Study of safety validation needs and approaches implied by SESAR

Jelmer J. Scholte and Henk A.P. Blom

Air Transport Safety Institute,
National Aerospace Laboratory NLR
Amsterdam, the Netherlands
scholte@nlr.nl, blom@nlr.nl

Alberto Pasquini

Deep Blue
Rome, Italy
alberto.pasquini@dblue.it

Abstract—**For European ANSPs, safety validation of changes in their ATM system has become common practice. However, the SESAR program is planning changes in air traffic operations in Europe that go much further than changes to an individual ANSP's ATM system. This paper identifies the issues on which safety validation approaches need extensions, in order to move from safety validation of changes to an ANSP's ATM system to safety validation in SESAR. Subsequently, it identifies approaches that address the identified extension needs. This way an integrated view is developed from the fragmented research results in this area.**

Keywords-Safety validation, ATM, SESAR.

I. INTRODUCTION

For European ANSPs, safety validation of changes in their ATM system has become common practice. As part of this, they are required by applicable safety regulations (EUROCONTROL's ESARR 4 [22] and its transposition in European Commission (EC) regulations [19]) to hand over a completed safety assessment for regulatory approval before introduction of the change. Several safety assessment methods have been submitted to EUROCONTROL's Safety Regulation Commission (SRC) as proposed means of compliance to ESARR 4, but full compliance has not yet been concluded [23]. Moreover, for future changes in ATM, it is highly questionable whether assuring compliance to ESARR 4 requirements is cost-effective for SESAR. For example, both current ESARR and current ICAO regulations adopt a conservative approach regarding airborne safety nets: both assume that safety risk reduction by airborne safety nets is taken into account neither in the safety target nor in the safety risk assessment. The consequence of this is that improvements in airborne safety nets and in collaboration between airborne and ground based safety nets are discouraged [4].

The Single European Sky ATM Research (SESAR) program is planning changes in air traffic operations in Europe that go much further than changes to an individual ANSP's ATM system. SESAR concepts of operations include changes for a multitude of stakeholders including many ANSPs, airlines and airports. The safety of such operations does not only depend on these stakeholders' individual performance, but also on their interactions. In addition, SESAR strives for ambitious objectives addressing almost contradictory Key Performance Areas (KPAs). The changes to be made are fundamental, increasing even more the importance of addressing safety validation since the concept development start. In the early design phases changes to concepts are still relatively easy to make, which makes the provision of feedback to designers the focus of safety validation. Only when the concept of operation matures, the focus of safety validation shifts to derivation of safety requirements and finally confirmation that the concept as developed is indeed safe.

In this paper issues are identified on which safety validation approaches need extensions, in order to move from safety validation of an ANSP's change to safety validation in SESAR. Subsequently, it is identified which approaches are available to address these extension needs. Although these kinds of questions are being addressed by several researchers inside and outside SESAR, a drawback is that this research is documented in a very fragmented way, which makes it impossible to grasp a complete picture. The aim of this paper is to review these fragmented sources and to provide an integrated view.

The paper is organized as follows. Section II lists relevant SRC and SESAR studies regarding safety validation needs. Section III discusses safety validation needs that are identified from the SESAR sources. These needs concern two categories: needs regarding organizing safety validation and needs regarding safety assessment. In Sections IV and V approaches are identified that aim to address these two categories of needs. Section VI provides concluding remarks.

II. RELEVANT SRC AND SESAR STUDIES REGARDING SAFETY VALIDATION NEEDS

EUROCONTROL SRC [23] evaluated the following methods on compliance to the ESARR 4 requirements [22] for safety assessment of a change to an ANSP's ATM system:

- Two versions ([16], [17]) of EATMP[1] Safety Assessment Methodology (SAM);

- An early version [33] of LVNL[2] safety criteria;

- EUROCAE[3] ED78a [20]; and

- DFS[4] safety assessment methodology ([13], [14]).

For each of these methods partial compliance was concluded and needs of extension were identified.

[1] European Air Traffic Management Programme
[2] Luchtverkeersleiding Nederland
[3] European Organisation for Civil Aviation Equipment
[4] Deutsche Flugsicherung

The question of which safety validation needs emerge for advanced ATM developments has been addressed by a large variety of studies conducted by SESAR. In order to get an overview, several task deliverables ([42] – [51]) from the SESAR Definition Phase (2004-2008) have been reviewed, each of which studies a specific aspect of importance for safety validation in SESAR. [42] provides an overview of the current ATM safety regulatory framework in Europe. [43] summarizes the basic principles of safety regulation, and presents a vision for the future of ATM safety regulation in which issues identified for the current arrangements are addressed. [44] investigates the elements of the SESAR concepts with respect to the impact on and feasibility for safety regulation, and the impact of regulations on the concept elements. [45] studies the impact of SESAR concepts and procedures on safety regulations, including compliance and synchronization with ICAO. [46] describes regulatory and legislative planning including roadmaps for SESAR's 'transversal areas'; these contribute to ensuring that all operational improvements will comply with appropriate safety, security, environment, human performance and contingency requirements and objectives. [47] defines a concept validation methodology that aims to address the complexity of the SESAR concepts. [48] studies the development strategy, including details on aim, content and deliverables in terms of the maturity of the concepts. [49] provides a safety management plan. It aims for an integrated approach to safety related activities, and for establishing an aligned vision for the future of ATM safety that will meet the needs of all stakeholders, now and in the future. [50] describes the system engineering methodology that aims to support SESAR's technical definition in line with the development strategy of [48]. And finally, [51] defines a master plan for management structures and processes.

