabler ID | Enabler Title | OI Step/Enabler Coverage |
|---|---|---|---|---|---|---|
| **PJ.02-W2-21.1** | Enhanced Airport Safety Nets for Controllers at A-SMGCS Airports | **AO-0104-B** | Enhanced Airport Safety Nets for Controllers at A-SMGCS Airports | **AERODROME-ATC-06b** | A-SMGCS incorporating the function that detects Conflicting ATC Clearances (CATC) on the entire airport surface | **OI step/Enable:** **Fully** **Enabler:** Required |
| | | | | **AERODROME-ATC-07b** | A-SMGCS incorporating the function that provides an advanced set of Conformance Monitoring Alerts for Controllers | **OI step/Enable:** **Fully** **Enabler:** Required |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | (CMAC) on the movement area | |
| | | | | **AERODROME-ATC-115** | A-SMGCS incorporating the function that provides RMCA/CMAC vs ATC Clearance alerts | **OI step/Enable:**<br>**Fully**<br>**Enabler:** Required |
| | | | | **AERODROME-ATC-116** | A-SMGCS incorporating the function that provides Runway-Busy notifications | **OI step/Enable:**<br>**Fully**<br>**Enabler:** Required |

**Figure 1: SESAR Solution PJ.02-W2-21.1 Scope and related OI steps**

The specific alerts covered by the OI Step of Solution PJ.02-W2-21.1 are:

- Enhanced CATC alerts:
    - CATC alert-Push-back vs Push-back
    - CATC alert-Push-back vs Taxi and Taxi vs Push-back
    - CATC alert-Taxi vs Taxi
    - CATC alert-Land vs Land
    - CATC alert-Take-off vs Land
    - CATC alert-Cross vs Land
    - CATC alert-Take-off vs Take-off (Converging SIDs)
- RMCA vs Clearance Alert
- CMAC vs Clearance Alert
- CMAC Occupied Stand

Moreover, the solution includes:

- The **predictive indication** and **runway notifications** which supports the ATCO in assessing the current situation and to decide whether it is safe to enter the next clearance or not. Hence the predict indicator prevents ATCO before giving the clearance.
- The concept of **Conditional clearance.** A conditional Clearance is an instruction that is issued by the air traffic controller and only takes effect when a certain condition is met (see OSED [13] section 3.3.2.2.2.2. for more details).

## 2.2 General Approach to Safety Assessment

This safety assessment is conducted as per the SESAR Safety Reference Material (SRM) which in turn is based on a twofold approach:

- a success approach which is concerned with the safety of the Solution operations in the absence of failure within the end-to-end Solution functional system, encompassing both Normal operation and Abnormal conditions,
- a conventional failure approach which is concerned with the safety of the Solution operations in the event of failures within the end-to-end Solution functional system.

These two approaches are applied to the derivation of safety properties at each of the successive lifecycle stages of the Solution development (Safety Requirements at service level and at design level).

## 2.3 Scope of the Safety Assessment

This report includes the setting of the Safety Criteria (SAC), a description of the key properties of the environment, the safety specification (at OSED level), safe design (at SPR level) and detailed safe design (at physical level). It also presents the assurance that the Safety Requirements defined herein are complete, correct and (from an implementation standpoint) realistic. Since the properties of the operational environment (OE) are crucial to the safety assessment, this assessment cannot be generic but specific to the OE defined in the solution.

The following parts of the PJ.02-W2-21.1 safety assessment lifecycle are covered by the current issue of the Safety Assessment Report:

- **V1** – through initial identification of safety implications of the Change and the definition of Safety Criteria
- **V2&V3** -through establishing **Safety Requirements at Service level (SRS)** to deliver the Safety Criteria and the derivation of **Safety Requirements at design level** (**SRD**) to satisfy the SRSs (based on combined safety analysis of the design, data analysis and safety-related measurements, observations and debriefing of the validation exercises). The safety assessment for Safety Requirements derivation will align with the design maturity. The safety assessment will be conducted to the level of granularity decided by the Project for the SPR-INTEROP/OSED and TS/IRS documents for the design of the Functional system for the Solution (encompassing people, procedures and equipment).

  The SRDs are derived during the V2&V3 phases of the development lifecycle. The purpose is to feed the SESAR Solution PJ.02-W2-21.1 SPR-INTEROP/OSED Part I and, if applicable, the TS/IRS document, with a complete and correct set of safety requirements at design level. Furthermore, where relevant, the requirements inform the validation exercises with respect to the inclusion of related additional validation objectives for which validation feedback is required.

The Safety assurance activities will be conducted in line with the SESAR 2020 Safety Policy [5], SESAR Safety Reference Material (SRM) [3] and accompanying Guidance [4] & [6].

## 2.4 Layout of the Document

The structure of this document follows the SESAR Safety Assessment Report template.

- Chapter 1 includes an executive Summary
- Chapter 2 provides general information about the SAR document
- Chapter 3 refers to the operational scenario and the safety criteria
- Chapter 4 contains the derivation of Safety Requirements at Service level for the ATS operational Solution.
- Chapter 5 documents the Safety Requirements at Design level (SRD) for the corresponding ATS operational Solution.
- Chapter 6 includes the conclusions of the safety assessment.
- Chapter 7 contains the acronyms and terminology of the document.
- Chapter 8 contains the references used in the document.

Additionally, following Appendices include:

- Appendix A presents the outcomes of the preliminary safety impact assessment and Safety Criteria determination.
- Appendix B presents the derivation of the Safety Requirements at ATS Service Level (SRS).
- Appendix C presents the risk analysis and the SRS derivation for abnormal conditions.
- Appendix D presents the risk analysis done at the level of the ATS service specification.
- Appendix E contains the design of the solution functional system for normal conditions.
- Appendix F contains the design of the solution functional system for abnormal conditions.
- Appendix G contains the design of the solution functional system addressing internal functional system failures.
- Appendix H contains the achievability of the Safety Criteria.
- Appendix I lists the assumptions, safety issues and limitations.

# 3 Setting the Scene of the safety assessment

The purpose of this section is to provide the main information collected within the SAF&HP Scoping and Change assessment and the Safety Plan development process in order to set the scene for the safety assessment documented in the SAR.

## 3.1 Operational concept overview and scope of the change

The concept includes Solution #02 and PJ.02-W2-21.1. Solution #02, which is based on the Routing and Planning of solution #22, laid the foundation. By using surveillance data and the integration of ATC clearances, taxi route and local procedures, Solution #02 focuses on detecting next three points:

- potential and actual clearance conflicts (Conflicting ATC Clearances, CATC),
- incursions,
- non-conformance to procedures or ATC clearances (Conformance Monitoring Alerts for Controllers, CMAC).

The present solution is based on this concept and tries to extend the application to the entire movement area. The solution also aims to reduce nuisance alerts (false positives), mostly caused by CATC alarms triggered too early for runway operations. The CATC alerts for Taxiway Operation take over and adapt the introduced Runway Operation concept, considering the individual safety-critical situations that can occur on taxiways and in the apron / stand / gate area.

According to that, the solution is focused on enhancing the Airport Safety Nets, to provide new alerts to controllers, increasing situational awareness and giving automated support to avoid hazardous situations. This is expected to raise benefits in Safety and Human Performance.

## 3.2 Solution Operational Environment and Key Properties

Solution Operational environment and Key Properties are elements of the environment (type of airspace and traffic density can be taken as examples) that can impact on the effects of the hazards.

As described in the OSED [13], Solution PJ.02-W2-21.1 will be applicable in the following Operating environment:

| OE | Applicable sub-OE | Special characteristics |
|---|---|---|
| Airports | very large / large / medium | Airports with A-SMGCS |

### 3.2.1 Airspace

The operational environment includes the airport surface (runways, taxiways and apron) along with aircraft and vehicles, as well as the CTR (control zone under tower responsibility which extends from the surface to a specified upper limit, established to protect air traffic operating to and from the airport).

### 3.2.2 Traffic

The solution considers aircraft and vehicle traffic on the runway protected areas, runways, the runway edges, the taxiways, and the parking positions. The alerting functions subject of this document apply to:

- Arriving aircraft
    - from transfer of responsibility from the Approach Control function at the start of final approach to the cessation of ATC responsibility;
    - through transfer of responsibility from the Runway Control function upon completion of the landing run and vacation of the Runway Protected Area to Apron/Ground control function;
- Departing aircraft
    - from initial contact with the Apron/ Ground Control function at the gate or stand to transfer of responsibility to the first airborne control function (TMA) or departure from the airport CTR;
    - through transfer of responsibility to the Runway Control function at or close to the runway holding point;
- Aircraft (which are not landing or departing) and vehicles, on the Apron and Taxiway areas (airport movement surface, outside the Runway Protected Area) or requiring access to these areas.

### 3.2.3 Traffic density

The alerts included in the solution are to be used in all traffic situations in medium, large and very large airports.

### 3.2.4 Weather and visibility conditions

The alert functions are intended to be an aid to situational awareness in all weather and visibility conditions.

### 3.2.5 Airports

Attending to the aerodrome layout:

- ATC service is provided at an airport with complex taxiway layout.
- ATC service is provided at an airport with medium taxiway layout.
- ATC service is provided at an airport with simple taxiway layout.
- ATC service is provided at an airport with a single runway.
- ATC service is provided at an airport with a several runways (crossing or parallel).
- ATC service is provided at adjacent airports with converging SIDs.

### 3.2.6 ATM capabilities

Solution PJ.02-W2-21.1 is expected to be implemented in A-SMGCS Airports. This A-SMGCS surveillance function:

- Provides a high-resolution map of the runways, adjacent runway protected areas, and taxiways;
- Indicates the position of all aircraft on the airport surface adjacent to the runways and their destination (runway, stand or other);
- Provides the identity and position of cooperating vehicles (those equipped with suitable transponders);
- Provides the position of non-cooperating vehicles.

SESAR 1 Solution #02 added the CMAC and CATC capabilities to the current A-SMGCS function, but further improvements are needed to broaden the scope of applicability to the whole airport movement area, and to enhance the performance of the safety nets (RMCA, CMAC and CATC).

The following ATM capabilities are required to support the operation of the updated CMAC and extended CATC alerts:

- A-SMGCS should be capable of supporting the following primary functions:
    - Surveillance;
    - Runway monitoring and conflict alerting (RMCA);
    - Routing
- The carriage of SSR transponders and/or ADS-B transmitters is mandatory for all mobiles which receive instructions from controllers.
- Flight Data Processing system supported by e.g., Electronic Flight Strips (EFS) is required to enable integration of ATC instructions with A-SMGCS surveillance data.

## 3.3 Stakeholders' expected benefits with potential Safety impact

Different stakeholders will have benefits with this solution, including safety, human Performance and Resilience benefits:

- Tower Controllers (TWR and GND): The Enhanced safety nets support the controllers increasing the situational awareness reducing the possibility of Human error and hence increasing Safety.
- Airport: PJ.02-W2-21.1 is expected to increase Resilience of the Airport. These benefits include:
    - a reduction of delays, diversions and cancelations caused by these incidents
    - a reduction of damaged and destroyed aircrafts due to the reduction of collisions.
- Flight Crew: Increase of safety on Airport. The tool alerts the controller in case of human error of the Flight Crew (incursions on taxiway/runway, misunderstanding, ..)
- Airlines: Avoid having to manage the consequences of collisions with other aircraft or vehicles (insurance claims, fixing the damage, cancelling flights, rescheduling, etc.)

## 3.4 Safety Criteria

Safety Criteria (SAC) define the acceptable level of safety (i.e., incident and accident risk level) to be achieved by the Solution under assessment, considering its impact on ATM/ANS functional system and its operation.

