

## Validation Guidelines

### Structure of these guidelines

This document consists of **two parts** (level 1 and level 2) :

- the first part (level 1) is the 'guidelines'. It is composed of **few pages** addressing relevant questions about validation;
- the second part (level 2) is support material for the 'guidelines', hyperlinks are inserted in the first part leading to more detail in the second part.

### Objective of these guidelines

The purpose of this Validation Guidelines Document is to explain why validation is necessary as a support to the process of deciding which directions to take towards the next generation ATM Systems. A side-objective is to support the creation of a common Eurocontrol culture and awareness about what needs to be done to "validate" ATM Concepts.

This document is principally aimed at EATMP programme and project managers who are tasked to develop Concepts to a level where they can be tested and evaluated.

These programmes/projects are expected to provide evidence on the performance of O.I's. based on the ATM 2000+ strategy objectives: **Safety, Economics, Capacity, Environment, National Security and Defence Requirements, Uniformity, Quality, Human Involvement and Commitment.**

➤ See ATM 2000+ an Overall strategy for Validation

The approach to Validation discussed in this document is intended to also support the Strategic Performance Framework (SPF) structure that identifies Operational Improvements (O.I's) as enabling changes to the services and functions within the Air Traffic Management System.

This is not a guide to creating a Validation Plan, such a template will be addressed as an update to the EATMP Project Management Handbook (expected 4 quarter 2002).

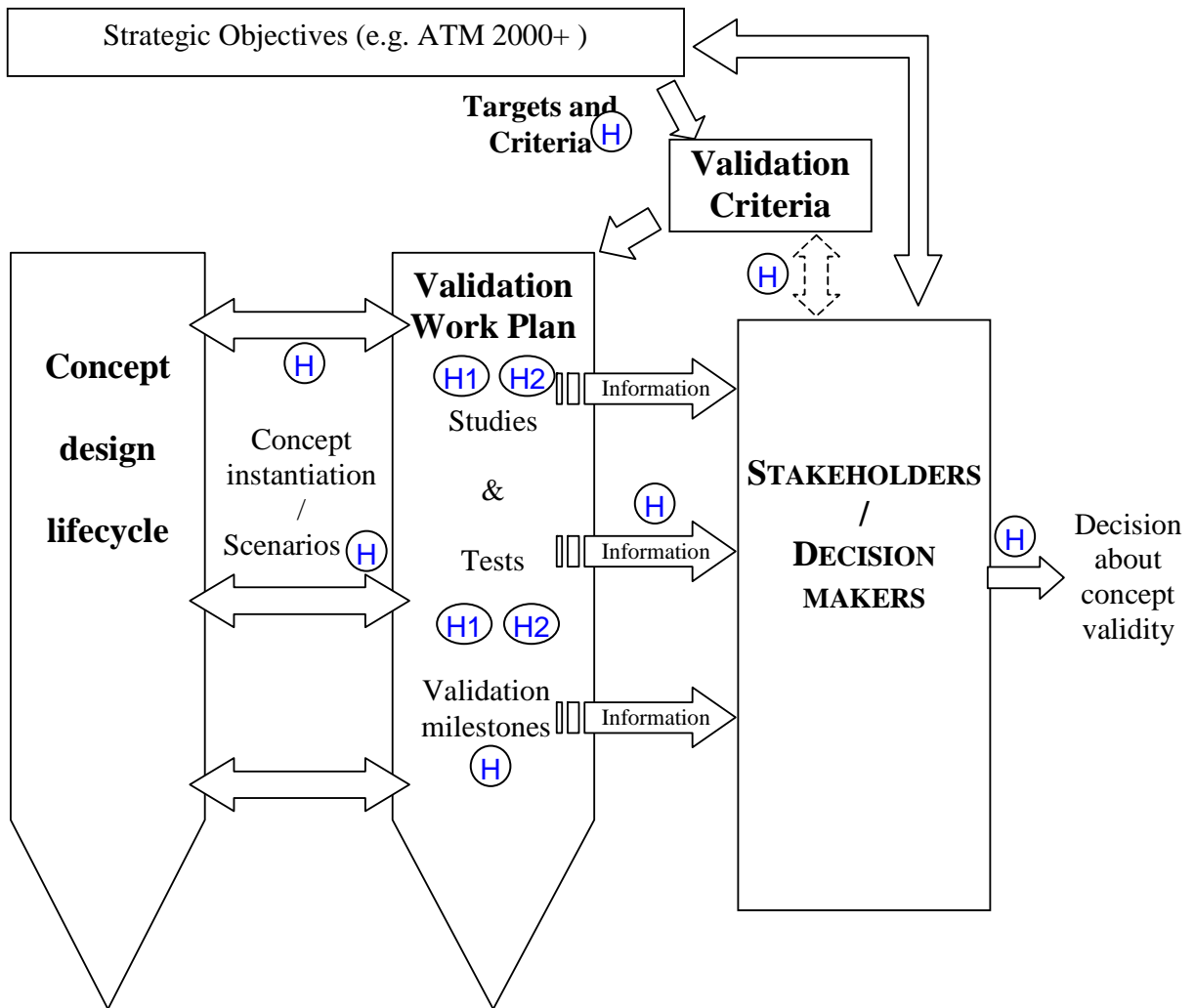
The 'guideline' addresses the following questions in Part 1 supported by additional detail in Part 2

- **Why** do I need to consider validation?
- **What** is validation?
- **When** (at what stages in my project) should a validation be planned and carried out?
- **How** should validation activities be integrated in my programme? (resources)
- **Who** should be involved in the validation, and what are the respective roles of the different participants?

There is an emphasis on safety concerns because the prime role of Air Traffic Control is as a Safety Service providing separation assurance. The position taken by these 'guidelines' is that it is impossible to refer to 'validation' of complex ATC or ATM systems without considering safety issues.

*The questions why, what, when, how and who and the supporting descriptions have been chosen as a result of a number of interviews made during the first phase of the VALSUP project (knowledge capture) in late 2001. Detailed results obtained from those interviews are presented in a separate 'interview synthesis' document. For more detail contact N. Makins – nigel.makins@eurocontrol.int.*

The following figure gives an overview of the main aspects presented in this document.



Overview of the validation context

H = hyperlink

## 1 Why validation?

Validation is the process of providing stakeholders with relevant information to help them make decisions about the suitability of continuing the development of a specific O.I.. It is the **stakeholders** who will **judge** if the concept is valid according to their own individual criteria.

To help identify potential criteria Stakeholders can be grouped as follows

- **Investors** – Airlines, Air Navigation Service Providers
- **Operators** – Controllers, pilots, dispatchers,
- **Airspace Users** – Airlines, Military, GA
- **Regulators** – ‘Safety’ guarantors
- **Technology providers** – ground systems, avionics, airframes.
- **R&D sponsors** – Eurocontrol, EC

The **acceptance criteria** of each stakeholder impacted by a programme/project should be identified before any experimental plans are devised.

### ***Why is validation necessary ?***

- Validation demonstrates the potential added value of the concept and ensures that the constraints it sets are acceptable. Validation consists of a) determining the expected added value and b) determining the resources requirements and constraints to implementation.
- Furthermore, when introducing a new concept it is necessary to check that it has no unforeseen negative side-effects on the ATM system.
- It will be stakeholders’ responsibility to decide the validity of a concept - based on potential gains set against their own criteria under the following categories Safety, Economics, Capacity, Environment, National Security and Defence Requirements, Uniformity, Quality, Human Involvement and Commitment

Safety is either directly or indirectly a major issue that determines whether the concept under development is acceptable. Safety, therefore, has an influence on all the other objectives at stake (capacity, economics, ...). Validation naturally encompasses Safety issues.

↘ [See The notion of Safety](#)

## 2 What is validation?

Validation consists in organising studies, tests and experiments to provide evidence about the expected performance capabilities of an O.I. along with identifying issues that need to be addressed before ‘implementation’ can be expected.

The process should be organised such that an O.I. can be shown to

- meet minimum performance targets,
- Supports the continued management of the ATM system in a way that is acceptable to stakeholder criteria.

Validation should take a System-wide approach to show that the candidate O.I provides an appropriate use of resources and funding.

Issues to be addressed include,

- Alternative solutions
- Resource requirements
- Institutional changes
- Training
- Technology performance
- Technology availability

Validation is not only the production of a final report, it is **a transparent process whereby all scenarios and assumptions are made available.**

➤ [See The outcome of the validation process](#)

➤ [See Validation objectives and other related objectives](#)

➤ [See Vocabulary: "validation objective"](#)

Regarding safety, Validation activities assess to what extent the safety requirements expressed or implied by the stakeholders are met by the new concept (i.e. by an ATM environment including the new concept).

➤ [See Conditions for Validation](#)

### 3 When is validation to be undertaken?

- Validation shall be considered as a continuous process throughout the concept design lifecycle.

#### *Link between the validation process and the design process*

- Validation is closely linked to the design of the concept and should be in line with the design phase of the concept development lifecycle.
- In the concept development lifecycle, the validation process is parallel to the design process. Both processes start from the stakeholder objectives and the derived requirements.
- However some validation milestones (e.g. according to the concept maturity) have to be established, in order to support decisions about whether to continue in a particular direction or to stop (i.e. **go/no-go decision** points).
- During the validation process, different issues can be investigated at different times, using different tools and techniques.

➤ [See Validation as a process](#)

➤ [See Categorisation of projects according to concept maturity](#)

## 4 How to perform validation?

- Validation is not only demonstrating that minimum performance targets can be achieved: it also **identifies which behavioural aspects, associated with the concept implementation, need to be analysed.** 'Behaviours' means those key situations that the proposed new ATM System will need to support or manage.
- Stakeholders are many and have different criteria to judge 'acceptability'. These **stakeholders and individual criteria should be determined at the outset of the programme.**
- **Key scenarios** are essential to demonstrate performance and behavioural characteristics of a new concept.

