Project no.: FP6-2005-TREN-4-Aero- 036826

CAATS II

COOPERATIVE APPROACH TO AIR TRAFFIC SERVICES II

Instrument: CA – Coordination Action

Thematic Priority: AERO-2005-1.3.1.4h

D13: GOOD PRACTICES FOR SAFETY ASSESSMENT IN R&D PROJECTS

-

PART 1: MAIN DOCUMENT

Due date of deliverable: **06/05/2009** **Actual submission date:** **08/10/2009**

Start date of project: **06/11/2006** **Duration:** **36 months**

Organisation name of lead for this deliverable: **Deep Blue**

Revision: **Draft**

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Change Log				
Revision	**Edition Date**	**Author**	**Modified Sections / Pages**	**Comments**
0.1				Document developed starting as revision and update of document : CAATS Deliverable D1.4 Safety Report Volume II: Safety Assessment Methodologies (Mariken Everdij and Henk Blom)
3.5	08/10/2009	Alberto Pasquini (Deep Blue), Jelmer Scholte (NLR)	All	First public version

This project has been carried out under a contract awarded by the European Commission

Executive Summary

One of the objectives of the Safety Case work package of the CAATS II project is to gather and disseminate good practices on Safety Assessment Methodologies for Research and Development (R&D) projects, used by the aviation organisations in the ECAC area and to identify opportunities for improvement of those practices. The primary purpose is to support and co-ordinate processes and methodologies across FP7 and SESAR ATM projects, supported and sponsored by the EC, in relation to Safety.

This document represents a significant revision of [CAATS, D1.4 P2] deliverable of the former CAATS project on Safety assessment emerging good practices, named Safety Report – Volume II Safety Assessment Methodologies. The aim of the revision is to up-date the document with respect to recent developments and to focus on the applicability of the methods and techniques for safety assessment to R&D projects for advanced developments
such as aimed for by SESAR. From the many sources, it appears that for such applications several new needs emerge, and that traditional approaches fall short. The document provides:

- An analysis of the general steps of a safety assessment process;
- Identification of the main current practices for safety assessment in R&D projects;
- Identification of emerging approaches for safety assessment in ATM R&D projects;
- Identification of the main emerging needs for safety assessment in R&D of major changes such as aimed for by SESAR; and
- Identification of approaches that support addressing the SESAR-identified emerging needs.

Whereas for each emerging need approaches have been identified that support addressing it, it has not been evaluated to which extent the emerging needs are satisfied. Also, it has not been considered whether approaches address the complementary emerging needs that were identified by sources other than SESAR. Integration of emerging approaches with each other and with established approaches has been identified as the key area of safety research that deserves significant attention.

This document consists of two parts. This Part 1 is the main document. Part 2 provides an overview and analysis of the many recent developments since the delivery of [CAATS, D1.4 P2] three years ago.

This project has been carried out under a contract awarded by the European Commission

Document Information	
Document title	D13 CAATS II GOOD PRACTICES FOR SAFETY ASSESSMENT IN R&D PROJECTS
Version	V3.5
Date	08 October 2009
Classification	PU
Work package	WP1.2
Document identification	CII-WP1.2-DBL-D13.1-V3.5-DE-PU

Contact Information
Isdefe, Ingenieria de Sistemas para la Defensa de España, S.A.
Attn. Mr. Carlos Regidor Gil
Edison 4
28006 Madrid
Spain
Tel.: +34 91 271 14 95
Fax: +34 91 564 5108
E-mail: cregidor@isdefe.es

This project has been carried out under a contract awarded by the European Commission

Table of Contents

This project has been carried out under a contract awarded by the European Commission

List of Figures

List of Tables

This project has been carried out under a contract awarded by the European Commission

1. INTRODUCTION

1.1 Purpose

The approach for safety assessment is relatively well consolidated for an ANSP assessing a change to its Air Traffic Management (ATM) system, including humans, procedures, and technical equipment. Safety assessment in Research and Development (R&D) for advanced developments as aimed for by SESAR the situation has however been subject of a lot of recent research. From this research it appears that several new needs emerge, and that traditional approaches fall short. This document provides an analysis of this research, with the objective of providing an overview of:

- Approaches already considered as good practices for safety assessment in R&D projects;
- Newly emerging approaches for safety assessment in R&D projects;
- The needs that emerge for safety assessment in R&D projects for advanced developments such as aimed for by SESAR; and
- Identified (current and/ or emerging) approaches that aim to address the SESAR-identified emerging needs.

This way, the document aims to gather and disseminate practices and needs for safety assessment in R&D projects, considering also the possible different levels of maturity of the ATM concepts investigated by the R&D projects. The document aims to support and foster a standardisation of safety assessment processes and methodologies across sixth and seventh framework programme ATM projects, supported and sponsored by the European Commission (EC), and across SESAR projects.

1.2 Background

In its Sixth Framework Programme (FP6), the European Commission proposed a paradigm shift in the way air traffic services are provided. This shift is being pursued through research, to achieve collaborative decision-making for a complete air and airport environment, including innovative research to increase the efficiency of air transport service provision. The overall objective is to achieve the Single European Sky and Eurocontrol's ATM2000+ Strategy.

More specifically, the Commission proposed a cluster of seven research areas, ranging from airport efficiency to cooperative air traffic management (ATM). The projects that are implementing these research areas in FP6 are based on previous knowledge and, in turn produce new knowledge. The research proposed by the Commission combines human factors, safety and airport efficiency with harmonised validation methodologies, supported by business cases and safety assessments.

An ATM concept is a potential solution for a problem identified in the ATM system. The development of an ATM concept has a life cycle in which the concept undergoes a maturity process. In order to avoid unrealistic expectations being placed upon experimental teams there is a need to create a 'Validation Strategy and Plan at the level of Programme management'.

The CAATS project of the sixth Framework Programme identified the European Operational Concept Validation Methodology (E-OCVM) as the baseline methodology for concept validation [E-OCVM, 2007]. E-OCVM is most applicable to the first three phases proposed in the AP5 maturity model. The AP5 model, described in the Operational Concept Validation Strategy Document [OCVSD] developed by FAA/Eurocontrol, proposes a five level concept maturity scale: Idea, establish concept principles (V1), initial 'proof of concept', prototypes (V2), concept integration and pre-ops simulations (V3), industrialization/procedure approval (V4) and

This project has been carried out under a contract awarded by the European Commission

implementation of processes/procedures (V5). In this process the stakeholders play an important role: they make decisions about the progress of the concept, based on its maturity, beyond the world of ATM R&D. E-OCVM focuses on describing the type of information that should be expected from the validation process and how this information should be structured in order to ensure that it is accessible and understandable by all stakeholders.

The objective of the Cooperative Approach to Air Traffic Services II (CAATS II) coordination action is to continue the work begun within the CAATS project by managing, consolidating and disseminating the knowledge produced in European ATM-related projects. It focuses on five areas namely safety, human factors, business (cost/benefits), environment and validation. On the basis of the good practices the intention is to develop 'cases' that can be integrated in E-OCVM, to provide a coordinated approach to Validation, avoiding overlapping and gaps in R&D projects.

The general objective of CAATS II are being fulfilled through activities performed in three work packages, which will focus on project management and coordination, knowledge management and consolidation, and dissemination of the results of CAATS II respectively. The most significant expected output of CAATS II is the achievement of a coordinated, cooperative approach in European ATM research. Good practice manuals have been produced in the areas of safety, human factors, business, environment and validation for use not only by European Commission projects but also by other interested stakeholders, in particular EUROCONTROL. Furthermore, 'cases' are developed on basis of these manuals and integrated in E-OCVM

The current document is related to the safety domain, proposing a revision of the CAATS 'Good Practices for Safety Assessment' [CAATS, D1.4 P2], now with focus on safety assessment in R&D for advanced developments. The companion document CAATS II D14 [CAATS II, D14] provides guidance for safety case development in early E-OCVM phases.

1.3 Document Structure

This document is organised as follows:

- Section 1 gives an introduction to the document, including background information on the CAATS II project and on the other project deliverables considered in this document, a glossary, and references to input material.
- Section 2 presents a model of the typical safety assessment steps, called "generalised eight-stages safety assessment", and discusses its current application in R&D projects.
- Section 3 describes the methods that are currently used in R&D projects for safety assessment (i.e., SAM, ED78A, TOPAZ).
- Section 4 presents emerging approaches for safety assessment in ATM R&D projects have been identified, including a literature review of techniques
- Section 5 explains the purpose and way of working of safety assessment in the specific context of R&D projects, presenting briefly the concept maturity model of the European Operational Concept Validation Methodology.
- Section 6 presents an overview of identified additional needs that emerge for safety assessment in R&D for advanced developments such as aimed for by SESAR.
- Section 7 presents approaches that aim to address those emerging needs that have been identified by SESAR.

The document has several appendices, which are contained in Part 2 of this document. The first four appendices provide the analysis that supports the core of this document:

This project has been carried out under a contract awarded by the European Commission

- Appendix I contains a review of documents and projects to collect information on practices and emerging needs.
- Appendix II presents an analysis of the reviewed sources views on (safety) validation per phase of E-OCVM.
- Appendix III presents the collection and analysis of information on management of relations between E-OCVM's safety case and the other cases in E-OCVM.
- Appendix IV presents the collection and analysis of information on assessing the maturity of a concept.

The remaining appendices give an extensive introduction of some of the main emerging practices identified in Section 4 of this document:

- Appendix V introduces SAME and its proposed usage in SESAR;
- Appendix VI introduces Safety Fundamentals; and
- Appendix VII introduces SAFMAC.

1.4 Acronyms

ANSP	Air Navigation Service Provider
ASAS	Airborne Separation Assurance System
ASOR	Allocation of Safety Objectives and Requirements
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Services
CAATS	Co-operative Approach to Air Traffic Services
CCA	Common Cause Analysis
CNS	Communication, Navigation and Surveillance
EATM	European Air Traffic Management
EATMP	European Air Traffic Management Programme
EATMP SAM	EATMP Safety Assessment Methodology
EC	European Commission
ECAC	European Civil Aviation Conference ("Association" of Europe's CAAs)
ED78A	RTCA/EUROCAE ED78A DO-264
E-OCVM	European Operational Concepì Validation Methodology
ESARR 4	Eurocontrol Safety Regulatory Requirement 4 (Risk Ass. and Mitigation in ATM)
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FHA	Functional Hazard Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FP6	European Commission's Sixth framework programme
FTA	Fault Tree Analysis
G2G	Gate to Gate
GAIN	Global Aviation Information Network
HAZOP	Hazard and Operability study
HEART	Human Error Assessment and Reduction Technique
HERA	Human Error in ATM
HTA	Hierarchical Task Analysis
HTRR	Hazard Tracking and Risk Resolution
ICAO	International Civil Aviation Organisation
MFF	Mediterranean Free Flight

This project has been carried out under a contract awarded by the European Commission

NASA	National Aeronautics and Space Agency
OHA	Operational Hazard Analysis
OSED	Operational Services Environment Definition
PDARS	Performance Data Analysis and Reporting System
PSSA	Preliminary System Safety Assessment
R&D	Research and Development
RTCA	Radio Technical Commission for Aeronautics Inc.
SAFSIM	Safety in Simulations
SAM	Safety Assessment Methodology
SAME	Safety Assessment Made Easier
SES	Single European Sky
SESAR	Single European Sky ATM Research
SFMEA	Software Failure Modes and Effects Analysis
SKE	Safety Key Element
SMHA	State Machine Hazard Analysis
SRC	Safety Regulation Commission
TCAS	Traffic alert and Collision Avoidance System
TOPAZ	Traffic Organization and Perturbation AnalyZer
TRACEr	Predictive Technique for the Analysis of Cognitive Errors
WP	Work Package

1.5 Reference Documents

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[Ale et al., 2006]	Ale B.J.M., Bellamy L.J., Cooke R.M. (3), Goossens L.H.J., Hale A.R., Roelen A.L.C.& Smith E.; Towards a causal model for air transport safety : an ongoing research project, In Safety Science ISSN 0925-7535 vol. 44, no8, pp. 657-673, 2006
[AP15]	FAA/Eurocontrol, ATM Safety Techniques and Toolbox, Safety Action Plan-15, Issue 1.1: For Comment, February 10, 2005. http://www.eurocontrol.int/eec/gallery/content/public/documents/EEC_safety_documents/Safety_Techniques_and_Toolbox_1.0.pdf
[Bishop, 1990]	P. G. Bishop (editor), Dependability of critical computer systems – Part 2: Techniques Directory, Elsevier, London, 1990.
[Blom et al. 2003a]	H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij and M.N.J. van der Park, Human cognition performance model to evaluate safe spacing in air traffic, Human Factors and Aerospace Safety, Vol. 3 (2003), pp. 59-82.
[Blom et al. 2003b]	H.A.P. Blom, M.B. Klompstra and G.J. Bakker, Accident risk assessment of simultaneous converging instrument approaches, Air Traffic Control Quarterly, Vol. 11 (2003), pp. 123-155.
[Blom et al., 1999]	Blom, H.A.P., M.H.C. Everdij and J. Daams, ARIBA (ATM system safety criticality Raises Issues in Balancing Actors responsibility) WP6 Final Report Part II Safety Cases for a new ATM operation, http://www.aribaproject.org, 1999

This project has been carried out under a contract awarded by the European Commission

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[Blom et al., 2001]	Blom HAP, Daams J, Nijhuis HB. Human cognition modelling in air traffic management safety assessment. In: Donohue GL and Zellweger AG (eds.), Air Transport Systems Engineering, AIAA, pp. 481-511, 2001.
[Blom et al., 2005]	Blom HAP, Corker KM, Stroeve SH. Study on the integration of human performance and accident risk assessment models: Air-MIDAS & TOPAZ. Proceedings 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
[Blom et al., 2006a]	H.A.P. Blom, S.H. Stroeve, H.H. de Jong, Safety Risk Assessment by Monte Carlo Simulation of Complex Safety Critical Operations, Eds: F. Redmill & F. Anderson, Proc. 14th Safety critical Systems Symposium, Bristol, UK, February 2006, Springer
[Blom et al., 2006b]	Blom, H.A.P. and Krystul, J. and Bakker, G.J. (2006) Free Flight Collision Risk Estimation by Sequential MC Simulation. In: Stochastic Hybrid Systems. Automation and Control Engineering Series 24. Taylor & Francis CRC Press, pp. 247-279. ISBN 0849390834
[Bush & Finkelstein, 2001]	D. Bush, & A. Finkelstein, Reuse of Safety Case Claims – An Initial Investigation, Proceedings of the London Communications Symposium, London, 2001.
[Bush, 2001]	D. Bush, Towards Formalising Reuse in Safety Cases, Proceedings of the INCOSE UK Spring Symposium, Tolleshunt Knights, Essex, Apr 2002.
[CAATS II WP1.2 TC]	Marga Martín Sanchez, Safety Criteria for Transitions between R&D Phases, CAATS II WP1.2, draft version 0.1, May 2009.
[CAATS II WP1.6 note]	John Harrison, Relationship between Cases, CII-WP1.6-ISD-051-V0.1-TW-CO, September 2008.
[CAATS II WS2]	M. Koolloos, Proceedings 2nd CAATS II workshop “how do we know we are building the right ATM system? – Applying a case based approach to assess performance” CII-WP2-ISD-045-V1.0-DE-PU, version 1.0, 18 November 2008.
[CAATS II, D11]	CAATS Consortium, “Common Approach to Teams”, Deliverable D11, Feb. 2008.
[CAATS II, D14]	J.J. Scholte et al., “Guidance for safety activities in operational concept validation”, CAATS II Deliverable D14, version 1.9, October 2009.
[CAATS II, D17]	CAATS Consortium, “Guidance document for a typical HUMAN FACTORS case”, CAATS II Deliverable D17, May 2009.
[CAATS II, D28]	CAATS Consortium, “Guide to a comprehensive incorporation of environmental, cost-benefit,, safety and human factors cases in the validation of ATM R&D projects”, CAATS II Deliverable D28, Jun. 2009.
[CAATS, D1.4 P2]	M.H.C. Everdij, H.A.P. Blom, Safety assessment methodologies, CAATS Deliverable D1.4 safety report, Part 2, 2006.