To obtain safety benefits, improvements in the performance of the barriers of Accident Incident Model (AIM) were defined. Thus, in SESAR 2020, the Accident Incident Model (AIM) for the Runway Collision and for Taxiway Collision [15] was used to derive the following Safety Acceptance Criteria. These SAC values have been obtained during an expert session, in which experts have analysed the solution, the applicable AIM models, and the information and documents listed in section 8 “References”.

- SAC #1: The number of Runway Conflicts arising from inefficient entry/exit management, take-off management or landing management (Severity Classification Scheme for Runway Collision model – RP2) shall be reduced by 7% when ATCO is supported by new predictive indications, runway notifications and alerts.

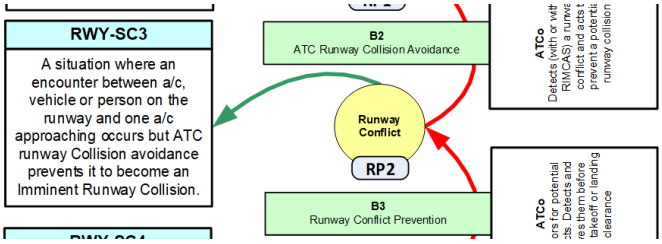


**Figure 2: Applicable SCS for SAC#1**

- SAC #2: The number of Taxiway/Apron[1] conflicts arising from induced taxiway /apron conflict and from induced pre-tactical taxiway/apron conflicts (Severity Classification Scheme for Taxiway accident model – TP2) shall be reduced by 5% when ATCO is supported by new predictive indications and alerts.

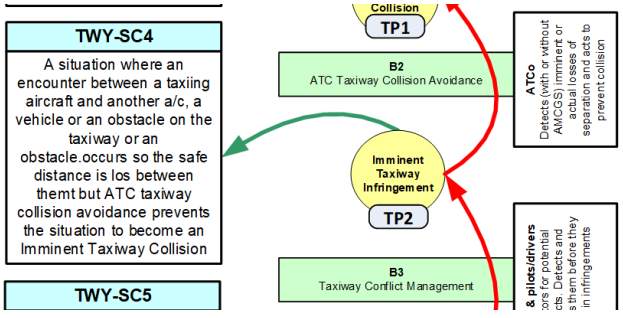


**Figure 3: Applicable SCS for SAC#2**

[1] Note that there is no specific Accident Incident Model (AIM) for Apron operations and, therefore, the one for Taxiway Collision was adapted as much as possible to apply it to Apron.

After considering the pre-existing and system-generated hazards that are impacting the concept studied by PJ02-W2-21.1, it is considered that the new alerting functions impact mostly the Runway Conflict Prevention barrier (B3) and Taxiway Conflict Management barrier (B3). Therefore, the objective is to improve the performance of these safety barriers to reduce the number of conflicts at the output of these barriers.

# 4 Safety specification at ATS service level

This section includes the derivation of the Safety Requirements at Service level (SRS) for the ATS operational Solution. This SRS specifies the desired safety behaviour of the change at its interface with the ATS operational context (including normal and abnormal conditions, and the failures of the functional system).

## 4.1 Overview of activities performed

This section addresses the following activities:

- Section 4.2. Derivation of Safety Requirements at ATS Service level (SRS) in view of mitigating the relevant risks inherent to aviation in normal conditions of operation.
- Section 4.3. Assessment of the adequacy of the ATS operational services provided by the Solution under abnormal conditions of the Operational Environment & derivation of necessary SRSs
- Section 4.4. Assessment of the adequacy of the ATS operational services provided by the Solution in the case of internal failures and mitigation of the Solution functional system-generated hazards through derivation of SRSs.
- Section 4.5. Verification of the operational safety specification process (mainly about obtaining Backing evidence from the properties of the processes by which Direct Evidence was gleaned).

## 4.2 Mitigation of Risks Inherent to Aviation – Normal conditions

This section presents the Safety Requirements at ATS Service level (SRS) derived for Normal conditions of operation, which are provided to ensure satisfaction of the Safety Criteria in Normal conditions of operation.

These Safety Requirements at the ATS Service level (SRS) show the desired safety behaviour of the solution considering normal conditions. SRS have been derived from the relevant Uses Cases described in the OSED and using EATMA Models at operational specification level to complete them.

### 4.2.1 Safety Requirements at ATS Service level (SRS) for Normal conditions of operation

In this section, a set of Safety Requirements of ATS Service level (SRS) for normal conditions of operation is presented. The complete analysis is included in Appendix B, while the following tables display a summary of the most relevant information.

First, the ATS operational services potentially impacted by the change in the relevant operational environment are compiled and related to the hazards inherent to aviation (identified in Appendix A.1) in order to address and mitigate them.

| ID | ATS Operational Service | Hazards inherent to aviation |
|---|---|---|
| **ATS-01** | Conflict detection and resolution | **Hr#1; Hr#2; Hr#3; Hr#4; Hr#5; Hr#6; Hr#7; Hr#8** |

**Table 1: ATS Operational services potentially impacted and Hazards inherent to aviation**

The consolidated list of the SRS for normal conditions of operation that have been derived in Appendix B are presented below.

| SRS ID | SRS for Normal conditions of operation | Related SAC |
|---|---|---|
| **SRS 001** | ATCO shall detect potential CATC through Predictive indicator | **SAC#1; SAC#2** |
| **SRS 002** | ATCO shall assess Predictive CATC Indication | **SAC#1; SAC#2** |
| **SRS 003** | ATCO shall provide clearance under a specific condition when operationally required | **SAC#1; SAC#2** |
| **SRS 004** | ATCO shall be aware in advance of any potential CATC conflict. | **SAC#1; SAC#2** |
| **SRS 005** | ATCO shall assess situation and manage CATC and CMAC alerts | **SAC#1; SAC#2** |
| **SRS 006** | ATCO shall cancel clearance and record change in the HMI | **SAC#1; SAC#2** |
| **SRS 007** | ATCO shall record ATC Clearance in the system | **SAC#1; SAC#2** |
| **SRS 008** | ATCO shall detect conflict CMAC vs ATC clearance | **SAC#1; SAC#2** |
| **SRS 009** | ATCO shall manage CMAC vs ATC clearance alert | **SAC#1; SAC#2** |
| **SRS 010** | ATCO shall detect stand occupied through Stand Occupied alert | **SAC#1; SAC#2** |
| **SRS 011** | ATCO shall manage stand occupied alert | **SAC#1; SAC#2** |
| **SRS 013** | ATCO shall be constantly and immediately aware about the operational status of the Runway, whether it is busy or it is affected by any conflict. | **SAC#1; SAC#2** |
| **SRS 014** | ATCO shall be aware in advance of any potential RMCA vs ATC clearance conflict. | **SAC#1; SAC#2** |
| **SRS 015** | ATCO shall manage RMCA vs ATC clearance conflict. | **SAC#1; SAC#2** |

**Table 2: List of SRS (functionality and performance) for normal conditions of operation**

### 4.2.2 Additional SRS related to adjacent airspace or neighbouring ATM Systems

No additional SRS related to adjacent airspace or neighbouring ATM Systems have been detected in relation with this Solution.

## 4.3 Mitigation of Risks Inherent to Aviation – Abnormal conditions

According to [3], “abnormal conditions” can be defined as *external changes in the operational environment that the ATM/ANS functional system may exceptionally encounter*. When these abnormal conditions appear, *the system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be tolerable*.

Looking at this solution, and as mentioned in [14], the use cases do not consider abnormal conditions that could affect the functionality of the Safety Support Tools. Nevertheless, a safety analysis is done

in this section in order to confirm this idea or in order to define the necessary abnormal conditions for the solution.

When talking about the mentioned "operational environment" for this solution, ATC working environment must be understood as the environment to be analysed, and the focus must be pointed only at instructions or clearances given by ATC based on the safety nets included in this solution (for example, CATC or CMAC alerts), and not into every instruction/clearance given.

Taking this into account, abnormal condition examples from documents [3] and [4] are not valid for this solution; as an example:

- Drop of visibility, strong wind, or solar storm: weather issues have not impact on the usability of the solution because the solution performance does not depend on the weather conditions.
- Unexpected runway closure, sudden activation of TSAs or aircraft emergency: this operational issue are not related to the solution and must be solved by ATC according to the regular procedures with/without the solution implemented.

Looking at the implemented alerts, no applicable special events are found, since the only inputs for these alerts are ATC instructions/clearances, and the alerts will be exclusively based in these inputs. As an example, if the ATC makes a mistake when controlling because an external event, this is not going to impact on the solution, because is not going to make the solution entering in a degrade state. The only degrade state for the alerts could be the malfunction of the alert because of a bad behaviour of the system; nevertheless, this can't be seen as an abnormal condition and must be analysed as a failure mode.

Therefore, as the solution is based on functionalities, no external events causing these functionalities enter on a degrade mode can be found. Consequently, no abnormal conditions are defined for this solution.

## 4.4 Mitigation of System-generated Risks (failure conditions)

This section presents the Safety Requirements at ATS Service level (SRS) associated with the operational hazards, which are caused by internal failures of the functional system.

This SRS complete the safety specification at operational service level, providing mitigation against the possible adverse effects that failures to the functional system might have.

### 4.4.1 Operational Hazards Identification and Analysis

This section presents the results from hazard identification and analysis included in Appendix D. For each hazard, it is shown:

- assessed operational effect,
- mitigations considered for assessing the operational effect (protecting against effect propagation) with a reference to existing safety barriers (as per the relevant AIM model), to existing SRS (functionality & performance) or, if applicable, to new derived SRS (functionality & performance).

- the assessed severity of the most probable effect from hazard occurrence as per the relevant AIM-based Severity Classification Scheme(s) (SCS) from Guidance G.3 of the "Guidance to Apply SESAR Safety Reference Material" [4].