### ***How to identify the validation objectives and criteria?***

- Validation is about demonstrating that the concept, (as represented by a certain instantiation of the concept), is acceptable, according to the criteria of the stakeholders. As a consequence, stakeholder involvement is necessary from the beginning to clarify their specific requirements (i.e. added value and constraints, to be used as **validation objectives**) and their criteria for accepting or rejecting the concept (to be used as **validation criteria**).
- The added value and the constraints may be expressed in relation to the eight objectives of the ATM2000+ overall strategy mentioned previously. In particular, the added value can be also expressed in terms of "social/perception" feeling which is related to the objective "Human Involvement and Commitment » of the ATM 2000+ overall strategy. **Expected added value and constraints are the basis for defining validation objectives.**
- To define the stakeholder requirements, it may be necessary to collect the different view points on their needs and to make explicit the acceptance and rejection criteria (to be used as validation criteria).
- **The stakeholder criteria will drive the programme and project designs.**

↘ [See Vocabulary Validation objectives and Validation criteria](#)

↘ [See How to identify the validation objectives and criteria?](#)

Briefly put, **validating Safety** is a matter of determining to which extent the safety objectives are met by the concept, or more precisely by the ATM environment including an implementation of the new concept, and are actually acceptable. In other words, it starts with an Analysis and Assessment of the Safety of the ATM environment including the new concept, and consists in checking whether the results are acceptable or not to the stakeholders.

↘ [See Can safety be validated?](#)

### ***What is the significance of measurable?***

- There is a natural scientific desire to measure performance and behaviour. The assumption being that if it is not measurable it cannot be improved. However there are issues that are important when considering how an O.I. impacts the way ATM behaves that may not be easy to express numerically or measurable in any other way. Thus Validation should identify those issues that are key to stakeholder acceptability and determine either suitable measures or suitable assessment processes to ensure that Stakeholders receive accurate information.

- The validation criteria and the associated methods to obtain appropriate measures may vary depending on concept maturity: e.g. for some criterion, only subjective or qualitative results will be collected at early stages of concept development, whereas at more advanced stages, quantitative results will be expected.

#### ***How to structure the validation plan?***

- As mentioned in “When is validation to be undertaken”, the validation process is closely linked to the design process. Therefore when defining the validation plan it may be useful to identify the main stages in the design process, and to associate validation steps to these stages with specific objectives for each of them.  
The validation process shall not be separated from the design process. The purpose is to integrate validation issues into the overall programme plan, according to a specific validation plan.
- Defining the outline validation plan shall be done at the beginning of the concept development programme. However, deciding on the detailed content shall not (and cannot) be done too early in the process. It is necessary to retain some flexibility.
- The validation plan shall take into account the stages in the concept maturity scale and the scope of the concept (i.e. its geographical coverage and the number of concerned stakeholders),
- The transparency of the validation plan is supported by various means including the use of structured data-bases such as the Validation Data Repository (VDR).

➤ [See Validation as a process](#)

➤ [See Categorisation of projects according to concept maturity](#)

#### ***How to choose the appropriate technique to deal with the validation objectives?***

The appropriate techniques that allow to determine to what extent the validation objectives are met by the system under development should be defined using a top-down approach but should also consider the environmental and external constraints (e.g. cost, availability of resources). The validation objectives can be broken down into validation requirements, from which lower level objectives and metrics and indicators can be further derived. From these pre-requisites, validation platform requirements are derived. These requirements and the external constraints constitute a good basis for choosing appropriate techniques. This approach is described in detail in the MAEVA Validation Guideline Handbook (VGH) (Step 1 and 2).

➤ [See MAEVA](#)

#### ***Validation techniques: what are the options?***

Several techniques can be used to conduct a validation; from literature studies to real life trials. To get a quick overview of their purpose and when they can be used during the validation process see Validation techniques.

➤ [See Validation techniques](#)

#### ***Why and how to build Scenarios?***

One of the critical issues in the validation process is the definition of operational scenarios. An operational scenario is a representation of an operational situation in which the ATM operational concept is subject to one or several validation exercises, to enable the characterisation and measurement of the operational concept performance (MAEVA).

Crucially, as every situation cannot be tested, these scenarios (also called test cases) shall be relevant for the concept and provide a representative sample of both **nominal** and **non-nominal** situations.

Scenarios depend heavily on the objectives of the validation. These can be targeted at safety or capacity issues. They shall be realistic and operationally relevant to gain acceptance by those participating into the validation exercise, on the one hand, and also by the clients of the validation results, on the other hand. However, the level of realism will depend on the validation objectives and the maturity of the concept.

Sufficient time and efforts should be allocated to the definition of scenarios. In particular, focus should be put on the definition of abnormal events, which are usually disregarded or forgotten. **Non-nominal situations are an essential aspect that should feature within the chosen scenario.**

↘ [See Scenario](#)

## 5 Who should be involved ?

### *Who should be involved in the overall validation process?*

- The **stakeholders involvement** is implicit and may be required along the process to provide support to the validation team.
- The validation team is in charge of providing evidence to support the stakeholders decision on the appropriateness of the concept.
- A person should be responsible for validation (as defined in MAEVA, see references). This person should also be involved in the development of the concept. **The validation manager (and its validation team) must be involved in the design process**, because s/he needs to understand the concept and the rationale for its development.
- As validation encompasses a large number of criteria (technical, operational, human factors, safety, economic), the validation team should be multi-disciplinary, and include proficiency in different domains. It should involve at least Operational, Human factors, Analysis, Safety and Technical experts. However a single individual may impersonate several domains in the validation team.

Concerning the safety aspects, safety is not a matter of concern only for experts or lawyers. Neither is it a matter of operational expertise only. Indeed, in order to be both useful and usable, safety considerations should be as comprehensive as possible, and at the same time strongly anchored in reality, i.e. in the real environment, objectives and constraints of air traffic control. Addressing safety issues is a matter of combining safety expertise and operational expertise

↘ [See more in Who to involve?](#)

↘ [See Organisational aspects](#)

## Detail Information: Level 2

### 6 ATM 2000+ an Overall strategy for Validation

« For all phases of flight, to enable the safe, economic, expeditious and orderly flow of traffic through the provision of ATM services which are adaptable and scalable to the requirements of all users and areas of European airspace. The services shall accommodate demand, be globally inter-operable, operate to uniform principles, be environmentally sustainable and satisfy national security requirements. »

The major Strategic Objectives are presented in the document ATM 2000+ Overall strategy. **Safety, Economics, Capacity, Environment, National Security and Defence Requirements, Uniformity, Quality, Human Involvement and Commitment.**

#### .6.1 Validation objectives and other related objectives

Confusion exists about validations objectives and other kinds of objectives commonly used. This section aims at listing and defining the various “objectives” met during the concept development and validation and at explaining how they are related.

**Operational Improvement:** The target ATM operational concept describes available options that are expected to satisfy the strategic. The ATM 2000+ strategy proposes a number of general directions for changes to achieve the target concept. The directions for changes comprises a series of complementary and stepped operational improvements (OI) in the core ATM processes.

**Concept objectives:** The concept aims at providing a solution to a specific problem for which an OI is associated. A concept is characterised by several options linked to the functions, the infrastructure, the roles and responsibilities of humans and systems.

The concept objectives are the formulation of the expectations related to the implementation of such concept, of the benefits the concept can bring to ATM and of its contribution to the OI to which it is related.

**Programme objectives:** The programme objectives encompass the design of the concept and the validation of the concept objectives. In particular, during the programme, it is necessary to check that all the concept objectives have been validated. Programme objectives may also include management and realisation objectives.

**Concept design objectives:** The objectives of the design are to define and to characterise clearly how the concept is implemented (e.g. the function, the infrastructures, the roles and the responsibilities associated to humans and systems).

**Validation objectives:** The validation objectives are the formulation of what is to be achieved in term of measurable factors (MAEVA definition but taking into account the meaning of “measurable” previously given in Section 4).

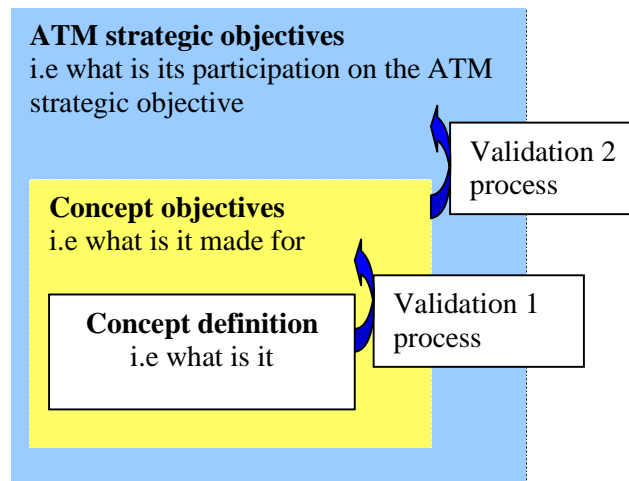
2 levels of validation processes can be distinguished for the concept (which is considered embedded in ATM context).

The concept must be validated in terms of:

- what is it developed for? (level 1): The validation objectives are to demonstrate that the concept succeeds in what it is planned for. E.g. demonstrate the usability of the concept. These objectives include the concept objectives.
  - What is its contribution to the fulfilment of ATM strategic objectives (level 2)? The validation objectives are to demonstrate the added value of the concept and the respect of the ATM constraints. E.g. demonstrate the increase in capacity resulting from the concept implementation.
- The traceability of contribution from level 1 to level 2 shall be provided using both top-down and bottom-up approaches.

- The two levels may seem artificial. According to the stakeholder needs, the distinction may be not necessary.
- The two levels of validation are not sequential and can be performed in parallel.

The following picture sketchily presents the two levels of validation which should be both addressed within the validation process.



**Simulation (experimentation) objectives:** During a real-time simulation, the concept is instantiated, fitted into a specific ATM environment, and is experimented. A real time simulation, which is one of the validation techniques, contributes to a partial validation. Simulation objectives encompass some of the validation objectives but not only. In the context of EEC, very often experimentation concerns both design and validation; at the beginning of a concept development lifecycle, the design is preponderant over validation in the simulation objectives and then, the trend is reversed. However, as already said, this document mainly focuses on validation and related objectives.

