EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

SAFETY REGULATION COMMISSION DOCUMENT
(SRC DOC)

SRC DOCUMENT 46

Annex C
Guidance on Interpreting and Using the Safety Scanning Results

Edition	**:**	**1.0**
Edition Date	**:**	**14 June 2011**
Status	**:**	**Released Issue**
Distribution	**:**	**General Public**
Category	**:**	**SRC Document**

F.2 DOCUMENT CHARACTERISTICS

TITLE		
SRC Document 46 – Annex C Guidance on Interpreting and Using the Safety Scanning Results		
Document Identifier	**Reference**	SRC Doc 46 – Annex C
srcdoc46_annex_c_e1.0_ri	**Edition Number**	1.0
	Edition Date	14.06.2011
Abstract		
The Safety Scanning Tool supports regulatory tasks such as oversight or approval processes. It utilizes a set of Safety Fundamentals as anchored in European law and demonstrates existing safety regulatory requirements as well as best practices in safety assessment. The Tool ideally is used iteratively use in the course of a life-cycle of a product. In initial phases it coordinates understanding of licensees and regulators on safety needs. In later phases it supports regulators in developing acceptance criteria for safety evidences provided by a licensee.		
Keywords		
Safety scanning	Safety Fundamentals	Safety Regulation
Contact Person(s)	**Tel**	**Unit**
Gary MORTON	+32 2 729 30 40	DSS/OVS/SAF

DOCUMENT INFORMATION					
Status		**Distribution**		**Category**	
Working Draft	☐	General Public	☑	Safety Regulatory Requirement	☐
Draft Issue	☐	Restricted EUROCONTROL	☐	Requirement Application Document	☐
Proposed Issue	☐	Restricted ESIMS	☐	ESARR Advisory Material	☐
Released Issue	☑	Restricted SRC	☐	SRC Document	☑
		Restricted SRCCG	☐	DSS/OVS Document	☐
		Restricted DSS/OVS	☐	Comment / Response Document	☐

COPIES OF SRC DELIVERABLES CAN BE OBTAINED FROM	
Oversight Division (DSS/OVS) EUROCONTROL Rue de la Fusée, 96 B-1130 Bruxelles	Tel: +32 2 729 51 38 Fax: +32 2 729 47 87 E-mail: sru@eurocontrol.int Website: www.eurocontrol.int/src

F.3 DOCUMENT APPROVAL

The following table identifies all management authorities who have approved this document.

Authority	Name and Signature	Date
Quality Control (DSS/OVS)	*« signed by Daniel Hartin »* (Daniel HARTIN)	14.06.2011
Head of Division (DSS/OVS)	*« signed by Juan Vazquez-Sanz »* (Juan VÁZQUEZ-SANZ)	14.06.2011
Chairman SCAN TF (SRCCG)	*« signed by Jos Nollet »* (Jos NOLLET)	14.06.2011
Chairman, SRC Co-ordination Group (SRCCG)	*« signed by Franz Nirschl »* (Franz NIRSCHL)	14.06.2011
Chairman, Safety Regulation Commission (SRC)	*« signed by Harry Daly »* (Harry DALY)	14.06.2011

(Space Left Intentionally Blank)

F.4 AMENDMENT RECORD

The following table records the complete history of this document.

Edition No.	Date	Reason for Change	Pages Affected
0.01	11-Dec-09	First draft.	All
0.02	31-Dec-09	Internal project group review.	All
0.03	11-Mar-10	Review SRCCG SCAN TF.	All
0.04	29-Nov-10	Update incorporate lessons learned Validation phase.	All
0.1	06-Dec-10	SRU quality review. Document sent for formal SRCCG consultation.	All
0.2	01-Feb-11	Document re-referenced as 'Annex C' to be consistent with SRC Doc 46, Appendix A. Document sent for formal SRC consultation.	All
0.3	06-Apr-11	Update following SRC consultation (RFC No. 1104).	All
1.0	14-Jun-11	Document formally released following SRC approval (RFC No. 1113).	References

(Space Left Intentionally Blank)

F.5 CONTENTS

1. GENERAL USE OF THE SAFETY SCANNING

The aim of this document is to provide guidance on interpreting and using the results of using the Safety Scanning Tool (SST). This guidance is intended to be used by a Safety analyst, whose task it is to interpret and consolidate the raw results coming out of a Safety scanning event. But in addition, the document is of use for an oversight authority when dealing with safety considerations coming from the Safety Scanning Tool. Guidance for the Moderator of a Safety scanning session is provided in a separate document, [SCR DOC 46 – Annex B, moderating].

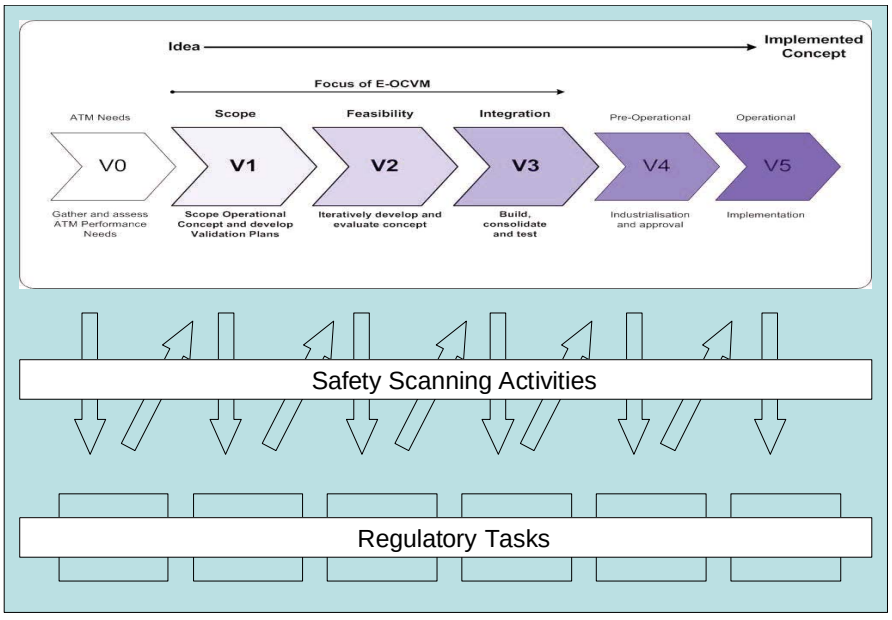
Section 2 provides guidance on how to interpret the answers to the Safety Scanning Tool in relation to the lifecycle stage of the Subject. The current section provides, as an introduction, a rationale for the relation between scanning and the lifecycle phases of the Subject.

1.1 Scanning as Safety Maturity Evaluation in the Course of the Lifecycle

The questions of the Safety scanning provide input in succeeding steps of a safety review. These inputs are called “Safety Considerations” and are the formalized result of a scanning activity. The results of the Safety scanning also formulate the basis for the NSAs’ oversight argument.

If for example there are “interdependencies” concerning an operational change and it is concluded that further analytical safety assessment is needed then this can have implications for the selection of a specific safety assessment methodology. The choice of the methodology has in turn an impact on the quality of the safety argument. As this quality determines the level of assurance that an oversight authority can take from the argument, it may determine whether the oversight authority needs additional actions from the ANSP to make the argument acceptable.

Whether the oversight authority needs to ask additional argumentation of a licensee also depends on the life cycle of a system development. This is illustrated in Picture 1, which depicts the life cycle stages according to the European Operational Concept Methodology (E-OCVM) [E-OCVM, 2007].