This project has been carried out under a contract awarded by the European Commission

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[CAATS, D1.4]	R.B.H.J. Jansen, CAATS Good practices and needs for improvement for safety key elements in Air Traffic Management, Final version, April 2006.
[Corker, 2000]	Corker, K. (2000), 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.
[De Jong et al,. 2007]	H.H. de Jong, H.A.P. Blom & S.H. Stroeve, How to identify unimaginable hazards? In: Proc. of the 25th ISSC, Baltimore, Maryland, August 13-17, 2007.
[De Jong, 2004]	H.H. de Jong, Guidelines for the identification of hazards; How to make unimaginable hazards imaginable? NLR Contract report 2004-094 for EUROCONTROL, March 2004, included in [EATMP SAM, 2007]: FHA, Ch. 3, GM B.2.
[Di Benedetto et al., 2008]	M.D. Di Benedetto, A. D'Innocenzo, 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. EUROCONTROL Experimental Centre, Paris , France .
[DOE, 2003]	U.S. Department of Energy, Lessons Learned Writing Tips, Sept. 2003, www.au.af.mil/au/awc/awcgate/lessons/sells/writips.pdf
[Dorbes et al., 2001]	A Dorbes, M Geissel, A Jackson, Integrating multiple viewpoints in the coherent design of advanced controller working positions, Digital Avionics Systems, 2001.
[EAM 4, 2004]	Eurocontrol SRC, EAM 4 / AMC Acceptable means of compliance with ESARR 4, Edition 3.0, 10 August 2004.
[EATM HF case, 2007]	Eurocontrol EATM The Human Factors Case: Guidance for Human Factors Integration, version 2.0, 29 June 2007
[EATMP SAM, 2007]	Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, Edition 2.2, 2007.
[ED78A, 2000]	ED78A/DO264 -"Guidelines for approval of the provision and use of Air Traffic Services supported by data communications" EUROCAE, December 2000. (This document is identical to the US equivalent RTCA DO-264)
[EN 50128]	CENELEC (Comité Européen de Normalisation Electrotecnique), European standard Pr EN 50128: Railway applications, Software for railway control and protection systems, January 1996; From the internet: Annex B: Bibliography of techniques, http://www.dsi.unifi.it/~fantechi/INFIND/50128a2.ps
[E-OCVM, 2007]	European Operational Concept Validation Methodology, http://www.eurocontrol.int/valug/public/standard_page/OCVMSupport.html
[ESARR 4]	Eurocontrol Safety Regulatory Requirement (ESARR), ESARR 4, Risk assessment and mitigation in ATM, Edition 1.0, 5 April 2001, http://www.eurocontrol.be/src/index.html (SRC publications – ESARR related).

This project has been carried out under a contract awarded by the European Commission

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[Everdij & Blom, 2007]	Everdij, M.H.C., Blom, H.A.P., 2007. Study of the quality of safety assessment methodology in air transport. In: Ann G. Boyer, Norman J. Gauthier (Eds.), Proceedings of the 25th International System Safety Conference, Engineering a Safer World, Hosted by the System Safety Society, Baltimore, Maryland USA, 13-17 August 2007, pp. 25-35.
[Everdij & Blom, 2008]	M.H.C. Everdij and H.A.P. Blom, Enhancing hybrid state Petri nets with the analysis power of stochastic hybrid processes, Proceedings 9th International Workshop on Discrete Event Systems (WODES), Göteborg, Sweden, May 2008, pp. 400-405.
[Everdij et al., 2006a]	Everdij, M.H.C., Blom, H.A.P., Nollet, J.W., Kraan, M.A., Need for novel approach in aviation safety validation. In: 2nd Eurocontrol Safety R&D Seminar Barcelona, Spain, October 2006.
[Everdij et al., 2006b]	M.H.C. Everdij, H.A.P. Blom and S.H. Stroeve, Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk, Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8), New Orleans, Louisiana, USA, May 2006.
[Everdij et al., 2006c]	M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom and B. Klein Obbink, Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets, In: H.A.P. Blom and J. Lygeros, editors, Stochastic hybrid systems: theory and safety critical applications, volume 337 of Lectures notes in control and information sciences (LNCIS), pages 325-350. Springer, 2006
[Everdij et al., 2007]	M.H.C. Everdij, H.A.P. Blom, and G.J. Bakker, Modelling lateral spacing and separation for airborne separation assurance using Petri nets, In: Transactions of The Society for Modeling and Simulation International, Volume 83, Number 5, May 2007, pp. 401-414.
[Everdij et al., 2009]	M.H.C. Everdij, 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
[FAA AC431, 2005]	FAA Advisory Circular 431-35.2, Reusable launch and reentry vehicle System Safety Process, July 2005, http://www.skybrary.aero/bookshelf/books/350.pdf
[FAA, 2000]	FAA System Safety Handbook, December 2000, www.asy.faa.gov/RISK/SSHandbook/contents.htm.
[Fowler et al., 2007]	D Fowler, G Le Galo, E Perrin and S Thomas, So it's reliable but is it safe?, Proceedings of the 7th US / Europe Seminar on ATM Research & Development, Barcelona, July 2007, www.atmseminar.org/past-seminars/7th-seminar-barcelona-spain-july-2007/papers/paper_041
[Fowler et al., 2009]	D. Fowler, E. Perrin, R. Pierce, A systems-engineering approach to assessing the safety of the SESAR Operational Concept 2020 Foresight, Eighth USA/Europe Air Traffic Management Research and Development Seminar, 2009

This project has been carried out under a contract awarded by the European Commission

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[GAIN AFSA, 2003]	GAIN Working Group B, Analytical Methods and Tools, Guide to methods and tools for Airline flight safety analysis, Second edition, June 2003, http://www.flightsafety.org/gain/analytical_methods_and_tools.pdf
[GAIN ATM, 2003]	GAIN Working Group B, Analytical Methods and Tools, Guide to methods and tools for safety analysis in air traffic management, First edition, June 2003, http://www.flightsafety.org/gain/methods_tools_safety_analysis.pdf
[Gibson & Kirwan, 2008]	Gibson, W.H. and Kirwan, B., 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
[Harvey et al., 2002]	A. Harvey, J. L. Marchand, H. Wagemans, & K. Vickery, "The validation data repository: a central source of validation information for managers and practitioners", Proc. of the 21st Digital Avionics Systems Conference, 2002.
[Hollnagel et al., 2006]	Hollnagel, E., Woods, D. D. and Leveson, N., (Eds.), Resilience Engineering – Concepts and Precepts, Ashgate Publishing, 2006
[Jacobson et al., 2009]	D. Jacobson, N. McDonald, B. Musy, HILAS: Human Interaction in the Lifecycle of Aviation Systems – Collaboration, Innovation and Learning, 13th International Conference on Human-Computer Interaction, San Diego 2009.
[Kelly & McDermid, 1997]	TP. Kelly, & J. McDermid, Safety Case Construction and Reuse using Patterns, Proc 16th Int Conf on Computer Safety, Reliability and Security (Safecomp '97)
[Kirwan, 1994]	B. Kirwan, A guide to practical human reliability assessment, Taylor and Francis, 1994.
[Kirwan, 1998]	B. Kirwan, Human error identification techniques for risk assessment of high risk systems – Part 1: Review and evaluation of techniques, Applied Ergonomics, Vol 29, No 3, pp. 157-177, 1998.
[Kletz, 1999]	Kletz T 1999, Hazop and Hazan; identifying and assessing process industry hazards, The Institution of Chemical Engi-neers, 4th ed.
[Kumamoto & Henley, 1996]	H. Kumamoto, E.J. Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists, IEEE Press, 1996.
[MUFTIS, 1996]	M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom, O.N. Fota, MUFTIS work package report 3.2, final report on safety model, Part I: Evaluation of hazard analysis techniques for application to en-route ATM, NLR TR 96196 L, 1996.
[NAS, 2008]	National Aeronautics and Space Administration, Best Practices for Researching and Documenting Lessons Learned, March 2008, klabs.org/DEI/lessons_learned/reports/cr-2008-214777.pdf
[OCVSD]	FAA/Eurocontrol, Operational concept validation strategy document, Action Plan 5: Validation and verificiation strategies, Ed. 2.0a, 31 March 2008.

This project has been carried out under a contract awarded by the European Commission

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[Perrin et al., 2007]	E. Perrin, B. Kirwan, R. Stroup, A systemic model of ATM safety: the Integrated Risk Picture, In: Proc. 7th US / Europe Seminar on ATM R&D, Barcelona, July 2007
[RESET, 2007]	H. Blom, M. Everdij, B. van Doorn, D. Bush, K. Slater, "Existing safety assessment methods versus Requirements", RESET project Deliverable D6.1, September 2007
[RESET, 2009]	H. Blom, "RESET WP7.1 Working Document: Managing the E-OCVM phase V1 Preliminary HF and safety case building process", Version 0.3, March 2009.
[Review SAM techniques, 2004]	EEC, Review of techniques to support the EATMP Safety Assessment Methodology, Volume I and II, EEC Note No. 01 / 04, Project SRD-3-E1, M.H.C. Everdij, January 2004; http://www.eurocontrol.int/eec/public/standard_page/DOC_Report_2004_001.html
[Safety Fundamentals, 2006]	Oliver Straeter, Managing Safety Proactively – Experiences on the Implementation of the Safety Agenda at Eurocontrol, international conference on Probabilistic Safety Assessment and Management 8 (PSAM 8), New Orleans, Louisiana, USA, 2006.
[Safety Methods Database]	Database containing over 700 safety assessment methods and techniques from various industries, Maintained by NLR, Available at http://www.nlr.nl/documents/flyers/SATdb.pdf
[SAME PT1, 2008]	Eurocontrol, Safety Assessment Made Easier, Part 1 - Safety Principles and an introduction to Safety Assessment Ed. 0.92, 11 July 08
[SARD v1.8, 2009]	Eurocontrol & CAATS II, "SARD Life Cycle Phase Transition Criteria - Annex A v1.8 clean.doc", distributed by Mete Çeliktin on 9 April 2009.
[SARD, 2008]	Eurocontrol, Strategic assessment of ATM R&D results, Assessment process & criteria, contact: Mete Çeliktin, mete.celiktin@eurocontrol.int , Version 1.0, 2008.
[SESAR CVM]	SESAR Definition Phase, Concept Validation Methodology, WP4.2/Task 4.2.1, Part of DLT-0710-421-01-00, version 1.0
[SESAR D6]	SESAR Definition Phase, Deliverable 6, Work Programme for 2008-2013, DLM-0710-002-02-00, 2007.
[SESAR DS]	SESAR Definition Phase, Development Strategy, WP4.2.1 System Engineering Development & Validation Process/D6, Part of DLT-0710-421-01-00
[SESAR MPMS]	SESAR Definition Phase, WP4.1.12/D5-D6, DLT-0701-041-00-08, 27-March-2008
[SESAR RLP]	SESAR Definition Phase, T3.4.6/D5 Regulatory - Legislative Planning, DLT-0710-346-00-05
[SESAR SEM]	SESAR Definition Phase, WP4.2.1/D6, System Engineering Methodology, DLT-0xxx-241-0x-0x, Status: DRAFT#02
[SESAR SMP]	SESAR Definition Phase, SESAR Safety Management Plan (SMP), WP4.2/Task 4.2.1, Part of DLT-0710-421-01-00

This project has been carried out under a contract awarded by the European Commission

LIST OF REFERENCE DOCUMENTS	
Short Reference	Author / Organisation, Title, Edition, Date and Reference
[SESAR WP1.6.1/ D1]	SESAR Consortium, "Air Transport Framework The Current Situation", July 2006.
[SESAR WP1.6.1/ D2]	SESAR Consortium, "Air Transport Framework The Performance Target", December 2006.
[SESAR WP1.6.2/ D3]	SESAR Consortium, "Air Transport Framework The ATM Target Project", September 2007.
[Shah et al., 2005]	Shah, A.P., Pritchett, A.R., Feigh, K.M., Kalaver, S.A., Jadhav, A., Corker, K.M., Holl, D.M., Bea, R.C., 2005. Analyzing air traffic management systems using agent based modelling and simulation. In: 6th USA/Europe ATM R&D Seminar, Baltimore, USA.
[Strater et al., 2007]	O. Strater, 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 of Eurocontrol Safety R&D Seminar, Rome, Italy, 24-26 Oct. 2007.
[Stroeve et al., 2003]	Stroeve SH, Blom HAP, Van der Park MNJ. Multi-agent situation awareness error evolution in accident risk modelling. Proceedings of the 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
[Stroeve et al., 2006]	S.H. Stroeve, H.A.P. Blom, G.J. Bakker, Safety risk impact analysis of an ATC runway incursion alert system, Eurocontrol Safety R&D Seminar, Barcelona, Spain, 25-27 October 2006.
[Stroeve et al., 2008]	Stroeve, S. H., Sharpanskykh, A., van Lambalgen, R. M. Kirwan, B. Safety culture analysis by agent-based organizational modelling. In Proceedings of the 7th EUROCONTROL Innovative Research Workshop & Exhibition, 2008.
[Stroeve et al., 2009]	Stroeve, S.H., H.A.P. Blom, G.J. (Bert) 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)
[Tversky & Kahneman, 1974]	A. Tversky, & D. Kahneman, Judgment under Uncertainty: Heuristics and Biases. Science(185), 1974
[Van Baren et al., 2002]	G.B. van Baren, L.J.P. Speijker, A.C. de Bruin, Wake vortex safety evaluation of single runway approaches under different weather and operational conditions, Proc. PSAM6, Puerto Rico, 2002.
[Van den Bos et al., 2009]	J.C. (Hans) van den Bos, Hans H. de Jong, and Roy B.H.J. Jansen, Apportioned ATC Safety Criteria Based on Accident Rates, In: ATC Quarterly, forthcoming, 2009
[Vernon & Perrin, 2007]	G. Vernon & E. Perrin, Methodology report for a Safety Target Achievement Roadmap (STAR), Eurocontrol report, May 2007

This project has been carried out under a contract awarded by the European Commission

2. GENERIC SAFETY ASSESSMENT PROCESS

The approach for safety assessment is relatively well consolidated for an ANSP assessing a change to its ATM system (including humans, procedures, and technical equipment). Requirements expressed in ESARR 4 [ESARR 4] cover risk tolerability for concepts and systems, and guidelines and support material are available to organise and conduct the safety assessment activities, including the deliverable on safety assessment produced in the CAATS project [CAATS, D1.4 P2].

However, little support is available for R&D projects, which are not subject to a regulated assessment process. The assessment should be tailored on the characteristics of the R&D projects (e.g. level of maturity of the concepts under investigation, aims of the project, relevance for the safety, etc.), but little support is available to understand what level of safety assessment is adequate, and how to assess the safety of concepts that are not stable. In this section we introduce a model of the safety assessment process that is general enough to be applicable to any maturity level of an ATM concept (either at the R&D or operational level) and that covers all the activities that are part of a safety assessment.

2.1 Phases of safety assessment

This section is based on the work done in FAA/Eurocontrol (with the support of NASA, NLR, NATS, CENA) Action plan 15: ATM Safety Techniques and Toolbox [AP15]. This work has been integrated and refined to address safety assessment even in the early phases of a concept development (e.g. concept definition, design and integration) that is, the typical maturity level of a concept in an ATM R&D project.

Safety assessment is the process through which it is assessed whether new proposed changes to an ATM system do not sacrifice safety and preferably make things better, whatever those changes are (e.g. new operational concepts, changes in ATM procedures, introduction of new technical systems or up-grading of the existing ones). This means that all possible impacts of a new operation or system, either positive or negative, should be assessed, and their combined safety effects determined. Initially, a safety assessment considers the proposed operation or system definition (often called the Operational Concept), and communicates these results with concept designers which could impact matters, for the better and/or for worse, with respect to safety. This analysis involves considering the scope of the assessment (affecting how far the analysis is taken particularly in terms of interactions with other system elements). Then, it involves identifying possible hazards and the severity of their consequences. Depending on the level of maturity of the concept, and on its stability, the analyst may then determine how probable these failures are, as well as how likely the operation is to recover from such failures. This culminates in an overall picture of the safety of the operation.

The safety assessment process is documented as a ‘safety case’, where all the evidence emerged during the safety assessment is collected, this is used to transmit all the information to future users of the concept. For example, if a R&D project is investigating a new concept and conducting an initial safety assessment, the results of this work will be included in a safety case that will be used by future projects investigating the same concept. When a concept is stable and mature enough for operation the safety case is used to justify to the regulatory authorities that the new proposed operation or operation change will not adversely affect safety.

Once the new design itself is operational, there becomes a need to continually monitor safety performance, so the responsibility for safety oversight then transfers to the management of the operational facility. Usually a safety activity will be created that will record safety-related events (e.g. losses of separation, TCAS events, etc.), for lessons learned purposes. Trends may occur

This project has been carried out under a contract awarded by the European Commission

for example related to local factors (e.g. particular controller working practices and changes in local sector design) or more widespread factors (e.g. shifts in controller demography and availability). The detection of trends that could compromise safety requires archiving relevant data and monitoring them continuously. The process cannot rely on human memory. When such a trend is detected and determined to be operationally significant, an appropriate reaction should occur to ensure that the operation returns to its safe performance. This amounts to organisational safety learning and should make part of the safety assessment and operation development process.

Safety Assessment of an air traffic operation can be seen as a seven-stage process with an eighth stage related to communication of results, as in the model proposed below and presented in figure 1. In most of the cases, not all these stages will be addressed within a single R&D project. Even within a single project safety assessment is usually iterative in nature: the process can iterate some of the stages as shown in the figure. In most of the R&D projects, not all these stages are addressed explicitly within a single iteration. Depending on the level of maturity of the concept under investigation, the process can be limited to, or skip some of those stages. Normally all the safety assessment processes include at least the initial stages up to the mitigation, however, the level of detail of those stages can change substantially from project to project and some of them can be skipped or minimal in some projects.

