# A PRACTICAL WORKSHOP-BASED METHOD TOWARDS RESILIENT DESIGN OF COMPLEX SOCIO-TECHNICAL SYSTEMS

M.H.C. Everdij [1] and S.H. Stroeve [2]

[1,2] Netherlands Aerospace Centre, Amsterdam, The Netherlands

[1] everdij@nlr.nl, [2] stroeve@nlr.nl

http://www.nlr.org

**Abstract**

Under the premise that a more resilient operation is better able to be safe and efficient, this paper presents a pragmatic approach for analysing the resilience of future air traffic management (ATM) operational concepts and improving their design. The approach uses a workshop with operational experts as a central element and follows 5 steps. The last two steps use key new elements specific for this approach; the first three steps are used in other safety methods as well, but are adapted to better support the last two steps. The approach is illustrated through application to an ATM operational concept that uses an Aircraft Surveillance Applications System (ASAS) for sequencing and merging of aircraft towards an airport. The output is an analysis of the resilience of the operation, and the identification of a range of recommendations for the design of this operation, such that its resilience can be improved.

## 1 INTRODUCTION

Before a design of an air traffic management (ATM) system can be put into operation, an analysis needs to show that it is sufficiently safe. Most of the focus of today's safety management systems is put on the identification and mitigation of hazards and failures. However, failure situations are rare and hence present a very limited picture when trying to design a socio-technical system that is safe as a whole. In the perspective of Safety-II and Resilience Engineering (RE) (Hollnagel, 2014), successes and failures of the socio-technical system both stem from performance variability. Different varying conditions may combine to hazardous situations due to their complexity and intractability. Not all such conditions can be expected and prepared for beforehand, and unexpected conditions will at some point occur. RE defines safety as the ability to succeed under both expected and unexpected varying conditions. Moreover, RE emphasises the need to well consider the multiple goals that the socio-technical system aims to achieve, which is not only safety but often also productivity, security, environmental sustainability, etc.

For an RE approach to be successful it will need to include: 1) a way to analyse the resilience of an operational design; and 2) a way to improve the operational design in order to make it more resilient. Without the first element, there is no way to understand where resilience comes from and where it can be improved. Without the second element there would be no engineering of resilience back into the design. The proper execution of these two elements requires experts in resilience and safety analysis, and operational experts. For ATM designs, the operational experts include air traffic controllers, pilots, supervisors, technical engineers, maintenance engineers, etc. These operational experts can change gears quickly and are trained in dynamically and creatively handling various new occurrences. They have the ability to deal with varying conditions and interacting human operators and technical systems in an operational context, and they have the ability to imagine themselves in a new context, such as a future operational design. As such, they have knowledge and experience that is essential not only for element 2 above (improving the operation), but also for element 1 (resilience analysis).

The RE approach presented in this paper makes effective use of operational experts in both the resilience analysis and the improvement of the operation, but uses limited RE jargon. A central element in the approach is the identification of the strategies that the operational experts use when dealing with varying conditions (or combinations thereof) in their daily work. The result of the RE approach is a deeper understanding of how the socio-technical ATM system deals with small and large, common and rare disruptions and conditions, at a level sufficient to identify improvements to the operational design.

This paper presents the results of application of the RE approach to a specific operational concept of Aircraft Surveillance Applications System Sequencing and Merging (ASAS S&M) conducted in (Everdij et al., 2016). The approach followed took as input the lessons learned during earlier applications of RE, such as (Herrera et al.,

2015). The objective of the current study was to test and further improve the RE approach by its application to the ASAS S&M concept in the design phase. It should be noted that the ASAS S&M concept is under development and that this paper does not conclusively evaluate the ASAS S&M concept. The paper merely aims to illustrate the RE approach, by using the ASAS S&M concept as a case.

The paper is structured as follows: Section 2 describes the RE approach, Section 3 describes the application to the case of ASAS S&M and presents some of the key results, Section 4 provides a discussion.