Picture 1. Regulators’ follow-up activities according to the life cycle of a system development [E-OCVM, 2007]

If for instance interdependencies are an issue in the early life cycle stages, the regulator should express his expectations to deal with the interdependencies properly during the remaining development phase. If a regulator has the position that interdependencies are an issue, he has to request a safety argument that deals sufficiently with these interdependencies. It is then up to the ANSP to provide an argument that deals with the issue and where needed use safety assessment methods that can effectively address this.

Oversight authorities have a set of tasks and tools that enable the review or oversight of a development and the eventual acceptance of a change and post-implementation monitoring [SRC DOC 46 – Annex D, regulatory advice]. These tasks and tools are:

- Approval,
- Review,
- Oversight,
- Incident analysis.

Through the E-OCVM stages V0-V5 [E-OCVM, 2007], these regulatory activities need to be applied and considered iteratively. “Applied” refers to review while “considered” refers to approval, oversight and incident analysis. The Safety Scanning Tool helps in fulfilling these tasks:

In early development phases the change is still under design. This allows developers some degree of flexibility in changing the concept when needed (usually V0 to V2). In general, safety arguments are under development and possible safety management activities are not yet determined in full. Key interrelations, which need to be reflected in the safety management principles can be clarified (especially when it comes to safety tasks and responsibilities). Also, the expectations for the content of safety arguments and basic design of the change can be identified. Through safety management and safety argument it should be identified whether changes in boundaries of the scope may change the safety performance. Safety scanning provides useful information to have such scoping information right at the beginning of a project (Example: Safety scanning of implications of a satellite based system for safety regulation and oversight would prevent misunderstanding in later review of safety cases). An effective application of the Safety Scanning Tool reveals the impact of the change and provides insights for an oversight authority which can be used to scope and plan its own activities during the succeeding stages.

In later phases where the design of the operational change is accomplished and is about to be implemented (usually V3 to V5), usually safety arguments are developed and safety management systems are amended where needed. The Safety Scanning Tool provides insights in how well the development phase took up the results from early Safety scans (V0 to V2) and gives more detailed recommendations on certain issues that may come up in late stages (e.g., unconsidered side-effects of a change). Of particular importance in latter phases is the suitability of analytical safety assessment methods to the nature of risk involved in the system (cf. ISO 31010; also [SCAN TF (2010, SST)]. For this particular issue, the Safety scanning method provides a separate Safety Methods Review Tool [SRC DOC 48]. This Tool supports the assessment of the usefulness of a method subject to the safety considerations that were identified.

(Space Left Intentionally Blank)

1.2 Scanning as Safety Maturity Evaluation Depending on the Size and Scope of the Change

In order to apply the Safety Scanning Tool to the different stages of a life cycle, the Moderator of the Tool has a particular role to adjust the scale of the questions to the general change ahead [SRC DOC 46 – Annex B, moderating]. The scale here refers to the technical content of the change that is being assessed (this could in principle be any part of the air transport operation) and the required level of detail of the expected answers in relation to the development stage and the general scope of change (single vs. multi actor change) as follows[1]:

Small Change (V0-V1-V2)

Single Actor

Aspects of the proposed Subject with a possible impact on safety should be highlighted. These aspects as well as efforts and considerations for their mitigation constitute the focal point of the iterative monitoring process.

Multi Actor

Specific demands concerning safety fundamentals aspects should be monitored under consideration of the combined efforts to detect and mitigate them by all the involved stakeholders. Also possible interdependencies and considerations about these should be timely highlighted by means of a thorough analysis of the scanning protocol.

Small Change (V3-V4-V5)

Single Actor

Mitigation efforts based on the results of the Safety scanning can be evaluated. Demands and concrete necessary actions concerning the proposed Subject which should be covered in the safety case can be formulated.

Multi Actor

The combined mitigation efforts and the identification of interdependencies should be clearly highlighted. Concrete recommendations and solutions to meet the safety demands as well continuity in safety considerations throughout the documented development process should be formulated to provide an unambiguous understanding for the safety case requirements.

Medium Change (V0-V1-V2)

Single Actor

The focal point for the safety analyst should be the early consideration of ways to control safety impacts already at the stages of the conceptual development of the Subject. Considerations about the possible interdependencies of the Subject's safety aspects should also be part of the safety monitoring, setting the stage for later safety assessment efforts.

[1] Note that there is a high potential that multi-actor changes are likely medium to large changes in practice. Nevertheless the following discusses all thinkable combinations.

Multi Actor

Opinions and assumptions of all involved stakeholders during the forming of the working hypothesis for the Subject should be taken into consideration and be part of the analysis. Especially aspects concerning the coordination needs towards the meeting of safety demands and possible issues of interdependencies between the fields of expertise as well as declared objectives concerning the Subject should be taken into consideration by the safety analyst.

Medium Change (V3-V4-V5)

Single Actor

Safety issues concerning the Subject should be compared to prior results to evaluate the mitigation process and the current state of the safety considerations. Information provided for meeting demands stemming from detected interdependencies of the Subject should be taken into consideration for the formulation of requirements for the safety case.

Multi Actor

The monitoring of the process and the safety related development of the Subject will have to be based on the comparison of earlier assessments and the current state, as reflected by the Safety scanning. Proof considering the adequate mitigation of safety aspects through coordination and consideration of interdependency issues constitutes the focal point for the safety case.

Large Change (V0-V1-V2)

Single Actor

Clearly stated formulation and perspective solution generation for mitigation of the impacts on safety should be the main focus of the safety analyst task during the early stages of development. Information stemming from the protocol should be thoroughly surveyed for the ongoing monitoring of the development. Any results from ongoing Safety scanning concerning the Subject should be taken into consideration. The safety analyst should explicitly highlight the need to take early action to reduce or eliminate any impact on the overall system safety.

Multi Actor

Search for indicating factors, which highlight the necessary coordination actions between involved stakeholders and mutual considerations of issues of interdependency. The adequacy of the ongoing process and assessment on basis of the Safety scanning protocols and results of the completeness of the planned mitigation process should be evaluated. Consultation of all stakeholders in all safety issues stemming from the Safety scanning need to take place as well as frequent monitoring of all iterations of the Safety scanning for the assessment of the current safety related state of the Subject.

Large Change (V3-V4-V5)

Single Actor

Meeting of requirements is important in the late stage of development. This could be done on the basis of the comparison between earlier and current assessments and explicit statement of urgent mitigation action prior to the issue process of the safety case. Necessary actions to be taken need to be explicitly notified and requirements of subsequent proof for the effectiveness of planned or taken action need to be stated. Safety scanning results should be surveyed frequently to monitor effectively any developments in the required direction.

Multi Actor

Thorough monitoring of the ongoing process and explicit statement of common requirements and necessary coordinating actions to meet the respective safety standards need to be performed considering consultation of all stakeholders involved in the development of the Subject. Detected inefficiencies and their mitigation to the upcoming issues of a safety case require explicit treatment also in respect to licensing procedures. Frequent monitoring of ongoing Safety scanning results and protocols for the monitoring and detection of the effectiveness of coordinated actions and mitigations supports such tasks.

By applying this approach, not only the oversight authority but also the licensee[2] is served. The oversight authority is much more prepared to specifically express which formal evidence he needs to get assurance. Where needed, the oversight authority can challenge the safety approach chosen by the licensee. This is both in the interest of the licensee (as in this case the oversight authority provides a relevant input to the safety responsibilities and performance of the licensee) and the safety assurance for the general public.

