Abstract: The CREDOS project aims to demonstrate the feasibility of a departure operation whereby the wake turbulence separations between successive aircraft are temporary suspended under specific (favourable) crosswind conditions. The present report is part of the CREDOS “Pre-implementation Safety Case” aiming at a safe introduction of the concept at European airports. In this report a Preliminary Safety Case (PSC) has been carried out according to the EUROCONTROL Air Navigation System Safety Assessment Methodology applied to the CREDOS Concept of Operations.
## Acronyms

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSP</td>
<td>Air Navigation Service Provider</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATM</td>
<td>Air Traffic Management</td>
</tr>
<tr>
<td>CND</td>
<td>Clearance Delivery</td>
</tr>
<tr>
<td>CREDOS</td>
<td>Crosswind Reduced Separations for Departure Operations</td>
</tr>
<tr>
<td>DEP</td>
<td>Departure Controller</td>
</tr>
<tr>
<td>DMAN</td>
<td>Departure Manager</td>
</tr>
<tr>
<td>EATMP</td>
<td>European Air Traffic Management Programme</td>
</tr>
<tr>
<td>ECAC</td>
<td>European Civil Aviation Conference</td>
</tr>
<tr>
<td>E-OCVM</td>
<td>European Operational Concept Validation Methodology</td>
</tr>
<tr>
<td>ESARR</td>
<td>Eurocontrol Safety Regulatory Requirements</td>
</tr>
<tr>
<td>EUROCONTROL</td>
<td>European Organisation for the Safety of Air Navigation</td>
</tr>
<tr>
<td>FHA</td>
<td>Functional Hazard Assessment</td>
</tr>
<tr>
<td>GND</td>
<td>Ground Controller</td>
</tr>
<tr>
<td>GSN</td>
<td>Goal Structured Notation</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>LIDAR</td>
<td>Light Detection and Ranging</td>
</tr>
<tr>
<td>METAR</td>
<td>Meteorological Terminal Aviation Routine Weather Report</td>
</tr>
<tr>
<td>NLR</td>
<td>Netherlands National Aerospace Laboratory</td>
</tr>
<tr>
<td>NM</td>
<td>Nautical Mile</td>
</tr>
<tr>
<td>PANS-ATM</td>
<td>Procedures for Air Navigation Services - Air Traffic Management</td>
</tr>
<tr>
<td>PSSA</td>
<td>Preliminary System Safety Assessment</td>
</tr>
<tr>
<td>PSC</td>
<td>Preliminary Safety Case</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>SAM</td>
<td>Safety Assessment Methodology</td>
</tr>
<tr>
<td>SID</td>
<td>Standard Instrument Departure</td>
</tr>
<tr>
<td>SO</td>
<td>Safety Objective</td>
</tr>
<tr>
<td>ST</td>
<td>Safety Target</td>
</tr>
<tr>
<td>SUP</td>
<td>ATC supervisor</td>
</tr>
<tr>
<td>TAF</td>
<td>Terminal Aerodrome Forecast</td>
</tr>
<tr>
<td>TMA</td>
<td>Terminal Maneouvring Area</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>TWR</td>
<td>Tower Controller</td>
</tr>
<tr>
<td>VESA</td>
<td>Vortex Encounter Severity Assessment</td>
</tr>
<tr>
<td>WVE</td>
<td>Wake Vortex Encounter</td>
</tr>
<tr>
<td>WT</td>
<td>Wake Turbulence</td>
</tr>
<tr>
<td>WTA</td>
<td>Wake Turbulence Advisory</td>
</tr>
<tr>
<td>WTSSAV</td>
<td>Wake Turbulence Separations Suspension Airspace Volume</td>
</tr>
</tbody>
</table>
Executive Summary

The CREDOS project aims to demonstrate the feasibility of a departure operation whereby the wake turbulence separations between successive aircraft are temporary suspended under favourable crosswind conditions. This study is part of the CREDOS “Pre-implementation Safety Case” aiming at safe introduction at European airports. A Preliminary Safety Case has been carried out according to the EUROCONTROL Air Navigation System Safety Assessment Methodology applied to the CREDOS Concept.

A generic safety argument for CREDOS is established. It covers the various parts of the life cycle including specification, implementation, transition to operational service, and operational service. As part of the CREDOS research activities mainly the safety argument for the specification phase is further elaborated. The CREDOS wake vortex safety management recommendations [15] provide guidelines to maintain an acceptable level of safety after CREDOS is introduced into operational service. The safety argument for the specification phase of CREDOS deals with intrinsic safety of the concept, design completeness, design correctness, design robustness, and mitigation of internal failures. A summary of the findings is provided in the following.

Intrinsic safety of the concept

The objective is to show that the CREDOS concept is intrinsically safe during normal operations, i.e. the concept is capable of satisfying the safety criteria, provided that a suitable system design could be produced and implemented. In view of the aim to provide a ‘generic’ concept of operations [10] with a high-level operational context and scope, it is concluded that both the operational context and the scope are sufficiently clearly described. However, in case of local implementation, specifics of the targeted air traffic control environment will have to be considered in more detail. A crosswind criterion is determined using both data collected during two measurement campaigns for wake vortices generated by departing aircraft at Frankfurt airport, as well as results from risk assessment simulations with an Airbus A-320 as follower aircraft. As long as only straight-out departures are considered, a crosswind threshold of about 7 to 8 knots seems to be necessary to sufficiently reduce the wake encounter risk in the area up to a height of 3000 ft when the separation is to be reduced down to 60 seconds. It has to be noted that for the risk assessment simulations no constraints on the SID combinations of leading and following aircraft are assumed. For additional guarantee that the encounter risk is significantly further reduced, the following aircraft may be starting on an upwind route. Risk assessment simulations explicitly taking this constraint into account should confirm this assumption. The key functionality of the
CREDOS concept is to reduce spacing between subsequent departing aircraft in case of favourable crosswind conditions. In the CREDOS concept, this spacing also depends on both the determination of the size of a Wake Turbulence Separations Suspension Airspace Volume (WTSSAV) and on the quality and reliability of a local validation campaign. As this dependency is complex, it is difficult to state that this key functionality has already been shown to be consistent with safety criteria.

**Design completeness**

The objective is to demonstrate that all necessary Safety Requirements have been specified, or assumptions have been stated, to cover all elements, in terms of system design, that are necessary to fully implement CREDOS operations. System boundaries are sufficiently clearly defined at this stage of the system development. The operational concept fully describes how the system intends to operate. High level concept safety validation objectives are specified and broken down further into initial safety validation requirements. It is observed that safety requirements on external elements have been specified in other documents. It is concluded that the CREDOS high-level system design is complete and can be used for further development and implementation.

**Design correctness**

The objective of this section is to show that the concept of the system design functions correctly and coherently under all normal environmental conditions. With respect to internal coherency, it is observed that internal coherency of the system design will be achieved if recommendations on controller familiarity, controller procedures, division of controller responsibilities, and SID compatibility are fully considered (see Section 5.2 for the full details). With respect to correct dynamic functioning of the design, it is observed that there are few issues to be resolved before implementation. The overall concept of CREDOS was well received by air traffic controllers participating in the real time simulations [11]. Four further recommendations should be taken into account for local implementations of CREDOS. These recommendations concern a) the mandatory transmission of wind information in take-off clearance for all aircraft in cases when a basic advisory tool is used, b) controller procedures that should be well defined in case of wrong turn (e.g. if departure controller acts first and then informs the runway controller or the other way around), c) refinement of the proposed phraseology for non-nominal events would need to be refined, and d) the use of a status indicator that takes into consideration the assigned SIDs for leading and following aircraft to assist the controller and reduce the risk of mistake. Overall, it is concluded that - provided that these recommendations are followed - there is sufficient evidence that the CREDOS system design as specified and simulated does function correctly and coherently.
**Design robustness**
The objective is to show that the application system design is robust against external abnormalities in the operational environment. Five external abnormalities are considered: aircraft failure (e.g. engine failure), voice communication system failure, degradation of surveillance systems information, meteorological systems information, and/or flight data/information. It is concluded that the CREDOS system can handle all these external abnormalities in a robust way, i.e. no risks that otherwise would not be present are induced. However, should a sudden decreased crosswind occur, the aircraft could be exposed to a higher wake encounter risk than anticipated. The use of wind monitoring systems up to about 2000 feet height is required for robustness.

**Mitigation of internal failures**
To show that all risks from internal failures are assessed and mitigated sufficiently, the EUROCONTROL Safety Assessment Methodology (SAM) is applied. A Functional Hazard Assessment (FHA) and a Preliminary System Safety Assessment (PSSA) are performed, using intermediate versions of the CREDOS Concept. The CREDOS FHA delivers six functional hazards with Safety Objectives. Using also the CREDOS PSSA fault trees, 22 safety requirements are derived: 5 for system elements, 13 for human operators and 4 for procedures. As a result of safety requirements set for human operators being too demanding and hence considered unachievable, the argument for mitigation of internal failures is not yet satisfied by the current FHA/PSSA. Revisiting FHA and PSSA is recommended, as both have been developed conservatively on the basis of 'worst case' outcomes. So far, little credit is given to mitigating factors present in the CREDOS concept. It is suggested to combine this revisiting effort with readdressing the FHA and PSSA on basis of the final concept of operations for CREDOS [10]. Readdressing the FHA and PSSA should then also better include performance of the CREDOS system and human performance aspects such as controller workload and radiotelephony usage.

**Overall conclusion**
Safety validation exercises specified in the CREDOS Validation strategy and plan are performed with the aim to gather the evidence to show that each of the five sub-arguments is satisfied. The main observations and findings are:

- Operational evaluation of the CREDOS concept and system design through real-time simulations seems to provide sufficient safety evidence regarding the arguments for system design completeness, correctness and robustness;

- Additional safety work will be needed to satisfy arguments for intrinsic safety and mitigation of internal failures (current safety requirements may be too demanding).
# Table of Contents

## Acronyms 3

### Executive Summary 5

### 1 Introduction 12

#### 1.1 Background and scope 12
#### 1.2 Objectives 12
#### 1.3 Approach and methodology 12
#### 1.4 Document structure 13

### 2 Safety argument 14

#### 2.1 Introduction 14
#### 2.2 Safety argument for the CREDOS specification 16

### 3 Intrinsic safety 20

#### 3.1 Introduction 20
#### 3.2 Operational context and scope 21
#### 3.3 Comparison with current operations 22
#### 3.4 Impact on the operational environment 24
#### 3.5 Key functionality 24
#### 3.6 Summary of findings 25

### 4 Design completeness 27

#### 4.1 Introduction 27
#### 4.2 System boundaries 28
#### 4.3 Concept of operations 31
#### 4.4 Concept safety validation requirements 33
#### 4.5 External elements 34
#### 4.6 Summary of findings 35

### 5 Design correctness 36

#### 5.1 Introduction 36
#### 5.2 Internal coherency of the system design and procedures 37
#### 5.3 Dynamic behaviour of the design 39
#### 5.4 Summary of findings 41
6 Design robustness 42
   6.1 Introduction 42
   6.2 Reaction to external failures 43
   6.3 Reaction to other abnormal conditions 44
   6.4 Summary of findings 45

7 Mitigation of internal failures 46
   7.1 Introduction 46
   7.2 Hazard identification 47
   7.3 Hazard severity 50
   7.4 Safety objectives 52
   7.5 Hazard cause identification 57
   7.6 Mitigations of the functional hazards 60
   7.7 Overview of safety requirements 61
   7.8 Summary of findings 63

8 Conclusions and recommendations 65

References 68
**List of Figures**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Safety approach [16]</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>Generic safety argument for CREDOS</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>Decomposition of Argument 1</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>Decomposition of Argument on Intrinsic Safety</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>Decomposition of Argument on Design Completeness (Arg1.2)</td>
<td>27</td>
</tr>
<tr>
<td>6</td>
<td>CREDOS initial functional system architecture</td>
<td>30</td>
</tr>
<tr>
<td>7</td>
<td>Decomposition of Argument on Design Correctness (Arg1.3)</td>
<td>36</td>
</tr>
<tr>
<td>8</td>
<td>Decomposition of Argument on Design Robustness (Arg1.4)</td>
<td>42</td>
</tr>
<tr>
<td>9</td>
<td>Decomposition of sub-argument on Mitigation of Internal Failures</td>
<td>46</td>
</tr>
<tr>
<td>10</td>
<td>Safety Objectives in Quantitative Method</td>
<td>53</td>
</tr>
</tbody>
</table>
List of Tables

Table 1 Human actors and their roles and responsibilities 32
Table 2 Main Hazards M1-M9 47
Table 3 Severity classes 50
Table 4 Effect and Severity Classification of CREDOS Operational Concept 51
Table 5 Maximum tolerable probability of Credos ATM direct contribution for severity classes 55
Table 6 Maximum allowable frequency of a specific hazard effect (ST) per take-off 56
Table 7 First indication of Safety Objective per hazard 56
Table 8 Safety requirements related to the CREDOS system 61
Table 9 Safety requirements related to human operators 61
Table 10 Safety requirements related to the CREDOS operation 62
1 Introduction

1.1 Background and scope

With the steady increase in air traffic, airports are under continuous pressure to increase aircraft handling capacity. One potential approach is to reduce the wake vortex separation distances between aircraft at take-off without compromising safety. The CREDOS project aims to develop and validate a new operation for Air Traffic Control (ATC) that would allow for a suspension of aircraft wake turbulence separation minima for departures in case of sufficient crosswind. The present separation of two minutes between departing aircraft (and even three minutes for aircraft departing behind the Airbus A380) is designed to defy problems aircraft may encounter in the wake of large aircraft. For airports with CREDOS in use, the aim is to reduce the time separation between aircraft departing at single runways to about 60 - 100 seconds in case of sufficient crosswind, while maintaining current ICAO radar distance separation rules (including the minimum wake turbulence radar separations for all aircraft types). As Preliminary Safety Case, this study addresses the specification stage of the concept of operations only. However, the Safety Argument, developed using Goal Structured Notation (GSN), does provide a framework for the development of assurance related to the implementation, transition and in-service stages of the CREDOS concept lifecycle.