The simulation objectives that are relative to validation are part of the global validation objectives.

Note: At EEC, validation objectives and simulation objectives are often mixed up. This is due to the experience of EEC people and the methods they currently use for validation, which are mainly based on simulation techniques. This confusion underlines the gap existing between what the clients want to do and what EEC can provide.

**Example of the datalink concept:**

- *Examples of concept objectives:*
  - Reduce the risk of controller/aircrew misunderstanding
  - Reduce ATC voice communication workload
  - Reduce voice channel congestion,
- *Validation objectives: level 1:* Does it improves air-ground communication? Does the datalink have no negative impact (e.g. lack of partyline can be well accepted)? Is it usable and feasible?
- *Validation objectives: level 2:* E.g. Does it increase capacity, safety?
- *Programme objectives:* E.g. Have we treated each validation objectives?

- *Experimentation objectives:* Can the controller acquire confidence in the proposed data link system? Which HMI is the best (design objectives)? What is the controller behaviour in case of datalink malfunction?

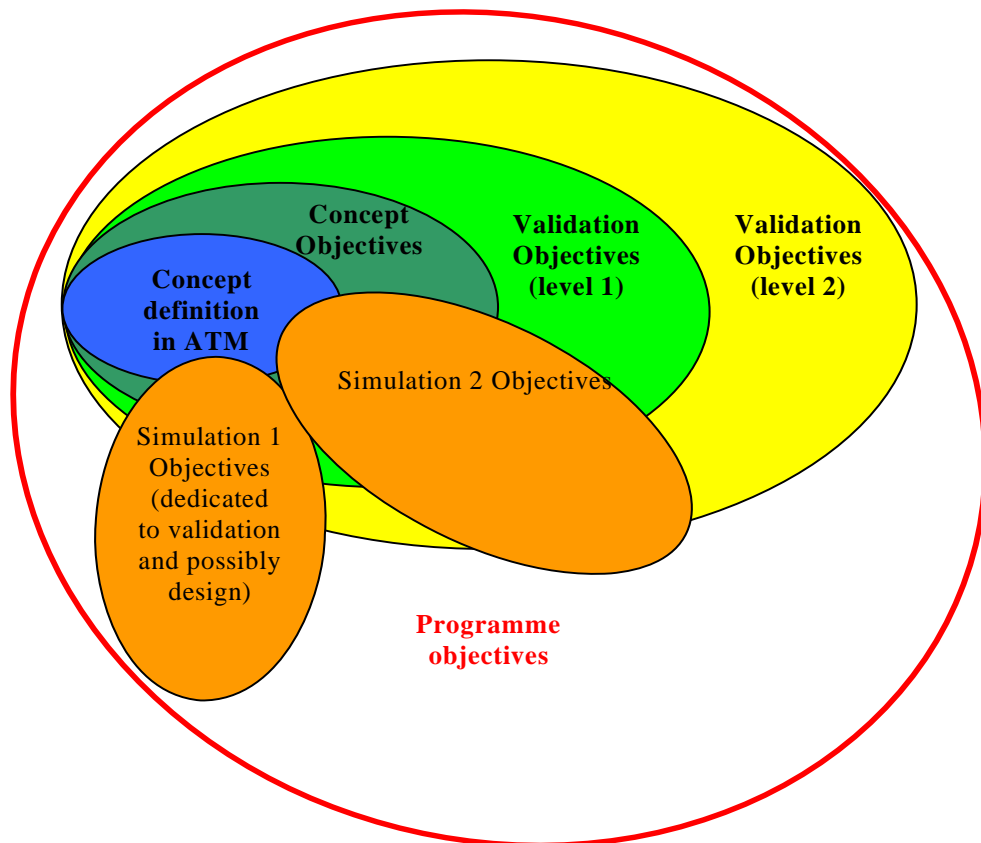


Figure 1: Relation between various objectives

**Legend:**

- The concept objectives rely on the concept definition. Validation objectives (level 1 and 2) rely on and encompass concept objectives.
- A simulation is applied to an instantiation of the concept in a specific ATM environment (and therefore addresses part of the concept definition). As a consequence, only some of the concept objectives will be investigated and only some of the validation objectives (level 1 and 2) will be treated during the simulation. Therefore simulation objectives related to validation include only part of the concept and validation (level 1 and 2) objectives.
- The programme objectives include not only the concept design and its validation, but also the execution of the simulations. Therefore the programme objectives include all the objectives mentioned above.

**.6.2 How to identify the validation objectives and criteria?**

- **The Stakeholders must be involved in the validation process.** Stakeholders are the actors in the ATM system whose support, co-operation and advice are important to ensure that the proposed operational concept can be brought into service.

Example of stakeholders:

- Actors of ATM system: Air Traffic services, Pilots, Airport operators, ATCOs, Regulators
- Other stakeholders: e.g. People living in the neighbourhood of an airport

- **Using a functional approach to identify the validation objectives:**

Conducting a functional analysis is a good approach for defining validation objectives.

A functional approach allows validation planners to formulate user needs in terms of **expected services** (instead of expected solutions).

The functional approach is focused at:

- the **expectations**, be they fully **rational** or wildly **subjective**, that the future users (providers and beneficiary of the expected services) have in respect of the concept ;
- the constraints resulting from different environmental situations where the concept is to be put at work ;

Indeed, a functional approach consolidates the different elements of the “true need” by defining and deriving various functions after the expected services. It helps also identifying acceptance and rejection criteria that represent the user judgement about the extent to which each function is provided. It also helps detecting the limits beyond which the expected service is considered as inadequately delivered (rejection criteria). A relative weight can be assigned to every criteria in order to assess the relevant trade-off between them (a multi-criteria sensitivity analysis may also be conducted by varying slightly these relative weights).

Validation criteria should be derived from stakeholders acceptance and rejection criteria.

**The first stages are the following:**

- Define the Scope of the system to be validated

This step is necessary to identify the functions and constraints (functional analysis). Choosing the right level of description of the system is very important as it supports the identification of those relevant stakeholders that must express their needs.

There is no general rule for deciding precisely what is to be considered as “within” or “outside” the boundaries of a system to be validated. Such notions as institutional and organisational boundaries may become more important in this respect than purely technical issues. Also, all boundary elements constituting the interface with adjacent systems should be represented at the right level of abstraction (a robust and stable service interface) to have the validation work focused at a reasonable perimeter of interest. (The reader should consider it perfectly normal to have to rework and refine that perimeter in the initial phase of the validation process).

To delineate the boundaries of the system, considering the direct users of a tool within the system allows to carry out a detailed analysis of the Human-Machine interaction, in other words, to study carefully the impact of the new tool on ATCO activity, which is important for treating the operational dimension of validation.

Various classical system representation can be used.

Example:

- Present the system to be developed as a black box,
- Identify all the external components (technical system, human actors, organisation(s) etc...) that have links with the system,
- Identify the links between the external components and the system in terms of services and constraints.

### - Establish the validation objectives

On the basis of the system description and its links with external components, the objectives associated to that instantiation of the concept (e.g. Level of performance, cost benefice, feasibility, etc) should be defined through the reformulation of user needs and constraints. A ranking of the objectives by relative priority should also be expressed.

The two levels of validation, presented previously, should be both addressed within the validation process.

**Warning:** it should be unrealistic to think that the needs and constraints must be identified exhaustively at the beginning of the programme. Refinement shall be necessary during the design process.

### **.6.3 The outcome of the validation process**

When a validation process has reached a successful outcome, the result is a validated system. It can be expressed as yielding “something recognised”, “an **adequate system**”, or even as the “right system” (validation is frequently denoted as “having the right system” while verification is merely about “having the system right”). Because the initial input to the validation process includes opinions and preferences of stakeholders (as user needs and perceived constraints) structured into user requirements and reflected into concept acceptance and rejection criteria, validation is not only a scientific process but also a social process (“**confidence building process**”) allowing to get a sufficient consensus on whether the objectives have been reached or not.

In such a complex socio-technical domain as ATM is, validating a new concept in a given environment shall be considered as the proof that the system built upon the concept is an adequate system.

Adequate; must be expressed in terms of operational criteria related to at least feasibility, performance, economy (i.e. the operational improvement established).

During the initial phase (identification of the stakeholders, capture of their needs and constraints, clarification of their criteria) any salient links existing between the criteria shall be clarified and if possible a model of the **trade-off** between them should be identified. It shall be used to prepare validation exercises and to analyse the data collected.

➤ [See also How to identify the validation objectives and criteria?](#)

### **.6.4 Validation as a process**

In [1] validation is defined as: « the process through which a desired level of confidence in the ability of a deliverable to operate in a real-life environment may be demonstrated against a pre-defined level of functionality, operability and performance. »

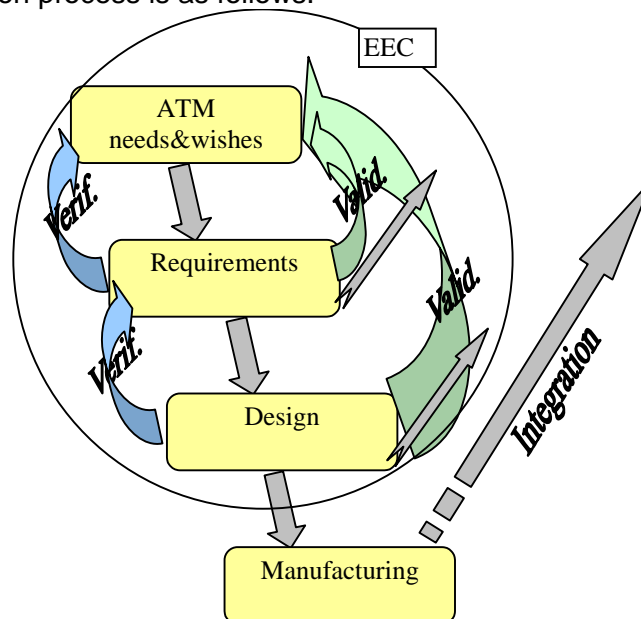
In relation with the global life cycle of a concept development, validation is linked to the design process. As such, validation concerns are closely linked with the design phase of the global life cycle and the degree of concept maturity.

