INDUSTRIAL RESEARCH

sesar JOINT UNDERTAKING

[SESAR Solution 25.1 SPR-INTEROP/OSED for V3 - Part II - Safety Assessment Report]

Deliverable ID:	**D7.1.002**
Dissemination Level:	**PU**
Project Acronym:	**PJ02-W2 AART**
Grant:	**874477**
Call:	**H2020-SESAR-2019-1**
Topic:	**Airport airside and runway throughput**
Consortium Coordinator:	**EUROCONTROL**
Edition Date:	**17 April 2023**
Edition:	**00.00.02**
Template Edition:	**00.00.03**

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Authoring & Approval

Authors of the document

Beneficiary	Date
UNIWARSAW	17 February 2023

Reviewers internal to the project

Beneficiary	Date

Reviewers external to the project

Beneficiary	Date

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

Beneficiary	Date
PANSA	13/03/2023
Airbus	13/03/2023
Dassault	13/03/2023

Rejected By - Representatives of beneficiaries involved in the project

Beneficiary	Date

Document History

Edition	Date	Status	Beneficiary	Justification
00.00.01	17 Feb 2023	Submitted for review	UNIWARSAW	
00.00.02	17 Apr 2023		UNIWARSAW	PJ19 comments

EUROPEAN PARTNERSHIP

Co-funded by the European Union

PJ02-W2 AART

AIRPORT AIRSIDE AND RUNWAY THROUGHPUT

This Safety Assessment Report 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

Table of Contents

EUROPEAN PARTNERSHIP
Co-funded by the European Union

List of Tables

List of Figures

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union

1 Executive Summary

Solution PJ.02-W2 Solution 25.1 – Enhanced runway condition awareness for runway excursion prevention – addresses concepts which allow the implementation of the systems that together aim to provide continuous awareness of the current and predicted runway condition:

- Runway Condition Awareness and Monitoring System (RCAMS) is a ground-based system operated by the Airport Operator. It performs a continuous assessment of current runway surface condition and provides a short-term forecast of runway conditions. Under Airport Operator control it disseminates this information to other stakeholders.
- On-board Braking Action Computation System (OBACS) is an airborne system generating reports of runway surface condition as sensed by the braking aircraft.

that help to continuously determine and disseminate runway condition in GRF format to flight deck, controllers and to airport operator when appropriate.

The SAR (Safety Assessment Report) draws upon the detailed descriptions of the Operating Environment and Use Cases documented in the PJ02-W2 Solution 25.1 SPR-INTEROP/OSED document in order to define a list of achievable Safety Criteria (SC) and is also contributing to the Operational Service and Environment Definition (OSED)/Safety and Performance Requirements (SPR)/Interoperability (INTEROP). As such it is not a self-contained document.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

2 Introduction

2.1 Background

The Operational Service and Environment Definition (OSED) describes the operational concept, the operational services, their environment, use cases and is used as the basis for assessing and establishing operational, safety, performance and interoperability requirements for the related systems detailed in the Safety and Performance Requirements (SPR) and INTEROP sections of this document. The OSED identifies the operational services supported by several entities within the ATM community and includes the operational expectations of the related systems.

2.2 General Approach to Safety Assessment

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

- a success approach which is concerned with the safety of the Solution service provision 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 service provision 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 stage V2 of PJ03b-06 Solution (precedessor) and V3 of this Solution development (Safety Requirements at service level and at design level). Part of Solution 25.1 development is a change of the scope of the implementation of the RCAMS system, focusing only on the Airport Operator tasks. Solution 25.1, contrary to PJ03b-06, is a non - Air Traffic Services Solution when safety assessment is concerned

The assurance of validation and verification of the safety assessment requirements is an on-going activity. A qualitative safety assessment has been performed on the basis of the Use Cases, Solution Scenarios VS Reference Scenario and Operating Method described in the OSED and validated through the exercises described in the VALP and recorded in the synthesis of validation results VALR for Shadow Mode Validation Exercise held from December 2021 to April 2022 and Real Time Simulation held in April 2022, as well as through the workshops organised by Solution partners – Airbus, Dassault and Uniwarsaw.

2.3 Scope of the Safety Assessment

This SPR-INTEROP/OSED identifies the operating method options that were analysed in the V3 phase to address Operational Improvement AO-216. It should also be noted that PJ.02-W2 Solution 25.1 work might also contribute to mature the OI AUO-0616, which is led by PJ.02-W2 Solution 25.2.

This document focuses mainly on the success approach to assess how much the identified pre-existing hazards already in aviation are expected to be reduced by the implementation RCAMS system, being also verified by airborne OBAC system.

Co-funded by the European Union

Based on the information detailed in the Solution PJ02-W2 Solution 25.1 SPR-INTEROP/OSED document, the SAR describes, through the definition of safety objectives (from the failure approach), how they could mitigate pre-existing hazards. Beneficially the part II SPR-INTEROP/OSED contains the Specimen Safety Assessment for an application of the RCAMS Solution in operations. The report presents even the assurance that the Safety Requirements for the V3 phase are complete, correct and realistic, thereby it provides all material to adequately contribute to Solution 25.1 Data Pack

2.4 Layout of the Document

- **Section 1** presents the executive summary of the document.
- **Section 2** provides background information regarding the definition, design and validation addressed in the PJ.02-W2-25.1 Concepts, the principles for safety assessment in SESAR Programme and the scope of this safety assessment
- **Section 3** provides the main information collected within the SAF&HP Scoping and Change assessment and Safety Assessment Plan development process in order to set the scene for the safety assessment documented in the SAR.
- **Section 4** presents the Safety Requirements at Service level for the corresponding “Other than ATS” operational Solution.
- **Section 5** documents the Safety Requirements at Design level (SRDs) for the corresponding “Other than ATS” operational Solution.
- **Section 6** shows the extent to which the achievability of the SRS has been demonstrated through the satisfaction of the success criteria of the safety validation objectives defined in relation to the Solution planned validation exercises or other specific validation means (e.g. data analysis, Safety and/or HP workshops).
- **Appendix A** presents the definition of the SRS (functionality and performance) in order to set the Service Safety Specification under normal (i.e. those conditions that are expected to occur on a day-to-day basis) and abnormal conditions of operation.
- **Appendix B** presents the results of the risk assessment done at the service specification level, including service hazards identification and assessment in view of deriving additional SRS.
- **Appendix C** shows how the Safety Requirements at Service level (SRS) for normal and abnormal conditions of operation derived in sections 4.2 and 4.3 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 and performance) for normal and abnormal conditions of operation.
- **Appendix D** presents the detailed risk evaluation and mitigation of the Service Hazards from section 4.4 performed at the level of the design of the solution functional system.
- **Appendix E** includes all the assumptions that were necessarily raised in deriving the above Safety Requirements, safety issues that were necessarily raised during the safety assessment and the operational limitations that were raised in the safety assessment.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

3 Setting the Scene of the safety assessment

3.1 Operational concept overview and scope of the change

Runway excursions account for nearly a quarter of all runway safety accidents, according to IATA. Solution PJ02-W2 25.1 aims to improve the assessment of runway surface contamination and global awareness in order to prevent runway excursions during take-off and landing.

The Solution 25.1 add to current operational method:

- Introduces Predicted Runway Surface Condition within time frame of 1 hour
- Disseminates the information about current and predicted Runway Condition Code, to give flight crews better possibility to prepare for their landing performance assessment. The runway condition assessment is performed by integration of additional inputs from embedded runway sensors and MET, surveillance data and aircraft report on breaking action (PIREP)
- Current and predicted RWYCC can be also supported by a SWIM service for more reliable dissemination.
- Runway decontamination activities are supported by the RCAMS predicted information provided to Airport Operator
- Runway Inspection team uses RCAMS as their support tool to enter their measurements and observations and to generate Runway Condition Report directly from the runway
- Decontamination and winter services actions can be planned by AO based on predictions provided by RCAMS
- Braking Action reported by Flight Crew is used as RCAMS input for runway condition assessment

For more detail on the operational concept refer to SESAR Solution PJ02-W2-25.1 SPR-INTEROP/OSED for V3 - Part I.

3.2 Solution Operational Environment and Key Properties

The relevant operational environment has been described in SPR-INTEROP/OSED, part I

3.3 Stakeholders' expected benefits with potential Safety impact

Solution 25.1 focuses on Airport Operator as the main stakeholder, taking into account also the expectations of ANSP, Airline and Flight Crew. As such, Solution 25.1 aims at reducing the risk of runway excursions during landing and take-off. Runway excursions are the most frequent type of runway safety accident (25% of all accidents over the 2015-2019 period according to 2019 IATA Safety Report). The risk of runway excursion can be mitigated by on-board and ground systems that help to determine and disseminate runway condition to pilots, controllers and airport operator when appropriate

Please refer to VALP p. I and SPR-INTEROP/OSED p. I for details of stakeholders expectations.