III. SAFETY VALIDATION NEEDS IDENTIFIED FROM SESAR SOURCES

This section presents safety validation needs that are identified from the SESAR sources presented in Section II. Table I provides an overview, distinguishing needs regarding organizing safety validation and needs regarding safety assessment.

TABLE I. OVERVIEW OF SAFETY VALIDATION NEEDS AND THEIR SESAR SOURCES

Needs regarding organizing safety validation
• Addressing E-OCVM requirements [47]
• Managing relations of the safety case with other cases [46]
• Addressing the multi-stakeholder nature [44]
• Addressing future safety regulations [42]

Needs regarding safety assessment
• Producing a macro safety case [49]
• Addressing the success side [49]
• Covering performance of human operators [49]
• Identifying unknown emergent risks [49]
• Covering organizational safety [46]

A. Needs regarding organizing safety validation

Addressing E-OCVM requirements: [47] identifies the European Operational Concept Validation Methodology (E-OCVM, [18]) as the basis of SESAR's concept validation methodology. E-OCVM aims to provide a common structure to an iterative and incremental approach to operational concept validation. It consists of three aspects:

- A Concept Lifecycle Model that reflects the maturity of the concept under investigation (see Fig. 1);

- A Structured Planning Framework that guides planning validation activities; and

- A Case-Based Approach used for providing key stakeholders focused information in an easily understood format.
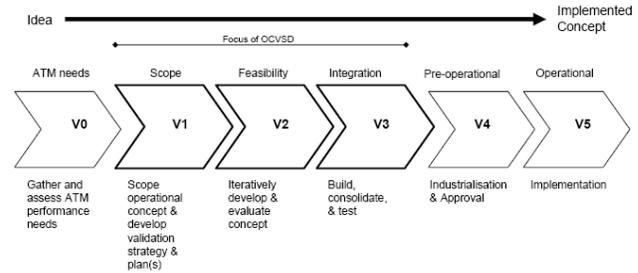

Figure 1. E-OCVM's Concept Lifecycle Model (from [18]).

Following E-OCVM, safety validation is done via the case-based approach. The handover by an ANSP of a completed safety assessment to a regulator as required by [22] and [19] effectively applies to phase V4 or V5 of E-OCVM's Concept Lifecycle Model. Implicitly, these are also the phases addressed by SRC in [23]. E-OCVM however poses specific requirements on the outputs of safety validation at the end of each of the Research and Development (R&D) phases (V0, V1, V2, and V3). Effectively, these specific requirements ask for:

- providing feedback to concept developers helpful to reduce the risks associated with new concepts, and

- structuring evidence into a presentable format that helps stakeholders identify the answers to their key questions.

Adherence to E-OCVM requirements aims to ensure that stakeholders can make a well-informed decision on further development of a concept, avoiding that the necessity of concept safety improvement is identified in a late stage of development, when modifications are extremely expensive.

Managing relations of the safety case with other cases: SESAR's regulatory and legislative planning document [46] identifies the need for an integrated management approach for all KPAs including safety. Management of performance during design phases is organized via E-OCVM's case-based approach, in which each case focuses on one performance aspect, e.g., safety, business, environment, or human factors.

Cases are usually managed by specialists in the domain investigated, with the human factors case being managed by human factor specialists, and the safety case by safety analysts. The different domains have different methods and techniques, usually at different levels of consolidation. The result of this partition of work can be a complete separation of the cases,

which can affect the efficacy and efficiency of development and validation. There is thus a need to manage relations of the safety case with other cases.

Example results of separation of cases include: 1) real-time simulations focusing on human factor aspects of a concept, without consideration for safety; 2) use of inconsistent assumptions in a safety case and another case, leading to incompatible results and difficulty in interpreting results by decision-makers regarding further concept development.

Addressing the multi-stakeholder nature: [44] identifies that the SESAR operational concept will fundamentally change the roles of many of the ATM stakeholders and, importantly, that these roles will change dynamically within the operation as a flight progresses. This will result in new safety responsibilities and new interfaces between stakeholders. Examples of such changes are in the fields of airspace organization & management, separation provision, and collision avoidance. Necessary precautions should be taken to ensure an appropriate approach towards safety for SESAR in its widest sense. This includes enabling safe implementation of SESAR concepts, minimizing project risks and related costs, and supporting decision-makers and investors in their requirements to provide information and the discharge of their explicit responsibilities and accountability towards safety in ATM. These conclusions of [44] emphasize the need to properly address the multi-stakeholder-nature of advancing air traffic operations.

An illustration of this need is the development of Continuous Descent Approaches [35] (CDAs). The safe execution of CDAs largely depends on the roles and collaboration of pilots and air traffic controllers (ATCos). Their joint behavior and performance thus needs to be well analyzed and captured in safety validation.

Addressing future safety regulations: Even though ATM safety regulations have contributed to the successful delivery of an acceptably safe ATM system across Europe so far, significant issues exist with respect to the current regulatory framework. The main issues that might impact safety of a future ATM system identified by [42] are in the field of:

- Solving the fragmentation and variability in regulations over different domains of air transport, and in the interpretation of regulations over European countries;

- Improving safety accountability: The complex safety regulatory framework and the often detailed and prescriptive nature of safety regulations easily result in confusion over safety accountability;

- Reducing duplication of regulations, as overlap and contradictions lead to confusion and difficulty;

- Reducing complexity of regulation, which otherwise leads to ambiguity regarding compliance; and

- Improving cost effectiveness: it should be clear how ATM safety regulation contributes to cost-effective management of safety.

