Studying hazards for resilience modelling in ATM

Mathematical Approach towards Resilience Engineering in ATM (MAREA)

Sybert H. Stroeve[1], Mariken H.C. Everdij[1], Henk A.P. Blom[1,2]
[1]National Aerospace Laboratory NLR, Air Transport Safety Institute, Amsterdam, The Netherlands
[2]TU Delft, Faculty of Aerospace Engineering, Delft, The Netherlands
E-mail: sybert.stroeve@nlr.nl, mariken.everdij@nlr.nl, henk.blom@nlr.nl

***Foreword* — This paper describes a project that is part of SESAR WP-E, which is addressing long-term and innovative research.**
***Abstract* — Resilience engineering purports to improve the safety in complex socio-technical systems, such as in air traffic management (ATM). The MAREA project aims to support a more systematic analysis of resilience in ATM by developing a mathematical modelling and analysis approach for resilience engineering in ATM. Key elements will be models for human-related aspects. This paper describes the basis for this development. It describes model constructs of existing safety analysis methods. It presents a broad set of ATM hazards, highlighting various sources of performance variability in the ATM socio-technical system. It discusses interviews with pilots and controllers about their ways to deal with hazards. It studies the potential of the existing model constructs to describe the performance variability indicated by the hazards. It is concluded that multi-agent dynamic risk modelling can represent a wide variety of performance variability in complex ATM scenarios and has the potential to systematically analyse risk and resilience.**

Keywords – resilience; safety; accident risk modelling; air traffic management; hazard.

I. INTRODUCTION

Resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions [1][2]. Resilience is important for complex socio-technical systems such as air traffic management (ATM), where large numbers of interacting human operators and technical systems, functioning in different organizations at a variety of locations, must control air traffic safely and efficiently in the context of uncertainty and disturbances (e.g. delays, weather, system malfunctioning). Although procedures and regulations tend to specify working processes in ATM to a considerable extent, the flexibility and system oversight of human operators are essential for efficient and safe operations in normal and more rare conditions [3]. In other words, human operators are essential to maintain resilience in the complex ATM system.

A key notion in arguing about the contributions of human operators to resilience is 'performance variability'. It is defined in [1] as 'the ways in which individuals and collective performances are adjusted to match current demands and resources, in order to ensure that things go right', where 'to ensure' should be considered as a goal. In a complex system such as ATM, performance variability is inevitable as well as useful. It may lead to success and failure, depending on the circumstances and interactions in ATM scenarios. Sources of human performance variability include [1]: under-specification of work, fundamental psychological factors (e.g. affecting perception), higher-level psychological factors (e.g. creativity), organizational factors, social factors and contextual factors.

The thinking on safety by using concepts as resilience and management of performance variability has been strongly supported by Erik Hollnagel and co-workers and their introduction of the Resilience Engineering research field [2] [4][5][6][7][8][9]. As will be argued in the paper, we recognized that the development of an adequate mathematical modelling and analysis approach is needed to bring resilience engineering effectively at work for the complex socio-technical system of ATM. This development is done in the MAREA project (Mathematical Approach towards Resilience Engineering in ATM).

This paper describes the first results of the MAREA project and it is structured as follows. Section II describes the MAREA project. Section III describes the identification of a broad set of hazards in ATM and the identification of ways that pilots and controllers deal with them. Section IV presents some key modelling methods for analysis of safety and resilience in ATM. Section V describes the coverage of hazards by current model constructs in ATM safety analysis. Section VI provides a discussion of the results.