3.4 Intended Operational use of the Service Concept

3.4.1 Intended use identified from SESAR Operational Solutions

PJ02-W2 Solution 25.1 did not identified other Solutions that are using services provided by Solution 25.1. The Runway Condition Report, as required by Global Reporting Format, produced with the use of AO-0216 and AO-0107, is used thanks to ATIS integration..

3.4.2 Other intended use outside-SESAR

N/A

3.5 Relevant applicable standards

- Commission Implementing Regulation (EU) 2020/469 of 14 February 2020 amending Regulation (EU) No 923/2012, Regulation (EU) No 139/2014 and Regulation (EU) 2017/373 as regards requirements for air traffic management/air navigation services, design of airspace structures and data quality, runway safety and repealing Regulation (EC) No 73/2010
- Commission Delegated Regulation (EU) 2020/2148 of 8 October 2020 amending Regulation (EU) No 139/2014 as regards runway safety and aeronautical data (Text with EEA relevance)
- ICAO Annex 14 - Aerodromes - Volume I - Aerodromes Design and Operations, 9th Edition, July 2022
- ICAO Annex 15 to the Convention on International Civil Aviation Aeronautical Information Services
- ICAO Guidance On The Issuance Of Snowtam (Applicable from 5 November 2020) - First Edition (V.1.0) February 2020
- ICAO Circular Assessment, Measurement and Reporting of Runway Surface Conditions (CIR 355)
- ICAO Procedures for Air Navigation Services (PANS) - Aerodromes (Doc 9981) 3rd Edition, 2020

EUROPEAN PARTNERSHIP

Co-funded by the European Union

4 Safety specification at Service level

4.1 Overview of activities performed

This section addresses the following activities:

- Derivation of Safety Requirements at Service level (SRS) in normal conditions of operations – section 4.2
- Assessment of the adequacy of the operational services provided by the Solution under abnormal conditions of the Operational Environment and derivation of necessary SRSs – section 4.3
- Assessment of the adequacy of the operational services provided by the Solution in the case of internal failures and mitigation of the Solution functional system generated hazards derivation of SRS – 4.4
- Verification of the operational safety specification process (mainly about obtaining Backing Evidence from the properties of the process by which Direct Evidence was gleaned) – Section 4.5

4.2 Service Safety specification – Normal conditions of operation

The SRS (functionality & performance) for normal conditions of operation are derived taking into account:

- All relevant Use Cases
- EATMA Models at operational specification level (NOV-5 diagrams).
- Impact on neighbouring ATM Systems.

The design characteristics/items of the Solution functional system should not be considered at this level but at the design level (in section 5.2), when the derived SRSs will enable the derivation of the Safety Requirements at Design level (SRD). For more detail on the SRS please go to Appendix A.

Relevant Use Cases

- Use Case PJ.02-W2-25-1: Elaborate Runway Condition Report
- Use Case PJ.02-W2-25-2-0: Runway Condition dissemination

SRS ID	SRS for Normal conditions of operation
SRS 001	The Airport Operator shall be provided with the Computed Current RWYCC and the Computed Predicted RWYCC values with the required certainty level.
SRS 002	Airport Operator within its Airport Duty Officer role shall perform the validation of Computed Current Runway Condition in a timely manner upon any significant change
SRS 003	The Airport Operator shall disseminate RCR in timely manner via ATIS or R/T means of communications.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SRS ID	SRS for Normal conditions of operation
SRS 004	All relevant ATS services shall have means to know the most up to date Current Runway Surface Condition of any runway the RCAMS system is operational and to inform about any observed discrepancies (PIREP).
SRS 005	Approach/Tower Runway ATCO shall disseminate the Current Runway Condition to the Flight Crew upon each change in a timely manner and/or on request.

Table 1: List of SRS (functionality and performance) for normal conditions of operation

Impact on neighbouring ATM systems

The functioning of this system may directly affect the indications of the ATIS system and also indirectly affect AMAN/DMAN systems […]

4.3 Service Safety specification - Abnormal conditions of operation

The SRS (functionality & performance) for abnormal conditions of operation are derived taking into account:

- All relevant Use Cases
- EATMA Models at operational specification level (NOV-5 diagrams).
- Impact on neighbouring ATM Systems.

The design characteristics/items of the Solution functional system should not be considered at this level but at the design level (in section 5.2), when the derived SRSs will enable the derivation of the Safety Requirements at Design level (SRD). For more detail on the SRS please refer to Appendix A.

SRS ID	SRS for abnormal conditions of operation
SRS 006	Whenever RCAMS system or its part is down, a degraded mode is provided
SRS 007	Whenever RCAMS output is not received by ATIS, an alternative manual input is provided

Table 2: List of additional SRS for Abnormal conditions of operation

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

4.4.1 Service Hazards identification and analysis

This section presents the consolidated results from the hazard identification, analysis and HAZID workshop (detailed working table, results and HAZID workshop participation are included in Appendix B)

ID	Service Hazard Description	Operational Effects	Mitigation of effects propagation	Severity *(most probable effect)*

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SH 01	Current and Predicted RWYCC values incorrect and higher than actual values.	Inadequate automated RCR input to AO	AO to validate any RCAMS RCR before dissemination. Machine Learning model trained to predict more conservative RWYCC values	(REF8), RE-SC3
SH 02	RCAMS system failure	Lack of automated RCR provision to AO	Fall back to manual inspection of the runway	(REF9)
SH 03	RCAMS – ATIS integration failure	RCR will not be submitted to ATIS after verification by AO automatically	Fall back to manual input of the RCR to ATIS by AO	(REF9)

Table 3: Service Hazards and Analysis

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

SRS ID	Additional Safety Requirements at Service level *(functionality & performance)*	Mitigated Service Hazard
SRS008	Provision of monitoring and alerting of the RCAMS functioning, reverting to manual AO procedures for RCR creation and dissemination	SH-01, SH-02, SH-03

Table 4: Additional SRS (functionality and performance) to mitigate Service hazards effects

SRS ID	Safety Requirements at Service level *(integrity/reliability)*	Related Service Hazard	Severity & IM

Table 5: Safety Requirements at Service level - integrity/reliability

For more detail on this section content access the Appendix A and B of the Document

4.5 Process assurance of the Safety Specification at service level

For more detail on this section content access the Appendix A and B of the Document.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

5 Safe Design of the Solution functional system

The purpose of this section is to document the Safety Requirements at Design level (SRDs) for the corresponding “Other than ATS” operational Solution.

The SRDs are design characteristics/items of the Solution functional system to ensure that the system operates as specified and is able to achieve the SRS (because based on the verification/demonstration of these characteristics/items, it could be concluded that the SRS are met, i.e. the Design safety drivers are satisfied).

Safety requirements at design level (SRD) are to be placed on the elements of the Solution functional System that are changed or affected by the change (through change in behaviour or through new interactions introduced).

The derived SRDs are to be consistent with the set of requirements produced by the Solution team in charge of SPR-INTEROP/OSED Part I (Section 4) and completeness and correctness of the full set of SRDs with regards to the satisfaction of the SRSs is to be shown.

5.1 Overview of activities performed

This section addresses the following activities:

- Introduction of the design model (initial or refined) of the Solution functional system – section 5.2
- Derivation of Safety Requirements (functionality & performance) at Design level (SRD) in normal and abnormal conditions of operation from the SRS (functionality and performance) of sections 4.2 and 4.3, and supported by the analysis of the initial or refined design model - section 5.3
- Assessment of the adequacy of the design (initial or refined) in the case of internal failures and mitigation of the Solution service hazards (identified at section 4.4.1) through derivation from SRS (integrity & reliability) of Safety Requirements (functionality & performance) and Safety Requirements (integrity & reliability) at Design level (SRD)- section 5.4
- Realism of the refined safe design (i.e. achievability and “testability” of the SRD) - section 5.5
- Safety process assurance at the initial or refined design level – section 5.6

5.2 Design model of the Solution Functional System

This sections contains the Design Model of the Solution functional system, which is a high-level architectural representation of the Solution system design

5.2.1 Description of the Design Model

5.2.1.1 [NOV-5]Elaborate Runway Condition Report

RCAMS maintains Current RWYCC, current runway condition and Predicted RWYCC, predicted runway condition, Airport Operator's awareness. Runway condition information is instantaneously disseminated and available to any stakeholder local to the airport who is connected directly to the RCAMS system (e.g. Tower Controllers, APOC, etc.) ore use ATIS.

