Safety Assessment Report (SAR) for Conflicting ATC Clearances

Document information	
Project title	Airport safety support tools for pilots, vehicle drivers and controllers
Project N°	06.07.01
Project Manager	DSNA
Deliverable Name	Safety Assessment Report (SAR) for Conflicting ATC Clearances
Deliverable ID	D29B
Edition	00.01.01
Template Version	03.00.00
Task contributors	
DLR, THALES, EUROCONTROL	

Abstract

This document contains the Specimen Safety Assessment for a typical application of the Conflicting ATC Clearances in airport operations. The report 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 Conflicting ATC Clearances SPR. The requirements in this document were determined through the success and the failure approach.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & company	Position / Title	Date
[redacted] DLR	[redacted]	21/11/2014
[redacted] EUROCONTROL		21/11/2014

Reviewed By - *Reviewers internal to the project.*		
Name & company	Position / Title	Date
[redacted] Thales	[redacted]	25/11/2013
[redacted]		13/01/2014
[redacted] DSNA		05/12/2013

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted] EUROCONTROL	[redacted]	25/11/2013

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & company	Position / Title	Date
[redacted] THALES	[redacted]	17/12/2014
[redacted] DLR		17/12/2014
[redacted] AIRBUS (approval by default)		17/12/2014
[redacted] EUROCONTROL (approval by default)		17/12/2014
[redacted] SEAC		17/12/2014
[redacted] DSNA		17/12/2014
[redacted] NORACON (approval by default)		17/12/2014

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection

Document History

Edition	Date	Status	Author	Justification
00.00.01	11/10/2013	Draft	[redacted] (DLR)	Initial version

00.00.02	20/11/2013	Draft	[redacted] (DLR)	Version updated on the basis of preliminary contribution provided by each partner
00.00.03	13/12/2013		[redacted] (DLR)	Version updated on the basis of reviewing by internal and external partner
00.00.04	05/02/2014	Draft	[redacted] (DLR)	Version updated on the basis of a further reviewing by internal partners.
00.00.05	25/02/2014	Draft	[redacted] (DLR)	Version updated on the basis of a further reviewing by internal partners.
00.00.09	07/03/2014	Final Version	[redacted] (DLR)	Version updated on the basis of a further reviewing by internal partner
00.01.00	16/04/2014	Final Version (handed over to SJU)	[redacted] (DSNA)	In Approval box, add THALES, AIRBUS, EUROCONTROL, DSNA as well as NORACON and ALENIA (approval by default)
00.01.01	21/11/2014	Final Version (for hand over to SJU)	[redacted] (DLR)	Version updated on the basis of comments by SJU

IPR (foreground)

This deliverable consists of) SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

This document contains the Specimen Safety Assessment for a typical application of the Conflicting ATC Clearances system. This is typical application of the OFA01.02.01 (Airport safety nets). The report 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 Conflicting ATC Clearances SPR [12]. The requirements were determined through the success and failure approach described in [1] and [2].

It is important to note that the term 'Conflicting' in the title refers to the fact that certain clearances input on the EFS at the same time by an ATCO do not comply with the local ATC rules/procedures , it does not mean that the aircraft/vehicles have ended up in confliction with each other.

1 Introduction

1.1 Background

Runway incursions are one of the most serious safety issues for ATM. In 2005 there were more than 600 runway incursions reported, this means that there are two incursions every day in the ECAC region.

In addition to runway incursions a significant number of incidents / accidents occur on taxiways and apron areas. International organisations such as ICAO, EUROCONTROL and European Commission (DG TREN) have run dedicated programmes for the prevention of ground accidents.

ICAO SMGCS Manual (Doc 9476) describes how traffic should be controlled on the surface of an airport, based on the principle of "see and be seen".

ICAO (Doc. 9830), EUROCAE (Doc ED.78B) and EUROCONTROL A-SMGCS Project have established the A-SMGCS Levels 1 (Surveillance function) and 2 (Control function including Safety Nets).

The European Commission (DG TREN) has also initiated major R&D projects (NUP-2, BETA, EMMA, EMMA2) dedicated to the future evolutions of A-SMGCS.

The current A-SMGCS Level 2 systems, which provide an alerting service for runway conflicts, have a limited scope; warnings are given to ATC only with a short time-ahead before a potential collision on active runway(s). They also suffer from performance limitations due to the technology employed.

Further improvements are therefore needed to broaden the scope of applicability to the whole airport movement area (to fulfil the ICAO A-SMGCS manual requirements), to permit an earlier detection of hazardous situations to eventually enhance the performance of the existing safety nets.

1.2 General Approach to Safety Assessment

1.2.1 A Broader approach

The safety assessment has been conducted in accordance with the SESAR Safety Reference Material [1], which itself is based on a twofold approach:

- a new success approach which is concerned with the safety of the Conflicting ATC Clearance System supported operations in the absence of failure, and
- a conventional failure approach which is concerned with the safety of the Conflicting ATC Clearance System supported operations in the event of failure within the system.

These two approaches are applied to the derivation of safety properties at each of three successive stages of the Conflicting ATC Clearance System development, described in the following chapter 1.3.

1.3 Scope of the Safety Assessment

1.3.1 Preparation and Initiation

Scoping and Change assessment is the process, recommended by SWP16.6, to identify the main safety issues associated with an OFA as soon as possible after an initial OSED (or equivalent CONOPS) has been developed and to help in deciding whether a full Safety Plan and Safety Assessment (as per the SRM [1]) are required.

1.3.2 Safety Specification at the OSED level

This phase addresses how safe the operation needs to be, in order to satisfy the Safety Acceptance Criteria. The process identifies specified operational environment, the pre-existing hazards that are inherent in the operational environment, and those hazards that are associated with potential failures modes occurring during the operation. Included in this phase is the FHA/OHA process, carried out on a representation of the ATC clearances approach at the ATM operational level. This level of assessment is normally documented in the OSED. Chapter 2 of this report provides results of the assessment carried out at the OSED level.

1.3.3 Safe Design at the SPR level

This phase assesses whether the proposed ATC clearance approach high-level system architecture design is able to achieve the level of safety specified as per chapter 3. Included in this phase is the PSSA process, which is intended to demonstrate that the proposed high-level system architecture design can reasonably be expected to deliver the required functionality and performance and achieve the required level of integrity, derived in the FHA/OHA. This level of assessment is normally documented in the SPR.

This phase is performed before the physical design and implementation of the physical system has been decided. It considers what the system will need to do, but without prejudging how the elements of the physical system should actually implement the required functionality, performance and integrity – the latter is the purpose of the SSA, as in 1.3.4 below. Chapter 3 of this report provides results of the assessment carried out at the SPR level.

1.3.4 Safe Design at Physical level

This phase addresses whether the physical system as designed and built achieves the required level of safety. Included in this phase is a substantial part of the SSA process. Unlike the two previous phases, which are concerned solely with requirements specification, SSA is mainly a requirements satisfaction process. Chapter 4 of this report indicates that no assessment has been carried out at Physical level. The physical level will be addressed during the local implementation.

1.4 Layout of the Document

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

- Chapter 1 (the present section) provides general information about the SAR document;
- Chapter 2 refers to the safety specifications at the OSED level.
- Chapter 3 contains the safe design at SPR level.
- Chapter 4 describes detailed safe design at physical level.

Additionally, the Appendices provide:

- Appendix A contains Accident incident model runway collision barrier model.
- Appendix B contains a consolidated list of safety objectives.
- Appendix C contains a consolidated list of safety requirements.
- Appendix D contains assumptions, safety issues and limitations
- Appendix E contains operational hazard assessment table.

1.5 Glossary of terms

A-SMGCS	*Advanced Surface Movement Guidance and Control System* is a system providing routing, guidance and surveillance for the control of aircraft and vehicles in order to maintain the declared surface movement rate under all weather conditions within the aerodrome visibility operational level (AVOL) while maintaining the required level of safety. *Advanced Surface Movement Guidance and Control System*. The A-SMGCS level 1 and 2: •provides a high resolution map of the runways and adjacent runway protected areas •indicates on the airport map the position and 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 •provide an alerting service for runway conflicts [13]
False Alert	A false alert is an alert which does not correspond to a situation requiring particular attention or action (e.g. caused by split tracks and radar reflections). An alert is given but no conflict exists. No alert should be indicated in this case. [14]
FDP/EFS	*Flight Data Processing/ Electronic Flight Strip*. FDP/EFS automates the production, distribution and administrative management of flight plan information and other air traffic control data and replaces the paper strip systems previously used by TWC. With the electronic flight strips all data updates received from an FDP system or by manual inputs are automatically available to all TWC. Note: In some places within the document the difference between FDP and EFS is not quite clear. The term EFS describes the HMI for the controller and the term FDP is the service behind the EFS. [9]
Nuisance Alert	Alert which is correctly generated according to the rule set but is considered operationally inappropriate. In contrast to false alerts, there is no objective definition for "nuisance alerts", but we use this name to label alerts which are not false alerts, but which at least one tower runway controller in the validation subjectively considered this alert as a nuisance. [14]
RIMS	*Runway Incursion Monitoring System*. The RIMS detects actual or potential runway incursions and provides an alert to TWC. The RIMS is shown as being logically separate from A-SMGCS since it can be regarded as a safety net rather than a continuously-acting control system. A number of alerts will be generated including • actual or potential runway incursion if an aircraft is taking off or is cleared to land • an aircraft enters the runway without a line-up instruction • an aircraft remains stationary after landing or after take-off clearance for a significant period of time (for example 15 seconds). [11]

Wrong Alert	an alert is given and a conflict exists (e.g. LUP/LUP) but a wrong type of alert is indicated (e.g. LUP/TOF). The correct type of conflict should be indicated instead (e.g. LUP/LUP). [4]

1.6 Acronyms and Terminology

Term	Definition
A/C	Aircraft
A/F	Airframe
ADS – B	Automatic Depend Surveillance – Broadcast
ADS – C	Automatic Depend Surveillance – Contract
A-SMGCS	Advanced – Surface Movement Guidance and Control System
ATC	Air Traffic Control
ATC System	In the context of this document the term ATC system refers to a combination of the A-SMGCS (Surveillance and Control) and the Electronic Flight Strips
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATS	Air Traffic Service
BETA	Operational Benefit Evaluation by Testing an A-SMGCS
BC	Basic Cause
CATC	Conflicting ATC Clearances
DG Tren	Directorate-General for Transport and Energy
DOD	Detailed Operational Description
EFS	Electronic Flight Strips
EMMA	European Airport Movement Management by A-SMGCS
EUROCAE	European Organisation for Civil Aviation Equipment
EUROCONTROL	European Organisation for the Safety of Air Navigation
FDP	Flight Data Processing
FHA	Functional Hazard Assessment
HMI	Human Machine Interface
ICAO	International Civil Aviation Organization

Term	Definition
OFA	Operational Focus Areas
OHA	Operational Hazard Assessment
OI	Operational Improvement
OSED	Operational Service and Environment Definition
PR	Performance Requirement
PSR	Primary Radar Surveillance
PSSA	Preliminary System Safety Assessment
R&D	Research and Development
RIMS	Runway Incursion Monitoring System
SDP	Surveillance Data Processing
SESAR	Single European Sky ATM Research Programme
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency.
SPR	Safety and Performance Requirements
SR	Safety Requirement
SSR	Secondary Surveillance Radar
SWP	Sub Work Package
TWC	Tower Runway Controller
VALP	Validation Plan
VALR	Validation Report

1.7 References

[1]. SESAR P16.06.01, Task T16.06.01-006, SESAR Safety Reference Material, Edition 00.02.02, 10th February 2012

[2]. SESAR P16.06.01, Task T16.06.01-006, Guidance to Apply the SESAR Safety Reference Material, Edition 00.01.02, 10th February 2012

[3]. SESAR P16.06.01, Task T16.06.01-007, OFA Safety Plan Template, Edition 00.01.02, 10th February 2012

[4]. V3 Conflicting ATC Clearances Validation Plan (VALP) Ed 00.01.00 (D18)

[5]. Updated OSED for "Conflicting ATC Clearances" Ed 00.01.00 (D16)

[6]. V2 Conflicting ATC Clearances Validation Report (VALR) Ed 00.01.00 (D15)

[7]. Runway Safety -February 12, 2010- Cardosi, K., Chase, S., and Eon, D – US. Department of Transportation, Volpe Center, Cambridge, MA [http://ntl.bts.gov/lib/35000/35000/35095/Cardosi_Runway_Safety_2010.pdf]

[8]. DOT/FAA/AR-01/66 Runway Safety: It's everybody's business July 2001

[9]. Updated SPR for "Conflicting ATC Clearances" Ed 00.01.02 (D17) Ed.00.01.00

[10].V 3 Conflicting ATC Clearances Validation Report (VALR) D19 Ed.00.01.00

[11].OSED for "Conflicting ATC Clearances" and "Conformance Monitoring for Controller" D28 Ed.00.01.00

[12].SPR for "Conflicting ATC Clearances" and "Conformance Monitoring for Controllers" Ed.00.01.00 (D29)

[13].ICAO Doc 9830: Advanced Surface Movement Guidance and Control Systems (A-SMGCS) Manual

[14].EUROCAE Minimum Aviation System Performance Specifications (MASPS) for ASMGCS (Level 1 and 2), Edition ED-87B, January 2008, including ED-87B amendment No 1 of January 2009

2 Safety specifications at the OSED Level

2.1 Scope

The Detection of Conflicting Clearances is a support tool for the Tower Runway Controller who is responsible for managing departing and arrival flights on the runway protected area. The Detection of Conflicting Clearances shall be applied to all mobiles under ATC control that are moving on the runway protected area (runways and parts of taxiways near the runway) of an airport.

This section addresses the following activities:

A description of the key properties of the Operational Environment that are relevant to the safety assessment will be done in **chapter 2.2.**

In **chapter 2.3 and 2.4** the setting of the SAfety Criteria will be fulfilled from the OFA Safety Plan, Reference [3]

Chapter 2.5 is an identification of the pre-existing hazards that affect traffic in the OFA relevant operational environment (airspace near the airport and airport). Further in this section is an identification of the risks of which operational services provided by the OFA may reasonably be expected to mitigate to some degree and extent.

Chapter 2.6 is a comprehensive determination of the operational services that are provided by the OFA to address the relevant pre-existing hazards and derivation of Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions.

In **chapter 2.7** will be done an assessment of the adequacy of the operational services provided by the OFA under abnormal conditions of the Operational Environment.

In **chapter 2.8** an assessment of the adequacy of the operational services provided by the OFA in the case of internal failures and mitigation of the system-generated hazards (derivation of Safety Objectives (failure approach)) will be done.

Chapter 2.9 considers the impacts of OFA operations on adjacent airspace or a neighbouring ATM Systems.

Chapter 2.10 describes the achievability of SAfety Criteria.

Chapter 2.11 deals with the validation and verification of the safety specification.

2.2 OFA Operational Environment and Key Properties

Operational environment and key properties are elements of the environment such as the type of airspace, traffic density, and that they can also aggravate the effects of the hazards. The Detection of Conflicting Clearances is a support tool for the Tower Runway Controller who is responsible for managing departing and arrival flights on the runway protected area.

2.2.1 Aerodrome runway protected area

In P06.07.01 Working Area 3 Conflicting ATC Clearances, we only consider the runway area and also aircraft and vehicles which can be outside the runway protected area. For example an aircraft can be given a line-up clearance while it has not reached the runway holding point.

2.2.2 Traffic characteristics

We consider aircraft and vehicle traffic on the runway protected areas, runways and the runway edges).

2.2.3 Traffic density

- ATC service for enter, cleared to land, line-up, cross RWY, and take-off is provided in low traffic situations.
- ATC service for enter, cleared to land, line-up, cross RWY, and take-off is provided in medium traffic situations.
- ATC service for enter, cleared to land, line-up, cross RWY, and take-off is provided in high traffic situations.

2.2.4 Visibility conditions

- ATC service for cleared to land, line-up, cross RWY, and take-off is provided in visibility condition 1:
    - Visibility sufficient for the pilot to taxi/to land and to avoid collision with other traffic on taxiways or runway(s) and at intersections by visual reference, and for personnel of control units to exercise control over all traffic on the basis of visual surveillance.
- ATC service for cleared to land, line-up, cross RWY, and take-off is provided in visibility condition 2:
    - Visibility sufficient for the pilot to taxi//to land and to avoid collision with other traffic on taxiways or runway(s) and at intersections by visual reference, but insufficient for personnel of control units to exercise control over all traffic on the basis of visual surveillance
- ATC service for cleared to land, line-up, cross RWY, and take-off is provided in visibility condition 3:
    - Visibility sufficient for the pilot to taxi/to land but insufficient for the pilot to avoid collision with other traffic on taxiways or runway(s) and at intersections by visual reference with other traffic, and insufficient for personnel of control units to exercise control over all traffic on the basis of visual surveillance.
- ATC service for cleared to land, line-up, cross RWY, and take-off is provided in visibility condition 4:
    - Visibility insufficient for the pilot to taxi by visual guidance only and insufficient for personnel of control units.

Visibility condition 1 will not be taken into account because impact of an operational hazard will be less severe than in visibility condition 2 or 3.

The traffic density and the visible conditions lead to twelve scenarios but some are not realistic e.g. high traffic in visibility condition 4 and some are not very stringent (e.g. low traffic in visibility condition 1). Table 1 depicts all possible combination with most relevant scenarios with a dark grey background; less realistic scenarios with a light grey background and non-realistic scenarios with a white background

	Vis Con 1	Vis Con 2	Vis Con 3	Vis Con 4
Low Traffic				
Medium Traffic				
High Traffic				

Table 1 Paired Visibility and Traffic Conditions

2.2.5 Aerodrome layout

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

For runway and taxiway layout, we keep only the more stringent conditions in terms of safety:

- Complex taxiway layout.
- Several runways.

As we assume that in our assessment, the airport will always have a complex taxiway layout and several runways.

2.2.6 A-SMGCS Surveillance

The A-SMGCS level 1:

- provides a high resolution map of the runways and adjacent runway protected areas,
- indicates on the airport map the position and 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.

The current A-SMGCS Level 2 systems, which provide an alerting service for runway conflicts, have a limited scope; warnings are given to ATC only with a short time-ahead before a potential collision on active runway(s). They also suffer from performance limitations due to the technology employed.

Further improvements are therefore needed to broaden the scope of applicability to the whole airport movement area (to fulfil the ICAO A-SMGCS manual requirements), to permit an earlier detection of hazardous situations to eventually enhance the performance of the existing safety nets.

2.3 Airspace Users Requirements

The Detection of Conflicting Clearances shall be applied to all mobiles under ATC control that are moving on the runway protected area (runways and runway edges) of an airport. The proposed improvement is the detection of inconsistent clearances input by the controller. This improvement is not to replace the existing A-SMGCS Level 2 RIMS but rather to complement and provide an extra layer of safety to prevent accidents to occur. The Detection of Conflicting Clearances is to provide an early detection of situations that if not corrected would end up in hazardous situations that would be detected in turn by the RIMS if in operation. This improvement is safety driven to reduce the number of Runway conflict [see REQ-06.02-DOD-6210.0003].

2.4 SAfety Criteria

The Accident Incident Model (AIM) for the Runway Collision (see Guidance D in **[2]**) has been used to derive the following Safety Acceptance Criteria:

SAC#1 The number of Runway conflict (RP 2) shall be reduced by 5% when ATC is supported by the conflicting ATC clearance Tool.

The Conflicting ATC clearance system impacts only the Runway conflict Prevention barrier (B3) and as indicated in 2.3 this system is safety driven. The objective is therefore to improve the performance of this safety barrier in order to reduce the number of Runway conflict (RP2) at the output of this barrier. The simplified Runway Collision Barrier Model depicted in Figure 1 illustrates the SAC location inside the barrier model.

It has been estimated that currently 5% of the runway conflict are stemming from conflicting ATC clearances given by ATC when considering a typical airport environment. It has been also estimated that, with such system in place, approximately 100% of conflicting ATC clearances will be detected. Therefore it has been decided to show that the number of Runway conflict is reduced by 5% when ATC is supported by the conflicting ATC clearances System (see SAC#1).

This 5% reduction has been compared with the Volpe Center Runway Safety study [7] which leads to similar results. Indeed runway conflicts with Landing aircraft are seen to be the most common type of runway conflict (44% of the cases) and 18% were attributed to Operational Error (controller). Regarding runway conflicts with aircraft taking off representing in this study 37% of cases, 40% were attributed to Operational Error. If we sum the two types of runway conflicts (conflict with landing a/c and conflict with a/c taking off) which represents more than 80% of the conflicts, we find that 23% of runway conflict are attributed to Operational Error. In accordance with [8] three main factors were identified for these Operational Errors: Controller forgot about something (e.g. memory lapse), Communication error between controller & pilot, and inadequate coordination among controllers in the tower. If we consider that conflicting ATC clearances are relative to the controller forgetting something (memory lapse), it represents approximately 30% of the Operational Error. Finally it could be estimated from [7] and [8] that 7% (23% * 30%) of the runway conflict are stemming from conflicting clearances given by ATC to pilots or vehicle drivers.

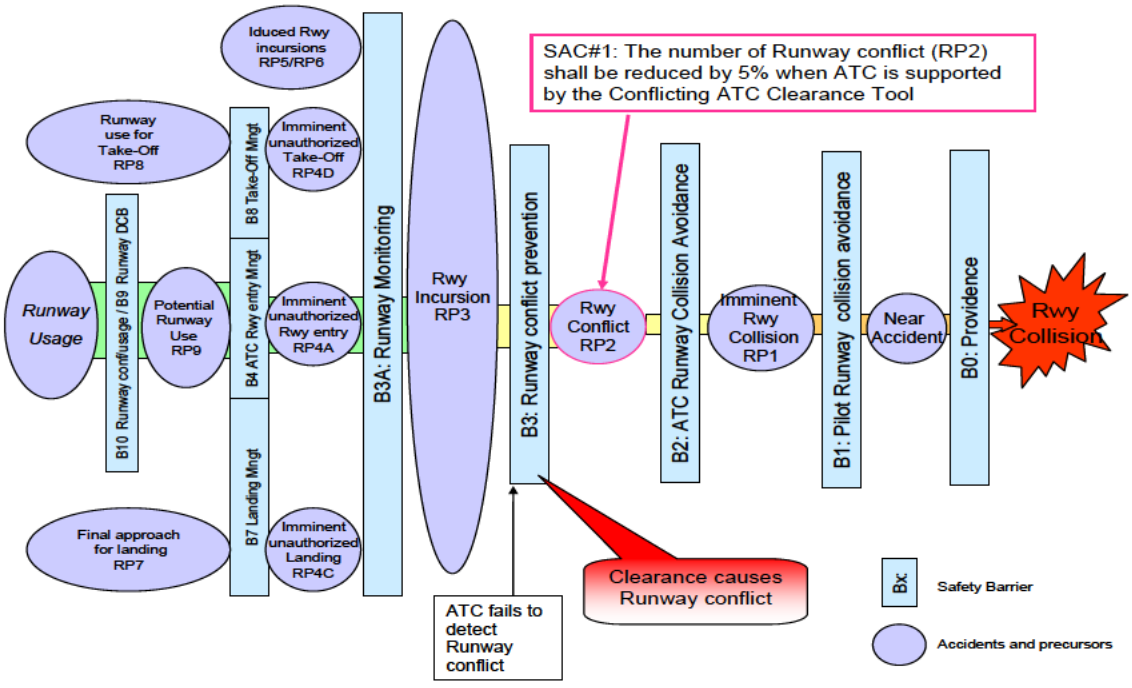


Figure 1 Simplified Runway Collision Barrier Model

2.5 Relevant Pre-existing Hazards

The pre-existing hazards that the ATM has to mitigate when considering airport operation and the conflicting ATC clearance System are as follows:

Hp#1 Situation in which the intended trajectory of two a/c are in conflict on the Runway Protected Area

Hp#2 Situation in which the intended trajectory of one a/c and a vehicle are in conflict on the Runway Protected Area

Hp#3 Situation in which the intended trajectory of two vehicles are in conflict on the Runway Protected Area

By definition, these hazards exist in the Operational Environment before any form of de-confliction has taken place. It is, therefore, the primary purpose of the Conflicting ATC Clearances System supported by the conflicting ATC clearance tool to mitigate those hazards such that the SAfety Criteria is satisfied.

Pre-existing hazards relative to the taxiway and apron management are not listed above because they are not relevant to the conflicting ATC clearances System.

2.6 Mitigation of the Pre-existing Risks – Normal Operations

The purpose of this section is to determine what operational services are provided to prevent runway conflict, and to derive Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions - i.e. those conditions that are expected to occur on a day-to-day basis[1].

2.6.1 Operational Services to Address the Pre-existing Hazards

The following Operational Services are provided by the ATC when considering the conflicting ATC clearance System, in order to address the above pre-existing hazards sufficiently to satisfy the Safety Criteria (SAC#1).

ID	ATM/ANS operational Service Objective	Pre-existing Hazards [Hp xx]
PCRwy1	Prevent Conflict between aircraft on the Runway Protected area (RPA)	Hp#1
PCRwy2	Prevent Conflict between aircraft and vehicle on the Runway Protected area (RPA)	Hp#2
PCRwy3	Prevent Conflict between vehicles on the Runway Protected area (RPA)	Hp#3

Table 2: ATM and Pre-existing Hazards relevant for the Conflicting ATC Clearances System

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

As mentioned in 2.4 the only safety barrier impacted by the conflicting ATC clearances System is the Runway conflict prevention (B3). The success-case Safety Objectives are derived to improve this safety barrier in order to meet the SAfety Criteria (SAC#1).

[1] see the abnormal conditions addressed in **section 2.7** and internal-failure conditions addressed in **section 2.8**.

These Safety Objectives are derived using the description of a typical Runway Protected Area where different mobiles (aircraft and vehicles) want to access (see Figure 2). The Conflicting ATC Clearances System shall monitor the occupancy of the Runway Protected Area and detect when conflicting ATC clearances are given to aircraft or vehicles which, when executed by pilots or vehicle drivers, will lead to runway conflict.

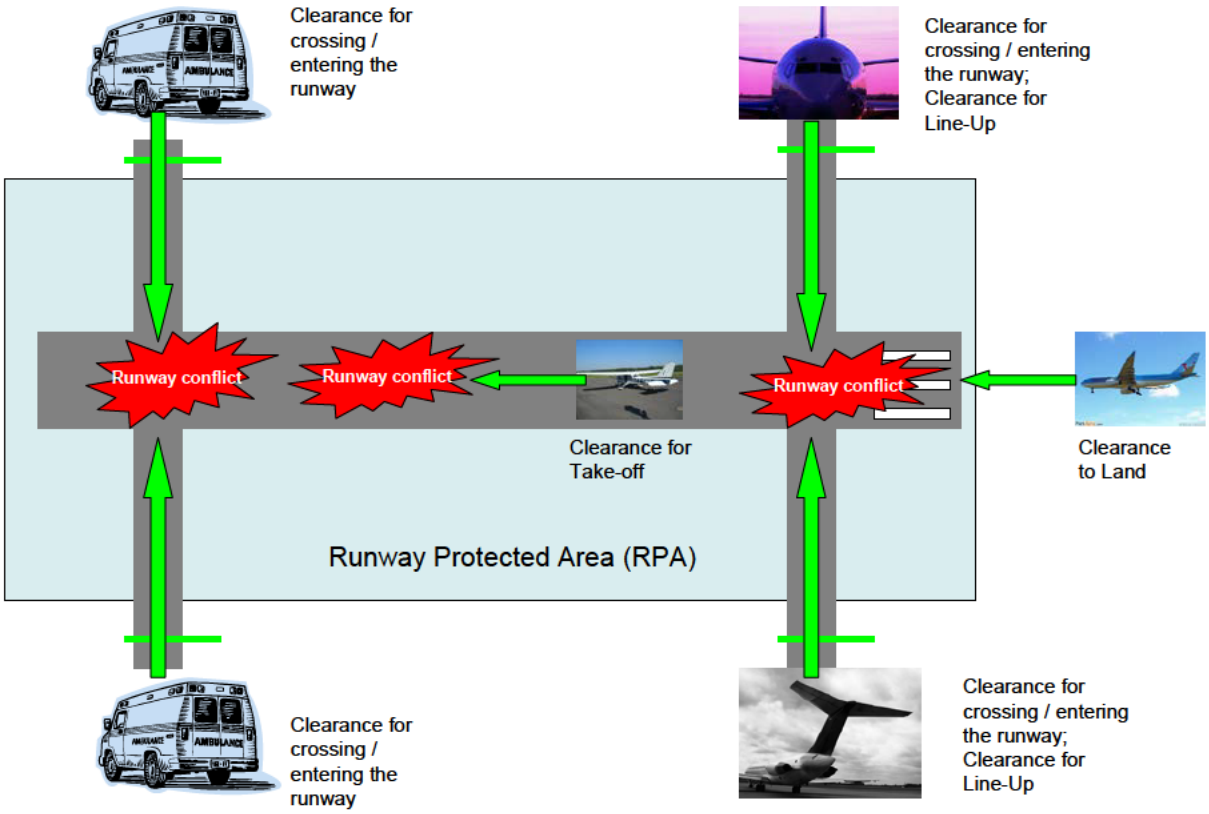


Figure 2 Management of the runway protected area

Considering the possibility of giving conflicting ATC clearances to mobiles as indicated above the following table identifies the success case Safety Objectives necessary to improve the Runway conflict prevention barrier.