➤ [See Categorisation of projects according to concept maturity.](#)

The validation plan aims at supporting the design of the detailed experimental plan that has to be done at each stage of validation.

In the ATM context, the validation process also aids detecting new needs, because, when designing such complex socio-technical systems, a top-down approach cannot yield from the outset an exhaustive list of requirements.

The general validation process is as follows:



According to a classical “V&V” description (Validation and Verification process in the life cycle), the figure above presents (with simplifications) the scope of the validation process performed at EEC within the overall validation process. The validation purposes can be summarised as follows:

- Prove that the requirements have been well defined to match the needs and wishes (in terms of verification and validation).
- Prove that the design has been well developed to match the system requirements (verification) and to match the operational needs and wishes (validation).

ATM needs and wishes correspond to the development of the concept in terms of: time horizon, airspace configuration, technology used, services, human roles and responsibilities in the system...

Requirements means written statements of what the system has to do but not how it is done. The requirements are written in terms of: technical functions, human tasks, tasks sharing between human, man-machine tasks sharing, safety, performance and interoperability statement.

Design means written statements of how the system is to be done (specifications) that is to say the technical functions specification, the HMI specification and the procedures.

## .6.5 Categorisation of projects according to concept maturity

- **Rough classification of projects in EEC:**

There are different types of projects led in EEC according to the client and -in relation- to the level of maturity of the concept.

Here is an overview of the categories of projects:

1. A given client has already performed the design process of the new system<sup>1</sup> most often in reply to some specific need and asks EEC to validate it (e.g. projects related to change in organisation such as re-sectorisation, new route network, or like RVSM in the last phases of concept definition, involving only some of the states). In such situations, the national organisation has performed the requirement analysis, and has designed at least roughly the solution he wants to implement. In that case, the client needs EEC because of its experience in organising real-time simulations and the availability of the required simulation equipment.
2. A given client “decides”<sup>2</sup> to modify its current system (e.g. change the CWP tools) and asks EEC to aid him with doing the design of the new system (e.g. DSI, ITI projects). There is a close link between the client and EEC. In that case, the role of EEC is to design the system (with the support of the client) and verify that what they have designed is conformed to the client’s objectives. There is no focus on technical validation related to the integration of the new system in the current system (this aspect is addressed separately at the stage when the system is transferred to the industry).
3. To meet the general economical needs (e.g. increase of capacity, safety ...) EEC participates to the development of new concepts that should meet the needs. Two types of concepts can be distinguished:
  - New concepts for a given actor (controller, pilot) that may have but a limited impact on the others actors (e.g. Free-route),
  - New concepts involving several actors (e.g. Data Link, ASAS concepts).

In those latter projects, EEC’s role is to design and “prove” that a given concept should meet the need (Very often in these projects, EEC participates as one partner among others - but with a specific role - as these projects are mainly EC projects involving several partners). The objective of concept “validation” is set on the foreground because the development of further projects related to a given concept can be carried on only if there is a good reason to think that it brings benefits in terms of capacity, safety and/or efficiency. In that context, the high level objectives are expressed in terms of capacity, safety, and efficiency. Other objectives such as feasibility, transition strategy (e.g.. how to address the user impact and the transition phase towards the new system) are frequently downplayed because they become important only at a later stage, when more concrete steps towards an operational deployment strategy have to be taken.

This document addresses mainly the third category of projects, i.e. those with the least degree of maturity in relation to the operational deployment horizon.

- **Proposition of projects categorisation after concept maturity**

This proposition is based on the document produced in the framework of FAA/Eurocontrol Action 5 plan [2] and the TRL proposed by FAA (Technology Readiness Level Transition Requirement) [3].

The development process can be broken down into three clearly identified stages as proposed in AP5.

- Stage 1: Development of the operational concept specifications;
- Stage 2: System procurement phase;
- Stage 3: Pre-operational (including training) and operational phases.

---

<sup>1</sup> In this context, system is heard as a change in the operational situation, that have consequence at least on the controllers. It can be a new tool, new procedure, change in airspace, etc...

<sup>2</sup> What are the reasons for this decision: the system is old and must be upgraded, the technology is mature, etc...

During these stages, the parties responsible for leading and conducting the validation have been defined.

According to the kind of concept and its scope (e.g. pan-European), EUROCONTROL can have a role in any of the three steps identified (e.g. in the RVSM programme, EUROCONTROL is tasked with a continued monitoring role after the implementation phase). However, the role of EUROCONTROL, and EEC, in validation is not so clear and should be clarified according to these steps.

As far as the development of a new concept/system is at an operational or functional level (stage 1), i.e. generic level without consideration of specificity of a ground infrastructure or architecture, EEC can/should be highly involved in validation that leads to the manufacturing phase.

After stage 1, EEC is no longer in charge of validation activities, but may remain in charge of monitoring and consolidating the validation activities conducted by others, especially for pan-European systems where interoperability shall be ensured. Moreover, feedback from the real world is also a necessary input for EEC further work.

**Final purpose of stage 1:** A clear and unambiguous description of the new ATM concept defined at a generic level, but applicable to any European countries (after adaptation and customisation to the specificity of each country).

Concept description in term of:

- Environment (e.g. airspace, traffic, equipment)
- Actors
- Actors' tasks and responsibilities
- Enablers (technology, system) to support the actors
- Events and the drivers of events
- Processes that take place and their relation
- Information flows
- Procedures (in nominal and non-nominal cases, i.e. emergency/contingency procedures)

Plus:

- Gap from current situation towards final concept
- Transition issues
- Training

Considering:

- Safety issues and performance, interoperability requirements
- Benefit analysis
- HF issues

Within this Stage 1, three sub-stages in the development phase have been identified as three relevant steps to which similar objectives are associated allowing us to categorise projects performed at EEC.

Taking into account the internal structure of the overall ATM system, validation may be focused at some elements of the ATM system rather than at the overall system. To do that, the first step is to identify which components of the ATM system are affected by the concept. That may lead to several validation processes executed in parallel.

| Phase            | Concept development<br>Concept Sketch/Outline/Design   | Feasibility phase<br>Initial System design  | Acceptability phase<br>Full operational specification  |
|------------------|--|---|--|
| Purposes         | Provide:<br>- Operating Environment description: ATM segment(s) concerned (scope), geographical application of the concept<br>- Functional requirements (services provided by segments)<br>- Actors: Roles and responsibilities (man/machine)<br><br>- Gap with current situation<br>- Operational scenarios | Provide :<br>- ATM System description<br>- Functional specifications,<br>- Technical issues<br>- Actors: tasks allocated to man /machine ; procedures ; general working method. | Provide:<br>- Detailed working method, procedures<br>- Human machine inter-action<br>- Technical System and HMI specifications<br>- System Performance required<br><br>Address:<br>- Training programmes<br>- Transition issues<br>- Selection of technical options? |
| Validation phase | <b>V1: Basic principles of a new concept are agreed.</b>   | <b>V2: Initial proof of concept (e.g. through model or early prototype)</b>   | <b>V3: Full specifications of concept, (e.g. pre-operational demonstration)</b>  |

To support the programme and its project managers it is important to clarify at each phase what validation is and is not, what the validation objectives are, what appropriate techniques should be selected, who must be involved in validation exercises etc...

## .6.6 Validation techniques

*The following information is extracted from MAEVA part III appendix 3 step 1. Additional information for each type of techniques can be found in MAEVA subparts: "Key characteristics", "ATM2000+ strategic objective(s)", "Maturity of the operational concept", "Scope".*

Among the possible usable techniques, simulation techniques are very used at EEC. However, it is important to stress that simulation techniques, in particular at EEC, can be used for both the design and the validation of a new concept. For example, fast-time or real-time simulations can be good techniques to explore the concept in its early phases of the development ([↘ see in the table: Stage 1/phase 1 in Categorisation of projects according to concept maturity](#)). In that case, these techniques are design support-tools. Such use of these techniques is outside the scope of this validation guideline, and will not be considered further.

- **Literature study**

### Definition

A literature study is the identification of suitable reference material, from which relevant parts can be used to support the validation.

### When can it be done?

It is recommended that literature studies be used at the start of the development cycle of an ATM operational concept.

- **Judgmental Technique**

### Definition

Opinions on an operational concept are collected from a panel of carefully selected individuals with (specific) knowledge on the concept. These opinions may be revised according to the analysis of the results, depending on the type of judgmental technique used (see variants). The aggregated/consolidated opinions provide evidence in support of the assumptions made in the validation exercise.

### When is it applicable ?

As this technique is based on subjective opinion, albeit with a "flavour" of professional objectivity, its results should be granted a relatively low level of confidence. It is therefore recommended that such expert opinion techniques be used at the beginning of the development cycle of an ATM operational concept.

### Variants

The different variants to the technique are the following ones (see MAEVA for more details):

- Structured brainstorm method;
- Unstructured brainstorm method;
- Open space method;
- Delphi method;
- Analytical Hierarchy Process (AHP);
- Quality Audit;

- **Analytical paper techniques**

Definition:

Model based techniques allowing predicting and analysing the impact of a given new concept on: technical, human factor, operational point of view.

When is it applicable?

These techniques allow at the early stage of the design process:

- to help and trace the choice made between options (e.g. using knowledge about the operational people cognitive process such as ITA for ATCOs, and ACOMOD and MACE from IMPACT project).
- to investigate the impact of the new concept onto the ATCOs tasks in terms of new procedures, new responsibilities, new team work, new required skills, new potential forms of errors. See IMPACT MATOS (software).

At a latter stage of the design process, these techniques help at analysing and formalising results obtained from other techniques application such as real time simulation. Then they act as model based analysis.