From this, [42] concludes that developing the ATM safety regulatory framework will be essential to the success of SESAR, and that this improvement should aim to provide a clear, unambiguous set of regulations integrated with the safety regulation of the other parts of the air transport industry. In validation of a concept it should thus be realized that it will eventually need to be proven sufficiently safe according to the safety regulatory framework that will be in force at the time of regulatory approval and implementation of the concept.

B. Needs regarding safety assessment

Producing a macro safety case: SESAR's safety management plan [49] describes that safety assessments in aviation and ATM industry have often focused on individual concept elements, rather than on the joint effect on safety of multiple changes in air traffic operations. SESAR however is defining advanced developments to air traffic operations, consisting of multiple local changes by various stakeholders. The relations and interactions between such individual operational changes need to be properly assessed. [49] identifies the need for a macro safety case for this, which is to be accompanied by an approach in defining suitable safety targets at an appropriate level for the macro case.

Addressing the success side: Safety assessments in aviation and ATM industry have often focused on what happens if a new or changed system fails in some way, whereas the potential positive contribution of the change is often left unaddressed. Likewise, the positive contribution of SESAR to aviation safety should also be considered, instead of focusing on failures of ATM only. From these observations from SESAR's safety management plan [49] the need to address the success side of a change is identified.

Covering performance of human operators: In future concepts proposed by SESAR, human operators will maintain a central position in ATM. Therefore the safety of air traffic operations will remain dependent on the role of human operators. So far, many safety techniques have not comprehensively covered the role of human operators in the ATM system. [49] emphasizes this need to cover performance of human operators appropriately in safety assessments.

Identifying unknown emergent risks: In [49] it is explained that with the introduction of advanced SESAR concepts yet unknown emergent risk may appear: new behavior and hazards will emerge that have not yet been seen before. Identification of such emergent risk is crucial to be able to take it into account in safety assessment and feedback to design.

Covering organizational safety: SESAR's regulatory and legislative planning document [46] identifies the need for an integrated management approach for safety and other KPAs. The way in which such management system in the eventual operations will be organized can have significant consequences for safety; therefore organizational aspects need to be taken into consideration in safety assessment.

IV. APPROACHES ADDRESSING NEEDS REGARDING ORGANIZING SAFETY VALIDATION

This section presents available approaches for each need identified in Section III.A regarding organizing safety validation.

A. Addressing E-OCVM requirements

E-OCVM [18] poses specific, new requirements to safety assessment, which all boil down to optimal information provision for enabling effective and efficient development and validation processes. Only since recently it has been studied how to tailor safety assessment to the maturity of the concept, and how to satisfy the E-OCVM requirements for its R&D phases V0 through V3. Publicly available examples of E-OCVM compliant safety cases for advanced concepts in these R&D phases have not yet been identified. Example plans aiming for E-OCVM compliant safety case development for advanced concepts in these phases are available (e.g., [49] and [25]). Table II shows the [8] proposed safety validation activities per E-OCVM R&D phase.

TABLE II.   SAFETY VALIDATION ACTIVITIES PER PHASE OF E-OCVM [8]

R&D phase of E-OCVM	Safety validation activities
V0: ATM needs	Identification of ATM safety performance needs (e.g., safety targets), and support to the identification of ATM barriers that need to be alleviated to reach the ATM needs.
V1: Scope	Safety analysis to determine an appropriate validation strategy, and to provide safety feedback to the development process.
V2: Feasibility	Safety analysis to determine feasibility of the concept, and to provide safety feedback to the development process.
V3: Integration	Safety analysis to provide evidence for the safety of the further detailed concept, and to provide safety feedback to the development process.

B. Managing relations of the safety case with other cases

The risk of thinking for a safety case is that other validation aspects like human factors or business tend to become out of sight for the safety experts, and the other way around with experts of other cases. Moreover, concept designers do not have the luxury to optimize for each separate case. One design should accommodate all cases. Managing relations between cases in the design phases could improve the efficiency of the validation process and increase the synergies between the analyses done by different experts.

Here, only relations in the field of concept evaluation and validation are considered. Relations with the concept development process are explicitly not considered. Concept development is often a struggle to satisfy objectives in several or all KPAs, with the role of validation being primarily in evaluation of concepts. For example, around airports environment and safety are often in conflict. It could well occur that an approach or departure procedure is proposed is developed aiming for noise abatement, which could negatively impact the safety case. Such relations are not considered here, as decision-makers are primarily responsible for balancing different KPAs, and concept developers are primarily responsible for developing concepts in accordance with the objectives. The validation concerns the evaluation of the proposed concept regarding the KPAs.