1.2 Objectives

The main aim of this study is to provide sufficient evidence to support the argument that the CREDOS operation will be acceptably safe. The objectives of this report are to:

- Document the results of the CREDOS Safety Assessment, which is conducted in accordance with the EUROCONTROL Safety Assessment Methodology (SAM);
- Conclude whether the CREDOS concept, as proposed, is acceptably safe;
- State requirements necessary to ensure that the specification is acceptably safe;
- Provide a basis for ANSPs to produce their own local safety cases, if applicable.

1.3 Approach and methodology

The CREDOS safety assessment will be conducted in accordance with the EUROCONTROL Safety Assessment Methodology (SAM) [3]. The SAM provides a generic process to be applied whenever a change is proposed within the European ATM environment. Figure 1 shows the CREDOS safety approach steps. One should note that SAM also covers a System Safety Assessment (SSA), but as CREDOS only covers the specification stage of the concept of operations, a SSA is not (yet) included.
The initial safety process for a change to the ATM system consists of a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and the production of a Preliminary Safety Case (PSC). A FHA is a hazard and consequence identification and analysis activity. By understanding the impact of system failures, the level of safety required of the concept can be determined. The FHA for the CREDOS operation is documented in D4-6 [7]. The objective of the PSSA is to demonstrate whether the assessed system architecture can reasonably be expected to achieve the safety criteria. The PSSA is documented in D4-7 [8]. The results of the FHA/PSSA are then used as basis for the Preliminary Safety Case. This provides further guidance on the requirements which are necessary to ensure safe CREDOS operations.

1.4 Document structure

The structure of this document is as follows. Section 2 presents the high-level safety argument. The Safety Argument which forms the basis of the Preliminary Safety Case is then sub-divided into lower level arguments which are addressed in Sections 3 to 7 of this document. Section 3 deals with intrinsic safety of the CREDOS operation. Section 4 deals with design completeness. Section 5 addresses design correctness. Section 6 provides evidence to demonstrate that the system design is robust. Section 7 addresses the identification and mitigation of internal failures. Section 8 presents the conclusions of this study and recommendations.
2 Safety argument

2.1 Introduction

The Preliminary Safety Case is a crucial step in a timeline of safety activities throughout the whole life cycle from concept and system design specification to system implementation towards transition to operational service and resulting in a continued new and safe operation. This generic Preliminary Safety Case has to show that the CREDOS concept and system design have been specified to be acceptably safe. European national air traffic control centres will then have safety evidence to proceed with the next step, and develop their local Safety Cases for local implementations and transitions to operation services. The safety argument used in CREDOS is based on ICAO guidance on how to conduct safety activities for flight procedure design (reference 2, Section 7.7). The method has been implemented by EUROCONTROL in the European region (reference 2, Appendix C) and is illustrated in Figure 2. Note that Arg2, Arg3, and Arg4 are outside scope of the CREDOS project, which deals with the specification phase only. Therefore these Arguments are To Be Developed (TBD).

Figure 2 Generic safety argument for CREDOS

Cr001
Acceptably safe means that the application of the CREDOS operation will not degrade safety

Arg0
CREDOS is acceptably safe.

Arg1
CREDOS has been specified to be acceptably safe

Arg2
CREDOS has been implemented in accordance with the specification

Arg3
The transition to operational service of CREDOS will be acceptably safe

Arg4
The safety of CREDOS will continue to be demonstrated in operational service

Figure 3

TBD

TBD

TBD
The generic safety argument is based on a Safety Claim (Arg 0), which states that "CREDOS is acceptably safe". The safety criterion (Cr001) can be based on a relative or absolute approach. A relative approach considers CREDOS to be acceptably safe if it can be shown that the risk associated with CREDOS operational scenarios is not higher than for equivalent current operational scenarios. An absolute approach would consider CREDOS to be acceptably safe if it can be shown that the risk of an accident with CREDOS is not higher than a pre-defined maximum Target Level of Safety (TLS). In CREDOS a relative approach is taken, and Cr001 is specified as "Acceptably safe means that the application of the CREDOS operation will not degrade safety" [5].

The claim is decomposed into four principal Safety Arguments, using Goal Structured Notation (GSN) convention, stating that an argument is only considered true if each of the sub-arguments are shown to be true. The four principal arguments form the basis for a full safety case, as would be required before introducing the concept into service.

Arg1 asserts that CREDOS has been specified to be acceptably safe. This argument is satisfied through a comprehensive safety assessment carried out in accordance with the ESARR 4 [1] and the EUROCONTROL Safety Assessment Methodology [3].

Arg2 asserts that CREDOS has been implemented in accordance with the specification derived in Arg1. This argument would be supported by the results of a full System Safety Assessment (SSA), to be carried out by the responsible ANSP.

Arg3 asserts that the transition to operational service of CREDOS approaches will be acceptably safe. This argument requires evidence that all preparations for operational service have been completed. A local ANSP is responsible for satisfying this argument.

Arg4 asserts that the safety of CREDOS will continue to be shown in operational service. Monitoring of operational safety by the ANSP is important to validate the conclusions of the initial safety assessment required for Arg1, and to ensure that any issues that arise during service are duly investigated and appropriate corrective action are taken. Only by monitoring the performance of the concept in service can it be determined whether the above safety criteria above have been met.

For the purpose of this Preliminary Safety Case only Arg1 is covered in detail. This sub-argument is further outlined and explained in the following sub-section, where it should be noted that the five safety case validation exercises as specified in the CREDOS Validation strategy and plan [5] are related to five sub-arguments (intrinsic safety, design completeness, design correctness, design robustness, and internal failures mitigation) for which safety case validation evidence will need to be gathered.
2.2 Safety argument for the CREDOS specification

The composition of Arg1 is presented in Figure 3 below. It comprises 5 sub-arguments, which reflect the need to consider risk under fault free conditions and explicit failures. Note that - throughout this document - the colour green is used to indicate that a (sub)-argument is satisfied, whereas yellow is used in case a (sub-)argument is not satisfied. Additionally, one should be aware that derived safety requirements have to be realistic and shall be achievable in a typical operational environment. Arguments 1.1, 1.2, 1.3, 1.4 mainly deal with the so-called Success Approach to safety assessment whereas Argument 1.5 deals with the Failure Approach (i.e. assuming that there are failures of new system components or human errors of the air traffic controllers and pilots) [16].

Figure 3 Decomposition of Argument 1

Intrinsic Safety of the Concept (Arg1.1)

Arg1.1 asserts that the CREDOS concept is intrinsically safe during normal operations, i.e. the concept is capable of satisfying the safety criteria, provided that a suitable system design could be produced and implemented.
Parameters which make the concept intrinsically safe are to be identified. In this context, key issues are:

- To assess the Wake Vortex Encounter (WVE) risks related to different CREDOS scenarios with a validated aircraft wake vortex encounter simulation model. It will have to be shown that these WVE risks are not higher than for equivalent current scenarios, i.e. that when CREDOS is applied the strength of the encountered wake turbulence will - on average - not be in excess of the strength of the wake turbulence that would be encountered with the current distance based criteria. A preliminary minimum crosswind condition criterion, ensuring that only turbulences with acceptable strength remain in the runway vicinity during the departure phase, when the following departure is cleared for take-off, shall be assessed. This preliminary minimum crosswind condition criterion shall be refined and validated as well as the resulting departure separations in the initial climb and departure phase.

- To assess the required size of a Wake Turbulence Separations Suspension Airspace Volume (WTSSAV) through a local wake vortex measurement campaign.

**Design Completeness (Arg1.2)**

Arg1.2 asserts that the design of the system is complete and correct. The objective is to show that Safety Requirements cover everything necessary in terms of system design to fulfil the concept. The evidence will demonstrate traceability between the basic concept, safety criteria and safety requirements. This implies that:

- A detailed concept of operations that fully describes how the system is intended to operate is available,
- The boundaries of the system are clearly defined,
- Concept safety requirements have been specified for each of the system components,
- Safety requirements on, and assumptions about, CREDOS external elements are captured.

**Design Correctness (Arg1.3)**

Arg1.3 asserts that the system design functions correctly and coherently under all normal operating conditions. The main issue here is the internal coherency and dynamic behaviour of the system over the full range of (normal operating) conditions to which the system is expected to be subjected in its operational environment. In this context, a key issue will be to evaluate the system design, human roles and responsibilities, the nominal scenarios, and all the use cases during real time simulations. It will also have to be shown that any deviations from the nominal scenario
or inputs from the CREDOS system components will not lead to an unexpected and unwanted safety hazard. Therefore, it will be necessary to investigate the effect of CREDOS on air traffic controller workload (as compared to the current situation). Three human ATC operators (supervisor, runway controller, and departure controller) and the flight crew will be most affected by the CREDOS operations. The main role of the pilot will be to take-off in a safe way as soon as possible after receiving the take-off clearance. It will have to be shown that the flight crew can cope with the concept of reduced separation. The main function of the runway controller is to provide aircraft lined-up for take-off with a take-off clearance, such that minimum separation requirements are satisfied. It will have to be shown that the runway controller can cope with varying separation time between subsequent aircraft, based on CREDOS conditions being met or not. It will have to be evaluated whether the provided information (HMI) is sufficient and displayed in an appropriate way to perform ATCo task. It will have to be shown that the runway controller is able to cope with all relevant scenarios. It will have to be established to which extent the runway controller is able to monitor the correctness or incorrectness of the CREDOS advisory information. The main function of the departure controller is to monitor that aircraft after take-off are properly separated, in agreement with governing conditions (either CREDOS or ICAO mode), and to take the appropriate actions if separation minima are (or threatened to be) violated. It will have to be shown that the departure controller is able to cope with suspended separations for light/medium aircraft behind a heavy, and to control aircraft such that the ICAO wake turbulence radar separation minima can be maintained.

**Design Robustness (Arg1.4)**

Arg1.4 asserts that the system design is robust against external abnormalities in the operational environment. Evidence is required to show that the system can continue to operate effectively and that such abnormalities do not cause the system to behave in a way which could induce risks that would otherwise not have been present. This concerns, for instance, sudden changes of the wind conditions and increased dependency on the CREDOS advisory information as sole source for providing a take-off clearance.

**Mitigation of Internal Failures (Arg1.5)**

Arg1.5 asserts that all risks from internal system failure have been mitigated sufficiently. The internal behaviour of the system is addressed from two perspectives; how loss of functionality could reduce the effectiveness of the system and how anomalous behaviour of the system could induce a risk that otherwise would not arise.
Basically, this sub-argument is aimed at specification of safety objectives and safety requirements for the integrity of the CREDOS system design. Typically, a key output will be a list of functional hazards for which 'bow-tie safety assessment models' will be constructed. A Functional Hazard Assessment (FHA) is usually performed to investigate the severity of the functional hazards. A Preliminary System Safety Assessment (PSSA) is usually performed to investigate any possible failure scenario that could lead to a functional hazard. It is also necessary to show that all foreseeable hazards are considered and that the aggregate overall risk meets the safety criteria.
3 Intrinsic safety

3.1 Introduction

The objective of this Section is to assert that the CREDOS concept is intrinsically safe during normal operations, i.e. the concept is capable of satisfying the safety criteria, provided that a suitable system design could be produced and implemented. This will deal with the so-called Success Case, without any failures of the new CREDOS system components or human errors of air traffic controllers and pilots in the CREDOS operations. Parameters which make the concept intrinsically safe are to be identified. In particular the following questions need to be addressed:

- Are the operational context and scope clearly defined?
- Is the difference with existing operations assessed to be acceptable?
- Is the impact on the operational environment assessed to be acceptable?
- Are the key functionality and performance criteria identified?

The associated strategy for satisfying Argument 1.1 is illustrated in Figure 4 below.

![Figure 4 Decomposition of Argument on Intrinsic Safety](image)
3.2 Operational context and scope

The basic idea behind CREDOS is that, for departure, the wake turbulence separation criteria may be relaxed on the runway and for the first part of the climb path when the crosswind is such that the wake turbulence generated by the preceding aircraft should have been blown out of the departure track of the succeeding aircraft. The proposed concept aims for a reduction of the 2-minute start interval currently applied for HEAVY – MEDIUM, HEAVY – LIGHT or MEDIUM – LIGHT aircraft combinations through suspension of both the runway wake turbulence time separation and the wake turbulence radar separation during take-off and first climb, when enabled by favourable crosswind conditions. The intention is not to introduce any new intermediate wake turbulence separation, but to totally suspend it, when a predefined CREDOS wind level is present.

The CREDOS concept is based on today’s technical environment. It does not require advanced tools such as DMAN or electronic flight strips and it is focusing on how to accommodate a single independent runway used in a segregated mode for departures only. It can be applied whenever the CREDOS crosswind requirements are met.

**Upwind & Downwind SIDs**

It is proposed in the concept to introduce a distinction between upwind and downwind SIDs. Indeed, CREDOS is based on the lateral transport of the wake turbulence due to the crosswind, therefore, the suspension of the wake turbulence separation minima may only be applied if the departing route of the second aircraft does not go in the direction where the wake turbulence generated by the first one is blown (i.e. the SID of the second aircraft is not downwind from that of the leader). In other words, CREDOS may be applied only for an aircraft departing on the same or an upwind SID compared to the departure of a preceding heavier aircraft. In the context of CREDOS, the suspension of wake turbulence separation minima concerns only the runway and the first part of the climb phase. Consequently, it should be possible to unambiguously identify upwind and downwind SIDs, even in the case of sharp turns shortly after the end of the runway. In any case, if upwind and downwind SIDs cannot be clearly determined, the proposed concept must not be applied for those particular SIDs.