- **Fast-time Technique**

Definition

For a fast-time technique (also known as 'compressed time technique') the behaviour of the real world element that is being validated is expressed in some mathematical model that defines the relationships between the input and output variables. For testing the hypotheses related to the higher and lower level objectives the performance of the real world element is assessed mathematically for some characteristic quality (e.g. accuracy). Operational subject matter experts are not required to perform this assessment.

An experimental design often used in combination with fast-time techniques (and normally only possible with fast-time techniques) is a Monte Carlo simulation, in which a large series of fast-time assessments is performed with random input.

When is it applicable?

Fast-time techniques may be used throughout the development life cycle, but are especially suitable for a preliminary assessment of a great number of options within a new ATM operational concept.

Since fast-time techniques can never completely represent the actions of a human operator their application lies mainly in the earlier stages of the validation life cycle.

Variants

The different variants to the technique are the following ones (see MAEVA for more details):

- Analytical Modelling Technique
- Fast-time Simulation

Additional information about 'Fast-time Simulation'

Fast-time simulation is an expression that is mostly used in relation to the analysis of (air) traffic movements based on an analytical model that represents the stepwise displacement of traffic over time. The models usually incorporate rule-based decisions that control the interactions between various actors being simulated and also with the events that take place. In general a fast-time simulation uses a model that can be adapted to the specific scenario that is being tested by changing the input parameters. The model itself does not need to be changed. With a fast-time simulation model, randomisation can usually be introduced either through the input data or through certain model settings. The randomisation is linked to the application of Monte Carlo simulations.

- **Real-time Technique**

### Definition

Real-time techniques are characterised by the participation of one or more subject matter experts (controllers, pilots, ...) that perform their operational tasks in a realistic real-time environment. Assessing the controller's and pilot's response and decision taking is an essential element of this technique.

The environment in which this technique is applied can range from a fully simulated system to an operational system in control of commercial or operational air traffic.

### When is it applicable?

The operational concept has to be described to the level of detail of tasks and responsibilities of the participants and procedures for interacting with the supporting systems need to be described too. This detailed definition of the operational concept will normally only be achieved in later stages of the validation life cycle.

Real time simulation can be used earlier in the design process but for design purpose (exploration of the concept) and not for validation purpose.

### Variants

The different variants to the technique are the following ones (see MAEVA for more details):

- Animation
- "Wizard-of-Oz" Simulation
- Real-time Simulation
- Field Test
- Shadow Mode Validation
- Operational Trial

### Additional information about 'Real-time Simulation'

In a real-time simulation, the technique is applied in an environment in which the main elements are simulated, especially air traffic. This makes the real-time simulation technique well suited to the validation, with a focus on human performance, of operational changes for which operational safety assessment has not yet been reached a high enough level of confidence, or for which there exists no model / empirical data on the way the human interacts with the system.

Air traffic can be simulated at different levels of detail, depending on the degree of realism which is required. A traffic generator can simulate part of the traffic fully automatically. Pseudo pilots making inputs to a traffic generator normally control most of the traffic. It may be implemented in a distributed mode, when the pseudo-pilots operate from different locations and are connected to the central simulator over a network (e.g. the Internet). For small numbers of individual flights cockpit simulators (static or moving base) can also be used.

Finally, it is possible to have a few real flights (generally, using specially equipped research aircraft) participating into the simulations. Although there is no peculiar name for that last option, this type of configuration certainly requires special attention for the integration of the aircraft in the experiment and co-ordination with the real world of ATC operations.

## **.6.7 Scenarios**

A scenario shall be characterised by:

- its location (geographic area)
- its timeframe (e.g. now or future)
- a sequence of events (occurring in nominal situation, or non nominal situations)

- an ATM environment: ATM procedures, airspace design, airspace type, traffic characteristics (e.g. flight plans, density), operational context (e.g. en-route, TMA), enablers (e.g. assumptions on equipment), key participants, working arrangements.

A generic method to define scenarios has been proposed (MAEVA Step 2.3). It is based on the following steps:

- Develop performance targets (criteria),
- Identify the time frame of interest,
- Identify the geographical area of interest,
- Select an appropriate baseline traffic sample,
- Identify the traffic growth coefficient to be applied,
- Develop traffic samples for the time frame and geographic area,
- Define the airspace,
- Define the events.

## 7 Safety issues

### **Why should Safety<sup>3</sup> be part of Validation?**

Among the stakeholders, some are primarily interested in Safety of the ATM<sup>4</sup>. This is the case of the regulator for example. But Safety is not only the concern of the regulator. The ATCOs themselves, the airlines, etc., are also concerned about Safety, although Safety for them may be one criterion among others. In fact, every stakeholder has, in one way or another, an interest in Safety. Indeed, Safety is related to the other criteria, at two different levels: first, by setting constraints within the very definition of the concept (a typical example is the self-limitation imposed on capacity gains because of safety concerns), and second, because an unsafe situation resulting in an accident would adversely impact the other criteria; for example, should an accident occur, then both capacity and economy would be affected.

#### **.7.1 Safety: the frame**

Validation focuses on ATM operational improvement achieved through a new concept. Somehow abusively, we talk about validation of a new concept. Abusively because, depending on the environment it is embedded in, a concept may add value or not. The same consideration applies to Safety. Therefore, "Safety of a new concept" is used as shorthand for "safety of ATM after inclusion of the new concept". Indeed, The safety of a concept considered in isolation, without any description of the operational environment it will be embedded in or of the operational procedures that will be developed, is meaningless.

↘ See The notion of Safety "Safety: an output of a system, not of a component" for further development.

#### **.7.2 The notion of Safety**

- **Definition**

**Safety** is commonly viewed as the absence of accidents. In that respect, it may be considered as a positive characteristic of a given situation. But it can also be considered as the result of a certain voluntary process, which is the process preventing any accident from occurring, and, by extension, denote that process itself. Both characterisations are correct and can even be merged. In other words, as Karl Weick coined it: "Safety is a dynamic non event".

- **Safety, Risk, Hazard, Accident: what is it all about?**

Several notions are commonly called for in hazardous industries e.g. ATM, such as Safety, Risk, Hazard, Accident. They all refer to different yet interdependent aspects that need to be clarified. In the context of safety issues, an **Accident** is a highly undesirable event which is terminal in some sense from the standpoint of the safety analysis (and it may be the consequence of a more or less complex sequence of other unwanted events). Depending on the domain of interest, an accident could be either a hull loss, a separation infringement, the

---

<sup>3</sup> Indeed, some of the stakeholders may voices their acceptability criterion related to accidents in terms of Risk rather than Safety. If in the end, Risk prevails over Safety, then what is meant by Safety within validation should rather be worded as Risk within validation. But in order to make it simple, the document will stick with the word Safety.

<sup>4</sup> Safety of the concept is not used as an expression on purpose. Indeed, a concept considered in isolation, without any idea of the operational environment it will be embedded in or of the operational procedures that will be developed is meaningless.

loss of a certain amount of money, or whatever is deemed unacceptable. Events, however tragic they may be, are not intrinsically accidents. The definition of accidents for a person or an organisation results from the characterisation of the events that are not acceptable from this person's or organisation's point of view. For example, not having enough snacks onboard a domestic flight is not considered an accident from the airline viewpoint (although it is an unpleasant event) though it may be considered as a very serious problem from the standpoint of the catering company, and thence categorised as an accident, the occurrence of which should be strictly minimised. The notion of **risk** combines the severity of the consequences of an unwanted event or accident with the probability of occurrence of that event or accident. Since it includes a probabilistic aspect, risk is not really an intuitive notion easy to manipulate. A **Hazard** is "something" (a failure, an element of context, ...) that might lead to an accident if not properly handled. For example, a pedestrian walking on a highway is a hazard, as well as the failure of the breaks is a hazard.

These notions are obviously not independent from each other. Since the perspective here is that of safety validation, the requirements are mostly defined in terms of safety. However, verifying that these requirements are met may require referring to some other notions presented in the previous paragraph.

- **Safety: an output of a system, not of a component**

Looking at safety as a process, understanding it is crucial for identifying who is in charge and what contributes to ensuring safety. It is commonly believed that the technical system is intrinsically safe, and that the main source of risk is the Human "component". However, if we take a closer look at the ATM system, it combines equipment, ATCOs, managers, procedures, organisational features that all function in an integrated way. Should a surveillance failure occur (i.e. a technical failure), the ATCOs will change their strategy and adapt themselves to the new situation in order to safely cope with it. The permanent interactions among all the components of the system makes it impossible to distinguish between them for singling out direct individual contributions to safety. Moreover, they all aim at ensuring a safe and efficient ATC service. In other words, they together constitute a system that cannot be broken down into independent elements, because the multiple interactions between the various parts that are a core feature of its functioning, would no longer be correctly captured and understood. Therefore, the Human Factor aspects that contribute to maintaining Safety are party to the very concept of Safety. In the same way, the safety of a sub-system or tool under development has no meaning in isolation. A new tool or sub-system plays a role in the safety of the overall system, but it cannot be considered in isolation to address safety issues. Considering a tool in isolation can make it possible to assess its coherence, reliability, responsiveness etc., but as far as the overall safety of ATC is concerned, the tool is to be considered as embedded into an operational environment. A wonderful tool allowing in principle to support ATCOs anticipating potential conflicts may have no impact on the safety of ATC if it is not actually used by ATCOs. It may even undermine safety if using it creates a risk of misusing or neglecting other essential tools. Therefore, the safety of a tool or sub-system or in our case the safety of a concept is a misnomer. It should be understood as the role (which may be positive, negative or both) of the concept in the safety of the overall ATC system.

In the rest of the section, Safety will always be referred to in this way, including the Human Factor aspects, and always considering that a new concept is embedded in an operational environment. Indeed, safety is always the output of the whole man-machine system. It is never the output of an isolated concept, or of an individual.