As a result and follow-up of CAATS II, [8] proposes a framework for managing relations between cases, which is illustrated in Fig. 2. The framework distinguishes relations between case teams, the case generation processes, the cases themselves, and the outputs. Example relations are: 1) different cases provide complementary but coherent outputs; and 2) different cases use the same validation exercises where possible (e.g., simulations or operational trials).
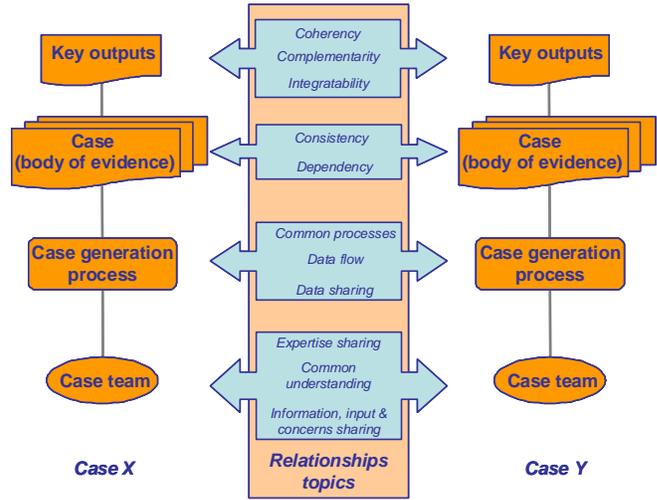

Figure 2.   Framework for relations between cases

More specifically, the human factors case and the safety case clearly relate. There is a clear overlap of activities to be conducted in these two cases. However the experience in handling this overlap effectively is rather under-developed.

With the environment case, no clear overlap or input-output relations of the safety case are identified. A scoping issue is which of these two cases should cover third party risk.

Finally, the business case integrates the results from all other cases, including the safety case. Safety gains or losses that may be caused by the introduction of a new concept must be taken into account in the business case. Models for assessing the economic value of safety gains or losses caused by the introduction of a new concept are emerging. Furthermore, the eventual cost of a new concept depends on the identification of unsafe elements in the safety case, as these unsafe elements potentially need mitigations or redevelopment, which are costly in time or budget.

C. Addressing the multi-stakeholder nature

As advanced concepts will fundamentally change the roles of many of the stakeholders in the ATM system and these roles will change dynamically within the operation as a flight progresses, the multi-stakeholder nature of advancing air traffic operations needs to be addressed.

[25] presents a safety validation framework, which has been developed to incorporate active stakeholder roles during the development and validation of a major change in air transport operations. In its detailed alignment with E-OCVM, the focus during the R&D phases V0 to V3 is on the macro level of institutional conditions, i.e., the interactions between stakeholders' organizations and operational control. Key issue is that during R&D the stakeholders should jointly adopt a

goal-oriented approach. This is put in practice via iteration of four processes, in which joint goals are set (set goals), concepts of operations are developed to reach these goals (plan), the consequences for the stakeholders are identified (act), and the concepts are jointly validated (joint safety validation). This is illustrated in Fig. 3. The joint safety validation should ensure that emergent behavior from interactions between the stakeholders is properly addressed.
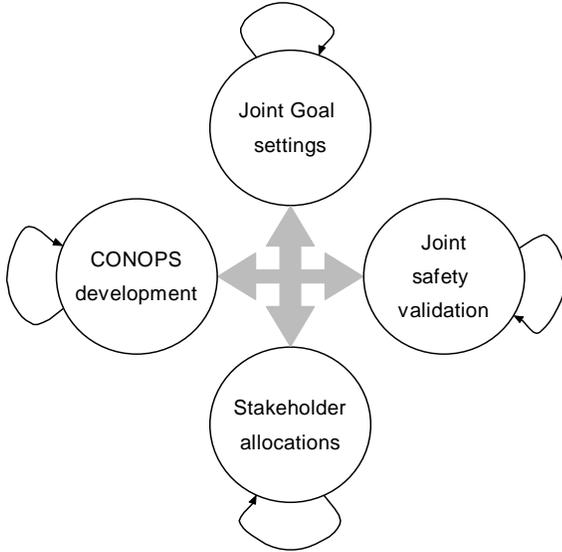

Figure 3. Main processes for active stakeholder involvement in the safety validation framework [25]

D. Addressing future safety regulations

As explained in Section III, significant issues exist with respect to the current regulatory framework, whereas the future regulatory framework needs to be addressed in safety validation. Two complementary approaches are identified for this, which are explained in the following.

Safety fundamentals [53] form a framework of basic safety rules that are independent from the implementation of a design. The main aspects of safety considered in this framework are safety regulation, safety management, operational safety and safety performance. Specific methods are developed to pro-actively consider operational concepts regarding these aspects early in their development lifecycle. Amongst others, this potentially leads to the identification of needed or anticipated changes in safety regulations, such that these can be properly addressed in concept development and validation. The Safety Screening method [52] has been used for the application of safety fundamentals to early SESAR concepts [44]. Safety Scanning [24] is developed in form of a safety fundamental tool by EUROCONTROL SRC to support National Supervisory Authorities in safety regulatory reviews.

[4] has shown that current ATM works with a very large number of minimum separation criteria. The RESET project [40] has verified that in order to accommodate a factor 2 increase in traffic demand over Europe, several of these minimum separation criteria are in need of a significant reduction. Since this cannot be accomplished without conducting a solid safety validation, the aim of RESET is to start the organization of a proper safety validation process for this. Impact assessment of changing minimum separation regulation will make part of this safety validation process.

V. APPROACHES ADDRESSING NEEDS REGARDING SAFETY ASSESSMENT

This section presents available approaches for each need identified in Section III.B regarding safety assessment. Table III provides an overview of the identified approaches per safety assessment need.