## 2 RE APPROACH

The RE approach has 5 steps, which follow Figure 1 below. The activities include (but are not limited to) the four main sessions of an RE workshop with participation of operational experts.

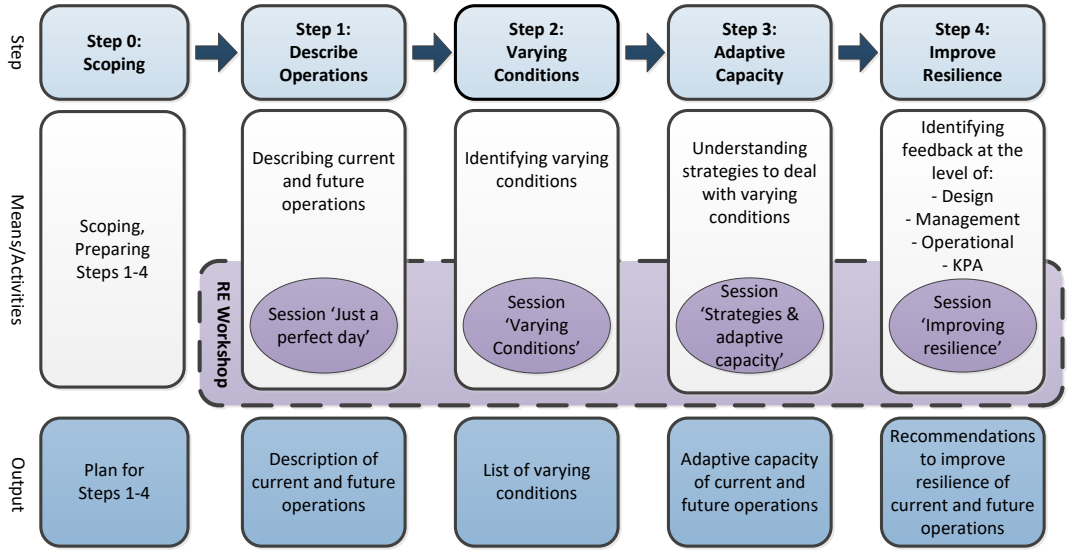


***Figure 1.*** *The RE approach follows five main steps*

The *Scoping* step (step 0) aims to plan and outline the study. The activities include developing the RE workshop structure and agenda, and arranging the logistics. The *Describe Operations* step (step 1) aims to build an initial understanding of the work-as-done in current ATM operations and of the way that future ATM operations are expected to be done. The activities include studying relevant material, interviewing experts, and doing observations in the field and at simulation facilities if feasible. The *Varying Conditions* step (step 2) aims at identifying a list of varying conditions that ATM operators and managers may have to deal with in the future and current ATM operation. The activities include studying relevant material such as safety analysis documents on related operations, and organising brainstorm sessions with operational experts. The *Adaptive Capacity* step (step 3) aims to obtain narrative descriptions of the strategies that operators and supervisors use when they are dealing with varying conditions in the current and the future ATM operation, and to analyse the adaptive capacity of the current and the future ATM operations. The activities include organising workshop sessions with air traffic controllers, pilots, and supervisors, as well as applying appropriate techniques to determine the adaptive capacity these operational experts have when dealing with varying conditions. The *Improve Resilience* step (step 4) aims at deriving recommendations for strengthening the resilience of current and future ATM operations. These recommendations are aimed to be translated into new or revised design requirements. The activities include a brainstorm session with the operational experts involved in step 3, who are asked to identify design improvements at the levels of design, management, operation and key performance areas such as safety, capacity, environment and cost-benefit. In addition, complementary design improvements are identified through analysis of all material collected so far.