II. THE MAREA PROJECT

The aim of the MAREA project is to develop an adequate mathematical modelling and analysis approach to support effective application of resilience engineering for the complex socio-technical system in ATM. MAREA is a joint project of NLR (Coordinator), VU University Amsterdam and University of l'Aquila. The project is part of the SESAR WP-E programme on long-term and innovative research in ATM. It is supported by the SESAR WP-E research network ComplexWorld, which focuses on the theme 'Mastering Complex Systems Safely'. With regard to the research questions posed in a white paper on complexity in ATM of the ComplexWorld network [10], the research in MAREA relates

This work is part of the SESAR WP-E programme on long-term and innovative research in ATM. It is co-financed by Eurocontrol on behalf of the SESAR Joint Undertaking.

to questions #6 (propagation of safety events), #8 (resilience assessment) and #10 (safety analysis feedback to design).

The work in MAREA is structured according to the following work packages:

- WP0 concerns project coordination and the final report.
- WP1 analyses to which extent current modelling formalisms are able to cover hazards and implied resilience needs. This includes the identification of models that are used in ATM safety assessment approaches, the identification of a representative set of hazards in ATM, an analysis of the resilience in dealing with these hazards by pilots and controllers, and an analysis of the coverage of the hazards and the human responses by models in ATM safety assessment.
- WP2 develops complementary psychological and organizational sub-models, and a formal way how these sub-models can be integrated in a multi-agent framework. Subsequently, it is tested to which extent the integrated sub-models cover the various hazards and the related pilot and controller responses.
- WP3 conducts a validation of the integrated multi-agent framework, including the added sub-models, by evaluating its capability in predicting the various hazards and the associated human responses.
- WP4 applies the methods to SESAR 2020 scenarios. It uses a formal approach of automata theory, including psychological and organizational sub-models identified in WP1 and WP2. The result is an identification of safety critical conditions of 4D trajectory-based SESAR 2020 scenarios.
- WP5 compares the MAREA approach with other resilience engineering approaches and safety assessment approaches. The integration of the novel approach in the design cycle of future ATM is addressed.
- WP6 concerns dissemination of the results.

The current paper presents results achieved in WP1.

III. HAZARDS IN ATM

A. *Identification of a broad set of hazards*

As a basis for the systematic evaluation of existing model constructs in ATM safety assessment as well as for the identification and validation of new model constructs, a wide list of hazards in ATM is identified. In this study, a hazard is broadly defined as “anything that may influence safety”. Hazards thus include a wide variety of events, conditions and performance aspects of human operators, technical systems, environmental conditions and their interactions.

NLR has developed an ATM Hazard Database, which includes a collection of hazards that were identified in a broad range of ATM safety assessments. The prime means by which these hazards were gathered is by brainstorm sessions with pilots, controllers and other experts. These hazard brainstorm sessions aim to push the boundary between functionally imaginable and functionally unimaginable hazards [11]. Consequently, considerable parts of these hazard brainstorm sessions address human behaviour, conditions and technical systems that influence human behaviour and interactions between humans. Overall, the ATM Hazard Database includes a broad set of hazards, addressing the performance of interacting humans, technical systems and contextual conditions for a large variety of ATM operations.

The collection of hazards in the ATM Hazard Database includes equal or similar hazards and hazards that refer to a study-specific context, e.g. airport layout and route structure. For the purpose of the MAREA project, we analysed all hazards in the ATM Hazard Database: we selected all unique hazards and we formulated them in a generalized way (i.e. without referring to study-specific details).

The identified hazards were structured in the following clusters: Aircraft systems, Navigation systems, Surveillance systems, Speech-based communication, Data-link-based communication, Pilot performance, Controller performance, ATC (Air Traffic Control) systems, ATC coordination, Weather, Traffic relations, Infrastructure & environment, and Other. Although various hazards might in principle be included in multiple clusters, as they may link to a variety of the aspects indicated in the clusters, each hazard is only included in one cluster.

The hazards resulting from the identification and the clustering include a total number of 525 unique and generalized hazards. An overview of the distribution of the hazards over the clusters as well as some examples of individual hazards are given in Table I. It can be observed that a large part of the hazards is directly related to human performance. The total set of hazards is split in two similarly sized sets: Set I for the development of new model constructs (WP2 of the MAREA project) and Set II for the validation of developed model constructs (WP3 of the project).