TABLE III. OVERVIEW OF IDENTIFIED APPROACHES PER SESAR SAFETY ASSESSMENT NEED

SESAR safety assessment need	Identified approaches
Producing a macro safety case	IRP [39] LVNL safety criteria [57] TOPAZ [5]
Addressing the success side	System engineering approach [26] TOPAZ [5]
Covering performance of human operators	Air-Midas [9] CARA [28] Human Assurance Levels [34] Human Factors Case [21] TOPAZ [5]
Identifying unknown emergent risks	Hazard brainstorming [11] Real-time simulations [1] Systemic Modeling [56]
Covering organizational safety	Organizational safety modeling [55] Resilience engineering [30] Scanning on safety fundamentals [53]

A. Approaches towards producing a macro safety case

The need for a macro safety case has a dual character: on the one hand interactions between different operational improvements need to be analyzed on safety, on the other hand suitable safety targets need to be defined for parts of the novel operation. Three approaches ([39], [57], [5]) are identified towards this.

[39] introduces the Integrated Risk Picture (IRP) which aims to integrate safety assessments for individual operational changes, covering their functional interactions and common causes. This provides a top-down approach considering the ATM system as a whole, complementing a bottom-up approach to assess risks associated to hazards affected or newly generated by the introduction of each individual operational change. A 'baseline' (IRP 2005) and a future risk picture version ('predicted IRP') have been developed. The predicted version models the safety impacts of all known ATM changes, in order to provide an indication whether safety targets can be achieved and to apportion an overall safety target based on the overall ATM contribution to aviation accident risks. The modeled performance of individual ATM elements is used as safety objectives for safety assessments for individual operational changes. The use of IRP is complemented by a 'Safety Targets Achievement Roadmap' [58] to interpolate between the baseline and the eventually foreseen situation, taking into account traffic growth and foreseen implementation planning. [26] proposes the use of predicted IRP for SESAR.

[57] presents LVNL safety criteria that are based on accident rates. The focus is on Air Traffic Control (ATC) - related accidents, being all accidents that ATC should prevent. This way, all accidents related to separation provision are considered, irrespective of which stakeholder (e.g., ANSP, airline) has causal contributions to the risk. An overall safety target for ATC-related accidents is apportioned into safety targets on the level of so-called ATC sub-products, which are comparable to parts of a flight forming a logical element within an ATC service or unit (e.g., 'taxiing', and 'line-up'). [57] proposes that individual safety assessments consider one or more operational improvements and connect this at the level of the ATC sub-products.

[5] presents the TOPAZ methodology for safety analysis of advanced air traffic operations. It addresses jointly all types of safety issues, including organizational, environmental, human-related and other hazards, and any of their combinations. Notably, it also considers all stakeholders relevant to the operation in an integrated way, enabling to cover well interactions such as between pilots and ATCos. It makes use of safety relevant scenarios that model the combinatorially many possible interactions between hazards and elements under control by different stakeholders. It features development and subsequent use of a Monte Carlo simulation tool set for selected parts of advanced operations. For other parts and other design options, possibilities are to adopt a qualitative approach, to use sensitivity analysis of the simulations of selected parts, to rerun simulations with adapted parameter settings, and to perform an advanced bias and uncertainty assessment.

B. Approaches in addressing the success side

Whereas safety assessments in aviation and ATM industry have often focused on failures of new systems, there is a need to address the success side of the change. Two approaches ([26], [5]) are identified for this.

[26] presents a system engineering approach to assessing safety. This approach extends upon EATMP SAM [17] by adopting the 'broader approach to safety assessment' of [27], which consists of complementary success and failure approaches:

- The success approach seeks to show that an ATM system will be acceptably safe in absence of failure;

- The failure approach seeks to show that an ATM system will still be acceptably safe, taking into account the possibility of (infrequent) failure.

This broader approach aims to translate future safety targets that apply to aircraft flights under the operational environment properties of SESAR 2020, to a high level specification of ATM services and their safety objectives. To accomplish this, the broader approach makes use of the predicted IRP [39].

Since its development, the safety assessment methodology TOPAZ [5] has considered success and failure in an integrated way. Hence, it forms a proven approach to covering both the success and failure side of a change. The method uses safety relevant scenarios in which it is modeled how the resolution of hazardous situations depends on the performance of multiple elements, acknowledging that performance variability goes further than the occurrence of failures, and that this plays an important role in safety.

C. Approaches in covering performance of human operators

As safety of air traffic operations will remain dependent on human operators, there is a need to cover their performance appropriately in safety assessments. Five approaches ([9], [28], [34], [21], [5]) are identified for ATM.

Air Man-machine Integration Design and Analysis System (Air-Midas) [9] is an approach in predictive modeling of human operator performance (flight crew and ATC) to evaluate the impact of automation developments in flight management and ATC.

Controller Action Reliability Assessment (CARA) [28] is a human reliability assessment technique, which can be used to quantify human reliability aspects as failure rates and success of mitigation actions in ATM.

[34] explores the use of Human Assurance Levels (HALs), which aim to ensure an appropriate level of Human Factors consideration/ integration in the system design and working practices commensurate with the risk for a particular system function relying on human performance. These HALs are then used at the leaves of fault/ event trees.

EUROCONTROL's Human Factors Case [21] is a process to systematically manage the identification and treatment of Human Factor issues early in a concept's lifecycle. In the CAATS II project [7], this Human Factors Case has been formalized for use in R&D in line with E-OCVM. Practices for managing relations between a safety case and a Human Factors case during R&D have already been discussed in Section IV.B.