1.3 Process of this Guidance Material

The following section provides food for thought to the Safety analyst who is going to interpret the raw results of a Safety scanning event, and to the oversight authority when dealing with safety considerations coming from the Safety Scanning Tool. For each Safety Fundamental, a generic guidance will be provided. The generic guidance takes into account existing safety regulations (e.g. Single European Sky) and key standards (e.g. ISO) as well as the Safety Scanning Tool results on fundamentals and analytical methods. The rationale behind the generic answers is provided in the reports related to the Safety Fundamentals [SRC DOC 46 – Annex A, Safety Fundamentals; SRC DOC 46 – Annex D, regulatory advice].

Suggested actions will be provided based on the maturity of a development according to the life cycle as well as based on the potential impact of an identified issue.

Related to each safety fundamental, guidance or actions will be suggested with respect to:

- What to do if the fundamental is affected with a potential negative impact on safety (i.e. “What if impact” in the table)?
- What if there is no indication for a negative impact on safety for this fundamental (i.e. “What if no impact” in the table)?

And

- What if the Subject is in the V0 to V2 stages of a life cycle, where the system is still under design (i.e. “Early Stages” in the table)?
- What if the Subject is in the V3 to V5 stages of a life cycle, where the design of the system is accomplished (i.e. “Late Stages” in the table)?

[2] The term „licensee” is introduced in the documents in order to subsume the range of potential service providers that need to be regulated (in the context of SESAR it comprises in particular ANSP, Airport Operations, Airlines, ground based manufacturers, aircraft manufactures).

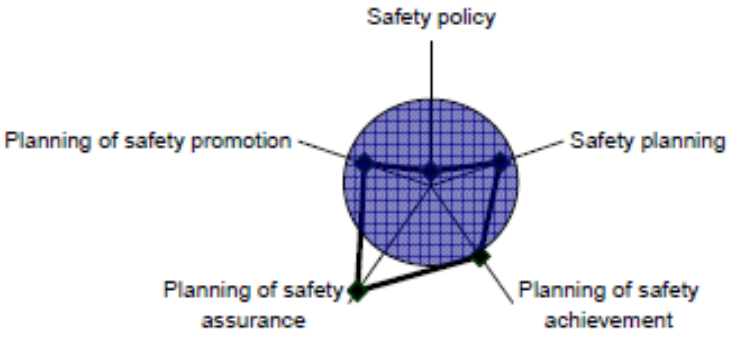
The generic guidance will be provided in a four-field table of the following style (Table 1).

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Generic guidance	Generic guidance
What if no impact	Generic guidance	Generic guidance

Table 1: Generic guidance in a four-field table

The matter of deciding if there is impact or no indication of impact is supported by the initial results page of the Safety Scanning Tool: The results of the Safety scanning session will automatically be presented in the form of ABC web charts. These web charts primarily serve two purposes. In the first place, they transform the answers on the questions concerning the Safety Fundamentals into a graphical representation of safety impact of the subject of discussion. Secondly, the web charts provide the basis for a comparison between the safety impact as displayed by the tool and the estimated safety impact as determined in the main part of the session.

Four different web charts are presented, showing the different safety perspectives (regulatory framework, safety management, operational safety, safety architecture) and their corresponding Safety Fundamentals. The web chart corresponding to the safety management part, for a hypothetical Subject, is provided in Picture 2.



Picture 2. The impact of the Subject on the Safety Fundamentals of the safety management perspective.

Each Safety Fundamental is represented by an axis with the points on the axis denoting the scoring of the answers on the questions regarding each fundamental. Scorings placed towards the center of the chart represent low scores, indicating less of a safety impact on the fundamentals ("What if no impact" in Table 1). Scorings more distant from the center represent high scores, indicating larger safety impact ("What if impact" in Table 1).

Note that if there is no impact, the generic guidance will usually still advise to pay average attention to the fundamental, also to verify whether the impact is indeed maintained to be low.

(Space Left Intentionally Blank)

2. INTERPRETATION OF THE SAFETY SCAN RESULTS

2.1 Safety Regulation

2.1.1 Regulatory Principles for Independent Oversight

Independent Oversight refers to the principle that the standards of safety to be achieved should be approved and monitored (i.e. oversight) by a competent body acting in the public interest, which is independent of service providers and designers/producers. The principle of independence is elementary to the entire concept of oversight. In order for the licensee to have benefit from oversight, independence is the guarantee for an honest external view and also the basis of an external statement of recognition of the safety performance of the licensee.

Any revealed inconsistencies or omissions concerning foreseeing and guaranteeing the independent oversight of the safety-related features of the proposed Subject should be highlighted at the earliest possible point to the licensee. Ensuring external, independent oversight of services and components is an essential part of ensuring total system safety as a whole. Therefore, the need for the prospective creation of the necessary communication and coordination interfaces with oversight bodies throughout the development of services and components should be explicitly stated under the perspective of its cardinal significance for granting approvals or acceptance of changes.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities need to address this structural issue at earliest convenience as it relates to licensees as well as regulatory oversight structures.	Operation should not become operable, due to lack of appropriate regulatory oversight.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Oversight authorities could consider verifying this statement together with the licensee.

At a late stage, detected inadequacies concerning independent oversight should lead the oversight authority to stop active involvement in a change process until the necessary structures are in place which will allow for the conduct of independent oversight prior to (as well as next to) the implementation.

If there is no clear indication of an inconsistent or inadequate fulfilment of this fundamental, the oversight authority should monitor the ongoing development on a mutually planned and accepted regular basis, also in order to monitor deviations from the fundamental objective and communicate these to the licensee. It is recommended to use the Safety Scanning Tool for the achievement of this purpose.

At a late stage, additional evidence for the fulfilment of the fundamental-relevant requirements should be provided by the legislator to allow approval or acceptance by an oversight authority to a licensee.

2.1.2 Structural Needs – Legal Mandate & Ability for Ensuring a Safe Standard

Ensuring a Safe Standard refers to the duty of all service providers and designers/producers to take all reasonable precautions to ensure that their services or products are safe.

In case the Safety scanning process reveals inconsistencies or ambiguities regarding the safe standard of the development then the oversight authority should explicitly state the need for providing all necessary means to ensure the compliance with the safety standards relevant to the change. The licensee should take existing standards, regulations and ongoing developments of safety standards and certification processes into account.

If these requirements are not met at a stage immediately prior to implementation, the oversight authority will be put in a position that he effectively does not give an acceptance or approval for implementation until these requirements are met in a way which will ensure safe operation.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities should address the need for evidence from the licensee to have ensured all reasonable means in the product development to assure safety. Clear expectations should be addressed to the licensee (e.g., to urge the need to reflect ISO 31010 properly).	Oversight authorities should not grant approvals or acceptance until sufficient evidence is provided that existing standards, regulations and ongoing developments of safety standards and certification processes have been taken into account.
What if no impact	Oversight authorities should address the need for evidence from the licensee to have ensured all reasonable means in the product development to assure safety. Clear expectations should be addressed to the licensee (e.g., to urge the need to reflect ISO 31010 properly).	Oversight authorities should consider asking for evidence for this statement.

The oversight authority should highlight the need for the existence and conformity with actual up to date safety standards and the need for a certification concerning compliance with existing standards and regulation to the licensee. Knowledge and conscious consideration of these issues should be taken into account during all stages of the development.