Taking into account the preliminary system-generated hazards included in Appendix A.2, and after an analysis about how these hazards could end when the system is operating, next table represents the Operational Hazards identified for the solution.

| ID | Operational Hazard Description | Operational Effects | Mitigation of effects propagation | Severity *(most probable effect)* |
|---|---|---|---|---|
| OH 01 | ATC do not correctly detect conflicting clearances (because of lack of detection or incorrect/incomplete information of CATC/ CMAC alert) | Conflict between aircrafts during the runway/taxiway/apron operation. | **SRS 001/SRS 002/SRS 003/SRS 004/SRS 005/SRS 006/SRS 007/SRS 008/SRS 009/SRS 010/SRS 011/SRS 012/SRS 013/SRS 014/SRS 015** | RWY-SC3<br><br>A situation where an encounter between a/c, vehicle or person on the runway and one a/c approaching occurs but ATC runway collision avoidance prevents it to become an Imminent Runway Collision<br><br>TWY-SC4<br><br>A situation where an encounter between taxiing aircraft and another a/c, a vehicle or an obstacle on the taxiway occurs so the safe distance is los between them, but ATC taxiway collision avoidance prevents the situation to become an Imminent Runway Collision |
| OH 02 | ATC do not correctly detect conflicting clearances (because of lack of detection or incorrect/incomplete information of RMCA vs CATC Alert or CMAC vs CATC alert) | Conflict between aircrafts during the runway/taxiway/apron operation. | **SRS 001/SRS 002/SRS 003/SRS 004/SRS 005/SRS 006/SRS 007/SRS 008/SRS 009/SRS 010/SRS 011/SRS 012/SRS 013/SRS 014/SRS 015** | RWY-SC3<br><br>A situation where an encounter between a/c, vehicle or person on the runway and one a/c approaching occurs but ATC runway collision avoidance prevents it to become an Imminent Runway Collision<br><br>TWY-SC4<br><br>A situation where an encounter between taxiing aircraft and another a/c, a vehicle or an obstacle on the taxiway occurs so the safe distance is los between them but ATC |

| | | | | |
|---|---|---|---|---|
| | | | | taxiway collision avoidance prevents the situation to become an Imminent Runway Collision |
| OH 03 | ATC do not detect correctly conflicting parking instruction (because of lack of detection or incorrect information of Stand Occupied CMAC alert) | Conflict between aircrafts during the parking phase. | **SRS 001/SRS 002/SRS 003/SRS 004/SRS 005/SRS 006/SRS 007/SRS 008/SRS 009/SRS 010/SRS 011/SRS 012/SRS 013/SRS 014/SRS 015** | TWY-SC4<br><br>A situation where an encounter between taxiing aircraft and another a/c, a vehicle or an obstacle on the taxiway occurs so the safe distance is lost between them but ATC taxiway collision avoidance prevents the situation to become an Imminent Runway Collision |

**Table 3: Operational Hazards and Analysis**

### 4.4.2 Safety Requirements at ATS Service level (SRS) associated to failure conditions

There are additional SRS (functionality & performance) associated to failure conditions that have been derived during the operational hazard assessment:

| SRS ID | Additional Safety Requirements at ATS Service level *(functionality & performance)* | Mitigated Operational Hazard |
|---|---|---|
| **SRS 012** | The System/Equipment supporting the solution has to meet the defined failure rate. | OH 01 & OH 02 & OH 03 |

**Table 4: Additional SRS to mitigate Operational hazards effects**

On the other hand, the SRS (integrity and reliability) associated to failure conditions are defined. In order to do so, the method included in the Guidance G of the "Guidance to apply SESAR Safety Reference Material" is followed. A quantitative definition of the SRSs integrity is defined considering the equation:

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

Where:

- **MTFoO** (Maximum Tolerable Frequency of Occurrence) is associated to the severity class of the Operational Hazard, according to the maximum tolerable frequency of occurrence for each severity class.
- **N** is the number of hazards for the severity class included in the SRM.
- **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.

| SRS ID | Safety Requirements at ATS Service level *(integrity/reliability)* | Related Operational Hazard | Severity & IM |
|---|---|---|---|
| **SRS 016a** | The frequency of a RWY event in which the CATC/ CMAC alert is not shown to ATC by the system shall be no more than 5e-7 per Flight Hour | OH 01 | RWY-SC3<br>IM=1 |
| **SRS 016b** | The frequency of a TWY event in which the CATC/ CMAC alert is not shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | OH 01 | TWY-SC4<br>IM=1 |
| **SRS 017a** | The frequency of a RWY event in which the CATC/ CMAC alert is incorrectly shown to ATC by the system shall be no more than 5e-7 per Flight Hour | OH 01 | RWY-SC3<br>IM=1 |

| SRS ID | Safety Requirements at ATS Service level *(integrity/reliability)* | Related Operational Hazard | Severity & IM |
|---|---|---|---|
| **SRS 017b** | The frequency of a TWY event in which the CATC/ CMAC alert is incorrectly shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | OH 01 | TWY-SC4 IM=1 |
| **SRS 018a** | The frequency of a RWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is not shown to ATC by the system shall be no more than 5e-7 per Flight Hour | OH 02 | RWY-SC3 IM=1 |
| **SRS 018b** | The frequency of a TWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is not shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | OH 02 | TWY-SC4 IM=1 |
| **SRS 019a** | The frequency of a RWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is incorrectly shown to ATC by the system shall be no more than 5e-7 per Flight Hour | OH 02 | RWY-SC3 IM=1 |
| **SRS 019b** | The frequency of a TWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is incorrectly shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | OH 02 | TWY-SC4 IM=1 |
| **SRS 020** | The frequency of a TWY event in which the Stand Occupied CMAC alert is not shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | OH 03 | TWY-SC4 IM=1 |
| **SRS 021** | The frequency of a TWY event in which the Stand Occupied CMAC alert is incorrectly shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | OH 03 | TWY-SC4 IM=1 |

**Table 5: Safety Requirements at Service level – integrity/reliability**

# 5 Safe Design of the Solution functional system

The purpose of this section is to document the Safety Requirements at Design level (SRD) for the ATS operational Solution. The set of Safety Requirements at Service level (SRS) identified in section 4 enables the derivation of a correct and complete set of Safety Requirements at Design level (SRD).

The Safety Requirements at Design level (SRD) are design characteristics/items of the Solution functional system to ensure that the system operates as specified and can achieve the SACs. SRD are placed on the elements that are changed or affected by the change.

The derived SRDs are consistent with the set of requirements produced, and completeness and correctness of the full set of SRDs with regards to the satisfaction of the Safety Criteria will be shown in the next sections of this document.

On the other hand, the assumptions, safety issues and limitations identified during the service specification process is recorded in Appendix I.

## 5.1 Overview of activities performed

This section addresses the following activities:

- section 5.2. Introduction of the design model (initial or refined) of the Solution functional system.
- section 5.3. Derivation of Safety Requirements (functionality & performance) at Design level (SRD) in normal conditions of operation from the SRS (functionality & performance) of section 4.2 and supported by the analysis of the initial or refined design model above.
- section 5.5. Assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution operational hazards (identified at section 4.4) through derivation from SRS (integrity/ reliability) of Safety Requirements (functionality & performance) and Safety Requirements (integrity/reliability) at Design level (SRD).
- section 5.6. Realism of the refined safe design (i.e., achievability and “testability” of the SRD).
- section 5.7. Safety process assurance at the initial or refined design level.

## 5.2 Design model of the Solution functional system

The Design Model of the Solution functional system represents the architecture combining the elements composing the Solution functional system in terms of procedures, human resources and equipment. Therefore, Safety requirements at design level (SRD) are to be placed on those elements.

This high-level architectural representation of the Solution system design is composed by eight NSV-5 diagrams which can be found in EATMA:

- Predictive Indication
- Conditional Clearance
- Extended CATC

- Updated CATC
- Stand Occupied
- Runway Busy Notification
- Runway In Conflict Notification

### 5.2.1 Description of the Design Model

The safety assessment refers to EATMA models, so no description is provided here.

### 5.2.2 Task Analysis

No specific information related to the Task analysis is relevant for the Safety Assessment.

## 5.3 Deriving Safety Requirements at Design level for Normal conditions of operation

This section presents the Safety Requirements at Design level (SRD) derived for Normal conditions of operation. The derivation of the SRD for Normal conditions of operation is mainly driven by the SRS (functionality & performance) for Normal conditions of operation from section 4.2.

### 5.3.1 Safety Requirements at Design level (SRD) – Normal conditions of operation

In this section, a set of Safety Requirements at Design level (SRD) for normal conditions of operation is presented. For each SRD, information about the element of the design model on which the SRD is placed, as well as the associated SRS, is provided

The complete analysis is included in Appendix E, while the following table displays a summary of the most relevant information.

| Safety Requirement ID [Design Model Element] | Safety Requirement (functionality & performance) | Derived from SRS (ID) |
|---|---|---|
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 001** – ATCO shall detect potential CATC through Predictive indicator |
| REQ-02-W2-21.1-TS-SAFE.0002 | The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0021 | The controller will be presented with an indicator on the HMI that informs the Controller that the input of a specific clearance for a mobile will trigger a CATC alert. | |

| Safety Requirement ID [Design Model Element] | Safety Requirement (functionality & performance) | Derived from SRS (ID) |
|---|---|---|
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 002 –** ATCO shall assess Predictive CATC Indication |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0022 | The controller when issuing a clearance to a mobile may link the clearance to a condition and enter the clearance and condition in the HMI | **SRS 003 –** ATCO shall provide clearance under a specific condition when operationally required |
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 004 –** ATCO shall be aware in advance of any potential CATC conflict. |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0002 | The Tower Ground Controller shall receive an alert when issuing a PUSH BACK clearance that conflicts with a previously input PUSH BACK clearance according to local rules and procedures. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0003 | The Tower Ground Controller shall receive an alert when entering a TAXI clearance via the HMI that conflicts with a previously input PUSH BACK clearance according to local rules and procedures. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0004 | The Tower Ground Controller shall receive an alert when entering a PUSH BACK clearance via the HMI that conflicts with a previously input TAXI clearance according to local rules and procedures. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0005 | The Tower Ground Controller shall receive an alert when entering a TAXI clearance for an aircraft A to taxi onto a taxiway where the aircraft A would obstruct the path of another aircraft B taxiing. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0006 | The Tower Ground Controller shall receive an alert when a TAXI clearance is entered via the HMI and another TAXI clearance was input previously where the two cleared routes are in opposite | |

| Safety Requirement ID [Design Model Element] | Safety Requirement (functionality & performance) | Derived from SRS (ID) |
|---|---|---|
| | directions on the same taxiway and are predicted to block each other (Deadlock Situation). | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0009 | The Tower Runway Controller shall receive an alert when a LAND clearance is input for an aircraft while a LAND clearance was previously given to another aircraft on the same runway and the separation minima on the runway (according to ICAO DOC4444) are not expected to be achieved the moment the second landing aircraft crosses the runway threshold. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0010 | The Tower Runway Controller shall receive an alert when a LAND clearance is input for an aircraft while previously a TAKE OFF clearance was input for another aircraft on the same runway and the separation minima on the runway (according to ICAO DOC4444) are not expected to be achieved the moment the landing aircraft crosses the runway threshold. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0011 | The Tower Runway Controller shall receive an alert when a LAND clearance is input for an aircraft while previously a CROSS clearance was input on another aircraft on the same runway and the separation minima on the RWY (according to ICAO DOC4444) are not expected to be achieved the moment the landing aircraft crosses the RWY threshold. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0013 | The Tower Runway Controller shall receive an alert if a TAKE OFF clearance is input for an aircraft, while a TAKE OFF clearance was previously input for another aircraft on a different runway and the ground or the air trajectories (SIDs) are converging according to local procedures/rules. | |

| Safety Requirement ID [Design Model Element] | Safety Requirement (functionality & performance) | Derived from SRS (ID) |
|---|---|---|
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 005 –** ATCO shall assess situation and manage CATC and CMAC alerts |
| A001 | The system allows the ATCO to cancel a clearance and record the change in the HMI. | **SRS 006 –** ATCO shall cancel clearance and record change in the HMI |
| A002 | The system allows the ATCO to record ATC clearances. | **SRS 007 –** ATCO shall record ATC Clearance in the system |
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 008 –** ATCO shall detect conflict CMAC vs ATC clearance |
| REQ-02-W2-21.1-TS-SAFE.0002 | The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0015 | The Tower Runway Controller shall receive an alert when a LINE UP/TAKE OFF/CROSS/ENTER or LAND clearance is entered via the HMI whilst a CMAC alert (RWY Incursion, No Take Off, No Land or Wrong Runway) is active for the same runway. | |
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 009 –** ATCO shall manage CMAC vs ATC clearance alert |
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 010 –** ATCO shall detect stand occupied through Stand Occupied alert |
| REQ-02-W2-21.1-SPRINTEROP-CM01.0001 | The Controller shall receive an INFORMATION Alert on the HMI when the allocated stand for an arrival flight is occupied. | |

| Safety Requirement ID [Design Model Element] | Safety Requirement (functionality & performance) | Derived from SRS (ID) |
|---|---|---|
| REQ-02-W2-21.1-SPRINTEROP-SAFE.0001 | ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | **SRS 011 –** ATCO shall manage stand occupied alert |
| REQ-02-W2-21.1-SPRINTEROP-RWAY.0005 | The Tower Runway Controller shall receive a visual indication if a runway is affected by any alert. | **SRS 013 –** ATCO shall be constantly and immediately aware about the operational status of the Runway, whether it is busy or it is affected by any conflict. |
| REQ-02-W2-21.1-SPRINTEROP-RWAY.0010 | The Tower Runway Controller shall receive a visual indication if a runway is currently occupied by any mobile or if a mobile has been cleared to use it. | |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0014 | The Tower Runway Controller shall receive an alert when a LINE UP/TAKE OFF/CROSS/ENTER or LAND clearance is entered via the HMI whilst an RMCA alert is active for the same runway. | **SRS 014 –** ATCO shall be aware in advance of any potential RMCA vs ATC clearance conflict. |
| REQ-02-W2-21.1-SPRINTEROP-CA01.0014 | The Tower Runway Controller shall receive an alert when a LINE UP/TAKE OFF/CROSS/ENTER or LAND clearance is entered via the HMI whilst an RMCA alert is active for the same runway. | **SRS 015 –** ATCO shall be able to manage RMCA vs ATC clearance conflict. |

**Table 6. Safety Requirements at design level (functionality and performance) satisfying SRS for Normal conditions of operation**

### 5.3.2 Static analysis of the functional system behaviour – Normal conditions of operation

No static analysis of the functional system behaviour – Normal conditions of operation has been developed in relation with this Solution.

