Analysis of safety assessment methodologies and criteria of FAB Europe Central partners
Jelmer J. Scholte, NLR Air Transport Safety Institute; scholte@nlr-atsi.nl

This paper is endorsed by FAB Europe Central’s Standing Committee Safety (SC SAF).

Abstract

Functional Airspace Blocks (FABs) are being developed in Europe as a step in the development of the Single European Sky. The FAB Europe Central (FAB EC) project is developing a FAB over Belgium, the Netherlands, Luxemburg, Germany, France and Switzerland. To assure the safe development of this FAB, proper safety cases will have to be presented to the applicable authorities. Each of the main six involved Air Navigation Service Providers (ANSPs) has its own safety assessment process and safety criteria, and each of the ANSPs is certified by its respective National Supervisory Authority (NSA). For common developments however it is not logical to follow different processes. In support of the development of a shared view on safety case development practices for use in FAB EC, purpose of the work described in this paper is to compare the safety assessment methodologies and criteria of the six main involved ANSPs. The main result is an analysis of methodologies and criteria, showing both important commonalities and significant differences, and where possible an understanding of the reasons for the differences. Based on these results, specific recommendations are made regarding the development of shared safety case development practices for use in FAB EC. Finally, it is sketched how the involved ANSPs are currently proceeding.

1. Introduction

In order to meet the future needs and challenges of a growing air travel and transport industry, the European Commission (EC) launched the Single European Sky (SES) initiative. As a step in the development of this SES, EC regulation [EC 551/2004] requires the development of airspace blocks that are based on operational requirements and established regardless of State boundaries, where the provision of air navigation services and related ancillary functions are optimised and/or integrated. Developing such a Functional Airspace Block (FAB) over Belgium, the Netherlands, Luxemburg, Germany, France and Switzerland is the objective of the FAB Europe Central (FAB EC) project.

In assuring the safe development of this FAB, proper safety cases will have to be presented to the applicable authorities. Each of the involved Air Navigation Service Providers (ANSPs) has its own safety assessment process and safety criteria, and each of these ANSPs has been certified by its respective National Supervisory Authority (NSA). The development of a safety case for FAB EC is likely to feature many changes that are common to or similar for several of the involved ANSPs. It would be inefficient to have

---

1 FAB Europe Central’s Standing Committee Safety consists of the following 7 organizations: ANA Luxembourg (Administration de la Navigation Aérienne Luxembourg), Belgocontrol, DFS (Deutsche Flugsicherung GmbH), DSNA (Direction des Services de la Navigation Aérienne), LVNL (Luchtverkeersleiding Nederland/ Air Traffic Control the Netherlands), MUAC (Eurocontrol Maastricht Upper Area Control Centre), and skyguide (swiss air navigation services ltd)
each ANSP assess safety individually for such subjects. Therefore a development is envisaged where these methodologies are converged towards each other, in order to safeguard the investment made by the ANSPs in their processes whilst allowing developments for FAB EC to start.

This paper describes the main results of a study done in 2008 [Scholte et al., 2008] that aimed to support reaching a shared view on safety case development practices for use in the FAB EC development, by comparing the safety assessment methodologies and criteria of six of the seven involved ANSPs: Belgocontrol, DFS, DSNA, LVNL, MUAC, and skyguide. This comparison aims to identify the main commonalities between these ANSPs’ methodologies and criteria, the main differences, and an understanding of the reasons for the differences. Unlike [Scholte et al., 2008], this paper presents differences and commonalities without disclosing details on individual ANSPs.

The analysis is based on inputs provided by the ANSPs in documents, open discussions in workshops with representatives of each ANSP, and reviews. Therefore, the ANSPs’ views on the current practical application of the own safety assessment methodology and criteria are the subject of the systematic analysis, including practical deviations and recent improvements that are not yet described in documents. No attempt has been made to verify the views of the involved ANSPs, and future developments are not considered in detail. The comparison has a focus on the safety assessment methodologies and criteria as they would be applied for changes that resemble the introduction of FAB EC best, i.e., large changes with potentially large impact. The actual safety assessment and mitigation activities proposed by the safety assessment methodologies receive a certain focus; less detail is provided on other important activities as planning, evaluating, and validating safety assessments.

As a first step in the comparison, a review was done of each ANSP’s documentation of its safety assessment methodology and criteria, and a few reports of performed safety assessments. Next, for each set of methodology and criteria a summary was developed. These summaries all used the same structure of eight themes, each further subdivided into more detailed topics. Workshops were next organized with representatives of the six ANSPs to develop a joint understanding of the main commonalities, the main differences, and the reasons for the differences. The two two-days’ workshops ([MoM WS1] [MoM WS2]) followed the structure of the summaries, and used them as input. Some further relevant material was used to finalize the analysis.