TABLE I. NUMBER OF HAZARDS PER CLUSTER AND HAZARD EXAMPLES

Hazard cluster	No.	Examples of hazards
Aircraft systems	27	• Aircraft cannot perform requested manoeuvre, since it is over its performance limits • False alert of an airborne system
Navigation systems	16	• Wrong waypoints in database, e.g. due to update of flight management system software, errors in database, outdated database
Surveillance systems	27	• Transponder sends wrong call-sign • Track drop
Speech-based communication	37	• Failure in frequency changes between subsequent air traffic controllers • Standard R/T not adhered to
Datalink-based communication	20	• Controller does not send a data-link message and forgets to give a clearance by voice
Pilot performance	124	• Over-reliance on system data • Pilot does not know the complexity of the traffic situation • Alert causes attention tunnelling • Change in ATC procedures leads to confusion by pilots • Pilot mixes up different types of ATC clearances • Pilot is fatigued and sleepy • Pilot validates without actually checking

Controller performance	110	• Risk of a conflict is underestimated • Controller wrongly evaluates traffic situation after an alert • Change of ATC procedures affects fluency of controller's performance • Controller has a wrong awareness about the intent of aircraft • Controllers getting very much used to new systems, such that it becomes hard to do without
ATC systems	25	• Flight plans of ATC system and FMS differ
ATC coordination	24	• ATC centres have different versions of aircraft trajectory plans • Controller is overloaded with coordination messages
Weather	27	• Weather forecast wrong • Strong variation in view (e.g. due to snowfall or fog patches)
Traffic relations	33	• Resolution of conflict leads to other conflict(s) • Differences in performance of different aircraft types, e.g. at a merging point
Infrastructure & environment	24	• Animals on the runway • Approach lights are not visible
Other	31	• Contingency procedures have not been tested • Insufficient capacity of an ATC centre due to strike or illness

B. Ways of pilots and controllers to deal with hazards

MAREA aims to develop new mathematical models that describe the performance of human operators in dealing with hazards and that support the analysis of the resilience following the interactions of the various agents in ATM scenarios. To obtain insight in the ways that pilots and controllers cope with hazards in their normal work, we organized interviews with pilots and controllers.

The interviews were based upon the identified generalized ATM hazards (Table I). In preparation of interviews with pilots and controllers we categorized the hazards in three classes A, B and C, based on the relationship with the human operator:

A. The occurrence of an event external to the human operator, where an event is a sudden situation with a limited duration;
B. A situation that is related to behaviour of the human operator;
C. A contextual condition (typically enduring) that impacts the behaviour of the human operator.

Depending on these classes different questions about the performance of a human operator in relation with each class were set up. These questions refer to the ways that operators may detect hazards, deal with them and whether there are related procedures.

Interviews were conducted with five air traffic controllers and two airline pilots, from four different European countries. The expertises of the controllers include control positions at ACC (area control centre), approach and tower; both pilots were airline pilots. In the interviews the pilots and controllers were asked to consider the way that the hazards may be coped with in their normal work, building on their operational knowledge and experience. Thus the scope is the performance of pilots and controllers in current ATM operations.

The results of these interviews provide an extensive overview of manifestations of practical performance variability as a result of hazards in ATM [12]. A key observation in the interviews is that for a lot of hazards there are no written procedures, but pilots and controllers react in various ways based upon their training, experience and what they regard as 'normal work'. As such, the interviews provide a basis for advancing models of human performance variability in ATM and thereby for analysis of resilience in ATM.

IV. MODELS IN ATM SAFETY ANALYSIS

As a basis for the analysis of existing model constructs in ATM safety studies, in this section we concisely describe four modelling methods: fault and event trees, as the most commonly used conventional method, and STAMP, FRAM and multi-agent dynamic risk modelling, as more recently developed systemic accident models.