**A GO / NO-GO methodology**

The runway controller will be able to determine for every departure behind a heavier aircraft whether or not CREDOS criteria such as crosswind conditions or SID geometry are met. It is proposed that the runway controller applies a GO/NO-GO methodology per aircraft pair (see reference 10 for the full details about this methodology).
The concept is based on the assumption that:
• Departures are controlled in an ATS surveillance system environment;
• ATS surveillance system based separation minima are applied between aircraft after departure;
• The runway controller is responsible for establishing ATS surveillance system based separation minima for departing aircraft;
• A single independent runway is used in a segregated mode for departures only.

Beyond the scope of CREDOS are:
• The suspension of the 3-minute wake turbulence separation rule when departing from an intersection has not been considered in the concept.
• Super-HEAVY aircraft, such as the Airbus 380, have not been included.
• Crosswind concepts applied for mixed-mode runways, dependent runways and for arrivals have yet to be developed.

Further details regarding the potential operational environment, operational context and scope are contained in the CREDOS FHA [7] and PSSA [8]. In view of the aim of the CREDOS project to provide a ‘generic’ concept of operations [10] with a high-level operational context and scope, it can be concluded that the sub argument 1.2.1 is (at a high-level) sufficiently satisfied. However, in case of local implementation, the specifics of the targeted air traffic control environment will have to be considered in more detail. Furthermore, it is noted that the results of a European tower control survey showed considerable differences between airports (this may make it difficult to realize and implement one CREDOS system that can be deployed at more European airports).

### 3.3 Comparison with current operations

In this context, a key issue will be to assess the Wake Vortex Encounter (WVE) risks related to different CREDOS scenarios with a validated aircraft wake vortex encounter simulation model. It will have to be shown that these WVE risks are not higher than for equivalent current scenarios, i.e. that when CREDOS is applied the strength of the encountered wake turbulence on average will not exceed the strength of the wake turbulence that would be encountered with the current distance based criteria. A preliminary minimum crosswind condition criterion, ensuring that only turbulence with acceptable strength remains in the runway vicinity during the departure phase when the following departure is cleared for take-off, shall be assessed. This preliminary minimum crosswind condition criterion shall be refined and validated as well as the resulting departure separations in both the immediate climb and the departure phase.
The preliminary crosswind criterion has been determined using data collected during two measurement campaigns for wake vortices generated by departing aircraft at Frankfurt airport [12]. The meteorological conditions spanned a wide range in terms of wind conditions, turbulence, and temperature stratification. The crosswind thresholds obtained through data analysis depend on assumptions of the corridor width that has to be cleared from wake vortices to decrease separations. Assuming a corridor width of 200 m crosswinds of about 7 knots are necessary to clear the corridor for a 60 s separation from wake vortices on a 95 % probability. It was however noted that reducing aircraft separation from 120 s to 60 s under favourable crosswind conditions might result in less but more intense wake vortex encounters. Therefore this initial crosswind threshold values obtained were further analysed through risk assessment.

The aim of this risk assessment [13] is to analyze safety in terms of wake encounter risks related to introducing the CREDO concept. Advanced models for simulation of pilot reactions during wake encounters, rating of the severity of encounters based on measurable aircraft parameters as well as generation of realistic take-off trajectory distributions have been produced. These models were combined with wake vortex behaviour and weather models into two simulation platforms, WakeScene-D and VESA-D, which are able to provide wake encounter risk assessments for departure under varying weather conditions. The simulation results confirm the initial crosswind criteria obtained from pure evaluation of wake vortex measurements at Frankfurt airport [12]. As long as only straight-out departures are considered, a crosswind threshold of 8 knots seems to be necessary to sufficiently reduce the wake encounter risk up to a height of 3000 ft when the separation shall be reduced down to 60 s. For heights up to only 300 ft a crosswind of 6 knots or more is already sufficient. The main cause for the difference between low and high height was identified to be the change of wind direction with altitude [14]. For this specific wake encounter risk assessment no constraints on the SID combinations of leading and following aircraft have been assumed. It is expected that by additionally ensuring the following aircraft is starting on an upwind route, encounter risk would be significantly further reduced. Simulations explicitly taking this constraint into account should confirm this assumption. It also has to be noted that the risk assessment has been performed only for the case with an Airbus A320 as follower aircraft. Other aircraft have not yet been evaluated.

As the risk assessment simulations only cover the case with an Airbus A-320 as follower aircraft, it is not possible to conclude that the differences from existing operations are fully understood and reconciled with safety criteria. Further work is needed in order to show that the difference with existing operations is acceptable.
3.4 Impact on the operational environment

The CREDOS system will affect the operational environment in various ways:

- Aircraft take-off wake turbulence separation standards will be suspended in case of favourable (cross)wind conditions based on the new Go/No-Go methodology;
- ATC workload may increase due to CREDOS, as the air traffic controllers will have more aircraft to handle. ATC real time simulations have investigated this issue [11].
- The runway controller will be responsible for establishing the surveillance system based separation minima for departing aircraft (see Section 5.2, Argument 1.3.1).

A potential increase in ATC workload has been identified in reference 11 and needs to be further assessed. It can not yet be concluded that the impact of CREDOS on the operational environment is consistent with safety criteria as provided by ESARR 4 [1].

3.5 Key functionality

Key functionality of the CREDOS concept is to reduce spacing between subsequent departing aircraft in case of favourable crosswind conditions. Since the concept is wind dependent, such functionality requires that wind conditions have to be monitored in the aircraft departure area. Wind monitoring capabilities define a volume surrounding the aircraft departure path within which the wind can be monitored and therefore, within which the wake turbulence separation may be suspended. The size of this ‘Wake Turbulence Separations Suspension Airspace Volume’ (WTSSAV) is determined by the technical capability to evaluate the wind condition in the area surrounding the departure path. Most of the time technical issues will limit the WTSSAV height, which then also defines the altitude at which the transition from CREDOS reduced spacing to ICAO standard wake turbulence separations has to be obtained. In conclusion, the size of the WTSSAV has to be defined locally on the basis of local wind monitoring means (height of the airspace volume), of the aircraft’s accuracy to fly the local departure paths (width of the airspace volume) and of the structure of the SIDs. Note that the WTSSAV used in CREDOS real-time simulations [11] has been defined as being 2000 feet height and 300 m width (150 m to either runway side). The WTSSAV length could be about 3.2NM. It is computed on the basis of aircraft climb rate performance as well.

On the basis of the weather measurement data collected, the WTSSAV size, aircraft types, and traffic mix performances, the suitable CREDOS spacing is determined prior to deployment. The CREDOS aircraft wake turbulence separation reduction, in case of sufficient crosswind component, is determined by all of the following three conditions:

- the time between two departures, when the WT separation minima are suspended, has to be sufficient to ensure that the WT is transported out of the departure path;
• consecutive departing aircraft always have to be separated by at least the applicable ATS surveillance system based separation minima;
• transition from CREDOS spacing to ICAO standard wake turbulence separation has to be obtained prior to the point at which the succeeding aircraft reaches the upper boundary of the WTSSAV.

The dependency of the resulting CREDOS spacing on the determination of the WTSSAV size, together with the quality and reliability of the local validation campaign is quite complex. At this stage it is therefore difficult to state that the key functionality has been shown to be consistent with safety criteria, i.e. that CREDOS would not degrade safety. Further work will be needed to fulfill argument 1.1.4, especially since the current approach to determine the size of the WTSSAV (see references 10 and 11) suggests that there will be different WTSSAV depending on the fleet at the airport.

3.6 Summary of findings

The objective of this Section is to show that the CREDOS concept is intrinsically safe during normal operations, i.e. without any CREDOS system failures or human errors. For this purpose four sub-arguments have been considered:

a) operational context and scope,
b) comparison with current operations,
c) impact on the operational environment, and
d) key functionality.

In view of the aim to provide a generic concept of operations [10] with a high-level operational context and scope, it is concluded that the operational context and scope have been sufficiently clearly described. However, for local implementation, specifics of the targeted air traffic control environment will have to be considered in more detail.

A potential increase in ATC workload has been identified in reference 11 and needs to be further assessed. It can not yet be concluded that the impact of CREDOS on the operational environment is consistent with safety criteria as provided by ESARR 4 [1].

A preliminary crosswind criterion has been determined using data collected during two measurement campaigns for wake vortices generated by departing aircraft at Frankfurt airport [12]. Assuming a corridor width of 200 m crosswinds of about 7 knots are necessary to clear the corridor for a 60 s separation from wake vortices on a 95 % probability. Risk assessment simulation results confirm this initial crosswind criteria obtained [13, 14]. As long as only straight-out departures are considered, a crosswind
threshold of 8 knots seems to be necessary to sufficiently reduce the wake encounter risk up to an altitude of 3000 ft when the separation shall be reduced down to 60s. For altitudes up to only 300 ft a crosswind of 6 knots or more is already sufficient. It has to be noted for this specific wake encounter risk assessment no constraints on the SID combinations of leading and following aircraft have been assumed. It is to be expected that by additionally ensuring the following aircraft is starting on an upwind route (see also section 3.2), the encounter risk would significantly be further reduced. Simulations explicitly taking this constraint into account should confirm this assumption. It also has to be noted that the risk assessment has been performed only for the case with an Airbus A320 as follower aircraft. Other aircraft have not yet been evaluated.

Key functionality of the CREDOS concept is to reduce spacing between subsequent departing aircraft in case of favourable crosswind conditions. As the dependence of the resulting spacing on both the determination of the WTSSAV size and the quality and reliability of the local validation campaign is quite complex, it is difficult to state that this identified key functionality has already been shown to be consistent with safety criteria.
4 Design completeness

4.1 Introduction

The objective of this section is to demonstrate that all necessary Safety Requirements have been specified, or assumptions have been stated, to cover all elements, in terms of system design, that are necessary to fully implement CREDOS operations. Argument 1.2 asserts that the design of the system is complete.

The strategy for satisfying Arg1.2 is to provide evidence that the following lower-level arguments are true:

- Arg1.2.1 The boundaries of the system are clearly defined.
- Arg1.2.2 The Concept of Operations fully describes how the system is intended to operate.
- Arg1.2.3 The concept safety validation objectives have been specified.
- Arg1.2.4 All safety requirements on external elements of the system have been captured.

Figure 5 Decomposition of Argument on Design Completeness (Arg1.2)
4.2 System boundaries

CREDOS is to be used for departing pairs of aircraft. Forming the CREDOS sequence of an aircraft can be started as early as when an aircraft request for start-up. The application of CREDOS separation suspension covers the initial climb segment up to the altitude where standard separation for approach radar control is to be obtained. This altitude will depend on the technical limitations of the airport wind measurement equipment. The initial concept is based on today’s environment (i.e. current wind measurement and prediction technology). It is assumed that reliability and integrity requirements can therefore be met with currently available technology and equipment. The scope of the CREDOS operation ends in the departure controller responsibility.

The CREDOS concept is focusing on how to accommodate a single independent runway used in a segregated mode for departures only, i.e. mixed mode operations are out of scope. For CREDOS a minimum visibility and cloud base may be required. Irrespective of this requirement on meteorological conditions, the safety study will consider instrument departures only for a single runway. However, CREDOS can be applied between any two consecutive departing aircraft if all CREDOS requirements are met. In the concept description, the departure sequence management is considered as either manual or automated (by the use of DMAN). DMAN is not required for CREDOS but would be beneficial in order to optimize the sequence.

CREDOS will require five new system components, which will interface with existing ATC systems. The 5 new CREDOS system components are described in the following:

**CREDOS Separation Mode Advisory**
The separation mode advisory provides advice concerning the possible suspension of wake turbulence separations, i.e. CREDOS wind conditions available or not available, including the expected time for future mode transitions (opportune activation or deactivation of the CREDOS system) for each runway. Such advice is based on meteorological forecast information, e.g. wind profile pictures, METAR, TAF.

**CREDOS Departure Planning Advisory**
The departure planning advisory provides up-to-date departure planning information and advisory on how to optimise the departure sequence while CREDOS wake turbulence separation suspension is applied, possibly using a Departure Manager (DMAN). The existing paper or electronic strips are used in order to highlight CREDOS information to each controller in the aircraft departure flow.
Items that can be highlighted are:

- weight category;
- holding point or intersection to be used;
- flight crew informed about CREDOS;
- acceptance of suspended separation by the flight crew;
- applicable SID is upwind or downwind;
- expected time of departure.

**CREDOS SID Wind Forecast Service**

The forecast service estimates the expected wind conditions for the departing aircraft along the applicable SID up to a certain altitude. No HMI is foreseen; the output data is used for the CREDOS Go/No-go indicator.

**CREDOS SID Wind Monitoring Service**

The wind monitoring service screens the wind conditions as experienced by the departing aircraft along the SID, up to a certain altitude. Information regarding the actual aircraft positions is derived from surveillance radars and possibly flight data processing. The monitoring information is updated in short intervals (e.g. 1 or 2 minutes). The output data is used for the CREDOS Go/No-go indicator, which is planned to be incorporated in existing ATC Human Machine Interfaces radar displays.

**CREDOS Go/No-Go Advisory**

The Go/No-go advisory indicates whether wake turbulence separation suspension (CREDOS mode) is possible for the next take-off. If CREDOS is available, a GO indication will appear on the HMI display; if CREDOS is not available a NO-GO indication appears. The HMI display should also include the actual nowcasted wind, enabling the runway controller to cross check whether the crosswind conditions for CREDOS are still met at take-off clearance time. Based on wind nowcast data and data from the SID Wind Forecast Service and Departure Planning Advisor, it provides:

- A Go/No-go indication for aircraft ready to depart (i.e. with or without CREDOS).
- Actual surface wind for cross checking Go/No-go indication against crosswind.