## 3 APPLICATION

The RE approach was applied to a specific future operational concept of ASAS S&M, set around a large European airport. The pilots on flights enabled with ASAS S&M can get an instruction from the air traffic controller to maintain a certain spacing (a time distance) with a specific target aircraft in front of them. This target aircraft can be on the same route ('sequencing'), or on another route that merges with the route of the

follower aircraft ('merging'). This operation differs from current operations, in which aircraft get heading (directions) and speed instructions from the controller to safely sequence and merge on their routes.

The ASAS S&M operation was set in the context of a larger operation, with an extended arrival management system supporting controlled time of arrival operations on an extended operational horizon. The airspace for the larger operation consisted of 6 sectors, but during the RE workshop, the main focus was on the sectors nearest the airport, where ASAS S&M was used. These were two terminal manoeuvring area (TMA) sectors and one arrival (ARR) sector. In addition there was the final approach sector (TWR) which included the runway itself. For each sector there was one executive controller. There was one supervisor for the TMA/ARR sectors, and one supervisor for TWR.

### 3.1 Step 0: Scoping

As part of step 0, a plan was developed for the activities to be conducted in steps 1-4, including RE workshop structure and agenda, the physical and electronic material to be used, and logistics like list of participants, meeting room venue, and role of each RE team member. Figure 1 shows the main sessions planned for the RE workshop. These were preceded by an introductory session to explain the purpose of the workshop and to summarise the ASAS S&M design. A debriefing was prepared in which the participants were to be asked for their feedback on the workshop organisation. One of the main concerns in the planning was to make sure that the activities had the appropriate set of well-experienced participants. For the RE workshop, we were able to invite 5 controllers with experience of the relevant air traffic control positions and including a supervisor, and 2 experienced airline pilots. In addition, there were between 2 and 6 observing participants with various ASAS and/or safety expertise. The RE team consisted of 5 members; two for moderating the workshop and making notes; one for leading the step 4 session; one in charge of the logistics, and one in charge of the debriefing.

### 3.2 Step 1: Describe operations

As part of step 1, the RE team studied available documentation on current and future ATM operations, including operational service and environment descriptions (OSED), validation plans, procedure and rule sets, etc. In addition, the team made observations during large-scale human-in-the-loop simulation sessions of the ASAS S&M operation. These human-in-the-loop simulations used experienced planning and executive air traffic controllers for each of the controller positions, who were tasked to safely and efficiently control traffic flown by over a dozen pseudo-pilots and one cockpit simulation. The simulations took place during two weeks plus one week of training, and were organised by a project in charge of validating the ASAS S&M concept in a larger context. During a few days, the RE team attended these simulations as guests in order to observe how the operators (i.e. controllers, pilots, supervisors) act and interact with each other and with their human machine interface and environment. An additional means used in step 1 was Session "Just a perfect day" in the RE workshop (see Figure 1). Herein, the participating operational experts (controllers, pilots, supervisors) explained what a typical day of operations without considerable varying conditions ('just a perfect day') looks like for them in their current work. Next they were asked to express their expectations of what such a perfect day would look like in the future ASAS S&M operation. This session served to achieve a common understanding of the operations from various perspectives. It is noted that the operational experts involved in the RE workshop were also part of the human-in-the-loop simulations described above. This significantly helped them in their operational comprehension of this future operation.

The information obtained from these means was summarised and documented, with references to the source of the information. The output was a better understanding of the ASAS S&M operation, the dynamics involved, the timing of activities, the human-machine interface, human-machine interactions, and the controller-controller and controller-pilot communications.

### 3.3 Step 2: Varying conditions

The main source for step 2 was a dedicated brainstorm session, organised with ATM operational experts as part of the RE workshop (see Figure 1). The operational experts were each given several prepared forms, and were asked to write down as many conditions as possible; rare conditions as well as normal conditions, and to consider situations within their control as well as situations outside of their control. During the brainstorm, a total of 49 varying conditions were identified, which (after the workshop) were organised into 12 clusters of similar or related conditions, i.e. Adverse weather conditions, Runways & taxiways conditions / availability, Airspace restrictions, Separation issue / missed approach, Traffic load evaluation, Differences in aircraft performance, Flights with emergency conditions, Controller performance, Pilot performance, Air Traffic Control system problem, ASAS S&M system unable to find solution, and Aircraft system problem. The list

included conditions that could be considered hazards, or situations with the potential to compromise safety, but there were also several 'normal' situations, such as temporary airspace restrictions, cultural differences, or situations with mixed traffic, such as arrivals of medium and heavy weight aircraft on a single runway, which controllers and pilots have to deal with in their daily work.