Additional evidence for the fulfilment of this fundamental must be on hand prior to the granting of the acceptance or approval. If such evidence is not or inadequately available, then no acceptance or approval should be granted until the licensee provides the oversight authority with sufficient and convincing evidence concerning the compliance with widely accepted and up-to-date safety standards.

Effectively dealing with this fundamental implies that also the oversight authority is fully aware of existing standards, regulations and ongoing developments of safety standards and certification processes.

2.1.3 Implementation needs for Responsibility for Safety

Responsibility for Safety is based on the principle that the prime responsibility for the safety of a service or product rests with the service provider or designer/producer. If this is not captured in specific legal provisions then the principle of due diligence applies.

At an early stage of component development, the oversight authority has to discuss the issue of responsibility for safety with the licensee in order to achieve a clear picture for considerations and planned procedures regarding the allocation, transfer and sharing of responsibilities between different parts within the organisation or between different organisations that may be affected by the implementation of the change. The way these shared responsibilities for safety issues are communicated and coordinated within an organisation or between organisations (in terms of interfaces) should be given as input for consideration for the licensee.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities cannot highlight the issue of responsibilities early enough. They should urgently address this issue – even without request of the licensee.	Oversight authorities should not grant approvals or acceptance until clear responsibility for safety is guaranteed.
What if no impact	Oversight authorities cannot highlight the issue of responsibilities early enough. They should watch whether the initial statement on responsibilities is still valid in the later development stages.	Oversight authorities should consider asking for evidence for this statement.

2.1.4 Need for New Regulations

The safety regulations need to be kept up to date, in order to reflect the state of the art in safety. Usually five years after publication standards are reviewed to determine whether revision is necessary.

At an early stage of operational development, the oversight authority has to discuss the potential of the change on existing regulations in order to be flexible in late stages.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities should investigate potential change of regulation.	Oversight authorities need to address the change via appropriate channels (ICAO, EU).
What if no impact	No specific action to do.	No specific action to do.

(Space Left Intentionally Blank)

2.2 Safety Management

2.2.1 Understanding and Openness in the Safety Policy

Understanding and Openness are defined as the degree to which the commitment to safety and setting out the strategic safety aims is performed. This performance should be done in such a way that all opinions and considerations within an organisation or from other organisations are taken into account in the safety policy. Safety policy should in this context be understood as the general safety approach for the development and should not be confused with the safety policy of organisations as they may be required to have in accordance with prevailing legal requirements. Understanding and Openness are essential enablers for an effective safety culture and are key requirements to an effective SMS and the safety regulatory confidence in the operation of an SMS.

If the regulator should detect deficiencies regarding the understanding and openness fundamentals in the proposed change or in the process regarding its implementation and integration in the embedding system, then explicit action should be required of the licensee to mitigate or to eliminate these deficiencies. The deficiencies could result in the need to revise the safety policy that an organisation has but is more likely to have an effect on the way this safety policy is effectively implemented (e.g. the assignment of safety responsibilities). The action to be requested depends on the stage of the development.

At early stages, a change in the safety policy on behalf of the licensee should prove an adequate countermeasure to the detected deficiencies. The request to be made should take specific notice on the need for a revision of informational flow processes and the intra- as well as the inter-organisational interfaces between the stakeholders involved in the development of the safety policy. This is aimed to ensure the prerequisites of the fundamentals at a strategic as well as an implementation level.

When deficiencies are detected at a late stage, the oversight authority should explicitly demand of the licensee to take all necessary precautions and countermeasures and carry out all necessary changes which will ensure the open flow of safety-related information and the understanding of safety-related issues throughout the whole range of the involved organisations and stakeholders. Unless these demands are satisfied to an acceptable and safety-ensuring degree, the regulator should consider not approving or accepting the implementation of the change.

If no indications for deficiencies or non-deliberate violations of the fundamentals are present, the oversight authority should consider asking for evidence regarding the achievement of the fundamentals. Evidence should refer to the description and explanation of the process of the consensus achievement regarding safety-related issues of the proposed development (a typical example of evidence in this case are approved meeting minutes). Suggestions for a systematic inclusion of all stakeholders in the decision and information processes should also be recommended to the licensee at the early development stages of the component.

(Space Left Intentionally Blank)

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Safety policy needs to be established or revisited by the developer or by licensee. The iterative use of the Safety Scanning Tool could be offered as an additional means to achieve or maintain consensus (e.g. on clarifying safety responsibilities either intra- or inter organisational).	If there is no understanding and openness then likely there is a tainted proposal to address safety which could negatively affect the safety of the development in the implementation (e.g., biases could exist which can range from biases toward a technical solution to biases towards a specific analytical safety assessment method).
What if no impact	Oversight authorities could suggest to systematically involve all stakeholders and to ask for evidence how consensus was achieved and how consensus is reflected in the safety policy.	The oversight authority needs to thoroughly monitor the succeeding steps of the licensee to provide evidence for safety.

2.2.2 Completeness and Freedom from Bias in Safety Planning

Completeness and Freedom from bias are defined as the appropriateness of the aims of the organisation, the resources and management structure chosen and the processes established in order to have the best safety-related solution.

In case of detected deficiencies at an early stage of development through the Safety scanning process, the oversight authority should request of the licensee to provide the documented decision-making process, the methods used to assess and plan the safety-related aspects and anticipated effects to the point of the Safety scanning, connected to the proposed development. Discussions, decisions and proposed solutions should be evaluated under the aspect of retaining or optimizing an established good safety practice for the total system.

At a late stage, the licensee should immediately address safety considerations delivered by the Safety scanning process, as any issue of incompleteness and existing bias related to the implementation of the change could seriously endanger the safety of the whole system in unpredictable ways. The licensee should be required to provide information regarding the documentation of the decision-making and the methodological process, which led to the final decision regarding the implementation intention of the proposed Subject. In general, oversight authorities currently do not oversee this nor are licensees always eager to provide such information. This observation as such should already raise interest with the oversight authorities.

If no indications for any deficiency concerning the Safety Fundamental are present at the point of the Safety scanning, the oversight authority should nevertheless consider asking the licensee for explicit evidence concerning the unobstructed and compliant implementation of the proposed change in relation to its safety-related completeness and freedom of bias. This point could be mostly relevant at the late stage of development and immediately prior to implementation of the proposed change. Providing information and the documentation of the complete decision-making process could be an adequate means for the regulator to request of the licensee to achieve this objective.

Effective auditing as part of the ongoing oversight may have built up confidence over time that the licensee addresses these fundamentals in an appropriate manner. It is the responsibility of the oversight authority to determine what level of involvement is needed.

The Report [SRC DOC 46 – Annex D, regulatory advice] of this series and also ISO 31010 might help in judging about incompleteness.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities should state the need to have clear evidences for the decision making process made in the product development which lead to the final decisions.	Known incompleteness is a legal issue that needs to be highlighted by the oversight authority. Likely also the safety argument will include this issue and reviews should in particular address the completeness and impact of decisions on the final product.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Oversight authorities could consider asking for evidence for this statement.

2.2.3 Responsibility and Practicability in the Planning of Safety Achievement

Responsibility and practicability are defined as the detailed means of translating the plan into reality by means of clear responsibilities for and practicability in safety achievement.