For each of the eight themes the main results of the analysis are presented in a separate section: status and role of methodology and criteria (Section 2); organization of safety assessment (Section 3); types of changes to assess (Section 4); scope of assessment (Section 5); safety criteria (Section 6); the assessment process (Section 7); modelling means and tools (Section 8); and communication (Section 9). Next, Section 10 describes the way forward, and Section 11 provides concluding remarks.

---

2 The adopted structure was developed based on requirements from [ESARR 4], the steps and sub-steps of [ANS SAM], the indicators for quality of safety validation from [Everdij et al., 2006], a previous analysis of ATM safety criteria of a number of ANSPs [De Jong, 2005] and, a FAB EC document providing a survey of the Safety Management Systems (SMSs) of the involved ANSPs [FAB EC WP7.5 ph1].
2. Status and role of methodology and criteria

The six sets of methodologies and criteria have in common that they have each reached a certain maturity, with safety assessment used for design and/or decision-making, but with continuous innovation still deemed necessary.

Eurocontrol’s [ESARR 4] and its transposition in EC regulation [CR 2096/2005] pose relevant requirements to ATM risk assessment and mitigation. Existing reviews of compliance to these regulations can play a role in the maturity of the methodologies and criteria.

In line with EC regulation [CR 1315/2007], NSAs review the ANSP’s methodology and criteria on their compliance to [CR 2096/2005] as part of their SES certification, and review selected individual applications. The six ANSPs have all been SES certified by their respective NSAs, which implies that these NSAs have evaluated the methodologies and criteria as being compliant to [CR 2096/2005]. At the moment of conducting this study, little to no experience existed yet with feedback from NSAs to individual applications, as the supervision process according to [CR 1315/2007] was still rather new.

For a review as proposed means of compliance (PMC) to ESARR 4, methodologies and criteria could be submitted to the Safety Regulation Unit (SRU). Some of the considered ANSPs submitted one or more versions of their safety assessment methodology and/or criteria to SRU as PMC to ESARR 4. Between 2001 (when ESARR 4 came in force) and 2008 (when this study was conducted) SRU published compliance reports for a total of three PMCs. These three include an earlier version of the safety criteria of one of the six ANSPs considered, and SAM [ANS SAM], to which the six sets of methodologies and criteria can all be related. For each of these three PMCs SRU concluded that some ESARR 4 requirements are fully met, and others are not (see [EAM 4 / AMC] for an overview).

Each of the six ANSPs has applied the methodology and criteria in many safety assessments, and is working on further improvement. The six ANSPs agree that further innovation to the methodology and criteria is needed. Each of the ANSPs uses safety assessment results for decision-making, including use of intermediate safety assessment results for detailing design, and for some ANSPs also for redesign. The eventual decision to implement a change is made only if a safety assessment is available in which the proposed design is shown to fulfil safety goals. For each ANSP, safety assessment is only one input for decision-making on the acceptability of a change, next to inputs regarding for example: capacity, efficiency, environmental aspects, legal aspects, interoperability aspects, company risks, economical aspects, and the safety perception by their Air Traffic Controllers.

3. Organization of safety assessment

Regarding the organization of the safety assessment, the relations with the NSA are organized to some extent similarly for the ANSPs, but interesting differences are identified in the internal roles and responsibilities.

EC regulation [CR 1315/2007] provides criteria by which it can be determined whether the NSA shall review the safety case. NSA review is required for changes for which the severity assessment conducted by the ANSP in accordance with [CR 2005/2096] determines a severity class 1 or 2 for the potential effects of the hazards.
identified, and for changes for which the introduction of new aviation standards is required. The changes for which the NSA shall review are called ‘major changes’, as opposed to ‘minor changes’, for which this review is not mandatory. At the moment of conducting this study, experience with this review process were still scarce. Three relevant observations were made by the involved ANSPs:

- The ANSPs need to provide a severity assessment following [CR 2096/2005] to allow the NSA to determine the need for review. Hence, this severity assessment is also necessary for assessments that do not need review.
- The severity of a hazard may not be a good indicator of risk, as risk depends also on the probability of occurrence of the hazard and its consequences of that severity.
- In line with [CR 2096/2005] it is required to determine severity by determining the ‘worst credible effect’ of hazards. However, other severity assessment approaches are available and may be preferred. A potential disadvantage of the required approach is that it is unclear how it respects the principle that each hazard can lead to an accident, depending on the conditions and the occurrence of other hazards.