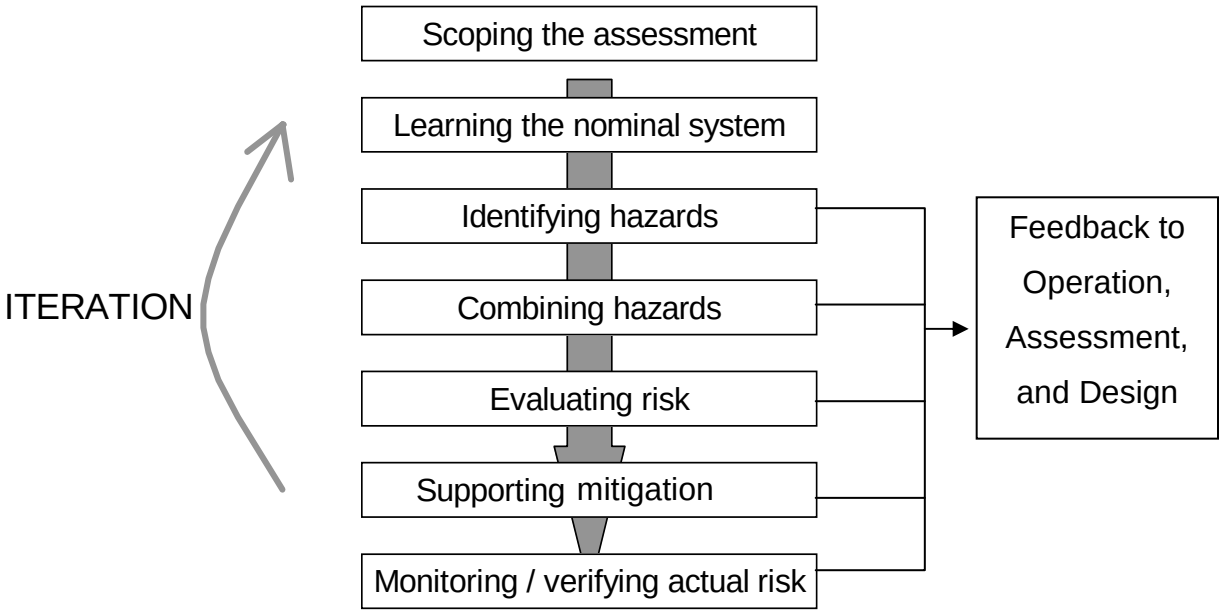


Figure 1 – A generalised Safety Assessment Process

The eighth stage has been included to address communications. Results of the safety assessment are produced from the early stages of the process, for example in the form of preliminary lists of hazards. These results are communicated to the project team in order to influence the concept design and address the safety problems of the concept under development. This communication should be part of all other stages; however, this is not included at the moment in the FAA/Eurocontrol Action plan 15. It is referred to as the 'eighth' Stage in this document.

This project has been carried out under a contract awarded by the European Commission

The following paragraphs outline the key aspects of these stages, including the 'eighth' stage dedicated to feedback provision. It is based on an interpretation of the AP15 model.

1. **Stage 1 – Scope the Assessment**

This stage entails the availability of an *operational concept* or *system specification*. It is difficult to conduct safety assessments without knowing what the operation is going to look like. However, it is not uncommon with early assessments that the operational concept itself is a living document and 'ever-evolving'. The project and the safety practitioner must specify the scope of the safety assessment and should outline a "route map" for the safety assessment. Therefore, it is essential to identify the level of maturity of the concept. The "route map" can include such pertinent information as the extent and depth of the safety assessment in the R&D project, including the number of process stages to be addressed, and where the operation boundaries are considered to be. The safety assessor needs such information to determine at this stage which safety method(s) are to be used, and to envision the likely safety-related resources such as access to operational personnel, the need for simulations and trials, etc.

The output of this stage should include at least a plan for the safety analysis cycle to be performed, and in case of a safety assessment process covering all the stages, an assignment of safety/risk criteria (e.g., target level of safety).

2. **Stage 2 – Learning the nominal operation**

Safety assessment is 'transitive' in nature; it requires an object, something to analyse. This is often not realised by non-safety practitioners. There is therefore a need to learn about the description of the operation and systems as it should work or function, this being the 'nominal' model.

There are various ways of modelling an operation for subsequent safety analysis, and indeed often this is done by the project or program in any case. In some cases special modelling approaches might be required, e.g. to analyse human tasks. These techniques are effectively abstractions of the operation from a particular viewpoint, and so the exact safety modelling requirements are a function of the aspects on which the safety practitioner intends to focus on.

The model can be at a very high level of abstraction for R&D projects investigating concepts that are at the initial maturity levels, and becomes more and more detailed as long as the concept progresses and becomes more stable and more detailed.

The output of this stage is a description of the operation and the systems used. This output is used to communicate with the operational concept designers.

3. **Stage 3 – Identify hazards**

This is one of the most critical stages in safety assessment, since if a hazard is not identified, it will not be considered further, and risk may be underestimated. Risks from all sources need to be considered. Such risks include those that may emanate from the operational concept itself, usually along the dimensions of hardware, software, procedures, and human elements, and those that have nothing to do with the concept but can affect it.

These latter considerations may relate to 'external events' in the environment (e.g. bad weather), or to failures or events in other operations that can affect the operation under consideration. One of the difficulties of hazard identification in ATM applications is that ATM is effectively a globally interoperable operation. This means firstly that it is difficult to know when a

This project has been carried out under a contract awarded by the European Commission

hazard identification exercise is complete. Secondly it means that there is much to consider, especially in terms of interactions of operation elements. Certain failures (e.g. power supply) will affect multiple operations, and loss of key data similarly can affect different operations in different ways. These are called common cause failures (identified by common cause analysis), and relate to what are called 'dependencies' between operations, and can lead either to new failure outcomes or elevated failure frequencies, so they need to be identified.

The output of this stage is a log with the identification of the possible hazards related to the concept under investigation.

4. Stage 4 – Combine hazards

Hazards and their contributions are aggregated to accident sequences into a risk model with which the total risk due to the proposed operation or change can be evaluated. This stage allows to weigh up the different identified risks and their various accident sequences, and in particular to determine if the risks will be within the target level of safety selected.

Since levels of risk are influenced (possibly quite significantly) by dependencies and common cause failures that exist between different parts of the risk model, risk modelling should include a dependency analysis (e.g. going through the risk model identifying common elements and dependencies). A complementary approach is to make use of a simulation which allows to evaluate multiple dynamical and dependent events, non-nominal scenarios, and permutations of such events and scenarios, and to make effective use of a larger variety of qualitative and quantitative input data (e.g. human performance models).

The output of this stage is a risk model that encapsulates and relates the different hazardous and recovery events into a homogeneous model. This risk model can then be quantified (this process is called 'evaluation'), delivering not only the overall risk estimate, but also the ability to determine which elements in the operation are most safety critical.

5. Stage 5 – Evaluate Risk

The aim of this stage is to determine properties of the risk model – in particular how often the various events are likely to occur. In some cases, databases will exist which can give such information, e.g. the likely time before failure of a radar screen, or the probability of a communication error between controller and pilot. In other cases, there may be techniques to estimate such values.

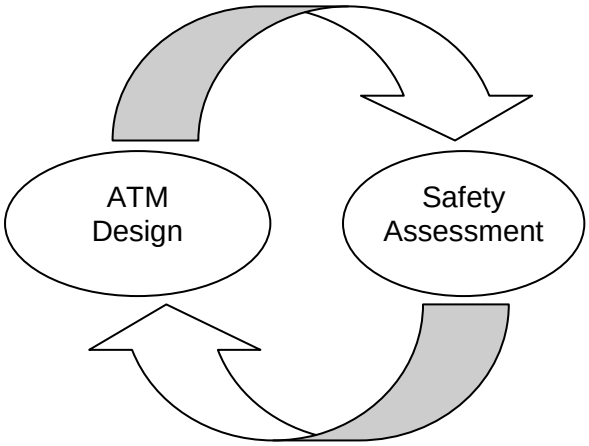
6. Stage 6 – Identify potential mitigating measures

The aim of this stage is to support concept developers in identifying potential mitigations or changes that could improve safety. Depending on the level of concept maturity this can be done at different levels of details. The analyst has to consider whether risk reduction is required, i.e. if the risk can be considered acceptable because qualitative or quantitative risk criteria are met. This sets the initial obligation to reduce risk, and tells the assessor the size of the challenge ahead. If the risk is in acceptable the effort to achieve further reductions is likely to be grossly disproportionate (although the duty holder is still expected to demonstrate this). If the risk is not acceptable, it shall be reduced adequately.

The output of this stage inform the designer about what should be done to reduce risk and increase safety.

This project has been carried out under a contract awarded by the European Commission

7. Stage 7 – Safety monitoring and verification



This stage is only applicable if the R&D project develops a real system (even if in the form of prototype). With respect to existing operations, this stage refers to the need to continually monitor overall operation safety performance and determine if the various safety requirements are performing their functions as expected. It requires a means of monitoring and analysing resultant safety data, and then drawing lessons from those data in sufficient time to react and prevent accidents from occurring. This is not trivial, and requires pre-definition of safety parameters and events, automatic and manual recording mechanisms, analysis tools, and data storage and retrieval operations (knowledge bases). It also of course requires a good safety culture that will accept such monitoring and analysis and will act on its conclusions, and a legal framework (a so-called 'just culture') that will protect controllers and pilots offering up much-needed safety information on human errors and other events that occur.

The output of this stage is a measurement of safety-related events and data against predictions.

8. Stage 8 – Feedback to Operation, Assessment, and Design

Within this stage results are communicated to the project team in order to influence the concept design and address the safety problems of the concept under development, as long as preliminary results are achieved. This feedback is an essential element in safety communication and leads to organisational learning. This communication should be part of all other stages; however, in this report it is referred to as the 'eighth' stage.

The principle aim of any safety assessment, and one of the major outputs of a safety assessment process, is an issue that does not always get the attention it deserves: **safety communication**. The value of a safety assessment is largest when there is a sound feedback communication to operational concept design. This is especially true in R&D projects when the main aim of a safety assessment activity is to produce feedback useful to improve the concept under investigation. With feedback communication, safety assessment is a way for the designers to learn where their design should be improved in order to become sufficiently safe. The aim of the whole safety assessment is to learn something, so that the design can be improved. This interaction between design and assessment is depicted in Figure 2.

Figure 2 – Feedback-based ATM design

This project has been carried out under a contract awarded by the European Commission

3. CURRENT METHODS USED FOR SAFETY ASSESSMENT IN R&D PROJECTS

This section describes the different methods that are used, with more frequency, for safety assessment in R&D projects. These methods resulted as the current good practices for safety assessment in R&D projects from an analysis of:

- CAATS target projects (R&D projects of the VI Framework Programme) as explained in Part 2, Appendix I.
- CAATS II target projects (R&D projects of the VI Framework Programme). A list of these projects is also reported in Part 2, Appendix I.
- Other relevant European R&D projects. A list of these projects is also reported in Part 2, Appendix I.
- Experience of the CAATS Safety Team with other National and International collaborative ATM R&D projects
- Surveys, questionnaires and analysis done during the CAATS and CAATS II projects.

In total the two CAATS projects considered 25 European research projects, of which 12 were considered with relevant safety related activities. Safety assessments of these projects were analysed in depth and revised, and the practices used were evaluated to identify the current good practices presented in this section (dealing with methods) and in the next one (dealing with techniques and tools). The results of the evaluation were reinforced by interviews, surveys and brainstorming sessions run at safety-relevant conferences and at the CAATS II workshops. The opinion of more than 80 safety experts were collected and analysed during these activities.

The criteria for selecting these methods, as good practices for safety assessment, are the criteria used in CAATS [CAATS, D1.4 P2] adapted to R&D projects. Good practice emerges in each sector, with experience. They have shown to work better than others making projects more effective in achieving their objectives. The basic criterion is that the practices delivered the desired performance, effectively, in more than one specific situation. The term best practice is stronger, requiring not only that there are practices proven to be effective, but that there is an agreement or an imposition of rules on how things should be done. The first CAATS project considered R&D in ATM not mature enough for such a level of standardisation and focused on good practices, defining a few criteria for identifying good practices. These include:

- Practices that are used often in the ATM domain
- Practices that are often referred to
- Practices that are well documented
- Practices that are publicly available
- Practices for which there is a training or education programme
- Practices that are considered in safety critical industries of other domains of application

We considered in this document only those safety assessment methods that are used in R&D projects. There is a large variety of other methods used by ANSP for mature concepts ready to move to operation. The interested readers can find a discussion about these methods in [CAATS, D1.4 P2].

The methods presented in this section are the following:

- Safety Assessment Methodology (SAM) [EATMP SAM, 2007]
- EUROCAE ED78A [ED78A, 2000]
- Traffic Organization and Perturbation AnalyZer (TOPAZ) [Blom et al., 2006a]

This project has been carried out under a contract awarded by the European Commission

3.1 Safety Assessment Methodology (SAM)

SAM [EATMP SAM, 2007] presents a general overview of an Air Navigation Systems safety assessment from an engineering perspective. The safety assessment activities are sub-divided into:

- Risk assessment activities, to identify hazards, and evaluate the associated risk tolerability,
- Safety engineering activities, to select, validate and implement counter measures to mitigate these risks, and
- Safety assurance activities, which involve specific planned and systematic actions that together provide confidence that all relevant hazards and hazard effects have been identified, and that all significant issues that could cause or contribute to those hazards and their effects have been considered.

The objective of the methodology is to define a means for providing assurance that an Air Navigation System is safe for operational use. It is an iterative process conducted throughout the system development life cycle, from initial system definition, through design, implementation, integration, transfer to operations, to operations and maintenance. The iterative process consists of a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and a System Safety Assessment (SSA).

The objectives of the FHA, the PSSA and the SSA are:

- Functional Hazard Assessment (FHA) analyses the potential consequences on safety resulting from the loss or degradation of system functions. Hazards are identified at the boundary of the systems, or service under assessment. Using service experience, engineering and operational judgement, the severity of each hazard effect is determined qualitatively and is placed in a class 1, 2, 3, 4 or 5 (with class 1 referring the most severe effect, and class 5 referring to no effect). *Safety Objectives* determine the maximum tolerable probability of occurrence of a hazard, in order to achieve a tolerable risk level.
- Preliminary System Safety Assessment (PSSA) determines that the proposed system architecture is expected to achieve the safety objectives. PSSA examines the proposed system architecture and determines how faults of system elements and/or external events could cause or contribute to the hazards and their effects identified in the FHA. Next, it supports the selection and validation of mitigation means that can be devised to eliminate, reduce or control the hazards and their end effects. System *Safety Requirements* are derived from Safety Objectives; they specify the potential means identified to prevent or to reduce hazards and their end effects to an acceptable level in combination with specific possible constraints or measures.
- System Safety Assessment (SSA) collects arguments, evidence and assurance to ensure that each system element as implemented meets its safety requirements and that the system as implemented meets its safety objectives throughout its operational lifetime (till decommissioning), i.e. the *Safety Assurance & Evidence Collection* step. It demonstrates that all risks have been eliminated or minimised as far as reasonably practicable in order to be acceptable, and subsequently monitors the safety performance of the system in service. The satisfaction of safety objectives is checked against data reflecting current performances to confirm that they continue to be achieved by the system.

It is noted, that SAM is currently being incorporated in SAME, which is one of the emerging approaches discussed in this document. An extensive introduction to SAME is provided in Part 2, Appendix V.

This project has been carried out under a contract awarded by the European Commission

3.2 EUROCAE ED78A

The EUROCAE ED78A document [ED78A, 2000] (identical to the RTCA DO-624), entitled "Guidelines for approval of the provision and use of Air Traffic Services supported by data communications" provides means to establish the operational, safety, performance, and interoperability requirements for ATS supported by data communications, to assess their validity, and to qualify the related CNS/ATM system. It is a single source document that provides guidance for approval of the CNS/ATM system and its operation where coordination is necessary across organizations. The guidance material considers the allocations of the operational, safety, performance, and interoperability requirements to the elements of the CNS/ATM system. These include ground-based elements, operational procedures, including the human, and aircraft equipage.

The process considered in ED78A consists of:

- approval planning,
- coordination of requirements determination across organizations,
- development and qualification of CNS/ATM systems at the organizational level,
- entry into service, and
- operations using ATS supported by data communications.

The Coordinated Requirements Determination process includes the interrelated processes that are coordinated by the stakeholders. These are:

- The identification of an Operational Services and Environment Description (OSED).
- The Operational Safety Assessment (OSA), including an Operational Hazard Assessment (OHA) and an Allocation of Safety Objectives and Requirements (ASOR);
- The Operational Performance Assessment (OPA), including communication, technical and human performance determination.
- The Interoperability Assessment (IA)

The processes are shown in figure 3 in logical sequence. Recognizing that there may be considerable overlap of processes, the logical sequence is also the recommended sequence.