Ref	Operational Service	Related AIM Barrier	Achieved by / Safety Objective [SO xx]
1	PCRwy1	B3 (Runway conflict prevention)	The Conflicting ATC Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area (***SO 01***). The Conflicting ATC Clearance System shall timely detect the conflicting clearances to allow ATC to solve the runway conflict (***SO 02***)
2	PCRwy2	B3 (Runway conflict prevention)	The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area (***SO 03***). The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the conflicting ATC clearances (***SO 02***)

Ref	Operational Service	Related AIM Barrier	Achieved by / Safety Objective [SO xx]
3	PCRwy3	B3 (Runway conflict prevention)	The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area (***SO 04***). The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the conflicting ATC clearances (***SO 02***)
4	PCRwy1, PCRwy2 and PCRwy3	B3 (Runway conflict prevention)	The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (aircraft or vehicles) (***SO 05***). Note: Clearances are transmitted by voice to mobiles but are not always "electronically" transmitted to the Conflicting ATC Clearances System.
5	PCRwy1, PCRwy2 and PCRwy3	B3 (Runway conflict prevention)	The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement. (***SO 06***). Note: This SO is associated to SAC#01 discussion (see 2.4) where it has been estimated that nearly 100% of conflicting ATC clearances will be detected. A detection rate of 99.9% means that the Conflicting ATC Clearances System misses only 1 of every 1000 conflicting ATC clearances situations.
6	PCRwy1, PCRwy2 and PCRwy3	B3 (Runway conflict prevention)	The Conflicting ATC Clearances System should not detect situations which do not lead to runway conflict (***PO 01***). Note: This Objective is not a Safety Objective per say but a Performance Objective in order to limit the increase of ATCo workload induced by nuisance/false alerts. Such ATCo workload increase may affect the nominal performance of the Runway conflict prevention barrier.

Table 3: Conflicting ATC Clearances Operational Services & Safety Objectives (success approach)

ID	Description
SO 01	The Conflicting ATC Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area
SO 02	The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the execution of the conflicting ATC clearances
SO 03	The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area
SO 04	The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area
SO 05	The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (Aircraft or vehicles)

ID	Description
SO 06	The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.

Table 4: List of Safety Objectives (success approach) for Normal Operations

In addition the following Performance Objective has been derived to address the conflicting ATC clearances system false alert rate. Alerts that prove not to involve true potential runway conflict will lower controller trust in the System and will increase controller workload explaining why such objective is necessary for an appropriate design of the System:

PO 01	The false alert rate of the Conflicting ATC Clearances System shall not be greater than 10-4 per movement[2]

Finally the question arises as to how the "total loss of the conflicting ATC clearances system" mode of failure should be modelled – i.e. whether the failure of the conflicting clearances system to operate should be dealt with as per the success (reducing) or failure (increasing) approach. We adopt the following general logic: if the loss of a device were simply the same as not having it in the first place, then this simply reduces the success performance; whereas, if the loss is greater than not having had the device (because the rest of the system had become dependent on its being there) then this increases the failure impact. With respect to the conflicting clearances system, and considering the working practices (e.g. currently no 'what if' functionality foreseen), we'll use the former to model it.

Figure 3 below provides a diagram of the different conditions associated with the conflicting ATC clearances System summarizing the safety and performance objectives identified in this section.

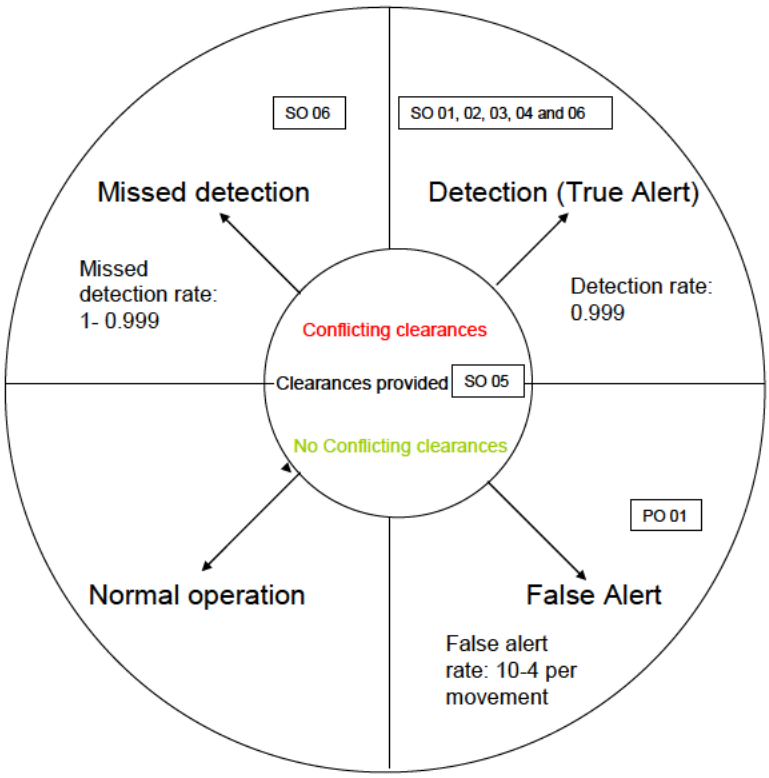


Figure 3 Diagram of the Conflicting ATC Clearances conditions

[2] Such frequency of occurrence leads to less than one false alert per operational week for an airport having 800 movements per day (departure and arrival)

2.6.3 Analysis of the Concept for Typical Airport Operations

The OSED section 3.2 [11] describes the different operational situations where conflicting ATC clearances can occur. These operational situations are:

- Line Up versus Line Up (Use Case 3 [5] [11] validated by V2 validation exercise VP 437[6] and V3 validation exercise VP438 [10])
- Line Up versus Cross/Enter (Validated by V2 validation exercise VP 437[6] and V3 validation exercise VP438 [10])
- Line Up versus Take Off (Validated by V2 validation exercise VP 437[6] and V3 validation exercise VP438 [10])
- Line Up versus Land (Validated by V2 validation exercise VP 437[6] and V3 validation exercise VP438 [10])
- Cross/Enter versus Line Up
- Cross/Enter versus Cross/Enter (Validated by V2 validation exercise VP 437[6])
- Cross/Enter versus Take Off (Validated by V2 validation exercise VP 437[6])
- Cross/Enter versus Land (Validated by V2 validation exercise VP 437[6])
- Take Off versus Line Up (validated by V3 validation exercise VP438 [10])
- Take Off versus Cross or Enter
- Take Off versus Take Off (Use Case 4 [5][11] validated by V2 validation exercise VP 437[6] V3 validation exercise VP438 [10]))
- Take Off versus Land (Validated by V2 validation exercise VP 437[6] V3 validation exercise VP438 [10]))
- Land versus Line Up (Use Case 1[11]) V3 validation exercise VP438 [10])
- Land versus Cross/Enter (Use Case 2[11]) V3 validation exercise VP438 [10])
- Land versus Take Off V3 validation exercise VP438 [10])
- Land versus Land (Validated by V2 validation exercise VP 437[6] V3 validation exercise VP438 [10])

The OSED section 6.1 [11] describes the operational requirements considering the above operational situations. It should be noted that the wording of the OSED requirements has changed in the new OSED version [11].The previous wording was: "*The Conflicting ATC Clearances System shall detect when xxx*" which has been replaced by "*The Tower Runway Controller shall receive an alert when xxx*".

The traceability between Success-case SOs identified in 2.6.2 and OSED requirements is provided in the following table:

Safety Objectives (success approach)	OSED requirements
SO 01 The Conflicting ATC Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	REQ-06.07.01-OSED-CATC.0001; REQ-06.07.01-OSED-CATC.0002; REQ-06.07.01-OSED-CATC.0003; REQ-06.07.01-OSED-CATC.0006; REQ-06.07.01-OSED-CATC.0007; REQ-06.07.01-OSED-CATC.0008; REQ-06.07.01-OSED-CATC.0009; REQ-06.07.01-OSED-CATC.0010; REQ-06.07.01-OSED-CATC.0011; REQ-06.07.01-OSED-CATC.0012; REQ-06.07.01-OSED-CATC.0013; REQ-06.07.01-OSED-CATC.0014; REQ-06.07.01-OSED-CATC.0015; REQ-06.07.01-OSED-CATC.0016; REQ-06.07.01-OSED-CATC.0017; REQ-06.07.01-OSED-CATC.0018; REQ-06.07.01-OSED-CATC.0019; REQ-06.07.01-OSED-CATC.0020; REQ-06.07.01-OSED-CATC.0021; REQ-06.07.01-OSED-CATC.0022; REQ-06.07.01-OSED-CATC.0055; REQ-06.07.01-OSED-CATC.0023; REQ-06.07.01-OSED-CATC.0056; REQ-06.07.01-OSED-CATC.0057;

Safety Objectives (success approach)	OSED requirements
	REQ-06.07.01-OSED-CATC.0058; REQ-06.07.01-OSED-CATC.0059; REQ-06.07.01-OSED-CATC.0024; REQ-06.07.01-OSED-CATC.0025; REQ-06.07.01-OSED-CATC.0060 and REQ-06.07.01-OSED-CATC.0061
SO 02 The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the execution of the conflicting ATC clearances	No OSED requirement
SO 03 The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	REQ-06.07.01-OSED-CATC.0004; REQ-06.07.01-OSED-CATC.0005; REQ-06.07.01-OSED-CATC.0010; REQ-06.07.01-OSED-CATC.0011; REQ-06.07.01-OSED-CATC.0012; REQ-06.07.01-OSED-CATC.0013; REQ-06.07.01-OSED-CATC.0014; REQ-06.07.01-OSED-CATC.0015 and REQ-06.07.01-OSED-CATC.0016
SO 04 The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	REQ-06.07.01-OSED-CATC.0010; REQ-06.07.01-OSED-CATC.0011 and REQ-06.07.01-OSED-CATC.0012
SO 05 The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (Aircraft or vehicles)	REQ-06.07.01-OSED-CATC.0026; REQ-06.07.01-OSED-CATC.0027; REQ-06.07.01-OSED-CATC.0028; REQ-06.07.01-OSED-CATC.0029; REQ-06.07.01-OSED-CATC.0030; REQ-06.07.01-OSED-CATC.0031
SO 06 The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.	No OSED requirement

Table 5: Traceability between Safety Objectives (success approach) and OSED requirements

In addition there is no OSED requirement associated to PO 01 ("When verifying potential conflicting ATC Clearances, the Conflicting ATC Clearances System shall not detect situations without risk of runway conflict (false alert) with a frequency of occurrence greater than 10^{-4} per movement").

The analysis of the conflicting ATC clearances System for typical airport operations does not lead to identify additional success-case safety objectives considering the validation activities at OSED level (e.g. results of the V2 Validation exercise [6]).

2.7 Airport operations supported by the Conflicting ATC clearances System under Abnormal Conditions

The purpose of this section is to assess the ability of airport operations supported by the Conflicting ATC clearances System to work through (robustness), or at least recover easily from (resilience), any abnormal conditions, external to the Conflicting ATC clearances System, that might be encountered relatively infrequently.

Such conditions cover both:

- failures (human or technical) external to the Conflicting ATC clearances System
- other significant, but infrequent events in the "Conflicting ATC clearances" operational environment.

2.7.1 Identification of Abnormal Conditions

In a discussion with all of our partners we could not identify abnormal conditions relevant to airport operations supported by the Conflicting ATC clearances System.

In cases the ATCO recognizes an abnormal higher alarm rate or an abnormal lower rate of detection, the ATCO is going to switch off only the CATC-System and continues without the system. This is the same situation as before introduction of the CATC-system. In this case only the RIMS will detect runway incursions.

Even a delayed or failed input of an ATC Clearance by the ATCO is not an abnormal condition. If an ATCO fails to input an ATC clearance it will be the same like a miss-detection of a conflicting situation. A miss-detection of a conflicting situation will be discussed in this document.

2.7.2 Potential Mitigations of Abnormal Conditions

NA

2.8 Mitigation of System-generated Risks (failure approach)

This section concerns the airport operations supported by the Conflicting ATC Clearances System in the case of internal failures. Before any conclusion can be reached concerning the adequacy of the safety specification of these operations, at the OSED level, it is necessary to assess the possible adverse effects that failures internal to the end-to-end System might have upon the provision of the relevant operational services described in section 2.6.1 and to derive safety objectives (failure approach) to mitigate against these effects.

2.8.1 Identification and Analysis of System-generated Hazards

From the analysis of the above description of the operational services and by considering, for each safety objective (from the success approach in Table 4 above), what would happen if the objectives were not satisfied (*i.e.* negate the safety objectives derived), the following system-generated hazards together with:

- the assessed immediate operational effect,
- the possible mitigations of the safety consequence of the operational effect with a reference to existing safety objectives (functionality and performance) or to safety objectives (functionality and performance) described in Table 6 below, and
- the assessed severity of the most probable effect from hazard occurrence as per the relevant Severity Classification Scheme(s) from Guidance E.2 of Reference **[2]**

are documented in Table 6 below.

Appendix E (OHA Table) provides the details on how the System-generated hazards have been identified and aggregated.

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
Hz 001	Failure to detect the conflicting clearances with the conflicting ATC clearances System	SO 01; SO 03; SO 04; SO 05; SO 06	*Two aircraft execute the conflicting clearances which lead potentially to a runway conflict *Aircraft and vehicle execute the conflicting clearances which lead potentially to a runway conflict *Two vehicles execute the conflicting clearances which lead potentially to a runway conflict *Aircraft/vehicles execute the clearances without the monitoring by the conflicting ATC clearances safety net	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot/driver runway collision avoidance** Pilot/driver detect (visually, by VHF monitoring or by the pilots/drivers situational display) an imminent runway collision and carries out successful avoidance action	SC3
Hz 002	Detection of the conflicting ATC clearances but with incomplete information	SO 01; SO 03; SO 04; SO 06	*Two aircraft execute the conflicting clearances which lead potentially to a runway conflict but the Conflicting ATC Clearances System detects partly the problem because one of few information(s) are missing (e.g. alert without the aircraft identification or without the type of conflicting clearances: line up vs line up; T/O vs T/O;…) *Aircraft and vehicle execute the conflicting clearances which lead potentially to a runway conflict but the Conflicting ATC Clearances System detects partly the problem because one of few information(s) are missing (e.g. alert without the mobile identification or without the type of conflicting clearances: line up vs cross/enter; cross/enter vs T/O;…) *Two vehicles execute the conflicting clearances which lead potentially to a runway conflict but the Conflicting ATC Clearances System detects partly the problem because one of few information(s) are missing (e.g. alert without the vehicle identification or without the type of conflicting clearances: cross/enter vs cross/enter)	** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she determines the missing identification and/or the missing type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	SC4

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Severity *(most probable effect)*
Hz 003	Detection of the conflicting ATC clearances but with incorrect information	SO 01; SO 03; SO 04; SO 06	*Two aircraft execute the conflicting clearances which lead potentially to a runway conflict and the Conflicting ATC Clearances System detects partly the problem because one or few information(s) are incorrect (e.g. alert with a wrong aircraft identification or with a wrong type of conflicting clearances: line up vs line up instead of T/O vs T/O) * Aircraft and vehicle execute the conflicting clearances which lead potentially to a runway conflict and the Conflicting ATC Clearances System detects partly the problem because one or few information(s) are incorrect (e.g. alert with a wrong mobile identification or with a wrong type of conflicting clearances: line up vs line up instead of Line up vs cross/enter) * Two vehicles execute the conflicting clearances which lead potentially to a runway conflict and the Conflicting ATC Clearances System detects partly the problem because one or few information(s) are incorrect (e.g. alert with a wrong vehicle identification or with a wrong type of conflicting clearances: line up vs cross/enter instead of cross/enter vs cross/enter)	*** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she detects the incorrect identification or the incorrect type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	SC4
Hz 004	Failure to solve the potential runway conflict after the conflicting ATC clearances System detection	SO 02	Aircraft and/or vehicles have executed the conflicting clearances which lead potentially to a runway conflict	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot/driver runway collision avoidance** Pilot/driver detects (visually, by VHF monitoring or by the pilots/drivers situational display) an imminent runway collision and carries out successful avoidance action	SC3

Table 6: System-Generated Hazards and Analysis

2.8.2 Derivation of Safety Objectives (integrity/reliability)

Safety Objectives (addressing integrity/reliability) shall limit the frequency with which the above System-generated hazards could be allowed to occur using the relevant Risk Classification Scheme.

Based on the Risk Classification Scheme (RCS) for the Runway Collision and the formula proposed to derive the safety objectives in Guidance E in ([2]), the following safety objectives have been derived:

ID	SO ID	Safety Objectives
Hz 001	SO 10	The frequency of occurrence of undetected conflicting ATC clearances leading to a potential runway conflict shall not be greater than $5.0x10^{-7}$ per movement
Hz 002	SO 11	The frequency of occurrence of detected conflicting ATC clearances without complete information regarding the potential runway conflict shall not be greater than $3.0x10^{-6}$ per flight per movement
Hz 003	SO 12	The frequency of occurrence of detected conflicting ATC clearances with incorrect information regarding the potential runway conflict shall not be greater than $3.0x10^{-6}$ per movement
Hz 004	SO 13	The frequency of occurrence of unresolved runway conflict after a positive detection of conflicting ATC clearances shall not be greater than $5.0x10^{-7}$ per movement

Table 7: Safety Objectives (integrity/reliability)

2.9 Impacts of OFA operations on adjacent airspace or on neighbouring ATM Systems

ATC Conflicting Clearances System is stand-alone system and doesn't have any impact to neighbouring ATM Systems. There is no impact on Apron Management, Final Approach and TMA.

2.10 Achievability of the SAfety Criteria

The general approach to showing that SAC#1 has the potential to be satisfied has been done through the specification of Safety Objectives (success and failure) in sections 2.6.2, 2.7.2, 2.8.2 and 2.9.

In terms of the Barrier Model as represented in 2.4, the crucial difference from the current system is that the Conflicting ATC clearances System enables the Runway conflict Prevention barrier to be strengthened. This additional safety net reduces the number of runway conflicts by detecting and solving most of the runway conflicts generated by the issuance of conflicting clearances.

The Conflicting ATC clearances system is not in itself designed to change the performance of other barriers. Thus, if all other barriers remain as effective, and if the runway usage remains the same, there would be fewer runway conflicts and consequently a lower risk of accident. In SESAR and considering the runway usage increase, the potential to improve safety is traded off for other types of benefit: capacity, efficiency/ flexibility or combinations thereof.

2.10.1 Benefit of conflicting ATC clearances System

The expected safety benefit to be gained from the baseline situation can be summarised as follows:

- early detection of potential runway conflict generated by conflicting ATC clearances
- provide an extra layer of safety to prevent runway accident

2.10.2 Risk assessment and satisfaction of the Safety Criteria

At the operational level, the main requirement is to show that the risk of runway conflict is reduced by 5%. It is recalled that 5% corresponds to the percentage of runway conflicts stemming from conflicting ATC clearances taking into account that the objective is to suppress completely this cause of runway conflicts.

. Normal Conditions

Description of airport operations associated to conflicting ATC clearances System allows deriving success-case Safety Objectives. The risk of runway conflict is reduced by 5% because any conflict generated by conflicting clearances is detected (SO 01, 03, 04) and is timely solved (SO 02). Furthermore the probability to detect these conflicting ATC clearances which lead to runway conflict shall be of at least 99,9% (SO 06) provided the clearances are provided ('inputted') to the Conflicting ATC Clearances System (SO 05).

Finally the probability of false alert generated by the conflicting ATC clearances System shall be less than 10^{-4}/movement (PO 01). With such objective the workload increase will be sufficiently low to prevent any effect on others safety barriers (e.g. Rwy Entry/exit management; Take-off management, Landing management, ATC runway Collision avoidance).

. Abnormal Conditions

No abnormal conditions identified.

. Failure Conditions

At the operational level, assessment of airport operations supported by the conflicting ATC clearances System in failure conditions identifies the Operational Hazards (System-generated Hazards) and determines the associated Failure-case Safety Objectives.

Failure-case Safety Objectives are required in order to limit the frequency with which the above System-generated hazards could be allowed to occur whilst ensuring that Safety Criteria specified in Section 2.4 above, could be met.

2.11 Validation & Verification of the Safety Specification

The Safety Objectives were derived

- basing on results of V2 trials, 2011 in Luxembourg, with three ATCOs, cf. D15,
- basing on workshop, Feb. 2012, in Brétigny with subject matter experts (meeting between P06.07.01 WA3 and P16.06.01
- basing on results of V3 trials, 2012 in Hamburg, with 11 ATCOs, cf. D19 [10],

A consolidated list of the Safety Objectives (functionality and performance) and Safety Objectives (integrity) is at appendix B.1, B.2 and B.3 respectively.

3 Safe Design at SPR Level

3.1 Scope

This section addresses the following activities:

- description of the Functional Model of the Conflicting ATC Clearances System – section3.2,
- description of the SPR-level model of the Conflicting ATC Clearances System – section 3.3,
- derivation, from the Safety Objectives (Functionality and Performance) of section 2, of Safety Requirements for the SPR-level design – section 3.3.2,
- analysis of the operation of the SPR-level design under normal operational conditions – section 3.4,
- analysis of the operation of the SPR-level design under abnormal conditions of the Operational Environment – section 3.5,

- assessment of the adequacy of the SPR-level design in the case of internal failures and mitigation of the system-generated hazards – section 3.6,
- justification that the SAfety Criteria are capable of being satisfied in a typical implementation – section 3.7,
- realism of the SPR-level design – section 3.8,
- validation & verification of the Specification – section 3.9.

3.2 Functional Model associated to the Conflicting ATC Clearances

The Functional Model in this context is a high level, abstract representation of the Conflicting ATC Clearances System functionality that describes what safety-related functions are performed and the data that is used by, and produced by those safety functions. This model bridges the Accident Incident barrier Model described at the operational level and the SPR-level Model which will be explained in section 3.3 below.

3.2.1 Description of Functional Model

The Functional Model associated to the Conflicting ATC Clearances System is shown in Figure 4 below and the components of the Model are described in sections 3.2.1.1 onwards. This Functional Model is a subpart of the ATM Functional Model for the SESAR Runway Operations (landing/take-off phases of flight).

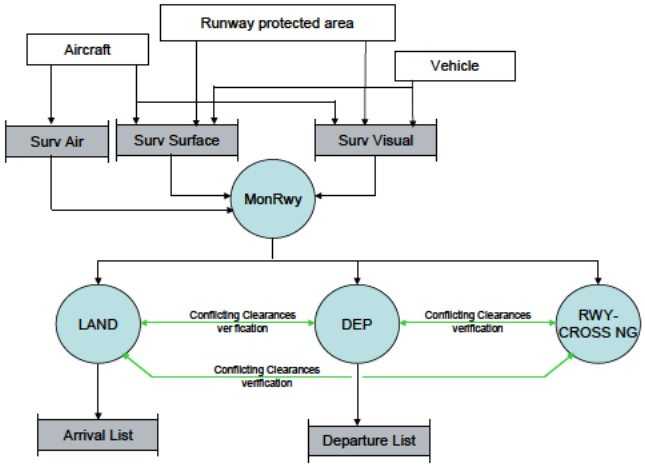
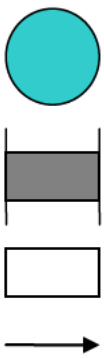


Figure 4 Functional Model associated to the Conflicting ATC Clearances System

The symbols used in the model are as follows:



Process- implements one or more safety functions, will be in general proceed in parallel with other processes in the model

Data source

External entity

Data flow

The following sections describe the entities in the model and the operation of the model

3.2.1.1 External Entities

Aircraft	Aircraft in flight, on the runway(s), and on the taxiways adjacent to the runway – mainly within the Runway Protected Area. The aircraft in flight will be (for a large airport) those on Final Approach, and those which have just departed.
Vehicles	Airport surface vehicles which require access to the runway – mainly patrol and emergency vehicles.
Runway protected area	The Runway Protected Area is a virtual volume around the runway which delineates the area which is under responsibility of the Runway control function. The area includes the navigation aids sensitive/critical areas and the Obstacle Free Zone for CAT II/III landings. Parts of the taxiways connecting with the runway are included in the area.

3.2.1.2 Data Sources

Surv Air	Electronic surveillance data giving the position and other relevant information on aircraft in flight in the vicinity of the airport to the Runway control functions. This information will be derived from appropriate sources including radar (SSR/PSR), ADS-B, ADS-C and Multilateration as appropriate or available.
Surv Surface	Electronic surveillance data giving the position and other information on aircraft and vehicles or the aerodrome surface. This information will be derived from appropriate sources including aerodrome surface movement radar, ADS-B, ADS-C and Multilateration as appropriate or available. Aircraft and vehicle identity is included in this surveillance data source.
Surv Visual	Information available to the Tower Runway Controller obtained by looking at the runway and other areas of interest via the windows in the Visual Control Room.
Arrival List	Flight data on arriving flights for each runway, sorted on arrival order and giving planned arrival time. This information may be provided by the Arrival Manager function.
Departure List	Flight data on departing flights for each runway, sorted on planned departure order and giving planned take-off time and trajectory (2d, 3d or 4d depending on the capacity of the aircraft and local system). This information may be provided by a Departure Manager function.

3.2.1.3 Safety functions

MonRwy	Monitor the occupancy of the Runway Protected Area, check that aircraft or vehicles are obeying clearances, formulate and execute responses to unexpected events including intrusion detection warnings.
LAND	Issue instructions necessary to cause an aircraft to land. Sub-functions within this process are: issue landing clearance when the runway protected area is unoccupied or there is a sufficient likelihood of the runway protected area being unoccupied

at the point of touch-down;

issue vacate instruction (the planned exit may be communicated by voice or datalink prior to touchdown.

issue go-around instruction (in the event of lack of actual or foreseen loss of runway exclusion due to intrusion, or other cause such as Navaid failure).

DEP Issue instructions necessary to permit an aircraft to take off. Sub-functions within this process are:

issue line-up instruction to permit aircraft to enter runway;

issue take-off clearance when runway is unoccupied and when sufficient separation has been achieved with preceding take-off;

issue vacate instruction (in the event of Rejected Take-Off).

RWY-Crossing Where an aircraft, vehicle or pedestrian has to cross an active runway or occupy it for some time (e.g. for surface inspection patrol), issue the necessary clearance on the basis of the runway current and predicted occupancy (inbound flights) and/or waiting departures.

3.2.1.4 Operation of the Model

MonRwy continually checks that runway occupancy is as previously planned, in other words that the runway is either unoccupied or that the currently instructed movement is in progress according to plan. **Surv Air** and **Surv Surface** inform MonRwy respectively about the position of aircraft in flight and about the position of mobiles (aircraft and vehicle) on the Runway Protected Area. Furthermore **Surv Visual** informs MonRwy about the position of aircraft in flight or mobiles (aircraft and vehicle) on the runway protected area if the airport visual conditions permit such surveillance.

The runway conflict prevention barrier is implemented by continual monitoring of the runway protected area (by the **MonRwy** function) and issuing clearances to use the runway (**Land**, **Dep** and **Rwy-Crossing** functions) provided that the previous movement has been completed and that there are no aircraft or vehicles creating an incursion (being present on the runway protected area without clearance).

Information from **MonRwy** is provided to **LAND, DEP and RWY-Crossing** functions.