Differences are identified in the arrangements that ANSPs have to timely notify its NSA of proposed changes differ, and in the role of NSAs in actual safety assessments. Example arrangements for notifying differ from doing this for many alterations including some that might be considered too insignificant to be considered a ‘change’, to clustering changes into a small number of large programs to be followed by the NSA. Some ANSPs invite the NSA to safety assessment sessions; although usually such invitation is not accepted. Here it may play a role that ‘involvement’ of the NSA may prevent or seem to prevent ‘independence’ of the NSA. The legal consequences of NSA involvement in the safety assessment process, even as an observer, are also not completely clear.

Main commonality in the internal organization of the safety assessment for a change is that a person is appointed as responsible for the change who is also responsible for a safety assessment being done, who also approves it, but who does usually not conduct the safety assessment. An interesting difference is identified when considering how the primary responsibility for safety assessment lies with operational experts, technical experts, or formal safety assessment experts, as four approaches are identified:

- Responsibility for safety assessments is with operational and/ or technical experts, who are supported by formal safety assessment experts.
- Responsibility for safety assessments is with operational and/ or technical experts, with specific responsibilities and training in formal safety assessment.
- Responsibility for safety assessments is with formal safety experts, who perform safety assessment supported by operational and/ or technical experts.
- Responsibility for the safety assessment is with an operational expert, technical expert, or a formal safety assessment expert, depending on the type of change.

The motivation provided for having primary responsibility with formal safety assessment experts is that critical changes may need specialization in formal safety assessment approaches. Even with these differences, a commonality is that in all cases somebody who has received specific training in formal safety assessment is usually part of the project team responsible for the change. Trainings mentioned are in-house training, on-the-job training, training from Eurocontrol IANS, and training from NLR.

Regarding decision-making on changes based on the safety assessments, at all ANSPs this generally involves the operational management, though at some ANSPs the
decision on certain smaller changes is sometimes taken on a lower level in the organisation. A safety assessment required for decision-making needs approval by at least the person responsible for the change, and usually by several persons more, for example the person responsible for the safety assessment, an independent reviewer, the head of operations, the safety manager, and depending on the scope, the technical department.

The roles of the safety management functions of the six ANSPs have provision of oversight, delivering support on a safety methodological level, and reviewing safety assessments in common. Also some differences are identified here:

- The safety management function is either only involved in development and maintenance of safety methods, or also applies the safety methods.
- Safety management can either be a dedicated process, or be embedded in a broader process for overall performance management of the ATM operation.

4. Types of changes to assess

The ANSPs’ views on the types of changes to be assessed on safety show many commonalities, but also a significant difference. Background is that regulations do not specify for which changes safety assessment is required. For example EC regulation [CR 2096/2005] requires air traffic service providers to do a safety assessment “for any changes to those parts of the ATM functional system and supporting arrangements within his managerial control”, while not further defining the term ‘change’. The six ANSPs have the following in common in the interpretation of this term:

- An event is only considered as change if the safety of air traffic may be influenced;
- Events considered to be already part of the ATM system and its ‘operational envelop’ (e.g., changing runway combinations) are not considered as changes. It is argued that the safety of such events is assured via [ESARR 3] and its transposition in EC regulations.
- Tactical actions that are not part of the operational envelop usually do not allow a formal safety assessment because of time pressure.

A further commonality is that currently none of the six ANSPs structurally performs safety assessment of institutional and organizational changes, such as merging or combining currently separate APP and ACC departments into one department. It is noted that ESARR 4 excludes these issues from its scope, but that [CR 2096/2005] does not make this restriction. The ANSPs argue that it should at least be considered whether such change can impact safety. Identified current practices do include a separate process for managing this type of changes, and more incidental safety assessment of this type of changes.

Also, a commonality is that the six ANSPs follow the principle that local implementations of ICAO described operations do not structurally need to be assessed on safety by themselves. It is agreed that for local implementations of large ICAO described operations (e.g., introducing parallel independent departures on runways that are not closely spaced), it is preferred to perform a safety assessment. For many small technical changes it is argued that safety is assured by detailed ICAO-defined procedures, such that a safety assessment of the specific local issues of the implementation may suffice.

The main identified difference for the type of changes to be assessed on safety follows from the ANSPs’ interpretation of the term ‘under managerial control’ in [CR 2096/2005]. Two approaches are identified:
All changes in the operation are considered that might influence the provision of safe separation on safety, independent from who is responsible for the change. This includes e.g., changes in the way Meteo provides its data, changes to the taxiway system, or changes to the airspace structure.