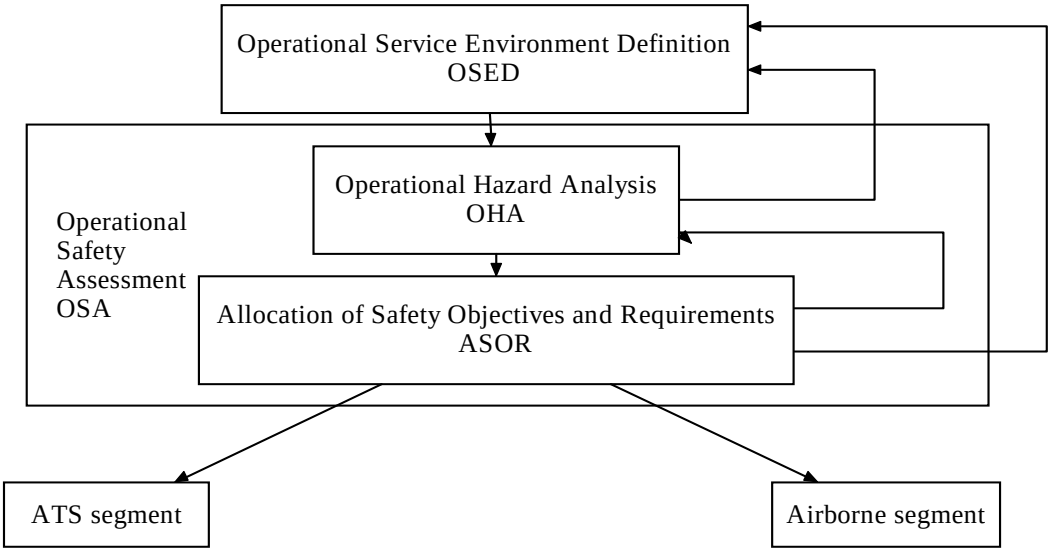


Figure 3 – Relationship between OSED, OHA and ASOR processes

This project has been carried out under a contract awarded by the European Commission

In the subsequent phases, it needs to be verified and ensured whether all requirements are satisfied. If not, this requires updates and feedback into the requirements determination. Development and qualification are considered iterative processes themselves: including requirements capture, design, integration, validation, verification and so on.

In the context of the OSA methodology, the objective of the OSED is to obtain the relevant information for the safety assessment of the CNS/ATM system under consideration. In a wider context, as considered in the RTCA/EUROCAE guidance, the OSED is also used as a basis for assessing and establishing the performance and interoperability requirements.

The purpose of the OHA step is to develop an end-to-end qualitative assessment of potential operational hazards. The next step is the ASOR, i.e. the establishment and allocation of safety objectives and requirements to stakeholders and elements of the CNS/ATM system. These stakeholders include ATS providers, ATS equipment manufacturers, supporting service providers, such as those that provide communication and weather services, aircraft and equipment manufacturers, and operators. The OHA and ASOR are interrelated and iterative processes.

The OHA is a qualitative assessment of the operational hazards associated with the OSED. For the OHA, operational functions are examined to identify and classify hazards that could adversely affect those functions. Based on a high level description of the operational procedures and airborne/ground functional characteristics, the identification of operational hazards should be supported by considerations including:

- functional failure;
- human failure to respond appropriately to functional failure;
- human error or omission during normal use;
- transitional hazards (those that may result by changing from existing to new operations);
- external factors (e.g. outages, weather).

Hazards are classified according to a standardised classification scheme based on hazard severity and taking into account effects at the aircraft, air traffic services and operations. Overall safety objectives are assigned to the identified hazards according to a risk classification matrix. The more severe the hazards are, the less frequently they are tolerated. Based on the OHA results, the ASOR allocates safety objectives to domains, develops and validates risk mitigation strategies, and allocates safety requirements to those domains.

3.3 Traffic Organization and Perturbation AnalyZer (TOPAZ)

TOPAZ (Traffic Organization and Perturbation AnalyZer) is an advanced accident risk assessment methodology that supports a scenario and Monte Carlo simulation-based accident risk assessment of an air traffic operation, which addresses all types of safety issues, including organisational, environmental, human-related and other hazards, and any of their combinations[1]. The main aim of TOPAZ is to model accident risks that are related to advances in air traffic management in order to provide feedback to the designers of the advanced operation regarding the main sources of unsafety as function of traffic and environment characteristics, including quantification. This produces for the advanced concept designers unique insight on which safety/capacity aspects of the design can best be addressed to realize the high level objective of improving capacity without sacrificing safety.

[1] It is noted that the Dynamic Risk Modelling and Monte Carlo simulations used in TOPAZ can also be applied as a technique in supporting other safety assessment methodologies.

This project has been carried out under a contract awarded by the European Commission

As the development of appropriate Monte Carlo simulation support may be demanding, it is important to notice that the TOPAZ accident risk assessment methodology can also be applied if such Monte Carlo simulation support is not yet developed for the operation considered. In that case expert judgement plays a larger role and uncertainty level may be relatively large. When the dynamic and stochastic effects are significant and the uncertainty in the assessed risk level is too large, than it is recommended to use Monte Carlo simulation support for the safety risk assessment.

Monte Carlo simulation based TOPAZ applications have been developed for several areas, such as en-route opposite traffic [Blom et al., 2003a], Double Missed Approach [Blom et al., 2003b], Wake vortex induced riks assessment [Van Baren et al., 2002], Active runway crossing [Stroeve et al., 2006], ASAS within route structure [Everdij et al., 2007], and ASAS without route structure [Blom et al., 2006b]. For these applications, stochastic modelling and analysis plays a key role. Typically, the stochastic modelling makes use of high-level Petri net specification formalism [Everdij et al., 2006c] [Everdij & Blom, 2008], human performance modelling [Blom et al., 2001] [Stroeve et al., 2003], and bias and uncertainty assessment [Everdij et al., 2006b].

An overview of the steps in the safety risk assessment cycle developed at NLR and presented in [Blom et al., 2006a] is given in Figure 4. Although the cycle itself is in line with the established risk assessment steps (e.g. [Kumamoto & Henley, 1996]), some of these steps differ significantly.

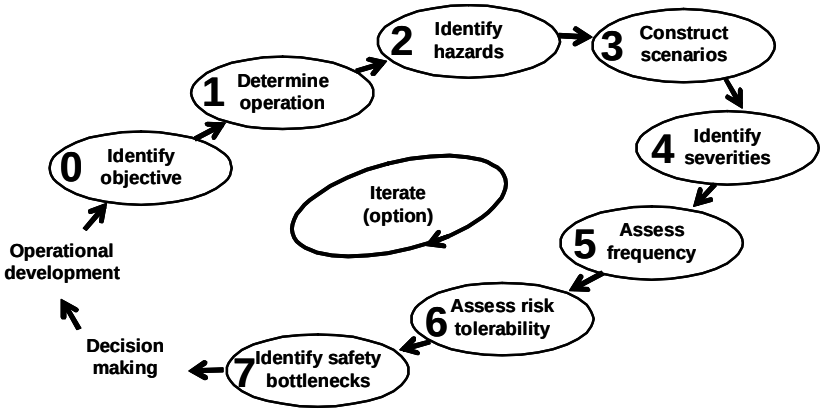


Figure 4 – TOPAZ risk analysis cycle

In step 0, the objective of the assessment is determined, as well as the safety management and regulatory context, the scope and the level of detail of the assessment. The actual safety assessment starts by determining the operation that is assessed (step 1). Next, hazards associated with the operation are identified (step 2), and aggregated into safety relevant scenarios (step 3). Using severity and frequency assessments (steps 4 and 5), the safety risk associated with each safety relevant is classified (step 6). For each safety relevant scenario with a (possibly) unacceptable safety risk, the main sources (safety bottlenecks) contributing to safety risks are identified (step 7), which help operational concept developers to learn for which safety issues they should develop improvements in the ATM design. If the ATM design is changed, a new safety risk assessment cycle of the operation must be performed in order to investigate how much the risk posed by previous safety issues has been decreased, and to

This project has been carried out under a contract awarded by the European Commission

assess any new safety issues that may have been introduced by the enhancements themselves.

Whenever, for a particular aspect of the operation under analysis, step 5 is more demanding than what can be assessed on safety using conventional methods (e.g. fault/event trees), then the TOPAZ methodology is to develop and subsequently use a Monte Carlo simulation tool set for the an advanced operation. For a number of advanced operations a dedicated TOPAZ tool set has already been developed and applied to operational concepts that range from runway crossing operations to airborne self separation concept studies, and during maturity stages ranging from V1 (early concept studies) through V6 (true operations). The main aim is to gain insight in the main risks of an operation and their causes. Once this is understood well, operational concept designers typically are able to improve the operational concept design such that these main risks are mitigated significantly.

3.4 Compliance of safety assessment methodologies to ESARR 4

Safety assessment methodologies can be submitted to EUROCONTROL Safety Regulation Commission (SRC) as proposed means of compliance to the ESARR 4 regulation for risk assessment and mitigation in ATM, that has been in force since 2001 [ESARR 4]. For all three methodologies introduced, this has been done. In 2004, the most recent document on the evaluation of proposed means of compliance with ESARR 4 [EAM 4, 2004] was published. This included statements on ED78A and an earlier version of SAM, which showed their partial compliance. For TOPAZ no evaluation has (yet) been started by SRC at the time of writing.

Whereas ESARR 4 is in force since 2001, at the time of writing, no methodology is known for which full compliance with ESARR 4 has been confirmed by SRC.

3.5 Coverage of the eight stages model by selected methods

An indicative evaluation of the stages, of the safety assessment process presented in Section 2, covered by each method presented above is reported in Table 1. However, it is worthwhile to note that the maturity, that is normally reached by ATM concepts in R&D projects, does not usually allow to arrive to stage 7 (‘Safety monitoring and verification’) that is normally relevant for systems close to implementation.

Table 1 – Coverage of the eight stages model

No	Stage of the Model	SAM	ED78A	TOPAZ
1	Scoping the Assessment	Yes	Partially (less detailed than the other two methods)	Yes
2	Learning the nominal operation	Yes	Yes	Yes
3	Identifying hazards	Yes	Yes	Yes
4	Combining hazards	Yes	No	Yes
5	Evaluating Risk	Yes (focus on negative contribution to safety)	Yes (focus on negative contribution to safety)	Yes
6	Identifying potential mitigating measures	Yes	Yes	Yes
7	Safety monitoring and verification	Yes (but rarely done in practice)	No	Optional (but rarely done in practice)

This project has been carried out under a contract awarded by the European Commission

8	Feedback to Operation, Assessment, and Design	Yes, focus is on safety requirements	Yes, focus is on safety requirements	Yes, focus is on learning

In conclusion, all three methods cover the eight AP15 stages rather well. Nevertheless there are some interesting differences for stages 4, 5, and 8. ED78A falls short in combining hazards (stage 4). TOPAZ on the other hand stands out in a positive way on evaluating both positive and negative contribution to safety risk (stage 5). For stage 8, ED78A and SAM focus on feedback in the form of safety requirements, whereas TOPAZ provides feedback with the focus on understanding the main sources of safety risk, and on sensitivity of risk to changes in parameter values. These sensitivity values provide system design experts the capability in seeing themselves how changes in safety requirements affect safety risk.

This project has been carried out under a contract awarded by the European Commission

4. EMERGING ASSESSMENT APPROACHES

This section presents emerging approaches in safety assessment in ATM R&D projects. Before presenting these emerging assessment approaches, first a literature review of techniques is presented, including reference to a database of more than 600 safety assessment techniques.

4.1 Literature review of safety assessment techniques

The previous sections outlined seven (or eight) stages in a safety assessment process; it did not provide detailed guidelines on how to perform each stage (nor did it intend to). Many different techniques are available to provide support for this. To obtain a broader view of the techniques that are available, allowing making a better choice among techniques to use, this section presents a literature review of the numerous safety assessment techniques and methods that are available and that each can support one or more of the stages of the generic safety assessment process. After this literature review, in the following subsections the focus is on emerging assessment approaches.

Table 2 provides references to recent survey documents, ordered chronologically, and the scope of each document.

Table 2 – References to recent safety methods survey documents

Reference	Scope
[Review SAM techniques, 2004]	This report presents the main results of a comprehensive survey conducted in 2002, aimed at collecting and evaluating techniques and methods that can be used to support the guidelines of the EATMP Safety Assessment Methodology (SAM). Over 500 techniques are collected that can possibly support EATMP SAM. The survey includes techniques used in other industries (e.g. nuclear power, tele-communications, chemical, aviation, etc.), so that ATM can borrow or adapt techniques found to be effective elsewhere. The survey only considers publicly available techniques and methods, hence no commercially available tools or facilities. Nineteen of these techniques are subsequently evaluated in more detail along a template format. These 19 techniques are believed to be able to support the SAM either immediately, or with some tailoring or adaptation to the ATM context. In addition, the report gives a selection of techniques that are judged to be significantly important and therefore deserve further development. Many details are provided in a separate Technical Annex.
[GAIN AFSA, 2003]	The purpose of this guide is to provide information on existing analytical methods and tools that can help the airline community turn their data into valuable information to improve safety. Summaries are presented for 57 methods and tools that can be used to analyze flight safety data including event reports and digital flight data. Global Aviation Information Network (GAIN) Working Group B (Analytical Methods and Tools) hopes that this guide will help increase the awareness of available methods and tools and assist airlines as they consider which tools to incorporate into their safety analysis activities.
[GAIN ATM, 2003]	This guide addresses both analytical tools that were developed specifically for air traffic safety analysis applications as well as other tools that were not developed for this purpose but could potentially be applied to air traffic safety analyses. The guide identifies about 80 air traffic management safety tools of many types. However, it is recognised that this is not a complete list and other relevant tools exist that are not included. Some tools have been deliberately excluded; for example, tools that address air traffic system capacity, delay, and efficiency, but not safety. On the other hand, some tools developed for airspace design or controller training, for example, could have a safety application and are included. Operational tools are not included; but tools that might be used to assess the

This project has been carried out under a contract awarded by the European Commission

Reference	Scope
	efficacy of such tools are included. This guide contains some tools that are not available outside the organisations that developed them. Some are in the prototype or early development phase. Information on these tools might still be useful to those interested in developing their own tools.

The list of techniques identified in [Review SAM techniques, 2004] has been used as a starting point for a "Database of Safety Assessment Methods", publicly available at [Safety Methods Database]. It has been complemented by the methods listed in [GAIN AFSA, 2003] and [GAIN ATM, 2003] and additional techniques identified during the CAATS project and the RESET project have been incorporated. It currently includes more than 600 techniques. The database contains for each technique some basic information such as acronym and full name, brief description, application (i.e. hardware / software / human / procedure / organisation), domain (e.g. used in aviation, nuclear industry, computer processes), age, and some references, and also indicates in which of the eight stages of the generic Safety Assessment Methodology process (see Section 2) the technique can be used.

The main sources used for this database are:

- Reference [MUFTIS, 1996], which contained a survey of safety assessment techniques performed by NLR in 1996, and which was used as a starting point.
- Several other available surveys on safety techniques, such as [Bishop, 1990], [FAA, 2000], [EN 50128], [Kirwan, 1998], [FAA AC431, 2005], [Kirwan, 1994], [GAIN AFSA, 2003], [GAIN ATM, 2003], which provided numerous additional techniques and descriptions.
- NLR and Eurocontrol experts provided names of additional techniques and references with explanations.
- Internet searches on safety assessment techniques provided many papers published on the Internet, or references for books or documents available in a library. Internet searches also provided details for techniques already gathered, such as age, description, full name if only an abbreviation was provided, domains of application. Usually, these searches led to many names and descriptions of new techniques and to new references, and also to previous surveys mentioned above.
- Additional techniques have been added in [CAATS, D1.4 P2] and [RESET, 2007].
- After internet publication of the database, readers have sent in suggestions for adding additional techniques.

The task to determine emerging good practices among all these safety techniques is challenging, however. It may be assumed that the safety methods database contains several techniques that may be considered good practice, but the definition of good practice will depend on which criteria are used (and the database does not aim to address this issue). The choice for techniques to use will be dependent on the air traffic operation to be assessed. More complex operations are more demanding on techniques to use than less complex operations or operations for which a similar version already has been assessed. Moreover, the choice of techniques may be personal, dependent on good experience with some techniques, and depending on the background of the safety practitioner.

While not considering the methodologies EATMP SAM, ED78A, TOPAZ already discussed in Section 3, we get a list of 29 techniques which may be considered among the good practices from the selections of [Review SAM techniques, 2004] and [AP15]. Table 3 indicates for each of these 29 techniques in which Stages of the generic safety assessment process they can be used, and for the assessment of which ATM concept aspects (hardware, software, human,

This project has been carried out under a contract awarded by the European Commission

procedures, organisation) they can be used. All this information is taken from [Safety Methods Database].