- **LAND** issues appropriate clearances when either the runway becomes unoccupied after the previous movement or when the likelihood of a loss of exclusion is sufficiently low (anticipated landing clearance). The **LAND** function may also issue a go-around instruction where the runway is not vacated early enough to ensure exclusion, or for other reason such as an incursion by a vehicle.
- **DEP** issues appropriate clearances (Line-up, conditional Line-up, T/O, etc.) necessary to permit an aircraft to take off when either the runway becomes unoccupied after the previous movement or when the likelihood of a loss of exclusion is sufficiently low.
- **RWY-Crossing** maintains a logical list of aircraft (under their own power or towed), ground vehicles which require access to the runway and provides clearances to cross or enter when exclusion from landing or departing aircraft will not be infringed.

The Conflicting ATC Clearances System will improve the safety performance of **LAND**, **DEP** and **RWY-Crossing** functions by verifying that there are no conflicting clearances given to mobiles (see green arrows in Figure 4). Such verification should eliminate runway conflicts originated by conflicting ATC clearances to satisfy the SAfety Criteria (SAC#1).
LAND, **DEP** and **RWY-Crossing** functions supported by these above verifications are the main means of mitigating pre-existing hazards Hp#1, Hp#2 and Hp#3.

3.2.2 Traceability

Table 8 shows how the relevant Safety Objectives (success approach) from section 2 maps on to the elements of the Functional Model.

Safety Objectives *(Functionality and Performance from success approach)*	**Mapping to Functional Model Elements**	
	Code	**Description**
SO 01 The Conflicting ATC Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	LAND, DEP and RWY-Crossing, Aircraft, Surv Air, Surv Surface	LAND, DEP and RWY-Crossing functions issue clearances to aircraft and they will detect potential conflicting clearances supported when necessary by surveillance information (Surv Air, Surv Surface).
SO 02 The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the execution of the conflicting ATC clearances	LAND, DEP and RWY-Crossing	LAND, DEP and RWY-Crossing functions will issue new clearances to prevent potential runway conflict when it has been detected that conflicting clearances to aircraft or vehicle have been previously given. Safety Recommendation 1(Rec001): It is recommended to make the verification of the conflicting ATC clearances before clearances are given to aircraft/vehicle in order to eliminate the need to give a new clearance in case of problem (What If tool)
SO 03 The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	LAND, DEP and RWY-Crossing, Aircraft, Vehicle, Surv Air, Surv Surface	LAND, DEP and RWY-Crossing functions issue clearances to aircraft/vehicle and they will detect conflicting clearances supported when necessary by surveillance information (Surv Air, Surv Surface).
SO 04 The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	LAND, DEP and RWY-Crossing, Vehicle, Surv Surface	RWY-Crossing function issue clearances to vehicles and they will detect conflicting clearances supported when necessary by surveillance information (Surv Surface).
SO 05 The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (Aircraft or vehicles)	LAND, DEP and RWY-Crossing, Arrival List, Departure List	LAND, DEP and RWY-Crossing functions issue clearances which are provided to the arrival list and/or departure List.
SO 06 The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.	LAND, DEP and RWY-Crossing Aircraft, Vehicle, Surv Air, Surv Surface	LAND, DEP and RWY-Crossing functions issue clearances to mobiles and they will detect conflicting clearances with a probability of 99.9% per movement.

Table 8: Traceability matrix –SO (success approach) to Functional Model

3.3 The Conflicting ATC Clearances System SPR-level Model

The SPR-level Model in this context is a high-level architectural representation of the conflicting ATC Clearances System design that is entirely independent of the eventual physical implementation of the design. The SPR-level Model describes the main human tasks, machine functions and airspace

design. In order to avoid unnecessary complexity, human-machine interfaces are not shown explicitly on the model – rather they are implicit between human actors and machine-based functions.

3.3.1 Description of SPR-level Model

The SPR-level Model associated to the Conflicting ATC Clearances System is shown in Figure 5 below and is described in sections 3.3.1.1 onwards. The SPR-level Design is the level at which Safety Requirements for Conflicting ATC Clearances System are specified.

This Model is a subpart of the ATM SPR-level Model for the SESAR Runway Operations (landing/take-off phases of flight).

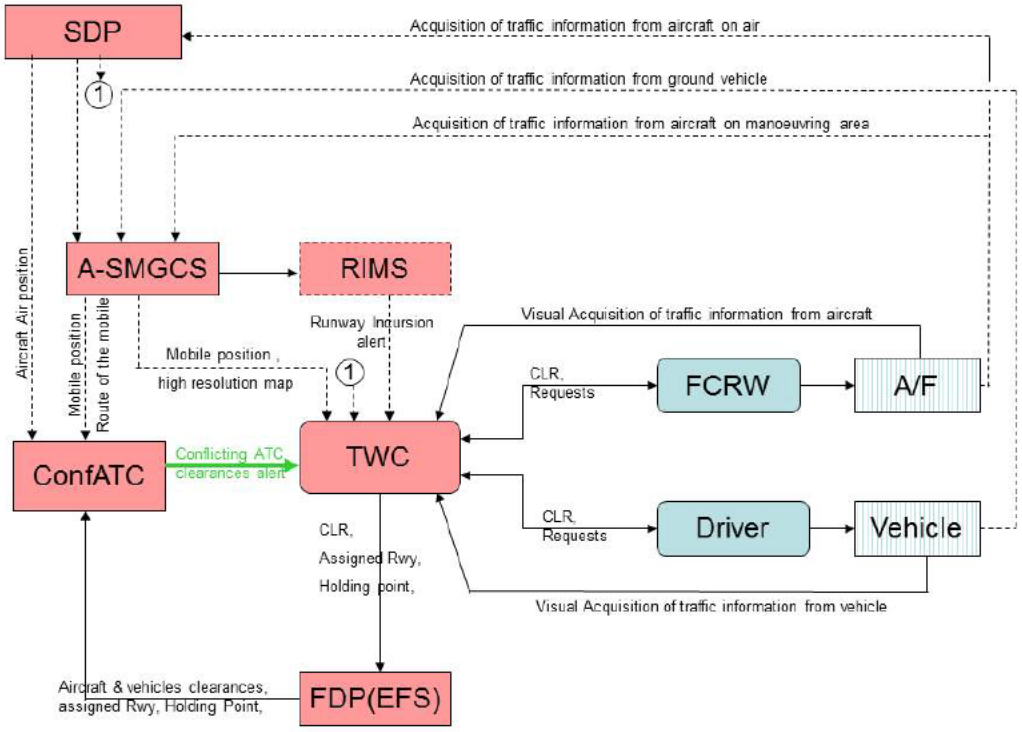
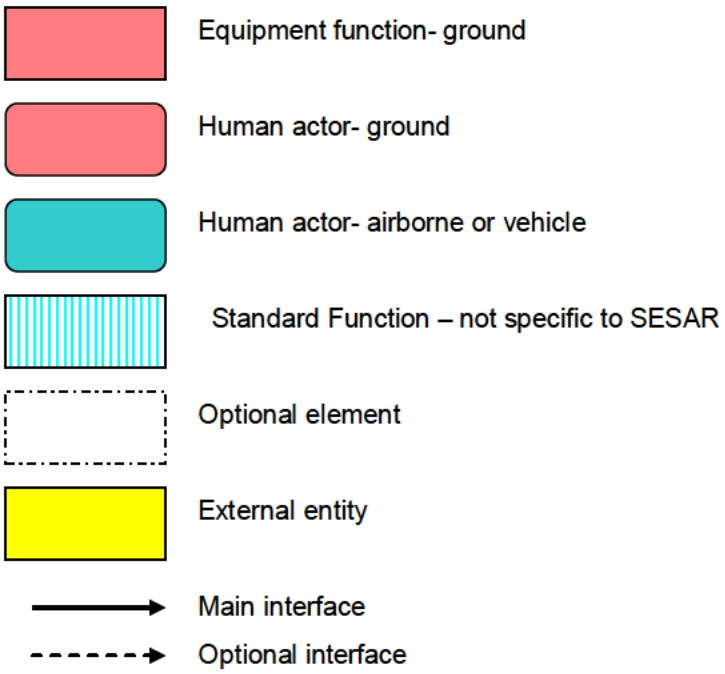


Figure 5 Conflicting ATC Clearances System SPR-level Model

The symbols used in the model are as follows:



The elements of the Model are described in the following sub-sections.

Note: although the ground based equipment elements and their interfaces to the TWC are shown separately, in practice the interface between the TWC and the majority of these equipment elements may be wholly or largely by means of an Integrated Tower Working Position (ITWP).

3.3.1.1 Aircraft/Vehicle Elements

A/F

Airframe. The (logical) A/F is defined to include also the engines and all other essential Aircraft systems. It responds to track-keeping control inputs received from manual input by the Flight Crew or from the AP/FD system.

The interface to A-SMGCS and RIMS includes all independent-surveillance (PSR, SSR Mode S) information provided to the ATM ground systems when the aircraft is on the aerodrome surface. There is also an interface to SDP when the aircraft is in flight.

Vehicle

Vehicle. The (logical) Vehicle is defined to include all essential vehicle systems to be driven on the runway protected area. It responds to control inputs from the vehicle driver.

The interface to A-SMGCS and RIMS includes all independent-surveillance (PSR, SSR Mode S) information provided to the ATM ground systems.

FCRW

Flight Crew. The Flight Crew remains ultimately responsible for the safe and orderly operation of the flight in compliance with the ICAO Rules of the Air, other relevant ICAO and EASA provisions, and within airline standard operating procedures.

The Flight Crew ensures that the aircraft operates in accordance with ATC clearances and instructions.

The main means of direct communications with the TWC will continue to be (voice) RT for time-critical transactions but supported by datalink for the

more routine tasks.

Driver *Vehicle driver.* People who drive vehicles or motorized equipment on airports in accordance with the airport rules. Vehicle driver get permission from TWC by radio or advanced coordination with ATC (pre-arranged plan) when entering in the runway protected area. The vehicle driver ensures that the vehicle operates in accordance with ATC clearances and instructions

3.3.1.2 Ground Elements

TWC *Tower Runway Controller.* The principal tasks of the TWC are to provide clearances and instructions to aircraft and ground vehicles which will maintain exclusive use of the runway for a given movement, to separate aircraft after Take-off, and to maintain separation of aircraft on Final Approach from other aerodrome traffic.

Considering runway operations, the main tasks of the TWC are to:

- assure exclusive access to the *runway(s) in use* by monitoring the runway protected area using visual surveillance and A-SMGCS
- issue landing clearances to aircraft when the Runway Protected Area is unoccupied or there is a very high probability that it will be unoccupied
- issue runway vacating instructions to aircraft
- issuing go-around instructions where a landing clearance cannot be provided or must be cancelled due to failure of previous aircraft to vacate the RPA or to an actual or possible runway conflict
- issuing line-up and take-off clearances to departing aircraft
- issuing crossing clearances for aircraft and vehicles

The main means of direct communications with the Flight Crew (FCRW) will continue to be (voice) RT for immediate communications but supported by data link. Communication with vehicle drivers is done by radio or advanced coordination with ATC.

FDP/EFS *Flight Data Processing/ Electronic Flight Strip.* FDP/EFS automates the production, distribution and administrative management of flight plan information and other air traffic control data and replaces the paper strip systems previously used by TWC. With the electronic flight strips all data updates received from an FDP system or by manual inputs are automatically available to all TWC.

Conf ATC *Conflicting ATC Clearances System.* To assist the TWC in preventing runway collision between mobiles (aircraft and vehicles) when conflicting ATC clearances are given. Conf ATC generates, in a timely manner, an alert to TWC indicating the conflicting clearances which could lead to a runway conflict if no correction is applied.

SDP *Surveillance Data Processing.* SDP correlates the various available sources of (independent and dependent) surveillance data – e.g. primary and secondary radar, ADS-B, ADS-C and Wide-area Multilateration (WAM), and provides (at least) the following information relevant to final approach and runway operations: Identification; Position; Altitude.

A-SMGCS *Advanced Surface Movement Guidance and Control System.* The A-SMGCS level 1:

provides a high resolution map of the runways and adjacent runway protected areas,

indicates on the airport map the position and 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.

RIMS *Runway Incursion Monitoring System.* The RIMS detects actual or potential runway incursions and provides an alert to TWC. The RIMS is shown as being logically separate from A-SMGCS since it can be regarded as a safety net rather than a continuously-acting control system. A number of alerts will be generated including

- actual or potential runway incursion if an aircraft is taking off or is cleared to land
- an aircraft enters the runway without a line-up instruction
- an aircraft remains stationary after landing or after take-off clearance for a significant period of time (for example 15 seconds).

3.3.1.3 External Entities

In this stage were no external entities identified.

3.3.1.4 Operation of SPR-level Model – Overview

This section describes the operation of the SPR-level model for typical airport operations when considering the scope of the conflicting ATC clearances System. Operations for landing, runway crossing and departing flights are described separately. Other runway control functions are not specifically addressed.

Landing aircraft

The TWC monitors the approach of each aircraft using SDP and visual surveillance when aircraft are sufficiently close to the runway threshold in suitable visibility.

The TWC will use the facilities of the A-SMGCS and visual observation in suitable conditions to determine whether the runway is clear of obstacles such as other aircraft or vehicle and will give the aircraft clearance to land when appropriate by voice to the FCRW.

The TWC will also clear the aircraft electronically by entering the landing clearance into the SDP/EFS interface. The Conf ATC will alert the TWC if the aircraft which is the subject of the landing clearance could be in conflict with another aircraft or vehicle on the runway due to the issuance of conflicting ATC clearances. If this occurs the TWC will take action which may include instructing the landing aircraft to go around.

After an aircraft is cleared to land, the RIMS element will monitor the runway and adjacent taxiways for conditions which might indicate a runway incursion and will alert the TWC; if this occurs the TWC will take action which may include instructing the landing aircraft to go around.

Departing aircraft

A departing aircraft is handed over to the TWC when the aircraft is close to the runway hold point. The TWC monitors the inbound traffic if interleaved operations are in use or if a landing runway conflicts with the take-off runway.

TWC considers that an aircraft can safely be lined up on the runway for take-off when preceding take-off has started its take-off run and is accelerating normally or when an inbound aircraft is sufficiently far from the threshold that a missed approach will not be required unless the line-up and take-off

manoeuvres are delayed unduly, and that there are no imminent or actual runway incursions in progress.

The information sources which the TWC uses to determine that a safe line up is possible comprise the SDP, A-SMGCS and visual observation if visibility permits. TWC will give the aircraft clearance for line-up when appropriate by voice to the FCRW.

The TWC will also clear the aircraft electronically by entering the clearance into the SDP/EFS interface. The Conf ATC will alert the TWC if the aircraft which is the subject of the line-up clearance could be in conflict with another aircraft on final approach or with an aircraft or a vehicle on the runway due to the issuance of conflicting ATC clearances. If this occurs the TWC will take action which may include instructing the departing aircraft to stop immediately the lining up or to ask the landing aircraft to go around.

At the appropriate time and if no conflicting ATC clearances for the lining-up is detected by the Conf ATC, the TWC gives the aircraft clearance for take-off by voice to FCRW. The TWC will also clear the aircraft electronically by entering the clearance into the SDP/EFS interface. The Conf ATC will alert the TWC if the aircraft which is the subject of the take-off clearance could be in conflict with another aircraft on final approach or with an aircraft or a vehicle on the runway due to the issuance of conflicting ATC clearances. If this occurs the TWC will take action which may include instructing the departing aircraft to stop immediately its take-off. If no conflicting ATC clearances for the take-off are detected by the Conf ATC, the TWC will monitor the take-off roll on the A-SMGCS and visually when conditions permit. RIMS will issue an alert to the TWC in circumstances where a runway incursion is imminent or in progress during the take-off roll.

In the event of a Rejected Take-Off (RTO), the TWC will instruct the aircraft to vacate by the most appropriate exit.

Runway Crossing

The TWC will use the facilities of the A-SMGCS and visual observation in suitable conditions to determine whether the runway is not occupied for landing or for take-off. She/he will give the crossing clearance to the mobile (aircraft or vehicle) when appropriate by voice to the FCRW or the vehicle driver.

The TWC will also clear the mobile (aircraft or vehicle) electronically by entering the crossing clearance into the SDP/EFS interface. The Conf ATC will alert the TWC if the mobile (aircraft or vehicle) which is the subject of the crossing clearance could be in conflict with another aircraft or vehicle on the runway due to the issuance of conflicting ATC clearances. If this occurs the TWC will take action which may include instructing to cancel the crossing clearance.

After a mobile (aircraft or vehicle) is cleared to cross, the RIMS element will monitor the runway and adjacent taxiways for conditions which might indicate a runway incursion and will alert the TWC; if this occurs the TWC will take action which may include instructing a landing aircraft to go around or a departing aircraft to stop immediately its take-off.

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

Table 9 below shows how the Safety Objectives (Functionality and Performance) derived in section 2 map on to the related elements of the SPR-level Model. Requirements and assumptions are derived based on the analysis of the SPR-level Model and this mapping exercise.

Table 10 provides the formalisation of the Safety Requirements (functionality and performance) which have been identified in Table 9.

Table 11 provides the formalisation of the Safety Assumptions which have been identified in Table 9.

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement (SR 00x) and/or Assumptions (A 00x)**	**Maps on to / Interface flow**
SO 01 The Conflicting ATC	TWC gives clearances and instructions to aircraft	TWC → FCRW

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement (SR 00x) and/or Assumptions (A 00x)**	**Maps on to / Interface flow**
Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	to line up, land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway (A 001)	
	TWC shall input clearances given to the aircraft to line up, land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway in the FDP/EFS (SR 001)	TWC → FDP/EFS
	TWC shall provide to the FDP/EFS the aircraft information relative to the assigned Runway and the holding point (SR 002).	TWC → FDP/EFS
	FDP/EFS shall provide to conf ATC the clearances given to the aircraft to land on, take off from, hold short of, cross, taxi and backtrack on the runway (SR 003)	FDP/EFS → Conf ATC
	FDP/EFS shall provide to conf ATC the aircraft information relative to the assigned Runway and the holding point (SR 004).	FDP/EFS → Conf ATC
	A-SMGCS provides position of aircraft taxiing on the runway protected area to TWC (A 002)	A/F→ A-SMGCS→ TWC
	A-SMGCS shall provide position of aircraft taxiing on the runway protected area to conf ATC (SR 005)	A/F→ A-SMGCS→ Conf ATC
	SDP provides position of aircraft which are in flight to TWC (A 003)	A/F→SDP→ TWC
	SDP shall provide position of aircraft which are in flight to conf ATC (SR 006)	A/F→ SDP→ Conf ATC
	Conf ATC shall provide alert to TWC when conflicting clearances are given to two mobiles which lead to a potential runway conflict between them (SR 007)	Conf ATC → TWC
	RIMS provides alert to TWC in case of aircraft runway conflicts(A 004)	A/F → RIMS → TWC
	The different alerts of the CATC system and RIMS shall be distinguishable for the Tower Runway Controller (SR 008)	Conf ATC → TWC RIMS → TWC
SO 02 The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the execution	TWC shall input clearances given to the aircraft/vehicles in the FDP/EFS as soon as practicable (SR 009). Note: This SR might be affected by Rec 01 recommending using Conf ATC as a predictive tool instead of a pure reactive tool. In such case the clearance will be entered in the EFS before	TWC → FDP/EFS

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement (SR 00x) and/or Assumptions (A 00x)**	**Maps on to / Interface flow**
of the conflicting ATC clearances	the transmission to the mobile (aircraft or vehicle).	
	Conf ATC shall provide alert to TWC within 1 second after any conflicting clearances are received from FDP/EFS (SR 010). Note: This SR participates to timely solve the potential runway conflict by alerting the TWC as quickly as possible (1 sec) in order to leave time for TWC to define and apply corrective actions.	FDP/EFS → Conf ATC → TWC
	When alerted by Conf ATC, TWC solves the potential runway conflict by issuing a corrective clearance or by confirming that the given clearances are acceptable (SR 011)	TWC → FCRW TWC → Vehicle driver
SO 03 The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	TWC gives clearances and instructions to aircraft to line up, to land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway (A 001)	TWC → FCRW
	TWC shall input clearances given to the aircraft to line up, land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway in the FDP/EFS (SR 001)	TWC → FDP/EFS
	TWC shall provide to the FDP/EFS the aircraft information relative to the assigned Runway and the holding point (SR 002).	TWC → FDP/EFS
	FDP/EFS shall provide to conf ATC the clearances given to the aircraft land on, take off from, hold short of, cross, taxi and backtrack on the runway (SR 003)	FDP/EFS → Conf ATC
	FDP/EFS shall provide to conf ATC the aircraft information relative to the assigned Runway and the holding point (SR 004).	FDP/EFS → Conf ATC
	TWC gives clearances and instructions to vehicles to enter or to cross the runway (A 005)	TWC → Driver
	TWC shall input clearances given to the vehicle to enter or to cross the runway in the FDP/EFS (SR 012)	TWC→ FDP/EFS
	TWC shall provide to the FDP/EFS the vehicle information relative to the assigned Runway and the holding point (SR 013).	TWC→ FDP/EFS
	FDP/EFS shall provide to conf ATC the clearances given to the vehicle to enter or to cross the runway (SR 014)	FDP/EFS → Conf ATC
	FDP/EFS shall provide to conf ATC the vehicle information relative to the assigned Runway and	FDP/EFS →

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement (SR 00x) and/or Assumptions (A 00x)**	**Maps on to / Interface flow**
	the holding point (SR 015).	Conf ATC
	A-SMGCS provides position of aircraft taxiing on the runway protected area to TWC (A 002)	A/F→ A-SMGCS→ TWC
	A-SMGCS provides position of vehicles being driven on the runway protected area to TWC (A 006)	Vehicle → A-SMGCS→ TWC
	A-SMGCS shall provide position of aircraft taxiing on the runway protected area to conf ATC (SR 005)	A/F→ A-SMGCS→ Conf ATC
	A-SMGCS shall provide position of vehicles being driven on the runway protected area to conf ATC (SR 016)	Vehicle → A-SMGCS→ Conf ATC
	SDP provides position of aircraft which are in flight to TWC (A 003)	A/F→ SDP→ TWC
	SDP shall provide position of aircraft which are in flight to conf ATC (SR 006)	A/F→ SDP→ Conf ATC
	Conf ATC shall provide alert to TWC when conflicting clearances are given to an aircraft and a vehicle which lead to a potential runway conflict between them (SR 017)	Conf ATC → TWC
	RIMS provides alert to TWC in case of aircraft runway conflicts(A 004)	A/F→ RIMS → TWC
	RIMS provides alert to TWC in case of vehicle runway conflicts(A 007)	Vehicle→ RIMS → TWC
	The different alerts of the CATC system and RIMS shall be distinguishable for the Tower Runway Controller (SR 008)	Conf ATC → TWC RIMS → TWC
SO 04 The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area	TWC gives clearances and instructions to vehicles to enter or to cross the runway (A 005)	TWC → Driver
	TWC shall input clearances given to the vehicle to enter or to cross the runway in the FDP/EFS (SR 012)	TWC→ FDP/EFS
	TWC shall provide to the FDP/EFS the vehicle information relative to the assigned Runway and the holding point (SR 013).	TWC→ FDP/EFS
	FDP/EFS shall provide to conf ATC the clearances given to the vehicle to enter or to cross the runway (SR 014)	FDP/EFS → Conf ATC
	FDP/EFS shall provide to conf ATC the vehicle information relative to the assigned Runway and	FDP/EFS →

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement (SR 00x) and/or Assumptions (A 00x)**	**Maps on to / Interface flow**
	the holding point (SR 015).	Conf ATC
	A-SMGCS provides position of vehicles being driven on the runway protected area to TWC (A 006)	Vehicle → A-SMGCS→ TWC
	A-SMGCS shall provide position of vehicles being driven on the runway protected area to conf ATC (SR 016)	Vehicle → A-SMGCS→ Conf ATC
	Conf ATC shall provide alert to TWC when conflicting clearances are given to two vehicles which lead to a potential runway conflict between them (SR 018)	Conf ATC → TWC
	RIMS provides alert to TWC in case of vehicle runway conflicts(A 007)	Vehicle→ RIMS → TWC
	The different alerts of the CATC system and RIMS shall be distinguishable for the Tower Runway Controller (SR 008)	Conf ATC → TWC RIMS → TWC
SO 05 The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (Aircraft or vehicles)	TWC shall input clearances given to the aircraft to land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway in the FDP/EFS (SR 001)	TWC→ FDP/EFS
	TWC shall input clearances given to the vehicle to enter or to cross the runway in the FDP/EFS (SR 012)	TWC→ FDP/EFS
	TWC shall input clearances given to the aircraft/vehicles in the FDP/EFS as soon as practicable (SR 009) Note: This SR might be affected by Rec 01 recommending using Conf ATC as a predictive tool instead of a pure reactive tool. In such case the clearance will be entered in the EFS before the transmission to the mobile (aircraft or vehicle).	TWC→ FDP/EFS
SO 06 The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.	TWC shall input clearances given to the aircraft to line up, land on, take off from, hold short of, cross, taxi and backtrack on the runway in the FDP/EFS (SR 001) FDP/EFS shall provide to conf ATC the clearances given to the aircraft to land on, take off from, hold short of, cross, taxi and backtrack on the runway (SR 003)	TWC→ FDP/EFS FDP/EFS → Conf ATC
	TWC shall input clearances given to the vehicle to enter or to cross the runway in the FDP/EFS (SR 012) FDP/EFS shall provide to conf ATC the	TWC→ FDP/EFS FDP/EFS →

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement (SR 00x) and/or Assumptions (A 00x)**	**Maps on to / Interface flow**
	clearances given to the vehicle to enter or to cross the runway (SR 014)	Conf ATC
	TWC shall provide to the FDP/EFS the aircraft information relative to the assigned Runway and the holding point (SR 002). FDP/EFS shall provide to conf ATC the aircraft information relative to the assigned Runway and the holding point (SR 004).	TWC→ FDP/EFS FDP/EFS → Conf ATC
	TWC shall provide to the FDP/EFS the vehicle information relative to the assigned Runway and the holding point (SR 013). FDP/EFS shall provide to conf ATC the vehicle information relative to the assigned Runway and the holding point (SR 015).	TWC→ FDP/EFS FDP/EFS → Conf ATC
	Conf ATC shall detect the conflicting ATC clearances with a probability of 99.9% per movement. (SR 019).	Conf ATC
	A-SMGCS performance shall be sufficiently accurate to support the Conf ATC detection rate of 99.9% per movement (SR 020).	A-SMGCS
	SDP performance shall be sufficiently accurate to support the Conf ATC detection rate of 99.9% per movement (SR 021).	SDP

Table 9: Mapping of Safety Objectives to SPR-level Model Elements

Safety Requirement (functionality & performance) **[SPR-level Model Element]**	**Requirement**	**Derived from Table 9**
SR 001 [TWC; FDP/EFS]	Tower Runway Controller shall input in the Electronic Flight Strip System (EFS) the clearances given to the aircraft to line up, land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway	SO 01; SO 03; SO 05; SO 06;
SR 002 [TWC; FDP/EFS]	Tower Runway Controller shall provide to the Electronic Flight Strip System (EFS) the aircraft information relative to the assigned Runway and the holding point	SO 01; SO 03; SO 06;
SR 003 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the clearances given to the aircraft to line up, land on, take off from, hold short of, cross, taxi and backtrack on the runway	SO 01; SO 03; SO 06;

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 9
SR 004 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the aircraft information relative to the assigned Runway and the holding point	SO 01; SO 03; SO 06;
SR 005 [A/F; A-SMGCS; Conf ATC]	A-SMGCS shall provide to the Conflicting ATC Clearances System the position of aircraft taxiing on the runway protected area	SO 01; SO 03
SR 006 [A/F; SDP; Conf ATC]	Surveillance System shall provide to the Conflicting ATC Clearances System the position of the aircraft in flight (landing and/or Take off)	SO 01; SO 03
SR 007 [Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide an alert to the Tower Runway Controller when clearances are given to two mobiles which, when executed, might lead to a runway conflict	SO 01
SR 008 [Conf ATC; RIMS; TWC]	The different alerts of the CATC system and RIMS shall be distinguishable for the Tower Runway Controller	SO 01; SO 03; SO 04
SR 009 [TWC; FDP/EFS]	The Tower Runway Controller shall input clearances given to the aircraft/vehicles in the Electronic Flight Strip System (EFS) as soon as practicable and within less than 3 seconds.	SO 02; SO 05
SR 010 [FDP/EFS; Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide alert to the Tower Runway Controller not more than 1 second following the reception of the conflicting clearances from the Electronic Flight Strip System (EFS)	SO 02
SR 011 [TWC; FCRW; Vehicle driver]	When alerted by the Conflicting ATC Clearances System, the Tower Runway Controller shall solve the potential runway conflict by issuing a corrective clearance or by confirming that the given clearances are acceptable.	SO 02
SR 012 [TWC; FDP/EFS]	The Tower Runway Controller shall input in the Electronic Flight Strip System (EFS) the clearances given to the vehicle to enter or to cross the runway	SO 03; SO 04; SO 05; SO 06
SR 013 [TWC; FDP/EFS]	The Tower Runway Controller shall provide to the Electronic Flight Strip System (EFS) the vehicle information relative to the assigned Runway and the holding point	SO 03; SO 04; SO 06
SR 014 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the clearances given to the vehicle to enter or to cross the runway	SO 03; SO 04; SO 06
SR 015	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the vehicle information	SO 03; SO 04;

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 9
[FDP/EFS; Conf ATC]	relative to the assigned Runway and the holding point	SO 06
SR 016 [Vehicle; A-SMGCS; Conf ATC]	A-SMGCS shall provide to the Conflicting ATC Clearances System the position of vehicles being driven on the runway protected area	SO 03; SO 04
SR 017 [Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide an alert to the Tower Runway Controller when clearances are given to an aircraft and a vehicle which, when executed, might lead to a runway conflict	SO 03
SR 018 [Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide an alert to the Tower Runway Controller when clearances are given to two vehicles which, when executed, might lead to a runway conflict between them	SO 04
SR 019 [Conf ATC]	The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.	SO 06
SR 020 [A-SMGCS]	The position accuracy of A-SMGCS shall be 7,5 meter on 95% confidence interval to support the Conflicting ATC Clearances System detection rate of 99,9% per movement.	SO 06
SR 021 [SDP]	Surveillance system shall be sufficiently accurate to support the Conflicting ATC Clearances System detection rate of 99.9% per movement.	SO 06

Table 10: Derivation of Safety Requirements (functionality and performance) from Safety Objectives

In addition the following Performance Requirement (PR 01) is derived to satisfy Performance Objective PO 01. This requirement encompasses most of the model elements and it is proposed to allocate lower level requirements through a specific analysis (fault tree) described in 3.4.3.