In principle only changes to the own ATM system are considered. The background of this difference is that either the delivery of safe separation to aircraft under control can be considered as primary responsibility, or the proper functioning of the own ATM system. It is noted that a practical problem for assessing the effects of changes for which a different organisation is responsible, may be that a formal mechanism should be in place to assure that the ANSP is timely aware of all such changes.

Whereas the ANSPs have in common that they each use a classification of changes to select or detail the safety assessment approach for a change, differences exist in the classes used and their use. Two approaches are identified:

- Explicitly tailoring the safety assessment approach to a parameter representing the safety criticality of the change (e.g., severity or safety significance).
- Current or future re-use of safety assessment material is decided upon based on a parameter indicating to which the change is unique.

An interesting observation on the class names adopted by ANSPs is that some have opposite connotations for some ANSPs; e.g., class 1 means highest safety criticality for one ANSP and lowest safety criticality for another ANSP.

5. Scope of assessment

In the ANSPs’ approaches to scoping the assessment both important commonalities and significant differences are identified. Several of the differences can be traced back to the existence of three leading motives in scope selection, of which one has been selected by each ANSP:

1. The scope is determined in terms of risk associated with certain accident types. Here, causes of accidents are included irrespective of whether they are in or outside the ANSP’s managerial domain. The rationale for this approach is that this way all risks related to safe separation provision are considered.

2. The scope is defined in terms of risks related to the consequences of hazards identified on the boundary of the ANSP. The rationale for this approach is that this way risks in the ANSP’s own managerial domain are focused upon. It is noted that in practice sometimes events on the boundary of ATC equipment and the Air Traffic Controller (ATCo) are considered as hazard on the boundary (e.g., radar failure).

3. The scope is defined in terms of risks related to the consequences of hazards identified on the boundary of a sub-system under assessment. The rationale for this approach is that this way the focus is on risks caused by e.g., a new sub-system.

The following identified differences are related to these leading motives:

- Using leading principle 1, airborne related hazards (e.g., a pilot not complying to a correct ATCo instruction) and airborne mitigations are both formally included in safety assessments, as far as they play a role in in-scope accident types. Using leading principles 2 and 3, airborne hazards are in principle not taken into account, and coverage of airborne aspects is restricted to airborne causes of a hazard on the defined boundary and the role of the airborne domain in mitigation of such hazards. It is noted
that if an ANSP’s change affects the pilot’s operation, then the ANSPs agree that it should be assured in one way or another that airborne hazards are properly assessed and mitigated.

- Using leading principle 1, risk in which the ANSP is involved but that is unrelated to separation responsibility (e.g., risk regarding VFR traffic in class E airspace) is not formally included. Here, the ANSP is however available for providing support in analysing the effects. Rationale is that the ANSP does not decide on the acceptability of safety risks for traffic for which the ANSP has no separation responsibility. Using leading principles 2 and 3, these risks are included in their safety assessments and decision processes.

- For leading principle 1, external events are included in scope as far as they play a role in the occurrence and prevention of in-scope accident types. For leading principles 2 and 3 external events are only included if they are a cause of an in-scope hazard, a mitigation for an in-scope hazards, and/ or if they provide relevant context for the circumstances under which in-scope hazards occur.

Whereas all six ANSPs include hazards resulting from ground-based safety nets in safety assessments of this safety net or of a different subsystem, a significant difference exists with respect to the benefits of airborne and ground-based safety nets. It is noted that the issue whether the benefits of ground-based safety nets should be included in safety assessments has been unclear since the adoption of ESARR 4 by SRC. Whereas ICAO’s en-route TLS value [ICAO Annex 11] assumes that ground based safety nets should be taken into account, ESARR 4 and its explanatory document [SRC pol doc 2] could be interpreted otherwise. This criticism is expressed in e.g., [Brooker, 2004]. Recently, SRC has proposed a policy paper [SRC AP 28] which tries to solve this confusion. In this paper it is explained that ground based safety nets may not be assumed just to deliver an assumed factor of safety improvement in safety assessments, but under a certain set of conditions the safety impact may be taken into account. Risk reduction by airborne systems is not yet taken into account by the current nor by the proposed SRC policy, and also [ICAO Annex 11] does not take risk reduction by airborne systems into account. Three approaches for covering benefits from safety nets have been identified among the six ANSPs:

- Not including benefits of airborne or ground safety nets in safety assessments;
- Includes benefits only of ground-based safety nets, and only as mitigation for hazards from which this safety net is independents;
- Including or excluding ground and/ or airborne safety nets depending on the type of change and situation.