Table 3 – Safety assessment techniques, with stages and concept aspects covered[2]. The concept aspects mentioned are hardware (Hw), software (Sw), Human (Hu), Procedure (Pr) and Organization (Or).

		Stages								ATM concept aspects				
Technique		**1** Scop	**2** Oper	**3** Hazid	**4** Model	**5** Risk	**6** Mitig	**7** Monit	**8** Feed	**Hw**	**Sw**	**Hu**	**Pr**	**Or**
1.	Air Safety Database			3				7	8	X	X	X	X	X
2.	Air-MIDAS				4	5				X		X	X	X
3.	ASRS (Aviation Safety Reporting System)			3				7	8	X		X	X	X
4.	Bias and Uncertainty assessment					5				X		X	X	X
5.	Bow-Tie Analysis						6			X		X	X	
6.	CCA (Common Cause Analysis)			3						X	X			
7.	Collision Risk Models					5							X	
8.	ETA (Event Tree Analysis)				4	5				X		X	X	
9.	External Events Analysis			3		5				X				
10.	FFC (Future Flight Central)			3								X	X	
11.	FMECA (Failure Modes Effects and Criticality Analysis)			3		5				X				
12.	FTA (Fault Tree Analysis)				4	5				X	X	X		
13.	HAZOP (Hazard and Operability study)			3	4		6			X	X	X		
14.	HEART (Human Error Assessment and Reduction Technique)					5						X		
15.	HERA (Human Error in ATM)			3								X		
16.	HTA (Hierarchical Task Analysis)		2									X		
17.	HTRR (Hazard Tracking and Risk Resolution)								8	X	x			
18.	Human Error Data Collection			3				7				X		
19.	Human Factors Case		2	3		5	6					X		
20.	ORR (Operational Readiness Review)							7		X	X		X	
21.	PDARS (Performance Data Analysis and Reporting System)							7					X	
22.	RCM (Reliability Centred Maintenance)		2	3			6			X		X		
23.	SADT (Structured Analysis		2							X	X			

[2] The methodologies EATMP SAM, ED78A, TOPAZ have already been considered in Section 3.

This project has been carried out under a contract awarded by the European Commission

		Stages								ATM concept aspects				
Technique		1 Scop	2 Oper	3 Hazid	4 Model	5 Risk	6 Mitig	7 Monit	8 Feed	Hw	Sw	Hu	Pr	Or
	and Design Technique)													
24.	SAFSIM (Safety in Simulations)			3		5						X	X	
25.	SFMEA (Software Failure Modes and Effects Analysis)			3						X	X			
26.	SIMMOD Pro				4							X	X	
27.	SMHA (State Machine Hazard Analysis)			3	4						X			
28.	TRACER-Lite (Predictive Technique for the Analysis of Cognitive Errors)			3			6					X		
29.	Use of Expert Judgement					5				X	X	X	X	
TOTAL		**2**	**4**	**15**	**6**	**11**	**5**	**5**	**4**	**17**	**10**	**19**	**13**	**4**
Percentage (TOTAL*100% / 52)		**4**	**7**	**30**	**10**	**22**	**10**	**10**	**7**	**63**	**38**	**69**	**47**	**16**

When looking at the number of techniques gathered in the database, one may conclude that there seems to be an uncontrolled growth in safety assessment techniques. An issue of concern also is that there seem to be few techniques that cover the first stage of the generic safety assessment process (Scope assessment) and the eighth stage (Communication and feedback).

4.2 Overview of approaches emerging for ATM

This section provides a short overview of ATM directed approaches that have more recently emerged that are of relevance for safety assessment in R&D projects. These newly emerging approaches are not yet widely used, and not completely stable (parts are subject to refinements). In line with this, they are not yet part of a training or education programme. They are the following:

- Safety Assessment Made Easier (SAME) ([SAME PT1, 2008], [Fowler et al., 2009]) is a method defined by EUROCONTROL as an extension of SAM by considering the positive contribution of the concept under investigation to aviation safety, in addition to the negative contribution to risk. SAME is also characterised by having the safety assessment driven by a safety argument structured according to system assurance objectives and activities. A detailed description of SAME is provided in Part 2, Appendix V.
- Safety Fundamentals [Safety Fundamentals, 2006] is a qualitative method for the preliminary evaluation of the main potential effects on safety of a new concept in terms of indicators of the impact on the safety regulation framework, safety performance, operational safety, and safety management. The method is intended for early feedback at the very initial stages of a concept development. A detailed description of Safety Fundamentals is provided in Part 2, Appendix VI.
- SAFMAC (Safety Validation of Major Changes, [Everdij et al., 2009]) provides a safety validation framework that emphasises the active roles and collaboration of multiple stakeholders during the development phases of air transport operations. The development of this safety validation framework started in [Everdij et al., 2006a] and is referred to as SAFMAC (SAFety validation of MAjor Changes), with involvement of NLR, LVNL, the Dutch

This project has been carried out under a contract awarded by the European Commission

Directorate General of Aviation and Maritime Affairs (DGLM) and Eurocontrol. A detailed description of SAFMAC is provided in Part 2, Appendix VII.

- Integrated Risk Picture (IRP) [Perrin et al., 2007] is a model from Eurocontrol aiming to show the relative safety priorities in the gate-to-gate ATM cycle. Both a baseline risk picture ('IRP 2005'); and future benchmark risk picture ('predicted') have been developed.
- Safety Targets Achievement Roadmap (STAR) [Vernon & Perrin, 2007] is a model from Eurocontrol aiming to keep track of joint effects on safety of multiple operational changes.
- Causal model for Air Transport Safety (CATS) [Ale et al., 2006] is a causal model developed with the aim of identifying weak spots in the aviation processes and assessing their effect on overall safety. The model has been developed by a consortium of Delft University of Technology, NLR, DNV, and White Queen.
- LVNL's safety risk apportioning approach: In [Van den Bos et al., 2009] the development of apportioned ATC safety criteria based on accident rates is presented. These criteria focus on Air Traffic Control-related accidents, which essentially correspond to the accidents ATC is to prevent and which can be objectively determined form accident data. The resulting overall ATC-related risk target is distributed over 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').
- Strategic Assessment of ATM R&D results (SARD) [SARD, 2008] process and criteria for the analysis of ATM R&D results per operational concept from a strategic view point. The set of criteria can be considered 'transition criteria' for determining whether and when operational concepts under validation can transfer to a next phase of E-OCVM's Concept Lifecycle Model. SARD is reviewed in Part 2, Appendix 8.
- Eurocontrol's Human Factor case [EATM HF case, 2007] is a process to systematically manage the identification and treatment of Human Factor issues as early as possible in a project's lifecycle.
- Controller Action Reliability Assessment (CARA) [Gibson & Kirwan, 2008] is a human reliability assessment technique, which can be used to quantify human performance in the context of Air Traffic Management (ATM).
- Investigation of a resilience engineering approach to ATM [Hollnagel et al., 2006]. Resilience engineering 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. In practice, there are two complementary streams of developments. One stream aims to maintain and improve the human cognition contribution to resilience [Hollnagel et al., 2006]. The other stream adopts a mathematical approach [Di Benedetto et al., 2008], which aims to enhance this human cognition contribution by using technological means that help the human in detecting and restoring from latent conditions which undermine the resilience effectiveness of human operators.
- Organizational safety modelling is investigated in [Stroeve et al., 2008]. It describes the development of an agent-based model for organizational safety, intending to support safety culture modelling and analysis.

4.3 Specific CAATS II emerging approaches

This section presents emerging approaches that have been developed by or with help of CAATS II. These approaches are not yet widely used, they are not yet stable and they are not part of a training or education programme. They are the following:

- Researchers responsible for SARD and for CAATS II jointly developed an improved and updated revision of SARD's detailed criteria [SARD v1.8, 2009]. In addition, CAATS II

This project has been carried out under a contract awarded by the European Commission

developed a draft proposal for a safety case specific extension of the SARD [CAATS II WP1.2 TC]. In Part 2, Appendix IV these sources are discussed.

- CAATS II developed a draft framework for defining and managing relations between cases in E-OCVM [CAATS II WP1.6 note], building further on initial work done in [CAATS II, D11]. Feedback to this framework was retrieved in the CAATS II second workshop [CAATS II WS2]. In Part 2, Appendix III these sources are discussed.

4.4 Overview of material emerging from SESAR

During the development, much material related to safety assessment in R&D projects emerged from the definition phase of the SESAR programme. This material consisted of six overall deliverables that summarized the main results from the work done, and of more detailed task deliverables. In Part 2 of this document a selection of relevant detailed task deliverables has been reviewed. The documents reviewed are described shortly in the following:

- SESAR Task 1.6.1/D1 "Study of safety regulatory framework" [SESAR WP1.6.1/ D1] gives an overview of the current ATM safety regulatory framework, and concludes that developing the ATM safety regulatory framework to provide a clear, unambiguous set of regulations integrated with the safety regulation of the other parts of the air transport industry will be essential to the success of SESAR.
- SESAR Task 1.6.1/D2 "Study of safety regulatory framework" [SESAR WP1.6.1/ D2] summarizes the basic principles of safety regulation, and presents a vision for the future of ATM safety regulation that addresses the issues identified for the current arrangements.
- SESAR Task 1.6.2/D3 "ATM safety regulation, SESAR Safety Screening & SESAR Concept" [SESAR WP1.6.2/ D3] investigates the different elements of the SESAR concepts with respect to the impact on and feasibility for safety regulation and the impact of the regulations on the elements of the SESAR concept. This is done by screening the concepts on Safety Fundamentals.
- SESAR Task 4.2.1/D6: "Safety management plan" [SESAR SMP] aims to provide an integrated approach to safety related activities to establish an aligned vision for the future of ATM safety that will meet the needs of all stakeholders, now and in the future. It does so by describing the key activities and elements to ensure that processes, responsibilities and expectations are clearly established to accompany the required continuous improvement of the safety performance of the future ATM environment.
- SESAR Task 4.2.1/D6: "Development strategy" [SESAR DS] aims to define in details the aim, the content and the SESAR Deliverables associated to every phase of a concept lifecycle model.
- SESAR Task 4.2.1/D6: "System engineering methodology" [SESAR SEM] aims to support the ATM technical definition by defining the common ATM system engineering methodological approach to be applied during the SESAR Development Phase, in line with [SESAR DS].
- SESAR Task 4.2.1/D6: "Concept validation methodology" [SESAR CVM] aims to define the use of E-OCVM, on which SESAR's Concept Validation Methodology (CVM) is based, on SESAR and to identify any enhancements that are required to address the complexity of the ATM Target Concept.
- SESAR Task 3.4.6/D5: "Regulatory and legislative planning" [SESAR RLP] aims to provide roadmaps for SESAR's 'Transversal Areas', which contribute to ensuring that SESAR's Operational Improvements will be defined, developed, deployed and operated in compliance with appropriate safety, security, environment, human performance & contingency requirements and objectives by applying appropriate related best practices.
- SESAR Task 4.1.12/D5-D6: "Master Plan Management Structures" [SESAR MPMS] aims to describe the necessary ATM Master Plan management structures and associated

This project has been carried out under a contract awarded by the European Commission

processes and to demonstrate how these processes may enable the cumulative commitment of all ATM stakeholders to be established and sustained.

The overall SESAR deliverable [SESAR D6] provides an overview of the SESAR Work Programme for 2008 to 2013.

This project has been carried out under a contract awarded by the European Commission

5. SAFETY ASSESSMENT IN R&D PROJECTS

This section explains the purpose and way of working of safety assessment in the specific context of R&D projects, also presenting briefly the concept maturity model of E-OCVM.

5.1 Safety assessment and concept lifecycle

The R&D community is continuously investigating new Operational Concepts that can advance the ATM services. These advancements include aspects such as increased throughput or capacity; reduction of environmental impact; increase in safety; and reduction of the air traffic service costs. The R&D community shall not only develop innovative ATM concepts, but also improve these concepts, and move these towards an operational status with a process of refinement and consolidation. The R&D community also has to provide adequate evidence that these concepts are able to deliver the planned enhancements while preserving or improving the overall system safety. This evidence shall demonstrate that new procedures can work safely in a real life environment while addressing the problems for which they were developed.

An operational concept has its own lifecycle during which the concept is continuously refined and improved. Different alternative versions of the concept can be considered, especially during the initial phases of the lifecycle. One of the aims of validation is to test these different versions and select those that are most promising for the later phases of the lifecycle. For European ATM R&D projects, the European Operational Concept Validation Methodology [E-OCVM, 2007] has become the reference framework for validation of ATM concepts. As part of such validation, safety assessment can identify preliminary feedback helpful to reduce the risks associated with a new concept and provide evidence for the safety of the concept. Quantity and characteristic of useful feedback, as well as the type of evidence, can differ, depending on the concept being at the very early stages of its lifecycle or being already well consolidated and mature. Ideally, the safety analysis should thus be tailored to the concept lifecycle, and the activities should be scoped on the basis of the maturity of the concept.

5.2 Concept Lifecycle Model proposed in E-OCVM

E-OCVM has been developed in a common effort of many European R&D organizations, supported by EUROCONTROL and the European Commission and in collaboration with United States Federal Aviation Administration. The aim of E-OCVM is to achieve consistency and to rationalise the validation work of ATM R&D projects. It is a reference of growing importance for the validation of ATM operational concepts in the European ATM R&D community. E-OCVM includes three aspects of validation that, when viewed together, help provide structure to an iterative and incremental approach to concept development and concept validation:

- The Concept Lifecycle Model (see Figure 5) facilitates the setting of appropriate validation objectives, the choice of evaluation techniques, shows how concept validation interfaces with product development and indicates where requirements should be determined;
- The Structured Planning Framework facilitates programme planning and transparency of the whole process; and
- The Case-Based Approach integrates many evaluation exercise results into key 'cases' that address stakeholder issues about ATM performance and behaviours.

This project has been carried out under a contract awarded by the European Commission

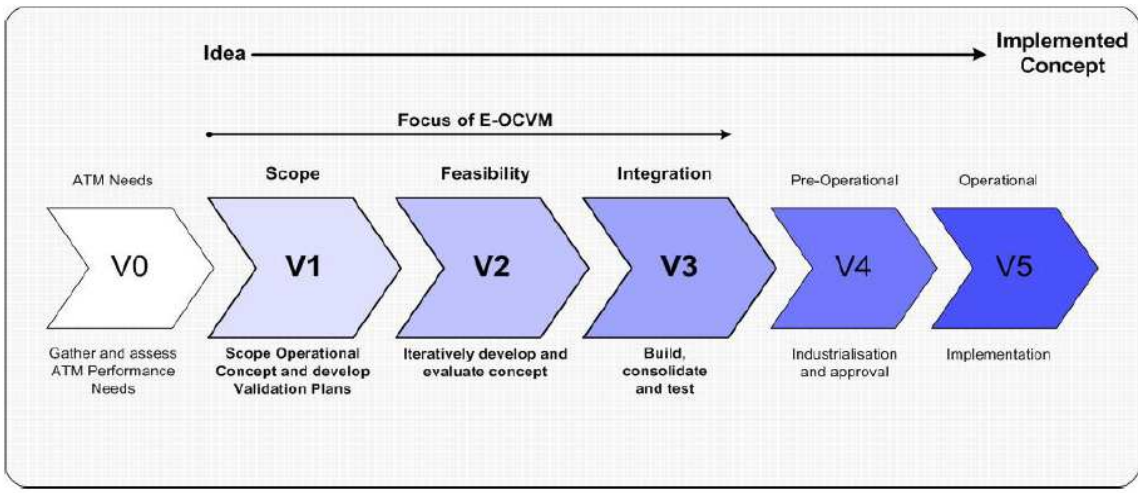


Figure 5 – E-OCVM's Concept Lifecycle Model

The concept lifecycle model promoted by E-OCVM (known also as concept maturity model), presents certain stages of development that need to be encountered by a concept before it can be considered as 'fit-for-purpose'. During the lifecycle of a concept it is proposed to have a few logical points where the progress of the concept towards an application are evaluated. These points naturally break the development of the concept into discrete phases. Projects are used as a mechanism for investigating specific aspects of the concept during specific lifecycle phases, for R&D particularly the early development phases. Figure 6 shows the three phases (V1 to V3) proposed by the E-OCVM concept maturity model as relevant for R&D projects, and describes them in some more detail.