PR 01 [Conf ATC; A-SMGCS; SDP; FDP/EFS; TWC]	The false alert rate of the Conflicting ATC Clearances System shall not be greater than 10^{-4} per movement.	PO 01

ID / [SPR-level Model Element]	Assumptions	Derived from Table 10

ID / [SPR-level Model Element]	Assumptions	Derived from Table 10
A 001 [TWC; FCRW]	The Tower Runway Controller gives clearances and instructions to aircraft to line up, land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway	SO 01; SO 03
A 002 [A/F; A-SMGCS;TWC]	A-SMGCS provides to the Tower Runway Controller the position of aircraft taxiing on the runway protected area	SO 01; SO 03
A 003 [A/F; SDP;TWC]	The Surveillance System provides to the Tower Runway Controller the position of aircraft in flight	SO 01; SO 03
A 004 [A/F; RIMS;TWC]	RIMS provides alert to the Tower Runway Controller in case of aircraft runway conflicts	SO 01; SO 03
A 005 [TWC; Vehicle driver]	The Tower Runway Controller gives clearances and instructions to vehicles to enter or to cross the runway	SO 03; SO 04
A 006 [Vehicle; A-SMGCS;TWC]	A-SMGCS provides to the Tower Runway Controller the position of vehicles being driven on the runway protected area	SO 03; SO 04
A 007 [Vehicle; RIMS;TWC]	RIMS provides alert to the Tower Runway Controller in case of vehicle runway conflicts	SO 03; SO 04
A 0nn		

Table 11: Assumptions made in deriving the above Safety Requirements

3.3.3 Traceability

Table 12 below shows how the external entities, data sources and safety functions of the Functional Model have been allocated to the related elements of the SPR-level Model.

FM Element		SPR-level Model Element	
Code	**Description**	**Code**	**Description**
External Entities			
Aircraft	Aircraft under control on final approach or on the runway protected area	A/F	Airframe
Vehicle	Ground vehicle on the runway protected area	Vehicle	Ground Vehicle

FM Element		SPR-level Model Element	
Code	**Description**	**Code**	**Description**
Runway Protected Area	Runway Protected Area of the airport	--	Represented by the airport charts/layout and in A-SMGCS
Data Sources			
Surv Air	Surveillance at ground level of aircraft in final approach	SDP	Surveillance Data Processing
Surv Surface	Surveillance at ground level of mobiles (aircraft or vehicle) on the runway protected area	A-SMGCS	Advanced Surface Movement Guidance and Control System
Surv Visual	Visual Surveillance	TWC	Tower Runway Controller
Departure List	Departure List	FDP/EFS	Flight Data Processing/ Electronic Flight Strip
Arrival List	Arrival List	FDP/EFS	Flight Data Processing/ Electronic Flight Strip
Safety Functions			
MonRwy	Monitor Runway Occupancy	TWC	Tower Runway Controller
		A-SMGCS	Advanced Surface Movement Guidance and Control System
		RIMS	Runway conflict Monitoring Tool
LAND	Land aircraft	TWC	Tower Runway Controller
		Conf ATC	Conflicting ATC Clearances System
		FCRW	Flight Crew
		SDP	Surveillance Data Processing
		A-SMGCS	Advanced Surface Movement Guidance and Control System
DEP	Depart aircraft	TWC	Tower Runway Controller
		Conf ATC	Conflicting ATC Clearances System
		FCRW	Flight Crew
		SDP	Surveillance Data Processing
		A-SMGCS	Advanced Surface Movement Guidance and Control System
RWY-Crossing	Runway crossing	TWC	Tower Runway Controller
		Conf ATC	Conflicting ATC Clearances System

FM Element		SPR-level Model Element	
Code	**Description**	**Code**	**Description**
		FCRW	Flight Crew
		Driver	Vehicle Driver
		A-SMGCS	Advanced Surface Movement Guidance and Control System

Table 12: Traceability between FM and SPR-level Model Elements

Table 13 below shows the mapping between the relevant OI steps and the SPR-level Model.

OI step code	OI step title	Related Barrier in AIM	Related FM Element(s)	Related SPR-level Model Element(s)
AO-0104-A	Airport Safety Nets including Taxiway and Apron	Runway conflict Prevention Barrier (B3)	LAND, DEP and RWY-Crossing	TWR
				Conf ATC
				FCRW
				Driver
				SDP
				A-SMGCS
			MonRwy	TWR
				A-SMGCS
		ATC Runway Collision Avoidance (B2)	MonRwy	TWR
				RIMS

Table 13: Traceability between OI steps and SPR-level Model Elements

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

This section is concerned with ensuring that the SPR-level design is complete, correct and internally coherent with respect to the Safety Requirements (success approach) derived for the normal operating conditions that were used to develop the corresponding Safety Objectives (success approach) in section 2.6.2.

The analysis necessarily depends on proving the Safety Requirements (Functionality and Performance) from three perspectives:

- a static view of the system behaviour using a Thread Analysis technique, as described in **section 3.4.2** for the scenarios for normal operations described in **section 3.4.1**)

- check that the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets, through static analysis and simulation - see **section 3.4.4**
- a dynamic view of the system behaviour using in particular Real-time simulations - see **section 3.4.5**

3.4.1 Scenarios for Normal Operations

The Normal Operational Scenarios are extracted from the OSED and captured in Table 14 below.

ID	Scenario	Rationale for the Choice
Use Case 1	Land Versus Line Up	Use Case as identified in the OSED [11]
Use Case 2	Land Versus Cross/Enter	Use Case as identified in the OSED [11]
Use Case 3	Line Up versus Line Up	Use Case as identified in the OSED [11]
Use Case 4	Take Off versus take-Off	Use Case as identified in the OSED [11]

Table 14: Operational Scenarios – Normal Conditions

3.4.2 Thread Analysis of the SPR-level Model – Normal Operations

Thread Analysis is similar to Use Case analysis except that it uses a particular graphical presentation in which the actions of the individual elements of the SPR-level Model, and the interactions between those elements, are represented as a continuous 'thread', from initiation to completion.

The main equipment functions and human tasks are described by reference to the related Safety Requirements although some relatively minor functions / tasks may be represented only in the Threads themselves.

Thread Analysis for the different scenario identified in Table 14 are carried out and additional safety requirements (functionality and performance) revealed during the analysis will be identified. These safety requirements (functionality and performance) will complement those identified in 3.3.2.

3.4.2.1 Use Case # 1: Land versus Line-Up

This Use case considers an aircraft landing on a runway (aircraft 1) and an aircraft lining up on the same runway (aircraft 2). Figure 6 describes the thread analysis and the attached tables (continuous flows and actions) identify the necessary requirements or assumptions to support such operation considering the given situation (Use case#1). Requirements/assumptions which have been already identified during the SPR level model analysis (3.3.2) are labelled SR00x/ A00x whereas new requirements/ assumptions are labelled SR00x/ A00x.

In addition to this thread analysis, three specific analysis focusing on the timing issues have been conducted. The aim of these analyses is to consolidate/validate the safety requirements related to time (SR009 and SR010). Such analysis should confirm if the identified safety performances are sufficient and, when necessary, identify additional requirements. These specific analyses are addressing when the Tower Runway Controller requests a go around for the landing aircraft (Figure 7); when the Tower Runway Controller cancels the line-up clearance (Figure 8) and when the Tower Runway Controller accepts the conflicting ATC clearances (Figure 9).

- Thread analysis in normal condition

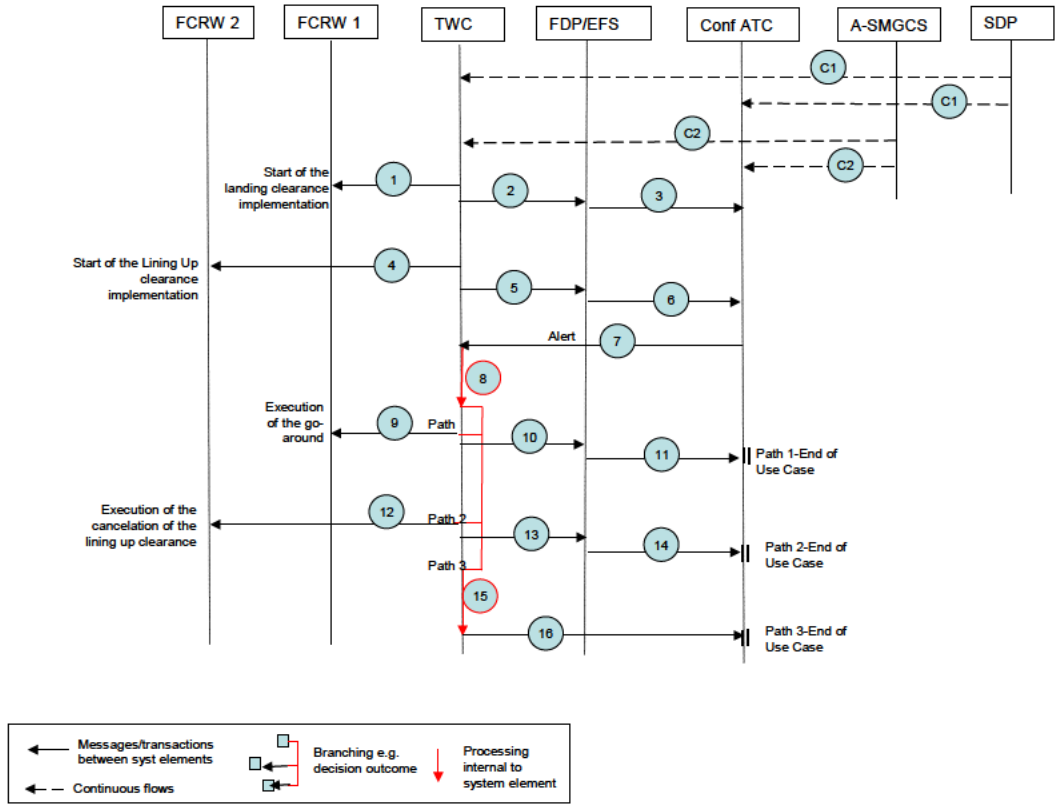


Figure 6 Thread analysis for Use Case#1: Land versus Line Up

Continuous flows	
C1	Surveillance Data Processing -SDP– passes continuous surveillance data of the aircraft 1 in final approach to TWC (A003) and to the conflicting ATC clearances System (ATC Conf)- (SR 006)
C2	A-SMGCS passes continuous position data of the aircraft 2 taxiing on the runway protected area to TWC (A002) and to the conflicting ATC clearances System (ATC Conf)- (SR 005)

Actions	
1	Tower Runway Controller (TWC) provides the landing clearance to the aircraft 1- (A001)
2	Tower Runway Controller (TWC) inputs the landing clearance into the electronic strip system (FDP/EFS)- (SR001)
3	The electronic strip system (FDP/EFS) provides the landing clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
4	Tower Runway Controller (TWC) provides the Line up clearance to aircraft 2- (A001)
5	Tower Runway Controller (TWC) inputs the Line up clearance into the electronic strip system (FDP/EFS)- (SR001)
6	The electronic strip system (FDP/EFS) provides the Line up clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
7	The conflicting ATC clearances System (Conf ATC) detects the conflicting clearance between the Landing and the Line up on the same runway (SR019) and raise an alert (SR007) considering the surveillance data information for the aircraft (SR 005 and SR 006)
8	Tower Runway Controller (TWC) reacts to the alert. [Path1: if TWC decide to provide a new clearance to aircraft 1go to 9] [Path2: if TWC decide to cancel the clearance to aircraft 2 go to 12]

Actions	
	[Path3: if TWC decide to accept the conflicting clearances go to 15]
9	Tower Runway Controller (TWC) react to the alert and request to aircraft 1 to execute a go-around - (SR011)
10	Tower Runway Controller (TWC) inputs the new aircraft clearance into the electronic strip system-(FDP/EFS)- (SR001)
11	The electronic strip system (FDP/EFS) provides the new aircraft clearance in the conflicting ATC clearances System (Conf ATC)- (SR003) [End of Use Case-Path 1]
12	Tower Runway Controller (TWC) react to the alert and cancel the Line up clearance to aircraft 2 (A001)
13	Tower Runway Controller (TWC) cancels the clearance in the electronic strip system (FDP/EFS)-(new SR022)
14	The electronic strip system (FDP/EFS) inform the conflicting ATC clearances System (Conf ATC) about the cancelled line up clearance for aircraft 2 (new SR023) [End of Use Case-Path 2]
15	Tower Runway Controller (TWC) accepts the conflicting clearances by assessing that the potential conflict will not lead to an actual runway conflict (new SR024)
16	Tower Runway Controller (TWC) accepts the conflicting clearances by informing the conflicting ATC clearances System (Conf ATC) - (new SR025) [End of Use Case-Path 3]

- Thread analysis focusing on timing issues.
  - Path 1: TWC requests a go around for the landing aircraft

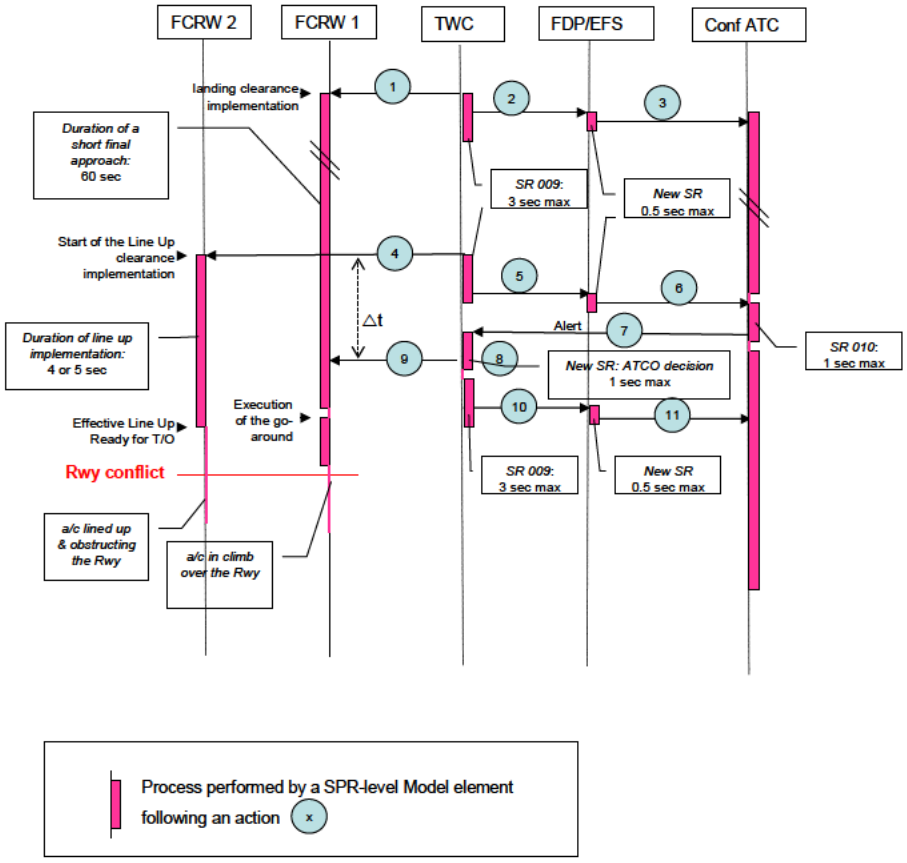


Figure 7 Timing analysis when TWC requests a go around for the landing aircraft

Considering path 1, Aircraft 2 is lining up on the runway and therefore the Go Around clearance provided by the Tower Runway Controller shall be executed before aircraft 1 crosses the same runway threshold to prevent the runway conflict. The analysis identifies that △t is the sizing criteria to

bound the time necessary for the Tower Runway Controller to detect the conflicting clearances and the flight crew 1 to execute the missed approach.

△t is the sum of actions 5, 6, 7 and 8/9 and should be less than the duration of the line up which is estimated to be 4 or 5 seconds. Action 5 is associated to SR 009 (TWC shall enter the clearance in the EFS not more than 3 sec after giving the clearance to the pilot) and Action 7 is associated to SR 010 (Conf Conflicting ATC Clearances System shall alert the TWC of the conflicting ATC clearances within 1 sec). There is no timing requirement presently identified for Action 6 and Action 8/9, it is therefore necessary to identify new requirements for the EFS to provide the clearance to Conf ATC within 0.5 sec (new SR026) and for the TWC to provide the Go Around clearance to the landing clearance within 1 sec (new SR027). The sum all these durations is still above 5 seconds, it means that at least one requirement should be more demanding in the timing domain and SR 009 seems to be the main candidate. To address that point a safety issue is open to verify if a more demanding SR 009 is achievable (Safety Issue 1)

Safety Issue 1 (I001): It shall be validated if the Tower Runway Controller could input clearance in the Electronic Flight Strip System (EFS) not more than 1 or 2 seconds after providing the clearance to the aircraft/vehicles. It is recalled that presently SR 009 requires 3 seconds.

- Path 2: TWC cancels the Line up clearance

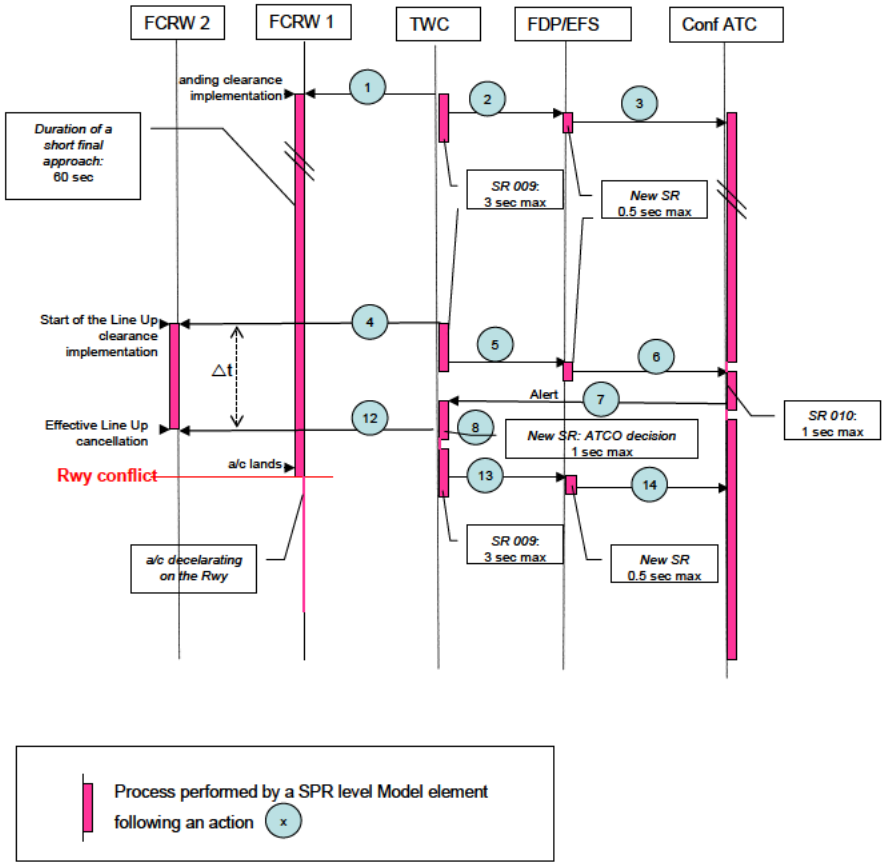


Figure 8 Timing analysis when TWC cancels the Line up clearance

Considering path 2, aircraft 2 is taxiing from the short holding point to the line up and the cancellation of the line Up clearance provided by the Tower Runway Controller shall be executed before aircraft 2 penetrates the runway to prevent the runway conflict with the landing aircraft. The timing analysis identifies that △t is the sizing criteria to bound the time necessary for the Tower Runway Controller to detect the conflicting clearances and the flight crew 2 to cancel the line up.

△t is the sum of actions 5, 6, 7 and 8/12 and should be less than the duration of the line up which is estimated to be 4 or 5 seconds. The duration of actions 5 and 7 have been recalled above for the Path 1 timing analysis and are valid for path 2. Similarly to path 1, there is no timing requirement presently identified for Action 6 and Action 8/12. The new requirement identified for path 1 regarding

Action 6 (SR026) is also applicable to path 2. Regarding action 8/12 it is necessary to identify a new requirement for the TWC to cancel the line up clearance within 1 sec (new SR028). The sum all these durations is still above 5 seconds, it means that Safety Issue 1 identified for path 1 is also applicable for path 2.

- Path 3: TWC accepts the conflicting ATC clearances

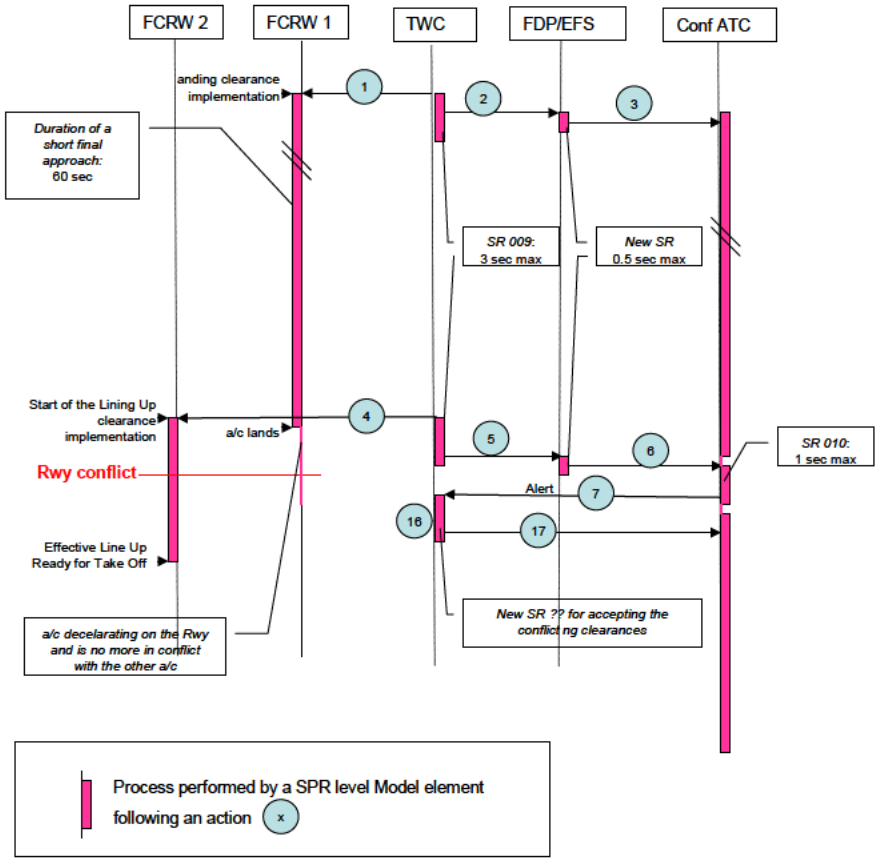


Figure 9 Timing analysis when TWC accepts the conflicting ATC clearances

Considering path 3, aircraft 1 will land before aircraft 2 penetrates the runway but a conflicting clearances alert is triggered. There is no critical timing issue for this path except that the acceptation of the conflicting ATC clearances by the Tower Runway Controller shall be made in a timely manner to acknowledge the triggered alert (new SR029). Indeed the alert, if not cancelled, could jeopardise the recognition of other alerts (e.g. RIMS).

3.4.2.2 Use Case # 1b Line-Up versus Land

This Use case considers an aircraft lining-up on a runway (aircraft 1) and an aircraft landing on the same runway (aircraft 2). The aim of this use case is to analyse if new requirements could derive as in use case 1 (Land versus Line-up). Figure 10 describes the thread analysis and the attached tables (continuous flows and actions) identify the necessary requirements or assumptions to support such operation considering the given situation (Use case#1). Requirements/assumptions which have been already identified during the SPR level model analysis (3.3.2) are labelled SR00x/ A00x whereas new requirements/ assumptions are labelled SR00x/ A00x.