TOPAZ [5] approach includes a systematic way of incorporating human performance modeling and simulation for ATCos and pilots (e.g., [3]). In [54] this has been extended with a systematic way of modeling the propagation of multi-agent situation awareness differences. In [2] it is explained that while Air-MIDAS is more detailed regarding ATCo and pilot performance, TOPAZ focuses on ATCo and pilot performance impact on accident risk. [10] shows that integration of the two approaches may be of complementary value for both.

D. Approaches in identifying unknown emergent risks

With the introduction of advanced concepts as aimed for by SESAR, unknown emergent risk may appear. Such risk is related to 'emergent behavior' which is characterized by what the interaction between multiple local behaviors (both nominal and non-nominal) yields more than the sum of the local behaviors. Three approaches ([11], [1], [56]) are identified.

Hazard brainstorming approaches with experienced pilots and ATCos can be used for identification of emergent risk. HAZOP (Hazard and Operability study, e.g., [31]) is used for identifying, analyzing and mitigating hazards in sessions with operational experts. [11] presents a brainstorming approach in which hazard identification is kept separate from hazard analysis and risk mitigation, using a focus on the identification of hazards that are functionally unimaginable. [12] shows that this can drastically increase the effectiveness of HAZOP.

Real-time simulations (e.g., using SAFSIM [1]) may be used for identification of emergent risk, including risk related to the emerging dynamics and interactions of the various elements in foreseen air transport operations. Also, identification of risk via expert elicitation can be improved by having operational experts take part in real-time simulations [38]. Inserting non-nominal events in the simulations can enable the identification of further related emergent behavior. Real-time simulations can vary in scale, and regularly serve multiple validation objectives simultaneously.

Recently, there has been a considerable impetus in safety science by approaches for risk assessment by systemic accident models ([29], [30], [32]). Systemic accident models describe the performance of a system as a whole, rather than on the level of events that may go wrong and related cause-effect mechanisms, such as in e.g. fault and event trees. The systemic approach considers accidents as emergent phenomena from the variability in the performance of interacting entities in an organization. In literature there are four systemic safety risk models for application to ATM: STAMP [32], FRAM [30], IRP [39] and TOPAZ [56]. Large scale Monte Carlo simulation of a systemic model, developed with the latter approach, allows filtration of emergent risks from the huge number of less relevant ones. For an active runway crossing operation, [6] compares a safety assessment using large scale Monte Carlo simulation with a systemic model versus an event sequence based safety assessment. This showed a significant difference in results due to explicit modeling of the dynamics of the operation, and the concurrent and interacting behaviors of pilots and controllers, which leads to emergent behavior that was neither identified through brainstorming nor through the event sequence based approach [6].

E. Approaches in covering organizational safety

The way in which future ATM will be organized can have significant consequences for safety. Therefore, organizational aspects need to be taken into account in safety assessment. Three approaches ([55], [30], [53]) are identified.

Organizational safety modeling for ATM is being studied in [55], and goes one step further than modeling humans and interactions between multiple humans, in the sense that groups of humans and interactions within and between groups are also considered. In [55], this is done through combined agent- and role-based modeling. The evaluation formalisms used include Bayesian Belief Nets and Monte Carlo simulations.

Resilience engineering [30] acknowledges that safety does not only depend on risk related to breakdown or malfunction, but also on the ability of a system to adjust to current conditions, which continuously change due to the complexity of air traffic operations. Resilience is often reached via a human cognition contribution, e.g., via coordination in unforeseen hazardous situations. Resilience can however also be reached via technological means (e.g., [15]) that help the human in detecting and recovering from latent conditions that undermine the effectiveness of human operators. An example is a tool that helps the operator in detecting hazardous situations resulting from differences in situation awareness.

In Section IV.D scanning on safety fundamentals [53] was discussed as a means towards addressing safety regulations. Other main aspects of safety considered in this framework are safety management, operational safety and safety performance. Consequently, scanning on safety fundamentals (e.g., using [52] or [24]) can be used to pro-actively identify safety management aspects and other organizational aspects of importance for safety.

VI. CONCLUDING REMARKS

This study has shown that several SESAR-identified safety validation needs exist beyond those of ANSPs. These needs appear to be of two categories:

- Needs regarding organizing safety validation, and
- Needs regarding safety assessment.

For each of the identified safety validation needs, relevant approaches have been described. For the needs regarding organizing safety validation, promising approaches are in an early phase of application. For the needs regarding safety assessment, there are multiple approaches (see Table III), of which some have proven to work, and some are new. It is recommended to gain experiences with the novel approaches, and to study the complementarity and integration of different approaches in order to combine their strengths.

The expectation is that most of the needs and approaches discussed in this paper also apply to NextGen. Although significant differences exist regarding ATM organization, gaining experience will improve from collaboration between SESAR and NextGen in safety validation.

REFERENCES

[1] Antonini, A, and Y. Kermarquer, SAFSIM, simulation for safety insights, EUROCONTROL, 2004.

[2] Blom H.A.P., K.M. Corker, and S.H. Stroeve, Study on the integration of human performance and accident risk assessment models: Air-MIDAS & TOPAZ. Proc. 6th USA/Europe ATM R&D Seminar, Baltimore, USA, (http://www.atmseminar.org/past-seminars/6th-seminar-baltimore-md-usa-june-2005/papers/paper_098), 2005.