Pre-requisites for the use of the Go/No-go Alerting Advisory are e.g.:

- Status of all CREDOS system components is set to "CREDOS active and OK".
- Sufficient quality of the input wind nowcasting data;
- No significant difference between CREDOS forecasting and monitoring information;
- No failure of one or more of the CREDOS systems components.
Figure 6 shows how the newly foreseen CREDOS system components, as defined in the CREDOS PSSA [8], are foreseen to interact with the existing ATM systems.

It can be concluded that the boundaries of the CREDOS system, including the interactions with the external environment, are described clearly and in sufficient detail for the 'specification phase'. For the 'implementation phase', further details regarding exact data/information of the parameters to be exchanged will be needed.
4.3 Concept of operations

The next sub-argument asserts that the Concept of Operations fully describes how the system is intended to operate. In this context, it has to be noted that the CREDOS project has brought forward 5 subsequent Concept of Operations versions (A, B, C, D, E). For convenience, the high-level principle underlying the concept is outlined below.

The proposed concept aims at a reduction of the currently used 2 minutes interval applicable for HEAVY – MEDIUM, HEAVY – LIGHT or MEDIUM – LIGHT aircraft combinations through the suspension of the runway wake turbulence time separation and the wake turbulence radar separation during take-off and first climb phase, when enabled by favourable crosswind conditions. The intention is not to introduce any new intermediate wake turbulence separation, but to totally suspend it, when predefined wind criteria are met. The CREDOS concept is based on today’s technical environment, and is assumed not to require advanced decision support tools.

It has been demonstrated in CREDOS that the crosswind component threshold would be about 7 to 8 knots [12, 13]. Application of the CREDOS concept requires that wind conditions have to be monitored and forecasted in the aircraft departure area. The extent of the concept is dependent on wind monitoring capabilities of the airport (such as wind measurements, wind now casts and/or forecasts), since the concept obviously does not apply where the wind cannot be accurately evaluated. These wind determination capabilities define an airspace surrounding the aircraft departure path within which the wind can be monitored, and within which the wake turbulence separation may be suspended. In the context of the CREDOS concept, this airspace is named “Wake Turbulence Suspended Separation Airspace Volume” (WTSSAV).

It is also proposed to apply a Go/No-go methodology per aircraft pair for the controller and that wake turbulence separations in distance and time should be suspended totally for the runway controller, when the determined crosswind is present. The Runway Controller will determine for every departure behind a heavier aircraft whether the criteria are met or not. However, during stable weather conditions, CREDOS can also be used for short term tactical planning purposes by forecasting the supposed length of the period when CREDOS would most likely be operated. The Tower Supervisor who activates the CREDOS system and HMI, and thereby implies that the Runway controller now can use CREDOS. Table 1 introduces the human actors for CREDOS.

It is concluded that the concept [10] fully describes how the system intends to operate.
Table 1 Human actors and their roles and responsibilities

<table>
<thead>
<tr>
<th>Actor</th>
<th>Current Responsibility</th>
<th>Specific/additional role in CREDOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tower ATC Supervisor (SUP)</td>
<td>Overall responsible for the planning of the tower operation. Monitors operations. Decides on arrival and departure rates. Proposes runway configuration. Gives permission for maintenance etc.</td>
<td>Decides when to activate the CREDOS system based on forecast, now cast and wind information as well as traffic demand, traffic mix and runway configuration.</td>
</tr>
<tr>
<td>Runway Controller (TWR)</td>
<td>In charge of take-off phases including runway and radar separation.</td>
<td>Puts in place and monitors safe separations and efficient spacing and sequence using the CREDOS suspension of wake turbulence separations. Receives and disseminates CREDOS critical wake vortex and weather information.</td>
</tr>
<tr>
<td>Ground Controller (GND)</td>
<td>Gives start-up and push-back clearance. Sequences arrivals and departures and manages queuing according to the runway and stand capacity/availability.</td>
<td>Uses DMAN (or similar) information based on CREDOS or adjusts manually to the CREDOS capacity and sequencing opportunities.</td>
</tr>
<tr>
<td>Clearance Delivery (CND)</td>
<td>Reads clearances to departing traffic.</td>
<td>Informs departures of CREDOS being in use.</td>
</tr>
<tr>
<td>Departure Radar Controller (DEP)</td>
<td>Separates safely aircraft on radar after departure. Manages an efficient flow of traffic out of the runway into the en-route or TMA sectors.</td>
<td>Monitors the CREDOS availability and application per flight. Receives and disseminates CREDOS critical wake vortex and weather information.</td>
</tr>
<tr>
<td>Flight crew</td>
<td>Navigates aircraft safely</td>
<td>Are aware of the CREDOS operation and the suspension of wake turbulence separations. Report CREDOS critical information.</td>
</tr>
<tr>
<td>TMA Supervisor</td>
<td>Plans and monitors the TMA operation</td>
<td>Is informed about CREDOS activation. May also initiate the activation of CREDOS operations.</td>
</tr>
</tbody>
</table>
4.4 Concept safety validation requirements

The following high level safety validation objective is identified [5]:

SA1  The application of the crosswind departure concept will not degrade safety.

This objective has been broken down in two low level safety validation objectives:

SA1.1 To build documented evidence that provides a convincing and valid argument that suspended departure separations under crosswind conditions will be as safe as, or safer than, the current ICAO wake turbulence separations for a generic airport environment.

SA1.2 To build documented evidence that provides a convincing and valid argument that implementation of the CREDOS procedures described in the CREDOS concept will be as safe as, or safer than, current departure operation in line with the ICAO rules.

On one hand the Safety Case is to evaluate the safety parameters of the proposed suspended separations (low-level validation objective SA1.1); on the other hand, it will assess the safety of the concept application in an operational environment (SA1.2).

Initial Validation requirements related to the SA1.1 objective

- A preliminary minimum crosswind condition criterion ensuring that only turbulence with acceptable strength remains in the runway vicinity during the Departure Phase, when the following departure is cleared for take-off, shall be assessed.
- Assessment / validation of proposed suspended separations will require integration of reliable models in fast time simulators. These models shall be validated.
- The preliminary crosswind criterion as well as the resulting departure separations in the Departure and Initial Climb Phase shall be refined and validated.

Initial Validation requirements related to the SA1.2 objective

- The Safety Case will assess the safety of the CREDOS concept and procedures that are the result of the concept design and evaluation phase. The CREDOS concept will evolve during the CREDOS project feasibility study and will, allow an increased departure rate by relieving wake turbulence constraints during the departure phase.
- The Safety Case shall show that the concept performs this function at an acceptable safety level. The acceptability of the safety level will be assessed relative to the safety level of present operations where wake vortex criteria are in force in accordance with the existing wake vortex separation criteria.
Validation Exercises for assessing the safe use of the operational concept in a realistic operational environment will be conducted in line with the E-OCVM requirements in terms of preparation, definition of objectives, tools selection, etc.

As such, it can be concluded that:

- high-level safety validation objectives have been specified for the concept;
- all safety validation objectives have been broken down into initial validation requirements as baseline for a safety assessment to be performed in CREDOS.

### 4.5 External elements

As described in Section 4.2, the CREDOS operational system is based on the introduction of five new system components. As shown in Figure 6, there are external elements to these five new system components. The three external elements are:

- Meteorological systems (*enhancement of existing systems*);
- Surveillance systems (*existing system*);
- Flight data processing systems (*existing system*).

It is assumed that the existing surveillance and flight data processing systems used in today's ATC operational environment do not need to be improved, i.e. the existing performance, reliability, accuracy and integrity capabilities will suffice. These existing systems will provide input data to the CREDOS components. The safety implications of incorrect/erroneous data generated by these two existing systems have (partly) been addressed as part of the CREDOS PSSA (see also Section 7). Potential requirements for enhancements to existing meteorological systems are captured as part of the CREDOS Concept development. They result from the determination of requirements for the size of the Wake Turbulence Suspended Separation Airspace Volume (WTSSAV) and the targeted CREDOS spacing (see reference 10 for the full details).

The following external elements, also part of the application, have been identified for further analysis: air ground communication, radar surveillance system (see Section 6).

Taking into consideration the requirements on these external elements as described in Sections 6 and 7 of this study and CREDOS references 10 and 11, it can be concluded that the safety requirements on external elements are indeed captured. In view of clarifying this conclusion - which is based on evidence provided in several separate documents - it might be worthwhile to document the traceability between the basic CREDOS system design and these safety requirements in a new separate Appendix.
4.6 Summary of findings

The objective of this Section is to demonstrate that all necessary Safety Requirements have been specified, or assumptions have been stated, to cover all elements, in terms of system design, that are necessary to fully implement CREDOS operations. This section has provided the argument and supporting evidence that the system boundaries are sufficiently clearly defined at this stage of the system development. The procedures and functions are described and the roles and responsibilities of the human actors are sufficiently clear to conclude that the concept [10] fully describes how the system intends to operate. High level concept safety validation objectives have been specified and broken down further into initial safety validation requirements. Safety requirements on and external elements have been specified in other documents (it might be worthwhile to document the traceability between the basic CREDOS system design and these safety requirements on external elements in a separate Appendix). As such, it is concluded that - at a high-level - system design (comprising architecture, components, interfaces) is complete and may be used for further system development.
5 Design correctness

5.1 Introduction

The objective of this section is to show that the concept of the system design functions correctly and coherently under all normal environmental conditions. The main issue in this argument is the internal coherency and dynamic behaviour of the system over the full range of conditions for which the system is expected to be subjected in its operational environment. The key elements to be addressed here are the internal coherency and the dynamic behaviour of the system. It needs to demonstrate that the functionality and data would remain consistent throughout the system, over the full range of conditions to which the system is expected to be subjected in its operational environment. In particular the following questions need to be addressed:

- Are the specified procedures coherent?
- Are the human actions coherent?
- Are the same data about the flight / intentions held by the various actors?
- Are there any undefined states of the system?

The strategy for satisfying Argument 1.3 is to provide enough evidence that the following lower-level arguments are true:

- Arg1.3.1 The design is internally coherent.
- Arg1.3.2 The design functions correctly under all reasonably foreseeable normal operating conditions

![Figure 7 Decomposition of Argument on Design Correctness (Arg1.3)](image-url)
Design Correctness of the Tower Controller functions

The main function of the Tower Controller is to provide aircraft lined-up for take-off with a take-off clearance, such that minimum separation requirements are satisfied. It has to be shown that:

- The controller can cope with varying time separation between subsequent aircraft, based on CREDOS conditions being met or not, and to evaluate whether the information to perform his task (HMI) is sufficient and displayed in an appropriate way.
- The controller is able to cope with various failure scenarios, such as:
  - undetected failure of the CREDOS system to establish that the departure corridor is free of wake vortices;
  - minimum radar separation infringement after being scheduled according to the CREDOS advisory information;
  - gross navigation errors (e.g., SID blunders);
  - aircraft reporting wake vortex upsets, while properly separated.

Design correctness of the Departure Controller functions

The main function of the departure controller is to monitor that aircraft after take-off are properly separated, in agreement with governing conditions (either CREDOS or ICAO separations) and to take the appropriate actions if separation minimums are (or threatened to be) violated. It has to be shown that:

- The controller is able to cope with suspended (CREDOS) separation of light/medium aircraft behind a heavy, and control aircraft such that when the aircraft leaves the WTSSAV, the required ICAO separation minima is restored.

5.2 Internal coherency of the system design and procedures

Working methods for RWY and DEP controllers are expected to change slightly because the controller has to consider additional factors (e.g. CREDOS status, SID assigned for leading and following aircraft) to determine whether or not CREDOS could be applied and plan departures more in advance. Nevertheless, the approach is to assume that proposed procedures are consistent with PANS-ATM procedures and that no specific procedures beyond these are required. Coherency of the procedures would therefore be ensured through the coherency of the ICAO PANS-ATM procedures.

Recall that currently the ICAO two minutes runway separations which apply regardless the wind conditions lead often to distance separation larger than the required ICAO wake turbulence separation (e.g., 5 NM for MEDIUM aircraft behind a HEAVY). The current application of these ICAO rules varies depending on the airport and/or the
country. Some service providers can apply 5 instead of 3 wake categories. In some European countries the towers that use TMA radar only apply the wake turbulence radar minima and not in combination with the wake turbulence runway separation minima as other countries. In CREDOS only the three present categories: HEAVY, MEDIUM and LIGHT are considered, but more categories have already been introduced by some European ANSPs. During the CREDOS concept development, it appeared that local variations in methodology, rating, roles and/or responsibilities exist.

As described in Section 4.3, the CREDOS concept idea consists in authorizing a suspension of the wake turbulence time and distance separation between certain pairs of departures depending on the strength and direction of the wind on the runway and during the initial part of the climb. The idea is to take advantage of the cross component of the wind which, when sufficient, blows the wake turbulence (i.e. the wake vortices) generated by the preceding aircraft out of the track of the follower aircraft, and therefore enables to suspend wake turbulence separation.

To what extent are the proposed CREDOS procedures and system design internally coherent? This aspect has been studied during the CREDOS real-time simulations, on the basis of a generic representation of the CREDOS concept and system design [11]. The findings with respect to internal coherency, which will be relevant for any local implementation of the CREDOS concept, are summarized in the following. It is assumed that internal coherency of the system design will be achieved if the below recommendations - as identified in the real time simulations [11] - are fully considered.

Controller familiarity:
- CREDOS operations most probably would not be used all the time. Therefore, it has to be assured that controllers maintain to be up to date with the concept and will be able to apply it any time. Training would be a prerequisite for this.