- Thread analysis in normal condition

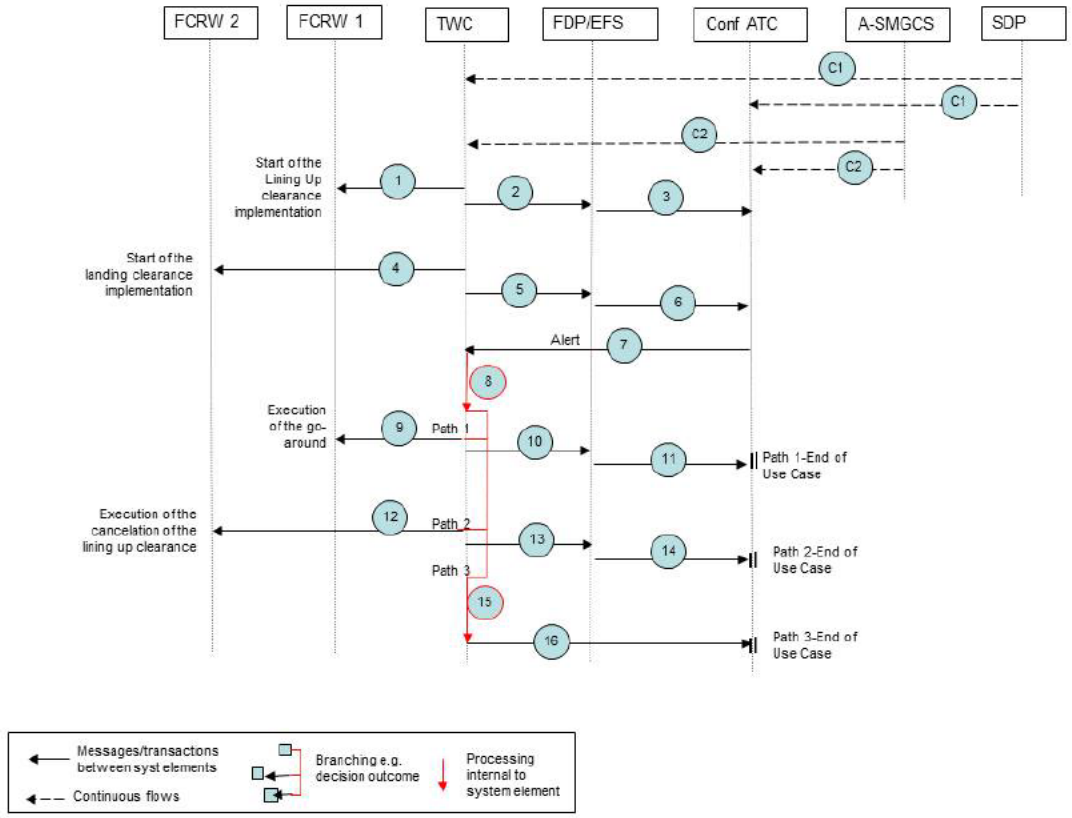


Figure 10 Thread analysis for Use Case#1b: Line Up versus Land

Continuous flows	
C1	Surveillance Data Processing -SDP– passes continuous surveillance data of the aircraft 2 in final approach to TWC (A003) and to the conflicting ATC clearances System (ATC Conf)- (SR 006)
C2	A-SMGCS passes continuous position data of the aircraft 1 taxiing on the runway protected area to TWC (A002) and to the conflicting ATC clearances System (ATC Conf)- (SR 005)

Actions	
1	Tower Runway Controller (TWC) provides the Line up clearance to aircraft 1- (A001)
2	Tower Runway Controller (TWC) inputs the Line up clearance into the electronic strip system (FDP/EFS)- (SR001)
3	The electronic strip system (FDP/EFS) provides the Line up clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
4	Tower Runway Controller (TWC) provides the landing clearance to the aircraft 2- (A001)
5	Tower Runway Controller (TWC) inputs the landing clearance into the electronic strip system (FDP/EFS)- (SR001)
6	The electronic strip system (FDP/EFS) provides the landing clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
7	The conflicting ATC clearances System (Conf ATC) detects the conflicting clearance between the Line up and the Landing on the same runway (SR019) and raise an alert (SR007) considering the surveillance data information for the aircraft (SR 005 and SR 006)
8	Tower Runway Controller (TWC) reacts to the alert. [Path1: if TWC decide to provide a new clearance to aircraft 1go to 9] [Path2: if TWC decide to cancel the clearance to aircraft 2 go to 12]

Actions	
	[Path3: if TWC decide to accept the conflicting clearances go to 15]
9	Tower Runway Controller (TWC) react to the alert and request to aircraft 2 to execute a go-around - (SR011) (if aircraft 1 is already lined up on the runway and aircraft 2 is near the runway threshold option12 and 15 are not possible)
10	Tower Runway Controller (TWC) inputs the new aircraft clearance into the electronic strip system-(FDP/EFS)- (SR001)
11	The electronic strip system (FDP/EFS) provides the new aircraft clearance in the conflicting ATC clearances System (Conf ATC)- (SR003) [End of Use Case-Path 1]
12	Tower Runway Controller (TWC) react to the alert and cancel the Line up clearance to aircraft 1 (A001)
13	Tower Runway Controller (TWC) cancels the clearance in the electronic strip system (FDP/EFS)-(new SR022)
14	The electronic strip system (FDP/EFS) inform the conflicting ATC clearances System (Conf ATC) about the cancelled line up clearance for aircraft 1 (new SR023) [End of Use Case-Path 2]
15	Tower Runway Controller (TWC) accepts the conflicting clearances by assessing that the potential conflict will not lead to an actual runway conflict. (new SR024)
16	Tower Runway Controller (TWC) accepts the conflicting clearances by informing the conflicting ATC clearances System (Conf ATC) - (new SR025) [End of Use Case-Path 3]

- Thread analysis focusing on timing issues.
  - Path 1: TWC requests a go around for the landing aircraft (if aircraft 1 is already lined up on the runway and aircraft 2 is near the runway threshold option12 and 15 are not possible)

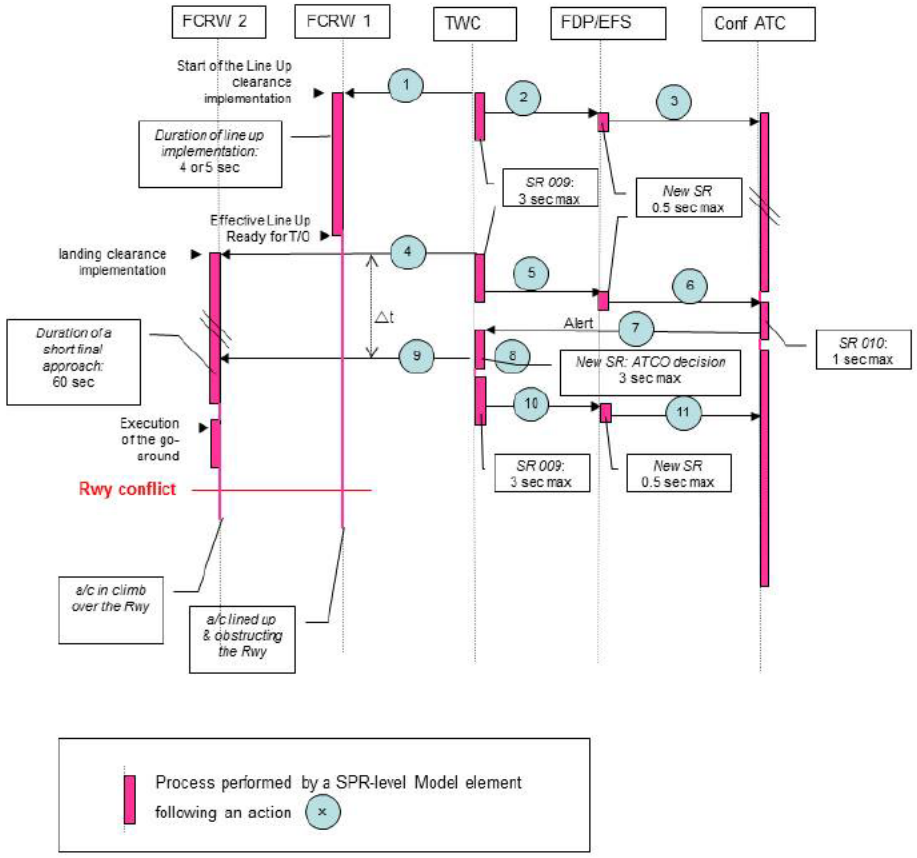


Figure 11 Timing analysis when TWC requests a go around for the landing aircraft

Considering path 1, Aircraft 1 is lining up on the runway and therefore the Go Around clearance provided by the Tower Runway Controller shall be executed before aircraft 2 crosses the same

runway threshold to prevent the runway conflict. The analysis identifies that △t is the sizing criteria to bound the time necessary for the Tower Runway Controller to detect the conflicting clearances and the flight crew 2 to execute the missed approach.

△t is the sum of actions 5, 6, 7 and 8/9. Action 5 is associated to SR 009 (TWC shall enter the clearance in the EFS not more than 3 sec after giving the clearance to the pilot) and Action 7 is associated to SR 010 (Conf Conflicting ATC Clearances System shall alert the TWC of the conflicting ATC clearances within 1 sec). There is no timing requirement presently identified for Action 6 and Action 8/9, it is therefore necessary to identify new requirements for the EFS to provide the clearance to Conf ATC within 0.5 sec (new SR026) and for the TWC to provide the Go Around clearance to the landing clearance within 3 sec (new SR027). The sum all these durations is still above 5 seconds, it means that at least one requirement should be more demanding in the timing domain and SR 009 seems to be the main candidate. To address that point a safety issue is open to verify if a more demanding SR 009 is achievable (Safety Issue 1)

Safety Issue 1 (I001): It shall be validated if the Tower Runway Controller could input clearance in the Electronic Flight Strip System (EFS) not more than 1 or 2 seconds after providing the clearance to the aircraft/vehicles. It is recalled that presently SR 009 requires 3 seconds.

- Path 2: TWC cancels the Line up clearance

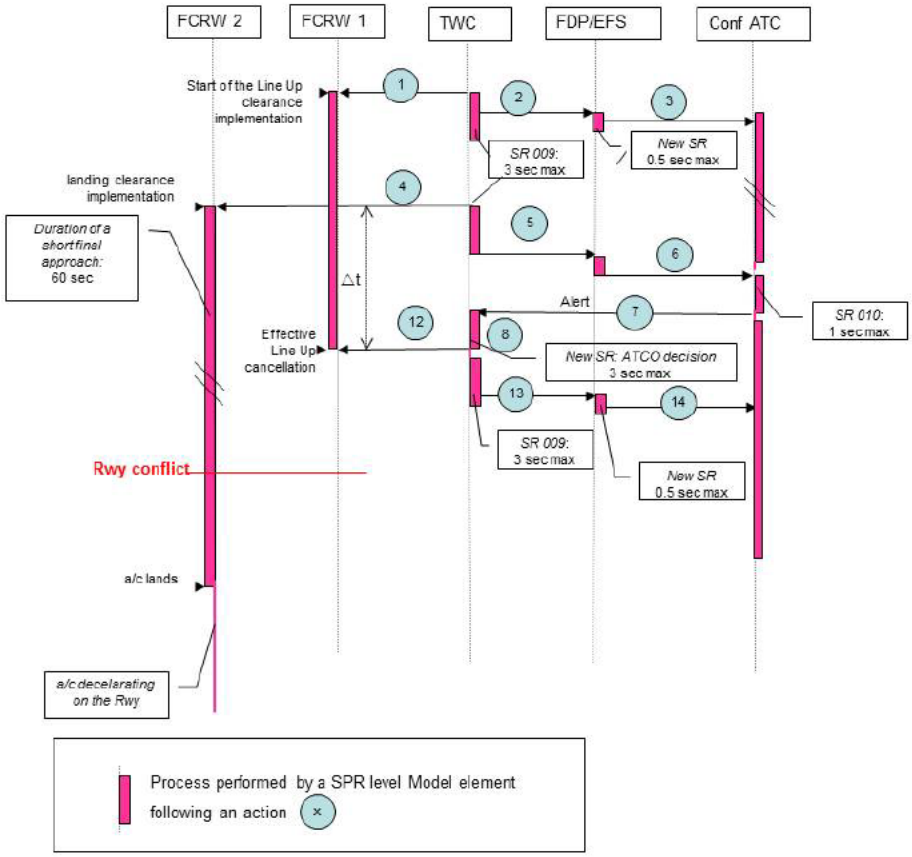


Figure 12 Timing analysis when TWC cancels the Line up clearance

Considering path 2, aircraft 1 is taxiing from the short holding point to the line up and the cancellation of the line Up clearance provided by the Tower Runway Controller shall be executed before aircraft 1 penetrates the runway to prevent the runway conflict with the landing aircraft. The timing analysis identifies that △t is the sizing criteria to bound the time necessary for the Tower Runway Controller to detect the conflicting clearances and the flight crew 1 to cancel the line up.

△t is the sum of actions 5, 6, 7 and 8/12 and should be less than the duration of the line up which is estimated to be 4 or 5 seconds. The duration of actions 5 and 7 have been recalled above for the Path 1 timing analysis and are valid for path 2. Similarly to path 1, there is no timing requirement presently identified for Action 6 and Action 8/12. The new requirement identified for path 1 regarding Action 6 (SR026) is also applicable to path 2. Regarding action 8/12 it is necessary to identify a new requirement for the TWC to cancel the line up clearance within 1 sec (new SR028). The sum all these durations is still above 5 seconds, it means that Safety Issue 1 identified for path 1 is also applicable for path 2.

- Path 3: TWC accepts the conflicting ATC clearances

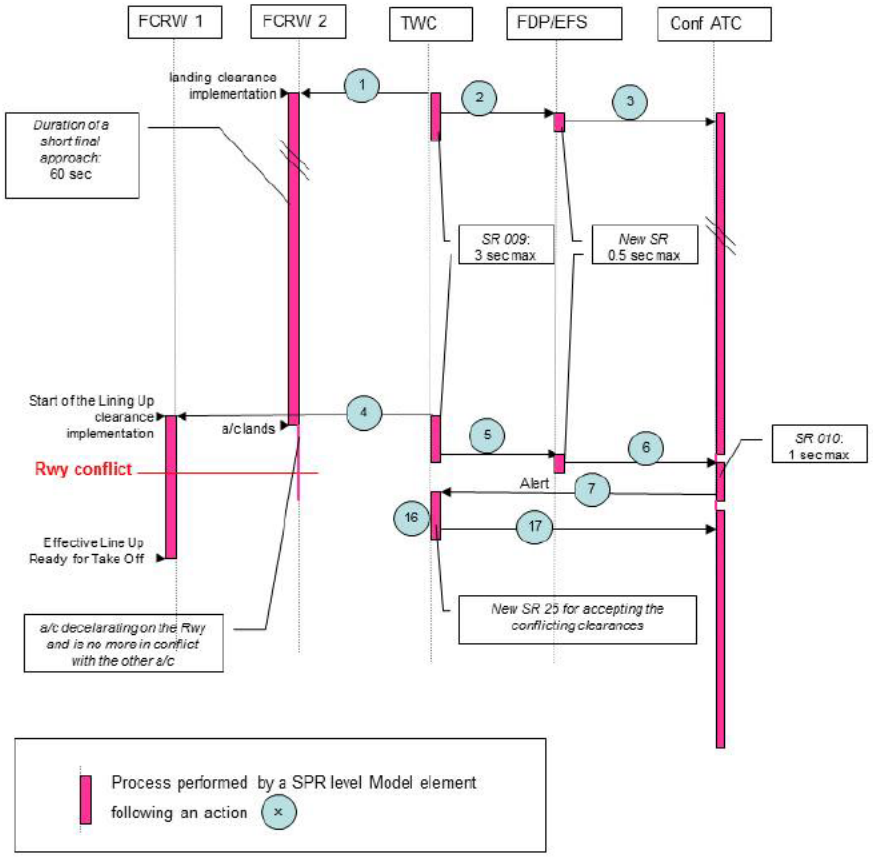


Figure 13 Timing analysis when TWC accepts the conflicting ATC clearances

Considering path 3, aircraft 2 will land before aircraft 1 penetrates the runway but a conflicting clearances alert is triggered. There is no critical timing issue for this path except that the acceptation of the conflicting ATC clearances by the Tower Runway Controller shall be made in a timely manner to acknowledge the triggered alert (new SR029). Indeed the alert, if not cancelled, could jeopardise the recognition of other alerts (e.g. RIMS).

To sum up there could no new requirements derived compared with use case 1. Only the timing analysis is different.

3.4.2.3 Use Case # 2: Land versus Cross-Enter

This Use case considers an aircraft landing on a runway and a vehicle wanting to cross the same runway. Figure 14 describes the thread analysis and the attached tables (continuous flows and actions) identify the necessary requirements or assumptions to support such operation considering the given situation (Use case#2). Requirements/assumptions which have been already identified during the SPR level model analysis (3.3.2)are labelled SR00x/ A00x whereas new requirements/ assumptions are labelled new SR00x/ new A00x or SR00x/ A00x if identified in previous thread analysis.

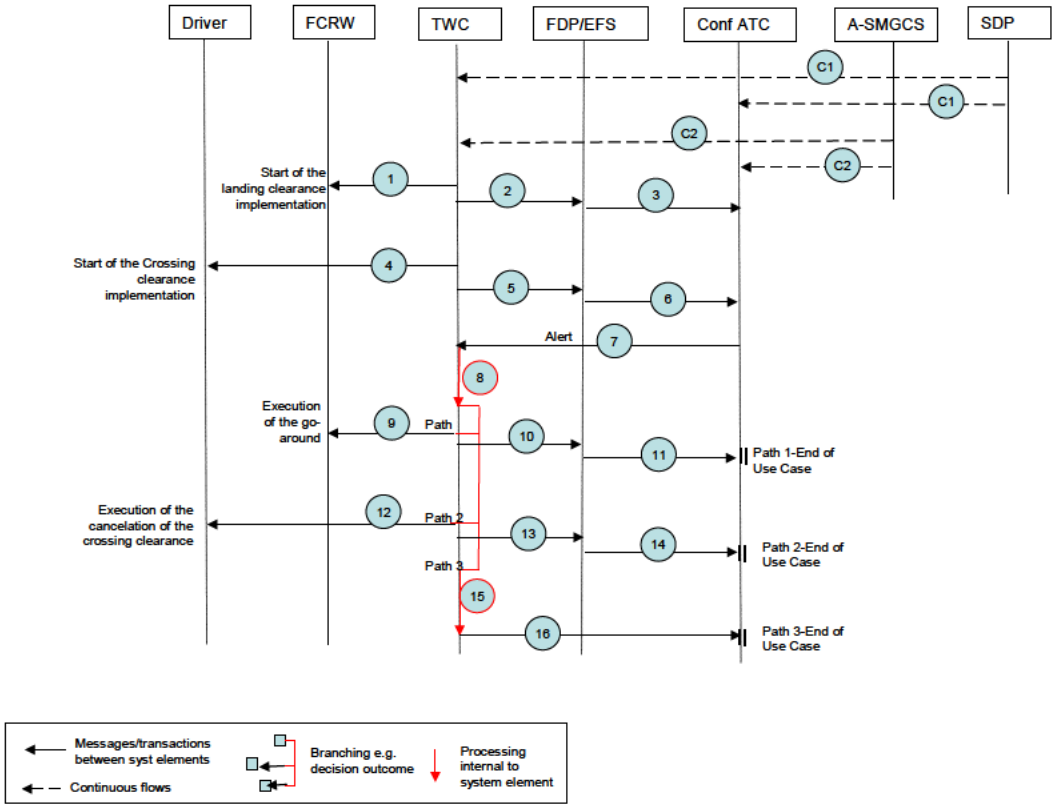


Figure 14 Thread analysis for Use Case#2: Land versus Cross/Enter

Continuous flows	
C1	Surveillance Data Processing -SDP– passes continuous surveillance data of the aircraft in final approach to TWC (A003) and to the conflicting ATC clearances System (ATC Conf)- (SR 006)
C2	A-SMGCS passes continuous ground position data of the vehicle to TWC (A006) and to the conflicting ATC clearances System (ATC Conf)- (SR 016)

Actions	
1	Tower Runway Controller (TWC) provides the landing clearance to the aircraft- (A001)
2	Tower Runway Controller (TWC) inputs the landing clearance into the electronic strip system (FDP/EFS)- (SR001)
3	The electronic strip system (FDP/EFS) provides the landing clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
4	Tower Runway Controller (TWC) provides the runway crossing clearance to vehicle- (A005)
5	Tower Runway Controller (TWC) inputs the crossing clearance into the electronic strip system (FDP/EFS)- (SR012)
6	The electronic strip system (FDP/EFS) provides the crossing clearance to the conflicting ATC clearances System (Conf ATC)- (SR014)
7	The conflicting ATC clearances System (Conf ATC) detects the conflicting clearance between the Landing aircraft and the vehicle crossing the same runway (SR019) and raise an alert (SR017) considering the surveillance data information for the aircraft (SR 006)and the vehicle (SR 016)
8	Tower Runway Controller (TWC) reacts to the alert. [Path1: if TWC decide to provide a new clearance to the aircraft go to 9] [Path2: if TWC decide to cancel the clearance to vehicle go to 12] [Path3: if TWC decide to accept the conflicting clearances go to 15]
9	Tower Runway Controller (TWC) react to the alert and request to the aircraft to execute a go-around - (SR011)

Actions	
10	Tower Runway Controller (TWC) inputs the new aircraft clearance into the electronic strip system-(FDP/EFS)- (SR001)
11	The electronic strip system (FDP/EFS) provides the new aircraft clearance in the conflicting ATC clearances System (Conf ATC)- (SR003) [End of Use Case-Path 1]
12	Tower Runway Controller (TWC) react to the alert and cancel the crossing clearance to the vehicle (A005)
13	Tower Runway Controller (TWC) cancels the clearance in the electronic strip system (FDP/EFS)-(SR022)
14	The electronic strip system (FDP/EFS) inform the conflicting ATC clearances System (Conf ATC) about the cancelled crossing clearance for the vehicle (SR023) [End of Use Case-Path 2]
15	Tower Runway Controller (TWC) accepts the conflicting clearances by assessing that the potential conflict will not lead to an actual runway conflict. (SR024)
16	Tower Runway Controller (TWC) accepts the conflicting clearances by informing the conflicting ATC clearances System (Conf ATC) - (SR025) [End of Use Case-Path 3]

3.4.2.4 Use Case # 3: Line Up versus Line Up

This Use case considers two aircraft lining up on the same runway (aircraft 1 and 2) without conditional Line up/Line up given in. Figure 15 describes the thread analysis and the attached tables (continuous flows and actions) identify the necessary requirements or assumptions to support such operation considering the given situation (Use case#3). Requirements/assumptions which have been already identified during the SPR level model analysis (3.3.2) are labelled SR00x/ A00x whereas new requirements/ assumptions are labelled new SR00x/ new A00x or SR00x/ A00x if identified in previous thread analysis.

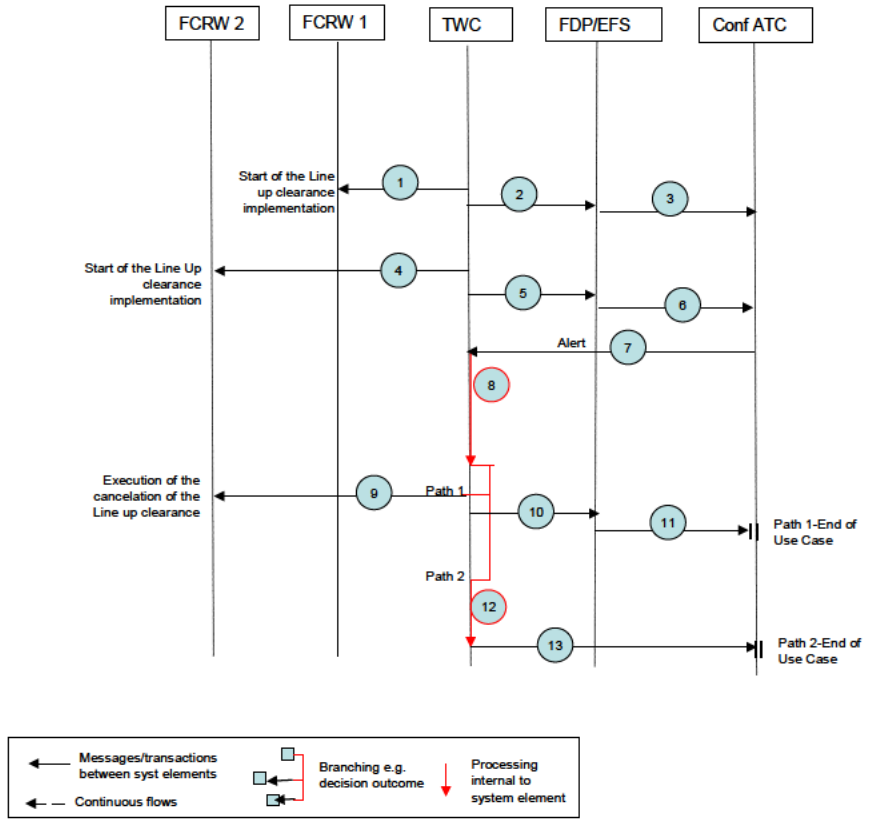


Figure 15 Thread analysis for Use Case#3: Line up versus Line up

Continuous flows	
C1	Not required for Line up versus Line Up situation
C2	Not required for Line up versus Line Up situation

Actions	
1	Tower Runway Controller (TWC) provides the Line up clearance to aircraft 1- (A001)
2	Tower Runway Controller (TWC) inputs the Line up clearance into the electronic strip system (FDP/EFS)- (SR001)
3	The electronic strip system (FDP/EFS) provides the Line up clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
4	Tower Runway Controller (TWC) provides the Line up clearance to aircraft 2- (A001)
5	Tower Runway Controller (TWC) inputs the Line up clearance into the electronic strip system (FDP/EFS)- (SR001)
6	The electronic strip system (FDP/EFS) provides the Line up clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
7	The conflicting ATC clearances System (Conf ATC) detects the conflicting clearance between the two Line up on the same runway (SR019) and raise an alert (SR007)
8	Tower Runway Controller (TWC) reacts to the alert. [Path1: decide to cancel the clearance to aircraft 2 go to 9] [Path2: if TWC decide to accept the conflicting clearances go to 12]
9	Tower Runway Controller (TWC) react to the alert and cancel the Line up clearance to aircraft 2 (A001)
10	Tower Runway Controller (TWC) cancels the clearance in the electronic strip system (FDP/EFS)- (SR022)
11	The electronic strip system (FDP/EFS) inform the conflicting ATC clearances System (Conf ATC) about the cancelled line up clearance for aircraft 2 (SR023) [End of Use Case-Path 1]
12	Tower Runway Controller (TWC) accepts the conflicting clearances by assessing that the potential conflict will not lead to an actual runway conflict. (SR024)
13	Tower Runway Controller (TWC) accepts the conflicting clearances by informing the conflicting ATC clearances System (Conf ATC) - (SR025) [End of Use Case-Path 2]

3.4.2.5 Use Case # 4: Take Off versus Take Off

This Use case considers two aircraft (aircraft 1 and 2) having been given Take Off clearances on the same runway or on crossing runways or on converging runways. Figure 16 describes the thread analysis and the attached tables (continuous flows and actions) identify the necessary requirements or assumptions to support such operation considering the given situation (Use case#4). Requirements/assumptions which have been already identified during the SPR level model analysis (3.3.2) are labelled SR00x/ A00x whereas new requirements/ assumptions are labelled new SR00x/ new A00x or SR00x/ A00x if identified in previous thread analysis.

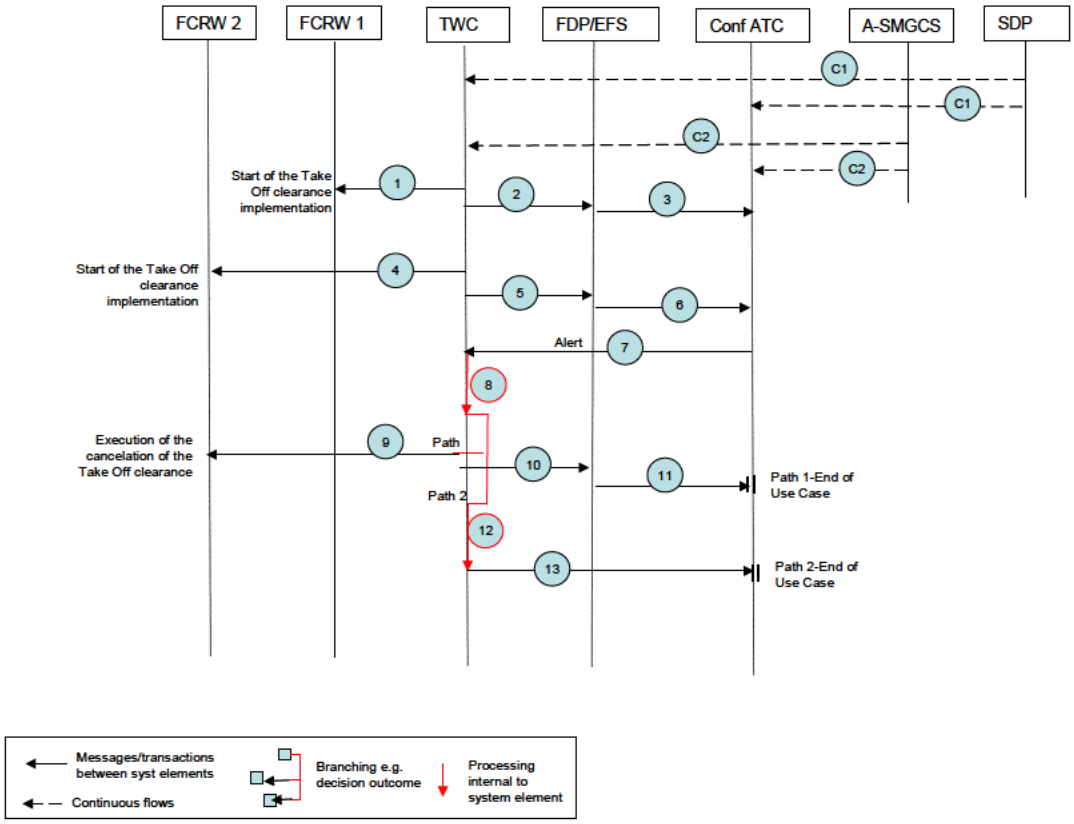


Figure 16 Thread analysis for Use Case#4: Take Off versus Take Off

Continuous flows	
C1	Surveillance Data Processing -SDP– passes continuous surveillance data of the aircraft 1 and 2 when lift off to TWC (A003) and to the conflicting ATC clearances System (ATC Conf)- (SR 006)
C2	A-SMGCS passes continuous position data of aircraft 1 and 2 taxiing on the runway protected area to TWC (A002) and to the conflicting ATC clearances System (ATC Conf)- (SR 005)

Actions	
1	Tower Runway Controller (TWC) provides the Take Off clearance to aircraft 1- (A001)
2	Tower Runway Controller (TWC) inputs the Take Off clearance into the electronic strip system (FDP/EFS) – (SR001)
3	The electronic strip system (FDP/EFS) provides the Take Off clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
4	Tower Runway Controller (TWC) provides the Take Off clearance to aircraft 2- (A001)
5	Tower Runway Controller (TWC) inputs the Take Off clearance into the electronic strip system (FDP/EFS)- (SR001)
6	The electronic strip system (FDP/EFS) provides the Take Off clearance to the conflicting ATC clearances System (Conf ATC)- (SR003)
7	The conflicting ATC clearances System (Conf ATC) detects the conflicting clearance between the two take off (SR019) and raise an alert (SR007) considering the surveillance data information (SR 005) and (SR 006)
8	Tower Runway Controller (TWC) reacts to the alert. [Path1: decide to cancel the clearance to aircraft 2 go to 9] [Path2: if TWC decide to accept the conflicting clearances go to 12]
9	Tower Runway Controller (TWC) react to the alert and cancel the Take Off clearance to aircraft 2 (A001)
10	Tower Runway Controller (TWC) cancels the clearance in the electronic strip system (FDP/EFS)- (SR022).