A. Fault and event trees

Following a long tradition in safety assessment of technical systems, air traffic operations are often assessed on the basis of fault and event trees. Fault and event trees are pictorial representations of Boolean logic relations between success and failure types of events. Event trees use forward logic, reasoning from an initiating event to its possible consequences; fault trees use backward logic, reasoning from a top event to its contributing causes. The duration of events and conditions in fault and event trees are not specified. Quantification in this model construct is based on the (conditional) probabilities of the events and conditions. Typical events include system failure, human error and recognition of safety-relevant conditions.

A main advantage of fault and event trees is that once these trees have been built, they are typically well understandable for large audiences; hence they well support risk communication. Various views on accident causation indicate that fault and event trees may not be adequate to represent the complexity of modern socio-technical systems [6][13]. Key determinants of this complexity include the number and variety of organizational entities (human, groups, technical systems), the number and types of interdependencies between organizational entities, the degree of distribution of the entities (single/multiple locations), the types of dynamic performance of the entities (static/slow/fast), and the number and types of hazards in the organization. Limitations of fault and event trees include the difficulty to represent the large number of interdependencies between organizational entities and the dynamics of these interdependencies.

B. STAMP

It is recognised by Nancy Leveson [13] that often applied sequential accident models, which explain accidents in terms of multiple events sequenced as a chain over time, and related reliability engineering techniques do not effectively account for (1) social and organizational factors in accidents, (2) system accident and software errors, (3) human error, and (4)

adaptation over time. To account for these aspects, [13] presents a model based on system and control theory: STAMP (Systems-Theoretic Accident Model and Processes). In the underlying concept of safety, accidents occur when external disturbances, component failures, or dysfunctional interactions among components of a socio-technical system are not adequately controlled.

STAMP uses mathematical constructs based on system dynamics to describe the dynamics of organizational processes, their control interrelations and effects on safety. System dynamics [14] takes a top-down modelling approach using sets of coupled differential equations with exogenous variables, such as stock and flow diagrams, to describe organizational processes. In line with the general tendency of system dynamics, the variables in STAMP models typically are at aggregated organizational levels. The models are evaluated via simulation runs showing dynamic traces of relevant variables. By varying model settings, the effects of conditions and decisions on dynamic traces for variables of interest can be evaluated.

In recent work [15], the use of STAMP has been widened to qualitative approaches for prospective hazard analysis, called STPA (System-Theoretic Process Analysis); safety-guided design, which proactively uses STPA; and retrospective analysis of accidents and incidents, called CAST (Causal Analysis based on STAMP). For the focus on the analysis of safety and resilience in MAREA, the prospective analysis of STPA and its use in design is most relevant. STPA has two main steps: (1) Identify the potential for inadequate control of a system to a hazardous state, e.g. a required control action is not provided or not followed, an incorrect or unsafe control action is provided, or the timing of a control action is not appropriate; (2) Determine how each potentially hazardous control action identified in step 1 could occur, using analysis sub-steps with regard to the relevant control structures and process models.

C. FRAM

The Functional Resonance Analysis Method (FRAM) is a method developed by Erik Hollnagel and colleagues for the purpose of Resilience Engineering [6][7][8][9]. A FRAM analysis of an operation consists of the following steps.