### **.7.3 How can Safety be integrated into Validation**

Even though the stakeholders may express their views in different ways when they talk about Safety, it is important to bear in mind that to all of them, in the end, the expected outcome is the same, that is a stable (and if possible decreasing) total number of ATM-induced accidents. The different kinds of proof (that the ATM system including the new concept is safe enough), and the variety of demonstration strategies, are due to cultural differences rather than to actual differences between the value of the various proofs. Frequently, a disagreements about how to carry out a demonstration on Safety performance stems from a divergence regarding the set of situations (and related scenarios or test cases) that has to be investigated before the demonstration is deemed valid.

Eventually, a consensus should be reached as to what is considered a Safety Requirement at the level of the ATM system, as well as for what test cases will effectively allow a valid demonstration to be carried out.

#### **.7.4 Conditions for Validation.**

Building the right system can be seen as building a system that meets the right functional safety requirements. Then, validation is a matter of checking that safety requirements are effectively guaranteeing a safe performance of the overall system, and that the system built meets those requirements. If safety is seen as a dynamic non-event, it cannot be validated as such. Therefore, a translation is needed to express Safety in terms of functional and non-functional requirements (e.g. the anti-collision should work with this level of performance, ...). In other words, safety validation consists in taking a number of measures to tackle undesirable events in the system, AND checking that these measures actually guarantee that safety is maintained. Eventually, safety can only be validated if it is addressed as a process rather than an outcome or end result<sup>5</sup>.

➤ [See RTCA SC-189/EUROCAE WG-53 methodology](#)

➤ [See Methodological documentation](#)

#### **.7.5 Certification and Validation of Safety aspects**

Building the right system and building a safe system are two different issues. Therefore, the requirements in terms of Safety can be different in both perspectives. Certification exclusively aims at verifying, in a socially formalised way, that certain rules for design, implementation and operation are respected throughout the development process. In Europe, this is achieved through checking the compliance of the designed system with pre-defined technical requirements and procedures. In this respect, certification is akin to the validation of safety aspects as we defined it with a focus at the process that maintain safety rather than on the output in terms of safety. The certification process mainly relies on safety analyses using standard dependability or RAMS<sup>6</sup> methods as suggested hereafter. However, so far, Human Factors aspects have been poorly addressed in certification. It is acknowledged as one of the main weaknesses of certification and developments are underway to make up for this gap.

#### **.7.6 Who to involve?**

---

<sup>5</sup> In that respect, Validation of Safety aspects should show a resemblance to Quality processes.

<sup>6</sup> RAMS stands for Reliability Availability, Maintainability, Safety. It refers to the discipline studying these performance criteria

To be pragmatic, safety analyses should involve people with a strong knowledge of the ATC operational environment. Indeed, since safety is an outcome of the whole ATM system rather than that of a concept considered in isolation, safety analysis should integrate knowledge on the way a new concept would fit into the activities of ATCOs (and pilots if needed), hence benefiting from knowledge on real operation.

At the same time, safety analyses, in order to be as rigorous and exhaustive as possible, should not be limited to the inventory and characterisation of well-known hazards. They should also try and detect hazards that have never been encountered or thought of in the past, and this requires expertise in and experience with safety. Indeed, Safety Analysis methods make it possible to enlarge the "search space" to an extremely wide set of situations. In addition, probabilistic methods also allow for prioritisation of the various risks.

Eventually, safety issues are to be addressed by using safety expertise and operational expertise in combination. Such combination would have to be applied to the "paper" analyses as well as to the simulation exercises, the two kinds of approaches being complementary and cross-fertilising each other. For example, a realistic "paper" analysis can pinpoint some failure scenarios that can be better understood, refined, adjusted or completed through simulation exercises of such a situation. Conversely, a simulation exercise yields new insights on how things are "really" dealt with in abnormal situations, and it can make it possible to think out new failure scenarios that were missed by a top-down approach, or to revise, after observing the reactions of the ATCOs involved in the simulation, the relative importance of some other failure scenarios.

#### **.7.7 Organisational aspects**

The collaboration between safety experts and operational experts doesn't seem easy to achieve. The situation looks like a conflict between the "paper" world, that of the safety experts, and the real world, that of the ATCOs. Such a conflict acts as a brake upon an efficient and useful approach to safety. A way forward would be a cultural change in both worlds.

Up to now, ATCOs involved in simulations are not always called upon to carry out safety analysis or to intervene at other stages of the design process for other purposes than "playing" with the new concepts/tools. Often, they are not really engaged in the development process and don't necessarily feel personally involved in the new concept or tool under development (except in some programmes where ATCOs share their time between their operational job and the participation in a concept development in EEC). Therefore, they are not always involved in the whole design process or in the safety analysis process. The ATCOs following the whole design process are EEC people who were former ATCOs. The main limitation it brings is then that their knowledge of ATC may become outdated. As for safety experts, they may not feel either totally responsible for operational safety since their contact with the real world is rather weak. Bringing together operational experts and safety experts and making them work as an integrated team deeply involved in the safety of the concept or tool under development would be a great step forward.

**Approaches to address Safety issues as part of Validation**

**.7.8 Can safety be validated?**

The major part of validation of Safety aspects for a new concept i.e. for the systems implementing the concept, is the analysis of Safety of the ATM environment including these systems.

- Several approaches have been developed to carry out a Safety Analysis of systems under development. Eurocontrol has defined some requirements for Risk Assessment in ATM that could as well apply to Safety Assessment, in a document from the ESARR series.

See EUROCONTROL Safety Regulatory Requirement - ESARR 4 - Risk Assessment and Mitigation in ATM

Also under development is a Safety Assessment Methodology (SAM) that would allow users to comply with these requirements.

↘ **See SAM - Safety Analysis Methodology**

- A handbook developed by the FAA provides a comprehensive description of a process to analyse and assess safety throughout the design process, including some details about the various methods applicable given the objectives at the various stages of design. Other possible resources to determine the safety validation activities to be integrated into a programme management plan are certification processes such as JAR 25 and 21 which were developed for certifying new A/C and changes to existing A/C

↘ **See Certification and Validation of Safety aspects**

↘ **See FAA - System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management**

- The **main objectives** of a Safety Analysis dedicated to validation could be roughly described as:
  - To define the boundaries of the system of interest,
  - To determine unacceptable or unwanted events.
  - To identify the various paths that may likely lead to these events; these paths can be described through a combination of technical failures, human-machine coupling failures, organisational features, ...<sup>7</sup> . ↘ **See The notion of Safety: an output of the system, not a component**
- To assess the probability of occurrence of failure scenarios derived from a probabilistic approach i.e. a risk analysis approach.

---

<sup>7</sup> Due to the very design of such systems, an unacceptable event almost never results from a single failure or error, and focusing on such single failures appears to be too simplistic an approach. Therefore, even though it is more complicated to describe and model, the emphasis should be put on realistic failure scenarios related to the ATC system in order to carry out a useful safety analysis

- To verify to which extent the results comply with the Safety requirements if the requirements are not met, and if the results still seem insufficient, to identify ways making progress, and to prioritise improvement actions.

- The methodologies used to address Safety Analysis throughout the design process articulate various methods, approaches or techniques dedicated to specific objectives, some of which may be used at various stages of design

↘ **See Safety Analysis methods: systemic and Human Factor aspects**

The available methods and approaches include **analytical techniques** – Functional Analysis, Failure Modes and Effects Analysis, Fault trees, Markov Graph, Petri Nets, ...-, as well as **simulation techniques** – real/fast time simulation, mental simulation, ...-, or even **real-life techniques** – shadow mode, tests, trials, operational feedback, ...

### **.7.9 Safety Analysis methods: systemic and Human Factor aspects**

A whole set of methods, from functional analysis, FMEA<sup>8</sup> to dynamic methods – Petri nets, Markov graphs, ..., through fault trees, or event trees, have been developed to address Reliability Availability Maintainability and Safety (RAMS° issues). All of them were initially focused on technical aspects. Then Human Factor aspects started to be included, operators being considered as technical components, hence being modelled through “human error” events. More recently, specific methods particularly Human Reliability Analysis methods were developed to better account for the actual participation of Humans in ensuring Safety. In addition, some of these global Safety Analysis methods are comprehensive and come out with proved results on Safety. Therefore, they can be used as part of validation.

### **.7.10 Safety Analysis during Design**

It is commonly believed that nothing wise can be said on the safety of a concept until it is mature enough to know a) how the system embodying it will look like and b) how it will be used. Some safety methods can be implemented at a functional level first, the analysis being refined as design progresses. Addressing safety issues at the very beginning of the design process is therefore not only recommended, but also feasible. One should however not aim at a detailed “material” or operation analysis at early stages of design, hence not expect very detailed results as to an operational procedure at these stages. Such results can be achieved later on in the design process (for example, when a prototype is available). However, the added value of early safety analyses shouldn't be underestimated: such analyses can prevent developing options that will turn out to be irrecoverably unsafe. As mentioned earlier, the methods to carry out Safety analyses, here predictive ones, combine equipment oriented methods as well as Human Factor methods.

### **.7.11 Safety cases: a restricted view?**

Safety Cases as they currently exist not only are focused on equipment only, but also seem to consist of a collection of statements on Safety that are not based on strong and explicit grounds. With such characteristics, they cannot be used as such as a basis for validation. However, Safety Analysis doesn't only boil down to such safety cases as mentioned in the previous paragraph.

---

<sup>8</sup> Failure Modes and Effects Analysis

## References

### Documents related to validation

Here are summaries of documents related to validation activity. The aim is to present an idea of the content but not to have an exhaustive view of their content. For detailed information, please report to the documentation.

#### 1. MAEVA

In the MAEVA Validation Guideline Handbook, it is said that “the objective of a validation process is to determine whether a specific ATM concept addresses the ATM problem of concern. This involves an ATM strategy taking account of the ATM concept to construct the validation exercises”.

They propose a mean to reach this objective presenting a 5 steps process for conducting an ATM validation exercise.

This Handbook contains 3 different parts:

Part 1 presents a high-level description of the 5 steps of the project providing the purpose, description, process diagram, inputs, outputs and responsibilities of each step.