Actions	
11	The electronic strip system (FDP/EFS) inform the conflicting ATC clearances System (Conf ATC) about the cancelled Take Off clearance for aircraft 2 (SR023) [End of Use Case-Path 1]
12	Tower Runway Controller (TWC) accepts the conflicting clearances by assessing that the potential conflict will not lead to an actual runway conflict. (SR024)
13	Tower Runway Controller (TWC) accepts the conflicting clearances by informing the conflicting ATC clearances System (Conf ATC) - (SR025) [End of Use Case-Path 2]

3.4.3 Case of non-conflicting ATC clearances situations where an alert is unduly triggered (false alert).

Performance Requirement (PR 01) specifies that false alert rate of the Conflicting ATC Clearances System shall not be greater than 10^{-4} per movement. This requirement satisfies performance Objective PO 01.

A false alert is defined as the indication of a conflicting ATC Clearances situation when such situation has not occurred (result of false detection). A false alert would cause a conflicting ATC Clearances Alert.

The objective of this analysis consists in determining how the system architecture can be made to support this performance requirement. For that purpose, the method consists in apportioning the performance requirement (PR 01) into lower level requirements to elements of the system.

Fault tree is used to identify the causes of the false alerts and quantitative lower level requirements are the means to express requirements for elements/parts of the system that will be subject to more in-depth assessment in further lifecycle steps.

False alerts occur by definition at any time during the airport operations whereas no conflicting ATC clearances situation exists. The following causes leading to false alerts have been captured into the fault tree (see Figure 13):

- Conflicting ATC Clearances System detects a conflicting ATC clearances situation due to wrong or corrupted inputs which are either:
  - a wrong clearance entered by the ATCo (Atco_Wrg_Clr)[3] or,
  - a surveillance data corruption (Surv_Dat_Corupt) or,
  - a FDP/EFS data corruption (EFS_Dat_Corupt)
- Conflicting ATC Clearances System detects a conflicting ATC clearances situation without faulty inputs. This cause is linked to conf ATC tool corruption (Conf_ATC_Corupt).

Note: For details on wrong clearance, surveillance data corruption, EFS data corruption and Conf ATC corruption see chapter 3.6.1.

One Safety Issue is raised regarding the achievability of the false alert rate. A lower false alert rate (e.g. 5.0x10-4 per movement instead of $1.0x10^{-4}$ per movement) should be defined considering the human performance and equipment integrity/reliability requirements specified in chapter 3.6. The specified false alert rate ($1.0x10^{-4}$), when considering an airport with 800 movements per day, corresponds to less than one false alert per operational week (0.6) whereas a relaxed False Alert rate of 5.0x10-4 corresponds to less than three false alerts per operational week (2.8) which seems to be acceptable.

Safety Issue 2 (I002): It should be validated if the Conflicting ATC Clearances False Alert rate requirement could be relaxed from $1.0x10^{-4}$ per movement to $5.0x10^{-4}$ per movement. If not, it should be shown if improved human performance associated with wrong clearances and improved equipment integrity/reliability requirements could be achieved.

[3] Assumption is made that wrong clearance entered by ATCo leads to a conflicting ATC clearances situation in 10% of cases (Wrg_Clr_Conf_Sit)..

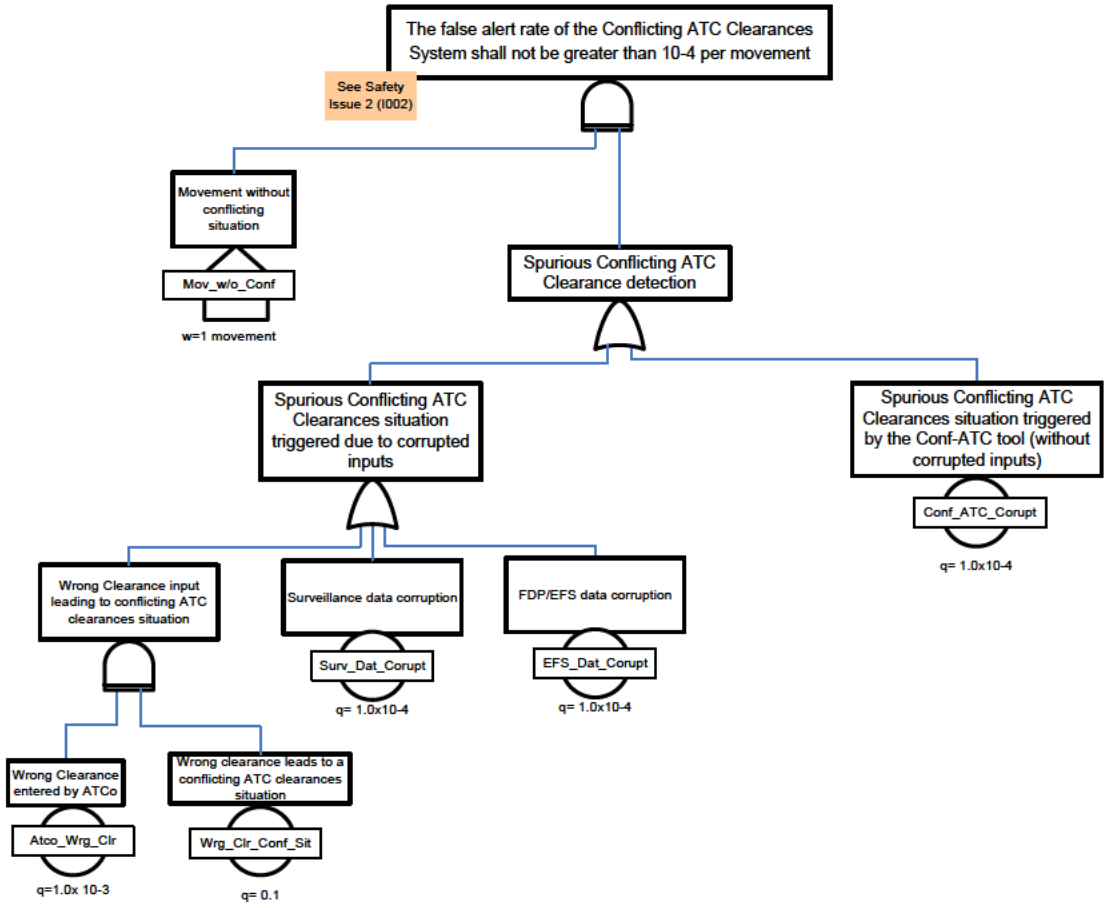


Figure 17 Conflicting ATC Clearances false alert fault tree

The following low level performance requirements have been derived from the above fault tree:

ID [SPR-level Model element]	Description
PR 01-01 [Conf ATC]	The conflicting ATC Clearances System shall not generate false alert with a probability greater than $1.0x10^{-4}$ per movement when no conflicting clearances and no corrupted inputs are present at the entry of the system.
PR 01-02 [A-SMGCS]	The conflicting ATC Clearances System shall not generate false alert with a probability greater than $1.0x10^{-4}$ per movement due to surveillance data corruption
PR 01-03 [FDP/EFS]	The conflicting ATC Clearances System shall not generate false alert with a probability greater than $1.0x10^{-4}$ per movement due to Electronic Flight Strip System data corruption
PR 01-04 [TWC] (See also SIR# 001 in section 3.6)	The Tower Runway Controller shall not enter wrong clearances in the System with a probability greater than $1.0x10^{-3}$. See Safety Issue 2 (I002).

Table 15 Performance Requirements

3.4.4 Effects on Safety Nets – Normal Operational Conditions

This section identifies how the effects on safety net will be evaluated. Further information about the evaluation of this system can be found in the V2 Validation Report [6] and the V3 Validation Plan [4].

3.4.5 Dynamic Analysis of the SPR-level Model – Normal Operational Conditions

The V3 validation shadow mode trials were performed by DFS at the airport environment in Hamburg with ten active and one retired ATCO between the 26th and 30th November 2012.

Table 16 shows the results of the Hamburg trials. For further information compare document V 3 Conflicting ATC Clearances Validation Report (VALR) D19 [10].

Validation Objective ID	Validation Objective Title	Exercise Results
OBJ-06.07.01-VALP-CATC.0003	Validation of "Line-Up versus Lineup"	Correct type of alert was trigged any time (altogether in 35 cases). No false alerts triggered. Positive feedback for two a/c receiving clearances on the same or adjacent holding points on the same RWY when multiple line-up is not authorised. Positive feedback for two a/c receiving clearances to line-up and are situated on the opposite ends of the same RWY. Positive feedback for two a/c receiving clearances to line-up and holding points are opposite on the same RWY No negative comments provided by experts.
OBJ-06.07.01-VALP-CATC.0004	Validation of "Line-up versus Cross	Correct type of alert was trigged any time (altogether in 18 cases). No false alerts triggered Positive feedback for an a/c and a mobile (a/c or vehicle) receiving clearances and holding points are opposing on the same RWY. No negative comments provided by experts. Conditional clearances were recommended.
OBJ-06.07.01-VALP-CATC.0005	Validation of "Line-up versus Enter"	Not tested but discussed with the ATCOs. Indifferent feedback for an a/c and a mobile (a/c or vehicle) receiving clearances and holding points are opposing on the same RWY
OBJ-06.07.01-VALP-CATC.0006	Validation of "Line-up versus Take-Off"	Correct type of alert was trigged any time (altogether in 27 cases). No false alerts triggered. Positive feedback for two a/c receiving Line-up and Take-Off clearances and a/c receiving the line-up clearance is in front

Validation Objective ID	Validation Objective Title	Exercise Results
		of the a/c receiving the Take-Off clearance on the same RWY. Positive feedback for two a/c receiving clearances and a/c are on the opposite ends of the same RWY
OBJ-06.07.01-VALP-CATC.0007	Validation of "Line-up versus Land"	Correct type of alert was trigged any time (altogether in 55 cases). No false alerts triggered. Positive feedback for two a/c receiving clearances and a/c receiving the Line-Up clearance is in front of the a/c receiving the landing clearance on the same RWY. Positive feedback for two a/c receiving clearances and a/c receiving clearances are on the opposite ends of the same RWY. No negative comments provided by experts.
OBJ-06.07.01-VALP-CATC.0008	Validation of "Cross versus Cross"	Correct type of alert was trigged any time (altogether in 4 cases). No false alerts triggered. Positive feedback for two mobiles (a/c or vehicle) both receiving clearances and holding points are opposing on the same RWY No negative feedback by experts.
OBJ-06.07.01-VALP-CATC.0009	Validation of "Cross versus Enter"	Not tested but positive feedback from ATCOs after discussion. OK for two mobiles (a/c or vehicle) receiving clearances and holding points are opposing on the same RWY.
OBJ-06.07.01-VALP-CATC.0002	Validation of "Enter versus Enter"	Not tested but positive feedback from ATCOs after discussion. OK for two mobiles (a/c or vehicle) both receiving clearances and holding points are opposing on the same RWY
OBJ-06.07.01-VALP-CATC.0011	Validation of "Cross versus Take- Off"	Correct type of alert was trigged any time (altogether in 25 cases). No false alerts triggered. Positive feedback for a mobile (a/c or vehicle) and an a/c receiving clearances and mobile receiving the Cross clearance is in front of the a/c receiving the Take-Off clearance on the same RWY. No negative comments provided by experts
OBJ-06.07.01-VALP-CATC.0012	Validation of "Enter versus Take-Off"	Not tested but positive feedback from ATCOs after discussion. OK for a mobile

Validation Objective ID	Validation Objective Title	Exercise Results
		(a/c or vehicle) and an a/c receiving clearances and mobile receiving the Enter clearance is in front of the a/c receiving the Take-Off clearance on the same RWY
OBJ-06.07.01-VALP-CATC.0013	Validation of "Cross versus Land"	Correct type of alert was trigged any time (altogether in 25 cases). No false alerts triggered. Positive feedback for a mobile (a/c or vehicle) and an a/c receiving clearances and mobile receiving the Cross clearance is in front of the a/c receiving the Landing clearance on the same RWY. No negative comments provided by experts
OBJ-06.07.01-VALP-CATC.0014	Validation of "Enter versus Land"	Not tested but positive feedback for a mobile (a/c or vehicle) and an a/c receiving clearances and mobile receiving the Enter clearance is in front of the a/c receiving the Landing clearance on the same RWY.
OBJ-06.07.01-VALP-CATC.0015	Validation of "Take-Off versus Take-Off"	Correct type of alert was trigged any time (altogether in 39 cases). No false alerts triggered Positive feedback for two a/c receiving clearances on the same RWY (e.g. Take-off RWY33 vs Take-off RWY33). Positive feedback for two a/c receiving clearances on different but converging RWYs and a/c trajectories are converging. Positive feedback for two a/c receiving clearances on different but intersecting RWYs and a/c trajectories are converging. Positive feedback for two a/c receiving clearances at opposite ends of the RWY (e.g. Take-off RWY33 vs Take-off RWY15). No negative comments provided by experts.
OBJ-06.07.01-VALP-CATC.0016	Validation of "Take-Off versus Land"	Correct type of alert was trigged any time (altogether in 96 cases). No false alerts triggered. Positive feedback for two a/c receiving clearances on the same RWY (e.g. Land RWY33 vs Take-off RWY33).

Validation Objective ID	Validation Objective Title	Exercise Results
		Positive feedback for two a/c receiving Land and Take-Off clearances on the same RWY but in opposite direction. Positive feedback for two a/c receiving clearances on different but intersecting RWYs and a/c trajectories are converging. Positive feedback for two a/c receiving at opposite ends of the RWY (e.g. Land RWY33 vs Take-off RWY15). No negative comments provided by experts.
OBJ-06.07.01-VALP-CATC.0017	Validation of "Land versus Land"	Correct type of alert was trigged any time (altogether in 55 cases). No false alerts triggered. Positive feedback for two a/c receiving clearances on the same RWY. Positive feedback for two a/c receiving clearances on different but intersecting RWYs and a/c trajectories are converging.). There was no negative feedback by experts.
OBJ-06.07.01-VALP-CATC.0018	Validation of generated Error Messages	Positive results in Questionnaire (several items) Safety net's proactive warnings highly appreciate by ATCOs (this was a recommendation in VALR [6]).
OBJ-06.07.01-VALP-CATC.0019	Validation of the audio alarm	Positive feedback. No negative comments about the audio alarms provided by experts.

Table 16: Exercise results of V3 Hamburg Trials

3.4.6 Additional Safety Requirements (functionality and performance) – Normal Operational Conditions

Table 17 below shows the additional safety requirements that have been revealed by the above analyses (in chapter 3.4.2 to 3.4.4)

ID [SPR-level Model element]	Description	Thread Action Number [Scenario # xx]
SR 022 [Conf ATC;TWC; FDP/EFS]	When the Tower Runway Controller decide to cancel a detected conflicting clearances, he/she shall inform the Electronic Flight Strip System (EFS) about this cancelation.	Use Case#1: Land Versus Line up Use Case#2: Land Versus Cross/Enter

ID [SPR-level Model element]	Description	Thread Action Number [Scenario # xx]
		Use Case#3: Line up Versus Line up Use Case#4: Take Off Versus Take Off
SR 023 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall inform the conflicting ATC clearances System about the cancelled clearance	Use Case#1: Land Versus Line up Use Case#2: Land Versus Cross/Enter Use Case#3: Line up Versus Line up Use Case#4: Take Off Versus Take Off
SR 024 [TWC]	The Tower Runway Controller shall accept the detected conflicting ATC clearances only when he/she has assessed that the potential conflict will not lead to an actual runway conflict.	Use Case#1: Land Versus Line up Use Case#2: Land Versus Cross/Enter Use Case#3: Line up Versus Line up Use Case#4: Take Off Versus Take Off
SR 025 [TWC; Conf ATC]	When a detected conflicting clearances is accepted by the Tower Runway Controller, he/she shall inform the conflicting ATC clearances System about this acceptation.	Use Case#1: Land Versus Line up Use Case#2: Land Versus Cross/Enter Use Case#3: Line up Versus Line up Use Case#4: Take Off Versus Take Off
SR 026 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System any clearance entered by the Tower Runway Controller within 0.5 second.	Use Case#1: Land Versus Line up Timing analysis
SR 027 [Conf ATC; TWC, FCRW, Driver]	When alerted by the Conflicting ATC Clearances System and where a corrective clearance is necessary to prevent the runway conflict, the Tower Runway Controller shall issue such corrective clearance as soon as practicable but at least within 3 seconds.	Use Case#1: Land Versus Line up Timing analysis
SR 028 [Conf ATC; TWC; FCRW; Driver]	When alerted by the Conflicting ATC Clearances System and where the last conflicting clearance entered shall be cancelled to prevent the runway conflict, the Tower Runway Controller shall cancel this clearance as soon as practicable but at least within 3 seconds	Use Case#1: Land Versus Line up Timing analysis
SR 029 [Conf ATC; TWC]	When alerted by the Conflicting ATC Clearances System and where the conflicting ATC clearances do not lead to a runway conflict, the Tower Runway Controller shall accept the conflicting ATC clearances as soon as practicable to cancel the alert but at least within 3 seconds.	Use Case#1: Land Versus Line up Timing analysis

Table 17: Additional SR from Thread Analysis – Normal Operational Conditions

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

There were no abnormal conditions identified.

3.5.1 Scenarios for Abnormal Conditions

NA

3.5.2 Derivation of Safety Requirements (Functionality and Performance) for Abnormal Conditions

NA

3.5.3 Thread Analysis of the SPR-level Model - Abnormal Conditions

NA

3.5.4 Effects on Safety Nets – Abnormal Operational Conditions

NA

3.5.5 Dynamic Analysis of the SPR-level Model – Abnormal Operational Conditions

NA

3.5.6 Additional Safety Requirements – Abnormal Operational Conditions

NA

3.6 Design Analysis – Case of Internal System Failures

The objective of this analysis consists in determining how the system architecture (encompassing people, procedures, equipment) designed for the conflicting ATC clearances approach operations can be made safe. For that purpose, the method consists in apportioning the Safety Objectives of each hazard into Safety Requirements to elements of the system.

Fault tree analysis is used to identify the causes of hazards and combinations thereof, accounting for safeguards already specified in the current standards and for any indication on their effectiveness.

Quantitative Safety Requirements are the means to express Safety Requirements for elements/parts of the system that will be subject to more in-depth safety assessment in further lifecycle steps.

The validity of the quantitative Safety Requirements is conditioned upon the validity of the Safety Objectives and on the accuracy of probabilistic data input to the fault trees.

3.6.1 Causal Analysis

For each system-generated hazard (see chapter 2.8.1), a top-down identification of internal system failures that could cause the hazard was conducted. The hazards are:

Hz 001 – Failure to detect the conflicting clearances with the conflicting ATC clearances System

Hz 002 – Detection of the conflicting ATC clearances but with incomplete information[4]

Hz 003 – Detection of the conflicting ATC clearances but with incorrect information[5]

Hz 004 – Failure to solve the potential runway conflict after the Conflicting ATC Clearances System detection

The purpose of the allocation of the causal analysis is to increase the detail of risk mitigation strategy through the identification of all possible causes. This way it will be possible to apportion the corresponding lower level Safety Objectives, and to identify the corresponding Safety Requirements allowing to meet the Safety Objective of the Operational Hazard under consideration.

A fault tree is produced for each selected hazard that provides a detailed overview of the contribution of all domains for a given hazard. Fault trees are elaborated by decomposing the hazard in a combination of failures (i.e. Basic Causes) linked by different gates: "AND" gates and "OR" gates. Once the fault tree is decomposed, the safety objective assigned to the hazard is apportioned among the failures identified and safety requirements are allocated. Mitigation Means (Safeguard) are proposed in order to reduce the likelihood of occurrence of the Operational Hazard. Mitigations which have been already identified during the design analysis in normal operation (sections 3.3 and 3.4) are labelled SR00x whereas new mitigations are labelled new SR00x.

3.6.1.1 Hz 001 - Failure to detect the conflicting clearances with the conflicting ATC clearances System

The conflicting ATC Clearances System does not detect the conflicting ATC Clearances situation. Basic causes for such failure have been captured in the Hz 001 Fault Tree (See Figure 14).

The Conflicting ATC Clearances is undetected by ATC if:

- The ATCo issue conflicting ATC clearances (Conf_Clr_Issued) and,
- The Conflicting ATC Clearances System does not detect the conflicting ATC clearances (see below) and
- The ATCo does not detect the conflicting ATC clearances with a faulty Conf-ATC-Tool (No_ATCo_Detect)

The Conflicting ATC Clearances System does not detect the conflicting ATC clearances if:

- Wrong, late or no clearance are entered in the System and this is not detected by ATCo (Atco_Wrg_Clr, Atco_Late_Clr, Atco_No_Clr) or,
- There is and undetected Electronic Flight Strip System loss (EFS_Und_Loss) or Electronic Flight Strip corrupted data (EFS_Dat_Corupt) or,
- There is and undetected Surveillance System loss (Surv_Und_Loss) or Surveillance corrupted data (Surv_Dat_Corupt) or,
- There is and undetected Conflicting ATC Clearances System loss (Conf_ATC_Und_Loss) or,
- The Conflicting ATC Clearances System misses the detection of the conflicting ATC clearances (Conf_ATC_Miss_Detect)

[4] This Hazard corresponds to an incomplete identification of the conflicting ATC Clearances situation
[5] This Hazard corresponds to an incorrect identification of the conflicting ATC Clearances situation

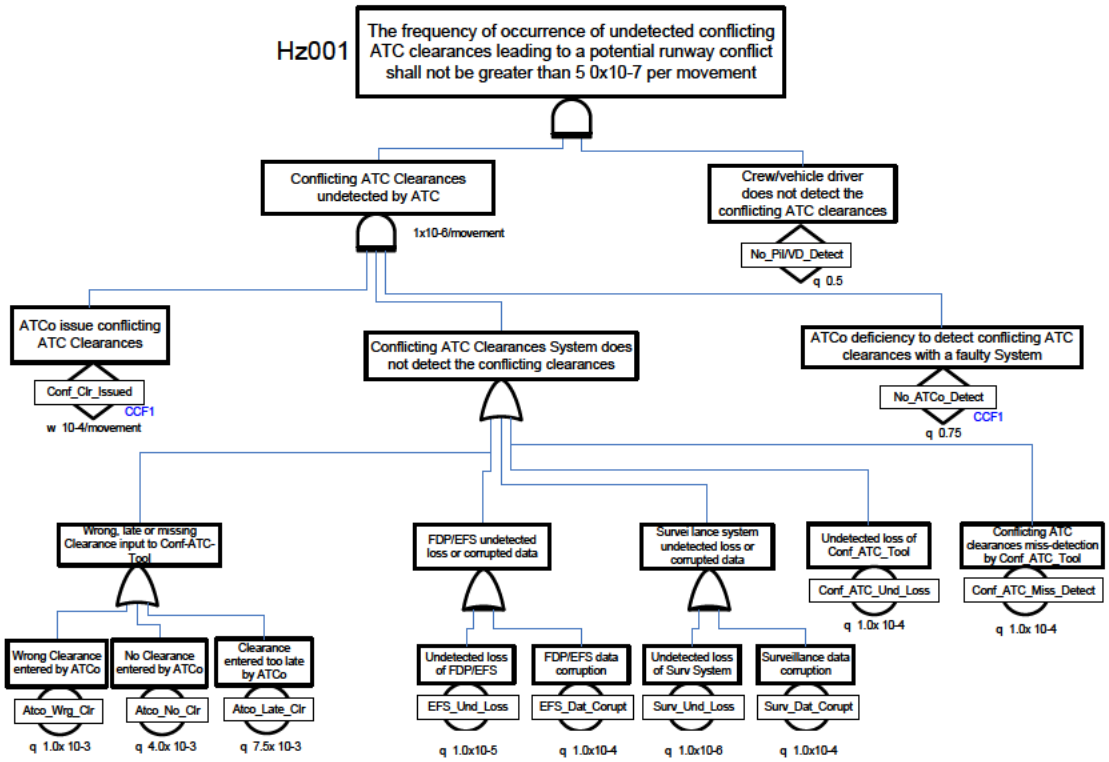


Figure 18 Hz 001 – Failure to detect the conflicting clearances with the conflicting ATC clearances system

The following table describes in more detail the basic causes for Hz 001 including the quantitative allocation aspect.

Hz 001 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
Atco_Wrg_Clr [TWC]	ATCo enters in the System a Clearance different from the one provided to aircraft/Vehicle	The wrong input is detected by ATCo and she/he monitors more carefully potential conflicts (New SR030).	Allocation is made for this cause considering an airport with 800 movements per day where ATCo will enter in the System less than one wrong clearance per op day (0.8). This leads to an allocation of: Q= 1.0x10-3 It is recommended to conduct a Human Reliability Assessment (HRA) to consolidate this allocation. →Safety Requirement to be derived (SIR#001).
Atco_No_Clr [TWC]	ATCo forgets to enter the Clearance in the System	The lack of input is detected by ATCo and she/he monitors more carefully potential conflicts (New SR030).	Allocation is made for this cause considering an airport with 800 movements per day where ATCo will not enter a clearance in the System more often than three times per op day. This leads to an allocation of: Q= 4.0x10-3 per movement It is recommended to conduct a Human Reliability Assessment (HRA) to consolidate this allocation. →Safety Requirement to be derived (SIR#002).
Atco_Late_Clr [TWC]	ATCo enters the Clearance in the System too late. Too late is defined by a clearance entered in the System more than 3 seconds after being provided it to the aircraft/vehicle via RT.	The late input is detected by ATCo and she/he monitors more carefully potential conflicts (New SR030).	Allocation is made for this cause considering an airport with 800 movements per day where ATCo will enter in the system no more than six delayed clearances per op day. This leads to an allocation of: Q= 7.5x10-3 per movement It is recommended to conduct a Human Reliability Assessment (HRA) to consolidate this allocation. →Safety Requirement to be derived (SIR#003).