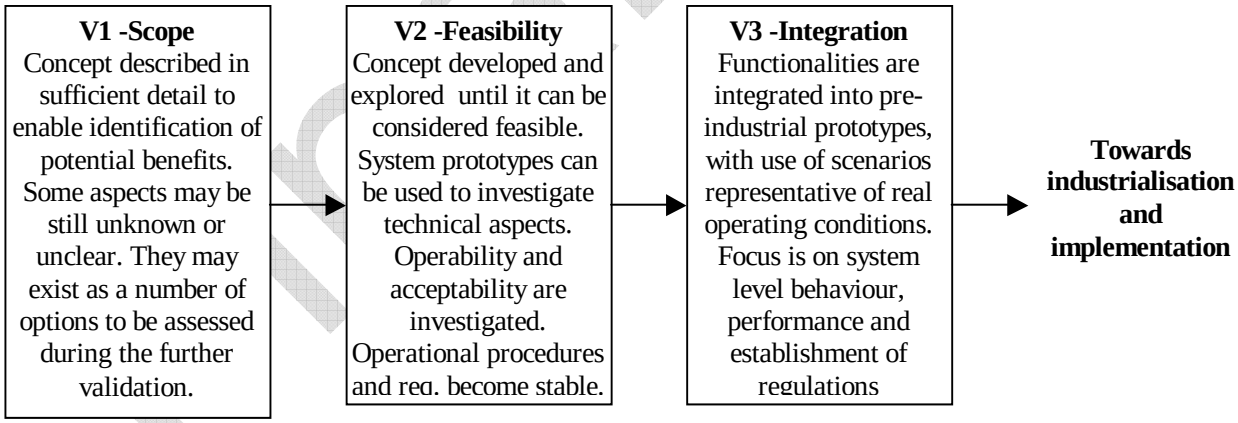


Figure 6 – Phases of the E-OCVM Concept Lifecycle model relevant for R&D projects

To clarify the issue, parallels can be drawn with the construction of a new car. Early mock-ups of 'concept cars' could be created to produce a more aerodynamic car, these mock-ups could be considered to understand if the new concept car can really bring benefits in terms of improved "air penetration" – this could be phase V1 above. This would support decisions about moving to prototyping the various component sub-systems. Then different projects would be created to develop brakes, engines and bodywork. The overall feasibility would be evaluated and this could be the equivalent of phase V2. At some point these would again be brought

This project has been carried out under a contract awarded by the European Commission

together as a prototype with greater fidelity than the mock-up but still not suitable to be industrialised. This would be used to ensure compatibility of the different aspects before further engineering commenced. Such a test could be considered as a point equivalent to the end of one of the lifecycle phases shown above.

The complexity of developing and moving into operation new ATM operational concepts generally exposes too many issues for one project to handle successfully. E-OCVM is based upon such development practise, and delivers the opportunity to have multiple R&D projects to design, build, test and evaluate a concept into a working application that can be industrialised. A real example of two large R&D projects contributing to the development of a concept at different levels of its maturity process is shown in figure 7.

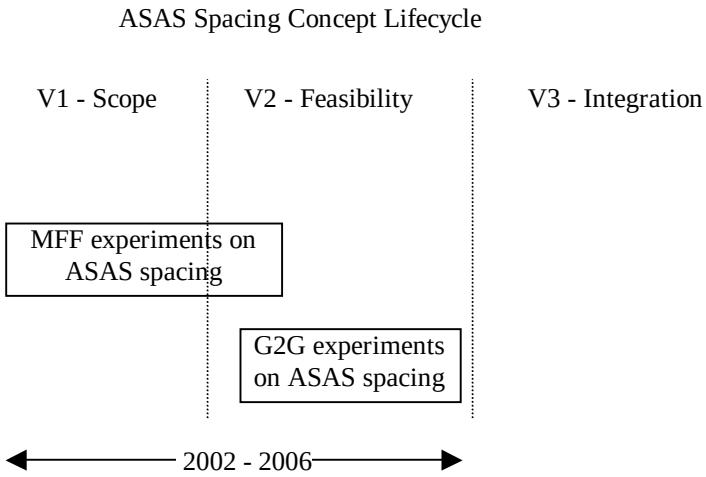


Figure 7 – Lifecycle of the ASAS Spacing concept with contribution of two R&D projects

The whole process is described as concept validation and it relies on co-ordination between the projects developing different aspects as well as the support of suitable integration tests in order to ensure the end application is fit for purpose

The introduction of the principle of a concept lifecycle model within E-OCVM has had two main objectives, one has been to provide a transparent structure to the ad hoc development process applied to ATM concepts, and the second has been to use that structure as a means to identify development and validation objectives appropriate to the state of maturity. A typical R&D project investigates concepts between level V1 and V3 of E-OCVM, while more mature concepts are usually addressed by development and implementation projects.

This project has been carried out under a contract awarded by the European Commission

5.3 Tailoring safety analysis to concept maturity

At the initial stages of the lifecycle (e.g. V1) a concept is still far from consolidated, there are often a number of possible technological and procedural solutions to be considered, and many aspects can not yet be defined. In these conditions the results of the safety analysis can only be preliminary. However, it is very important to have preliminary safety analysis feedback about the risks implied with the implementation of the concept because at this stage such feedback can relatively easily be taken into consideration, in making significant concept changes and in selecting the technological and procedural options with less risk of eventually leading to unsuccessful deployment. An example of projects considered for this analysis is reported in Part 2, Appendix I, while the different maturity levels of the concepts of these projects is evidenced in Part 2, Appendix II, Table II.1.

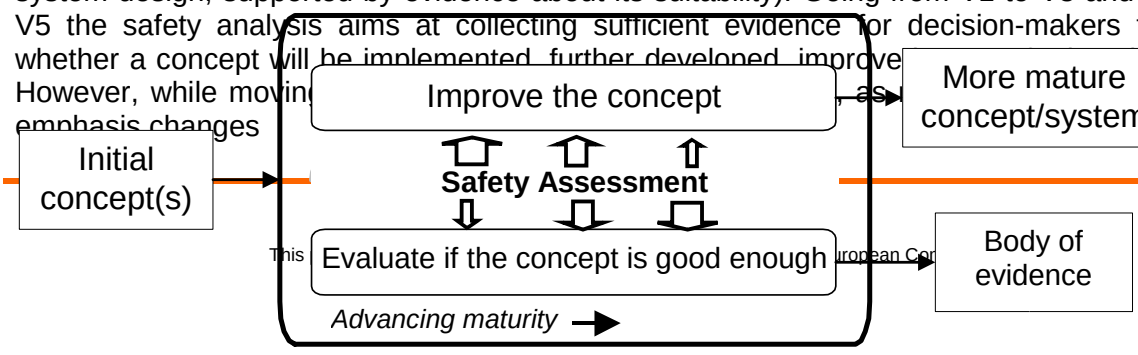
On the contrary, when the concept is more stable and mature (e.g. at the level V3), there are already industrial prototypes and well defined and consolidated scenarios of usage. This allows the collection of more formal evidence about safety, useful for the following phases of the safety assessment and for the safety case, while it is less easy to influence the overall concept design with safety feedback.

Tables II.2 to II.5 of Appendix I shows the approaches to safety assessment for different R&D projects at different phases of the concept lifecycle model. The different levels of consolidation of the concept would require a safety analysis that is tailored to the maturity level, however there is little experience about this tailoring activity at the moment, and little support available. The safety analysis approach of a more mature operational concept, ready for implementation, is already consolidated with relatively stable requirements and methodological references. This is not the case when safety analysis refers to R&D projects investigating concepts at the maturity level V1, V2, and V3 of E-OCVM maturity model. At these maturity levels there is not yet a consolidated solution, and there is not a standardised support to tailor safety assessment on the basis of the concept maturity.

5.4 Providing feedback versus assuring safety

The concept evolves while moving through the maturity levels (V1, V2, and V3). Often several different options of the concept are considered and only the most promising are investigated more in depth. The role of safety assessment should be very active in this process to help understanding and **IMPROVING** the most promising and safe options, and to discard those affected by major or "expensive to solve" safety problems. Then, in research projects there is a strong need for early feedback. In addition, during this process the concept is much more in evolution than in V4 and V5. Specific technical solutions are not yet identified, not all the assumptions are verified at the same level of depth, operational aspects are not fully investigated. This need for early feedback combined with a much more “fuzzy and evolving concept” means that the type of evidence cannot be the same that can be provided while in V4 and V5. One cannot use the same analysis techniques or have the same level of consolidation and the same confidence in the results.

The balance of the assessment will change, as the project seeks to turn the input (some sort of idea or immature concept) into the output (a related, better defined and more robust concept or system design, supported by evidence about its suitability). Going from V1 to V3 and further to V5 the safety analysis aims at collecting sufficient evidence for decision-makers to decide whether a concept will be implemented, further developed, improve[illegible]eloped. However, while movin[illegible], as[illegible]e 8, the emphasis changes



- From providing early feedback for major design improvement and preliminary evidence the concept could be safe
- To collect sufficient information that the concept as finally developed and implemented, is acceptably safe. This means that the underlying concept is safe, that the design is complete, that the system is safe under all conditions, and that the design is robust against abnormalities.

Figure 8 – Focus of the assessment during the concept lifecycle

This different emphasis can also be seen going from Table II.2 (related to maturity level V0) to II.5 (maturity level V3) of Appendix II.

5.5 Fostering re-use of safety results in R&D

We have seen that multiple research projects can contribute to the validation of the same concept. The sequence of these projects can ensure that the concept becomes more stable and mature and progresses along its lifecycle. In such a context re-use of safety results, obtained from previous projects investigating the same concept, becomes of paramount importance to contain the costs of safety assessment and to take into account the safety feedback and recommendations of previous investigators.

However, there has been a dramatic lack of methodologies and tools to foster re-usability of project results. Knowledge is linked to people, and the main channel, to re-use the results of past projects is to involve the teams that obtained those results. As an example we can consider the two projects introduced above. In the MFF safety assessment one of the major hazards was considered the target misidentification by the delegated aircraft. The existing fallback procedure, which consisted of the delegated read-back of the target position, was considered not adequate to prevent this hazard, especially if there were more than one potential target in the vicinity with similar identification code. Moreover, the read-back was sometimes left out without the controller detecting the omission. A target misidentification could have critical consequences as the delegated may inadvertently loose separation with third party traffic. This hazard was irrelevant during the G2G Real Time Simulation because of the automatic up-link of the target identification data. As a consequence several of the most severe possible consequences considered in MFF disappeared. This very important result passed almost inadvertently because the piece of equipment providing the automatic up-link was already embedded in the G2G technical platform, and not added as a consequence of a specific safety requirement. Then, the importance of having an automatic up-link would have been under evaluated. This was not the case only because of the presence in the safety team of the same staff already involved in MFF, who could appreciate the difference and the significant safety benefits due to this piece of equipment.

Another reason limiting the re-usability of results across different projects is the presence of project related assumptions. Assumptions are an essential and unavoidable element of safety analysis. They are often necessary to provide a frame for the evaluation process, but, they can also have a powerful effect on the conclusions of the safety analysis that should not be underestimated. Different projects tend to have different assumptions, and often the implications of those assumptions are not adequately investigated. In addition, some assumptions that are reasonable at the beginning of the project may turn out to be inappropriate at a later stage or when the results are moved from one project to another. Assumptions are also often used to determine the boundaries of the operational environment and of the system under analysis. It is difficult to conduct safety analysis without knowing what the operation is going to look like. The

This project has been carried out under a contract awarded by the European Commission

project must specify the scope of the safety analysis and pertinent information as what part of the ATM system is relevant for the safety analysis and where the operation boundaries are considered to be. However, it is not uncommon in the early phases of a concept lifecycle that the operational environment evolves. All these reasons may influence significantly the possibility to re-use results of previous projects.

A set of conditions are needed to facilitate the re-use of safety results across different projects. These conditions are listed in the following.

1. Formal identification of the system under analysis and of the operational conditions considered. If the extent of the safety analysis is not well defined potential future users of the analysis results will not be in condition to understand what has been included. Possible examples of questions concerning the identification of the system are: is the software considered as part of the system and are its potential failures included in the analysis? Is the concerned aerial part (and the possible pilot behaviour) considered?
2. Definition of the assumptions and of their implications. Assumptions are an essential and unavoidable element of safety analysis. They are often necessary to provide a frame for the evaluation process, but, they can also have a powerful effect on the conclusions of the safety analysis that should not be underestimated. The introduction of unmotivated assumptions in safety analysis is a widely recognised issue in the scientific literature [Tversky & Kahneman, 1974]. Different projects tend to have different assumptions, and often the implications of those assumptions are not adequately investigated. A clear definition of the assumptions adopted and an analysis of their implication are essentials to allow re-usability of results.
3. Standardised assessment methods. A standardised assessment method would facilitate a better understanding of the extent and type of analysis done to experts not directly involved in the assessment activities. In addition, a standardised assessment method allowing to partition the analysis, would allow a more direct and substantial re-use of the analysis of those system/concept components that are not changed during the concept evolution.
4. Use of standard templates. The adoption of standard templates would facilitate the identification of the issues of importance in a usually wide, and not easy to browse, software analysis documentation, especially with regard to lessons learnt. This would facilitate communication and mutual, easy, understanding.
5. Public repositories of safety assessment results. Public repositories would be needed to store safety assessment results in a standardised format, and to allow an easy identification of the issues of relevance.

We will discuss in the following what is available or under development to help safety analysts in satisfying each of conditions presented above.

Formal identification of the system – Models have been used, in the ATM and aeronautical domain, to facilitate the understanding of the system functions and architectures. The primary purpose of these models is usually to support the design of the system and the definition of its architectural, and sometime functional, requirements. However, some of these models can also support the formal identification of the system, to determine the part considered in the safety analysis. Even a ConOps can be considered a kind of system model because they describe the system in terms of humans, procedures and equipments in relation to the environment. Different possible system configuration can be considered through ConOps whose different versions may represent different system options, and over time ConOps versions may be more and more detailed.

This project has been carried out under a contract awarded by the European Commission

An example, borrowed from other domains of application is the UML based models used in the CORE project [Dorbes et al., 2001]. The Unified Modelling Language (UML) is an open method used to specify, visualise, construct and document the artefacts of a system under development. UML offers a standard way to describe the system, including its conceptual components such as: actors, business processes and system's components, and activities as well as concrete things such as: software, hardware, and tools. A more specific, safety oriented model, is proposed for example in [Jacobson et al., 2009]. The Operational Process Model (OPM) is a functional model representing graphically socio-technical systems for safety analysis, applied to evaluate changes introduced in the aviation domain.

However, none of these models has been used explicitly to understand the extent of the safety assessment, that is, to identify what components have been considered as part of the system during the analysis and what have been excluded from it, and further research to understand their applicability for this specific purpose would be needed.

Definition of the assumptions and of their implications. Little work has been done to support a clear definition of assumptions (e.g. template for their definition, main elements to consider, how to discuss their credibility) and analyse their implication (e.g. impact of the assumption on the system, how to estimate the effect of possible assumption violations). Some results are available from works aimed at re-using the structure of safety cases, in other domains of application, see for example reference [Kelly & McDermid, 1997]. In this work the author discuss how to structure the assumptions in a standard format in the context of safety argument reasoning. The aim is to avoid infringements of critical assumptions due to changes in the context of a safety argument, leading to inappropriate reuse of patterns in safety cases.

Standardised assessment methods – SAM is one of the standard safety assessment methods in use for R&D projects. However, it is used in several cases but with different modalities that do not allow an exact understanding of the extent of the work done when using it. Some authors suggests that possibilities could arrive with a wide adoption of an argument based approach. The evidence that has been used to demonstrate an argument, could be re-used in other systems if the argument remain the same. Some experiments in this direction have been tried by NATS, see for example the reference [Bush & Finkelstein, 2001] and [Bush, 2001]. In these works the authors examine the current state of tools and techniques, and finds that some of the pre-requisites that need to be satisfied for ensuring an effective safety case re-use can be met. However, further development of practice is required in the area of tools, process and customer/supplier relations. The authors combine a typical system engineering lifecycle with a typical safety case development process and show how the tasks and activities of a Safety Engineer practising safety case artefact reuse would fit in, and the use that engineer might make of the safety case repository at each stage. The "broader approach to safety assessment" proposed in SAME represents an argument based systems-engineering approach to safety assessment and as such it is a contribution in response to the need of standardisation.

Use of standard templates – Several guidelines and studies are available to support the preparation of documents, especially those concerned with writing templates for technical documents and for reporting lessons learnt. Of particular reference we consider [DOE, 2003], and [NAS, 2008]. The lessons considered in the first two references are mainly related to operational problems and not to validation, however the way suggested for the organisation of the report, the general writing tips and the list of topics to be included, are fully applicable. The "broader approach to safety assessment" proposed in SAME involves a standard safety argument template, which hosts the safety evidence collected while going from V0 to V3. Would two teams work in parallel, on two alternatives of a concept, that structure allows easy

This project has been carried out under a contract awarded by the European Commission

comparison of safety relevant feedback. The same applies when a team hands over the work done by a previous one.