If the Safety scanning process reveals any inconsistencies or deficiencies of the fundamentals of responsibility and practicability in an early stage of the development then the oversight authority should request of the licensee to address the revealed issues during the ongoing design process. Any action to be taken has to be in accordance with existing and applicable legislation and should include modifications in the planned design process, in order to eliminate any ambiguities concerning the allocation of responsibilities and the transfer connected to the actual implementation of the change and the subsequent operation at the earliest possible point. The licensee has to assess and provide information regarding the well-established and well-working practices, which are or could be relevant for embedding and operating the proposed change within his operations. In this way, it will be ensured that requirements concerning the fundamental of practicability will also be met at an early point in the development to ensure a problem-free operability of the total system.

If inconsistencies regarding the fundamentals should be revealed through the process of the Safety scanning at a late stage of the development, then the oversight authority will need to consider holding off the implementation until the allocation of responsibilities and the transfer process is clear to, and accepted by all parties involved in the implementation. The implementation process can only restart, if no ambiguities are left regarding the fundamentals.

If there are no apparent deficiencies the oversight authority should at an early stage monitor the development process and regularly make use of the Safety Scanning Tool to verify or where needed indicate a needed redirection of the efforts to satisfy the requirements to meet the fundamentals.

Prior to the implementation of the proposed Subject, the licensee should provide explicit evidence that relevant needs related to responsibility and practicability will be met in the best possible way. Such evidence can be part of the safety argument but could equally well be found in a “transition plan”.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities should state the need to have clear proposal how to achieve responsibility for final decisions.	Oversight authorities should not grant approvals or acceptance until responsibilities are clear enough to proceed.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Oversight authorities could consider asking for evidence for this statement.

2.2.4 Detectability and Feedback in the Planning of Safety Assurance

Detectability and Feedback are defined as the detectability of safety issues by continuously monitoring of safety performance (feedback) in order to realize safety assurance.

If the Safety scanning process indicates deficiencies in the specific fundamentals at an early stage of development, the oversight authority should explicitly highlight the need for the existence of technical and administrative instances for detectability and safety-related feedback within the organisation and specifically related to the function /operation of the proposed change. The licensee should provide his planned concept introducing all critical aspects of the fundamental like valid and usable safety indicators, established practice methods for safety-data analysis (e.g. event analysis), cooperation between organisations and information flow concerning critical safety aspects related to the component or/and the use of the component within the operational system boundaries, etc.

At a late stage of development, the oversight authority should consider holding the implementation and approval or acceptance process until the licensee provides explicit information about the coverage and the adequacy of the planned safety-related feedback methods, interfaces and internal or external feedback loops related to the proposed change.

If the Safety scanning process reveals no indications of any deficiencies concerning the detectability and safety-related feedback fundamentals, it is recommended to monitor the development process regarding the gradual implementation of the concept in practice on a regular basis. An iterative use of the Safety Scanning Tool is recommended for discussing the monitoring activities.

At the late stage of the development, the oversight authority should ask of the licensee to provide explicit evidence of the planned means to achieve a valid fulfilment of the detectability and safety-related feedback fundamentals.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities should state the need to have clear proposals on how to provide feedback.	Oversight authorities should not grant approvals or acceptance until effective monitoring of safety issues is guaranteed.

What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Oversight authorities could consider asking for evidence for this statement.

2.2.5 Responsiveness and Learning Responsiveness and Learning in the Planning of Safety Promotion

Responsiveness and Learning are defined as the way of totality ensuring a continuous improvement process, timely corrective actions (responsiveness) and dissemination of lessons learned (learning) in the planning of Safety Promotion.

Not being able to timely respond to changing demands or incompletely defined service often leads to the fact that safety problems persist for a long time and work-around solutions are developed which potentially, leads, in the long term, to violations. Especially if systems are complex with many involved stakeholders, the time needed to implement a required change might drastically increase.

Any system needs to be effective in the way safety is improved. However, complex systems with lots of internal and external suppliers may be sluggish in the reaction - even on very critical safety related events. Improvements might be initiated too late. Knowledge gained by further development of the “state of the art” in system technology or procedures might be considered too late or too slow for improving the system. In both cases latent weaknesses persist, safety issues remain without improvement with the potential to lead to safety critical events.

Such a situation is critical from the safety regulatory point of view. If information from an event is not used timely to improve the system, the organisation could be addressed in a legal action for injunction (i.e. safety regulatory risk). If the development of “state of the art” is not well taken into account, legally the organisation could possibly run into an issue of negligence (IAEA, 2006).

In order to fulfil its regulatory responsibility to act for the health and safety of the public, safety regulatory bodies need to address the lack of responsiveness.

Several levels exist in regulation to ensure oversight of responsiveness in organisations like the requirement to report the results of an incident investigation in a specific timeframe (RSK, 2008); periodic safety assessments (in the nuclear industry every 10 years) to check the overall status of a system (BFS, 2004). Standards providing underlying guidance on the methodologies used need continuous updates every five years in order to keep the required methodologies up to date and valid.

In case the Safety scanning process reveals inconsistencies or deficiencies concerning the responsiveness and learning fundamentals, the oversight authority should highlight this to the licensee and require subsequent actions to meet the respective requirements. A structural design should be able to demonstrate a prospective conceptual and methodological basis for the timely and safety-relevant appropriate identification of improvement needs in the system related to the proposed change.

The impairments that result from organisational factors to any efforts concerning a safety-related response and the ability of the organisation to learn from failures in an efficient manner should be identified at the most early design stage. In general “lessons learned” from previous development may have been forgotten or not been given to the developers. The oversight authority should refer to the importance of an acceptable solution as providing assurance for the acceptance or approval of the change.

If deficiencies are still prevailing at a late stage of development, the oversight authority should explicitly state the need for the fulfilment of the fundamental and agree with the licensee on the timeframe for the presentation of an acceptable concept for responsiveness and learning. The existence of the concept should be considered as a necessary precondition for the acceptance or approval of the change.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight authorities should ensure that the licensee knows that he has a structural issue to solve, which might endanger acceptance or approval of the change.	If there is an issue with responsiveness and learning, the licensee has a structural issue to solve. Oversight authorities should make the implementation of an appropriate solution within a limited period a precondition for granting an approval or acceptance.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Oversight authorities could consider asking for evidence for this statement.

If the Safety scanning process reveals no indications of deficiencies concerning the fundamentals, then the oversight authority has to monitor the development with regard to possible issues with the responsiveness and learning process concerning the implementation of the proposed change. It is recommended to conduct Safety scanning on a mutually accepted regular basis, with the purpose of ensuring the existence of an acceptable concept throughout the development process of the proposed Subject.

Over time, the oversight authority should require of the licensee to provide evidence for the existence and the (conceptual, methodological and time-related) adequacy of the change concerning the Safety Fundamentals of responsiveness and learning. This is to be considered part of the ongoing oversight of the effectiveness of the SMS.

(Space Left Intentionally Blank)

2.3 Safety Performance – Operational Safety Aspects

2.3.1 Procedures

Procedures describe which actions are required by human operators to deliver a service. Effective procedures include definition of roles, responsibilities, structure, content, detail, and realism. From an oversight point of view, it is necessary to identify that responsibilities of different actors are clearly established (e.g. the airspace designers, the inspectors for calibration in flight, the AIS providers and the providers of digital data to avionics, in relation to instrument procedures).

Procedures are a well-established aspect of achieving and verifying safe performance. Over- and under-proceduralisation may however lead to safety issues. Over-proceduralisation leads to less flexibility, hence leads to less ability to cope with unforeseen situations; under-proceduralisation leads to lack of consistency in operations, which then gives opportunity for acting outside the operational envelope which is considered as safe.

The oversight authority should request of the licensee to clarify possible tasks, roles, responsibilities of the human operators involved with the proposed development.