Hz 001 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
EFS_Und_Loss [FDP/EFS]	Undetected FDP/EFS loss which lead to loss of communication between FDP/EFS and the Conflicting ATC Clearances System (e.g. loss of clearances)	ATCo detects the conflicting ATC clearances despite the faulty System (See No_Atco_Det_Fail below).	Allocation for this cause leads to a probability of Q= 1.0x10-5. It is estimated that such failure does not occur more often than 2 times per year and that such failure is detected following a period of several minutes (e.g. 3 minutes by ATCo detection following the inability to enter clearances, frozen screen, new flight plans not appearing,…). → No Safety Requirement derived (FDP/EFS failure rate should satisfy such reliability requirement)
EFS_Dat_Corupt [FDP/EFS]	FDP/EFS data corruption between FDP/EFS and the Conflicting ATC Clearances System (e.g. wrong clearances)	ATCo detects the conflicting ATC clearances despite the faulty System (See No_Atco_Det_Fail below).	Allocation for this cause leads to a probability of Q= 1.0x10-4 It is estimated that such failure does not occur more often than 1 time per year and that such failure is not detected. → No Safety Requirement derived (FDP/EFS failure rate should satisfy such integrity requirement)
Surv_Und_Loss [A-SMGCS]	Undetected Surveillance System loss which lead to loss of communication between A-SMGCS and the Conflicting ATC Clearances System (e.g. loss of mobile position)	ATCo detects the conflicting ATC clearances despite the faulty System (See No_Atco_Det_Fail below).	Allocation for this cause leads to a probability of Q= 1.0x10-6 It is estimated that such failure does not occur more often than 1 time per year and that such failure is detected following a period of 30 seconds by ATCo (mobiles frozen on the A-SMGCS display, no display refreshment, no new mobiles acquisition,…). → No Safety Requirement derived (A-SMGCS failure rate should satisfy such reliability requirement)
Surv_Dat_Corupt [A-SMGCS]	Surveillance data corruption between A-SMGCS and the Conflicting ATC Clearances System (e.g. erroneous mobile position)	ATCo detects the conflicting ATC clearances despite the faulty System (See No_Atco_Det_Fail below).	Allocation for this cause leads to a probability of Q= 1.0x10-4 It is estimated that such failure does not occur more often than 1 time per year and that such failure is not detected. → No Safety Requirement derived (A-SMGCS failure rate should satisfy such integrity requirement)

Hz 001 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
Conf_ATC_Und_Loss [Conf ATC]	Undetected Conflicting ATC Clearances System loss (e.g. No alarm triggered when conflicting ATC clearances are issued)	ATCo detects the conflicting ATC clearances despite the faulty System (See No_Atco_Det_Fail below).	A top-down allocation is made for this cause leading to a probability of 1.0x10-4. When considering this probability it means that such failure should not occur more often than 1 times per year and that such failure is detected in a period not greater than one hour. →Safety Requirement to be derived (SIR#004).
Conf_ATC_Miss_Detect [Conf ATC]	Miss-detection of the conflicting ATC clearances by the Conflicting ATC Clearances System (e.g. No alarm triggered when conflicting ATC clearances are issued)	ATCo detects the conflicting ATC clearances despite the faulty System (See No_Atco_Det_Fail below).	A top-down allocation is made for this cause leading to a probability of 1.0x10-4. →Safety Requirement to be derived (SIR#005).
Conf_Clr_Issued [TWC]	Basic cause required for such Hazard. Indeed ATCo shall provide conflicting ATC clearances to two mobiles.	NA	It is estimated that conflicting ATC Clearances occur once in every 10000 movements w= 1.0x10-4 per movement
No_Atco_Det_Fail	The ATCo does not detect the conflicting ATC clearances situation with a faulty System	NA	Assumption is made that ATCo does not detect the conflicting ATC clearances situation with a faulty System in 75% of cases: Q=0.75. See Common Cause Failure CCF 1 explanation in chapter 3.6.2.
No_Pil/VD_Detect [FCRW], [Vehicle Driver]	NA	Flight Crew or Pilot Driver detect conflicting ATC clearances with another mobile (e.g. through RT communication listening). This is a mitigation when conflicting ATC clearances are undetected by the ATC. →Assumption is made that Pilot/Vehicle Driver does not detect the conflicting ATC clearances situation in 50% of cases (No_Pil/VD_Detect)	NA

3.6.1.2 Hz 002 - Detection of the conflicting ATC clearances but with incomplete information

The conflicting ATC Clearances System detects the conflicting situation but the Alarm does not provide all the information like mobile identification, type of conflicting ATC clearances (e.g. Line Up versus Line Up), assigned runways or Accept/Cancel selection. Basic causes for such failure have been captured in the Hz 002 Fault Tree (See Figure 15).

Incomplete information relative to the Alarm triggered by the Conflicting ATC Clearances system are provided when there is either:

- No Mobile identification due to:
  - Surveillance corrupted data (Surv_Dat_Corupt) or
  - Conflicting ATC Clearances System corruption (Conf_ATC_Corupt) or
- No “Conflicting ATC Clearances” type displayed due to Conflicting ATC Clearances System corruption (Conf_ATC_Corupt)
- No “Assigned Runways” displayed due to:
  - Conflicting ATC Clearances System corruption (Conf_ATC_Corupt) or
  - Electronic Flight Strip corrupted data (EFS_Dat_Corupt)
- No “Accept/Cancel” selection displayed due to Conflicting ATC Clearances System corruption (Conf_ATC_Corupt)

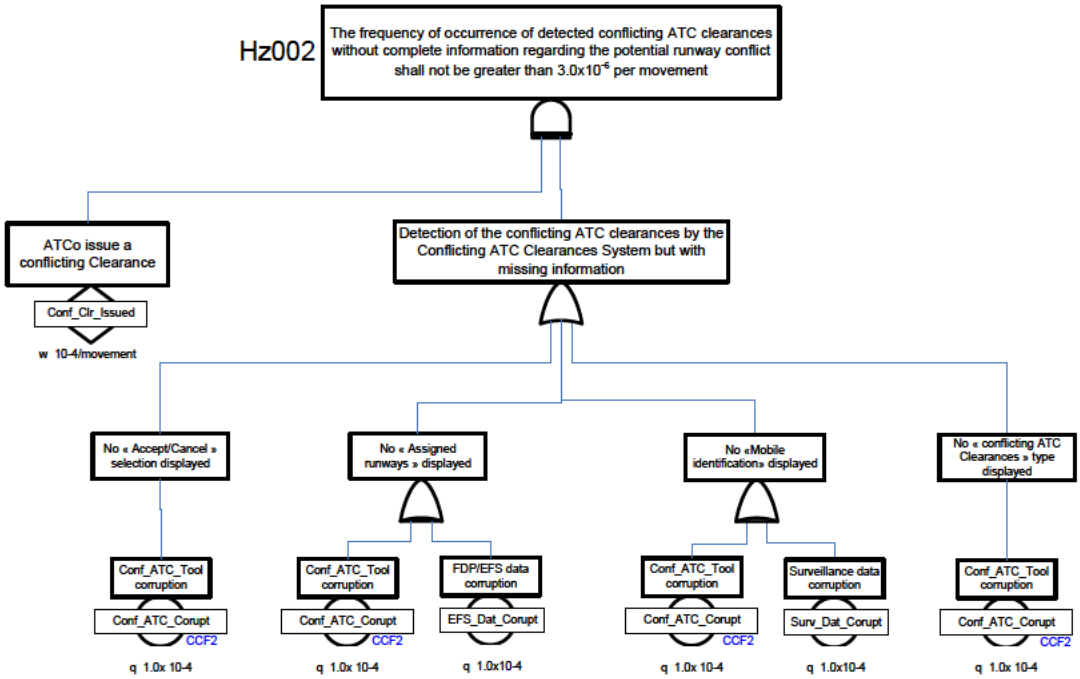


Figure 19 Hz 002 – Detection of the conflicting ATC clearances but with incomplete information

The following table describes in more detail the basic causes for Hz 002 including the quantitative allocation aspect.

Hz 002 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
EFS_Dat_Corupt [FDP/EFS]	FDP/EFS data corruption between FDP/EFS and the Conflicting ATC Clearances System which lead to no "Assigned Runways" information displayed.	ATCo detects that there is missing element and tries to determine the missing part. If the missing information is not timely determined he/she monitors more carefully potential conflicts (New SR031).	Allocation for this cause already made for Hz 001: Q= 1.0x10-4
Surv_Dat_Corupt [A-SMGCS]	Surveillance data corruption between A-SMGCS and the Conflicting ATC Clearances System which lead to no "Mobile Identification" information displayed.	ATCo detects that there is missing element and tries to determine the missing part. If the missing information is not timely determined he/she monitors more carefully potential conflicts (New SR031).	Allocation for this cause already made for Hz 001: Q= 1.0x10-4
Conf_ATC_Corrupt [Conf ATC]	Conflicting ATC Clearances System internal failure (e.g. Hw and/or Sw) which lead to following information not displayed: • "Mobile Identification" and/or, • "Assigned Runways" and/or • "Conflicting ATC Clearance type" and/or • "Accept/Cancel" selection	ATCo detects that there is missing element(s) and tries to determine the missing part(s). If the missing information is not timely determined he/she monitors more carefully potential conflicts (New SR031).	A top-down allocation is made for this cause, leading to a probability of 1.0x10-3. However as explained in chapter 3.6.2 for the CCF2 aspect and considering requirement already derived for Hz001 applicable to the Conficting ATC Clearances System, it leads to an allocation of : Q= 1.0x10-4. →Safety Requirement to be derived (SIR#006).
Conf_Clr_Issued [TWC]	Basic cause required for such Hazard. Indeed ATCo shall provide conflicting ATC clearances to two mobiles.	NA	It is estimated that conflicting ATC Clearances are provided once in every 10000 movements w= 1.0x10-4 per movement

3.6.1.3 Hz 003 - Detection of the conflicting ATC clearances but with incorrect information

The conflicting ATC Clearances System detects the conflicting situation but the Alarm provides incorrect information like erroneous mobile identification, erroneous type of conflicting ATC clearances or erroneous assigned runways. Basic causes for such failure have been captured in the Hz 003 Fault Tree (See Figure 16).

Incorrect information relative to the alarm triggered by the Conflicting ATC Clearances system are provided when there is either:

- Erroneous Mobile identification due to:
  - Surveillance corrupted data (Surv_Dat_Corupt) or
  - Conflicting ATC Clearances System corruption (Conf_ATC_Corupt) or
- Erroneous "Conflicting ATC Clearances" type displayed due to Conflicting ATC Clearances System corruption (Conf_ATC_Corupt)
- Erroneous "Assigned Runways" displayed due to:
  - Conflicting ATC Clearances System corruption (Conf_ATC_Corupt) or
  - Electronic Flight Strip corrupted data (EFS_Dat_Corupt)

- Erroneous “Accept/Cancel” selection displayed due to Conflicting ATC Clearances System corruption (Conf_ATC_Corupt)

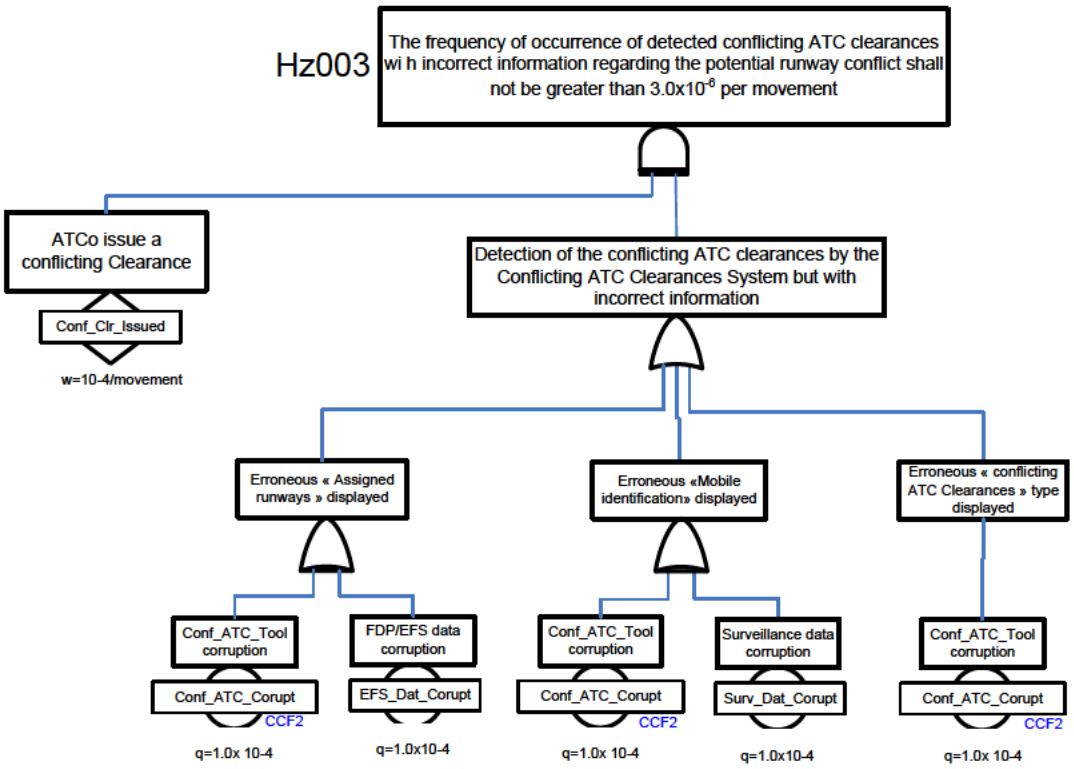


Figure 20 Hz 003 – Detection of the conflicting ATC clearances but with incorrect information

The following table describes in more detail the basic causes for Hz 003 including the quantitative allocation aspect.

Hz 003 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
EFS_Dat_Corupt [FDP/EFS]	FDP/EFS data corruption between FDP/EFS and the Conflicting ATC Clearances System which lead to erroneous "Assigned Runways" information	ATCo will detect that there is incorrect element based on his/her situational awareness of the current traffic on the runway protected area. Because an Alarm is triggered he/she monitors more carefully any potential conflicts (New SR032).	Allocation for this cause already made for Hz 001: Q= 1.0x10-4
Surv_Dat_Corupt [A-SMGCS]	Surveillance data corruption between A-SMGCS and the Conflicting ATC Clearances System which lead to erroneous "Mobile Identification"	ATCo will detect that there is incorrect element based on his/her situational awareness of the current traffic on the runway protected area. Because an Alarm is triggered he/she monitors more carefully any potential conflicts (New SR032).	Allocation for this cause already made for Hz 001: Q= 1.0x10-4
Conf_ATC_Corrupt [Conf ATC]	Conflicting ATC Clearances System internal failure (e.g. Hw and/or Sw) which lead the following erroneous information: • "Mobile Identification" and/or, • "Assigned Runways" and/or • "Conflicting ATC Clearance type" and/or	ATCo will detect that there is incorrect element(s) based on his/her situational awareness of the current traffic on the runway protected area. Because an Alarm is triggered he/she monitors more carefully any potential conflicts (New SR032).	Allocation for this cause already made for Hz 002: Q= 1.0x10-4 →Safety Requirement to be derived (SIR#007).
Conf_Clr_Issued [TWC]	Basic cause required for such Hazard. Indeed ATCo shall provide first conflicting ATC clearances to two mobiles.	NA	It is estimated that conflicting ATC Clearances are provided once in every 10000 movements w= 1.0x10-4 per movement

3.6.1.4 Hz 004 - Failure to solve the potential runway conflict after the Conflicting ATC Clearances System detection

The conflicting ATC Clearances System detects the conflicting situation but it is not possible to timely solve the situation. Basic causes for such failure have been captured in the Hz 004 Fault Tree (See Figure 17) and are the following:

- The ATCo does not handle/interpret the System Alarm properly:
  - By accepting the conflicting ATC clearances whereas he shouldn't accept it considering the conflicting situation or
  - by not cancelling the conflicting clearance with the mobile whereas the situation is conflicting or
  - by cancelling the conflicting clearance too late
- The Conflicting ATC Clearance System triggers the Alarm but considering mobile's conflict geometry/closing speed there is not sufficient time for ATCo and pilot/Vehicle driver to prevent the loss of separation.

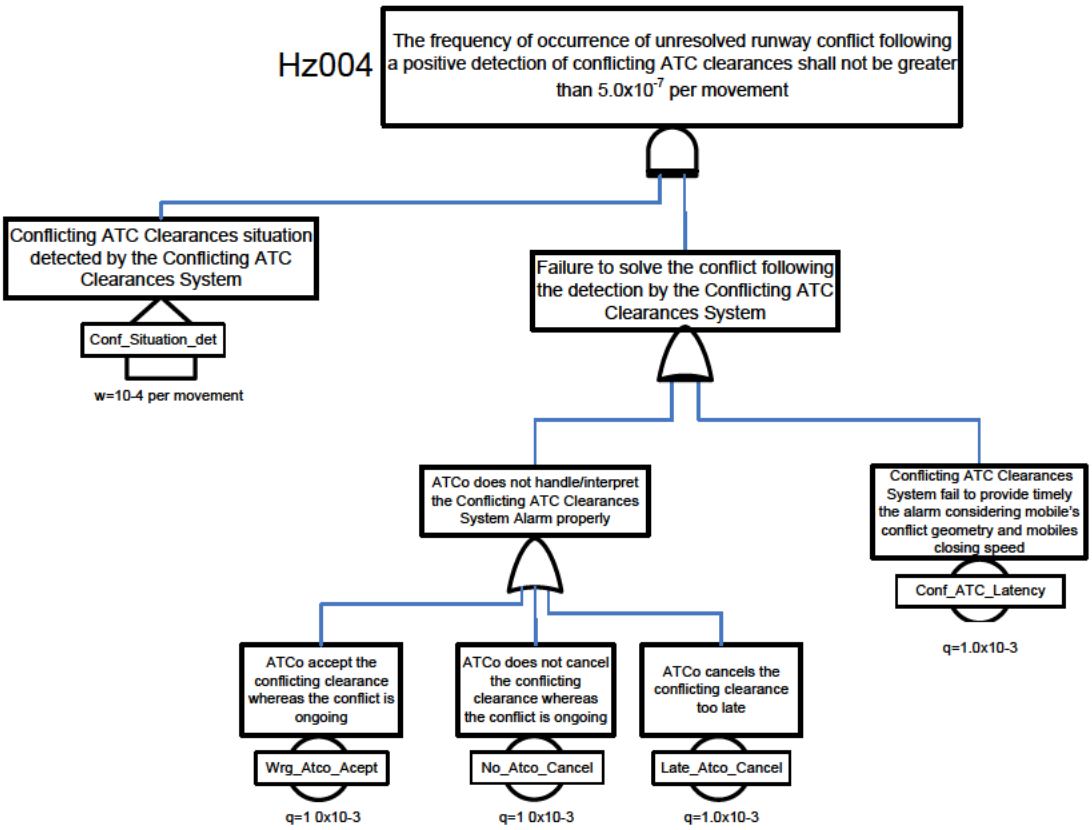


Figure 21 Hz 004 – Failure to solve the potential runway conflict after the conflicting ATC clearances System detection

The following table describes in more detail the basic causes for Hz 004 including the quantitative allocation aspect.

Hz 004 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
Wrg_Atco_Acept [TWC]	ATCo does not interpret the alarm properly and "Accept" the conflicting ATC clearances whereas he should not do it considering that there is an ongoing conflict	When alerted by the Conflicting ATC Clearances System, the Tower Runway Controller shall solve the potential runway conflict by issuing a corrective clearance or by confirming that the given clearances are acceptable (SR 011). The ATCo shall accept the detected conflicting ATC clearances only when he/she has assessed that the potential conflict will not lead to an actual runway conflict (SR 024).	Allocation is made for this cause leading to a probability of Q= 1.0x10-3. It is estimated that ATCo will wrongly accept the conflicting ATC Clearances situation once per 1000 actual conflicting situations. It is recommended to conduct a Human Reliability Assessment (HRA) to consolidate this allocation. →Safety Requirement to be derived (SIR#008).
No_Atco_Cancel [TWC]	ATCo does not "Cancel" the conflicting ATC clearances whereas he should do it considering that there is an ongoing conflict. "Cancel" means cancelling the clearance within the System and also with the mobile.	When alerted by the Conflicting ATC Clearances System, the Tower Runway Controller shall solve the potential runway conflict by issuing a corrective clearance or by confirming that the given clearances are acceptable (SR 011). When alerted by the Conflicting ATC Clearances System and where the last conflicting clearance entered shall be cancelled to prevent the runway conflict, the Tower Runway Controller shall cancel this clearance within 1 second (SR 028).	Allocation is made for this cause leading to a probability of Q= 1.0x10-3. It is estimated that ATCo will not cancel the conflicting ATC Clearances with the mobile once per 1000 actual conflicting situations. It is recommended to conduct a Human Reliability Assessment (HRA) to consolidate this allocation. →Safety Requirement to be derived (SIR#009).
Late_Atco_Cancel [TWC]	ATCo "Cancel" the conflicting ATC clearances too late whereas he should did it quickly considering the ongoing conflict. "Cancel" means cancelling the clearance within the System and also with the mobile.	When alerted by the Conflicting ATC Clearances System, the Tower Runway Controller shall solve the potential runway conflict by issuing a corrective clearance or by confirming that the given clearances are acceptable (SR 011). When alerted by the Conflicting ATC Clearances System and where the last conflicting clearance entered shall be cancelled to prevent the runway conflict, the Tower Runway Controller shall cancel this clearance within 1 second (SR 028).	Allocation is made for this cause leading to a probability of Q= 1.0x10-3. It is estimated that ATCo will cancel the conflicting ATC Clearances too late not more than once per 1000 actual conflicting situations. It is recommended to conduct a Human Reliability Assessment (HRA) to consolidate this allocation. →Safety Requirement to be derived (SIR#010).
Conf_ATC_Latency [Conf ATC]	Conflicting ATC Clearances System triggers the Alarm to the ATCo but considering mobile's conflict geometry and mobiles closing speed there is not sufficient time to solve the conflict before the	The following safety issue is raised: **Safety Issue 003** (I003): It should be verified for each type of conflicting ATC Clearances situation that, when an Alarm is triggered, ATCo and Flight Crew	Allocation is made for this cause leading to a probability of Q= 1.0x10-3. It is estimated, following a triggered Alarm, that in less than 0.1% of the cases the alarm will be triggered too late leading to the

Hz 004 Basic Causes [SPR-level Model Element]	Failure Causes description	Safeguards	Quantification
	loss of separation.	(or vehicle driver) have sufficient time to solve the conflict before it leads to loss of separation. This verification is essential when the geometry and the closing speed between mobiles necessitate to provide an Alarm as early as possible (e.g. Line Up vs Landing, Line Up vs Take Off, Cross/Enter vs Land, Cross/Enter vs Take Off).	impossibility for ATCo and Pilot/Vehicle to solve the conflict before loss of separation. →Safety Requirement to be derived (SIR#011).
Conf_Situation_Det [Conf ATC]	Basic cause required for such Hazard. Indeed the Conflicting ATC Clearances System should trigger an Alarm first.	NA	It is estimated that conflicting ATC Clearances are provided once in every 10000 movements and that the System detects the situation with a probability of 1. w= 1.0x10-4 per movement

3.6.2 Common Cause Analysis

Within Fault Trees, a number of internal fault tree dependencies have been identified in chapter 3.6.1 as follows:

*For Hazard 1, the controller which issued conflicting ATC clearances (Conf_Clr_Issued) might also not detect the conflicting situation with a faulty system (No_ATCo_Detect). Because this is the same person who makes these two tasks (CCF1), this leads to a high dependency. Without the consideration of this common cause, controller's failure to detect the conflicting situation is relatively low and around 25% but considering this CCF and using the THERP Dependency Modeling[6] it leads to a failure rate of 75%. Therefore the ATCo deficiency to detect conflicting ATC Clearances with a faulty System has a probability of 0.75 and not 0.25.

*For Hazards 2 and 3, the conflicting ATC Clearances tool failure (corruption) could lead to incomplete and/or incorrect identification of the conflicting ATC Clearances situation. Such failure is common (CCF2) for several identification elements (assigned runways, mobile identification, type of conflicting ATC clearances,…). A top down allocation for this failure element leads to a not very demanding allocation without considering this CCF (around 5.0x10-3). On the other hand and when considering Hazard 1, a similar failure leads to specify a probability of 1.0x10-4, it has been decided to allocate this same probability for Hazards 2 and 3 addressing de facto the common cause aspect by a far more demanding allocation (1.0x10-4 instead of 5.0x10-3).

Between Hazards, the bottom up assessment of causes shows that Conflicting ATC Clearances System internal failure could lead to all of the identified Hazards. Indeed an undetected loss of the Conflicting ATC Clearance System or miss detection could lead to Hz 001, a corrupted Conflicting ATC Clearance System could lead to incomplete information (Hz 002) or to corrupted information (Hz 003). For that reason and considering that Tower Controller will rely more and more on this tool, it has been verified if the allocation put on this tool is still acceptable. Considering that the probability associated to the integrity/reliability of this tool is similar to A-SMGCS or EFS, it has been decided not to require more demanding performances despite that such failure could affect more than one hazard.

In addition, loss of the Conflicting ATC Clearances System could lead to a higher workload of the Tower Controller in some cases. The reason for the higher workload is that the Controller has to identify and assess critical situation by themselves. However the detected loss of the ATC conflicting system could not lead to new hazardous situations because the controller will detect conflicting

[6] The THERP dependency modelling technique enables a conditional probability to be calculated based on the assessed level of dependence between the errors. Given two sequential tasks, A and B, where their probabilities of failure are P(A) and P(B) respectively, the conditional probability of task B, P (B/A) can be calculated for high dependency as P(B)=(1+P(B))/2

situations as before knowing that System has failed and based on the knowledge of the traffic (situational awareness).

3.6.3 Formalization of Mitigations

Considering the outcome of the causal analysis (see section 3.6.1) and more particularly the "Safeguards" identified in each table accompanying the hazards fault trees, Table 18 below formalize the system generated hazard mitigation (new SR00x) which have not been already captured during the design analysis in normal conditions.

Reference	Mitigation to System generated Hazards	Hazards
SR 030 [TWC]	The Tower Runway Controller shall verify that ATC clearances entered in the Electronic flight Strip System are the same than those provided to aircraft or vehicles.	Hz 001
SR 031 [TWC]	The Tower Runway Controller shall verify that the triggered alert provides complete information for the conflicting ATC clearances situation. If not, he/she should determine the missing part based on his/her situational awareness of the current traffic on the runway protected area.	Hz 002
SR 032 [TWC]	The Tower Runway Controller shall verify the triggered alert and detect, whenever practicable, incorrect Alarm information based on his/her situational awareness of the current traffic on the runway protected area.	Hz 003

Table 18 Additional success-case safety requirements to mitigate System generated Hazards

3.6.4 Safety Requirements (integrity/reliability)

Considering the outcome of the causal analysis (see chapter 3.6.1) the following Table 19 defines the safety requirements (integrity/reliability) to limit the frequency with which each identified system failure could be allowed to occur, taking into account of the mitigations, such that the residual risk is within the specified safety objectives.

Reference	Safety Requirement (Integrity/reliability)	Hazards
SIR#001 [TWC]	The number of wrong clearances input in the system shall not be greater than one per operational day	Hz 001
SIR#002 [TWC]	The probability that the Tower Runway Controller does not enter a clearance (when he/she should do it) in the Conflicting ATC Clearances System should be kept to a minimum.	Hz 001
SIR#003 [TWC]	The probability that the Tower Runway Controller enters a clearance in the Conflicting ATC Clearances System too late (more than 3 seconds after it has been provided to aircraft/vehicle) should be kept to a minimum.	Hz 001

Reference	Safety Requirement (Integrity/reliability)	Hazards
SIR#004 [Conf ATC]	The probability of an undetected loss of the Conflicting ATC Clearances System shall be less than $1.0x10^{-4}$ per movement.	Hz 001
SIR#005 [Conf ATC]	The probability of conflicting ATC clearances situation miss-detection by the Conflicting ATC Clearance System shall be less than $1.0x10^{-4}$ per movement.	Hz 001
SIR#006 [Conf ATC]	When an Alarm is triggered by the Conflicting ATC Clearance System, probability that incomplete identification of the conflicting situation is displayed to the Tower Runway Controller shall be less than $1.0x10^{-4}$ per movement.	Hz 002
SIR#007 [Conf ATC]	When an Alarm is triggered by the Conflicting ATC Clearance System, probability that incorrect identification of the conflicting situation is displayed to the Tower Runway Controller shall be less than $1.0x10^{-4}$ per movement.	Hz 003
SIR#008 [TWC]	The probability that the Tower Runway Controller does not handle/interpret the alarm properly by "Accepting" the conflicting ATC clearances whereas he shouldn't do it due to a potential conflict shall be less than $1.0x10^{-3}$.	Hz 004
SIR#009 [TWC]	The probability that the Tower Runway Controller does not handle/interpret the alarm properly by not "Cancelling" the conflicting clearance with the mobile whereas he should do it due to a potential conflict shall be less than 1.0x10-3.	Hz 004
SIR#010 [TWC]	The probability that the Tower Runway Controller does not handle/interpret the alarm properly by "Cancelling" the conflicting clearance with the mobile too late (within more than 1 second) shall be less than $1.0x10^{-3}$ per movement.	Hz 004
SIR#011 [Conf ATC]	When an alert is triggered by the Conflicting ATC Clearance System, the probability that Tower Runway Controller, flight Crew and Vehicle driver have not sufficient time to solve the conflict before an accident occurs should be kept to a minimum. See Safety Issue 3 (I003).	Hz 004
SIR#012 [Conf ATC]	The Tower Runway Controller shall be trained on the conflicting ATC system and on the importance of reacting promptly against a triggered alert to solve the conflicting ATC situation.	Hz 001, Hz 004

Table 19 Safety Requirements (Integrity/reliability)

3.7 Achievability of the SAfety Criteria

In section 2.10 of the present document the assessment of the achievability of the Safety Criteria defined in section 2.4 has been performed in through specifications safety objectives.