### 3.4 Step 3: Adaptive capacity

This step included two distinct sub-activities. The first included the organisation of Session "Strategies & Adaptive Capacity" in the RE workshop (see Figure 1). In this session, for each cluster of varying conditions identified in step 2, a representative varying condition (or a combination of such conditions) was selected and the operational experts (controllers, pilots, supervisors) were asked to explain the strategy or strategies they use or envisage to use when dealing with this varying condition; first in current operations, and next in future ASAS S&M operations. Each such strategy description was derived by asking appropriate questions; Table 1 presents the question set used for this. This set was designed to cover the principles of resilience (see also discussion in Section 4) and it uses terminology that corresponds to the experience of operators in ATM. The results of the session were documented in narrative form, describing what the participants said as well as possible, thus making sure that the context in which they said it was captured. This provided the raw data that could be used as input to the more detailed adaptive capacity analysis.

***Table 1.*** *Questions used to elicit operator strategies per varying condition. They were used for both current and future operations*

| | |
|---|---|
| **Frequency** | In what way and how often could the varying condition occur? |
| **Detection** | Who or what would detect the varying condition, and how? |
| **Strategy / Adaptation** | What is the strategy to deal with the varying condition, i.e.: How would you act / adapt to the varying condition, with whom would you interact and coordinate, what resources are used? |
| **Learning / Training** | How is the strategy acquired, for instance is it part of basic training, is it learned by experience? |
| **Trade-offs** | What are the trade-offs and what are the effects of applying the strategy on ATM key performance areas such as safety, capacity, costs, and environment? |

The second sub-activity, executed after the RE workshop, was to analyse 'base and extra adaptive capacity'. This technique was loosely based on the Stress-Strain model of Woods et al. (2013), which is a framework for analysis of how a system stretches to handle surprises. In the technique, for each varying condition discussed in the RE workshop, and for both the current operation and the ASAS S&M operation, the capacity of the ATM system to recognise and handle the varying condition was identified. In some situations this capacity involved the use of elements already covered by the design of the ATM system, including procedures and training (base adaptive capacity); in some situations it required more creativity and experience from the human operators (extra adaptive capacity). The notes of the RE workshop were used as the input to this analysis. For each varying condition, the results were documented using the format of Table 2. The table was next analysed in order to investigate trends between the results for the different varying conditions. For several situations and varying conditions, the strategies for dealing with them appeared to be not covered by procedures and training, but to be learned on the job. Controllers and pilots require experience and creativity when they are confronted with these situations.

***Table 2.*** *Presentation of analysis results of the base and adaptive capacity per varying condition*

| **Varying condition.** Here the ID and brief description of the varying condition is discussed | |
|---|---|
| **Adaptive capacity in current operation.** Description of the way that the varying condition can be recognized in the current operation, how it can be handled by the pilots and by the controllers, and the implications for the base or extra adaptive capacity. | **Adaptive capacity in future operation.** Description of the change in recognition, strategies, and adaptive capacity of the future ASAS S&M operation in comparison with the current operation. |
| **Summary.** Summary of the above, in terms of base and extra adaptive capacity required by controllers and pilots in current operation. | **Summary.** Summary of the above, in terms of the change in adaptive capacity required by controllers and pilots in future operation compared to current. |

### 3.5 Step 4: Improve resilience

For this step, a brainstorm session with operational experts was organised as part of the RE workshop (session "Improve resilience" in Figure 1). Herein the experts were split up into smaller groups and were asked to identify measures to improve the resilience of current and future ATM operations at four levels:

- Design level, including hardware and software, human factors, procedures, airspace structure, layout of the workplace, etc.
- Management level, including supervisors, managers and their procedures and processes for managing and controlling the organisation.
- Operational level, including training, organisational learning, team considerations, safety culture, etc.
- KPA (Key Performance Areas) level, including effects on safety, capacity, environment, cost-benefit.