Provided rationales for including the benefits of safety nets in safety assessments are to give incentive to improvement of airborne safety nets, ground-based safety nets, and their collaboration, and to be able to compare assessed safety levels with actual safety levels. A provided rationale for excluding safety nets in safety assessments is to strive for delivering safety without depending on safety nets.

Further results regarding scoping of the safety assessment are:

- The scope can be detailed in terms of e.g., functions, system elements or partial operations.
• Recently, [Fowler et al., 2007] raised awareness that historically many safety assessments focused on ‘failure’ of a certain ATM sub-system, whereas the ‘success’ side of a change has often not properly been addressed. Most ANSPs already include aspects unrelated to failure of the considered ATM sub-system in one way or another in their safety assessment approach. An identified way of doing this include covering all risks involved in an accident type in an integrated way, including both risk related to failure and risk in absence of failure in an integrated way.

• Security issues are either not considered in safety assessments, or to some extent as cause of safety hazards. The rationales provided here are that on one hand safety and security of air traffic operations have their obvious interrelations, but on the other hand safety and security assessments each have their own characteristics.

• Combinations of hazards start to be addressed in one way or another by most ANSPs. The approaches vary from using only sequential modelling of causes and failing mitigations, via covering also the most obvious combinations of hazard as a new hazard, to connecting relevant combinations of hazards in a risk model.

6. Safety criteria

Whereas the six ANSPs have in common that they have some experience with the development of ATM safety criteria, many differences are identified in the statements and derivation of their criteria. An objective comparison of their stringency based on the values used is deemed not to be feasible. This view is supported by an earlier attempt to compare two sets of ATM safety criteria [De Jong, 2005].

The first development among the ANSPs were started in 1998, and several sets of safety criteria have been improved or updated over the years. Four approaches in development of safety criteria have been used:

• Development of a risk classification scheme starting from ESARR 4 using one of the models from [ED125];
• Development of a risk classification scheme is developed starting from ESARR 4 using on a conjectural density function of the number of risks over the magnitude of the risks;
• Development of a scheme based on incident data;
• Development of criteria based on worldwide accident statistics.

The multiple differences in the statement of the ANSPs’ criteria include:

• The criteria being purely quantitative, or a mix of quantitative and qualitative;
• Direct applicability of the criteria to the scope of assessments; or the necessity to first tailor them to the level of e.g., ATC units, flight phases, or all hazards of a certain class;
• The number of different classes used to classify risk and to indicate the consequences for decision-making (this number ranges from two to four);
• The criteria being defined in terms of risk related to the worst credible effect of hazards, to all effects of hazards, or only to accidents;
• The various units in which frequencies are expressed;

It is noted that also in the use of criteria differences are identified: The criteria are either used early in safety assessment for the definition of safety objectives, which are
used in the further safety assessment; or at the end of the safety assessment, in comparing them with the assessed risk level.

7. The assessment process

An important commonality in the safety assessment process is that the ANSP each uses a similar phasing, and that they all use similar process steps. Differences exist in which activities are done per phase, and in how the process steps are done. In this section, first the phasing is considered, and next some detail on a number of process steps or activities is presented.

The six safety assessment methodologies all adopt the overall phasing of SAM [ANS-SAM], first investigating whether an ATM sub-system or concept can be made sufficiently safe (FHA phase), next how it can be made sufficiently safe (PSSA phase), and finally whether it has been made sufficiently safe (SSA phase). The sub-steps of the phases are for none of the ANSPs completely similar to each other or to SAM: different sub-steps are used, sub-steps are differently grouped, and a complete risk assessment cycle of identifying, analysing and mitigating risk is either in principal done once or in each of the three phases. Background of these differences is formed by methodologies being developed prior or in parallel to SAM, and by the tailoring of methodologies to the considered company.

Learning the operation: Before starting the safety assessment, the assessors usually first retrieve a good understanding of the operation or concept under development. At ANSPs where the safety assessment performers are not involved in the development process there is a more significant need to learn the operation under development. Primary identified ways to do this are studying the design material, and functionally decomposing the system.

Hazard identification: All six ANSPs use workshops as primary means for hazard identification. In these workshops, some ANSPs adopt a functional decomposition approach, some a ‘pure’ brainstorming approach, and some combine these two approaches. Information from literature, databases, and previous studies are used for preparation of workshops or for completion of the results. It is noted that SAM [ANS SAM] presents guidance for both the functional decomposition approach (FHA, Chapter 3, GM B1) and the ‘pure’ brainstorming approach (FHA, Chapter 3, GM B2, originally developed in [De Jong, 2004]), and recommends to have the functional decomposition approach take place after the brainstorming approach.