For both the given SAC (#1) it has been proven that the Conflicting ATC Clearances System is not itself designed to change the performances of others barriers of the SESAR AIM models where safety objectives are applied.

At SPR-design level, SOs have been mapped versus safety requirements for normal conditions and new functional and integrity/reliability safety requirements have defined and mapped to all previously identified hazards.

Therefore for each of the input SAC, the same conclusions can be derived as reported in sections 2.10.1 and 2.10.2, for SAC#1.

3.8 Realism of the SPR-level Design

3.8.1 Achievability of Safety Requirements / Assumptions

Some of the performance and integrity requirements could not be tested because no false alerts occurred during the validation exercise at Hamburg Airport.

3.8.2 "Testability" of Safety Requirements

The inherent problem of the V3 validation exercise at Hamburg Airport in November 2012 was that the controllers had to be forced to produce conflicting ATC clearances situations to test the concept. The tower runway controller was briefed to make an input to the EFS for an aircraft in accordance to a clearance by the real operational tower runway controller in the control tower. The validation supervisor identified a second aircraft and asked the tower runway controller in the validation scenario to give now a pre-defined conflicting ATC clearance. For example, the tower runway controller made a TOF clearance input on the EFS for an aircraft. After that he gave – on order of the validation supervisor – a CRS clearance to another aircraft on the same runway in front of the taking-off aircraft. This resulted in a TOF/CRS conflict.

This is the reason why it was not possible to testify realistic reaction time of the ATCOs.

3.9 Validation & Verification of the Safe Design at SPR Level

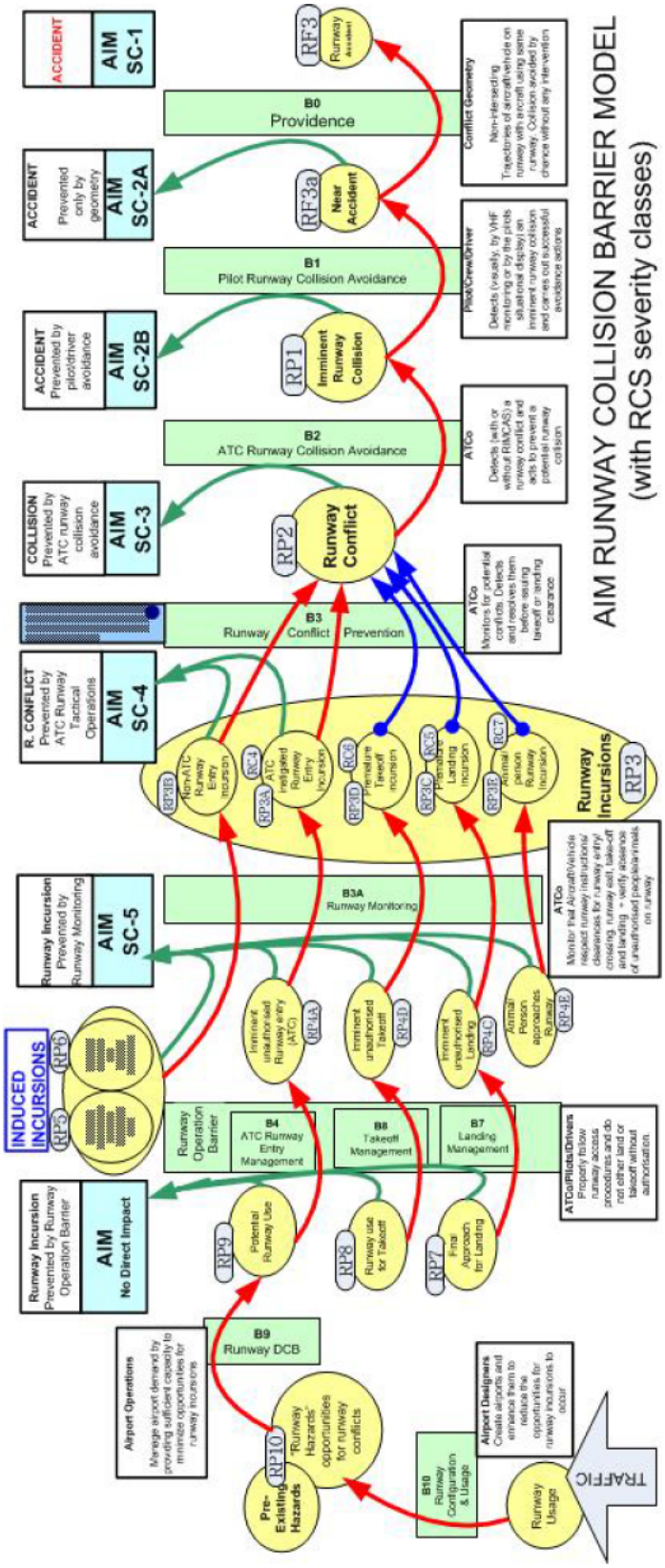
The consolidated lists of safety requirements are reported in Appendix C for the functional and integrity.

The testing of the alerts in real time simulations V2 and V3 shadow mode trials has already proved to be very positive. For further information compare the V 3 Conflicting ATC Clearances Validation Report (VALR) D19 [10].

4 Detailed Safe Design at Physical Level

The design of the system at physical level is out of scope of the present document version.

Appendix A AIM Runway Collision Barrier Model



Appendix B Consolidated List of Safety Objectives

B.1 Safety Objectives (Functionality and Performance)

ID	Description
SO 01	The Conflicting ATC Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area.
SO 02	The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the execution of the conflicting ATC clearances.
SO 03	The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area.
SO 04	The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area.
SO 05	The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (Aircraft or vehicles).
SO 06	The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.

B.2 Performance Objectives

ID	Description
PO 01	The false alert rate of the Conflicting ATC Clearances System shall not be greater than 10-4 per movement

B.3 Safety Objectives (Integrity)

ID	SO ID	Safety Objectives
Hz 001	SO 10	The frequency of occurrence of undetected conflicting ATC clearances leading to a potential runway conflict shall not be greater than $5.0x10^{-7}$ per movement
Hz 002	SO 11	The frequency of occurrence of detected conflicting ATC clearances without complete information regarding the potential runway conflict shall not be greater than $3.0x10^{-6}$ per flight per movement
Hz 003	SO 12	The frequency of occurrence of detected conflicting ATC clearances with incorrect information regarding the potential runway conflict shall not be greater than $3.0x10^{-6}$ per movement.
Hz 004	SO 13	The frequency of occurrence of unresolved runway conflict after a positive detection of conflicting ATC clearances shall not be greater than $5.0x10^{-7}$ per movement

Appendix C Consolidated List of Safety Requirements

C.1 Safety Requirements (Functionality and Performance)

ID [SPR-level Model Element]	Requirement
SR 001 [TWC; FDP/EFS]	Tower Runway Controller shall input in the Electronic Flight Strip System (EFS) the clearances given to the aircraft to line up, land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway
SR 002 [TWC; FDP/EFS]	Tower Runway Controller shall provide to the Electronic Flight Strip System (EFS) the aircraft information relative to the assigned Runway and the holding point
SR 003 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the clearances given to the aircraft to line up land on, take off from, hold short of, cross, taxi and backtrack on the runway
SR 004 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the aircraft information relative to the assigned Runway and the holding point
SR 005 [A/F; A-SMGCS; Conf ATC]	A-SMGCS shall provide to the Conflicting ATC Clearances System the position of aircraft taxiing on the runway protected area
SR 006 [A/F; SDP; Conf ATC]	Surveillance System shall provide to the Conflicting ATC Clearances System the position of aircraft in flight (landing and/or Take off)
SR 007 [Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide an alert to the Tower Runway Controller when clearances are given to two mobiles which, when executed, might lead to a runway conflict.
SR 008 [Conf ATC; RIMS; TWC]	The different alerts of the CATC system and RIMS shall be distinguishable for the Tower Runway Controller
SR 009 [TWC; FDP/EFS]	The Tower Runway Controller shall input clearances given to the aircraft/vehicles in the Electronic Flight Strip System (EFS) as soon as practicable and within less than 3 seconds.
SR 010 [FDP/EFS; Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide alert to the Tower Runway Controller not more than 1 second following the reception of the conflicting clearance from the Electronic Flight Strip System (EFS)
SR 011 [TWC; FCRW; Vehicle driver]	When alerted by the Conflicting ATC Clearances System, the Tower Runway Controller shall solve the potential runway conflict by issuing a corrective clearance or by confirming that the given clearances are acceptable.
SR 012 [TWC; FDP/EFS]	The Tower Runway Controller shall input in the Electronic Flight Strip System (EFS) the clearances given to the vehicle to enter or to cross the runway

SR 013 [TWC; FDP/EFS]	The Tower Runway Controller shall provide to the Electronic Flight Strip System (EFS) the vehicle information relative to the assigned Runway and the holding point
SR 014 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the clearances given to the vehicle to enter or to cross the runway
SR 015 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System the vehicle information relative to the assigned Runway and the holding point
SR 016 [Vehicle; A-SMGCS; Conf ATC]	A-SMGCS shall provide to the Conflicting ATC Clearances System the position of vehicles being driven on the runway protected area
SR 017 [Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide an alert to the Tower Runway Controller when clearances are given to an aircraft and a vehicle which, when executed, might lead to a runway conflict
SR 018 [Conf ATC; TWC]	The Conflicting ATC Clearances System shall provide an alert to the Tower Runway Controller when clearances are given to two vehicles which, when executed, might lead to a runway conflict
SR 019 [Conf ATC]	The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.9% per movement.
SR 020 [A-SMGCS]	The position accuracy of A-SMGCS shall be 7,5 meter on 95% confidence interval to support the Conflicting ATC Clearances System detection rate of 99,9% per movement.
SR 021 [SDP]	Surveillance system shall be sufficiently accurate to support the Conflicting ATC Clearances System detection rate of 99.9% per movement.
SR 022 [Conf ATC;TWC; FDP/EFS]	When the Tower Runway Controller decides to cancel a detected conflicting ATC clearance, he/she shall inform the Electronic Flight Strip System about this cancelation.
SR 023 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall inform the conflicting ATC clearances System about the cancelled clearance
SR 024 [TWC]	The Tower Runway Controller shall accept the detected conflicting ATC clearances only when he/she has assessed that the potential conflict will not lead to an actual runway conflict
SR 025 [TWC; Conf ATC]	When a detected conflicting clearance is accepted by the Tower Runway Controller, he/she shall inform the conflicting ATC clearances System about this acceptation.
SR 026 [FDP/EFS; Conf ATC]	The Electronic Flight Strip System (EFS) shall provide to the Conflicting ATC Clearances System any clearance entered by the Tower Runway Controller within 0.5 second.

SR 027 [Conf ATC; TWC, FCRW, Driver]	When alerted by the Conflicting ATC Clearances System and where a corrective clearance is necessary to prevent the runway conflict, the Tower Runway Controller shall issue such corrective clearance as soon as practicable but at least within 3 seconds
SR 028 [Conf ATC; TWC; FCRW; Driver]	When alerted by the Conflicting ATC Clearances System and where the last conflicting clearance entered shall be cancelled to prevent the runway conflict, the Tower Runway Controller shall cancel this clearance as soon as practicable but at least within 3 seconds
SR 029 [Conf ATC; TWC]	When alerted by the Conflicting ATC Clearances System and where the conflicting ATC clearances do not lead to a runway conflict, the Tower Runway Controller shall accept the conflicting ATC clearances as soon as practicable to cancel the alert but at least within 3 seconds.
SR 030 [TWC]	The Tower Runway Controller shall verify that ATC clearances entered in the Electronic flight Strip System are the same than those provided to aircraft or vehicles.
SR 031 [TWC]	The Tower Runway Controller shall verify that the triggered Alarm provides complete information for the conflicting ATC clearances situation. If not, he/she should determine the missing part based on his/her situational awareness of the current traffic on the runway protected area.
SR 032 [TWC]	The Tower Runway Controller shall verify the triggered Alarm and detect, whenever practicable, incorrect Alarm information based on his/her situational awareness of the current traffic on the runway protected area.

C.2 Performance Requirements

ID **[SPR-level Model Element]**	**Requirement**
PR 01 [Conf ATC; A-SMGCS; SDP; FDP/EFS; TWC]	The false alert rate of the Conflicting ATC Clearances System shall not be greater than 10^{-4} per movement.
PR 01-01 [Conf ATC]	The conflicting ATC Clearances System shall not generate false alert with a probability greater than $1.0x10^{-4}$ per movement when no conflicting clearances and no corrupted inputs are present at the entry of the system.
PR 01-02 [A-SMGCS]	The conflicting ATC Clearances System shall not generate false alert with a probability greater than $1.0x10^{-4}$ per movement due to surveillance data corruption
PR 01-03 [FDP/EFS]	The conflicting ATC Clearances System shall not generate false alert with a probability greater than $1.0x10^{-4}$ per movement due to Electronic Flight Strip System data corruption
PR 01-04 [TWC]	The Tower Runway Controller shall not enter wrong clearances in the System with a probability greater than $1.0x10^{-3}$. See Safety Issue 2 (I002).

C.3 Safety Requirements (Integrity)

Reference	Safety Requirement (Integrity/reliability)
SIR#001 [TWC]	The number of wrong clearances input in the system shall not be greater than one per operational day
SIR#002 [TWC]	The probability that the Tower Runway Controller does not enter a clearance (when he/she should do it) in the Conflicting ATC Clearances System should be keep to a minimum.
SIR#003 [TWC]	The probability that the Tower Runway Controller enters a clearance in the Conflicting ATC Clearances System too late (more than 3 seconds after it has been provided to aircraft/vehicle) should be keep to a minimum.
SIR#004 [Conf ATC]	The probability of an undetected loss of the Conflicting ATC Clearances System shall be less than $1.0x10^{-4}$ per movement.
SIR#005 [Conf ATC]	The probability of conflicting ATC clearances situation miss-detection by the Conflicting ATC Clearance System shall be less than $1.0x10^{-4}$ per movement.
SIR#006 [Conf ATC]	When an Alarm is triggered by the Conflicting ATC Clearance System, probability that incomplete identification of the conflicting situation is displayed to the Tower Runway Controller shall be less than $1.0x10^{-4}$ per movement.
SIR#007 [Conf ATC]	When an Alarm is triggered by the Conflicting ATC Clearance System, probability that incorrect identification of the conflicting situation is displayed to the Tower Runway Controller shall be less than $1.0x10^{-4}$ per movement.
SIR#008 [TWC]	The probability that the Tower Runway Controller does not handle/interpret the alarm properly by "Accepting" the conflicting ATC clearances whereas he shouldn't do it due to a potential conflict shall be less than $1.0x10^{-3}$.
SIR#009 [TWC]	The probability that the Tower Runway Controller does not handle/interpret the alarm properly by not "Cancelling" the conflicting clearance with the mobile whereas he should do it due to a potential conflict shall be less than $1.0x10^{-3}$.
SIR#010 [TWC]	The probability that the Tower Runway Controller does not handle/interpret the alarm properly by "Cancelling" the conflicting clearance with the mobile too late (within more than 1 second) shall be less than $1.0x10^{-3}$ per movement.
SIR#011 [Conf ATC]	When an alert is triggered by the Conflicting ATC Clearance System, the probability that Tower Runway Controller, flight Crew and Vehicle driver have not sufficient time to solve the conflict before an accident occurs should be kept to a minimum. See Safety Issue 3 (I003).
SIR#012 [Conf ATC]	The Tower Runway Controller shall be trained on the conflicting ATC system and on the importance of reacting promptly against a triggered alert to solve the conflicting ATC situation

Appendix D Assumptions, Safety Issues, Recommendations & Limitations

D.1 Assumptions log

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

ID / [SPR-level Model Element]	Assumptions	Validation
A 001 [TWC; FCRW]	The Tower Runway Controller gives clearances and instructions to aircraft to land on, take off from, go around, hold short of, cross, taxi and backtrack on the runway	ICAO Annex 11/ PANS-ATM
A 002 [A/F; A-SMGCS;TWC]	A-SMGCS provides to the Tower Runway Controller the position of aircraft taxiing on the runway protected area	??
A 003 [A/F; SDP;TWC]	The Surveillance System provides to the Tower Runway Controller the position of aircraft in flight	??
A 004 [A/F; RIMS;TWC]	RIMS provides alert to the Tower Runway Controller in case of aircraft runway conflicts	??
A 005 [TWC; Vehicle driver]	The Tower Runway Controller gives clearances and instructions to vehicles to enter or to cross the runway	ICAO Annex 11/ PANS-ATM
A 006 [Vehicle; A-SMGCS;TWC]	A-SMGCS provides to the Tower Runway Controller the position of vehicles being driven on the runway protected area	??
A 007 [Vehicle; RIMS;TWC]	RIMS provides alert to the Tower Runway Controller in case of vehicle runway conflicts	??

D.2 Safety Issues log

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

Ref	Safety issue	Resolution
I001	It shall be validated if the Tower Runway Controller could input clearance in the Electronic Flight Strip System (EFS) not more than 1 or 2 seconds after providing the clearance to the aircraft/vehicles. It is recalled that presently SR 009 requires 3 seconds.	???

I002	It should be validated if the Conflicting ATC Clearances False Alert rate requirement could be relaxed from 1.0x10-4 per movement to 5.0x10-4 per movement. If not, it should be shown if improved human performance associated with wrong clearances and improved equipment integrity/reliability requirements could be achieved.	
I003	It should be verified for each type of conflicting ATC Clearances situation that, when an Alarm is triggered, ATCo and Flight Crew (or vehicle driver) have sufficient time to solve the conflict before it leads to loss of separation. This verification is essential when the geometry and the closing speed between mobiles necessitate to provide an Alarm as early as possible (e.g. Line Up vs Landing, Line Up vs Take Off, Cross/Enter vs Land, Cross/Enter vs Take Off).	

D.3 Safety Recommendation

The following Safety Recommendations were raised during the safety assessment:

Ref	Safety Recommendation	Resolution
Rec001	It is recommended to make the verification of the conflicting ATC clearances before clearances are given to aircraft/vehicle in order to eliminate the need to give a new clearance in case of problem (predictive (What If tool) instead of reactive)	The prototype built by WP12.03.02 and WP12.05.02 tested at Hamburg Airport in 2012 provided a "What if" tool
Rec002		

D.4 Operational Limitations log

The following Operational Limitations were necessarily raised during the safety assessment:

Ref	Operational Limitations	Resolution
L001		
L002		

Appendix E OHA Table

Failure of service	Example of causes (logical level)	Operational Effects	Possible mitigation of effects of failure	Hazards generated at service level	Severity
SO#1: The Conflicting ATC Clearances System shall detect when two aircraft receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area					
Fail to detect the conflicting ATC clearances between two aircraft	• Conflicting ATC Clearances System unavailable • Electronic Flight Strip System unavailable • Corrupted Conflicting ATC Clearances System functionalities • Corrupted Electronic Flight Strip System functionalities • Tower Runway Controller does not enter the clearance(s) • Tower Runway Controller do not see/heard the conflicting ATC clearances alert • Corrupted/inaccurate Surveillance data inhibits the conflicting ATC clearances alert (erroneous exemption to the rule)	The two aircraft execute the conflicting clearances which lead potentially to a runway conflict	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot runway collision avoidance** Pilot detects (visually, by VHF monitoring or by the pilots situational display) an imminent runway collision and carries out successful avoidance action	**Hz 001. Failure to detect the conflicting clearances with the conflicting ATC clearances System**	SC3
Partially fail to detect the conflicting ATC clearances between two aircraft	• Corrupted Conflicting ATC Clearances System functionalities • Corrupted Electronic Flight Strip System	The two aircraft execute the conflicting clearances which lead potentially to a runway conflict but the Conflicting ATC Clearances System detects partly the problem because one of few information(s)	*** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she determines the missing identification and/or the missing type of conflicting ATC Clearances. It	**Hz 002. Detection of the conflicting ATC clearances but with incomplete information**	SC4

Failure of service	Example of causes (logical level)	Operational Effects	Possible mitigation of effects of failure	Hazards generated at service level	Severity
	functionalities ?? • Corrupted/inaccurate Surveillance data	are missing (e.g. alert without the aircraft identification or without the type of conflicting clearances: line up vs line up; T/O vs T/O;…)	leads to a slight increase of ATCo workload		
		The two aircraft execute the conflicting clearances which lead potentially to a runway conflict and the Conflicting ATC Clearances System detects partly the problem because one or few information(s) are incorrect (e.g. alert with a wrong aircraft identification or with a wrong type of conflicting clearances: line up vs line up instead of T/O vs T/O)	*** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she detects the incorrect identification or the incorrect type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	**Hz 003. detection of the conflicting ATC clearances but with incorrect information**	SC4
SO#2: The Conflicting ATC Clearances System shall timely trigger an interaction by the Tower Runway Controller to solve the potential runway conflict generated by the execution of the conflicting ATC clearances					
Fail to timely solve the potential runway conflict generated by the conflicting ATC clearances	• Tower Runway Controller do not see/heard timely the conflicting ATC clearances alert • Tower Runway Controller do not provide a new clearance in time to the aircraft/vehicle	Aircraft and/or vehicles have executed the conflicting clearances which lead potentially to a runway conflict	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot/driver runway collision avoidance** Pilot/driver detects (visually, by VHF monitoring or by the pilots/drivers situational display) an imminent runway collision and carries out successful avoidance action	**Hz 004. Failure to solve the potential runway conflict after the conflicting ATC clearances System detection**	SC3
SO#3: The Conflicting ATC Clearances System shall detect when an aircraft and a vehicle receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area					
Fail to detect the conflicting ATC clearances between the aircraft and the vehicle	• Conflicting ATC Clearances System unavailable • Electronic Flight Strip System unavailable • Corrupted Conflicting ATC Clearances System	Aircraft and vehicle execute the conflicting clearances which lead potentially to a runway conflict	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot/driver runway collision avoidance** Pilot/driver detects (visually, by VHF	**Hz 001. Failure to detect the conflicting clearances with the conflicting ATC clearances System**	SC3

Failure of service	Example of causes (logical level)	Operational Effects	Possible mitigation of effects of failure	Hazards generated at service level	Severity
	functionalities • Corrupted Electronic Flight Strip System functionalities • Tower Runway Controller does not enter the clearance(s) • Tower Runway Controller do not see/heard the conflicting ATC clearances alert • Corrupted Surveillance data inhibits the conflicting ATC clearances alert (erroneous exemption to the rule)		monitoring or by the pilots/drivers situational display) an imminent runway collision and carries out successful avoidance action		
Partially fail to detect the conflicting ATC clearances between the aircraft and the vehicle	• Corrupted Conflicting ATC Clearances System functionalities • Corrupted Electronic Flight Strip System functionalities ?? • Corrupted/inaccurate Surveillance data	Aircraft and vehicle execute the conflicting clearances which lead potentially to a runway conflict but the Conflicting ATC Clearances System detects partly the problem because one of few information(s) are missing (e.g. alert without the mobile identification or without the type of conflicting clearances: line up vs cross/enter; cross/enter vs T/O;…)	*** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she determines the missing identification and/or the missing type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	**Hz 002. Detection of the conflicting ATC clearances but with incomplete information**	SC4
		Aircraft and vehicle execute the conflicting clearances which lead potentially to a runway conflict and the Conflicting ATC Clearances System detects partly the problem because one or few information(s) are incorrect (e.g. alert with a wrong mobile identification or with a wrong type of conflicting clearances: line up	*** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she detects the incorrect identification or the incorrect type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	**Hz 003. detection of the conflicting ATC clearances but with incorrect information**	SC4

Failure of service	Example of causes (logical level)	Operational Effects	Possible mitigation of effects of failure	Hazards generated at service level	Severity
		vs line up instead of Line up vs cross/enter)			
SO#4: The Conflicting ATC Clearances System shall detect when two vehicles receive conflicting ATC clearances which lead potentially to a runway conflict inside the runway protected area					
Fail to detect the conflicting ATC clearances between the two vehicles	• Conflicting ATC Clearances System unavailable • Electronic Flight Strip System unavailable • Corrupted Conflicting ATC Clearances System functionalities • Corrupted Electronic Flight Strip System functionalities • Tower Runway Controller does not enter the clearance(s) • Tower Runway Controller do not see/heard the conflicting ATC clearances alert • Corrupted Surveillance data inhibits the conflicting ATC clearances alert (erroneous exemption to the rule)	The two vehicles execute the conflicting clearances which lead potentially to a runway conflict	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Driver runway collision avoidance** Driver detects (visually, by VHF/UHF monitoring or by the drivers situational display) an imminent runway collision and carries out successful avoidance action	**Hz 001. Failure to detect the conflicting clearances with the conflicting ATC clearances System**	SC3
Partially fail to detect the conflicting ATC clearances	• Corrupted Conflicting ATC Clearances System functionalities • Corrupted Electronic	The two vehicles execute the conflicting clearances which lead potentially to a runway conflict but the Conflicting ATC Clearances	***Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she determines the missing	**Hz 002. Detection of the conflicting ATC clearances but with incomplete**	SC4

Failure of service	Example of causes (logical level)	Operational Effects	Possible mitigation of effects of failure	Hazards generated at service level	Severity
between the two vehicles	Flight Strip System functionalities?? • Corrupted/inaccurate Surveillance data	System detects partly the problem because one of few information(s) are missing (e.g. alert without the vehicle identification or without the type of conflicting clearances: cross/enter vs cross/enter)	identification and/or the missing type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	**information**	
		The two vehicles execute the conflicting clearances which lead potentially to a runway conflict and the Conflicting ATC Clearances System detects partly the problem because one or few information(s) are incorrect (e.g. alert with a wrong vehicle identification or with a wrong type of conflicting clearances: line up vs cross/enter instead of cross/enter vs cross/enter)	*** Runway conflict Prevention** ATCo reacts to the partial alert and monitors for potential conflicts. He/she detects the incorrect identification or the incorrect type of conflicting ATC Clearances. It leads to a slight increase of ATCo workload	**Hz 003. detection of the conflicting ATC clearances but with incorrect information**	SC4
SO#5: The Conflicting ATC Clearances System shall be informed about clearances given to mobiles (Aircraft or vehicles)					
Fail to provide the clearances to the Conflicting ATC Clearances System: No Clearance provided	• Electronic Flight Strip System unavailable • Tower Runway Controller does not enter the clearance(s)	Aircraft/vehicles execute the clearances without the monitoring by the conflicting ATC clearances safety net	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot/driver runway collision avoidance** Pilot/driver detects (visually, by VHF monitoring or by the pilots/drivers situational display) an imminent runway collision and carries out successful avoidance action	**Hz 001. Failure to detect the conflicting clearances with the conflicting ATC clearances System**	SC3
Fail to provide the clearances to the Conflicting ATC Clearances System: Wrong clearance provided	• Corrupted Electronic Flight Strip System functionalities • Tower Runway Controller does not enter the correct clearance(s)	Aircraft/vehicles execute the clearances without the monitoring by the conflicting ATC clearances safety net	***ATC runway collision avoidance** ATCo detects (with or without RIMS) the runway conflict and acts to prevent a potential runway collision ***Pilot/driver runway collision avoidance** Pilot/driver detects (visually, by VHF	**Hz 001. Failure to detect the conflicting clearances with the conflicting ATC clearances System**	SC3

Failure of service	Example of causes (logical level)	Operational Effects	Possible mitigation of effects of failure	Hazards generated at service level	Severity
			monitoring or by the pilots/drivers situational display) an imminent runway collision and carries out successful avoidance action		
		Aircraft/vehicles execute the clearances in accordance with the clearances transmitted by voice. However if the wrong clearance entered in the Conflicting ATC Clearances System generate a false alert, there will be a slight degradation of the runway conflict prevention barrier due to an unduly increase of ATCo workload in order to address the erroneous detection of conflicting ATC clearances	ATCo reacts to the alert and monitors for potential conflicts. He/she detects that there is no conflict. Unduly increase of ATCo workload	**Not a Safety Hazard** but addressed by PO 1 "The Conflicting ATC Clearances System when verifying potential conflicting ATC Clearances shall not detect situations without risk of runway conflict (false alert) with a frequency of occurrence greater than 10^{-3} per movement.	--
SO#6: The Conflicting ATC Clearances System shall detect the conflicting ATC clearances with a probability of 99.5%					
Fail to detect the conflicting ATC clearances	**See results for SO#1, #3 and #4.**				

-END OF DOCUMENT -