### 5.3.3 Dynamic Analysis of the functional system behaviour – Normal conditions of operation

A dynamic analysis of the functional system behaviour under normal conditions of operation in relation with the solution has been carry out in the VALR [16] and described in E.3.

According to that, no additional safety requirements are necessary to establish.

### 5.3.4 Effects on Enhanced Airport Safety Nets – Normal conditions of operation

No effects on Safety Nets are detected for this solution.

## 5.4 Deriving Safety Requirements at Design level for Abnormal conditions of operation

As said before in section 4.3, no abnormal conditions related to this solution has been identified, so no SRDs are derived.

## 5.5 Safety Requirements at Design level addressing Internal Functional System Failures

This section presents the Safety Requirements at Design level (SRD) associated to internal failures of the Solution functional system. Safety requirements at design level – SRD are derived from the SRS (functionality & performance) and SRS (integrity/reliability) which have been identified in section 4.4.

The following Safety requirements at design level (SRD) are to be included:

- SRD (functionality & performance) derived to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard
- SRD (integrity/reliability) to limit the frequency with which failure of modified/new equipment elements in the Solution functional system could be allowed to occur
- If applicable, SRD (functionality & performance) derived to provide mitigation against operational hazard effects (protective mitigation, from the SRS (functionality & performance) derived during the operational hazard assessment at section 4.4.1).

### 5.5.1 Design analysis addressing internal functional system failures

The design analysis addressing internal functional system failures has been conducted through:

- A top-down causal analysis through Fault Trees that show for each operational hazard, its causes and the associated mitigations.
- A bottom-up analysis through a Failure Modes and Effects Analysis, for selected parts of the Solution functional system, to determine potential common cause failures but also in order to allow a more in-depth causal analysis of certain parts of the functional system design

The aim of this work is to:

- Ensure identification of a complete list of Solution functional system failures that could cause each operational hazard.
- Ensure identification of the required Mitigation means preventing causes to occur or preventing their effect to propagate towards each operational hazard
- Contribute to demonstrate the feasibility and effectiveness of the contingency procedures associated to the degraded modes of operation in which the functional system might enter as a result of certain failure modes

- Determine potential common cause failures and ensure their mitigation through dedicated SRD or design choice.

An overview of the main outcomes of these analyses is included in Appendix G.

### 5.5.2 Safety Requirements at Design level associated to internal functional system failures

The table below contains the consolidated list of Safety Requirements at Design level associated to internal system failures.

| Safety Requirement ID | Safety Requirement at Design level (SRD) (functionality & performance) | Derived from SRS (ID) or Common cause failure |
|---|---|---|
| **REQ-02-W2.21.1-TS-SAFE.0002** | The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | SRS 012 |

## 5.6 Realism of the safe design

### 5.6.1 Achievability of Safety Requirements (SRD) and Assumptions

The Safety Requirements identified in section 5.3 to 5.5 have been determined and validated based on the results of the validation activities. The involvement of operational and technical experts during this process ensures the achievability of the safety requirements (SRD) and assumptions.

### 5.6.2 Verification of Safety Requirements (SRD)

The safety requirements (SRD) were validated whilst conducting the validation exercise and via involvement of experts during the process.

# 6 Safety Criteria achievability

The purpose of this section is to provide conclusions of the safety assessment for the ATS operational Solution.

The Safety Criteria set in section 3.4 are expected to be achieved through the Safety Requirements at ATS Service level (SRS) identified in section 4, which have been derived into safety requirements at design level (SRD)) in section 5. The Safety Criteria should be achieved by implementing these safety requirements.

The validation exercise allows to verify the compliance with the defined safety criteria for all safety validation objectives. This confirms the ATS Operational enables the solution and maintains the level of safety.

The extent of this safety assessment is recorded in Appendix H.

# 7 Acronyms and Terminology

| Acronym | Definition |
|---|---|
| AART | Airport Airside And Runway Throughput |
| AIM | Accident Incident Model |
| AMC | Acceptable Means of Compliance |
| ANS | Air Navigation Services |
| A-SMGCS | Advanced Surface Movement Guidance and Control System |
| ATC | Air Traffic Control |
| ATCO | Air Traffic Control Officer |
| ATM | Air Traffic Management |
| ATS | Air Traffic Services |
| CATC | Conflicting ATC Clearances |
| CMAC | Conformance Monitoring Alerts for Controllers |
| CONOPS | Concept of Operations |
| EATMA | European Air Traffic Management Architecture |
| FHA | Functional Hazard Assessment |
| HP | Human Performance |
| IRS | Interface Requirement Specification |
| iSRD | initial Safety Requirement at Design level |
| OHA | Operational Hazard Assessment |
| OI | Operational Improvement |
| OSED | Operational Service and Environment Definition |
| RMCA | Runway Monitoring and Conflict Alerting |
| rSRD | refined Safety Requirement at Design level |
| RWY/TWY | Runway/Taxiway |
| SAC/SC | Safety Criteria |

| | |
|---|---|
| SAM | Safety Assessment Methodology |
| SAR | Safety Assessment Report |
| SPR | Safety and Performance Requirements |
| SRM | SESAR Reference Material |
| SRD | Safety Requirements at Design level |
| SRS | Safety Requirements at ATS Service Level |
| TS | Technical Specifications |
| VALP | Validation Plan |

**Table 7: Acronyms**

The following table presents a list of the most important terminology used along the document.

| Term | Definition |
|---|---|
| A-SMGCS | A system providing as a minimum Surveillance and can include Airport Safety Support, Routing and Guidance to aircraft and vehicles in order to maintain the airport throughput under all local weather conditions whilst maintaining the required level of safety. |
| Alert | An indication of an existing or pending situation during aerodrome operations, or an indication of abnormal A-SMGCS operation, that requires attention/action. |
| CATC | CATC provides an alert when the Controller inputs an electronic clearance via the Human Machine Interface (HMI), which according to a set of locally agreed rules is not permitted from an operational and safety point of view when compared to any other previously input electronic clearance. |
| Clearance | Authorization for an aircraft to proceed under conditions specified by an air traffic control unit.<br><br>Note 1: For convenience, the term 'air traffic control clearance' is frequently abbreviated to 'clearance' when used in appropriate contexts. |
| Functional System | A combination of procedures, human resources, and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions (Regulation (EU) No 2017/373 [1]) |
| Conditional Clearance | A conditional clearance is a clearance issued by an air traffic controller which does not become effective until a specified condition has been satisfied. |
| CMAC | CMAC provides Controllers with appropriate alerts when the A-SMGCS detects the non-conformance to procedures or clearances for traffic on runways, taxiways and in the apron/stand/gate area. |
| Hazard | Any condition, event, or circumstance which could induce a harmful effect (Regulation (EU) No 2017/373 [1]) |

| Term | Definition |
|---|---|
| Predictive Indication | The Predictive Indication is displayed on a track label or electronic flight strip (or any aircraft representation on the controller's main screen) that is associated with a clearance that has not yet been given to a mobile, showing that this clearance, if given, would be conflictual with another active clearance given to another mobile. |
| Risk | The combination of the overall probability or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect (Regulation (EU) No 2017/373 [1]) |
| Runway notification | The Runway Notification displays the current status of the runway to notify the controller when clearing a mobile to use that runway would result in a potential conflict. |
| Safety Criteria | Criteria that allow the ATS provider to determine the safety acceptability of a change to a functional system, based on the analysis of the risks posed by the introduction of the change (Regulation (EU) No 2017/373 [1]) |
| Safety Requirement at Design Level | Design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SACs (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SACs are met). |
| Safety Requirement at Service Level | Requirements that specify the desired safety behavior of the change at its interface with the ATS operational context considering normal and abnormal conditions of the context (success approach) and the failures of the functional system (failure approach). |
| Solution Functional System | Designates the Solution Functional ATM/ANS System as defined in Regulation (EU) No 2017/373 [1] (i.e., encompassing procedures, human resources, and equipment). |

**Table 8: Glossary of terms**

# 8 References

## Safety

[1] Regulation (EU) No 2017/373 laying down common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011 and (EU) No 1035/2011 and amending Regulation (EU) No 677/2011 (and associated AMC and GM)

[2] SAM EUROCONTROL Safety Assessment Methodology, Edition 2.0

[3] SESAR Safety Reference Material – Edition 04.01, December 2018

[4] Guidance to Apply SESAR Safety Reference Material – Edition 03.01, December 2018

[5] SESAR 2020 Safety Policy

[6] STELLAR Slideboard, Safety part (complementary guidance)

## Reference documents

[7] PJ19 CI - D4.0.070 - SESAR Human Performance Assessment Process V1 to V3- including VLDs - edition 00.03.02, 27/08/2020 (Edition 3.2)

[8] PJ19-W2 CI - D2.0.002 - High Level Operational Requirements for Wave 2 Solutions, edition 00.01.02, date 04/12/2020

[9] PJ19 CI - D2.5 - SESAR Concept of Operations (CONOPS 2019), edition 01.00.00, date May 2019SESAR Solution PJ.02-W2-21.1 D6.1.001 SPR-INTEROP/OSED Intermediate version, edition 00.01.02, 13 April 2021

[10]PJ03B-01 - D2.1.120 - V2 OSED-SPR-INTEROP Part I, edition 01.00.00, 31 July 2019

[11]PJ03B-01 - D2.1.120 - V2 OSED-SPR-INTEROP Part II – SAR, edition 01.00.00, 31 July 2019

[13]SESAR Solution PJ.02-W2-21.1 – D6.1.002 - SPR/INTEROP OSED for V3 – Part I, Edition 00.02.02, 24 May 2023.

[14]SESAR Solution PJ.02-W2-21.1 - D6.1.004 - VALP Part I, edition 00.01.00, 26/08/2021

[15] Runway Collision (RC) & associated AIM model (AIM models 2020

[16]SESAR Solution PJ.02-W2-21.1 – D6.1.006 - Validation Report (VALR) for V3, edition 00.01.02, 24 May 2023.