Controller procedures:
- Procedures must be well defined and clear, also for non-nominal events. The communication phraseology must be well defined and as simple as possible.

Division of controller responsibilities:
- At present, it is not (yet) fully clear how and where exactly the separation would need to be increased to the minimum required radar separation minima. It appeared not clear if it would be the runway controller or departure controller who would have responsibility and control of the concerned aircraft during the transition to radar separation. Special attention therefore needs to be given to the handover of control from the runway controller to the departure controller.
SID Compatibility:

• The level of complexity of the SID structure will influence the usability of CREDOS. SIDs must be CREDOS compatible for each pair of aircraft being cleared on reduced separation, taking into account the wind direction. Each take-off clearance under CREDOS must pass this SID compatibility check, and this information must be given to the controller. An appropriate and robust support tool would be required and would need to be developed. Safety nets, such as e-strips including information about SID to be flown and applicability of CREDOS or advanced Go/No-go display HMI's should be considered.

• There might be a risk that reduced separation would be applied even if the SID configuration of the follower does not allow it. Especially at the beginning of CREDOS mode being active, it appears to be possible for a runway controller to forget a check of the SID configuration for the following aircraft. Once reminded, the operations usually are correct further on. Proper training and enhancements in support of routine operations seem to be especially beneficial.

5.3 Dynamic behaviour of the design

The CREDOS team has conducted real time simulations (RTS) to study the impact of reduced take-off separations on ATC. The purpose was to evaluate the potential ATC mitigation for each of four non-nominal events as derived from the CREDOS FHA [7]:

• Discrepancy in advisory to controllers (i.e. CREDOS operation is active while the Wake Turbulence Advisory indication is not correct, implying that the crosswind information is not consistent with the status of CREDOS; for instance green GO light is on, while the crosswind is not sufficient for CREDOS operations).

• Wake turbulence encounter while the CREDOS separation is applied and wind is sufficient.

• Flight deviation from planned trajectory – incorrect track keeping of leading or following aircraft (an aircraft would not follow the designated SID).

• Aircraft catching-up the preceding one (the following aircraft was much faster than the preceding one, implying that separation would be less than expected).

Discrepancy between WTA (Go/No-go) and wind information

Discrepancy between the Go/No-go indication and the wind indication can result in runway controller issuing CREDOS reduced separation take-off clearance when the wind conditions are not sufficient. The situation when the Go/No-go indication was incorrect according to the wind strength was covered during simulations; i.e. the wind strength was not sufficient for applying CREDOS separations, while the green 'Go' indication was on. During simulations the sudden wind drop was not noticed
immediately by the runway controller. However, if controllers checked the wind information before issuing the clearance applying reduced separation, the discrepancy was always noticed. Inconsistency of displayed information was captured by the runway controller in most cases when CREDOS pairs were concerned. Recommended is that in cases where the most basic advisory tool is used at the airport (only Go/No-go display), a procedure for the runway controller includes mandatory transmission of wind information in take-off clearance for all aircraft. This would introduce a safety net that enables the runway controller to be always aware of wind conditions while applying reduced separations and cross check an eventual discrepancy displayed.

*Wake turbulence encounter*
Several times pilots reported wake encounter during simulations. In such situations responsibilities and actions expected from controllers are the same in CREDOS mode operations as in today's operations. However, in the case of CREDOS being active, controllers have less time to take any action while the distance between aircraft is smaller than in nowadays operations. During simulations, the responses to WT encounter reported by pilots were appropriate; CREDOS was suspended once the WT encounter was reported. However, later it was decided to change this action and controllers were not obliged to suspend CREDOS after the WT encounter was reported. Once it was not mandatory to suspend CREDOS after the WT encounter, the coordination between the runway and departure controller was conducted via phone, when agreements on eventual climb restrictions for the following aircraft were made. In most cases, the aircraft that encounter WT continued the flight, while the following aircraft was given a restriction to stop climb at 2000 ft or 3000 ft until departure controller allowed further climb.

*Flight deviation from planned trajectory*
Deviation from the assigned trajectory can result in loss of separation between aircraft and/or entering into the area where wake is present. During simulations, in situations when aircraft deviated from the planned trajectory, the controllers actions were appropriate. However, such events momentarily increased workload. No difficulties have been encountered with solving the deviation matter. The occurrence is the same as in today's operations and nothing unusual or new has been introduced in this case. Nevertheless, flying the correct SID is crucial for safety of operations. Otherwise, it may lead to loss of separation and highly increase controller’s workload, especially in a busy environment. It is recommended that procedures for controllers should be well defined in case of a wrong turn, i.e. if the departure controller should act first and then inform the runway controller, or the other way around.
Aircraft catching-up the preceding one

This event could not be successfully simulated. Nevertheless, in the case of a few pairs of aircraft, the follower was faster than the preceding aircraft and the departure controller had to take one or both aircraft off the SID in order to maintain the separation. This did not cause problems with handling all the traffic, but momentarily increased the workload.

It was also analyzed how the ATCo manages the new mode of operations. Although an understanding of the causes of each hazard is desirable to enable the development of preventative mitigations, in the simulations it was the effects of the hazard occurrence which was studied. Six scenarios were simulated and several comments were made by controllers participating in the simulations (see Section 5.4 for a summary of findings).

5.4 Summary of findings

The objective of this section is to show that the concept of the system design functions correctly and coherently under all normal environmental conditions. With respect to internal coherency, it is observed that internal coherency of the system design will be achieved if recommendations on controller familiarity, controller procedures, division of controller responsibilities, and SID compatibility (see Section 5.2) are fully considered. With respect to correct dynamic functioning of the design, it is observed that there are few issues to be resolved before implementation. The overall concept of CREDOS was well received by air traffic controllers participating in the real time simulations [11]. Four recommendations should be taken into account for local implementations of CREDOS:

• In cases where a basic advisory tool is used at the airport (only Go/No-go display), the procedure for the runway controller should include mandatory transmission of wind information in take-off clearance for all aircraft. This would introduce a safety net that enables runway controller to always be aware of wind conditions while applying reduced separations and cross check an eventual discrepancy displayed.
• Procedures for controllers should be well defined in case of wrong turn, i.e. if the departure controller should act first and then inform the runway controller or the other way around.
• The proposed phraseology for non-nominal events would need to be refined.
• A status indicator that takes into consideration the assigned SIDs for leading and following aircraft could assist the controller and reduce the risk of mistake.

Overall, it may be concluded that - provided that these recommendations are followed - there is sufficient evidence that the CREDOS system as specified and simulated does function correctly and coherently under foreseeable normal environmental conditions.
6 Design robustness

6.1 Introduction

The objectives of this section are to show that the application system design is robust against external abnormalities in the operational environment. Evidence is required to show that the system can continue to operate effectively and that such abnormalities do not cause the system to behave in a way which could induce risks that would otherwise not be present. The reaction of the system to abnormal events in its operational environment is to be considered from the following perspective:

- Can the system continue to operate?
- Could such conditions cause the system to behave in a way that introduces additional risks?

The strategy for satisfying Arg1.4 is to provide evidence that both of the following lower level arguments are true:

1. Arg1.4.1 The system can react safely to all reasonably foreseeable external failures, i.e. failures in its adjacent systems
2. Arg1.4.2 The system can react safely to all other reasonably foreseeable abnormal external conditions in its environment.

Figure 8 Decomposition of Argument on Design Robustness (Arg1.4)
6.2 Reaction to external failures

When considering external failures to the CREDOS system, the resultant effect was of most concern. The "CREDOS system" consists of:

a) Separation Mode Advisor,
b) Departure Planning Advisor,
c) SID Wind Forecast,
d) Go/No-Go Advisor, and
e) SID Wind Monitoring (see Figure 6).

External systems that are foreseen to provide input to the 5 new CREDOS components are: meteorological systems, surveillance systems, and flight data processing systems. The effect of any failure would be minimal if the sufficient separation between aircraft is maintained and no wake vortex is encountered. External failures which could cause separation minima infringement and/or wake vortex encounter are:

- Aircraft failure (e.g. engine failure)
- Voice communication system failure
- Degradation of surveillance systems information
- Degradation of meteorological systems information
- Degradation of flight data/information

**Aircraft failure**

In case of aircraft failure (e.g. engine failure), this would involve application of the same procedures as in today's operations. Because aircraft systems failures are independent of CREDOS operations, the likelihood of such external failures would be no greater than for the current operational practice. Therefore, the CREDOS operational system is not less robust against aircraft system failures than the current operational system.

**Voice communication system failure**

Concerning this external failure, it is noted that a failure of the voice communication system would be most hazardous if it could lead to an early take-off. However, usually such failure would then immediately be known by the pilot of a departing aircraft as no take-off clearance would be heard. Similarly, the controller would not hear a read-back from the flight crew. As such, the likelihood and impact of voice-communication failure would be no greater than for the current operational system. Concerning procedures in case of voice communication system failure, once the pilot is airborne, the same contingency procedure as for the current operations apply. Thus, the system is no less robust against voice-communication failure than the current operational system.
Degradation of surveillance systems information
An external failure of the surveillance systems could lead to erroneous information regarding the flight track that is used for monitoring the wind along the flown SID.

As a consequence the SID wind now-cast would not be correct, and there could be a (significant) discrepancy between the predicted wind and the wind now-cast. In this case, the CREDOS system would be able to continue to operate. As a CREDOS take-off clearance would be based on the Go/No-Go advisory, it is expected that this would not impose additionally risks. It is more likely that the CREDOS system would be shut down in case a controller would note the discrepancy of the wind information.

Degradation of meteorological systems information
An external failure of the meteorological systems would lead to wrong input for the CREDOS separation mode advisor and the CREDOS SID wind forecast system, and might therefore lead to a wrong Go/No-go advice. As the runway controller will cross-check the Go/No-go indication against the actual surface crosswind (via anemometers), the CREDOS operations are robust against such failures. Most likely CREDOS will be shut down, because apparently the quality of the input wind data would not be sufficient.

Degradation of flight data and/or information
An external failure of the flight data processing systems would imply that a wrong flight plan, aircraft type, or SID could be used by the Departure Planning Advisor. As the controllers will verify cross check this information through standard communications prior to take-off, the CREDOS operations are also robust against such external failures.

6.3 Reaction to other abnormal conditions
The following possible abnormal condition has been identified:
- Sudden wind changes

Sudden wind changes
The CREDOS system is wind dependent, and the wind speed and direction have to be monitored in real-time for the area that encompasses the departure path where standard ICAO separation for area control is to be obtained. Sudden wind changes are indicated by the system and if they appear to be insufficient for CREDOS operations, the ATC Supervisor can decide about the deactivation of the CREDOS system and operations. However, should a sudden wind change (towards decreased crosswind)
occur when an aircraft is just airborne (and still at relatively low altitude), with e.g. less than about 90 seconds separation with the preceding aircraft, then this aircraft would be exposed to higher wake encounter risk than anticipated. The use of wind monitoring systems up to about 2000 feet height is therefore recommended. In terms of the high level design, it is clear that care should be taken to ensure that CREDOS system would not be less robust to extreme weather conditions than the current operational system.

6.4 Summary of findings

The objectives of this section are to show that the application system design is robust against external abnormalities in the operational environment. Evidence is required to show that the system can continue to operate effectively and that such abnormalities do not cause the system to behave in a way which could induce risks that would otherwise not have been present. Five external abnormalities have been considered:

- Aircraft failure (e.g. engine failure)
- Voice communication system failure
- Degradation of surveillance systems information
- Degradation of meteorological systems information
- Degradation of flight data and/or information

As motivated in Section 6.2, the CREDOS system can handle all the above external abnormalities in a robust way. However, should a sudden unexpected strong wind change (towards decreased crosswind) occur, then an aircraft could be exposed to higher wake encounter risk than anticipated. The use of wind monitoring systems up to about 2000 feet height is required for robustness, as care should be taken to ensure that CREDOS system would not be less robust to extreme weather conditions than the current system.

CREDOS is an operational concept that is not very vulnerable to other factors that might distract or delay a CREDOS take-off clearance, as this would only provide a longer separation and therefore, does not increase any risk. What is more, CREDOS is not relying on intervention from controllers in order to be considered sufficiently safe.

Taking into account the recommendation to use wind monitoring systems up to a height of about 200 feet, there is sufficient evidence to show that the system design is robust against the external failures and other abnormalities that have been identified in adjacent systems (external to the CREDOS system) and the operating environment.
7 Mitigation of internal failures

7.1 Introduction

The objective of this section is to show that all risks from internal failures have been assessed and mitigated. Internal failure of the system is assessed from 2 perspectives:

1. How would the loss of functionality reduce the effectiveness of the system?
2. How would the anomalous behaviour of the system induce risks that might otherwise not occur?

The strategy for satisfying this sub-argument 1.5 is to provide evidence that the following lower-level arguments are true:

1. Arg1.5.1 All reasonably foreseeable hazards have been identified.
2. Arg1.5.2 Severity of the effects of each hazard has been assessed, taking into account mitigations specified in the CREDOS operational system description.
3. Arg1.5.3 Safety objectives have been set for each hazard such that the corresponding aggregate risk is within the specified safety criteria.
4. Arg1.5.4 All reasonably foreseeable causes of all hazards have been identified.
5. Arg1.5.5 All external and internal mitigation have been captured as either safety requirements or as assumptions as appropriate.

Figure 9 Decomposition of sub-argument on Mitigation of Internal Failures
7.2 Hazard identification

Possible degradations of the system functions which might result in potential safety hazards are to be identified. As such, this activity starts with raising the functional hazards rather than to determine causes (reason) behind these failures. The functional hazards are those hazards situated at the boundary of the system description and are the consequences of failures within the system, combination of failures and interactions with other systems and external events. According to the EUROCONTROL SAM [3], the recommended method for identifying hazards is the combination of:

1. Systematic application of sets of keywords (for failure modes and external events) to each function of the system under assessment. The SAM provides examples [3].
2. Brainstorming sessions aiming at finding “functionally unimaginable” hazards by assessing normal, abnormal and particular combinations of unrelated events.
3. Analysis of hazard databases, accident and incident reports, and/or other related FHAs.