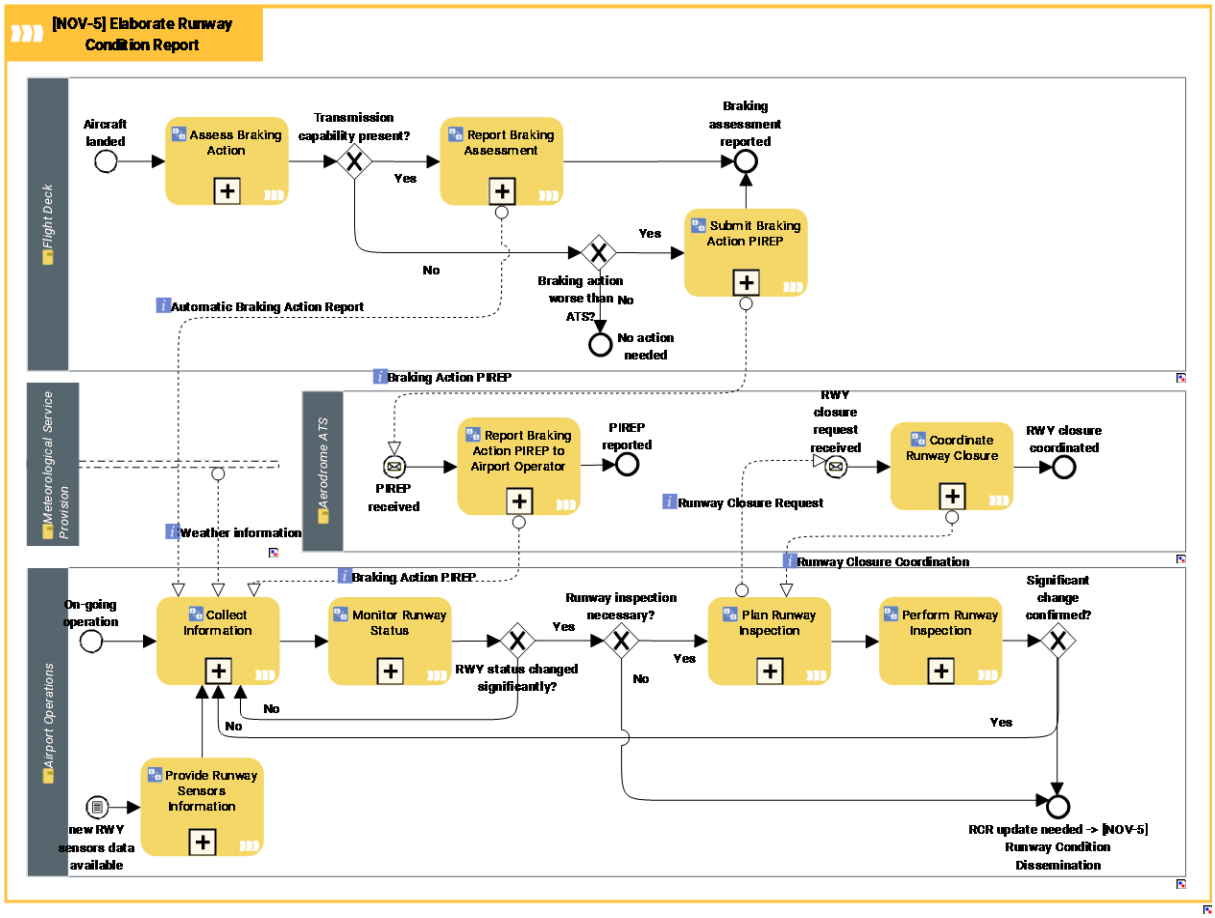


Figure 1 [NOV-5]Elaborate Runway Condition Report

5.2.1.2 [NOV-5]Decontamination Execution

After maintenance actions are completed by the Winter Services Team, AO goes back to runway monitoring.

EUROPEAN PARTNERSHIP
Co-funded by the European Union

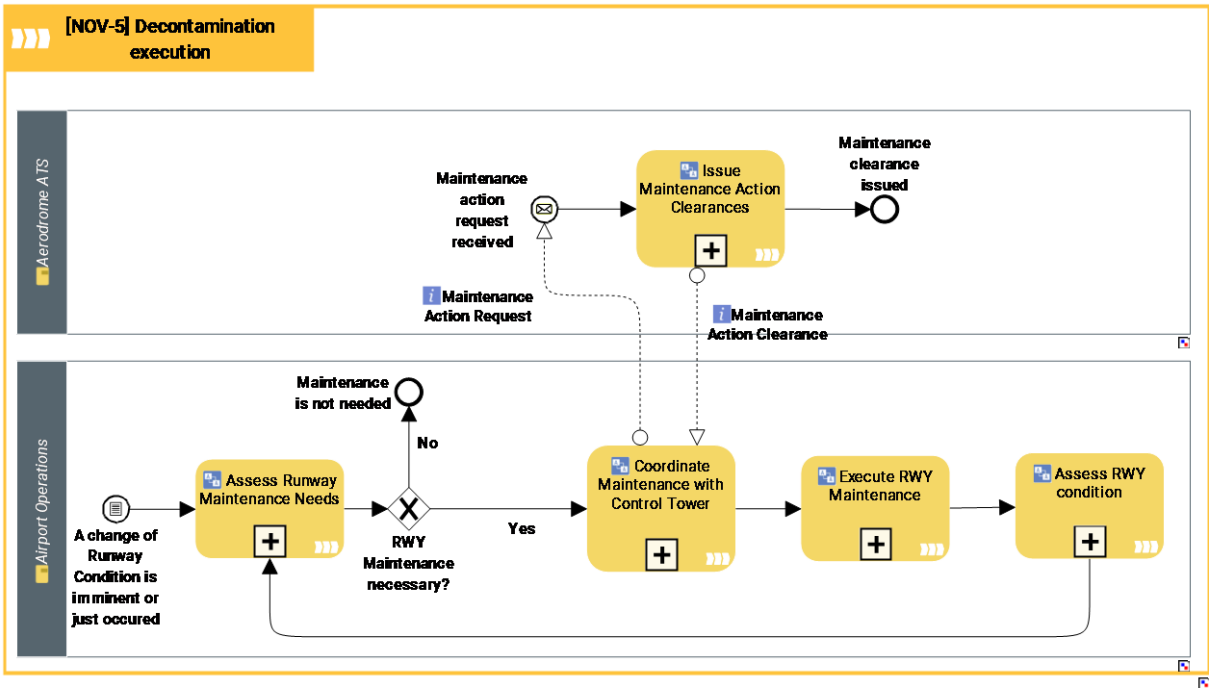


Figure 2 [NOV-5] Decontamination Execution

5.2.2 Task Analysis

Non required, the solution seeks an automated model where Human Resources tasks are not required (besides RCR validation and confirmation by the AO)

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

The purpose of this section is to present the Safety Requirements at Design level (SRD) derived for Normal and Abnormal conditions of operation following related SAF-GUI in STELLAR.

The derivation of Safety requirements at design level - SRD for Normal and Abnormal conditions of operation is mainly driven by the SRS (functionality and performance) for Normal and Abnormal conditions of operation from sections 4.2 and 4.3.

Meanwhile additional SRD might be identified (and need to be documented here) from the static view and dynamic view analysis of the system behaviour in normal and abnormal operational conditions that needs to be conducted in order to show completeness/correctness of the Safety Requirements (Functionality and Performance)

5.3.1 Safety Requirements at Design level (SRD) – Normal and Abnormal conditions

In this section it is provided the consolidated list of Safety Requirements at Design level (SRDs) (functionality and performance) for Normal and Abnormal conditions of operations derived by

EUROPEAN PARTNERSHIP
Co-funded by the European Union

mapping the Safety Requirements at Service level (SRSs) for Normal and Abnormal conditions of operation documented in section 4.2 and 4.3 onto the related elements of the Design Model.

The detail of the derivation process is included in Appendix C.

Safety Requirement ID [Design Model Element]	Safety Requirement (functionality & performance)	Derived from SRS (ID)

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

5.3.2 Additional SRD from Static analysis of the functional system behaviour

Non Applicable (Appendix C.2.)

5.3.3 Additional SRD from Dynamic analysis of the functional system behaviour

Non Applicable (Appendix C.3.)

5.3.4 Effects on Safety Nets

Non Applicable (Appendix C.3.)

5.4 Safety Requirements at design level addressing Internal Functional System Failures

The purpose of this section is to present the Safety Requirements at Design level (SRD) addressing internal system failures derived following the SAM-PSSA [2] and related SAF-GUI in STELLAR.

Safety requirements at design level - SRD are derived from the SRS associated to failure conditions which have been identified in section 4.4.