Part 2 is a more detailed presentation of the different activities and sub-activities of each step.

Part 3 carries additional highly specific information related to methods and criteria applicable to the execution of the activities/subactivities described in parts I and II. The particular items described in part III cover validation techniques, experimental design, validation platforms, data collection methods data types and data analyses methods

Different actors are presented for these validation exercises. They are the program manager, the development teams, the validation manager, the validation team and in a different way the exercise participants, the validation analyser, the customer and the stakeholders.

Concerning specifically the validation techniques, 4 families are presented: literature studies, judgmental techniques, fast time techniques and real-time techniques (more detailed in the part III).

Here is a quick description of the objectives of each of the 5 steps of the validation exercise:

Step 1: the purpose of this step is to obtain an understanding of the ATM problem that needs to be solved and the operational concept developed, in order to address this problem (performance target).

Step 2: the purpose of this step is to take the requirements specification of the exercise, develop the specification of the exercise to be conducted and make all the necessary arrangements to prepare for the exercise runs.

Step 3: the purpose of this step is to take measurements specified for the exercise runs.

Step 4: the purpose of this step is to analyse measurements taken during the exercise runs to determine whether the hypotheses can be supported and whether robust conclusions can be proposed.

Step 5: the purpose of this step is to develop conclusions and recommendations based on the analysis conducted and disseminate them in a readily understandable manner to the stakeholders in order to help them judging whether the system can meet the performance targets.

References:

MAEVA: Validation guideline handbook; MVA/ISD/WP1/13DI\_10

MAEVA: D2.2-Validation methodology; MVA/ISD/WP2/22DN\_21

MAEVA: D2.3-Scenario Definition for validation exercises; MVA/ISD/WP2/23DA\_20

## **2. FAA/Eurocontrol: MoC on R&D: action plan 5. Operational Concept Validation Strategy Document. Vxx date yyy**

The Operational Concept Validation Strategy Document tries to share common definitions and to define best practices, analyses and acceptance methods.

Definitions of validation, verification and certification are given clarifying their interaction.

In the scope to develop a structured and logical framework to identify "*possible solutions to meet regional air transport needs until 2015*", a generic validation process has been described. This process is broken into 3 stages and 5 validation transitions have been defined during this 3-stages-process.

The three stages are the following ones:- In the first stage, the "operational concept specification" is developed. The relevant lead organisations here are EUROCONTROL, EC  
- The second stage is the "system procurement phase"; and the system suppliers will often conduct the validation exercises (factory acceptance tests)  
- The third stage represents the pre-operational (including training) and operational phases. The service providers and airspace users will lead and conduct the validation exercises on site.

The 5 validation transitions are the following ones:

- The basic principles of a new concept are observed, reported and agreed: V1.
- Initial proof of concept through model or early prototype: V2.
- Full specification of concept, pre-operational demonstration: V3.
- Production, integration and verification of components (factory acceptance): V4.
- Sign off for operation through on site formal validation: V5.

The 3 first validation transitions intervene in the first stage and the two other ones at the end of each other stage.

In the document, a stress is given on the need to have a "firm discipline", i.e. to have common plan and common practices between the different development authorities and between the different organisations that do validation activities.

The last part of the document is dedicated to describe the strategy implementation, i.e. "Validation exercises have to be conducted and presented to the relevant decision making bodies in a manner which satisfies the four validation principles, namely: application of discipline, good practices, selection of options and building of confidence". To ensure this, it is necessary that "co-operation between the region be established to co-ordinate operational concept validation". The strategy implementation implies the different points:

- A description of the 4 levels of validation methodologies is made (Paper studies and inspections; Simulations and analysis using modelling tools; Implementations with prototypes, in a simulated environment/exposed to the real world; Implementations with parts of the actual target system: in a simulated environment / exposed to the real world) and it is asked to have a consensus on appropriate use of methodologies
- Validation objectives comprehension is exposed as an essential information when mapping simulation measures onto project objectives

- VDR\* is exposed too as an important tool to capture, preserve and make available validation related data
- Validation environment is seen to address the development technology. This point is developed.
- The last point presented in this strategy implementation is the creation of confidence that requires a certain number of actions to conduct.

\*: VDR (Validation Data Repository) : "the centre for capturing, preserving and making available validation related data, including objectives, procedures, configurations, validation environments, exercise data, results and conclusions".

### 3. FAA 'Operational Concept Validation Process'

The FAA OCVP purpose is to describe the validation process (strategies and mechanisms that will be used to validate the ATS Concept of Operations) for the development of National Airspace System to achieve objectives in 2005.

In a first time, the FAA makes a link between AMS and OCVP – AMS following the entire life-cycle of a concept, the OCVP corresponds to its first step: 'mission analysis'. This corresponds to all the pre-industrialisation, or pre-implementation, phase: development of the operational concept specification.

The approach of the OCVP is described as a 3 phases process including "Problem Definition", "Analysis" and "Synthesis".

The "*problem definition*" phase ask to integrate various users and service providers inputs in order to develop detailed problem statements to address the strategic objectives: capacity, efficiency, flexibility, predictability, productivity, accessibility, safety, operator workload, situation awareness, and performance.

In this phase, a functional decomposition of the service provided is made first, and an allocation of the different functions is made to identify which function is currently implemented and which one will have to be implemented on a future NAS functionality.

Then a comparative analysis is made to see the gaps and overlaps between the current system functionality and the desired system functionality as expressed for future concept of operation.

The next step is benchmark that has to be done to compare the performance of the existing NAS and to find suitable metrics for the specific study objectives.

Then assumptions have to be maid and constraints have to be kept in mind.

To finish, a repository of NAS models and databases is available to support the validation process

The "*analysis*" phase involves the planning, design, research method selection, conduct and data collection and reduction activities. The methods used are paper studies, fast time simulation studies, modelling, real-time human-in-the-loop and rapid prototyping. Typically, the following steps are involved in conducting a validation study: Define study specific objectives, Form a team, Identify the type of study, Develop experiment plan, Develop detailed metrics, Develop scenarios and select equipment, Schedule laboratory and support personnel, Conduct shakedown testing, Conduct simulation and collect data, Analyse data and develop recommendations, Provide data/information to NAS model and database.

Synthesis phase is the interpretation of the results and those interpretations will be translated in a technical report to provide an assessment of the validity of the concepts to state if performance goals can be met, on what extent, the operational issues discovered during the analysis, the potential alternative concepts, set of validated operational requirements, recommendations for procedural changes necessary, support tools necessary, human

factors issues, changes in the NAS architecture, update of the existing models and databases

Roles and responsibilities are identified at the end of the document, this team is described as needing to contain: FAA and industry representatives, participants from Airways Facilities, air traffic airlines and labour organisations. The team is partitioned into a management team and a system analysis team.

#### 4. **IMPACT project: an Eurocontrol project including a method and 4 tools.**

3 of the 4 tools can be used for validation purpose.

**IMPACT** deals with methodological issues in managing the transition towards the future ATM systems from a Human Factors point of view.

Assuming that new concepts will have an impact on the controllers' job, the question **IMPACT** addresses is : How can we analyse, predict and manage this impact in order to design acceptable new systems and to prepare the necessary upgrade training for controllers ?

In answer to this question, **IMPACT** provides a methodological framework as well as analysis support tools dedicated to concept design, requirement formalisation, system & training design and evaluation. Through this material, **IMPACT** proposes a coherent process based on change analysis to deal with Human Factors integration in the design process for future ATM systems.

3 tools have been developed focusing on the analysis of **change** :

- **ACOMOD** : an integrated cognitive model of the controllers to analyse change;
- **MACE** : a decision support tool for clarifying new concepts and predicting their impact;
- **MATOS** : a support tool for task modelling.

#### 5. **RTCA SC-189/EUROCAE WG-53 methodology**

The RTCA SC-189/EUROCAE WG-53 methodology provides guidance material to establish the operational, safety, performance and interoperability requirements for ATS supported data communications, to assess their validity and to qualify the related CNS/ATM system.

The methodology covers the following processes:

- approval planning,
- coordinated requirements determination,
- development and qualification of a system element,
- entry into service
- operations.

The **approval planning** is the process of describing the system, establishing the approval basis, proposing the means of compliance, and identifying tasks and schedule for the approval of a new or modified elements of the CNS/ATM system related to ATS supported by data communication.

The **coordinated requirement determination** establishes the requirements that require coordination among organisations involved in the development, qualification, operation and approval of the CNS/ATM system.

The outputs of the coordination requirement determination process are an OSED, a SPR standard and an INTEROP standard.

**Operational Services and Environment Definition (OSED):** The OSED identifies the service descriptions, including operational communication process, operational performances expectations, selected technologies, and characteristics of the intended operation environment.

**Operational Safety and Performance Requirements (SPR) Standard:** The SPR standard is used to coordinate the operational, safety and performance objectives and allocate requirements for the different approval types.

**Interoperability Requirement (INTEROP) Standard:** The INTEROP Standard is used to provide sufficient information to enable different stakeholders to develop system elements that are compatible for an operation implementation.

The coordination requirement determination process consists of several sub-processes: the **Operational Services and Environment Information Capture (OSEIC)**. The OSEIC captures in a systematic and formal way the operational objectives of the operators and the ATS providers, in term of the implementation of ATS supported by data communication. The process involves all the potential applicants, including the operators, the aircraft modifiers, system integrators, equipment designers, ATS providers, communication service providers and approval authorities. The OSEIC produces the OSED.

the Operational Safety Assessment (OSA) that includes an Operational Hazard Assessment (OHA) and an Allocation of Safety Objectives and Requirements (ASOR). The input of the OSA are derived from the OSED.

**Operational Hazard Assessment (OHA):** The OHA is a qualitative assessment of the operational hazards associated with the OSED. Overall safety objectives are assigned to the identified hazards.