Hazard structuring: In hazard identification workshops based on functional decomposition, the moderator of the workshop usually takes care that the output is already structured e.g., into hazards, causes, and consequences. In case a ‘pure brainstorming’ approach is used, the resulting list of unsorted hazards needs structuring. The approach used for this is that a risk model is developed, which is done either during or after the workshop.

Effect identification and severity assessment: A number of approaches are used for identifying the effects of the hazards and assessing their severity: The worst credible effects of hazards are considered, all their effects are considered, or only accident consequences are considered. For each ANSP, the approach is already determined by the similar differences identified in the statements of the safety criteria. For severity
assessment, the applicable severity class is either directly selected from [ESARR 4], or the severity indicators from SAM are used.

Safety objectives specification: Four approaches are identified in the specification of safety objectives:

- Safety objectives are allocated to a level comparable to flight phases, and can already be selected from the safety criteria at the start of the safety assessment.
- Safety objectives are allocated to the level of individual hazards. After severity assessment, the conditional probability that a hazard leads to effects of the considered severity is assessed and taken into account in the determination of the safety objectives.
- Safety objectives are allocated to the level of individual hazards. After severity assessment, the safety objective is directly assigned from the safety criteria based on the assessed severity.

An important argument (see also [ANS SAM], GM G to FHA Chapter 3) for selecting the latter approach is that it is relatively easy to apply, because the recurring difficult estimation of conditional probabilities in safety assessments has been avoided by including a generic estimate in the safety criteria. An important argument for selecting the first or second approach is that the conditional probability of a hazard leading to effects of a certain severity is generally dependent on the specific change and hazard considered; using a pre-defined conditional probability may thus lead to safety objectives being too stringent or too lenient.

Safety requirement specification: To enable safety objectives to be achieved, usually safety requirements are identified on a lower level, typically the level of ATM system elements that can uniquely be allocated to a human operator, a procedure, or a piece of equipment. Often, a risk model is used in which the occurrence of hazards and their effects is modelled in terms of the frequency of causes that can uniquely be allocated to humans, procedures, and equipment. The following two approaches are predominantly used in identification of safety requirements:

- The top-down approach, in which the safety objective is decomposed into candidate safety requirements on the level of causes, in such a way that satisfaction of the candidate safety requirements implies satisfaction of the safety objectives. If all these candidate safety requirements are realistic and attainable then these are designated to be safety requirements, potentially after some fine-tuning. Otherwise, alternative candidate safety requirements are identified, or additional mitigation means are identified.

- The bottom-up approach, in which attainable and realistic candidate safety requirements are allocated to the causes, and it is verified whether satisfaction of these would guarantee satisfaction of the safety objectives. If this is the case, the candidate safety requirements can be designated to be safety requirements, and otherwise more stringent candidate safety requirements are identified, or new risk mitigations are identified using a risk mitigation strategy.

In each of the six ANSPs, the top-down approach is primarily used, the bottom-up approach is primarily used, or both approaches are combined. Two complementary approaches have been identified, one based on ‘system criticality’, and one based on safety requirements coming from standards for security of technical equipment. In a variation to the bottom-up approach, the frequencies of causes is assessed based on a
detailed design, and once the safety objective is met this design turns into a set of safety requirements.

Identified formats in which safety requirements are expressed are assurance levels (Software Assurance Levels, Procedure Assurance Levels, and Human Assurance Levels), training requirements, new procedures, and quantitative or qualitative requirements on hardware (e.g., on integrity and reliability).

**Frequency assessment:** A variation in approaches has been identified on the following topics:

- Using only absolute assessments or allowing relative assessments. Identified reasons for only using absolute assessments are to maintain coherence between safety assessments, and a good view on the complete safety risk picture of the ANSP. Provided reasons for using relative arguments or complete relative safety assessments are that changes are often triggered by foreseen safety improvements, and that they sometimes make the safety assessment less complex or labour-intensive.

- Assessing human performance. Several approaches are adopted for this particularly difficult item, including qualitative assessments, the use of human assurance levels, expert judgement, surveys, monitoring certain indicators in operations, considering incident reports, simulations, and Eurocontrol’s Human Factors case.

- Dealing with uncertainty; identified approaches are striving for the collection of more data, introducing the new concept in phases, use of balanced expert judgement, use of uncertainty bands, use of ALARP principles, and use of conservatism.