The following Safety Requirements at Design Level (SRD) are to be included (derived from a top-down causal analysis of the Service Hazards identified in section 4.4.1, from a bottom-up failure modes and effects analysis encompassing the analysis of common causes and , if applicable, from the SRS (functionality & Performance) derived during the Service Hazard assessment section 4.4.1):

- SRD (functionality and performance): derived to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the service 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 and performance) derived to provide mitigation against service hazard effects (protective mitigation, from the SRS (functionality & performance) derived during the Service Hazard assessment.

5.4.1 Design analysis addressing internal functional system failures

As identified before, the top down analysis revealed the following process:

Co-funded by the European Union

- Identification of a complete list of Solution functional system failures that could cause each service hazard. The only service identified is the "Provision of runway condition report", therefore the only functional system failure that could cause a service hazard is the failure of this service. For more detail please access Section 4.4 and Appendix B.
- Identification of the required Mitigation means preventing causes to occur or preventing their effect to propagate up to the service hazard. The means identified are returning to old operating method processing the RCR through manual or R/T means without the Current and Predicted RWYCC.
- Demonstration of 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. This is validated by following validation objectives:
    a. OBJ-02-W2-25.1-V3-VALP-0013
    b. OBJ-02-W2-25.1-V3-VALP-0013a
    c. OBJ-02-W2-25.1-V3-VALP-0013b
    d. OBJ-02-W2-25.1-V3-VALP-0013c
    e. OBJ-02-W2-25.1-V3-VALP-0013d
    f. OBJ-02-W2-25.1-V3-VALP-0013e
- Determine potential common cause failures and ensure their mitigation through dedicated SRD or design choice as it is included in Appendix D.

5.4.2 Safety Requirements at design level addressing internal system failures

The following Table 10 provides consolidated list of Safety Requirements at Design level (functionality and performance) addressing internal system failures with the SRD (functionality and performance) derived from the SRS documented in section 4.4 to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the service hazard, with due consideration for mitigating the common cause failures.

No SRD (integrity/reliability) were required taking into account the Additional SRD (functionality & performance elaborated to cover the whole SRS documented in section 4.4.

To access more detail go to Appendix D

Safety Requirement ID	Safety Requirement at Design level (SRD) (functionality & performance)	Derived from SRS (ID) or Common Cause failure
SRD 004	Implementation of monitoring and alerting of the RCAMS functioning, enabling reverting to manual AO procedures for RCR creation and dissemination during RCAMS system failures	**SRS 008**

Table 7. Additional SRD (functionality & performance) to mitigate the service hazards

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Safety Requirement ID	Safety Requirement at Design level (SRD) (Integrity/Reliability)	Derived from SRS (ID) or Common Cause failure
SRD 001	RCAMS system shall validate the RCR in accordance with the available information and assure the correct information is available	**SRS 001; SRS-002**
SRD 002	The RCAMS system shall assure the correct computation, visualization and distribution to all the involved Stakeholders of the Current and Predicted RWYCC	**SRS 003; SRS 004; SRS 005**
SRD 003	The RCAMS system shall have the possibility to seamlessly provide degraded mode, until RCAMS system parts recover from the failure.	**SRS 006; SRS 007**

Table 8. SRD (integrity/reliability) to mitigate the service hazards

5.5 Realism of the safe design

The RCAMS system, although being a new development, is based on set of commercially available and proven components, both in terms of infrastructure (runway sensors, AWOS, Linux/Windows servers) and in terms of software (Machine Learning models, containerization) as well as in terms of data storage and transmission. Automated prediction of Current and Predicted RWYCC can be successfully implemented even on a small scale and is less complex and workload intensive, that manual inspection of the runway.

As stated above, it is considered that the SRDs are highly achievable and will not require additional development neither expenses.

5.6 Process assurance for a Safe Design

Assurance is achieved as explained in the previous section 5.5

EUROPEAN PARTNERSHIP

Co-funded by the European Union

6 Demonstration of Service specification achievability

Within the HAZID and Safety sessions held 23/03/2022 and further re-visited the 14/04/2022, where a hazard identification has been conducted, involving operational experts which were relevant for the use of services provided by the solution. That allowed to understand the potential safety implication of the solution as per the paragraphs below.

The Safety driver will be the conformance of Runway condition estimation to the quality and reliability expectations of stakeholders. The safety demonstration strategy is:

1. Prove conformance quality and reliability requirements for RWYCC -> include a safety validation objective in VALP Part I in view of demonstrating the conformance to these data quality requirements within the VAL EXE

Identifier	OBJ-02-W2-25.1-V3-VALP-0013b
Objective	Runway condition code estimation, as well as, contaminant type, depth and coverage assessment shall be accurate and reliable.
Title	Trustworthy assessment of runway condition
Category	Safety
Key environment conditions	
V Phase	V3

2. Argue that in case of degraded Runway Condition Report received, a mitigation will be implemented (safety requirement) in terms of a RCAMS real-time monitoring tool as part of the validation platform. When RWYCC information lost or not reliable, the system will detect a potential anomaly and AO would revert to using manual inspection and input to ATIS – performance degraded, but safety ensured.

3. Perform a Safety assessment workshop with operational experts when OSED starts to mature but not too late for allowing potential safety requirements to be checked in the VAL EXE (if feasible) and included in the final OSED. Taking into account synergies with 25.2, either experts from that solution might be invited or a joint safety workshop might be organized.

7 Acronyms and Terminology

Acronym	Definition
AIM	Accident-Incident Model
ANS	Air Navigational Services
ANSP	Air Navigation Service Provider
AOC	Airline Operations and Control Centre
AOP	Airport Operations Plan
APOC	Airport Operations Centre
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
BIM	Benefit and Impact Mechanism
BIZ	Business Jet
CFME	Continuous Friction Measuring Equipment: a device designed to produce continuous measurement of runway friction values
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations
CR	Change Request
DO	Duty Officer
EASA	European Aviation Safety Agency
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
E-OCVM	European Operational Concept Validation Methodology
ER	En-Route
FC	Flight Crew
FHA	Functional Hazard Analysis

EUROPEAN PARTNERSHIP

Co-funded by the European Union

FM	Functional Model
GND	Ground
GRF	Global Reporting Format
HMI	Human Machine Interface
HPA	Human Performance Assessment
HPAP	Human Performance Assessment Plan
HTA	Hierarchical Task Analysis
ICAO	International Civil Aviation Organization
IM	Impact Modification
INTEROP	Interoperability Requirements
KPA	Key Performance Area
LW	Lech Wałęsa
OBACS	On-board Braking Action Computation System
OSED	Operational Service and Environment Definition
PIREP	PIlot REPort (Pilot air report)
PSSA	Preliminary System Safety Assessment
RCAM	Runway Condition Assessment Matrix
RCAMS	Runway Condition Assessment Matrix System
RCR	Runway Condition Report
RE	Runway Excursion
ROAAS	Runway Overrun Awareness and Alerting System
ROT	Runway Occupancy Time
RTO	Rejected Take-Off
RTS	Real Time Simulation
RWY	Runway
RWYCC	Runway Condition Code
SAA	Safety Assurance Activities

EUROPEAN PARTNERSHIP

Co-funded by the European Union

SAC	SAfety Criteria
SAFE	Safer Airports and Flights for Europe (SESAR Project PJ.03B)
SAM	Safety Assessment Methodology
SAP	Safety Assessment Plan
SAR	Safety Assessment Report
SC	Severity Class
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SNOWTAM	Snow-related NOTAM
SO	Safety Objective
SPR	Safety and Performance Requirements
SRD	Safety Requirements at Design level
SRM	Safety Reference Material
SRS	Safety Requirement as Service level
SSA	System Safety Assessment
TALPA	Take-off And Landing Performance Assessment
TMA	Terminal Manoeuvring Area
TO	Take-off
TOMS	Take-off Monitoring System
TS	Technical Specification
VALP	Validation Plan
VALR	Validation Report
VALS	Validation Strategy

Table 9: Acronyms and terminology

Co-funded by the European Union

8 References

Safety

[1] (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 V2.1 (https://www.eurocontrol.int/tool/safety-assessment-methodology)

[3] SESAR 2020 Safety Policy

[4] SESAR, Safety Reference Material, Edition 4.1, December 2018

[5] SESAR, Guidance to Apply the SESAR Safety Reference Material, Edition 3.1, December 2018

[6] SESAR Safety Assessment Report (SAR) Template

[7] SESAR P16.06.01, Task T16.06.01-004, Process for the Safety Review of SESAR Safety Documentation, Edition 00.01.02, 10th February 2012

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

[9] SESAR, Resilience Engineering Guidance, May 2016

PJ.02 documents

[10] SESAR Solution PJ.02-W2-25.1 SPR-INTEROP/OSED for V3 (final) part I, Ed. 03.01, 10 February 2023

[11] SESAR Solution PJ.02-W2-25 V3 Validation Plan part I

[12] SESAR Solution PJ.02-W2-25 V3 Validation Plan – part IV – Human Performance Assessment Plan

Other documents

[13] Runway Safety – Accident Analysis Report 2010-2014 – 1st edition – IATA – 2015

[14] Procedures for Air Navigation Services — Aerodromes (PANS-Aerodromes) – 2nd edition – ICAO Doc 9981 – 2016.