**Allocation of Safety Objectives and Requirements (ASOR):** Based on the OHA results, the ASOR allocates safety objectives to organisations, develops and validates risk mitigation strategies that are shared by multiple organisations and allocate safety requirements to those organisations.

the **Operation Performance Assessment (OPA)**. The OPA includes the determination of Required Communication Performance (RCP) type (issued from the OSED), allocation of RCP type to human (human performance) and technical elements of the system (RCTP) and allocation of RCTP to technical elements of the CNS/ATM system.

the **Interoperability Assessment (IA)**. The IA reviews the technical, functional and interface requirements for the defined technologies and allocate the requirement to different stakeholders and subsequent approval processes. Interoperability requirements are the minimum functional and technical requirements that provide the basis for ensuring compatibility among the various elements of the CNS/ATM system using specific technologies.

The OSA, OPA and IA includes the following generic activities: Identification of requirements, Co-ordination of requirements, Allocation of requirements and Validation of requirements.

The **development and qualification of a system element** are processes that are performed by each stakeholder to ensure that their element of the CNS/ATM system is produced with assurance that operational, safety, performance and interoperability objectives and requirements from the SPR and INTEROP standards are met.

The **entry into service** is the process whereby a state responsible for an airspace coordinate with all appropriate stakeholders the results of the development and qualification activities performed at the organisational level for CNS/ATM integration and preparation for operations.

The **Operations** include the process of ensuring that the operational, safety, performance and interoperability objectives and requirements for the ATS and operating environment are maintained through operations.

This methodology, developed to support the approval of the provision and use of ATS supported by data communication is now used by different projects having various objectives. In particular, the OSA methodology is used to support safety assessment in the development of new ATM concepts.

## Documentation related to Safety

### 6. EUROCONTROL – ATM 2000+

This document presents Eurocontrol's strategy for the coming years. It covers all the aspects Eurocontrol is supposed to address, including Safety. The general objective in terms of safety is worded as:

- "to improve safety levels by ensuring that the number of ATM-induced accidents and serious or risk bearing incidents do not increase and, where possible, decrease".

This general objective goes together with three refined objectives that are:

- "to ensure safety objectives can be achieved in the most efficient and economic way with minimum adverse effect on operational conditions",

- "to introduce safety tools which encompass all phases of flight from gate-to-gate in line with ICAO policy",

- "to introduce harmonised ATM safety policy, performance assessment and evaluation methodologies within ECAC States".

### 7. Internal Eurocontrol regulatory documentation

#### **EUROCONTROL Safety Regulatory Requirement - ESARR 4 - Risk Assessment and Mitigation in ATM**

This document presents the requirements in terms of risk assessment and mitigation, including hazard identification, in ATM when introducing and/or planning changes to the ATM system. These requirements are based on a systemic view of the aviation system and of ATM. Therefore, they combine human, procedural and equipment (hardware and software) aspects.

#### Brief comments

- The requirements presented in ESARR 4 document are quite ambitious as for the various objectives to be achieved in terms of safety analysis and risk mitigation.
- The document doesn't give much detail about the methods, techniques, tools to be used to meet these objectives. However, a Safety expert should be able to associate appropriate methods to the various requirements<sup>9</sup>. In addition, the ESARR 4 document refers to the EATMP SAM SAF ET1.ST03.1000-MAN- (Ed 1.0) as a useful guidance to implement the ESARR 4 safety regulatory requirement.

### 8. Methodological documentation

#### **FAA – System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management**

This handbook provides "best" practices in system safety engineering and management. It describes the process to analyse system safety throughout the life cycle of a concept, as well as the methods and techniques available to implement that process. For example, it describes the various steps to perform a hazard analysis as follows:

- Describe and bound the system in accordance with system description instructions (provided earlier in the handbook as well)
- Perform functional analysis if appropriate to the system under study
- Develop a preliminary hazard list
- Identify contributory hazards, initiators, or any other causes

<sup>9</sup> It may not be so easy or clear though for the requirements explicitly related to human factor aspects.

- Establish hazard control baseline by identifying existing controls when appropriate
- Determine potential outcomes, effects, or harm
- Perform a risk assessment of the severity of consequence and likelihood of occurrence
- Rank hazards according to risks
- Develop a set of recommendations and requirements to eliminate or control risks
- Provide managers, designers, test planners, and other affected decision makers with the information and data needed to permit effective trade-offs
- Conduct hazard tracking and risk resolution of medium and high risks. Verify that recommendations and requirements identified in step 9 have been implemented
- Demonstrate compliance with given safety related technical specifications, operational requirements, and design criteria

#### Brief comments

- The System Safety Handbook is a comprehensive document, rather dedicated to safety people than to managers given the level of detail of the information provided. However, for safety people, it provides a very useful overview of safety activities to be carried out throughout the design process, as well as of the methods available.
- A table (9-1 in Chapter 9: Analysis Techniques) provides an overview of over 80 analysis methods and techniques, with, for each of them, a brief summary, and some details about their applicability and use. Again, this table is not reproduced here for it is addressed to safety engineers rather than to project managers.

### **SAM – Safety Analysis Methodology**

SAM is the methodology referred to in the ESARR 4 document. It breaks down into three parts. SAM is still under development, and the first part is the only one to be available up to now.

The safety assessment methodology applies to ground-based components of Air Navigation Systems in the first instance. Later issues will address the integration of airborne and satellite systems.

The methodology considers only the safety aspects of the Air Navigation System. Other attributes of the system, aiming, for example, to achieve capacity and/or efficiency objectives, are not addressed by the proposed methodology.

The methodology does not address Air Navigation System certification issues. However, the application of the principles described in this manual could prepare to and support a certification process of Air Navigation Systems.

The methodology does not address organisational aspects related to safety assessment. For each project, organisational entities involved in the safety assessment process should be identified and their respective responsibilities specified.

The safety assessment process consists of three major steps:

- **Functional Hazard Assessment (FHA)** : its objectives are to determine the Safety Objectives to be achieved by the system. The necessary inputs are the description of the system, the description of the operational environment and, when appropriate, the safety regulatory requirements. Outputs will be the safety objectives and the hazards list.
- **Preliminary System Safety Assessment (PSSA)** : its objectives are to establish that the proposed system architecture is expected to meet the safety objectives. The necessary inputs are the proposed system architecture(s) and the safety objectives and hazards list. Outputs will be the safety requirements for each system element and a rationale for the selection of risk mitigation means.
- **System Safety Assessment (SSA)** : its objectives are to confirm that the system is safe for its operational purpose and operational environment. The necessary inputs are the system element requirements, next the implemented system element and integrated

system and at the end the validated system. Outputs will be the safety assurance material and the safety management procedures for operations and maintenance.

The safety analysis (FHA, PSSA, SSA) interacts with the EATMP Programme development processes to validate the safety requirements allocated to EATMP Programme functions, associated complementary distributed functions and operational aspects (operational and maintenance procedures). Then, transition to operations requires safety oversight of the system and decommissioning of the system necessitate assessment of impact on safety. The “Air Navigation System Safety Assessment Methodology” (SAM) and its associated awareness document (SAANS), developed in the framework of the Safety Domain, provides guidelines for conducting a system safety assessment and recommendations for the usage of some assessment techniques.

## 9. Vocabulary

The definitions provided hereafter are issued from the MAEVA:VGH.

**VALIDATION SCENARIO:** Representation of an operational situation in which an ATM operational concept is validated within one or several validation exercises, to enable the measurement and characterisation of the operational concept's performance. Descriptions of validation scenarios should cover location, timeframe, events and ATM environment.

**STAKEHOLDERS:** Actors in the ATM system whose support, co-operation and advice is important in ensuring that a proposed operational concept can be brought into service.

**VALIDATION:** The process through which a desired level of confidence in the ability of an operational concept to operate in a real-life environment may be demonstrated to the user, against the actual needs captured as a pre-defined level of functionality, operability and performance.

**VALIDATION AIM:** Clear, unambiguous definition of what is to be achieved through the conduct of a validation exercise. In the context of ATM validation, to provide information that demonstrates the feasibility of an ATM operational concept and that the concept provides a solution to the specific ATM problem it has been designed to address.

**VALIDATION CRITERIA:** Metrics and their target associated values used to determine whether a configuration has been validated.

**VALIDATION DESIGN:** Step within the validation process consisting of the design of specific validation procedures and exercises for specific configurations of the ATM operational concept.

**VALIDATION ENVIRONMENT:** The validation facilities and services to be deployed for a validation exercise, including a specification of the location where they will be deployed.

**VALIDATION MASTER PLAN:** The schedule of validation exercises to be performed for the European Commission's Fifth Framework Programme projects to determine whether, taken together, they fulfil the performance requirements of the future European ATM system.

**VALIDATION OBJECTIVE:** Formulation of a validation aim in terms of measurable factors.

**Warning** concerning what "measurable" means: VALSUP considers that some validation objectives can not be associated to objective and/or statistical data. To agree with MAEVA's definition, "measurable" shall cover the social, confidence building issues.

**VALIDATION PROCESS:** Process which encompasses overall validation, defining the tasks to be performed to validate a system from the time the system is first identified as a subject to be validated until the validated system is in operation.

**VALIDATION REQUIREMENTS:** Instantiation and/or breakdown of the high level validation objectives for a specific ATM operational concept, derived as a function of the individual components which make up the operational concept to be validated.

## Authors

Comments and criticism on this Eurocontrol document to

Nigel Makins [nigel.makins@eurocontrol.int](mailto:nigel.makins@eurocontrol.int)  
Nathalie DeBeler [nathalie.de-beler@eurocontrol.int](mailto:nathalie.de-beler@eurocontrol.int)  
Anne Cloerec [cloereca@sofreavia.fr](mailto:cloereca@sofreavia.fr)  
Philippe Freard [freardp@sofreavia.int](mailto:freardp@sofreavia.int)  
Corinne Bieder [cbieder@dedale.net](mailto:cbieder@dedale.net) (safety issues)

With thanks to Prof. Eric Hollnagel for his wealth of information.

Bretigny  
02/04/2002