[3] Blom, H.A.P., J. Daams and H.B. Nijhuis, Human cognition modelling in Air Traffic Management safety assessment, In: Air Transportation Systems Engineering, edited by G.L. Donohue and A.G. Zellweger, Vol. 193 in Progress in Astronautics and Aeronautics, Paul Zarchan, Editor-in-Chief, Chapter 30, pp. 481-511, 2001.

[4] Blom, H.A.P., M.H.C. Everdij, B.A. van Doorn, D. Bush, and K. Slater, Existing safety assessment methods versus Requirements, RESET D6.1, http://reset.aena.es/servlet/document.listPublic# , 2008.

[5] Blom, H.A.P., S.H. Stroeve, and H.H. de Jong, Safety Risk Assessment by Monte Carlo Simulation of Complex Safety Critical Operations, Eds: F. Redmill and F. Anderson, Proc. 14th Safety critical Systems Symposium, Bristol, UK, February 2006, Springer.

[6] Blom, H.A.P., S.H. Stroeve, J.J. Scholte, and H.H. de Jong, Accident risk analysis benchmarking Monte Carlo simulation versus event sequences. Proc. ICRAT, Fairfax, VA, June 1-4, 2008, pp. 177-184.

[7] CAATS II, D17: Guidance document for a typical human factors case, http://www.caats2.isdefe.es/servlet/document.listPublic, 2009.

[8] CAATS II, D28: Guide for a comprehensive incorporation of cases in ATM R&D projects, draft version 0.5, 06-11-2009.

[9] Corker, K.M., Cognitive Models & Control: Human & System Dynamics in Advanced Airspace Operations, Eds: N. Sarter and R. Amalberti, Cognitive Engineering in the Aviation Domain, Lawrence Earlbaum Associates, New Jersey, 2000.

[10] Corker, K.M., H.A.P. Blom, and S.H. Stroeve, Study on the integration of human performance and accident risk assessment models: Air-MIDAS and TOPAZ, Proc. Int. Seminar on Aviation Psychology, Oklahoma, USA, 18-21, April 2005.

[11] De Jong, H.H., Guidelines for the identification of hazards; How to make unimaginable hazards imaginable? NLR Contract report 2004-094 for EUROCONTROL (Part of [17]: FHA, Ch. 3, GM B.2), March 2004.

[12] De Jong, H.H., H.A.P. Blom and S.H. Stroeve, How to identify unimaginable hazards? In: Proc. 25th ISSC, Baltimore, Maryland, 2007.

[13] DFS, Safety Assessment Handbook Volume 1: Introduction to the Methodology, Version 1.02, dated 24 November 2003.

[14] DFS, VYK.01, Corporate Directive Safety Assessment, V1.0.1, 2003.

[15] Di Benedetto, M.D., A. D'Innocenzo, and A. Petriccone. Automatic Verification of Temporal Properties of Air Traffic Management Procedures Using Hybrid Systems. 7th EUROCONTROL Innovative Research Workshop & Exhibition. December 2-4, 2008.

[16] EATMP, Air Navigation System Safety Assessment Methodology (FHA), SAF.ET1.ST03.1000-MAN-01-00, Ed.1.0, April 2000.

[17] EATMP, Air Navigation System Safety Assessment Methodology (SAM), SAF.ET1.ST03.1000-MAN-01, Ed.2.0, 2004.

[18] EATMP, European Operational Concept Validation Methodology, v2.0, http://www.eurocontrol.int/valug/public/standard_page/OCVMSupport.html, 2007.

[19] EC, Commission Regulation No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services.

[20] EUROCAE, ED78A Guidelines for approval of the provision and use of ATS supported by data communications, December 2000.

[21] EUROCONTROL EATM The Human Factors Case: Guidance for Human Factors Integration, version 2.0, 29 June 2007

[22] EUROCONTROL Safety Regulatory Requirement (ESARR), ESARR 4, Risk assessment and mitigation in ATM, Edition 1.0, 5 April 2001.

[23] EUROCONTROL SRC, EAM 4 / AMC Acceptable means of compliance with ESARR 4, Edition 4.0, 26 October 2009.

[24] EUROCONTROL, ASRO, Safety fundamentals for safety scanning, Ed.1.0, 3 August 2009.

[25] Everdij, M.H.C., H.A.P. Blom, J.J. Scholte, J.W. Nollet and B. Kraan, Developing a framework for safety validation of multi-stakeholder changes in air transport operations, Safety Science, Elsevier, Vol. 47, pp. 405-420, March 2009.

[26] Fowler, D., E. Perrin, and R. Pierce, A systems-engineering approach to assessing the safety of the SESAR Operational Concept 2020 Foresight, 8th USA/Europe ATM R&D Seminar, 2009.

[27] Fowler, D., G. Le Galo, E. Perrin and S. Thomas, So it's reliable but is it safe?, Proc. 7th USA/Europe ATM R&D Seminar, Barcelona, July 2007, www.atmseminar.org/past-seminars/7th-seminar-barcelona-spain-july-2007/papers/paper_041.

[28] Gibson, W.H., and B. Kirwan, Application of the CARA HRA Tool to Air Traffic Management Safety Cases, EEC May 2008, http://www.eurocontrol.int/eec/gallery/content/public/document/eec/conference/paper/2008/002_Application_of_CARA.pdf.

[29] Hollnagel E., Barriers and accident prevention, Ashgate, Hampshire, UK, 2004.