[15] Annex 14 to the Convention on International Civil Aviation (Aerodromes), Volume I – Aerodrome Design and Operations, 8th edition – ICAO – July 2018.

[16] Annex 15 to the Convention on International Civil Aviation (Aeronautical Information Services), 16th edition – ICAO – 2018.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix A Defining the Service Safety Specification for Normal and Abnormal conditions of operation

This appendix presents the definition of the SRS (functionality and performance) in order to set the Service Safety Specification under normal (i.e. those conditions that are expected to occur on a day-to-day basis) and abnormal conditions of operation.

The set of SRS has to be complete for the scope of the change brought in by the Solution. The consolidated list is provided in Sections 4.2 (normal conditions of operation) and 4.3 (abnormal conditions of operation).

A.1 SRS obtained from other operational solutions or standards

A.2 EATMA Process models or alternative description

With respect to the changes brought by Solution PJ02-W2-25.1, two use cases from OSED part I have been retained for SRS derivation:

- Use Case PJ.02-W2-25-1: “Elaborate Runway Condition Report”
- Use Case PJ.02-W2-25-2: “Runway Condition dissemination”

Runway decontamination is considered as not modified in its process, however, once the solution is implemented, it will be triggered based on RCAMS information. The model of the use case PJ.02-W2-25-2-5 “Decontamination execution” is thus not used for SRS derivation, nevertheless the trigger of a runway decontamination, now based on RCAMS information, has to be considered in the consequences resulting from Elaborate runway condition steps.

A.2.1 Use Case PJ.02-W2-25-1: “Elaborate Runway Condition Report”

This view reproduces the Use Case PJ.02-W2-25-1 NOV-5 diagram:

Co-funded by the European Union

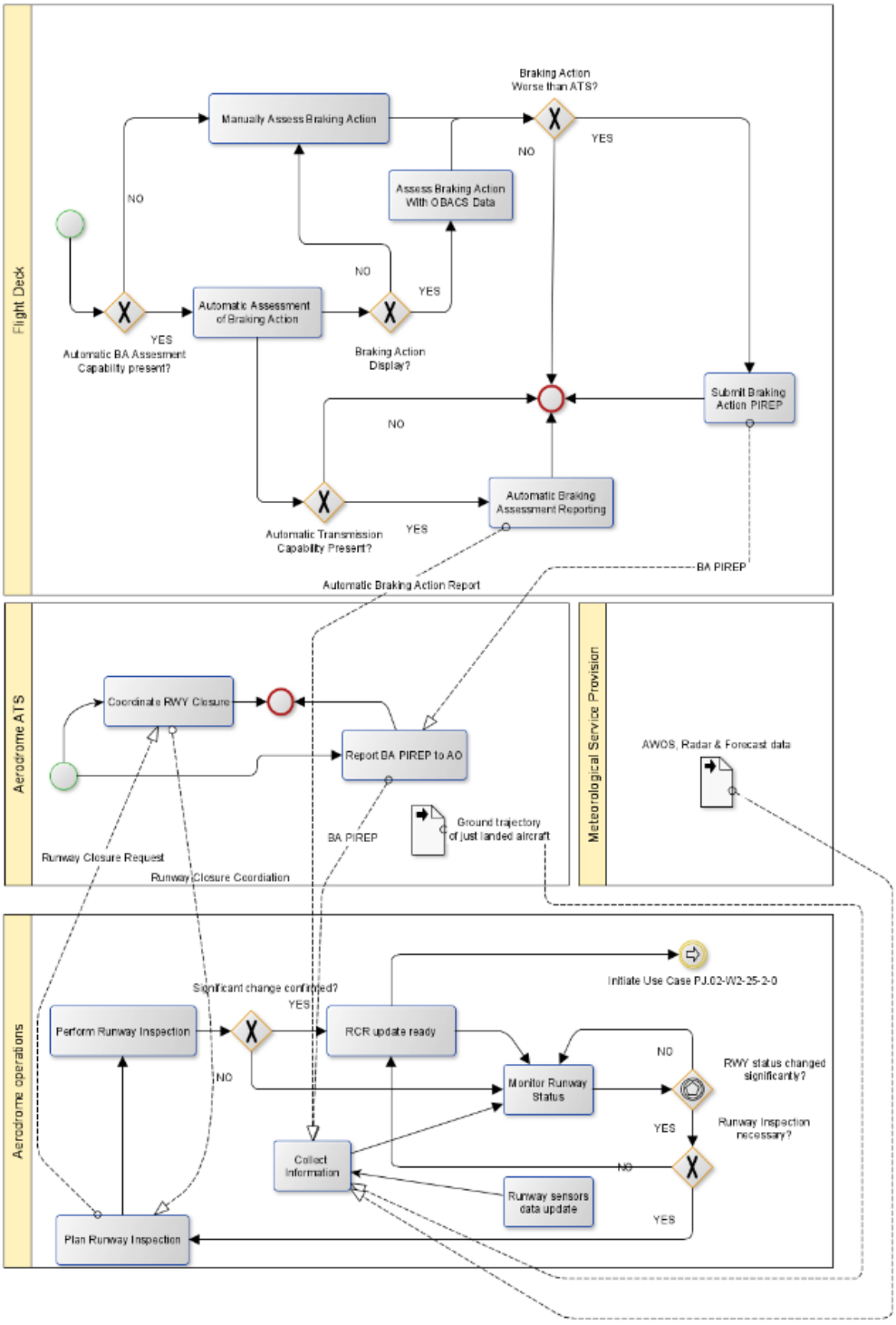


Figure 3 [NOV5] Elaborate runway condition

The main differences between new and previous method on this use case are:

Activity	Impact	Change

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Assess Current Runway Surface Condition	Update	The current runway condition assessment, still using ICAO Global Reporting Format based on RCAM (runway condition assessment matrix) and manual measures during runway inspections, is performed by integration of additional inputs: from embedded runway sensors, MET data, surveillance data, aircraft report on braking action, etc. This allows a continuous and more accurate assessment of runway surface condition and limit the runway inspection needs for seamless airport operations.
Assess Predicted Runway Surface Condition	Introduce	
Automatically Compute Braking Action	Introduce	
Collect Information	Introduce	
Execute Runway Decontamination	Update	Runway decontamination activities are now supported by RCAMS information provided to AO.
Manually Assess Braking Action	Update	No change in Braking Action assessment by Flight Crew, which may be reported in adverse weather situation when braking action experienced was worse than expected. Braking action reported in PIREP will now be introduced in RCAMS to enter runway surface condition assessment process. OBACS will assist the flight crew in PIREP generation in cases when automatic braking action downlink was not feasible.
Monitor and Update Runway Status	Introduce	
Perform Runway Inspection	Update	Runway inspection teams uses RCAMS as support tool to enter their measures and observations.
Plan Runway Decontamination	Update	Decontamination need can be identified by Airport Duty Officer based on information provided by RCAMS.
Plan Runway Inspection	Update	Runway inspection need can be identified using RCAMS. Runway inspection measures (contaminant type depth coverage on each runway thirds) are used as RCAMS inputs for runway condition assessment.
Report Braking Action PIREP to Airport Operator	Update	Braking Action reported by Flight Crew is used as RCAMS input for runway condition assessment (direct input from Tower Controller who received the information).