# Appendix A Preliminary safety impact assessment

## A.1 Relevant Hazards Inherent to Aviation

Before performing the safety assessment for the introduction of a new concept, it is mandatory to understand the impact it would have in the overall ATM risk picture. The SRM Guidance D and E provides a set of Accident Incident Models (AIM – one per each type of accident), which represent an integrated risk picture with respect to ATM contribution to aviation accidents.

Next table presents the relevant aviation hazards in the operational environment before the implementation of the solution. It presents the relevant aviation hazards that have been identified, and which continue to be applicable within the current scope.

| Hazards inherent to aviation [Hi] | ATM-related accident type & AIM model |
|---|---|
| **Hi#1** "Situation in which the intended trajectory of a landing aircraft is conflicting with another aircraft or vehicle on the runway area;" | Runway Collision (RC) & associated AIM model (AIM models 2020) [15] |
| **Hi#2.** "Situation in which the intended 3-D route of a taxiing aircraft would lead to collision with a ground vehicle or another aircraft on RWY or close to ground on landing / take-off" | Runway Collision (RC) & associated AIM model (AIM models 2020) [15] |
| **Hi#3.** "Situation in which the intended 3-D route of a taxiing aircraft would lead to collision with an obstacle, a ground vehicle or another aircraft on apron or TWY" | Taxiway accident & associated AIM model (AIM models 2020) [15] |
| **Hi#4.** Aircraft using a closed runway | Runway Collision (RC) & associated AIM model (AIM models 2020) [15] |

**Table 9. Hazards inherent to aviation relevant for the Solution**

## A.2 Functional system-generated hazards (preliminary)

Operational hazards could be generated by the reference functional system (before the introduction of the Change) and potentially be impacted by the Change. These hazards have been identified in the frame of the HP&SAF scoping & change assessment session held in July 2021.

This preliminary identification was made to facilitate the identification of the safety impact of the Change, in terms of which operational hazards (generated by the functional system in the scope) are modified by the Change.

| Functional system-generated hazards (preliminary) | Impacted (new/modified) & justification |
|---|---|
| **Hr#1:** Failure by the ATC system (CATC alerting functions) to detect the **conflicting ATC clearances** that potentially lead to a conflict between two aircraft during the **runway operation** (take-off and landing). | If the alert is not triggered due to an ATC system failure the Runway Tower Controller and the Flight Crew will be relied upon to identify the potentially hazardous situation and to resolve the problem as quickly and safely as possible. This is often the case today at airports where some of these alerts do not exist. |
| **Hr#2:** Failure by the ATC system (CATC alerting functions) to detect the **conflicting ATC clearances** that potentially lead to a conflict between two aircraft in the **taxiway/apron.** | If the alert is not triggered due to an ATC system failure the Tower Ground Controller, Apron manager and the Flight Crew will be relied upon to identify the potentially hazardous situation and to resolve the problem as quickly and safely as possible. This is often the case today at airports where these alerts do not exist. |
| **Hr#3:** The ATC system (CATC alerting functions) detects **conflicting ATC clearances** based on incorrect information and triggers a false CATC alert. | The controller will assess the situation and detect the false CATC alert. These false alerts could reduce the situational awareness and increase the workload. |
| **Hr#4:** The ATC system (CATC alerting functions) detects **conflicting ATC clearances** based on incomplete information and triggers a false CATC alert. | The controller will assess the situation and detect the false CATC alert. These false alerts could reduce the situational awareness and increase the workload. |
| **Hr#5:** Failure by the ATC system (**CMAC** alerting functions) to detect the occupation of the **parking stand** assigned to an aircraft (the stand is occupied but the system does not trigger the alert) | In the event that no alert is raised due to an ATC system failure, the Tower Ground Controller/Apron Manager and flight crew will be confident in identifying and resolving the issue as quickly and safely as possible.<br>This situation often occurs today where these warnings do not exist. |
| **Hr#6:** Failure by the ATC system (CMAC alerting functions) to detect the occupation of the **parking stand** assigned to an aircraft (the stand is empty, but the system triggers the CMAC alert) | In the case of a false alert the Tower Ground Controller/Apron Manager will assess the situation as soon as the alert is presented, and if the alert is deemed to be false, cancel the alert and inform the supervisor of the error. |
| **Hr#7:** Failure of the ATC system to compute an aircraft's speed and position to predict the possibility of two cleared aircraft (or an aircraft and a vehicle) conflicting. | This failure can affect to:<br>• Extended CATC alerts (for ground and runway operations)<br>• RMCA alerts vs ATC Clearances<br>• CMAC Alerts vs ATC Clearances<br>• the Predictive Indication |

| Functional system-generated hazards (preliminary) | Impacted (new/modified) & justification |
|---|---|
| | • The Runway Notifications.<br><br>Not detecting a potential conflict increases the risk of a hazardous incident.<br><br>Addressing false positives caused by the uncertain forecast can decrease situational awareness and increase workload. |
| **Hr#8:** The failure of the ATC system to calculate the speed and position of an aircraft to predict the possibility of a conflict can result in a false positive detection of potential conflicts. | A false positive detection triggers nuisance alerts that bind the controller's attention so that other critical traffic developments may not be sufficiently noticed. |
| **Hr9:** Failure to display the correct runway status | In case the "Runway Busy Notification" / "Runway In Conflict Notification" is not in accordance with the current alerting status, it can reduce situational awareness and increase workload. |

**Table 10. Functional system-generated hazards applicable to the Solution (preliminary list)**

# Appendix B Derivation of SRS (Functionality & Performance) for Normal conditions of operation

This appendix presents the derivation of the SRS (functionality & performance) to mitigate the hazards under normal conditions of operation, i.e., those conditions that are expected to occur on a day-to-day basis.

The description of the new operating method is available via:

- The description of each Use Case for normal conditions, included in the OSED document (see [13], section 3.3.2).
- The EATMA representation as per the Operational layer (i.e. the NOV-5 diagrams related to the above-mentioned UC, where each one of them is described through a process model made up of activities interacting via information flows; see [13], section 3.3.2.2).

The consolidated list of SRSs is provided in Section 4.2.1.

## B.1 EATMA Process models or alternative description

In this section, a copy of the EATMA process models regarding each one of the mentioned Use Cases is included.