As part of the CREDOS safety activities, the first two approaches have been used. The brainstorm session for the CREDOS FHA was held with an expert group formed to provide the necessary operational input during the assessment. The experts did have diverse operational background ranging from Air Traffic Control, airline operation and former test pilot operation to the field of safety assessment. An extensive list of hazards/functional failures being the result of the brainstorm session is provided in the CREDOS FHA [7]. The systematic and brainstorm hazards/functional failures have grouped into the nine Main Hazards (Table 2, M1-M9), according to their expected commonality in effect. The hazard ID is complemented with a reference to the function. The Main Hazards will be used for setting the Safety Objectives (see also Section 7.4).

Table 2 Main Hazards M1-M9

<table>
<thead>
<tr>
<th>Function</th>
<th>ID.</th>
<th>Main Hazard</th>
<th>Hazard / Functional Failure description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wake Turbulence Advisory</td>
<td>M1- (WTA)</td>
<td>CREDOS operation is active while WAKE TURBULENCE ADVISORY is not correct (DETECTED)</td>
<td>(Partial) Loss of Wind information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detected erroneous wind information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Partial) Loss of departure information (SID’s etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detected erroneous departure information (SID’s etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Partial) Loss of Wake Turbulence Advisory service (Go/No-go interface)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detected erroneous Wake Turbulence Advisory service (Go/No-go interface)</td>
</tr>
<tr>
<td>Runway Controller</td>
<td>M2- (WTA)</td>
<td>Inconsistent information from Wake Turbulence Advisory service</td>
<td></td>
</tr>
<tr>
<td>M3- (RWY)</td>
<td>CREDS operation is active while WAKE TURBULENCE ADVISORY is not correct (UNDETECTED)</td>
<td>(Partial) Loss of wind information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Undetected erroneous wind information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Partial) Loss of departure information (SIDs, …)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Undetected erroneous departure information (SIDs, …)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Partial) Loss of Wake Turbulence Advisory service (Go/No-go interface)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Undetected erroneous Wake Turbulence Advisory service (Go/No-go interface)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overall system failure. Undetected erroneous operation of CREDS. (Aircraft departs with reduced separation after the ATCO gave the take off clearance when it is not applicable.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wind changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorrect weather prediction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RWY controller applies CREDS while conditions are not met (CREDS system functions correctly)</td>
<td>Misunderstood operation of Wake Turbulence Advisory service by user</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RWY clears aircraft too short after the first one resulting in less than the CREDS separation (fails to check the Go/No-go interface)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RWY applies CREDS separation while SIDs are not suitable for it (fails to check the Go/No-go interface)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unauthorized use of CREDS operation when it hasn’t been covered in the specifications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wrong separation applied – 3NM instead of 5NM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Granting CREDS separation and/or take off clearance when the Go/No-go is red.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ATCO’s mindset is wrong (switching between two runways when only one is under CREDS conditions may cause the controllers confusion and mistake).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RWY looking at the wrong interface (e.g. interface of other runway, or too many displays around).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ATCO does not notice the change of the Go/No-go from green to red.</td>
<td></td>
</tr>
<tr>
<td>M4-</td>
<td>RWY controller</td>
<td>3NM separation is not achieved (but less)</td>
<td></td>
</tr>
<tr>
<td>(RWY) applies CREDOS with less than 3 NM while CREDOS conditions are met</td>
<td>Separation is less than CREDOS separation, due to aircraft speed differences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departure controller</td>
<td>M5- (DEP) Separation is less than ICAO wake vortex separation after 4 NM</td>
<td>DEP fails to monitor correct application of CREDOS (observing minimum crosswinds and correct SIDs being used by aircraft)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3NM distance may not be safe as separation between two aircraft flying on the same and upwind SID, after 4NM from the departure end of runway</td>
<td>DEP uses CREDOS separation beyond the scope (e.g. outside 4 NM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Standard separation is not achieved after 4NM from the departure end of runway.</td>
<td>Flight crew uses incorrect SID and ICAO/std separation is not achieved after 4 NM</td>
<td></td>
</tr>
<tr>
<td>M6- (DEP) (Wake) avoiding action may pose new risk on aircraft</td>
<td>The way DEP would re-establish ICAO separations by vectoring. (Vectoring onto downwind SID may not be safe; terrain obstacle may become a hazard.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DEP may have problems with restoring the ICAO/standard separations in case crosswind turns out to be insufficient.</td>
<td>Limited capability to maneuver to avoid wake encounter by the following aircraft.</td>
<td></td>
</tr>
<tr>
<td>Flight crew</td>
<td>M7- (CREW) Incorrect track keeping of leading or following aircraft</td>
<td>Aircraft track keeping is poor, the succeeding aircraft crosses the wake of the preceding one</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Difference between the planned flight path and actual lateral flight path (due to CB, noise abatement etc.)</td>
<td>Aircraft flying with different accuracy on the first SID segment.</td>
<td></td>
</tr>
<tr>
<td>M8 (CREW) In anticipating action CREW turns aircraft to unsafe side (Wake Vortex), into other traffic or into terrain.</td>
<td>Engine failure and flying downwind afterwards</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pilot avoiding wake vortex on his own initiative with/without TCAS or ADSB.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Crew initiates take-off while CREDOS conditions are not met. Flight crew misinterprets take-off clearance and takes-off without CREDOS conditions being met.

7.3 Hazard severity

This step comprises the identification of possible consequences of the hazards on the ATM system and aircraft operations. For the assessment of effects and severity a distinction has been made between a detected and undetected effect of the hazards. The effects and severity of the nine main hazards have been identified during a second expert brainstorm session. The EATMP SAM Severity Classification Scheme [3] has been used to determine the severity class 1 to 5.

Table 3 Severity classes

<table>
<thead>
<tr>
<th>Severity class</th>
<th>Effect on operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Accident</td>
</tr>
<tr>
<td>2</td>
<td>Serious incident</td>
</tr>
<tr>
<td>3</td>
<td>Major incident</td>
</tr>
<tr>
<td>4</td>
<td>Significant incident</td>
</tr>
<tr>
<td>5</td>
<td>No immediate effect on safety</td>
</tr>
</tbody>
</table>

The output of the hazard effect and severity session has been summarized in Table 4 (next page). This table can be read as follows:

- In the first column the function is given to which the main hazard refers.
- The second column gives the hazard ID (number and functional reference)
- The third column states the effect.
- The fourth column states the barriers if any.
- In the fifth column the severity class has been given.

Looking at the results of Table 4 in more detail, the expert’s line of reasoning can be summarized as follows: A wake encounter at low speed and low altitude could result in an event with severity 1 (accident). A wake encounter at low speed at higher altitude

---

1 In this report a barrier is defined as any mechanism that reduces the probability of a hazard leading to an accident or incident.
(say >500ft) could result in an event with severity 2. The increased chance of a wake encounter could lead to an event with severity 3 or 4; an event with no immediate effect may lead to severity 5.

Table 4: Effect and Severity Classification of CREDOS Operational Concept

<table>
<thead>
<tr>
<th>Function</th>
<th>Hazard ID</th>
<th>Hazard effect</th>
<th>Barrier</th>
<th>Severity Class</th>
</tr>
</thead>
</table>
| Wake Turbulence Advisory service | M1- (WTA) | Distinction:  
- Detected before Take-Off clearance: No effect on safety  
- Detected after T/O clearance in low speed T/O region  
- Detected after T/O clearance in high speed T/O region or thereafter (encountering wake-vortex just after lift-off)  
- Undetected (encountering wake-vortex just after lift-off) | Detected by RWY or crew (RTO, heading or turn into wind) by DEP (heading)  
In general: Cockpit detection equipment might be implemented in future | ➢ 5  
➢ 4  
➢ 1 |
| Runway Controller | M2- (WTA) |  
- SID error leading a/c (goes in upwind direction) (Detected)  
- SID error following a/c goes in downwind direction (Detected)  
- SID error (undetected), following aircrafts flight path into wake region. | Detected by DEP; issues track correction  
Possibilities for detection by DEP are reduced. SID seldom turn < 500 ft height. In general: radar vectored departures might mitigate this hazard | ➢ 4  
➢ 2(1-3) |
| Runway Controller | M3- (RWY) | Effect is same as M1-M2 | RWY is not a barrier in this case. Pilot is the potential mitigation. Pilot might detected it or might not. | ➢ 1 |
| Runway Controller | M4- (RWY) | The radar separation is not met, but there is no problem from a WV point of view. Infringement of radar separation. |  | ➢ 5 |
| Departure Controller | M5- (DEP) | Infringement of WV separation |  | ➢ 3-4 |
| Departure Controller | M6- (DEP) |  | Not really CREDOS specific |  |
### 7.4 Safety objectives

In this Section the Safety Objectives (SOs) for the CREDOS concept are derived. The general goal of setting SO is to achieve an acceptable risk for the system. A Safety Objective specifies the maximum acceptable frequency for the occurrence of a hazard. The generic principle chosen is that the system safety level will be set according to the Eurocontrol Safety Regulatory Requirement 4, named Risk Assessment and Mitigation in ATM (ESARR4) to the largest extent possible [1]. The ESARR4 requirement addresses the acceptable level of system risk when changing an ATM System. As the ESARR4 poses, a quantitative safety level on the overall ATM risk, a Quantitative Method will be used for setting the Safety Objectives in accordance with the SAM.

This method consists of the following steps (see also Figure 10):

1. **Identify all hazard effects.**

   For each single hazard being identified at the boundary of the system under assessment, all effects of hazard should be identified, taking into account the effectiveness of possible defenses (barriers) outside the system under assessment, that could prevent or not the hazard to have certain effect on operations, including the aircraft operations.

2. **Allocate severity class to each hazard effect.**

   After all hazard effects have been identified, severity classification should take place, in accordance with the Severity Classification Scheme. Severity class should be associated with each identified hazard effect.

3. **Calculate the conditional probability (Pe).**

   The process of calculating the probability of the hazard to generate each of its effects (Pe) should take place.
4. Allocate the Safety Objective by applying the Risk Classification Scheme.

Risk Classification Scheme/Matrix defined by the Organization should be used to associate the maximum acceptable rate of occurrence of hazard effect (Safety Target ST)) with the corresponding severity class of the hazard effect.

So, if the overall frequency of hazard effect (ST) is specified in the Risk Classification Scheme provided by the Organization in terms of maximum acceptable frequency of occurrence for each severity class, and the probability of the hazard to generate each of its effect is calculated (Pe), then a Safety Objective for the hazard itself is specified by dividing those two values for each different effect and choosing the most stringent one (the lowest figure) between the results.

Note that when applying this method, the principle of the worst credible case is applied when setting the Safety Objective, by choosing the most stringent one, among different values calculated \( \min (ST_m / Pe_n) \), taking into account not only the severity of the effects but also the probability of the effect as a consequence of the hazard.

**Note:** the number of hazards is to be taken into account (for example include it in Pe or divide \( ST_m / Pe_n \) by the number of hazards for that class of severity) in order to ensure that the sum of all Safety Objectives comply with Safety Targets.

![Figure 10 Safety Objectives in Quantitative Method](image-url)
In order to take the hazard’s largest contribution to ‘un-safety’ into account, it is possible to take into account the "worst" or "worst credible" effect of each hazard when setting the Safety Objective. The worst case identifies the effect that has the most severe consequences. The worst credible case aims at identifying the highest contribution of a hazard to a high or the highest risk. Credible implies that it is not unreasonable to expect to experience this combination of extreme conditions within the operational lifetime of the system. However, selecting the worst credible case (instead of the “worst case”) by expert judgment has turned out to be difficult. Therefore, in this study the "worst case" has been used to set conditional probabilities and Safety Objectives. In this way the Safety Objectives are set for the most severe effect of each hazard.

The ESARR4 requirement [1] addresses the acceptable level of system risk when changing an ATM System, while covering the elements of humans, procedures and equipment. The ESARR4 sets a limit on those hazards where the ATM system has a direct contribution to. According to ESARR4, the direct ATM system contribution to an accident/incident is defined as "where at least one ATM event or item was judged to be directly in the casual chain of events leading to an accident or incident". Without that ATM event, it is considered the occurrence would not have happened”. ESARR4 does not clearly specify whether the errors of aircraft/pilot are included in this safety budget. For a conservative approach, in this study the aircraft/crew errors are included in the ESARR4 budget. The minimum safety specification in ESARR4 refers to the safety performance of the overall ATM system at ECAC and national level and is not directly applicable to the classification of individual hazards. The maximum tolerable probability of ATM direct contributing to an accident (severity class 1) of a commercial air transport aircraft is $1.55 \times 10^{-8}$ accidents per flight hour or alternatively as set per flight $2.31 \times 10^{-8}$. For setting maximum frequencies to events other than severity 1 (2, 3, 4 and 5), the SAM [3] has been used.

During the process of translating the ESARR4 into requirements for the CREDOS concept, the following assumptions are made:

- Aircraft/crew errors are included in the assessment provided associated hazards would not have existed when CREDOS would not have been in operation.
- Accident data on ATM related contributions is used for allocating the ESARR4 - complete flight-risk budget to the take-off phase budget.
• For setting maximum frequencies to events other than severity 1 (2, 3, 4 and 5), the SAM Guidance Material E: Risk Classification Scheme, edition 2.1, has been used.