- *Identifying functions:* Functions (e.g. activities, tasks) in the operation are identified and the following six aspects are described for each function: *Input* of the function; *Output* produced by the function; *Resource*, representing items such as hardware, procedures, software that are used to carry out the function; *Control*, describing items such as physical laws, work organization or control systems that supervise or restrict the function; *Precondition*, describing a condition that should exist for the function to evolve; and *Time*, describing time restrictions of the function.
- *Characterizing variability:* FRAM uses the following eleven common performance conditions (CPCs) as a basis for the analysis of potential variability in FRAM functions: 1) Availability of personnel and equipment, 2) Training, preparation competence, 3) Communication quality, 4) Human-machine interaction, operational support, 5) Availability of procedures, 6) Work conditions, 7) Goals, number and conflicts, 8) Available time, 9) Circadian rhythm, stress, 10) Team collaboration, 11) Organizational quality. The variability in a function resulting from these CPCs is determined qualitatively in terms of stability, predictability, sufficiency and boundaries of performance. The resulting variability can be expressed as failure modes or variability phenotypes, such as timing, duration, distance, speed, direction, sequence, quantity, accuracy, etc. [7].
- *Defining functional resonance:* The relations between the functions are described. In particular, the output of a function may be an input, precondition, or resource, control or time constraints for another function. The possible ways are assessed how the potential performance variability may spread through the interconnected system (e.g. dampen or amplify). The aim of this analysis is to find combinations of variability of the functions that may lead to 'functional resonance', i.e. situations where the system loses its capability to safely manage variability [1]. This analysis is done by qualitative reasoning on the functions' variability and interactions.
- *Identifying barriers and indicators:* The last step identifies barriers for variability and specifies required performance monitoring. The barriers intend to dampen too large variability and they can be distinguished in physical, functional, symbolic and incorporeal barrier systems [6]. The specification of indicators is focused on the detection of undesired variability. This step can be considered to be part of the design of an operation and the associated safety management, based upon the analysis results obtained in the previous steps.

FRAM has yet rarely been applied for actual safety analysis in ATM, but an illustration of its capabilities is provided for a safety study of a Minimum Safety Altitude Warning (MSAW) system in [9]. In this study a FRAM model was developed that includes ATM functions, such as monitoring, planning, coordination and pilot-controller communication, specific MSAW functions, such as generating MSAW alert or enabling MSAW alert, and organizational functions, such as manage resources and manage teamwork. It is assumed [9] that human performance variability can be represented by a function being precise/acceptable/imprecise qua precision and 'too early'/'on-time'/'too late' qua timing. Instantiations of interactions between the functions are provided during several phases in an approach scenario, where the MSAW alert was enabled imprecisely and the traffic situation evolves such that an MSAW alert should be given. These instantiations are given by graphical representations of the interactions between the functions and associated qualitative reasoning. Using such paper and pencil methods a qualitative evaluation of the MSAW system is illustrated for a particular combination of conditions.

D. *Multi-agent dynamic risk modelling*

Multi-agent dynamic risk modelling (DRM) is a method that is part of the TOPAZ safety risk methodology for the evaluation of air traffic accident risks [16]. It uses Monte Carlo simulations in combination with bias and uncertainty evaluations to obtain quantitative accident risk probabilities and insight in key contributions to the accident risk [17]. The bias and uncertainty evaluations include assessment of the impact on the risk of hazards that are not well covered by the dynamic risk model.

At a syntactic level, a multi-agent DRM is specified by a Stochastically and Dynamically Coloured Petri Net (SDCPN) [18]. At a semantic level several model constructs have been applied in multi-agent DRM, including the ones highlighted in the list below. Examples of these model constructs are provided in [12].