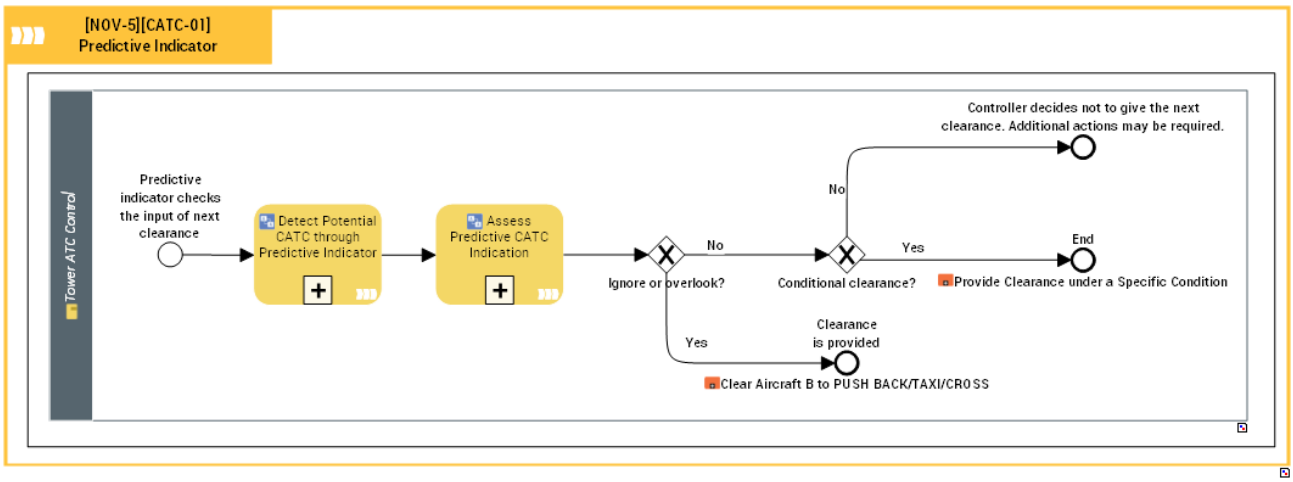


**Figure 4: EATMA NOV-5 Model [CATC-01] Predictive Indicator**

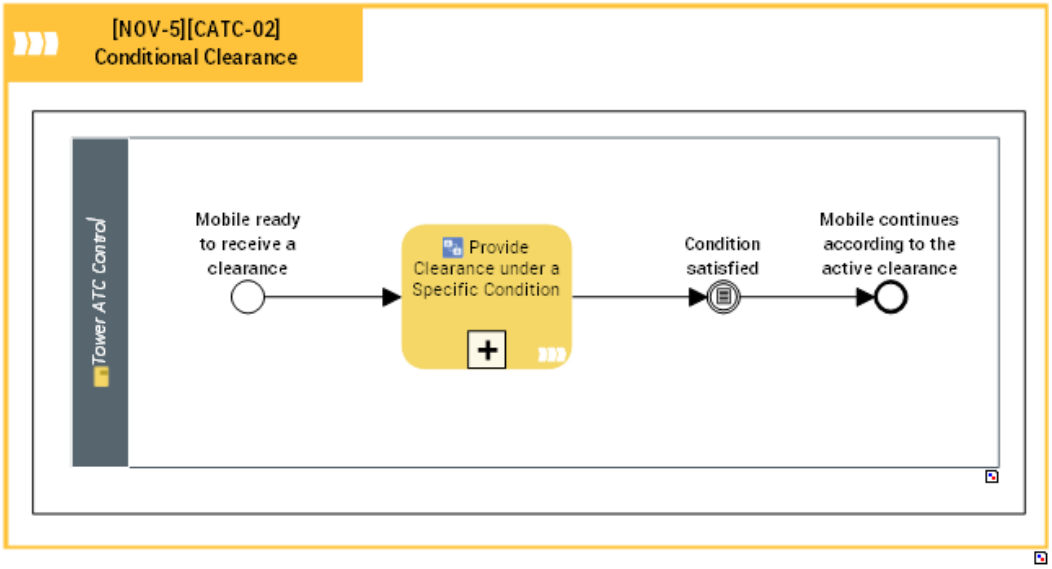


Figure 5: EATMA NOV-5 Model [CATC-02] Conditional Clearance

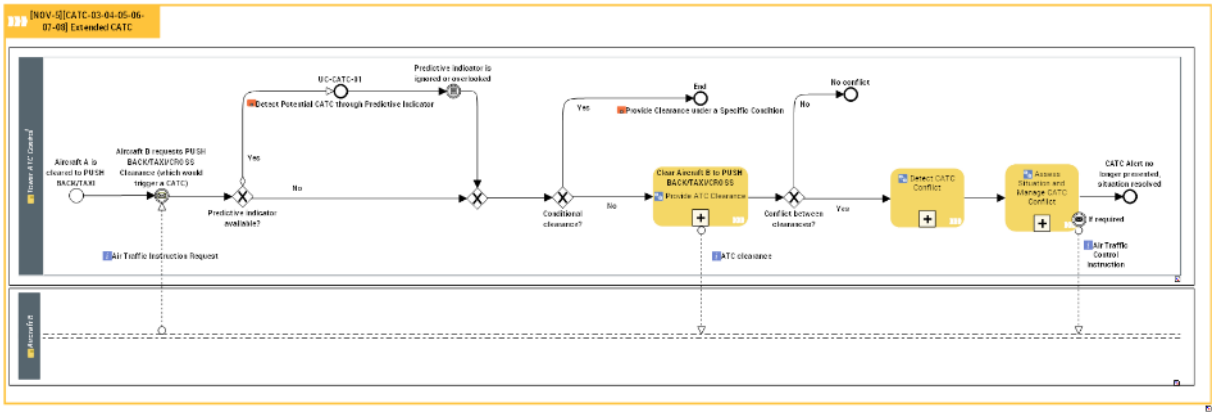

Figure 6: EATMA NOV-5 Model [CATC-03-04-05-06-07-08] Extended CATC

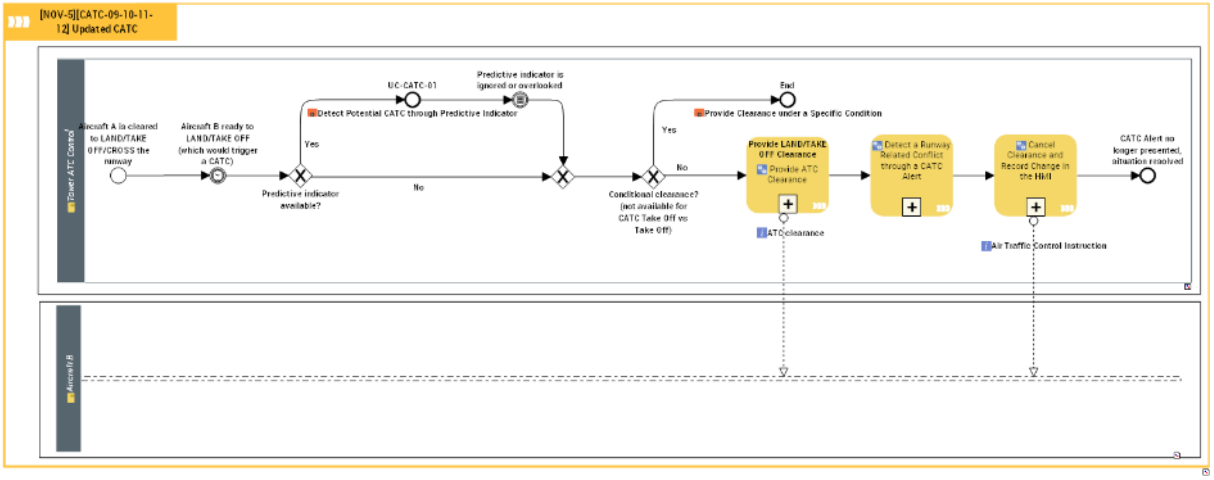

Figure 7: EATMA NOV-5 Model [CATC-09-10-11-12] Updated CATC

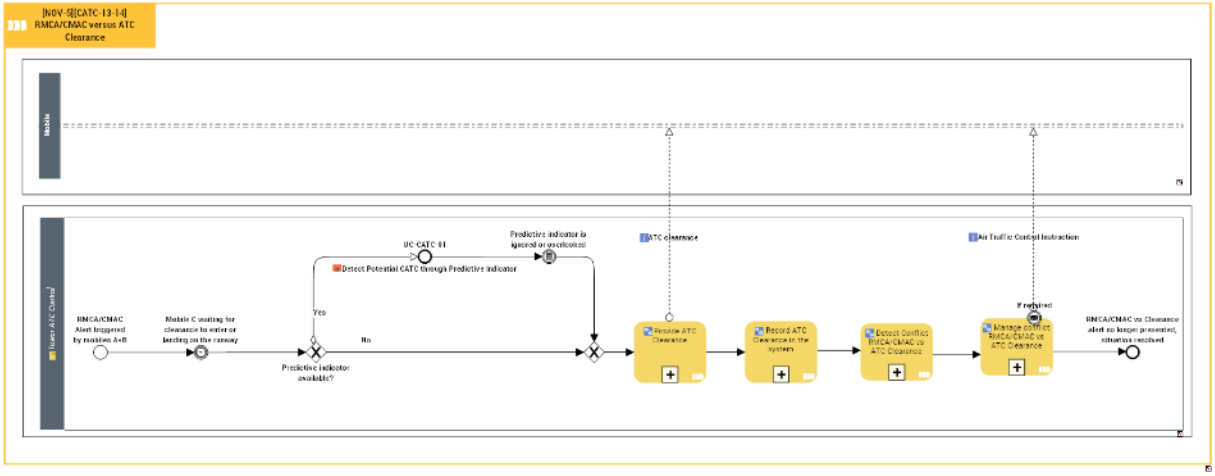


Figure 8: EATMA NOV-5 Model [CATC-13-14] RMCA/CMAC vs ATC Clearance

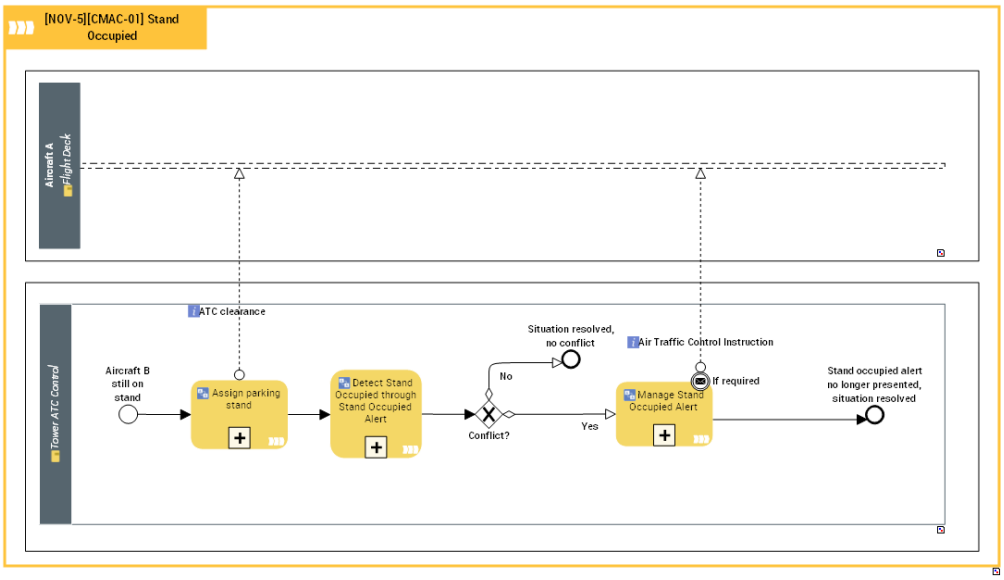


Figure 9: EATMA NOV-5 Model [CMAC-01] Stand Occupied

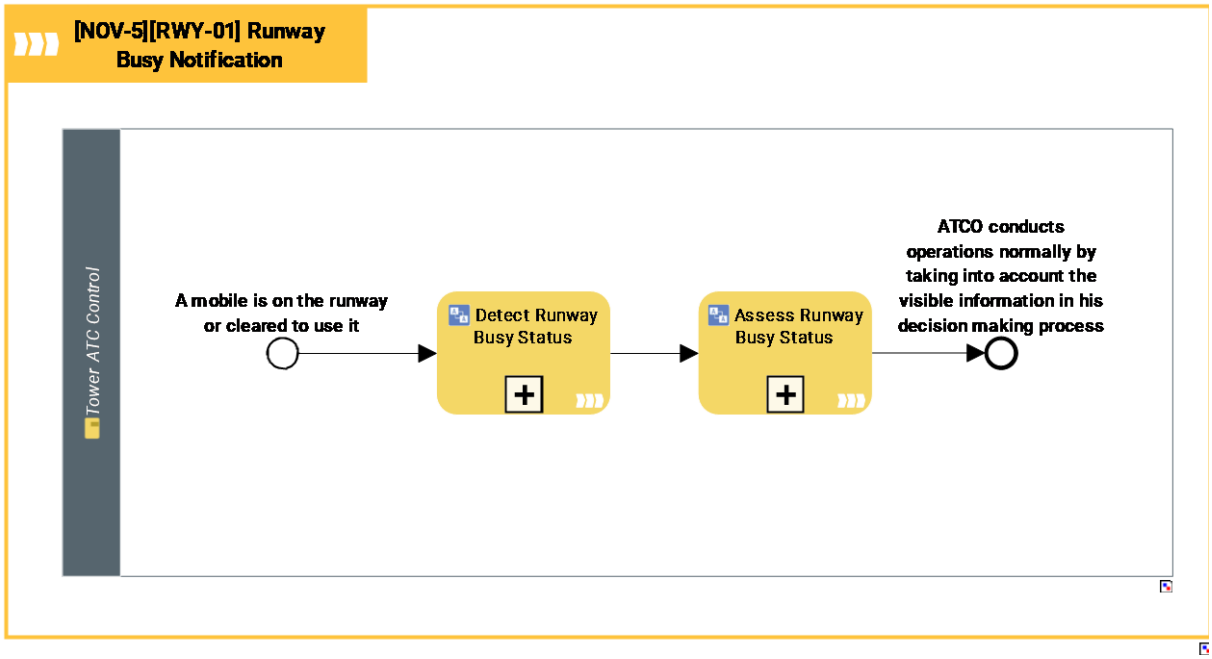


Figure 10: EATMA NOV-5 Model [RWY-01] Runway Busy Notification

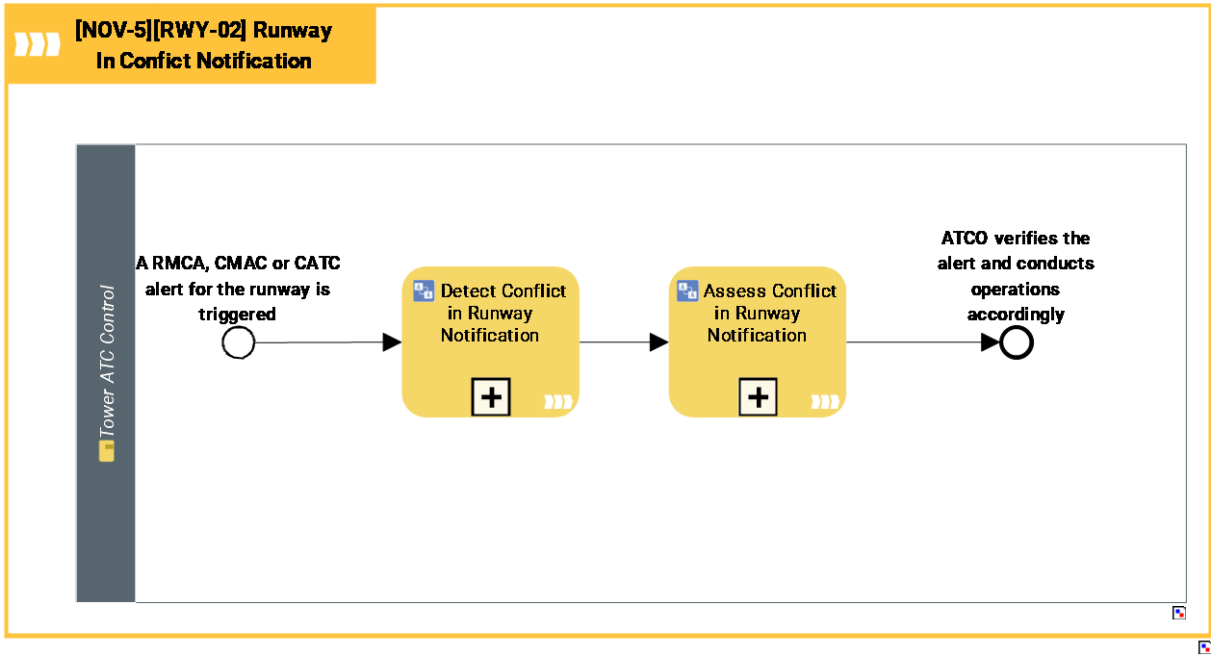


Figure 11: EATMA NOV-5 Model [RWY-02] Runway In Conflict Notification

## B.2 Derivation of SRS for Normal Operations

To derive the SRS for Normal Operations, the EATMA representations presented in section B.1 are analysed in such a way that, for each ATS Operational Service within each Use Case:

- it is checked whether the identified changes are safety relevant, i.e., if the change could impact the efficiency of a safety barrier or the occurrence of a safety precursor;
- a list of SRS is derived in order to describe the safety-relevant changes in the delivery of that operational service by the Solution (the change might impact the WHAT or the HOW of the operational service).