Using accident data per accident type [4] approximately 4% of all ATM related accidents are wake-vortex accidents. It must be noted that this figure represents all ATM related (directly- and not-directly contributing) accidents and ESARR4 makes reference to the ATM direct contributions, only. However, because no other more suitable data is available, it is assumed that the ratio for the flight phases will be the same. Hence, this ratio (4%) of the accident data, valid for today's standard departure operations will be used for the apportionment of the ESARR4 and risk budget. To achieve the same level of safety the same apportionment will be placed on the risk budget of the CREDOS operation. Given the fact that the majority of wake vortex accidents are in the final approach or take-off phase one can assume an equal distribution of the 4% ratio (take-off and landing both 2%). A more sophisticated distribution is difficult to make due to the limited number of accidents of this type. One can now derive maximum tolerable probabilities for each of the five severity classes [7].

Table 5 Maximum tolerable probability of Credos ATM direct contribution for severity classes

<table>
<thead>
<tr>
<th>Severity Class</th>
<th>Maximum Tolerable Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$0.5 \times 10^{-9}$ per take-off</td>
</tr>
<tr>
<td>2</td>
<td>$0.3 \times 10^{-6}$ per take-off</td>
</tr>
<tr>
<td>3</td>
<td>$0.3 \times 10^{-5}$ per take-off</td>
</tr>
<tr>
<td>4</td>
<td>$0.3 \times 10^{-3}$ per take-off</td>
</tr>
</tbody>
</table>

Next step for setting Safety Objectives is the calculation of conditional probabilities. A first estimate for each of the conditional probabilities for each hazard effect has been determined using expert judgment. These estimates serve as first indication of the possible Safety Objectives (Table 6). In order to get the maximum allowable frequency, the maximum tolerable probability of the CREDOS operation per severity class has been divided by the number of hazards identified in the respective class.
Table 6 Maximum allowable frequency of a specific hazard effect (ST) per take-off

<table>
<thead>
<tr>
<th>Severity class</th>
<th>Hazards ID</th>
<th>Maximum allowable frequency of a hazard effect (ST) (per take-off)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>M1&amp;2, M3, M9</td>
<td>0.167*10^{-9}</td>
</tr>
<tr>
<td>2</td>
<td>M7, M8</td>
<td>0.15 *10^{-6}</td>
</tr>
<tr>
<td>3</td>
<td>M5</td>
<td>0.3*10^{-5}</td>
</tr>
<tr>
<td>4</td>
<td>None identified</td>
<td>None identified</td>
</tr>
<tr>
<td>5</td>
<td>M4</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Using the first estimate of the conditional probability (Pe) of each worst effect as determined, an indication of the Safety Objective (SO) per hazard can be determined by dividing the ST by the Pe. The Safety Objective specifies the maximum acceptable frequency for the occurrence of a hazard itself. The first estimates for each conditional probability (Pe) are provided and motivated in the CREDOS FHA [7]. Table 7 also provides the Safety Objective (SO) for each of the main hazards.

Table 7 First indication of Safety Objective per hazard

<table>
<thead>
<tr>
<th>Main hazard ID</th>
<th>Description</th>
<th>Severity of worst case</th>
<th>First estimate of conditional probability</th>
<th>First indication of Safety Objective (per hazard / per take-off)</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1&amp;2 (H1)</td>
<td>CREDOS operation active while wake turbulence advisory is not correct (detected and undetected)</td>
<td>1</td>
<td>1*10^{-2}</td>
<td>1*10^{-8}</td>
</tr>
<tr>
<td>M3 (H2)</td>
<td>RWY controller applies CREDOS while conditions are not met (CREDOS system functions correctly)</td>
<td>1</td>
<td>1*10^{-2}</td>
<td>1*10^{-8}</td>
</tr>
<tr>
<td>M4</td>
<td>RWY controller applies CREDOS with less than 3 NM while CREDOS conditions are met.</td>
<td>5</td>
<td>Not safety related</td>
<td>Not safety related</td>
</tr>
<tr>
<td>M5 (H3)</td>
<td>Separation is less than ICAO wake vortex separation after 4NM</td>
<td>3</td>
<td>2*10^{-2}</td>
<td>1*10^{-4}</td>
</tr>
<tr>
<td>M7 (H4)</td>
<td>Incorrect track keeping of leading or following aircraft</td>
<td>2</td>
<td>2*10^{-2}</td>
<td>5*10^{-6}</td>
</tr>
<tr>
<td>M8 (H5)</td>
<td>In anticipating action crew turns to unsafe side (WV, traffic or terrain)</td>
<td>2</td>
<td>2*10^{-2}</td>
<td>5*10^{-6}</td>
</tr>
<tr>
<td>M9 (H6)</td>
<td>Crew initiates take-off while CREDOS conditions are not met</td>
<td>1</td>
<td>1*10^{-2}</td>
<td>1*10^{-8}</td>
</tr>
</tbody>
</table>
7.5 Hazard cause identification

Nine main hazards have been identified initially (Table 2). However, when considering the consequences of the main hazards, the following was concluded in the FHA [7]:

- Main hazard M6 (“wake avoiding action - by the departure controller - may pose a new risk on an aircraft”) is not CREDOS specific and this hazard is therefore not further considered;
- No safety related consequences were identified for main hazard M4 (“RC applies CREDOS with less than 3NM while CREDOS conditions are met”) and therefore analysis of this hazard is not further considered;
- Main hazards M1 (“CREDOS operation is active while wake turbulence advisory is not correct – detected”) and M2 (“CREDOS operation is active while wake turbulence advisory is not correct – undetected”) were combined into one hazard in the FHA because their consequences are identical.

The first 3 functional hazards (H1, H2, H3), as given in Table 7, describe comparable situations: an aircraft taking-off before the ICAO separation time has passed, while there is no assurance that wake turbulence of the previous aircraft is blown out. Where hazards H1, H2 and H3 cover faulty initiation of the CREDOS operation, functional hazard H4 focuses on an incorrect termination of the CREDOS operation. This hazard considers the possibility that ICAO wake turbulence radar separation is not established at the moment the second aircraft leaves the WTSSAV. Functional hazards H5 and H6 are concerned with an improper application of the CREDOS operation. Aircraft may deviate from their assigned standard instrument departure route due to system inaccuracies or technical errors (functional hazard H5), or due to a decision made by the crew for operational reasons (functional hazard H6). The consequence of these deviations can be that the aircraft crosses the lateral boundaries of the WTSSAV, in which case no assurance can be given that its flight path will be free of wake vortices.

Fault trees have been developed for each of the six hazards to describe the relation between the occurrence of a hazard and its potential causes. The draft fault trees were reviewed during two workshops. The first workshop was held on 17 April 2009 at NLR and was attended by an airline pilot of KLM and research test pilot of NLR, two R&D engineers, of which one was an instrument flight procedure designer, and a senior R&D manager. The second PSSA workshop was held on 14 May 2009 at NLR. That session was also attended by two former air traffic controller, an engineer and retired MD11-pilot, and a principle scientist. In the following, potential causes for each of the functional hazards were discussed. Associated fault trees are given in the PSSA [8].
**Functional Hazard H1: CREDOS operation active while wake turbulence advisory is not correct.** As this functional hazard is concerned with failures of the CREDOS system, Figure 6 forms the basis for identification of potential causes to this hazard. The figure shows that errors in the Go/No-go advice can stem from internal errors in the CREDOS Go/No-go Advisory module or from erroneous output from either the CREDOS SID Wind Forecast module or the CREDOS SID Wind Monitoring module. Moreover, errors in the output from the CREDOS Departure Planning Advisor module are expected to lead directly to erroneous input in the CREDOS Go/No-go Advisory module. The role of departure planning in the CREDOS concept of operations is not yet determined. One option (the ‘light version’\(^2\)) is that CREDOS provides its advice based on weather conditions only and that the runway controller is responsible for determining the applicability of the advice to each pair of aircraft, taking into account their weight categories and planned SIDs. Another option (the ‘full version’), considered in the current study, assumes that CREDOS system takes weight categories and departure information into account and provides an aircraft pair specific advice to apply CREDOS or not. In the absence of system failures, an incorrect Go/No-go advice could occur if the forecasted wind as used in the advice is not realized in practice. Wind forecasts will have a specified reliability, leaving space for unreliability of wind forecast. The effect of an unreliable wind forecast can be the same as that of an incorrect wind forecast.

**Functional hazard H2: RWY controller applies CREDOS while conditions are not met**
An incorrect CREDOS clearance due to a controller error can be the result from a mistake by the controller in reading the HMI, or due to a controller action that conflicts with the CREDOS operational concept. Several events when the controller does not work in conformance to the CREDOS concept have been identified in the FHA:

- The controller fails to perform the checks specified in the operational concept and clears an aircraft under the assumption that CREDOS conditions still apply;
- The controller applies suspended separation to aircraft pair although combination of their weight categories or their departure paths do not allow such suspension;
- The controller does not account for an additional time delay that ensures that the aircraft will have standard ICAO separation from its predecessor at the moment it reaches the boundaries of the WTSSAV;
- The controller confuses two runways and clears an aircraft on a non-CREDOS runway for an operation under suspended separation; or

\(^2\) The light option has been tested in the real-time simulations.
• The controller performs an unauthorized action that is not specified in the operational concept, for instance due to time pressure.

**Functional hazard H3: Separation is less than ICAO wake vortex separation after 4 NM**

Currently, the flight crew is responsible for avoiding the wake turbulence of an aircraft that have departed previously. The flight crew normally times the take-off initiation of the previous aircraft and makes sure that sufficient time has elapsed before commencing their own take-off. Because a take-off clearance under suspended separation can be expected between 60 and 100 seconds after take-off roll initiation of the previous aircraft, it makes little sense for the flight crew to time the start of the previous aircraft. The flight crew commences take-off directly (or shortly) after receiving a clearance from the air traffic controller. In case the flight crew misinterprets a CREDOS take-off clearance, it can be expected that the aircraft will take-off too early behind the previous aircraft.

**Functional hazard H4: Incorrect track keeping of leading or following aircraft**

The study initially identified two main causes of why the minimum wake turbulence radar separation is not achieved at the moment the second aircraft reaches the boundaries of the WTSSAV. These are: a faulty hand over from the runway controller to the departure controller, or a failure of the aircraft to follow the assigned SID. Possibility of an error in the CREDOS system causing the advisory trigger line to be displayed wrongly on the screen was added during the workshop. The following causes were identified that can lead to the occurrence of this hazard:

- The runway controller issues the take-off clearance before the first aircraft has crossed the advisory trigger line;
- The advisory trigger line is displayed at a wrong location on the screen (too close to the runway);
- The following aircraft catches up with the preceding aircraft due to speed differences;
- The flight crew does not follow the SID that was assigned;
- The aircraft has poor track keeping performance.

The latter two causes will bring the second aircraft outside the lateral boundaries of the WTSSAV (as also covered in hazards H5 and H6).

---

3 The CREDOS advisory trigger line is part of the CREDOS Human Machine Interface developed to assist the air traffic controllers in establishing ICAO radar wake separation minima when the aircraft is handed over by the runway controller to the departure controller (usually after leaving the WTSSAV).
**Functional hazard H5: In anticipating action, crew turns to unsafe side**

An aircraft may deviate from the SID used in CREDOS system planning for the following reasons:

- The track keeping capability of the aircraft (e.g. the flight management system and the flight control system) is not accurate enough to keep the aircraft within the lateral boundaries of the WTSSAV;
- The SID that is used by the aircraft’s flight management system differs from the one that is used in the CREDOS planning, for instance due to an error (e.g. in coding, promulgating, or uploading the procedure), or because it is outdated.

**Functional hazard H6: Crew initiates take-off while CREDOS conditions are not met**

The flight crew may deviate from its assigned SID in case of an engine failure, or for other safety reasons such as to avoid other traffic, expected wake turbulence or cumulonimbus (Cb) cloud formations.

### 7.6 Mitigations of the functional hazards

**Functional hazard H1: CREDOS operation active while wake turbulence advisory is not correct.** The runway controller can detect errors in the Go/No-go advice due to a system failure for instance using his/her expertise, or by checking the advice with actual crosswind measurements. This check is a mandatory task of the runway controller in the current CREDOS concept of operations. Obvious errors will most likely be discovered and no CREDOS operation will be initiated in such cases. However, given the current lack of detail of the concept of operations, it is not certain which failures can be detected by the runway controller and which not. Therefore, no credit can be given to the detection possibility.

**Functional hazard H2: RWY controller applies CREDOS while conditions are not met**

There are several cues in the HMI for the controller. An incorrect take-off clearance is only given when the controller misreads the Go/No-go indication, fails to check the actual crosswind, and fails to observe that the trigger advisory line on the radar display is not displayed. No mitigations (such as training, supervision) are specified for controller actions that conflict with the operational concept.

**Functional hazard H3: Separation is less than ICAO wake vortex separation after 4 NM**

No mitigations are identified for this hazard. Note that the runway controller should notice the start of the take-off roll and may be able to warn the flight crew. This is not represented in the fault tree.
**Functional hazard H6: Crew initiates take-off while CREDOS conditions are not met**

The deviation captured under this hazard is a result of flight crew decision making when a safety related event occurs. Such decisions are made taking into account the (remaining) performance capabilities of the aircraft and the presence of terrain and other traffic. The possibility of a wake turbulence encounter is of less concern under these circumstances, but may be taken into account. Because no credit can be given to the decision, the fault tree for this hazard does not include such mitigation.

### 7.7 Overview of safety requirements

This section provides an overview of the safety requirements identified above, grouped into requirements for the CREDOS system, the human operators, and the operation.