- *Multi-agent situation awareness:* The concept of situation awareness addresses perception of elements in the environment, their interpretation and the projection of the future status [19]. In an air traffic environment with multiple human operators, these aspects and associated errors of situation awareness depend on various human-human and human-machine interactions. The multi-agent situation awareness model construct describes the situation awareness of each agent (human operator, technical system) as time-dependent information of other agents, including identity, continuous state variables, mode variables and intent variables [20][21]. Achieving, acquiring and maintaining situation awareness depends on processes as observation, communication and reasoning, which are part of the tasks of the agent.
- *Task identification / scheduling / execution:* Given that a human operator has a number of tasks, the task identification construct determines the ways that the human operator identifies the tasks that need to be performed at a particular time instance, the task scheduling construct determines which tasks may be performed concurrently and a priority among tasks that cannot be performed concurrently, and the task execution model construct describes the performance of a human operator with regard to the execution of a specific task.
- *Cognitive control mode:* The cognitive control mode (CCM) modelling construct considers that humans can function in a number of cognitive control modes, such as Strategic, Tactical, Opportunistic and Scrambled [22]. The cognitive control mode may depend on human performance aspects such as the range of tasks to be done and the situation awareness of the human. It influences human performance aspects such as the planning horizon and the accuracy of task performance.
- *Human error:* The human error modelling construct considers that the execution of a task by a human operator may include large deviations from normal and intended practice and that such deviations may be expressed as 'errors'. The human error modelling construct does not represent in detail the mechanisms that may have given rise to the error, but it considers the behaviour resulting from these mechanisms at a probabilistic level for a specific task.
- *Decision making:* The decision making model construct describes the decision making on the basis of the situation awareness and decision rules by a human agent.
- *System mode:* A model construct that considers that the behaviour of a technical system can be described by modes. These modes are dynamically changing discrete states for the functioning the technical systems, such as failure conditions, system settings, etc.
- *Dynamic variability:* A model construct that describes the variability of states of agents due to dynamic processes. For instance, it can describe the movements of an aircraft according to differential equations relating states such as position, velocity, acceleration and thrust.
- *Stochastic variability:* A model construct to describe the stochastic variability in the performance of human operators and technical systems. For a human operator it specifies the variability in task aspects, e.g. duration, start time, accuracy, etc., in a contextual condition, i.e. given the state of other human performance model constructs, such as situation awareness, cognitive control mode and other human modes. The variability is represented by probability density functions with moments that may be functions of the contextual condition. Similarly, the variability of system functioning is described by context-dependent probability density functions.

E. *Key characteristics of safety modelling methods*

A summary of key characteristics of the discussed safety modelling methods is provided in Table II below.

TABLE II. KEY CHARACTERISTICS OF SAFETY MODELLING METHODS

Aspect	**FT/ET**	**STAMP**	**FRAM**	**Multi-agent DRM**
Scope	Operation	Organization	Operation	Operation
Techniques	Relations between events in trees	System dynamics	Qualitative relations between functions	Agent models, SDCPN
Model evaluation technique	Calculation of nested event probabilities	Simulation of system dynamics	Qualitative analysis by pen & paper	Monte Carlo simulation, speed-up techniques
Sensitivity analysis	Sensitivity for event probabilities may be evaluated, but is typically not done.	Study of variation in simulation traces for various settings	Not supported	Risk sensitivity & uncertainty of local aspects. Overall risk uncertainty.
Safety output	Risk probabilities, main risk contributions (events)	Quantitative safety indicators	Qualitative insight in safety-relevant relations between functions	Risk probabilities, risk sensitivities, and insight in key contributions (events, agents)

V. HAZARD COVERAGE BY EXISTING MODEL CONSTRUCTS

For safety risk assessments it is important that the model constructs cover all hazards identified. This section analyses the potential of hazard coverage by the methods of Section IV.

A. *Fault and event trees*

Fault and event trees represent specific orderings and/or logical combinations of events and conditions. The model constructs in these trees consider the ordering of relations between events and quantification is achieved by adopting probabilities for the events.

Considering the identified hazards, e.g. 'Failure of GPS system', 'Pilots do not monitor R/T indicated presence of other aircraft', 'Pilot is fatigued and sleepy' or 'Controller ignores an alert (no evaluation)', almost all hazards can be considered as an event or a condition. As a result, all these hazards could be included in a fault and/or event tree. In other words, the model construct in these trees is so generic that all these hazards can be represented in a fault/event tree. However, the question is *how* the events and conditions should be included in the fault/event tree structure and how *appropriate values* may be obtained for their probabilities in a safety analysis. As we have also argued previously [23][24], fault/event trees cannot well represent the large range of possible combinations of event occurrences in (dynamic) ATM scenarios, and it is very hard to obtain appropriate probability values of dependent events and conditions in ATM scenarios.