The necessity (but also the possibility to provide) for detailed, clear and unambiguous procedures increases proportionately during the development stages. A thorough overall consideration about procedures and their consistency with the existing procedural framework should be already established at the earliest stages of the development. Respectively, sufficiently detailed information concerning the crucial procedural aspects and requirements of the development (e.g. appropriate degree of proceduralisation, specific roles and responsibilities) should only be provided to the oversight authorities at the later stages of the component development.

If the safety consideration is not raised related to this fundamental, the oversight authority should state this fact explicitly. In a safety argument that is offered for acceptance of a change procedures are often mentioned as needed or in place. Procedures as such however also require validation of their suitability in operations.

In case of an assessment of consistency and compliance of the proposed change with the existing regulatory framework (e.g. procedures often find their basis on criteria or practices set by ICAO), considerations should be made concerning the possible requirements and needs for flexibility of the proposed procedures. Given that procedures are intended for efficient and safe operational application, if a degree of deviation from the existing regulations is to be considered as necessary, requests by the licensee should be formulated in a concrete and realistic way. If in agreement, the licensee and oversight authority become de facto partners in a common need to have the regulations amended.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authorities should request the developer to lay out the responsibilities clearly.	Oversight authorities should consider not accepting the change in case of lacking or non-validated procedures. A safety argument should provide sufficient evidence for the validation of procedures where due consideration is given to a possible trade off between flexibility and consistency.

What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Evidence for the realism, effectiveness and joint feasibility of the procedures should be sought in validation activities of the change (e.g. in dry runs).

2.3.2 Competence

Competence is defined as the capabilities of the staff working on the operational, technical and procedural aspects of the environment they are working in. This fundamental relates to all conceivable staff involved in aviation and not only those that are subject to licensing directives. Competence needs time to be built up, and although competence issues normally become apparent during real time operations it is an issue that needs consideration during the early development phases.

If the Safety scanning reveals inadequacies or vagueness in the description of the necessary staff competencies specific to the operation and maintenance of the proposed Subject, oversight authorities should request of the licensee adequate proof and clarity as well as conformity to existing regulations and legislations. These existing regulations and legislations in general require that staff is properly trained to exercise their tasks.

If the proposed Subject requires different and specific qualifications and/or training compared to the existing ones then oversight authorities should request of the licensee to provide a specific description of the necessary operative competences of the complete staff involved with the implemented development (including maintenance tasks and requirements). Such a specification should be accompanied with a plan on how competence requirements can be met prior to implementation.

If the descriptions of the competences leave no doubt about the competences of the staff involved with the operation and maintenance of the proposed change, a respective statement should indicate this fact.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authority should highlight the importance of this fundamental for final acceptance but has no immediate requirement for action because building of competence is under the discretion of the licensee.	Oversight authorities should consider not accepting the change in case of lacking competence; this will result in a potential of delay of operations.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Evidence should be asked and verified on the appropriateness of level of competence.

(Space Left Intentionally Blank)

2.3.3 Human-machine Interaction

Human-machine interaction is defined as the quality of the interaction between the system and the human which is needed to provide the intended service. It includes in particular workplace design, workstation ergonomics, usability, working environment, and job-induced fatigue. System and equipment complexity are recognizable performance factors that influence human reliability and have the potential to lead to human error. Examples of technical systems which may lead to human error are; complexity and amount of equipment; functional dependencies or dependencies between control systems, safety systems or barriers.

The licensee should address considerations on emerging issues concerning aspects of human-machine interaction and physical and cognitive ergonomics already at the early stages of the proposed Subject. Requirements on compliance and / or amendment of the planned human-machine features of the components should be guided by already existing norms and regulations for safe and user-centred design (e.g. ISO 10075).

Continuous review of the component development is recommended already when an adequate description of the planned human-machine features exists in the early development stages. This review could facilitate the monitoring the implementation of the planned features as well as a clear understanding and adequate briefing of the oversight body concerning in case of trade-offs or deviations from the initially envisaged design and their impact on the overall system safety.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authority should highlight the importance of this fundamental for final acceptance but has no immediate requirement for action.	Oversight authorities should consider not accepting the change in case of unresolved HMI considerations; this will result in a potential of delay of operations.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Evidence should be asked and verified on the appropriateness of the HMI.

2.3.4 Operating Environment

The Operating Environment is defined as the conditions under which the operation takes place. Conditions should be understood as e.g. variable weather conditions, traffic mix, airspace classification, etc. Environmental aspects are important conditions for human performance, which need consideration at the design stage because they are usually not modifiable.

Licensees should involve oversight authorities early in project phases where there is still flexibility in the development to ensure that relevant different operating environments are taken under consideration. Such an early involvement is likely to increase the sense of assurance. It should be expected that developers are very familiar with the environment where the development is intended to be implement. However with developments that have an effect outside a typical area (e.g. outside the national boundary), specific national considerations may not be known by the developer.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authority should highlight the importance of this fundamental for final acceptance and recommend to licensee to interact in line with the expected implementation area.	Oversight authorities should consider not to accept the change in case of unresolved operating environment considerations; this will result in a potential of delay of operations
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Evidence should be asked and verified on the appropriateness assumptions taken on the operating environment and possible trade-off conditions.

The licensee should take action and revise the development under consideration in order to meet all the foreseen requirements for the specific operating environment. If the development is intended to be applied in more than one context, the modifications on the development should take into account all possible critical parameters, in order to ensure both acceptable working conditions and system operation within the predefined safety boundaries.

The oversight authorities should request this consideration in an explicit way, which should provide assurance on meeting requirements of the proposed change for this fundamental.

The requested statement of the licensee should refer explicitly that the fulfilment of the requirements refer directly to the specific stage of development and that a continuous consideration of this issue will take into account the dynamic nature of the specific demands of the operational environment.

2.3.5 Organisation

Organisation is defined as the managerial aspects of the working environment. Organisation is covering the managerial aspects of the working environment like the human resources required to operate the system and provide service.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Oversight organisations should be tested on their capability of dealing with the system change (e.g. necessary cooperation between regulators). Regarding the licensee, the oversight authority could highlight the need to have an appropriate and clear organisational structure, but this is no regulatory requirement at this stage;	Regarding the licensee, oversight authorities should consider not to accept the change in case of unresolved organisational aspects.
What if no impact	No oversight activity required at this stage.	Oversight authorities could consider asking for evidence for this statement.

As a general position, oversight authorities should consider requesting the licensee to provide evidence concerning the highlighted organisational aspects related to the safe and undisturbed operation of the component and the embedding system as soon as possible.

If the Safety scanning activities reveal no evidence concerning organisational aspects, which could contribute to a breach of the Safety Fundamental, a respective statement should explicitly highlight this fact.

2.3.6 Communication

Communication is defined as the interaction between people which includes aeronautical telecommunication. Adequate communication between and amongst different players in the air transport operations like controller, pilots, flow managers, maintenance staff, manufacturers, management, regulation is key for safe operation.

In case the Safety scanning reveals inadequacies in the prospective or actual design of communication regarding the proposed change, then the oversight authority should request of the licensee to take action to address any ambiguities that could threaten the safety of the overall system operations. Communication design should, due to its criticality for safe system operation, be addressed as intra-organisational as well as inter-organisational aspect. The current communications could both be affected by or affect the proposed development. At the late stages prior to the implementation of the component, communication design should be able to exhibit a maximal adequacy and conformity to the operational needs and characteristics of the embedding system, in order to ensure its operability and safety on the long term.