Public repositories of safety assessment results – There is one concrete example of public repository for validation results coming from ATM R&D projects, called Validation Data Repository (VDR), hosted and managed by EUROCONTROL [Harvey et al., 2002]. VDR is not specifically addressed to safety but rather a repository of information about Validation Exercises in R&D project, with their objectives, methods, design, metrics, results and findings. This information is mapped to standard reference lists to enable sorting, filtering and searching by a number of parameters such as Key Performance Areas, Operational Improvements and Validation Techniques. It was developed in close liaison with the development of the validation methodology under MAEVA and is the recommended validation information tool by E-OCVM [E-OCVM, 2007]. VDR captures Validation Objectives hierarchy to provide a framework against which the context of the validation exercises could be mapped. At the moment VDR contains the results of several European R&D projects with details of findings in terms of results, conclusions and recommendations and the links between them.

An initiative dedicated to safety is Skybrary. Skybrary is an electronic repository of safety data related to ATM and aviation safety in general. It is built of a hyperlinked network of articles, and is supported and developed by a partnership that includes Eurocontrol, ICAO and Flight Safety Foundation. The objective of Skybrary is to make available a source of information and reference for anyone interested in aviation safety. Being a single and most comprehensive portal for access to the available aviation safety data it should also serve as an “easy-to-find” tool for experts and aviation professionals. Skybrary is accessible via the web site www.skybrary.aero. In the future a new section called SAsbrary (Safety Assessment library) will be developed and will be the Safety assessment repository of the Safety Cases.

This project has been carried out under a contract awarded by the European Commission

6. EMERGING NEEDS FOR SAFETY ASSESSMENT IN R&D

Purpose of this chapter is to present an overview of identified additional needs that emerge for safety assessment in R&D for advanced developments such as aimed for by SESAR. These emerging needs have been identified in the review of sources documented in Appendix I (Part 2 of this document). This review considered the relevant detailed SESAR task deliverables (among which the SESAR Safety Management Plan [SESAR SMP]) and relevant documents from other research projects.

The emerging needs identified by SESAR receive focus in the remainder of this document. Therefore, in Section 6.1 the SESAR identified emerging needs are first collected and summarized. Review of sources other than SESAR revealed confirmation of several of the SESAR identified emerging needs and identification of complementary emerging needs; these are presented in Section 6.2.

6.1 Emerging needs identified by SESAR

In this section the SESAR-identified emerging needs are introduced, as they follow from the SESAR source documents from which they were identified. First, these emerging needs are listed, including the relevant SESAR source and the reference to its identification in Part 2 of this document:

Table 4 – Overview of emerging needs identified by SESAR

Id.	Description of emerging need	Source	Relevant appendix in Part 2
A.	The need for a 'macro' safety case	[SESAR SMP]	Appendix I.6
B.	The need to address safety regulations	[SESAR WP1.6.1/D1]	Appendix I.2
C.	The need to address the multi-stakeholder nature of advancing air traffic operations	[SESAR WP1.6.2/D3]	Appendix I.2
D.	The need to address the success side of a change	[SESAR SMP]	Appendix I.6
E.	The need to cover performance of human operators	[SESAR SMP]	Appendix I.6
F.	The need to identify unknown 'emergent' risks	[SESAR SMP]	Appendix I.6
G.	The need to address E-OCVM requirements	[SESAR CVM]	Appendix I.5
H.	The need to assess concept maturity	[SESAR DS]	Appendix I.3
I.	The need for managing relations between cases	[SESAR RLP]	Appendix I.7

The need for a 'macro' safety case (A) – In aviation and ATM industry safety assessments have focused on individual concept elements, rather than on the joint effect on safety of multiple changes in air traffic operations. SESAR is defining advanced developments to air traffic operations, consisting of multiple local changes by various stakeholders. As the relations and interactions between such individual operational changes need to be properly assessed, the need for a 'macro' safety case is identified in [SESAR SMP]. This is to be accompanied by an approach in defining suitable safety targets at a suitable level for the macro case.

The need to address safety regulations (B) – 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. Main conclusion of [SESAR WP1.6.1/ D1] is that developing the ATM safety regulatory framework will be essential to the success of SESAR. This improvement should be aimed at providing a clear,

This project has been carried out under a contract awarded by the European Commission

unambiguous set of regulations integrated with the safety regulation of the other parts of the air transport industry. Main issues are in the field of:

- Fragmentation and variability in regulations and their interpretation.
- Safety accountability: The complex safety regulatory framework and the often detailed and prescriptive nature of safety regulations can result in confusion over safety accountability;
- Duplication of regulations: overlap and contradictions leading to confusion and difficulty;
- Complexity of regulation, leading to difficulty to comply;
- Transparency, as ATM regulations are frequently too detailed and prescriptive in nature;
- Harmonisation of industry regulation, with a lack of harmonisation in safety regulation in air transport, while conflicts in regulatory requirements could lead to safety being compromised;
- Proportionality and cost effectiveness: it is not possible to determine whether ATM safety regulation is cost-effective, nor whether resources are being deployed in a way that will minimise risk.

In summary, safety regulations need to be properly addressed.

The need to address the multi-stakeholder nature of advancing air traffic operations (C) – The SESAR operational concept will introduce significant changes to the way in which ATM is performed. The concept will fundamentally change the roles of many of the stakeholders in the ATM system and, importantly, these roles will change dynamically within the operation as a flight progresses. This will result in new ATM safety responsibilities and new interfaces between stakeholders. Examples of such changes are in the field of:

- Airspace Organisation & Management;
- Separation Provision
- Collision Avoidance

Necessary precautions should thus be taken to ensure an appropriate approach towards safety for SESAR in its widest sense, to enable an acceptably safe implementation of the SESAR concepts, to minimize SESAR project risks and related costs, and to support the EC and SJU in their respective requirements to provide information and the discharge of their explicit responsibilities and accountability towards safety in ATM. From these conclusions from [SESAR WP1.6.2/ D3] the emerging need is identified to properly address the multi-stakeholder-nature of advancing air traffic operations.

The need to address the success side of a change (D) – In aviation and ATM industry safety assessments have focused on what happens if a new or changed system fails in some way. The potential positive contribution of the change is often left unaddressed. Similarly, instead of focusing on failures of ATM only, the positive contribution of SESAR to aviation safety should also be considered. Therefore, [SESAR SMP] the need is identified to address the success side of a change.

The need to cover performance of human operators (E) – In future concepts proposed by SESAR, ATM will remain to be driven by the role of human operators. Therefore the safety of air traffic operations will remain to depend on the role of human operators. So far, many safety techniques have not comprehensively covered for the role of the human operators in the ATM system [SESAR SMP]. There is thus a need to cover performance of human operators appropriately in safety assessments.

The need to identify unknown 'emergent' risks (F) – With the introduction of advanced developments as aimed for by SESAR, yet unknown 'emergent' risk may appear. New behaviour and new hazards will emerge that have not yet been seen in ATM. As hazard

This project has been carried out under a contract awarded by the European Commission

identification is a crucial step in safety assessments, the need to identify unknown 'emergent' risks is identified from [SESAR SMP].

The need to address E-OCVM requirements (G) – [SESAR CVM] identifies E-OCVM as a common approach to all projects contributing to the validation of operational concepts, and takes it as the basis of the SESAR concept validation methodology. As safety assessment in R&D is done as part of a general validation process, there is a need to address E-OCVM requirements. In particular, E-OCVM puts requirements on the output of safety case development at the end of the phases V0, V1, V2, and V3 of the validation process.

The need to assess concept maturity (H) – E-OCVM provides a sound common foundation for the lifecycle definition of R&D projects that begin since the very early immature concepts and develop until late stages of implementation. In [SESAR DS] it is put forward that it is essential to assess the level of maturity of the subject of the lifecycle before moving to the next phase in the lifecycle, and that decision points should be established to assess the level of maturity and to decide whether to go through the next phase. Accordingly, there is a need to assess concept maturity.

The need for managing relations between cases (I) – In [SESAR RLP], the need for an integrated management approach is identified which manages safety and other performance areas as business and environment in an integrated way. In the R&D phases, management of performance is organized via E-OCVM's case-based approach, in which cases are used to

- Provide preliminary feedback helpful to reduce the risks associated with a new concept; and
- Structure the evidence into a presentable format that helps stakeholders identify the answers to their key questions.

Cases are usually managed by specialists in the domain investigated, for example, the human factor case is managed by specialists on human factor, safety case by safety analysts and so on. In addition, the different domains have different methods and techniques, usually at different levels of consolidation. The consequence of this partition of the work, together with the different levels of maturity of methods and techniques, can be a complete separation of cases from each other. Accordingly, there is a need to manage relations between cases.

6.2 Emerging needs identified by other sources

As has become clear from the review in Part 2, there are a few other sources that identified independently of SESAR emerging needs for safety assessment in R&D for advanced developments. These sources confirmed several of the SESAR-identified emerging needs, and a number of complementary emerging needs, which are introduced in the current subsection. In the following table they are first listed (including relevant source and reference to its identification in Part 2 of this document):

Table 5 – Overview of complementary emerging needs identified by sources other than SESAR

Id.	Description of complementary emerging need	Source	Relevant appendix in Part 2
a.	The need for support for 'scoping of safety assessment'	[CAATS, D1.4]	Appendix I.9
b.	The need for support for 'feedback to operations, assessment and design'	[CAATS, D1.4]	Appendix I.9
c.	The need to cover organisational aspects	[CAATS, D1.4]	Appendix I.9

This project has been carried out under a contract awarded by the European Commission

d.	The need for joint validation of multiple actors requirements	[Everdij et al., 2009]	Appendix I.13
e.	The need to take into account the role of government policy makers	[Everdij et al., 2009]	Appendix I.13
f.	The need to determine the quality of safety validation	[Everdij & Blom, 2007]	Appendix I.13
g.	The need to address challenges posed to safety validation by concepts aiming for separation reduction	[RESET, 2007]	Appendix I.14
h.	The need to pro-actively consider safety performance, operational safety, safety management early in the development lifecycle of the operational concept	[Safety Fundamentals, 2006]	Appendix I.16.

The need for support for 'scoping of safety assessment' (a) – In [CAATS, D1.4 P2] it is identified that the key role of the "Scoping the assessment" stage of AP15's generic safety assessment process is often heavily underestimated. Poor scoping may lead to great concerns as miscommunication with stakeholders, confusion during the safety assessment process, inefficiency of safety assessment iterations; and selecting an inappropriate safety assessment method. Therefore the need for support of this step is identified.

The need for support for 'feedback to operations, assessment and design' (b) – Another step of AP15's generic safety assessment process that is often heavily underestimated is the 'feedback to operations, assessment and design' step. Lack of such feedback may lead to poor management of safety in ATM, also in the R&D process, where safety assessment feedback should enable developers to improve their concepts, and decision-makers to make optimal decisions on further development. The need for support for this step is identified in [CAATS, D1.4 P2].

The need to cover organisational aspects (c) – In aviation and ATM industry safety assessments have rarely considered organisational aspects. Some examples of organisational aspects are: behaviour of individuals, crew and team resource management, company culture, training of operational staff and safety experts, maintenance of procedures, and tactical and strategic information patterns (i.e., who knows what and how, and in time, and in line with roles and responsibilities?). In [CAATS, D1.4 P2] the need to cover such organisational aspects is identified.

The need for joint validation of multiple actors requirements (d) – In safety assessment, safety requirements posed should be validated, i.e., it should be considered whether the safety requirements are feasible and whether they enable reaching the safety goal set. In the development of SAFMAC [Everdij et al., 2009] it is identified that due to the high complexity of air traffic management and the multiple stakeholders vested interests, in practice it is even more demanding to set joint goals for all stakeholders together, let alone start with requirements that are validated against the joint goal setting. As none of the established approaches handles this, SAFMAC identifies this as an emerging need.

The need to take into account the role of government policy makers (e) – The government forms a special type of stakeholder. In addition to having regular stakeholder roles, it has a role as visionary policy maker for its people. For major changes in air transport operations, the role of the policy maker is of particular relevance due to the part they play as investors in infrastructure and in coordinating with neighbouring countries. In some situations, the policy maker is also the national regulator, who has a special additional role in major changes. From

This project has been carried out under a contract awarded by the European Commission

this, [Everdij et al., 2009] identifies the need to take into account the role of government policy makers. It notes that the only elements that are arranged are the certifying authorities, but these have no role to play in the economic judgement.

The need to determine the quality of safety validation (f) – Safety assessment and validation of large changes in air traffic can be done in different ways, and the quality of the result will depend on, e.g., how the process is done, on the quality of the input and the experts used, which safety issues were evaluated, et cetera. Advantage can be taken of the many methods available in the database of safety methods [Safety Methods Database] introduced in Section 4.1. Based on practical experience in using this database for the search of relevant safety methods, the need is identified in [Everdij & Blom, 2007] for the development of an appropriate set of safety validation quality indicators, which should help such searching.

The need to address challenges posed to safety validation by concepts aiming for separation reduction (g) – Safety assessment for concepts involving the definition or re-definition of minimum separation minima put specific demands on the safety assessment approach to be applied. As an example [RESET, 2007] identifies the desired output of such safety assessments is often in the form of a curve of safety risk as a function of the minimum separation value, which is compared to the applicable Target Level of Safety, and of an explanation of the background of the shape of this function. From this, the need to address challenges posed to safety validation by concepts aiming for separation reduction is identified.

The need to pro-actively consider safety performance, operational safety, safety management early in the development lifecycle of the operational concept (h) – In [Safety Fundamentals, 2006], that there is a need to involve safety appropriately early in the design of new concepts, as the effects of lacking pro-activeness include quick-fixes of problems wthat bring new problems, cost intensive technical fixes or even restarting of the concept development phase, and delay of project delivery. Safety should be proactively considered in four aspects: Safety performance (addressing total system safety, including relations and interactions between all sub-parts), Operational safety aspects (addressing the joint performance of static and dynamic aspects including humans, procedures and technical systems), Management of the performance (addressing the role of the organisation and its management in achieving safety), and Safety regulation (addressing the legal framework). In complement to need (B) discussed in Section 6.1, from this the need is identified to pro-actively consider safety performance, operational safety, and safety management early in the development lifecycle of the operational concept.

This project has been carried out under a contract awarded by the European Commission

7. APPROACHES IN SUPPORT OF SESAR-IDENTIFIED EMERGING NEEDS

This section presents identified approaches that aim to address the SESAR-identified emerging needs. These can both be current approaches and newly emerging approaches. They are presented per emerging need.

7.1 Approaches for a 'macro' safety case (A)

There is a need for a 'macro' safety case, which has a dual character: at one hand interactions between different operational improvements need to be analysed on safety, at the other hand suitable safety targets need to be defined for parts of the novel operation. The following complementary approaches have been identified towards this:

1. Integrated Risk Picture (IRP), as an overall incident-accident model of the ATM system organizing and integrating safety assessments for individual operational changes;
2. Apportioned ATC safety criteria based on accident rates [Van den Bos et al., 2009]; and
3. Performing 'joint safety analysis' using TOPAZ.

Re 1: In [Fowler et al., 2009] it is explained how an Integrated Risk Picture (IRP) is used for the SESAR operational concept as overall incident-accident model of the ATM system. This way, safety assessments for individual operational changes are organized and integrated, covering their functional interactions and common causes. Accordingly, this forms a top-down approach considering the ATM system as a whole, complementing a bottom-up approach to assess risks associated to hazards that are either affected or newly generated by the introduction of each individual operational change.
IRP is introduced in more detail in [Perrin et al., 2007], where it is explained how a 'baseline' (IRP 2005) and a future risk picture ('predicted') version of IRP have been developed. The 'predicted' version aims to model the safety impacts of all known ATM changes, leading to an indication whether the safety targets can be achieved, and enabling apportionment of an overall safety target based on the overall ATM contribution to aviation accident risks, by assuming the modelled performance of individual ATM elements as safety objectives for safety assessments for individual operational changes. To ensure safety also between the baseline and the eventually foreseen situation, the use of IRP is complemented by a 'Safety Targets Achievement Roadmap' [Vernon & Perrin, 2007], which takes into account traffic growth and the foreseen implementation planning.

Re 2: In [Van den Bos et al., 2009] apportioned ATC safety criteria are presented that are based on accident rates. The focus is on 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'). Individual safety assessments consider one or more operational improvements and connect to the level of the ATC-sub products.

Re 3: TOPAZ has been developed for 'joint safety analysis' of advanced air traffic operations. It addresses all types of safety issues, including organizational, environmental, human-related and other hazards, and any of their combinations. Notably, it also considers all relevant stakeholders in an integrated way, enabling to cover well interactions such as between pilots an Air Traffic Controllers. 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 a simulation, to rerun

This project has been carried out under a contract awarded by the European Commission

simulations with adapted parameter settings, and to cover it via an advanced bias and uncertainty assessment.

7.2 Approaches to address safety regulations (B)

As significant issues exist with respect to the current regulatory framework, there is a need to address safety regulations in safety assessment in R&D. The following approaches have been identified for this:

1. Methods for early scanning of concepts on Safety Fundamentals;
2. Identification of complementary regulation needs, and showing via safety assessment the impact of improving standing regulations or not.
3. Performing safety assessment assuming current regulations, and laying down needs for changes in assumptions.