The following Table 11 provides the derivation of SRS in normal conditions of operation driven by EATMA Process Models associated to this Solution.

| ATS Operational Service | EATMA Use Case-Activity or Flow | Derived SRS | Related SAC# (AIM Barrier or Precursor) |
|---|---|---|---|
| Conflict detection and resolution | Predictive Indicator | **SRS 001 –** ATCO shall detect potential CATC through Predictive indicator | **SAC#1; SAC#2** |
| Conflict detection and resolution | Predictive Indicator | **SRS 002:** ATCO shall assess Predictive CATC Indication | **SAC#1; SAC#2** |
| Conflict detection and resolution | Conditional Clearance | **SRS 003 –** ATCO shall provide clearance under a specific condition when operationally required | **SAC#1; SAC#2** |
| Conflict detection and resolution | Extended CATC | **SRS 004 –** ATCO shall be aware in advance of any potential CATC conflict. | **SAC#1; SAC#2** |
| Conflict detection and resolution | Extended CATC | **SRS 005 –** ATCO shall assess situation and manage CATC and CMAC alerts | **SAC#1; SAC#2** |
| Conflict detection and resolution | Updated CATC | **SRS 006 –** ATCO shall cancel clearance and record change in the HMI | **SAC#1; SAC#2** |
| Conflict detection and resolution | CMAC vs ATC Clearance | **SRS 007 –** ATCO shall record ATC Clearance in the system | **SAC#1; SAC#2** |
| Conflict detection and resolution | CMAC vs ATC Clearance | **SRS 008 –** ATCO shall detect conflict CMAC vs ATC clearance | **SAC#1; SAC#2** |
| Conflict detection and resolution | CMAC vs ATC Clearance | **SRS 009 –** ATCO shall manage CMAC vs ATC clearance alert | **SAC#1; SAC#2** |

| ATS Operational Service | EATMA Use Case-Activity or Flow | Derived SRS | Related SAC# (AIM Barrier or Precursor) |
|---|---|---|---|
| Conflict detection and resolution | Stand Occupied | **SRS 010 –** ATCO shall detect stand occupied through Stand Occupied alert | **SAC#1; SAC#2** |
| Conflict detection and resolution | Stand Occupied | **SRS 011 –** ATCO shall manage stand occupied alert | **SAC#1; SAC#2** |
| Conflict detection and resolution | Runway Busy Notification<br>Runway In Conflict Notification | **SRS 013 –** ATCO shall be constantly and immediately aware about the operational status of the Runway, whether it is busy or it is affected by any conflict. | **SAC#1; SAC#2** |
| Conflict detection and resolution | RMCA vs ATC Clearance | **SRS 014 –** ATCO shall be aware in advance of any potential RMCA vs ATC clearance conflict. | **SAC#1; SAC#2** |
| Conflict detection and resolution | RMCA vs ATC Clearance | **SRS 015 –** ATCO shall manage RMCA vs ATC clearance conflict. | **SAC#1; SAC#2** |

**Table 11: Derivation of SRS for Normal Operations driven by EATMA Process models**

# Appendix C Risk analysis of Abnormal conditions and derivation of SRS (functionality & performance)

According to section 4.3, no abnormal conditions are defined for this solution.

# Appendix D Risk analysis addressing internal functional system failures and derivation of SRS

This appendix presents the risk analysis done at the level of the ATS service specification, including operational hazards identification and analysis in view of deriving additional SRS.

## D.1 HAZID workshop

The solution related hazards have been identified in a safety experts session held in December 2022. During this session, preliminary hazards included in Appendix A.2 were reviewed and Operational Hazards were defined. Considering the preliminary list of hazards, safety experts did the following comments:

- It is not necessary to maintain Hr#1 and Hr#2 as particular hazards. Both hazards are based on the ATC system failure when detecting conflicting clearances, so they can be merged on a unique hazard.
- It is not necessary to maintain Hr#3 and Hr#4 as particular hazards. Both are based on a malfunction of the solution deriving in a false alert, so they can be merged on a unique hazard.
- It is not necessary to maintain Hr#5 and Hr#6 as particular hazards. Both are based on a malfunction of the solution deriving in an erroneous ATC action, so they can be merged on a unique hazard.
- Hr#7, Hr#8 and Hr#9 are hazards based on the malfunction of the system, leading in a wrong information to ATC and, therefore, a wrong ATC action.

Considering these comments and that the operational hazards must be focused on ATC performance when using the solution, it was decided to stablish hazards that represent ATC not being able to detect and solve safety events. This way, it is not necessary to distinguish the preliminary event and the following operational hazards were defined.

- OH 01: ATC do not correctly detect conflicting clearances (because of lack of detection or incorrect/incomplete information of CATC/ CMAC alert)
- OH 02: ATC do not correctly detect conflicting clearances (because of lack of detection or incorrect/incomplete information of RMCA vs CATC Alert or CMAC vs CATC alert)
- OH 03: ATC do not detect correctly conflicting parking instruction (because of lack of detection or incorrect information of Stand Occupied CMAC alert)

It was decided to stablish one operational hazard referred to parking operations because of its particular characteristics. Hr#5 and Hr#6 are related with this OH-03.

On the other hand, it was decided to stablish two different operational hazards related to CATC and CMAC alerts. Hr#1, Hr#2, Hr#3, Hr#4, Hr#7, Hr#8, and Hr#9 are related with OH-01 and OH-02, being seen as malfunctions of the solution, which lead in ATC not correctly using the alerts.

## D.2 HAZID participation list

Stephen Straub (Solution Leader from DFS), Sergio Cámara (safety expert from ENAIRE), Arancha García (safety expert from ENAIRE), Rebeca Llorente (project member from ENAIRE), David Concostrina (safety expert from Ineco) and Angela Abad (Safety expert from Ineco).

# Appendix E Designing the Solution functional system for normal conditions

## E.1 Deriving SRD from the SRS

The Table 12 below shows how the Safety Requirements at ATS Service level (SRS) for normal conditions of operation derived in section 4.2.1 map onto the related elements of the Design Model (functional system components or interactions/data flows) and derive Safety Requirements at Design level (SRD) (functionality & performance) for normal conditions of operation. It includes the following information:

- the SRS (functionality & performance) to mitigate risk in normal condition, as presented in section 4.2.
- the derived SRD driven by the mapping of the SRS onto the related elements of the Design Model, accompanied by relevant Assumptions as appropriate.
- the Design Model elements (functional system components or interactions/data flows or external elements impacted by the Change) relevant for the derived SRD and/or assumptions.

The consolidated list of derived SRDs is to be included in section 5.3, while the associated assumptions are included in the Assumptions log table from Appendix Appendix I

| SRS for Normal Operation (ID & content) | Safety Requirement at Design level[2] (SRD) or Assumption | Maps onto |
|---|---|---|
| **SRS 001 –** ATCO shall detect potential CATC through Predictive indicator | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | External: equipment |
| | SRD 003: The Controller will be presented with an indicator on the HMI that informs the Controller that the input of a specific clearance for a mobile will trigger a CATC alert. | External: equipment |
| **SRS 002 –** ATCO shall assess Predictive CATC Indication | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| **SRS 003 –** ATCO shall provide clearance under a specific condition when operationally required | SRD 004: The Controller when issuing a clearance to a mobile may link the clearance to a condition and enter the clearance and condition in the HMI | ATC training |
| **SRS 004 –** ATCO shall be aware in advance of any potential CATC conflict. | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| | SRD 005: The Tower Ground Controller shall receive an alert when issuing a PUSH BACK clearance that conflicts with a previously input PUSH BACK clearance according to local rules and procedures. | External: equipment |
| | SRD 006: The Tower Ground Controller shall receive an alert when entering a TAXI clearance via the HMI that conflicts with a previously input PUSH BACK clearance according to local rules and procedures | External: equipment |
| | SRD 007: The Tower Ground Controller shall receive an alert when entering a PUSH BACK clearance via the HMI that conflicts with a previously input TAXI clearance according to local rules and procedures. | External: equipment |
| | SRD 008: The Tower Ground Controller shall receive an alert when entering a TAXI clearance for an aircraft A to taxi onto a taxiway where the aircraft A would obstruct the path of another aircraft B taxiing. | External: equipment |
| | SRD 009: The Tower Ground Controller shall receive an alert when a TAXI clearance is entered via the HMI and another TAXI clearance was input previously where the two cleared routes are in opposite directions on the same taxiway and are predicted to block each other (Deadlock Situation). | External: equipment |
| | SRD 010: The Tower Runway Controller shall receive an alert when a LAND clearance is input for an aircraft while a LAND clearance was previously given to another aircraft on the same runway and the separation minima on the runway (according to ICAO DOC4444) are not expected to be achieved the moment the second landing aircraft crosses the runway threshold. | External: equipment |
| | SRD 011: The Tower Runway Controller shall receive an alert when a LAND clearance is input for an aircraft while previously a TAKE OFF clearance was input for another aircraft on the same runway and the separation minima on the runway (according to ICAO DOC4444) are not expected to be achieved the moment the landing aircraft crosses the runway threshold. | External: equipment |

[2] iSRD for the initial design or rSRD for the refined design

| | | |
|---|---|---|
| | SRD 012: The Tower Runway Controller shall receive an alert when a LAND clearance is input for an aircraft while previously a CROSS clearance was input on another aircraft on the same runway and the separation minima on the RWY (according to ICAO DOC4444) are not expected to be achieved the moment the landing aircraft crosses the RWY threshold. | External: equipment |
| | SRD 013: The Tower Runway Controller shall receive an alert if a TAKE OFF clearance is input for an aircraft, while a TAKE OFF clearance was previously input for another aircraft on a different runway and the ground or the air trajectories (SIDs) are converging according to local procedures/rules. | External: equipment |
| **SRS 005 –** ATCO shall assess situation and manage CATC and CMAC alerts | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| **SRS 006 –** ATCO shall cancel clearance and record change in the HMI | A001: The system allows the ATCO to cancel a clearance and record the change in the HMI. | External: equipment |
| **SRS 007 –** ATCO shall record ATC Clearance in the system | A002: The system allows the ATCO to record ATC clearances. | External: equipment |
| **SRS 008 –** ATCO shall detect conflict CMAC vs ATC clearance | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | External: equipment |
| | SRD 014: The Tower Runway Controller shall receive an alert when a LINE UP/TAKE OFF/CROSS/ENTER or LAND clearance is entered via the HMI whilst a CMAC alert (RWY Incursion, No Take Off, No Land or Wrong Runway) is active for the same runway. | External: equipment |
| **SRS 009 –** ATCO shall manage CMAC vs ATC clearance alert | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| **SRS 010 –** ATCO shall detect stand occupied through Stand Occupied alert | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| | SRD 015: The Controller shall receive an INFORMATION Alert on the HMI when the allocated stand for an arrival flight is occupied. | External: equipment |
| **SRS 011 –** ATCO shall manage stand occupied alert | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | ATC training |
| **SRS 012:** The System / Equipment supporting the solution has to meet the defined failure rate. | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | External: equipment |
| **SRS 013 –** ATCO shall be constantly and immediately aware about the operational status of the Runway, whether it is busy or it is affected by any conflict. | SRD 016: The Tower Runway Controller shall receive a visual indication if a runway is affected by any alert. | External: equipment |
| | SRD 017: The Tower Runway Controller shall receive a visual indication if a runway is currently occupied by any mobile or if a mobile has been cleared to use it. | External: equipment |
| **SRS 014 –** ATCO shall be aware in advance of any potential RMCA vs ATC clearance conflict. | SRD 018: The Tower Runway Controller shall receive an alert when a LINE UP/TAKE OFF/CROSS/ENTER or LAND clearance is entered via the HMI whilst an RMCA alert is active for the same runway. | External: equipment |
| **SRS 015 –** ATCO shall be able to manage RMCA vs ATC clearance conflict. | SRD 018: The Tower Runway Controller shall receive an alert when a LINE UP/TAKE OFF/CROSS/ENTER or LAND clearance is entered via the HMI whilst an RMCA alert is active for the same runway. | External: equipment |

**Table 12: SRD derived by mapping SRS for normal conditions of operation to Design Model Elements**

## E.2 Static analysis of the solution functional system behaviour

No static analysis has been conducted.