A.2.2 Use Case PJ.02-W2-25-2: “Runway Condition dissemination”

This view reproduces the Use Case PJ.02-W2-25-2 NOV-5 diagram:

Co-funded by the European Union

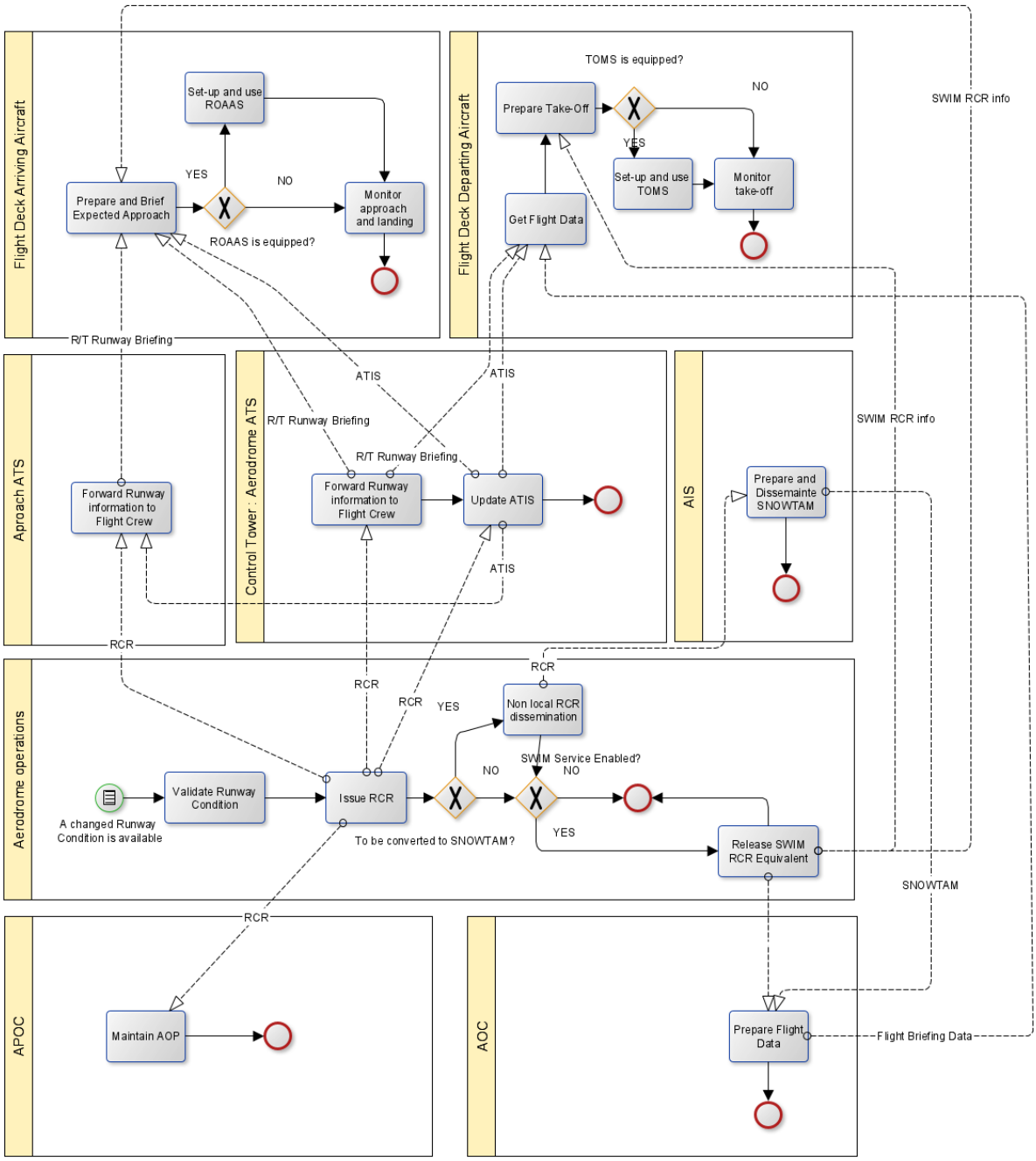


Figure 4 [NOV5] Runway Condition dissemination

The main differences between new and previous method on this use case are:

Activity	Impact	Change
Disseminate ATIS	Update	In addition to ICAO Global Reporting Format information about runway condition, addition of prediction to give flight crews element for them to prepare their take-off and landing performance assessment.

EUROPEAN PARTNERSHIP
Co-funded by the European Union

Provide Runway Condition for any rwy in the area	Update	Addition of prediction about runway condition for better landing performance assessment by Flight Crews.
Disseminate Runway Status	Update	Solution will complement RCR with prediction on runway condition. Current and predicted Runway condition dissemination could also be supported by a SWIM service.

A.3 Derivation of SRS for Normal conditions of operation

From the models presented and the modifications between pre/post methods identified, this section recalls the nominal flow of activities for each use case and identifies a set of requirements for activities for which the change may impact the efficiency of a safety barrier or the occurrence of a safety precursor.

As a reminder, from VALP part II, the SAC selected for PJ02-W2-25.1 is:

The rate of approaches initiated to runways with a more degraded runway condition than the one used for landing calculation shall be reduced.

It is associated to AIM model for Runway Excursions and to the following barriers:

RWY EXC Barrier	Title	Comment
REB1 (SC-2a)	Crew/ AC runway deceleration / stopping action	Pilot corrects/adapts runway deceleration and stopping parameters considering the current weather and runway conditions to ensure final landing
REB2 (SC-2b)	Management of short final and flare	Pilot corrects/adapts short final and flare parameters considering the current weather and runway conditions to ensure a stable touchdown
REB5 (SC-4)	Management of runway conditions wrt weather	ATC/pilot to check/ensure weather conditions are suitable for landing

A.3.1 Use Case PJ.02-W2-25-1: “Elaborate Runway Condition Report”

Nominal flow of activities (based on OSED part I), for use case PJ.02-W2-25-1:

[1] Runway condition is automatically assessed. Data is provided:

- continuously by Surface Condition sensors or (optionally) by visual inspection from AO, MET & (optionally) surveillance data

- by flight crew of a just landed aircraft reporting Braking Action, the Tower Controller reports to the AO who then enters the Braking Action in the RCAMS; or controllers may have means to input reported Braking Action directly in RCAMS

- or automatically: computed braking action provided by equipped aircraft

Co-funded by the European Union

[2] On any ground data or MET update (METEO-03c, METEO-04c) or new data given by Weather based RWYCC prediction model, the RCAMS re-evaluates RWYCC

[3] New computed Runway Condition is compared to currently published RCR. Alerts are raised in case of differences.

[4] Airport Operator can decide on runway inspection. Runway closure is then coordinated with Tower. Runway inspection result is used in this case to validate RCAMS alerts.

Service	EATMA Use Case- Activity or Flow	Derived SRS
E.g. UC1: Mission Trajectory Management in Short Term Planning Phase		
Assess Current Runway Surface Condition	Runway condition is automatically assessed. Data is provided continuously by Surface Condition sensors	**SRS 001 :** The Airport Operator shall be provided with the Computed Current RWYCC and the Computed Predicted RWYCC values with the required certainty level Airport Operator within its Airport Duty Officer role shall perform the validation of Computed Current Runway Condition in a timely manner upon any significant change
	Runway condition is automatically assessed. Data is provided by flight crew of a just landed aircraft reporting Braking Action	**:** All relevant ATS services shall have means to know the most up to date Current Runway Surface Condition of any runway the RCAMS system is operational and to inform about any observed discrepancies (PIREP).

Table 10: Derivation of SRS for Normal Operations driven by EATMA Process models

A.3.2 Use Case PJ.02-W2-25-2: "Runway Condition Dissemination"

Nominal flow of activities (based on OSED part I), for use case PJ.02-W2-25-2:

[1] Airport Operator verifies contents of RCR and supplements it with any additional information
[2] Airport Operator validates the RCR content and activates the RCR dissemination.

[3] RCAMS disseminates the RCR locally via automatic means, to APOC, Tower Runway Controller, Tower Supervisor.

In addition, if RCR contains information about snow, slush, standing water, ice or frost it is disseminated to AIS for subsequent SNOWTAM publication.

In parallel the RCR is published via SWIM service available via subscriptions to Flight Crew, Non local ATS (e.g. Executive Approach Controller), AOC.

[4] In case of change, especially sudden or unexpected, new runway condition is highlighted to strengthen Air Traffic Controllers awareness; if necessary, the Airport Operator may contact directly the Tower Runway Controller or the Tower Supervision Controller.

[5] Tower Supervisor Controller broadcasts the information on runway condition via ATIS, and informs the Tower Runway Controller of the new runway condition.

Co-funded by the European Union

[6] If necessary, the Tower Runway Controller relays the information of the new runway condition to the Executive Approach Controller.

[7] Flight crew retrieves runway condition information and use it to monitor take-off or landing, using ROAAS and TOMS when available.

The following Table 20 provides the derivation of SRS in Normal Operations for use case PJ.02-W2-25-2:

ATS Operational Service	EATMA Use Case-Activity or Flow	Derived SRS	Related SAC# (AIM Barrier or Precursor)
Issuance of RCR	Airport Operator validates the RCR content	**SRS 002;**	
	RCAMS disseminates the RCR locally via automatic means, to APOC, Tower Runway Controller, Tower Supervisor.	**SRS 003:** The Airport Operator shall disseminate RCR in timely manner via ATIS or R/T means of communications.	
Disseminate ATIS	Flight crew retrieves runway condition information *and/or:* Tower Supervisor Controller broadcasts the information on runway condition via ATIS.	**SRS 004:** All relevant ATS services shall have means to know the most up to date Current Runway Surface Condition of any runway the RCAMS system is operational and to inform about any observed discrepancies (PIREP). **SRS 005:** Approach/Tower Runway ATCO shall disseminate the Current Runway Condition to the Flight Crew upon each change in a timely manner and/or on request.	