**SSA phase:** In the SSA phase evidences are gathered on whether the behaviour of the sub-system or concept is indeed in accordance with the safety requirements. This is usually a recurrent and iterative process for the six ANSPs, in which qualitative and quantitative arguments are given to justify the acceptability of the risks. Evidences are retrieved from new design documents coming available, testing, simulations, empirical expert judgement, audits, et cetera. In case a safety requirement or safety objective is not met, usually iteration of the PSSA phase or FHA and PSSA phases are needed. Some ANSPs define indicators that will be monitored with specific attention in the SSA. All ANSPs use phases that are distinguished in the SSA phase. A fairly common phasing is formed by the four phases Implementation & Integration, Transfer into Operations, Operations & Maintenance, and Decommissioning, though deviations exist. Also, different approaches exist to tackling each of these phases, e.g., the ‘transition’ phase is considered integrally in the safety assessment, as a separate phase in the safety assessment, or in a separate safety assessment. All ANSPs consider the ‘decommissioning’ phase only once it becomes imminent.

### 8. Modelling means and tools

The comparison of modelling means and tools shows a rich variation, as all involved ANSPs use modelling means, analysis tools, and/ or tools for quantification of parameters. Some ANSPs prescribe certain modelling means to maintain coherence, whereas others prefer to select a mean depending on the specific study. To give a taste of the variation, identified means to model risk in terms of contributing parameters are fault and event trees, Bayesian Belief Networks, Collision Risk Models (e.g., for specific studies involving deviations on track), and TOPAZ (e.g., for studies in which the geometry of conflicts is important in the assessment of conditional collision risk). Further
analysis tools in use include Structured Analysis and Design Technique (SADT) for functional decomposition, mainly for technical issues, and Failure Mode and Effect Analysis (FMEA). A modelling tool used for documentation of a safety case is Goal Structured Notation (GSN). For quantification of parameters, all ANSPs have used statistical data, fast time or real-time simulations, and expert judgement. Also the use of literature studies and studies for similar subjects is mentioned.

9. Communication

The communication related to safety assessment at the six ANSPs shows many common points, with for example all ANSPs agreeing on the importance of effective feedback from safety assessment to the operational development process. The main identified difference is that this feedback is either assured by the developers being responsible for doing the safety assessment, or by having effective communication loops between safety assessment team and development team.

At all six ANSPs, templates or specific formats are in use for documentation of safety assessments, which differ in scope and structure. For example, safety assessments are either documented as a whole, or per main phase of the assessment. A document control process and archiving policy is usually in force. The policy with respect to sharing of safety assessments with others is very different for some ANSPs, varying from the ANSP considering all safety assessments to be of a sensitive nature, to sharing of all safety assessments with interesting persons or organizations.

All ANSPs provide attention to traceability in safety assessments, although the level of traceability is sometimes tailored to the significance of the safety assessment. An identified aspect of traceability is how the relations are between safety criteria, safety objectives, safety requirements, mitigation means, and the evidences for their attainability and effectiveness. Also traceability of assumptions is mentioned. Some ANSPs start to give attention to traceability of safety requirement identification over different safety assessments.

ANSPs have further internal communication platforms for sharing of experiences, presenting safety assessment results, discussing potential improvements to safety assessment methodologies, et cetera. These communication platforms include regular meetings, ad-hoc meetings, and articles on intranet or in a bulletin. At most ANSPs safety assessments are internally shared via e.g., intranet or a database, at the other ANSPs access to safety assessment is reached via the SMU. Communication of safety assessments to affected stakeholders is also mentioned as a highly important activity.

10. Discussion

The analysis shows both important commonalities and significant differences. For further development of a common methodology and criteria for use in common parts of a safety assessment, specific recommendations have been made for five key activities:

a. Development of criteria for determining the common parts of a safety assessment:
   New operational concepts subject to safety assessment will likely have aspects that are common to all FAB EC partners, aspects that are common to a smaller number of FAB EC partners and changes that are unique to one FAB EC partner. Likewise, parts of the safety assessment can be common to the FAB EC partners, or local. Criteria could be developed to facilitate determining the common parts of a safety assessment.
The many commonalities in the ANSPs’ interpretations of ‘changes’ for which safety assessment is needed (Section 4) may facilitate determining the common parts of a safety assessment. The main issues in determining such common parts are expected to be unrelated to the few identified differences, as more significant issues will need to be addressed, e.g., how to make a sensible division between FAB EC-wide and local issues, as for all FAB EC wide changes local and FAB EC wide issues may be identified.

b. Definition of the scope of the common parts of a safety assessment: The many common views of the ANSPs to the scope of a safety assessment identified in Section 5 make a good starting point. Most of the identified differences are mainly on a technical level, and for these it should be well possible to define an appropriate approach in scope definition that is acceptable to all six ANSPs. Some differences were identified that are more on a fundamental and/or philosophical level, and that potentially have significant practical consequences:

- To which extent should hazards outside the managerial domain of the ANSPs be included in the common safety assessment?
- To which extent should benefits of ground-based and airborne safety nets be taken into account in the scope of an assessment?