In conclusion, while fault and event trees may represent a variety of combinations of hazards, they often do not support effective assessment of the risk posed by these hazards nor of the level of resilience of the organization to deal with these hazards. Since the model construct in fault/event trees is so generic and it (thus) forms a large gap between the model and the physical reality, often little can be learnt from it with regard to the safety implications of the hazards.

B. *STAMP*

In STAMP [13] the focus has been on models for organizational processes and control mechanisms using system dynamics model constructs. The focus in these models on processes at aggregated organizational levels rather than at the level of agents (humans, technical systems) means that these models emphasize processes at the blunt end rather than interactions between individuals and technical systems at the sharp end. This indicates that model constructs are lacking for ATM hazards that relate to pilots, controllers, technical systems and their interactions. In particular, most of the hazards identified in our study reside on the sharp end or account for the effect of organizational aspects on human operators working at the sharp end.

In the recent broadening of STAMP to qualitative approaches for, among others, prospective hazard analysis (STPA), it has also been recognized by Nancy Leveson that additional techniques are needed for effective use of STPA in analysis of complex, human and software-intensive systems [15]. This recognition is well in line with the need identified in MAREA to develop a broader set of model constructs for analysis of safety and resilience of complex socio-technical systems, with a key focus on human related aspects.

C. *FRAM*

The basic model construct in FRAM is the hexagon with connections for input, precondition, resource, control and time, which all in some way impact the function performance, and a connection for output, which provides the result of the function. In principle, hazards may be considered to have influence on the interconnections between functions and/or on the variability of the functions. For instance, in an analysis of an MSAW system [9], human performance variability with respect to precision and timeliness were considered. In more conclusive analyses, more combinations of performance variability of the interacting functions may have to be accounted for. For instance, consider the broader list of performance variability aspects addressed by the common performance conditions of [7] or the lists of hazards identified in this study. However, a method for systematic evaluation of the large variety in possible combinations is yet lacking in FRAM. This limits its applicability to ATM safety assessments where combinations of performance variability and function interactions should be accounted for systematically.

In conclusion, key insights in the development of FRAM are the recognized need to focus on positive contributions of human performance in achieving resilience in complex systems and the recognition that thinking in terms of performance variability rather than human error is required to attain a better understanding of safety of complex systems. To this end, FRAM diagrams provide a broad overview of aspects of functions in an operation, interactions between the functions and human-related sources of variability of the performance of the functions. Introduction of methods for systematic evaluation of the impact of interactions between functions and performance variability of the functions is expected to be of significant benefit for FRAM.

D. *Multi-agent DRM*

Multi-agent dynamic risk modelling uses stochastic dynamic models of the performance of human operators and technical systems as a basis for accident risk assessment by Monte Carlo simulations and uncertainty evaluations. As these models have the potential to systematically represent performance variability of socio-technical systems, we performed a more detailed analysis of the numbers of hazards existing multi-agent DRM model constructs (as explained in Section IV) can cover.

For each of the hazards of Set I we identified the multi-agent DRM model constructs that can be used to represent the hazard in a multi-agent DRM [12]. An overview of the numbers of hazards that are well covered by one or several model constructs is provided in Table III. It indicates that 58% of the generalized hazards is well covered by the existing

multi-agent DRM model constructs, 11% is partly covered and 30% is not covered.

TABLE III. NUMBER OF HAZARDS AND COVERAGE PER CLUSTER

Hazard cluster	Number of hazards	Hazard coverage		
		Well	*Partly*	*Not*
Aircraft systems	14	11	2	1
Navigation systems	8	7	0	1
Surveillance systems	14	14	0	0
Speech-based communication	19	13	2	4
Datalink-based communication	10	9	0	1
Pilot performance	62	31	13	18
Controller performance	55	23	7	25
ATC systems	13	7	2	4
ATC coordination	12	8	0	4
Weather	14	2	4	8
Traffic	17	13	0	4
Infrastructure & environment	12	11	0	1
Other	18	6	0	10
Total	**266**	**155**	**30**	**81**

The hazards that are not or partly covered by the existing multi-agent DRM model constructs (i.e. 111 single hazards) have been aggregated in groups of hazards that are reflections of a similar phenomenon. The result of this process is shown in Table IV; the underlying single hazards are given in [12]. Thus, 40 groups have been found, which include 1 up to 9 single hazards.