A.4 Derivation of SRS for Abnormal conditions of operation

A.4.1 Identification of Abnormal Conditions

The following abnormal conditions were identified as being part of the solution success approach

- Maintenance of RCAMS or its parts
- RCAMS input data issue (same Use Case PJ.02-W2-25-3
- Failure of RCAMS local dissemination

Co-funded by the European Union

A.4.2 Risk analysis of Abnormal Conditions and derivation of SRS (Functionality&Performance)

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SRS xxx]
	Runway sensor under maintenance	May impact the measured runway friction	**SRS 010**: If a measure means is under maintenance, it shall not prevent continuous reassessment of runway condition based on other data (resilience to missing data)
	A/C automatic report not available	May prevent report of a degraded braking action	**SRS 011**: in the case of a degraded braking action detected by one A/C, if an automatic report is not available, flight crew PIREP shall be transmitted to AO (via ATS)
	RCAMS input data issue (see Use Case PJ.02-W2-25-3)	May impact RCR reliability	**SRS 012:** RCAMS shall use multiple independent data sources for runway condition elaboration
			SRS 013: If RCAMS detects input data issue (erroneous or missing), it shall be indicated to Duty Officer
			SRS 014: In case of input data issue indicated, it is the responsibility of the Duty Officer to use or not this data
ABN 4	Failure of RCAMS local dissemination	A degraded condition may not be propagated when needed	**SRS 015:** in case of RCAMS dissemination failure, other means shall be available (eg R/T)
ABN 5	Arriving aircraft changing runway after RCR reception	Flight crew of arriving may not be aware of degraded condition on alternate runway	**SRS 016:** As for ATIS report, all runways conditions shall be made available to arriving A/C
ABN 6	Intensity of meteorological phenomena (usually precipitation) leads to accumulation rates comparable to system update rate	RCR may not be up to date, and arriving/departing A/C may not be aware of a rapidly degrading condition	**SRS 017:** in case of intense phenomena, controller shall be able to advise arriving A/C without delay as done prior to RCAMS

ABN 7	Late runway inspection results	RCR may not be up to date, and arriving/departing A/C may not be aware of a rapidly degrading condition	**SRS 018:** if runway inspection is decided by AO, a conservative runway condition shall be published prior to runway inspection results

Table 11: Risk analysis for Abnormal conditions of operation

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix B Risk assessment of the change at service level

B.1 HAZID workshop

The HAZID workshop was held on the 23/03/2022 and further re-visited the 14/04/2022, where a hazard identification has been conducted, involving operational experts which were relevant for the use of services provided by the solution. That allowed to understand the potential safety implication of the solution as per the paragraphs below.

The AIM applicable to the Solution is not complete and as a result it does not contain quantitative information. Moreover, neither Transition CONOPS nor Programme level Validation Targets do not express quantitative safety targets for Solution PJ.03b-06. This situation is a result of very limited documentary materials (occurrences) regarding RE resulted solely from landing on weather affected RWY. Especially in relation to weather impact on RWY suitability during approach and landing.

Generally REs during landing occur when one of the following situation appear:

- Unstable approach ending with long touchdown,
- Unstable approach ending with touchdown with exceeded speed,
- Inefficient braking action during landing roll resulting from various reasons.
- Additionally can occur in situation of aircraft approaching on unsuitable RWY e.g. in result of FC/ATCO error or weather impact on RWY condition.

All situations are partially covered by available AIM model but without providing quantitative information.

RCAMS is not intended to influence somehow on the problem of detecting or stabilisation of unstable approach but is aiming at reduction of its consequences (severity).

Main role of the RCAMS is to prevent touchdown if available RWY distance is not sufficient to safely stop the aircraft in given conditions. Such situation can occur if aircraft is directed on unsuitable (due to weather) RWY (last case) or if aircraft touchdown long or with exceeded horizontal speed (two first cases). Therefore it should be expected that RCAMS mainly by providing resilient, and actual RWYCC to the FC and/or ATCO will reduce rate of initiating of approach to weather affected (or expected to be affected in short time period) RWY in situation deceleration distance necessary to stop aircraft in given RWY conditions would be longer than available RWY distance (without FC being aware of it). (Other RCAMS subsystems are not covered by this consideration: RCAMS, TOMS, etc)

Second role of RCAMS is to prevent continuation of landing roll if current deceleration path is not sufficient to ensure safe stop of the aircraft on available RWY distance in given RWY conditions and is sufficient to safely abort landing and start (e.g. in case of failure to achieve maximum braking). Therefore it can be expected that RCAMS by providing relevant information/alert to the FC will reduce the rate of RE resulted from failure to achieve necessary braking after touchdown / during landing roll.

Take-off is not covered by the consideration as well.

The Solution provides data to involved stakeholders (Current and Predicted RWYCC) which contributes to enhancing the management of runway condition and A/C configuration during landing approach. As part of the standard operational process there is a need for the calculated RWYCC to meet certain data quality requirements laid down by ICAO Guidance On The Issuance Of Snowtam

- The dissemination of RCR with more degraded RWYCC than actual (with no safety impact)

- The failure to disseminate correct RWYCC, resulting in negative impact on the identified Safety Criteria. That involves a potential safety impact.

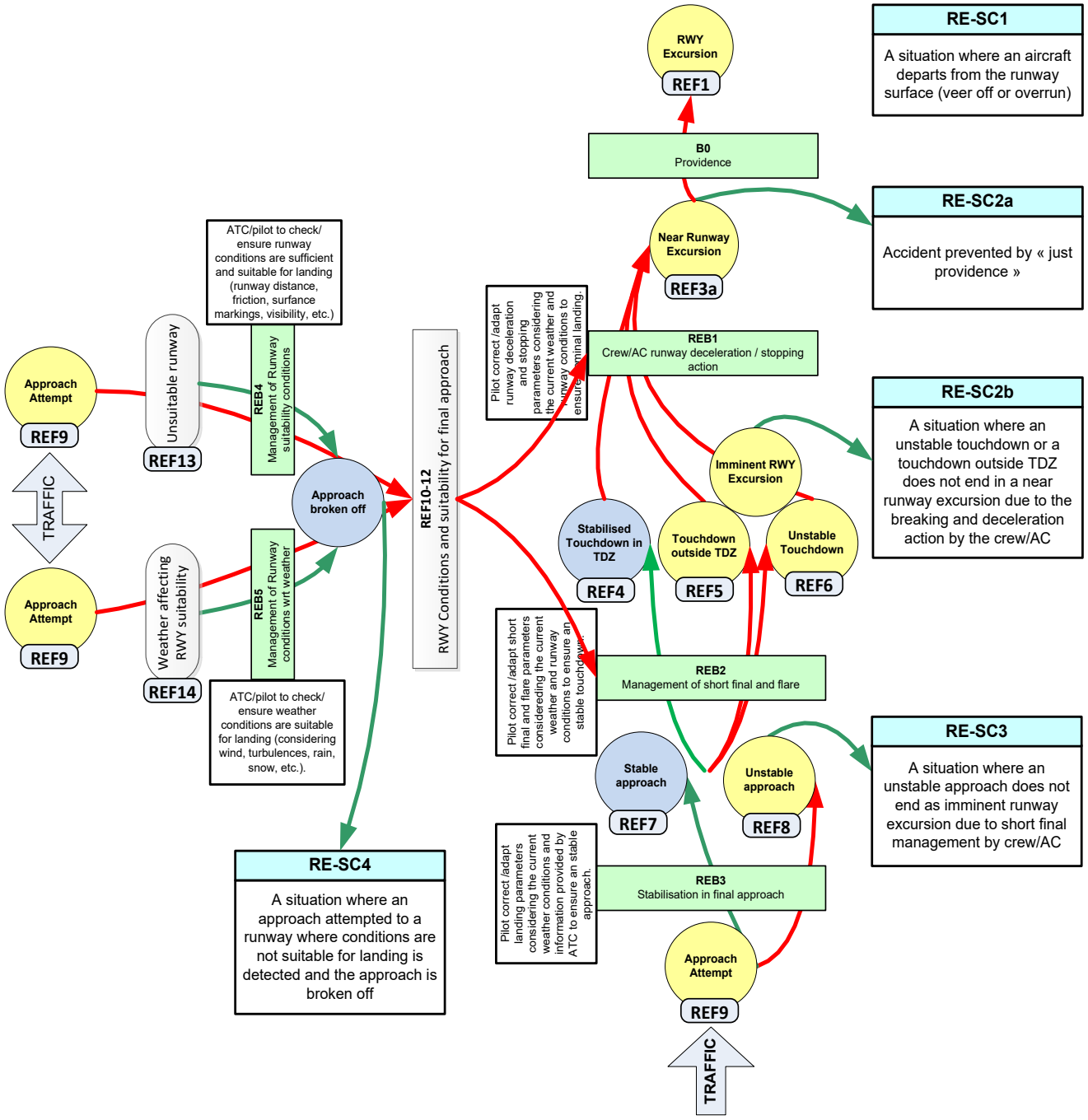
The identified Safety Criteria for PJ02-W2 Solution 25.1 is:

PJ02-W2 Solution 25.1 Safety Criteria	Related AIM barriers
The rate of approaches to a runway with a more degraded runway condition that the one use for landing calculations shall be reduced	REB1; REB2; REB5

REB1 (SC-2a)	Crew / AC runway deceleration / stopping action	Pilot corrects/adapts runway deceleration and stopping parameters considering the current weather and runway conditions to ensure final landing
REB2 (SC-2b)	Management of short final and flare	Pilot corrects/adapts short final and flare parameters considering the current weather and runway conditions to ensure a stable touchdown
REB5 (SC-4)	Management of runway condition when wet	ATC/pilot to check/ensure weather conditions are suitable for landing

EUROPEAN PARTNERSHIP

Co-funded by the European Union



Severity Class Scheme for Runway Excursion (related to landing only)

AIM RWY EXC BARRIER MODEL (Landing) v0.3

Figure 5 Severity Class Scheme for Runway Excursion

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Service failure mode	Example of causes & preventive mitigations	Operational Effect (through service provision to ATS or aircraft)	Mitigations protecting against propagation of effects	Service hazard & Severity
Hz 1: Undue degradation of runway condition at AO level	Technical causes (sensors, communication): erroneous BA reported, undetected erroneous runway sensor, (or combined erroneous runway sensor with a delay in A/C transmission) S/W in RCAMS: (integration and telecommunications failures, software malfunctions) Unexpected conditions: e.g. accumulation of A/C deicing/anti-icing liquid on the runway Note: runway maintenance (anti icing liquid, salt) taken into account in the RCAMS model	Undue runway inspection A/C rerouting to another suitable airfield or holding pattern until weight decreased enough to match runway state performance for landing A/C going around	Duty officer validation of runway condition before any publication	No safety effect
Hz 2: Undue runway closure	See above	Limited in time awaiting inspection results A/C rerouting to another suitable airfield or holding pattern until runway is cleared or going-around	Time-limited as inspection will quickly enable re-opening Note: RCAMS benefit: a better runway information allow for less runway closures	No safety effect

Use Case / Service failure mode	Example of causes & preventive mitigations	Operational Effect (through service provision to ATS or aircraft)	Mitigations protecting against propagation of effects	Service hazard & Severity
Hz 3: Non detected runway degradation	Unexpected and severe change of weather condition not included in MET sources Partial contamination of the runway, beyond sensors coverage	RWY friction lower than reported (runway condition higher than reality) No runway inspection is requested whereas it is needed	It is mitigated prior to emission A conservative value is disseminated Duty officer validation of runway condition before any publication ATS may be aware of other PIREP and adapt ATIS It is mitigated as soon as another source detects the degradation, as the worst condition is retained	SC-3
Hz 4: Dissemination of erroneous (better than measured) value of runway condition (but not NIL friction, ie degraded but not requiring immediate runway closure)	RCR validation failure or late detection of an erroneous RCR Undetected need for a runway inspection Or causes above, but not detected in time prior to dissemination	RWY friction experienced by A/C is lower than expected (runway condition higher than reality) May lead to late go-around for arriving A/C At worst it leads to a runway excursion	AC adaptation to degraded braking (manually or via ROAAS) -> this FC will issue a PIREP or warn by R/T ATS may be aware of another PIREP and warn FC in final	SC-2B

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Use Case / Service failure mode	Example of causes & preventive mitigations	Operational Effect (through service provision to ATS or aircraft)	Mitigations protecting against propagation of effects	Service hazard & Severity
Hz 5: Undetected need for runway closure	Complete failure of elaboration and dissemination of the need to close the runway (including reference system detection means (prior to the solution))	AC may land on an unsuitable runway At worst potential runway excursion	Late adaptation to degraded braking Runway inspection will be preventively launched to check runway state if meteorological conditions are not consistent with RCC.	SC-2A

Table 12. Full HAZID working table

EUROPEAN PARTNERSHIP

Co-funded by the European Union

B.2 HAZID participation list

Name/Beneficiary	Position/Title
Stephane Picaut / DASSAULT AVIATION	VALP Task Leader
Radoslaw Sulek / UNIWARSAW	SAR Task Leader
Janek Malawko / UNIWARSAW	Solution Contributor
Catherine Wisler / AIRBUS	Solution Contributor

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix C Designing the Solution functional system for Normal and Abnormal conditions of operation

C.1 Deriving SRD from the SRS

SRS for Normal and Abnormal Operation (ID & content)	Safety Requirement at Design level[1] (SRD) or Assumption	Maps onto
SRS 001:	SRD 001:	
SRS 002:	SRD 001:	
SRS 003: The Airport Operator shall disseminate RCR in timely manner via ATIS or R/T means of communications.		Integration with ATIS
SRS 004: All relevant ATS services shall have means to know the most up to date Current Runway Surface Condition of any runway the RCAMS system is operational and to inform about any observed discrepancies (PIREP).		Integration with external systems of AU
SRS 005: Approach/Tower Runway ATCO shall disseminate the Current Runway Condition to the Flight Crew upon each change in a timely manner and/or on request		Integration with external systems of AU
SRS 006: Whenever RCAMS system or its part is down, a degraded mode is provided		

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

Co-funded by the European Union

SRS 007: Whenever RCAMS output is not received by ATIS, an alternative manual input is provided		External element a

Table 13: SRD derived by mapping SRS for normal and abnormal conditions of operation to Design Model Elements

C.2 Static analysis of the solution functional system behaviour

Non applicable

C.3 Dynamic analysis of the Solution functional system behaviour

Non applicable

EUROPEAN PARTNERSHIP

Co-funded by the European Union

Appendix D Designing the Solution functional system addressing internal functional system failures

This appendix presents the detailed risk evaluation and mitigation of the Service Hazards from section 4.4 performed at the level of the design of the solution functional system.

D.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 (SRS 008):

- ·SRD (functionality and performance) in order to provide adequate mitigations to reduce the likelihood that specific failures would propagate up to the service 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.

D.1.1 Top-down analysis of the design

Cause ID (in fault tree)	Cause	Detailed description	Mitigation/Safety Requirement
C01	RCAMS system sensors failure	Runway sensors, AWOS and radar are down and could not provide the service defined	Degraded mode is provided. An alternative manual input to ATIS is provided
C02	RCAMS system integration with ATIS failure	The ATIS system is not able to keep the communication process and the data could not be transmitted	Degraded mode is provided. An alternative manual input to ATIS is provided
C03	RCAMS Machine Learning model failure to calculate accurate RWYCC	The data is not reliable due to the failure of the Machine Learning model	Degraded mode is provided. An alternative manual input to ATIS is provided

Table 14. Example of table detailing one service hazard causes and associated preventive mitigations (SRD)

D.1.2 Bottom-up analysis of the design

Co-funded by the European Union

Functional system element	Failure mode	Effects	Mitigation/Safety Requirement	Service hazard
RCAMS system	RCAMS system functioning and /or integrations fail	RAMS system - ATIS exchange of information is either impossible or the data integrity could not be assured	OBJ-02-W2-25.1-V3-VALP-0013	

Table 15. Example of FMEA (Failure Modes and Effects Analysis) table

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

SRS (functionality& performance) for protective mitigation (ID & content)	Safety Requirement at Design level[2] (SRD) or Assumption	Maps onto
SRS 008: Provision of monitoring and alerting of the RCAMS functioning, reverting to manual AO procedures for RCR creation and dissemination	SRD 004:	RWYCC dissemination to Stakeholders
SRS 008: Provision of monitoring and alerting of the RCAMS functioning, reverting to manual AO procedures for RCR creation and dissemination	SRD 004:	RWYCC dissemination to Stakeholders

Table 16: SRD derived by mapping SRS (functionality & performance) for degraded conditions on to Design Model Elements

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

Appendix E Assumptions, Safety Issues & Limitations

E.1 Assumptions log

No Assumptions were required and therefore documented

E.2 Safety Issues log

No additional safety issues were risen during the meetings (besides the ones contained in the hazard identification in Appendix B), therefore there is no Safety Issues log.

E.3 Operational Limitations log

No operations limitations were raised during the meetings, therefore there is no Operational Limitations log.

EUROPEAN PARTNERSHIP

Co-funded by the European Union

-END OF DOCUMENT-

EUROPEAN PARTNERSHIP

Co-funded by the European Union

EUROPEAN PARTNERSHIP

Co-funded by the European Union