A common view is best derived on these issues before starting an actual safety assessment.

c. Definition of safety criteria for use in the common parts of a safety assessment: As the safety criteria of the six involved ANSPs show many differences in statement and in derivation, and as an objective comparison of their stringency is not expected to be possible, it is deemed best to start a separate activity for determining safety criteria for use in the common parts of a safety assessment. This activity should not be limited to considering the differences and commonalities between the ANSPs’ safety criteria identified in Section 6, as several additional issues play a role. Example issues are: how can a total allowable safety risk budget be distributed over the common parts of a safety assessment and the local parts? How can a risk budget be distributed over involved states and ANSPs? Depending on the answers to such questions, it could occur that a certain assessed safety risk level for one element in the FAB would be acceptable in some states, but not in the other states.

d. Definition of safety assessment approach for common parts of a safety assessment:

The comparison of the safety assessment approach and techniques in use by the six ANSPs (Sections 7 and 8) show sufficient grounds to develop a common approach, and also show a rich variation of techniques. This variation provides an opportunity to learn from each other, and to develop an approach that is as much as possible suitable for a FAB EC safety assessment. These should also take profit of the ANSPs’ ongoing improvement and innovation regarding safety assessment methodology and criteria. The development of the safety assessment approach is expected best to be done supported by discussions on a technical level, in which the approach and techniques most suitable for a FAB EC safety assessment are selected.

e. Determining the organization of the common parts of a safety assessment: In determining the organization of a safety assessment, the leading motive of the improvement of ATM should not be lost: The overall development and validation process of improved ATM should be effectively organized. The common parts of a
safety assessment and the relations with other processes should hence be organized in line with this leading motive. It is of particular importance that safety assessment results are timely taken into account in the operational and technical design. Therefore, effective feedback loops and iteration of safety assessment activities deserve attention in the definition of the organization. Likewise, the relations with the decision-makers in the multi-stakeholder development process should be paid attention to, as should the relation with other stakeholders and the NSAs. Further topics of importance in safety assessment organization include the definition of responsibilities, the involvement of each of the ANSPs, the roles of formal review and/or validation processes, documentation of (partial) results, and the relations with the local parts of a safety assessment.

As significant time and effort is expected to be needed to further develop a common safety assessment approach for common changes, two pragmatic alternative approaches have been proposed in [FAB EC SRAM]. These can directly be used as they are directly based on the six current sets of methodologies and criteria. The two approaches, which both assume a common and local parts of the safety assessment, are as follows:

- Selection of one existing set of methodology and criteria for the specific change: All ANSPs that plan to implement the change use the same methodology and criteria. The selected set of methodology and criteria is one of the existing 6 sets of methodologies and criteria of the affected ANSPs.
- Selection of a mix of joint and individual existing methodology and criteria for the specific change: ANSPs to a large extent use their own methodology and criteria. A joint approach is only used for selected activities in the specific safety assessment, such as a joint hazard identification session.

11. Concluding remarks

A systematic analysis of the safety assessment methodologies and criteria of six of the ANSPs involved in FAB EC has resulted in an overview of the main commonalities and differences. Identified commonalities that are of importance for the development of a common approach for the FAB EC partners include:

- The safety assessment methodologies and criteria have all reached a certain level of maturity, with safety assessment used for design and/or decision-making, but also with continuous innovation still deemed necessary.
- Similar process steps and a similar phasing are adopted by the six methodologies. Several important differences were identified, which indicate that there is a lot room for learning from alternate approaches and for learning which approaches are most suitable for a specific safety assessment. These differences include:
  - The scope of an assessment is defined as a subset of the ANSP’s functional system, or as a subset of the air traffic operation including other actors involved in maintaining separation.
  - Safety criteria show many differences in statement and in development.
  - A rich variety of safety assessment techniques and tools is used.

Based on the analysis, recommendations have been provided for a number of key activities for the development of methodology and criteria for use in common parts of a
FAB EC safety case. These further activities cannot be seen independently from the development of the operational concept, and from choices made or to be made with respect to Safety Management. As significant time and effort is expected to be needed for such development, two pragmatic alternative approaches have been proposed in [FAB EC SRAM] that can directly be used. The application of these two approaches will allow the ANSPs to further learn from each others’ methods, and may contribute to the eventual development of a common methodology and criteria.

Acknowledgements
The author would like to thank Belgocontrol, DFS, DSNA, LVNL, MUAC, and skyguide for their key inputs in this study and for their permission to publish the results in this paper.

12. References