Due to the undoubted criticality of communication, the licensee should provide evidence for the adequacy of the communication design, even if the Safety scanning does not highlight any problems with the fundamental for the proposed development.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Regarding the licensee, oversight authorities could highlight the need to address communication issues in the safety argument	Oversight authorities should consider not accepting the change in case unresolved communication aspects are not properly represented in the safety argument.
What if no impact	No oversight activity required at this stage.	Oversight authorities could consider asking for evidence for this statement.

2.3.7 Reliability

Reliability is defined as the overall safety performance, including the potential of recovering from unwanted situations or failures in time. Reliability is an overall view on operational safety combining all elements of the entire safety performance. It describes the potential to perform safely in a stable manner with absence of breakdowns or service interruptions.

If the process of Safety scanning shows deficiencies or ambiguities in the proposed change concerning this fundamental, explicit instruction to the licensee should take place. Reliability-related instructions should take into consideration the stage of development and should cover all three phases of reliability i.e. prevention, detection and recoverability.

It should be made clear to the licensee that if these prerequisites for the proposed development are not effectively met or if inadequate consideration of the fundamental during given in the development and in the safety argument, no approval or acceptance can be given.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	If already at this stage there are issues with reliability, the oversight authority should highlight to the licensee to address these in system design and system safety arguments.	Oversight authorities should not grant approvals or acceptance for operations.
What if no impact	The oversight authority should highlight the need to have evidence about this statement for final acceptance.	Oversight authorities could consider asking for evidence for this statement and are likely not in the position to grant acceptance if no evidence exists.

Even if no indication of impact for the fundamental of reliability is present in the Safety scanning process, the oversight authority should ask for additional explicit evidence for the system-compatible and reliable design of the proposed change prior to the approval or acceptance.

2.4 Safety Performance – Safety Architecture and Technology

2.4.1 Transparency

Transparency describes the ability to specify clearly, what the result of the change is on the performance of the operation, and how the changed task will perform consistently as specified. From an institutional point of view this may also include a clear identification of the legal responsibilities (e.g. of the Galileo designer as distinct from the service provider of the Galileo signal in space).

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authority will need to insist on the development of clear specifications (technical, procedural, legal) in order to have sufficient confidence in the further development.	If safety arguments are delivered despite a lack of transparency, safety arguments are likely to have an insufficient level of detail or might contain assumptions, which are so unfounded that they may not reflect the reality of the system. Approval should not be given and potential re-assessment will need to be required from the licensee. The oversight authority should clarify that this decision is based on the lack of transparency.
What if no impact	An oversight authority' task could be to conduct regular re-checks of this fundamental for possible changes during the development.	If the design is transparent and can be explained clearly, the regulator will be able to grant acceptance of a proposed design.

In case this fundamental is affected, the oversight authority is generally faced with an incomplete or ambiguous design, which is difficult to be fully understood. It might also be that specifications are not well outlined (for either: technical systems, human procedures or legal responsibilities). A possible pitfall here is that the reviewer at the oversight authority starts making his/her own assumptions on what is meant. This is a normal initial human reaction but should be avoided.

Usually issues of transparency reoccur during the lifecycle of a product. This means that with further development of a product specific issues of transparency (on a more detailed level) might occur.

2.4.2 Redundancy

Redundancy is defined as the use of independent components performing the same function thereby protecting the system against breakdown due to single component failure (single point of failure). In turn, independently redundant components can be based on the same technology (e.g. duplicated engines or duplicated ILS transmitters) or on dissimilar technologies (e.g. radar plus ADS or line-of-sight data link plus satellite data link). From the regulatory point of view, some responsibilities (e.g. decisions on obligations to equip are addressed to both air operators and ANSPs, or protection of the aeronautical frequency bands or of the aerodrome surroundings) belong to governmental prerogatives, at either national or EU level.

Redundancy is needed to cover uncertainties due to all possible impacts and to make the system robust / resilient against operational uncertainties, which could not be anticipated in the design.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Lack of Redundancy is a potential safety problem. In principle, the system then would require a higher reliability of the singular components (e.g., if only one pilot is left in the cockpit, the overall remaining aeroplane-system consisting of the automated system and the pilot should be at least as safe as the initial (complete) system).	The data used for an analytical assessment need in a safety argument needs to have high quality. The safety arguments need to have a broad spectrum of scenarios to show that the system is either redundant or sufficiently robust.
What if no impact	The oversight authority requires evidence for a statement that redundancy is not an issue. This means the licensee needs to provide proof for having enough redundancy in the system in line with the importance of the system.	In case there is a built-in redundancy there is likely to be a budget for safety established as part of an analytical method. The subject of change might be included in the analytical safety assessment and the oversight authority could be satisfied with the applied method.

2.4.3 Interdependence

Interdependence is defined as the degree to which a system interacts in an intended or unintended manner with other systems (unintended interdependence may result e.g. in common cause failures or propagation of errors into adjacent systems).

Interdependencies should be taken into account when providing safety arguments for a change to an individual system. In current analytical safety assessments, often interdependencies are not investigated in detail and assumptions are often made and consequently accepted without evidence. A number of measures should be put in place to oversee the subject of change efficiently within the context of the total system.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	Suitable method(s) for analysis of interdependencies need to be selected by the licensee.	A safety argument for a change of a licensee needs to address this issue in particular.
What if no impact	If the Safety scanning reveals no obvious interdependencies, there might be some becoming more evident in the succeeding stages of assessment. A general recommendation should be stated that providing evidence for absence of interdependencies is required.	Many popular safety assessment methods (e.g., fault-tree / event-tree) have only limited capabilities to deal with interdependencies. If such methods are used, it is likely that the absence of interdependencies is an artefact of the method rather than reality. The oversight authority should advise the licensee to provide additional evidence that interdependencies are addressed effectively.

For any the approval of a principal way ahead, the licensee should be made aware of his responsibility to address this issue and consequently be required to provide sufficient evidence on how interdependencies are and will be addressed in the safety management and assessment process.

The regulator could use the Safety Methods Review Tool [SRC DOC 48; SCAN TF (2011, SMRT questions)] and ISO 31010 in order to get a feeling how suitable the selected method(s) by the licensee are to address this issue effectively.

2.4.4 Functionality

Functionality is defined as the correctness, consistency and un-ambiguity of the behaviour of the system. An important distinction for Functionality is the one between design-based situations (everything a design might have thought of as potential safety relevant scenarios and risks) as well as beyond design-based situations (the unforeseen events and risks). Functionality describes how well a system is able to deliver in both design-based situations as well as in beyond design-based situations.

Issues of inadequate functionality relate to possible problems with the functional reliability and availability of the proposed feature. Such problems, if not addressed early on at the development and testing stage prior to implementation, can have a severe impact on the overall system safety. They represent so called latent conditions within the system, which under circumstances could undermine the safety boundaries of system operations.

In case the regulators using the Safety Scanning Tool face a possible lack or possible inadequacies of functionality concerning the proposed Subject or features of it, they should request of the licensee a founded analysis and subsequent proof regarding the functional features of the proposed Subject. The analysis should be conducted both on terms of technical- as well as human factors-related functionality.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The regulator should highlight the importance of this fundamental for final acceptance but has no immediate requirement for action.	A review of a safety argument for a change needs to address in particular the appropriateness of the scope and completeness of scenarios the licensee has assessed.
What if no impact	If the Safety scanning reveals no obvious issues with functionality, there might be some becoming more evident in the succeeding stages of assessment.	A regulator needs to review carefully the safety case as the absence of issues with functionality might be an artefact of the method rather than reality. The regulator should advise the licensee to redo the safety case, unless other evidence is provided on the absence of any issue with functionality. (same as with interdependencies)

Regulators can refer to norms and regulations concerning minimum requirements of the functionality of components or procedures, in case such references are available or existing.