It was key to have this brainstorm session near the end of the RE workshop, such that the earlier sessions created an environment of thinking in terms of resilience and adaptive capacity. After the RE workshop, the documented results of steps 1, 2 and 3 were reviewed and analysed by the RE team in order to identify additional improvements and making sure that nothing was missed. Subsequently, the improvements identified through the above means were formulated by the RE team as recommendations to improve the resilience of future ATM operations, which were next reviewed by operation designers.

For the ASAS S&M case, the identified improvements included requirements to re-design the airspace and adjacent sectors in order to better accommodate the new operation. Also, a need was identified for a new tool to assist the controller in converting spacing distance to seconds, and that displays the spacing time between aircraft. There was also a need to set a maximum to the traffic capacity in ASAS S&M operations, at a level that can be effectively downsized in the case of sudden runway capacity reduction. The pilots identified a need to get information during their pre-flight briefing on whether the ASAS S&M procedure is in use at the destination airport, because this would have impact on the amount of fuel to take.

## 4 DISCUSSION

This paper presented a pragmatic approach for RE. The workshop-centred RE steps were successfully applied to the current and to ASAS S&M approach operations. This led to the identification of a range of recommendations for the design of the future ASAS S&M operation, such that its resilience can be improved.

Steps 0, 1 and 2 are preparatory, and have similarities with many other safety analysis methods. Nevertheless, their proper execution is essential to the success of the application. Especially in step 2 (varying conditions) it is important to maintain a wide scope, and include not only hazardous situations but also situations that are considered part of the daily job, and that call for the operator's attention because they require coordination and communication.

Steps 3 and 4 are specific for this RE approach, even though some elements are also used elsewhere. The first subactivity of step 3 (identification of strategies) has been designed to address all principles and aspects of resilience such as those defined in (Woltjer et al., 2015). E.g., 'signals and cues' is addressed by the question how the condition can be detected, and how it is monitored while it unfolds; 'margins, adaptive capacity' is addressed by the question that asks about the strategy when dealing with the condition; 'timing and synchronisation' and 'cascading' are addressed by the questions that ask how the experts interact and coordinate while the situation unfolds; 'under-specification' is addressed by the question about training or experience; 'goal trade-offs' is addressed by the question that asks about the trade-offs; 'work-as-done' and 'varying conditions', are addressed by asking the experts about their strategy when dealing with a varying condition, and by sessions 'just a perfect day' and 'identification of varying conditions' in the workshop.

The second subactivity of step 3 (analysis of adaptive capacity) uses this as input to analysing the resilience of the ATM socio-technical system, by way of analysing how this socio-technical system adapts to varying conditions. This paper illustrated the use of a technique called base and extra adaptive capacity analysis, which distinguishes situations that are covered by procedures and training (base adaptive capacity), and situations that require experience and creativity from the operators (extra adaptive capacity). The focus is primarily on individuals, either at the sharp end or at higher managerial levels, and on how they interact with other individuals, technical systems and their environment. More advanced techniques are required to get to a level of resilience emerging out of multiple complex and dynamic interactions between multiple operators and their environment. Stroeve & Everdij (2017) discuss what it takes to be able to address such challenging levels, and show how agent-based modelling and simulation can be effectively used to this end. The agents in such model have time-dependent states, inputs and outputs, and the evolution of these states, the impact of the input

signals on the states, and the implications of the states for the output signals are represented by sets of model constructs. These model constructs include key constructs for the agent's situation awareness in a multi-agent environment, task-related (identification, scheduling, execution, decision making) model constructs, task load and contextual control mode as workload-related model constructs, and variability-related model constructs representing dynamics, stochasticity and errors in human performance. Together with constructs for technical systems performance and environment, they form a model that is effectively used for qualitative or quantitative analysis of resilience of complex systems.