Re 1: Safety Fundamentals [Safety Fundamentals, 2006] reflect a framework of basic safety rules that are independent from the design implementation. The main four aspects of safety considered in this framework are safety regulation, safety management, operational safety and safety performance. An early scanning on safety fundamentals can be used to pro-actively consider safety early in the development lifecycle of an operational concept, potentially leading to amongst others the identification of needed or anticipated changes in safety regulations. Hence, early scanning on safety fundamentals helps in properly addressing safety regulations in concept development and validation. A detailed description of Safety Fundamentals is provided in Part 2, Appendix VI.

There are a few specific methods designed to support the analysis of Safety Fundamentals, usually based on structured elicitation of expert opinion. These include

- Safety Screening, which has been used during the application of Safety Fundamentals to new SESAR concepts in the SESAR initial phases ([SESAR 1.6.2/D3], [Strater et al., 2007]), and
- Safety Scanning developed in form of tool by the EUROCONTROL Safety Regulation Commission (SRC) in collaboration with several ANSP to support the NSAs in safety regulatory reviews.

Re 2: In the draft [RESET, 2009] it is argued that identified needs for improvement of the safety regulatory framework impact safety assessment in R&D. A concept under study in R&D will eventually need to be proven sufficiently safe according to the safety regulatory framework that will be in force at the time of certification and implementation of the concept. A concept will thus have to show that it satisfies the requirements of a future safety regulatory framework. As this future safety regulatory framework is not yet available, this forms a 'moving target' for safety assessment in R&D. It is not straightforward to deal with this moving target for safety assessment in R&D. In the draft [RESET, 2009], it is first identified which changes are needed in the safety regulatory framework to enable successful development of considered concepts with decreased separation. Next, safety assessment is proposed according to current requirements and requirements from anticipated changes in regulations.

As an example of such anticipated change, [RESET, 2007] identifies that the current ESARR and ICAO have in common that their current approach is conservative regarding airborne safety nets, in the sense that both assume that the safety risk impact is not taken into account, neither in the safety target nor in the safety risk assessment. The consequence of this is that developments in airborne safety nets and in improving collaboration between airborne and ground based safety nets would be discouraged. Accordingly, [RESET, 2007] recommends both ICAO and SRC to further develop their regulation regarding safety nets.

This project has been carried out under a contract awarded by the European Commission

Re 3: In [SESAR SMP] it is proposed to perform safety assessment in line with current regulations. For items not yet covered by current regulations it proposes to work with assumptions and safety requirements, which may next be adopted in complementary regulation.

7.3 Approaches to address the multi-stakeholder nature of advancing air traffic operations (C)

Advanced concepts will fundamentally change the roles of many of the stakeholders in the ATM system and, importantly, these roles will change dynamically within the operation as a flight progresses. Therefore there is a need to address the multi-stakeholder nature of advancing air traffic operations. SAFMAC has been identified as approach that aims to address this need:

SAFMAC [Everdij et al., 2009] is a safety validation framework, which has been developed to incorporate into safety validation the active roles that have to be played by stakeholders during the development phases 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' organisations 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), conops versions are developed to reach these goals (plan), the consequences for the stakeholders are identified (act), and the conops version is jointly validated (joint safety validation). The joint safety validation should make sure that emergent behaviour from interactions between the stakeholders is properly addressed. It is noted that the TOPAZ methodology has been used since its development for such joint safety validation. A detailed description of SAFMAC is provided in Part 2, Appendix VII.

7.4 Approaches to address the success side of a change (D)

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. The following approaches have been identified for this:

1. TOPAZ; and
2. SAME.

Re 1: Since its development the safety assessment methodology TOPAZ considers success and failure in an integrated way, and hence 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 modelled 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.

Re 2: Safety Assessment Made Easier (SAME) ([SAME PT1, 2008], [Fowler et al., 2007]) is developed by EUROCONTROL as an extension of SAM. Where SAM focused on the negative contribution to risk, SAME also considers the positive contribution of the concept under investigation to aviation safety. It does this by proposing a 'broader approach to safety assessment', consisting of complementary success and failure approaches:

- The success approach seeks to show that an ATM system will be acceptably safe in the 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.

In SAME the safety assessment is driven by a safety argument structured according to system assurance objectives and activities. In [Fowler et al., 2009] the use of SAME for the SESAR

This project has been carried out under a contract awarded by the European Commission

operational concept is explained. A detailed description of SAME is provided in Part 2, Appendix V.

7.5 Approaches to cover performance of human operators (E)

As safety of air traffic operators will remain to depend on the role of human operators, there is a need to cover performance of human operators appropriately in safety assessments. The following approaches have been identified for ATM:

1. Eurocontrol's Human Factor case
2. Human Assurance Levels (HALs)
3. Controller Action Reliability Assessment (CARA)
4. Human performance modelling in TOPAZ
5. Resilience engineering approaches
6. Organisational safety modelling

Re 1: Eurocontrol's Human Factor case [EATM HF case, 2007] is a process to systematically manage the identification and treatment of Human Factor issues as early as possible in a project's lifecycle. In the CAATS II project, this Human Factor case has been formalized [CAATS II, D17] for use in line with E-OCVM in the R&D phases.

Re 2: In SAM, the use of Human Assurance Levels (HALs) is explored, 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. Usually, these HALs are used at the leafs of fault/ event trees. SAME, which is incorporating SAM, also proposes the use of HALs.

Re 3: CARA (Controller Action Reliability Assessment, [Gibson & Kirwan, 2008]) is a human reliability assessment technique, which can be used to quantify human reliability aspects as failure rates and success of mitigation actions in the context of Air Traffic Management (ATM).

Re 4: TOPAZ uses systemic modelling that includes modelling of human performance (e.g., [Stroeve et al., 2009]). Motivation for this is that covering human actors via probabilities in fault and event tree approaches has the serious limitation that this way the impact of concurrent and dynamic behaviour on risk cannot effectively be taken into account. To incorporate for interactions between multiple human actors, TOPAZ includes modelling of multi-agent situation awareness [Stroeve et al., 2003]. Also, it has been evaluated [Blom et al., 2005] regarding possible integration with the human performance model in Air Midas (Air Man-machine Integration Design and Analysis) [Corker, 2000].

Re 5: Resilience engineering [Hollnagel et al., 2006]. Resilience engineering 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. Both the human cognition contribution to resilience (e.g., via coordinating in unforeseen hazardous situations) and possible technological means (see e.g., [Di Benedetto et al., 2008]) that help the human in detecting and restoring from latent conditions which undermine the resilience effectiveness of human operators (e.g., tools that help the operator detect hazardous situations resulting from differences in situation awareness).

Re 6: Modelling of organizations organizational safety modelling for ATM is being studied in [Stroeve et al., 2008]. This goes one step further than modelling humans and interactions between multiple humans, in the sense that groups of humans and interactions within and between groups are also considered.

This project has been carried out under a contract awarded by the European Commission

7.6 Approaches to identify unknown 'emergent' risks (F)

With the introduction of advanced developments as aimed for by SESAR, yet unknown 'emergent' risk may appear. Such risk is related to 'emergent behaviour' which is characterized by what the interaction between multiple local behaviours (both nominal and non-nominal) yields more than the sum of the local behaviours.

Accordingly there is a need to identify such unknown 'emergent' risk. Several complementary approaches have been identified for the identification of such emergent risk:

1. HAZOP
2. A "pure" brainstorming approach
3. Real-time simulations
4. Stochastic modelling and Monte Carlo simulations.

Re 1: HAZOP (Hazard and Operability study, see for instance [Kletz, 1999]) is used for identifying, analyzing and mitigating hazards in sessions with operational experts. The identification is done via brainstorming along keywords. Whereas the more classically adopted hazard identification approach of functional decomposition is directed towards identification of failures of individual functions, HAZOP also enables identifying emergent hazards.

Re 2: The 'pure brainstorming' hazard identification approach (originally developed in [De Jong, 2004], but also incorporated in [EATMP SAM, 2007]), puts large emphasis on identification of hazards that are functionally unimaginable, e.g., because they are associated to systems functioning well (e.g., controllers over-relying on new alerting systems), because they are only remotely associated with failures (e.g., differences in situation awareness, variations in effectiveness of conflict detection and resolution), or because they are related to implicit functions relevant for safety only recognized after failure. In [De Jong et al,. 2007] it is explained that the 'pure brainstorming' approach can drastically increase the effectiveness of HAZOP by keeping hazard identification separate from hazard analysis and risk mitigation.

Re 3: Real-time simulations (e.g., using SAFSIM) 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. Non-nominal events can often be inserted in the simulations, enabling the identification of further, related, emergent behaviour. Real-time simulations can vary in scale, and regularly serve multiple validation objectives simultaneously. Still, the usually low number of runs plays a role in the efficacy in identification of emergent behaviour.

Re 4: Stochastic modelling and Monte Carlo simulations: In this approach, first a stochastic model is developed, which is next subject of large numbers of Monte Carlo simulations. The results of these simulations allow risky behaviour to come to the surface. Only once these are known, it is analyzed from which interactions between which local behaviours this risky overall behaviour stems. This approach allows the identification of emergent behaviour due to interactions of local functional behaviour and also various non-nominal effects, including local issues as situation awareness, human performance, and random effects (e.g., weather). [De Jong et al., 2007] presents an example of identification of high-risk emerging system behaviour from a background of combinatorially many possible system behaviours with lower risk.

Note: Classical approaches to identification of hazards are usually more focused on identification of risk related to individual system elements. Search of literature, reporting systems and databases is usually a good mean to complement such identification. Whereas

This project has been carried out under a contract awarded by the European Commission

such searches may not be very effective in identifying emergent risk, search of similar safety studies might be a useful complementary mean for identification of emerging risk.

7.7 Approaches to address E-OCVM requirements (G)

As safety assessment in R&D is done as part of a general validation process in which stakeholders need to be regularly informed, there is a need to address E-OCVM requirements. Only since recently, it has been studied how to tailor safety assessment methods on the basis of the maturity of the concept under investigation, e.g. what should be done for concept at phase V1 of E-OCVM, what at phase V2 and so on. Table 6 summarizes which sources present general validation views per phase of E-OCVM, and Table 7 summarizes which sources present a view on safety validation per phase of E-OCVM.

Table 6 – Overview of phases for which the sources present a general validation view per phase of E-OCVM.

source	ATM need (V0)	Scope (V1)	Feasibility (V2)	Integration (V3)
SESAR DS		X	X	X
SESAR SEM		X	X	X
SESAR CVM		X	X	X
SARD	X	X	X	X

Table 7 – Overview of phases for which the sources present a view on safety validation per phase of E-OCVM. Phases that are not applicable due to the maturity of the considered concept are marked with n/a.

source	ATM need (V0)	Scope (V1)	Feasibility (V2)	Integration (V3)
SESAR WP 1.6	X			
SESAR SMP	X	X	X	X
SAME	X	X	X	X
SAFMAC	X	X	X	X
RESET		X	n/a	n/a
iFly		X	X	X

In Appendix II in Part 2 of this document, an analysis is presented of those views that were available on the date on which collection of information by CAATS II closed. For each phase, the leading view from E-OCVM is presented, as well as the commonalities with and complementarities to E-OCVM of other sources' views. From the analysis, it is concluded that knowledge on working with E-OCVM in safety assessment in R&D is only just building up, and that there are several candidate approaches for addressing E-OCVM requirements.

7.8 Approaches to assess concept maturity (H)

Projects need to understand the current maturity of the concepts they are working on, especially if any aspects are less mature than the rest, and how far they have progressed in improving and making the concept more mature and stable. The ideal would be to have objective and shared criteria to evaluate whether an operational concept can be transferred to a next phase of the E-OCVM concept lifecycle model, i.e., transition criteria. The following approaches for this have been identified:

1. Strategic Assessment of ATM R&D results (SARD);
2. Recent draft improvements to SARD by researchers involved in SARD and CAATS II;

This project has been carried out under a contract awarded by the European Commission

3. Transition criteria developed as part of SAME.

Re 1: The Strategic Assessment of ATM R&D results (SARD) defines a process and a set of criteria for the analysis of ATM R&D results per operational concept from a strategic view point. The process assesses the maturity of operational concepts, in terms of the phases of the Concept Lifecycle Model of E-OCVM, and their improvement steps. It analyzes the results obtained in relevant projects on specific operational concept (i.e. where we are? what has been achieved during last period of 1-2 years? what are the implications of results for the strategic objectives and performance targets?) and to provide recommendations for next steps. In principle it can be used for any ATM improvement under development. The process should be applied to assess regularly the maturity of concept elements in the SESAR development phase, feeding the maintenance of the SESAR Master Plan. The SARD process has been successfully applied and further improved through application to two ATM operational concepts. Detailed information about SARD is contained in Part 2, Appendix IV.2.

Re 2: Recently, researchers responsible for SARD and for CAATS II have jointly developed an improved and updated revision of SARD's detailed criteria per phase of the Concept Lifecycle Model. In addition, CAATS II proposed a safety case specific extension of the SARD transition criteria, addressing the personalisation of the criteria for the safety aspects, and producing guidance to safety case for the SARD application. However, these improvements are very recent and have not yet been validated through a practical application to R&D projects. Detailed information about this improvement of SARD are proposed in Part 2, Appendix IV.3 and in reference [CAATS II, D28].

Re 3: Criteria for evaluating the level of maturity of the safety relevant aspects of a concept have also been provided within SAME. In particular, SAME was mapped into the E-OCVM lifecycle phases, identifying: the safety assessment activities that are typical for a concept that is at level of maturity V0, V1, V2 and V3; the typical inputs and outputs of the safety assessment for these levels; the related transition criteria from V0 to V1, V1 to V2 and V2 to V3. These improvements are very recent and have not yet been validated through a practical application to R&D projects. Detailed information about the transition criteria proposed by SAME are reported in Part 2, Appendix V.2.

7.9 Approaches for managing relations between cases (I)

In R&D projects several cases runs in parallel and investigate the most important characteristics of the concept under analysis. Relations between different cases have so far been very limited in R&D projects, in spite of the similarities between the work to be done for each case and the potential synergies. The consequence of this partition of the work, together with the different levels of maturity of methods and techniques, can be a complete separation of cases from each other. Accordingly, there is a need to manage relations between cases. CAATS II has developed material on managing relations between cases.

Appendix III describes the state of practice regarding relations between cases in the current R&D projects, with special attention to the relations between human factor and safety case. This includes a CAATS II developed framework for relations between cases that was proposed and refined with the collaboration of several experts of the different cases concerned (safety, human factor, environment, business). This work leaded to the preliminary identification of the phases in which different cases should interact with each other and of the type of information they should exchange. The proposed approach and the preliminary results achieved are presented in Part 2, Appendix III and in reference [CAATS II, D28]. For the specific relations between safety and human factor cases some results are also presented in [CAATS II, D17]. The RESET

This project has been carried out under a contract awarded by the European Commission

project [RESET, 2009] aims to use this relation framework in specific for the relations between the safety and the human factor case in the phase V1 of E-OCVM.

This project has been carried out under a contract awarded by the European Commission

8. CONCLUDING REMARKS

An inventory has been made of practices for safety assessment in R&D. Due to multiple recent developments, the inventory forms a significant major revision over the one made three years ago by CAATS [CAATS, D1.4 P2]. The main aim was to up-date the document with respect to recent developments and to focus on the applicability of the methods and techniques for safety assessment to R&D projects for advanced developments such as aimed for by SESAR. The inventory has been done based on a huge collection of inputs from SESAR, other research projects, surveys and questionnaires and analysis documented in Part 2 of this report.

After an analysis of the general steps of a safety assessment process (Section 2), the main current practices for safety assessment in R&D projects have been identified as being SAM, ED78A, and TOPAZ (Section 3). Next, emerging approaches for safety assessment in ATM R&D projects have been identified, including a literature review of techniques (Section 4). Then, the purpose and way of working of safety assessment in the specific context of R&D projects, was explained, presenting briefly the concept maturity model of E-OCVM (Section 5).

Whereas the approach for safety assessment is relatively well consolidated for an ANSP assessing a change to its Air Traffic Management (ATM) system, including humans, procedures, and technical equipment, it appears from the literature review that safety assessment in Research and Development (R&D) for advanced developments as aimed for by SESAR the situation has been subject of a lot of recent research. From this research it appears that several new needs emerge, and that traditional approaches fall short. Emerging needs identified by SESAR and complementary emerging needs identified by other sources have been explained (Section 6).

For each of the SESAR-identified emerging needs, approaches have been identified that aim to address it (Section 7). These approaches include both approaches that are already practice, and approaches that are emerging and still in further development. It has not been evaluated to which extent the various approaches fulfil the SESAR-identified needs, nor has it been evaluated whether the complementary emerging needs identified by sources other than SESAR are addressed. Integration of the various novel emerging approaches with each other and with established approaches typically has received limited attention.

This project has been carried out under a contract awarded by the European Commission