The licensee has additionally to conduct a thorough risk analysis, which will reveal the criticality of a possible failure of all significant features of the proposed Subject to the overall system operations. Such risk analysis should include design-based situations (known or anticipated at the time of design) as well as considerations about possible beyond-design situations and their relation to the component functionality.

In case the Safety scanning does not reveal any issues concerning the current and expected functioning of the component, a respective statement should be asked to substantiate this point.

It is recommended to request of the licensee a constant monitoring and report concerning the functioning of the critical component throughout all subsequent stages of the development, from the idea to the point of the implementation and further operational use.

2.4.5 Integrity

Integrity is defined as the trustworthiness of the system inputs and outputs, i.e. their freedom from errors in the output given correct input (fail-safe principle; absence of errors of commission) (i.e. the system will not translate the input in an unexpected unintended output).

Lack in integrity may result in unintended outcomes which are called errors of commission in safety assessments (i.e., the performance is in an unanticipated manner related to the input information). Errors of commission are difficult to model and hence usually not considered in analytical safety assessments. They might stem from all sorts of system elements like hardware, software, procedures, organisation or human reliability. Consequently, analytical risk assessments might underestimate the risk or not reveal the existence of the risk.

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authority could highlight the importance to address potential safety issues due to lack in integrity.	Errors of commission are usually not represented in analytical safety assessments and hence a review of a safety argument will probably not reveal the issues. The oversight authority should seek evidence of the fundamental being addressed.
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Errors of commissions might become an issue when the system is in operation; Monitoring activities and incident analyses should be verified as being put in place. Pre-implementation validation activities should be asked and reviewed when necessary to verify the proper functioning and the absence of errors of commission.

Detected inadequacies or ambiguities of the proposed Subject referring to the fundamental of integrity could pose a threat to safe operations. Threats due to lack of integrity occur usually in terms of errors of commission, which represent the undetected processing of faulty or incorrect input which affects the subsequent output of the system.

The oversight authority should request of the licensee to either eliminate or improve the components features which according to the results of the Safety Scanning exhibit an uncertain or inadequate integrity.

If the Safety scanning process reveals no issues of suspected or ascertained lack of integrity concerning the proposed Subject under discussion, a respective statement should be asked to substantiate this fact.

It is recommended to explicitly point at the time constraints (e.g. stage of component development in respect to time of scanning) of the component examination, as the fundamental of integrity is of primary significance for the safety architecture of the total system performance.

2.4.6 Maintainability

Maintainability is defined as the ability to maintain the system in working order throughout its life. This includes preventive maintainability, on-line maintenance, and reparability. From an oversight point of view it includes establishing which organisations and which persons have the responsibility of maintaining and, in of case of failure, returning the system to service. In ATM/ANS this is a prominent area of concern as ATM in general is often a continuous 24/7 activity. Because of this systems may be maintained, re-configured or repaired during real time operations. Loss and/or interruption of continuous service including the effect on operations (see also interdependencies) should be considered during the development.

An oversight authority should consider requiring the licensee to provide specific information concerning the maintenance process of the proposed Subject. The relevant information should leave no room for ambiguities concerning the responsibilities and the documentation at each development stage and for each modus of maintenance (i.e. preventive, on-line and corrective / reparative maintenance).

Suggested action for the oversight authority	Early Stages	Late Stages
What if impact	The oversight authority could issue a recommendation to address maintenance issues before any detailed review of safety performance.	In particular, latent failure analysis needs to be verified in the safety argument. Maintenance issues should preferably be tested or validated on their relevance and possible impact in the dry run of the system
What if no impact	The oversight authority should keep the issue in mind and ensure that the fundamental is consequently addressed in the further development (iterative use of SST).	Maintenance issues should be tested on absence in the dry run of the system.

Information concerning the compatibility of the maintenance requirements and procedures of a specific component with the performance of the overall system should be sought.

Ambiguity in description of the maintenance fundamental results in latent conditions, which could contribute to a partial or total performance breakdown. Therefore latent failure analysis should take place to complement the ongoing risk analysis of the component as a stand-alone system.

Existing or available regulation and legislation should be taken into account when available to examine the compliance and amendment requirements concerning the proposed Subject.

If no safety considerations for the fundamental of maintenance are defined by using the Safety scanning, a clear statement should be made to highlight this fact. It should be kept in mind that information concerning maintenance requirements and the detection process of the possible latent errors should be considered during the different development stages and the respective specific features of the component while it is being developed. A continuous review at each development stage is a necessary condition to ensure compliance with the maintenance fundamental throughout the whole life span of the component and the embedding system during and after implementation.

3. DISCUSSION

After a session in which a user uses the Safety Scanning Tool [SCAN TF 2010, SST], the output needs to be interpreted, analysed, consolidated and documented in a final report; this task is done by a Safety Analyst. The aim of the current document was to provide guidance for such Safety Analyst.

This document provided general recommendations for oversight activities flowing out of applications of the Safety Scanning Tool at various life-cycle stages. These recommendations are based on European law as well as best practices in safety.

It is suggested to implement this guidance in further versions of the Tool in order to create clear relationships between the Safety scanning results and the oversight activities that arise from the results. Such functionality of the Tool would ease the implementation of the recommended actions resulting in a safe introduction of changes to the ATM system.

4. REFERENCES

- E-OCVM (2007) European Operational Concept Validation Methodology (E-OCVM), Edition 2.0, 17 March 2007, http://www.eurocontrol.int/valfor/gallery/content/ public/E-OCVM_v2_Small.pdf
- SCAN TF (2010, SST questions) SCAN Task Force, Development of a Set of Questions for the Safety Scanning Tool, Edition 1.0, 11 March 2010, M.H.C. Everdij, H. Korteweg, J. Penny, O. Straeter, T. Longhurst.
- SCAN TF (2010, SST) SCAN Task Force, Safety Scanning Tool, Excel-based Tool, 11 March 2010, A. Burrage, O. Straeter, M.H.C. Everdij.
- SCAN TF (2010, SMRT) SCAN Task Force, Safety Methods Review Tool, Excel-based Tool, 11 March 2010, A. Burrage, M.H.C. Everdij.
- SCAN TF (2011, SMRT questions) SCAN Task Force, Development of a Set of Questions for the Safety Methods Review Tool, Edition 1.1, 11 April 2011, M.H.C. Everdij, O. Straeter, J.W. Nollet, H. Korteweg.
- SCAN TF (2011, multi actor) SCAN Task Force, Safety scanning as part of the oversight process, version 1.0, 26 May 2011, H. Korteweg, O. Straeter, J.W. Nollet, M.A. Kraan.
- SRC DOC 46 – Annex A, Safety Fundamentals – SCAN Task Force, Safety Fundamentals for Safety scanning.
- SRC DOC 46 – Annex B, moderating – SCAN Task Force, Guidance for moderating a Safety scanning event.
- SRC DOC – Annex D, regulatory advice – SCAN Task Force, Supporting Regulatory Tasks with Safety scanning.
- SRC DOC 48 – SCAN Task Force, Safety Method Review.
- SO/IEC 31010. Risk management – Risk assessment techniques. ISO. Geneve.

(***)