The success of step 4 is for a large part dependent on the proper execution and success of step 3. For one, the workshop moderators need to make sure that all aspects of resilience are addressed. Therefore, it is important that these moderators are trained in the principles of resilience and Safety II, and are able to subtly steer the operational participants into thinking in terms of these principles as well, without using the associated jargon. Secondly, step 3 helps the operational experts to get a mind-set of thinking in terms of resilience, rather than for example in failures and errors. Thirdly, the operational experts get a chance to talk about their daily work in a systematic way, and with other operational experts. This helps them look for areas in which their job can be improved and how their actions affect others. For this, it is important that step 3 covers a wide area of varying conditions and the strategies to deal with them. Fourthly, it is important to have an appropriate and complementary set of participants, including experienced controllers, pilots, supervisors and technical personnel. The most valuable output emerges from the interaction between these experts.

The success of step 4 also benefits from the results obtained in the other steps. The information collected in the observations of the human-in-the-loop simulations, the 'Just a perfect day' session, the 'Strategies and adaptive capacity' session, and the analysis of base and adaptive capacity or the use of more advanced techniques after the workshop each provide input to the identification of design recommendations. The analysis of the complete collection of inputs provides background material and justification for the recommendations, and makes sure that nothing relevant is missed.

The operators in our RE workshop were very positive about the approach, which allowed them to explain all the things they do to make ATM safe, rather than getting blamed for some rare and difficult situations they were not able to completely solve given the circumstances. During the debriefing, they explained that before the workshop, the term 'resilience' was just a word. But now, it appears to be a part of life, something that they use in their everyday work.

**Acknowledgements**

The research reported upon was funded as part of the SESAR Joint Undertaking within P16.06.01b. We gratefully acknowledge the contribution of operational experts (especially air traffic controllers, and staff association and airspace user representatives) and project members and safety experts of the ASAS S&M projects, and the SJU P16.06.01b project members from ENAV (especially Massimiliano Bottone and Marco Paino), INDRA (especially Cristina Díaz Domínguez), NORACON (especially Billy Josefsson), EUROCONTROL (especially Ella Pinska) and IFATCA (especially Tom Laursen). The views and opinions in this publication are of the authors and are not intended to represent the positions of SESAR JU or its project member organisations.

**REFERENCES**

Everdij, M., Stroeve, S., Bottone, M., Díaz Domínguez, C., De Gelder, N. & Paino, M. (2016). *ASAS - Interim Report 2014*, SESAR Project 16.06.01b: Application of Resilience Guidance to Multiple Remote Tower and ASAS S&M, Deliverable D03-001

Herrera, I., Smoker, A., Pinska-Chauvin, E., Feuerberg, B., Schwarz, M., Josefsson, B. (2015) Resilience engineering (RE) in design: initial application of a new RE assessment method to the multiple remote tower concept. *Proceedings 6th REA Symposium: Managing Resilience*

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Farnham, UK: Ashgate

Stroeve, S.H. & Everdij, M.H.C. (2017). Agent-based modelling and mental simulation for resilience engineering in air transport, *Safety Science*, 93: 29-49

Woltjer, R., Pinska-Chauvin, E., Laursen, T. & Josefsson, B. (2015). Towards understanding work-as-done in air traffic management safety assessment and design. *Reliab. Engineering & System Safety*, 141: 115-130

Woods, D.D., Chan, Y.J. & Wreathall, J. (2013). The Stress-Strain Model of Resilience Operationalizes the Four Cornerstones of Resilience Engineering, *Proceedings 5th REA Symposium: Managing Trade-offs*