**Table 8 Safety requirements related to the CREDOS system**

<table>
<thead>
<tr>
<th>ID</th>
<th>The probability...</th>
<th>... shall be no greater than ... per take-off</th>
<th>Related hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR1</td>
<td>of an undetected error in the wind forecast, leading to an erroneous Go/No-Go indication</td>
<td>$2 \times 10^{-9}$</td>
<td>H1</td>
</tr>
<tr>
<td>SR2</td>
<td>of an undetected error in the wind nowcast, leading to an erroneous Go/No-Go indication</td>
<td>$2 \times 10^{-9}$</td>
<td>H1</td>
</tr>
<tr>
<td>SR3</td>
<td>of an undetected error in the departure planning, leading to an erroneous Go/No-Go indication</td>
<td>$2 \times 10^{-9}$</td>
<td>H1</td>
</tr>
<tr>
<td>SR4</td>
<td>of an undetected failure of the WTA module, leading to an erroneous Go/No-Go indication</td>
<td>$2 \times 10^{-9}$</td>
<td>H1</td>
</tr>
<tr>
<td>SR5</td>
<td>that the advisory trigger line is displayed wrongly on the radar display</td>
<td>$9 \times 10^{-6}$</td>
<td>H4</td>
</tr>
</tbody>
</table>

**Table 9 Safety requirements related to human operators**

<table>
<thead>
<tr>
<th>ID</th>
<th>The probability...</th>
<th>... shall be no greater than ... per take-off</th>
<th>Related hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR6</td>
<td>that the runway controller misreads the Go/No-Go indication</td>
<td>$5 \times 10^{-5}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR7</td>
<td>that the runway controller fails to check the actual wind</td>
<td>$1 \times 10^{-2}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR8</td>
<td>that the runway controller fails to see that the advisory trigger line is not displayed</td>
<td>$1 \times 10^{-2}$</td>
<td>H2</td>
</tr>
<tr>
<td>ID</td>
<td>The probability...</td>
<td>... shall be no greater than ... per take-off</td>
<td>Related hazard</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SR9</td>
<td>that the runway controller fails to inspect the Go/No-Go indication</td>
<td>$1 \times 10^{-9}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR10</td>
<td>that the runway controller applies CREDOS to an unsuitable aircraft pair</td>
<td>$1 \times 10^{-9}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR11</td>
<td>that the runway controller applies insufficient wake turbulence radar separation</td>
<td>$1 \times 10^{-9}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR12</td>
<td>that the runway controller confuses a non-CREDOS runway with a CREDOS runway</td>
<td>$1 \times 10^{-9}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR13</td>
<td>that the runway controller uses CREDOS differently than specified in the operational concept</td>
<td>$1 \times 10^{-9}$</td>
<td>H2</td>
</tr>
<tr>
<td>SR14</td>
<td>that the runway controller issues a take-off clearance before the predecessor has crossed the advisory trigger line</td>
<td>$3 \times 10^{-5}$</td>
<td>H4</td>
</tr>
<tr>
<td>SR15</td>
<td>that the flight crew misinterprets a communication as a take-off clearance for a CREDOS operation and subsequently starts the take-off roll</td>
<td>$1 \times 10^{-8}$</td>
<td>H3</td>
</tr>
<tr>
<td>SR16</td>
<td>that the flight crew selects the wrong SID</td>
<td>$3 \times 10^{-5}$</td>
<td>H4</td>
</tr>
<tr>
<td>SR17</td>
<td>of the crew deviating from its SID due to engine failure</td>
<td>$1 \times 10^{-6}$</td>
<td>H6</td>
</tr>
<tr>
<td>SR18</td>
<td>of the crew deviating from its SID to avoid clouds (Cb), other traffic, or expected wake turbulence</td>
<td>$4 \times 10^{-6}$</td>
<td>H6</td>
</tr>
</tbody>
</table>

Table 10 Safety requirements related to the CREDOS operation

<table>
<thead>
<tr>
<th>ID</th>
<th>The probability...</th>
<th>... shall be no greater than ... per take-off</th>
<th>Related hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR19</td>
<td>of an unjust Go/No-Go indication due to an unreliable wind forecast</td>
<td>$2 \times 10^{-9}$</td>
<td>H1</td>
</tr>
<tr>
<td>SR20</td>
<td>that an aircraft catches up on its predecessor due to speed differences</td>
<td>$3 \times 10^{-5}$</td>
<td>H4</td>
</tr>
<tr>
<td>SR21</td>
<td>that the aircraft deviates laterally outside the boundaries of the Wake Turbulence Separations Suspension Airspace Volume (WTSSAV)</td>
<td>$1 \times 10^{-6}$</td>
<td>H4, H5</td>
</tr>
</tbody>
</table>
The approach taken in the PSSA [8] is to apportion the Safety Objectives derived in the FHA for each functional hazard over the known causes of these hazards, and to translate the resulting tolerable risk portions into safety requirements. At this point, the PSSA must show that the resulting safety requirements are deemed to be achievable and can be implemented by stakeholders. Many safety requirements set to human operators such as the runway controller or the flight crew are in the order of $10^{-9}$ per take-off. This equates to one instance (e.g. error) in one billion departures. A runway controller will experience less than one million departures during his/her career, a pilot at most in the order of ten thousands. A requirement in the order of $10^{-9}$ per take-off set to human operators is therefore most likely too demanding. The stringent requirements set to system elements demand a high-performance system architecture. Such a system will need to have a high level of redundancy, which could significantly increase the cost of the system. Whether such level of redundancy is economically achievable with the CREDOS system, is to be assessed in a cost-benefit analysis.

### 7.8 Summary of findings

To show that all risks from internal failures have been assessed and mitigated sufficiently, the EUROCONTROL Safety Assessment Methodology (SAM) [3] has been applied. A FHA and a PSSA have been performed, using intermediate versions of the CREDOS Concept. These intermediate concept versions are not fully the same as the final CREDOS concept of operation version [10] that has recently been published.

The CREDOS FHA delivered six functional hazards with corresponding Safety Objectives. As part of the PSSA, fault trees were developed based on the proposed system architecture and the task descriptions to represent the cause/hazard relations for each of the identified hazards. The fault trees were reviewed by safety experts and operational experts in two workshops. From these fault trees, and using the Safety Objectives set during the FHA, a total of 22 safety requirements were derived: 5 for CREDOS system elements, 13 for human operators and 4 for procedures.

As a result of some safety requirements set for human operators being too demanding and hence considered unachievable, the current safety assessment does not yet
provide a basis for the safe operational introduction of the CREDOS concept. Revisiting the derivation of the safety objectives is recommended, as they have initially been developed on the basis of the 'worst case' outcome, instead of a 'worst credible case' outcome. Reconsideration of the FHA safety objectives is recommended, and should focus on quantification of the barriers in the event trees: how likely is it that the hazard will evolve into its worst credible outcome. The PSSA itself has also been set up in a conservative way. So far, little credit has been given to mitigating factors present in the CREDOS concept. A review of the CREDOS system design, of the human tasks and of the operational procedures is recommended to better describe possible mitigations. Subsequently, the fault trees should be adapted to account for these mitigations. Finally, it is suggested to readdress the FHA and PSSA on the basis of the final concept of operations for CREDOS (D4-11). The current PSSA primarily considers failures within the CREDOS operational concept. Readdressing the FHA and PSSA should then also better include performance of the CREDOS system and human performance aspects such as controller workload and radiotelephony usage.
8 Conclusions and recommendations

The CREDOS project aims to demonstrate the feasibility of a departure operation whereby the wake turbulence separations between successive aircraft are temporarily suspended under favourable crosswind conditions. This study is part of the CREDOS “Pre-implementation Safety Case” aiming at safe introduction at European airports. A Preliminary Safety Case has been carried out according to the EUROCONTROL Air Navigation System Safety Assessment Methodology applied to the CREDOS Concept.

A generic safety argument for CREDOS has been established. It covers the various parts of the life cycle including specification, implementation, transition to operational service, and operational service. As part of the CREDOS research activities mainly the safety argument for the specification phase has been further elaborated. The CREDOS wake vortex safety management recommendations [15] provide guidelines to maintain an acceptable level of safety after CREDOS is introduced into operational service. The safety argument for the specification phase of CREDOS deals with intrinsic safety of the concept, design completeness, design correctness, design robustness, and mitigation of internal failures. A summary of the findings is provided in the following.

Intrinsic safety of the concept
The objective is to show that the CREDOS concept is intrinsically safe during normal operations, i.e. the concept is capable of satisfying the safety criteria, provided that a suitable system design could be produced and implemented. In view of the aim to provide a ‘generic’ concept of operations [10] with a high-level operational context and scope, it is concluded that both the operational context and the scope are sufficiently clearly described. However, in case of local implementation, specifics of the targeted air traffic control environment will have to be considered in more detail. A crosswind criterion has been determined using both data collected during two measurement campaigns for wake vortices generated by departing aircraft at Frankfurt airport, as well as results from risk assessment simulations with an Airbus A-320 as follower aircraft. As long as only straight-out departures are considered, a crosswind threshold of about 7 to 8 knots seems to be necessary to sufficiently reduce the wake encounter risk in the area up to a height of 3000 ft when the separation is to be reduced down to 60 seconds. It has to be noted that for the risk assessment simulations no constraints on the SID combinations of leading and following aircraft have been assumed. For additional guarantee that the encounter risk is significantly further reduced, the following aircraft may be starting on an upwind route. Risk assessment simulations explicitly taking this constraint into account should confirm this assumption. The key
functionality of the CREDOS concept is to reduce spacing between subsequent departing aircraft in case of favourable crosswind conditions. In the CREDOS concept, this spacing also depends on both the determination of the size of a Wake Turbulence Separations Suspension Airspace Volume (WTSSAV) and on the quality and reliability of a local validation campaign. As this dependency is complex, it is difficult to state that this key functionality has already been shown to be consistent with safety criteria.

Design completeness
The objective is to demonstrate that all necessary Safety Requirements have been specified, or assumptions have been stated, to cover all elements, in terms of system design, that are necessary to fully implement CREDOS operations. System boundaries are sufficiently clearly defined at this stage of the system development. The operational concept fully describes how the system intends to operate. High level concept safety validation objectives have been specified and broken down further into initial safety validation requirements. It is observed that safety requirements on external elements have been specified in other documents. It is concluded that the high-level system design is complete and can be used for further development and implementation.

Design correctness
The objective of this section is to show that the concept of the system design functions correctly and coherently under all normal environmental conditions. With respect to internal coherency, it is observed that internal coherency of the system design will be achieved if recommendations on controller familiarity, controller procedures, division of controller responsibilities, and SID compatibility are fully considered (see Section 5.2 for the full details). With respect to correct dynamic functioning of the design, it is observed that there are few issues to be resolved before implementation. The overall concept of CREDOS was well received by air traffic controllers participating in the real time simulations [11]. Four further recommendations should be taken into account for local implementations of CREDOS. These recommendations concern a) the mandatory transmission of wind information in take-off clearance for all aircraft in cases when a basic advisory tool is used, b) controller procedures that should be well defined in case of wrong turn (e.g. if departure controller acts first and then informs the runway controller or the other way around), c) refinement of the proposed phraseology for non-nominal events would need to be refined, and d) the use of a status indicator that takes into consideration the assigned SIDs for leading and following aircraft to assist the controller and reduce the risk of mistake. Overall, it is concluded that - provided that these recommendations are followed - there is sufficient evidence that the CREDOS system design as specified and simulated does function correctly and coherently.
Design robustness
The objective is to show that the application system design is robust against external abnormalities in the operational environment. Five external abnormalities have been considered: aircraft failure (e.g. engine failure), voice communication system failure, degradation of surveillance systems information, meteorological systems information, and/or flight data/information. It is concluded that the CREDOS system can handle all these external abnormalities in a robust way, i.e. no risks that otherwise would not be present are induced. However, should a sudden decreased crosswind occur, the aircraft could be exposed to a higher wake encounter risk than anticipated. The use of wind monitoring systems up to about 2000 feet height is required for robustness.

Mitigation of internal failures
To show that all risks from internal failures have been assessed and mitigated sufficiently, the EUROCONTROL Safety Assessment Methodology (SAM) [3] has been applied. A Functional Hazard Assessment (FHA) [7] and a Preliminary System Safety Assessment (PSSA) [8] have been performed, using intermediate versions of the CREDOS Concept. The CREDOS FHA delivered six functional hazards with Safety Objectives. Using also the CREDOS PSSA fault trees, 22 safety requirements were derived: 5 for system elements, 13 for human operators and 4 for procedures. As a result of safety requirements set for human operators being too demanding and hence considered unachievable, the argument for mitigation of internal failures is not yet satisfied by the current FHA/PSSA. Revisiting FHA and PSSA is recommended, as both have been developed conservatively on the basis of 'worst case' outcomes. So far, little credit has been given to mitigating factors present in the CREDOS concept. It is suggested to combine this revisiting effort with readdressing the FHA and PSSA on basis of the final concept of operations for CREDOS [10]. Readdressing the FHA and PSSA should then also better include performance of the CREDOS system and human performance aspects such as controller workload and radiotelephony usage.

Overall conclusion
Safety validation exercises specified in the CREDOS Validation strategy and plan [5] have been performed with the aim to gather the evidence to show that each of the five sub-arguments is satisfied. The main observations and findings are:

- Operational evaluation of the CREDOS concept and system design through real-time simulations seems to have provided sufficient safety evidence regarding the arguments for system design completeness, correctness and robustness;
- Additional safety work will be needed to satisfy arguments for intrinsic safety and mitigation of internal failures (current safety requirements may be too demanding).
References

[5] CREDOS D4-3; Validation strategy and plan
[9] CREDOS D4-10; Human Factors Case
[10] CREDOS D4-11; Operational concept
[12] CREDOS D2-6; WP2 Data analysis and wake vortex behaviour modelling
[14] CREDOS D3-10; Safe separation distances for take off and departure