## E.3 Dynamic analysis of the Solution functional system behaviour

For this solution, a total of three validation exercises have been carried out in order to reach maturity level V3. The exercises, described in the VALR [16], are:

- EXE-02.21.1-V3-VALP-001 performed by DFS with shadow mode trials on Düsseldorf Airport layout (large airport),
- EXE-02.21.1-V3-VALP-003 performed by ENAIRE used real-time simulations on the layout of Barcelona Airport (very large airport), and
- EXE-02.21.1-V3-VALP-004 performed by LEONARDO, used real-time simulations on the layout of Sofia Airport (medium airport).

Based on the results, several conclusions and recommendations were derived. Attending to these results, they can be summarized as follows:

- The local procedures must be fully supported by the Safety Support Tools, otherwise, unnecessary mental workload can be generated for ATC. It is recommended to thoroughly study the adaptation of detection rules to local procedures before deployment.
- The analysis of the results of the long-term runs in cooperation with local airport controllers, leads to a clear picture of what support the controllers expect from the CATC service and which alerts are undesirable in which situation.
- Implementation of a calibration approach that optimizes CATC alerts to ensure the best possible alert trigger timing.
- The CATC and CMAC alerts in combination with RMCA should be well selected to adequately support safety.
- The deployment of the Safety Support Tools is considered a complex task. A possible approach to simplify this task is the specification of a Minimum Viable Product (MVP) that allows a first trial installation for a limited number of alerts, on which the necessary deployment steps can be practiced.
- The actual relevance of the RMCA/CMAC vs. ATC Clearance alerts should be checked for the respective airport in real operation.
- The ATCOs must know and understand the rules and parameters applied by the conflict detection. This helps to avoid misinterpretations, reduces the mental workload, and shortens the reaction time. Proper training is a key factor in improving safety.

Analysing all the recommendations from a safety approach, it is considered that, except the one talking about ATC training, it is not necessary to establish additional safety requirements. Every recommendation can be seen as an operational improvement of the solution when deployed, but they are not safety issues and then, no safety actions must be taken.

The training recommendation is already included in this document by SRD 001, so no more requirements are stablished.

# Appendix F Designing the Solution Functional system for Abnormal conditions of operation

No abnormal conditions are defined for this solution.

# Appendix G Designing the Solution functional system addressing internal functional system failures

This appendix presents the detailed risk evaluation and mitigation of the operational hazards identified at section 4.4, performed at the level of the design of the Solution functional system.

## G.1 Deriving SRD from the SRS (integrity/reliability)

The purpose is to derive from the SRS (integrity/reliability) that have been derived in section 4.4.2:

- SRD (functionality & performance) in order to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the operational hazard.
- SRD (integrity/ reliability) to limit the frequency with which failure of modified/new equipment elements in the Solution Functional system could be allowed to occur.

The above should be derived with consideration of the common cause failures (in case such failures are revealed by the common causes analysis).

## G.1.1 Top-down causal analysis

| Cause ID | Cause | Detailed description | Mitigation/Safety Requirement |
|---|---|---|---|
| **OH01:** ATC do not correctly detect conflicting clearances (because of lack of detection or incorrect/incomplete information of CATC/ CMAC alert;) | | | |
| CA01 | ATCO is not able to use the solution | ATCO is not able to use the information because a lack of training. ATCO doesn't use or uses incorrectly the information from the solution. | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. |
| CA02 | CATC alert is no available | Alert is not available because lack or incorrect information. ATCO has not enough information to use the solution. | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **OH02:** ATC do not correctly detect conflicting clearances (because of lack of detection or incorrect/incomplete information of RMCA vs CATC Alert or CMAC vs CATC alert;) | | | |
| CA01 | ATCO is not able to use the solution | ATCO is not able to use the information because a lack of training. ATCO doesn't use or uses incorrectly the information from the solution. | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. |
| CA02 | CATC/RMCA/CMAC alert is no available | Alert is not available because lack or incorrect information. ATCO has not enough information to use the solution. | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **OH03:** ATC do not detect correctly conflicting parking instruction (because of lack of detection or incorrect information of Stand Occupied CMAC alert) | | | |
| CA01 | ATCO is not able to use the solution | ATCO is not able to use the information because a lack of training. ATCO doesn't use or uses incorrectly the information from the solution. | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. |
| CA02 | CMAC alert is no available | Alert is not available because lack or incorrect information. ATCO has not enough information to use the solution. | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |

## G.1.2 Bottom-up failure modes and effects analysis

| Functional system element | Failure mode | Effects | Mitigation/Safety Requirement | Operational hazard |
|---|---|---|---|---|
| ATCO | ATCO is not able to use the solution | ATCO doesn't use the information properly and the event is not avoided | SRD 001: ATC staff shall be trained in how to use the CATC and CMAC alert system and how to recognize and manage the CATC and CMAC alerts. | OH1 & OH2 & OH3 |
| Equipment | CATC alert is no available | Alert doesn't show the information properly and the event is not avoided | SRD 002: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. | OH1 & OH2 & OH3 |
| | CATC/RMCA/CMAC alert is no available | | | |
| | CMAC alert is no available | | | |

## G.2 Deriving SRD from the SRS (functionality & performance) for protective mitigation

The purpose of this section is to derive SRD (functionality & performance) from the SRS (functionality & performance) that have been derived in section 4.4.2 to provide mitigation against operational hazard effects (protective mitigation), with consideration of the potential common cause failures that might affect the operational hazard causes and its protective mitigation.

| | **Safety Requirement at Design level[3] (SRD) or Assumption** |
|---|---|
| **SRS 012:** The System/Equipment supporting the solution has to meet the defined failure rate. | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 016a:** The frequency of a RWY event in which the CATC/ CMAC alert is not shown to ATC by the system shall be no more than 5e-7 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 016b:** The frequency of a TWY event in which the CATC/ CMAC alert is not shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 017a:** The frequency of a RWY event in which the CATC/ CMAC alert is incorrectly shown to ATC by the system shall be no more than 5e-7 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 017b:** The frequency of a TWY event in which the CATC/ CMAC alert is incorrectly shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 018a:** The frequency of a RWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is not shown to ATC by the system shall be no more than 5e-7 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 018b:** The frequency of a TWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is not shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 019a:** The frequency of a RWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is incorrectly shown to ATC by the system shall be no more than 5e-7 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 019b:** The frequency of a TWY event in which the RMCA vs CATC Alert or CMAC vs CATC alert is incorrectly shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |

[3] iSRD for the initial design or rSRD for the refined design

| | Safety Requirement at Design level[3] (SRD) or Assumption |
|---|---|
| **SRS 020:** The frequency of a TWY event in which the Stand Occupied CMAC alert is not shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |
| **SRS 021:** The frequency of a TWY event in which the Stand Occupied CMAC alert is incorrectly shown to ATC by the system shall be no more than 3,3e-3 per Flight Hour | **SRD 002**: The system deploying the Extended Airport Safety Nets shall be certified and correctly maintained. |

# Appendix H Demonstration of Safety Criteria achievability

This section shows the extent to which the achievability of the Safety Criteria has been demonstrated through the satisfaction of the success criteria of the safety validation objectives defined in relation to the Solution RTS.

The demonstration holds to the extent where this exercise addresses all the SRS (functionality & performance), and more specifically, all the derived SRD (functionality & performance) (the SAC achievability accounting for internal functional system failures, i.e., considering the integrity/reliability safety requirements can be demonstrated only by predictive safety assessment – see sections 4.4 and 5.5).

The safety-related outcomes of the RTS brings therefore an essential contribution to the demonstration of the Safety Criteria achievability by the Solution design.

The safety-relevant results of the validation are summarized in the following table, in which the extent to which the relevant SRDs have been covered is indicated.

| Exercise Safety Validation Objective & related SAC(s) | Success criterion | Coverage (SRS) | Validation results |
|---|---|---|---|
| EX3-OBJ-02.21.1-V3-VALP-SAF-001: Safety Impact of Enhanced Safety Support Tools<br><br>[SAC #1; SAC #2] | EX3-CRT-02.21.1-V3-VALP-SAF-001-001: The Situational awareness will be improved | **SRS 001**: fully covered<br>**SRS 002**: fully covered<br>**SRS 003**: fully covered<br>**SRS 004**: fully covered<br>**SRS 005**: fully covered<br>**SRS 006**: fully covered<br>**SRS 007**: fully covered<br>**SRS 008**: fully covered<br>**SRS 009**: fully covered<br>**SRS 010**: fully covered<br>**SRS 011**: fully covered<br>**SRS 012**: fully covered<br>**SRS 013**: fully covered<br>**SRS 014**: fully covered<br>**SRS 015**: fully covered | ATCOs confirm that the Safety Support Tools improve Situational Awareness |
| | EX3-CRT-02.21.1-V3-VALP-SAF-001-002: The proportion of Runway conflicts will decrease (compared to the reference) | N/A | ATCOs confirm that CATC alerts for Runway Operations increase safety by supporting the ATCO to reduce runway conflicts. |
| | EX3-CRT-02.21.1-V3-VALP-SAF-001-003: The proportion of Ground conflicts (taxiway and apron) will decrease (compared to the reference) | N/A | ATCOs confirm that CATC and CMAC alerts for Ground Operations increase safety by supporting the ATCO to reduce apron and taxiway conflicts. |

**Table 13: Solution Safety Validation results**

# Appendix I Assumptions, Safety Issues & Limitations

## I.1 Assumptions log

Assumptions are statements that are taken for granted or that are considered true. They are usually related to matters outside the scope of the change, but which are essential to the completeness and/or correctness of the safety assessment results.

In this section, all the assumptions are listed in table 12. Moreover, a rationale or evidence on which the validity of these assumptions is based is provided.

| Ref | Assumption | Validation |
|---|---|---|
| A001 | The system allows the ATCO to cancel a clearance and record the change in the HMI. | System functionality |
| A002 | The system allows the ATCO to record ATC clearances. | System functionality |

**Table 14: Assumptions log**

## I.2 Safety Issues log

No safety issues are identified on this solution.

## I.3 Operational Limitations log

No Operational Limitations were raised during the development of the safety assessment.

**-END OF DOCUMENT-**

Beneficiaries contributing to Solution PJ.02-W2-21.1