[30] Hollnagel, E., D.D. Woods, and N. Leveson (Eds.), Resilience Engineering – Concepts and Precepts, Ashgate Publishing, 2006.

[31] Kletz, T., Hazop and Hazan; identifying and assessing process industry hazards, The Institution of Chemical Engineers, 4th ed., 1999.

[32] Leveson N., A new accident model for engineering safer systems, Safety Science 42:237-270, 2004.

[33] LVNL, D/R&D 03/018: LVNL Safety Criteria, V1.0, 25th April 2003.

[34] Mana, P., J.-M. De Rede, and D. Fowler, Assurance levels for ATM elements: Human (HAL), Operational Procedure (PAL), Software (SWAL), 2nd IET International Conference on System Safety 2007 (CP532), p.13–19 doi:10.1049/cp:20070434.

[35] McMillan, D., The continuous rise of continuous descents, In: International Airport Review, issue 6, 2009.

[36] Mosquera, D., & G. Cuevas, Separation Minima Standards: Research of Current Applicable Minima Laid Down and Foundations, ICRAT, 2008.

[37] Pasquini, A., and J.J. Scholte, CAATS II D13, Good practices for safety assessment in R&D projects, in 2 parts, v. 3.6, http://www.caats2.isdefe.es/servlet/document.listPublic, October 2009.

[38] Pasquini, A., S. Pozzi, and G. McAuley, Eliciting Information for Safety Assessment. Safety Science, Vol.46 (10), pp.1469–1482, Elsevier, 2008.

[39] Perrin, E., B. Kirwan, and R. Stroup, A systemic model of ATM safety: the Integrated Risk Picture, In: Proc. 7th USA/Europe ATM R&D Seminar, Barcelona, July 2007.

[40] RESET consortium, RESET website, http://reset.aena.es .

[41] Scholte, J.J., H.A.P. Blom, A. Pasquini, and B.A. van Doorn, CAATS II D14 "Guidance document for a typical safety case", v1.91, http://www.caats2.isdefe.es/servlet/document.listPublic, October 2009.

[42] SESAR Consortium, SESAR WP1.6.1/D1, Air Transport Framework The Current Situation, July 2006.

[43] SESAR Consortium, SESAR WP1.6.1/D2, Air Transport Framework The Performance Target, December 2006.

[44] SESAR Consortium, SESAR WP1.6.2/ D3,"Air Transport Framework The ATM Target Project, September 2007.

[45] SESAR Consortium, SESAR WP1.6.2/ D4, Study of Impact of New Concepts and Procedures on Safety Regulations, including Compliance and Synchronisation with ICAO Safety Standards, February 2008.

[46] SESAR Definition Phase, T3.4.6/D5 Regulatory - Legislative Planning, DLT-0710-346-00-05, version 0.05, May 2008.

[47] SESAR Definition Phase, Task 4.2.1/D6 Concept Validation Methodology, Part of DLT-0710-421-01-00, version 1.0, May 2008.

[48] SESAR Definition Phase, Task 4.2.1/D6 Development Strategy, Part of DLT-0710-421-01-00, version 1.0, May 2008.

[49] SESAR Definition Phase, Task 4.2.1/D6 Sesar Safety Management Plan, Part of DLT-0710-421-01-00, version 1.0, May 2008.

[50] SESAR Definition Phase, Task 4.2.1/D6 System Engineering Methodology, Part of DLT-0710-421-01-00, version 1.0, May 2008.

[51] SESAR Definition Phase, WP4.1.12/D5-D6 SESAR Definition Phase, DLT-0701-041-00-081, April 2008.

[52] Straeter, O., M. Everdij, J. Smeltink, J. Nollet, J. Kovarova, H. Korteweg, A. Burrage, Safety Screening – Experiences in applying a proactive approach to concept development within SESAR, Procs. EUROCONTROL Safety R&D Seminar, Rome, Italy, 24-26 Oct. 2007.

[53] Straeter, O., Managing Safety Proactively – Experiences on the Implementation of the Safety Agenda at EUROCONTROL, In: Proc. PSAM 8, New Orleans, Louisiana, USA, 2006.

[54] Stroeve S.H., H.A.P. Blom, and M.N.J. Van der Park. Multi-agent situation awareness error evolution in accident risk modeling. Proc. 5th USA/Europe ATM R&D Seminar, Budapest, Hungary, (http://www.atmseminar.org/past-seminars/5th-seminar-budapest-hungary-june-2003/papers/paper_067), 2003.

[55] Stroeve, S.H., A. Sharpanskykh, R.M. van Lambalgen, and B. Kirwan, Safety culture analysis by agent-based organizational modeling, In: Proc. 7th EUROCONTROL Innovative Research Workshop & Exhibition, 2008.

[56] Stroeve, S.H., H.A.P. Blom, and G.J. Bakker, Systemic accident risk assessment in air traffic by Monte Carlo simulation, Safety Science, Vol. 47 (2009), pp. 238-249 (http://dx.doi.org/10.1016/j.ssci.2008.04.003).

[57] Van den Bos, J.C., H.H. de Jong, and R.B.H.J. Jansen, Apportioned ATC Safety Criteria Based on Accident Rates, In: ATC Quarterly, vol.17 no.3, 2009.

[58] Vernon G., and E. Perrin, Methodology report for a Safety Target Achievement Roadmap (STAR), EUROCONTROL report, May 2007.