TABLE IV. GROUPS OF HAZARDS NOT COMPLETELY COVERED BY CURRENT MULTI-AGENT DRM CONSTRUCTS

Group of hazards not or only partly covered by current multi-agent DRM constructs	Number of hazards
Handling of inconsistent, confusing or uncertain information by a human operator	9
The trust by a human in a system and the effect on the performance of the human	9
Bad weather or weather change	8
Bending rules to gain some advantage, with potential effects on safety	7
Complex or unclear procedures leading to confusion by a human	7
Changes or differences in procedures leading to confusion, errors or lack of operational fluency by a human	6
Lack of experience, training or testing with degraded modes, fall-back options and contingency procedures	6
Cultural or language differences	5
Handling of flight progress strips by a controller	5
Security intrusion (e.g. hijack) and potential effects (e.g. military intervention)	4
Organizational changes (e.g. other functions, colleagues) or problems (e.g. strike) affecting the performance of a human operator	4
Lack of appropriate maintenance of technical systems	3
Negotiation processing and the effect of the feeling and behaviour of humans	3
The causes and effects of fatigue and sleepiness of humans	3
Feeling to be put in second place / not fully respected	2
Feeling restricted in freedom to perform as a human considers best	2
Attention tunnelling	2
Lack of training and the effects on the performance of humans	2
Difficulty for humans to have a mental model of a 4D trajectory and the effect on their performance	2
Poor safety culture and its effect on the performance of humans	2
Deciding on risks and priorities of complex air traffic scenarios	2
Display clutter or display not well visible and the effect on the behaviour and situation awareness of humans	2
Problems with access rights to System Wide Information Exchange System	2
Unmanned Aerial Vehicles	2
Unstabilised approach	1
Handling of inconsistent information by a technical system	1
Complex procedure causes R/T overload	1
A jolly atmosphere	1
The trust by a human in another human and the effect on the performance of the human	1
Human does not know when to take action	1
Clutter of audio messages and the effect on the behaviour and situation awareness of humans	1
Human losing interest in new information because of large number of information updates	1
Complacency of a human	1
Radar coverage problems when merging or splitting ATC sectors	1
Weather forecast wrong	1
Strong turbulence	1
Icing of the wings	1
High uncertainty in planning due to the influence of many agents	1
Agent not willing to share information with another agent (e.g. military and civil ATC)	1
Uncontrolled aircraft	1

VI. DISCUSSION

A key notion in arguing about the contributions of human operators to resilience is 'performance variability'. As a structured approach for the identification of sources of performance variability in ATM, in this report we used a broad set of hazards in the ATM Hazard Database of NLR. The hazards in this database address 'anything that may influence safety' and have primarily been identified in brainstorm sessions, which aim to include a broad coverage of human behaviour, conditions influencing human behaviour and human-human and human-machine interactions. We identified a set of unique and generalized hazards in the database, leading to 525 hazards. Many of these hazards refer to human performance or describe contextual conditions for pilots and controllers. These hazards thus provide a broad overview of sources for performance variability in ATM, with a focus on human performance.

To obtain an overview of manifestations of performance variability as a result of the hazards, we interviewed controllers and pilots about the ways that they would deal with the hazards and how their work would be impacted, and about the existence of related procedures. The detailed results in [12] provide an extensive overview of practical performance variability in ATM. These results provide a basis for advancing models of human performance variability in ATM and thereby for analysis of resilience in ATM.

We studied the ability of several methods to systematically describe and analyse performance variability in ATM as a way towards understanding resilience in ATM.

- Fault and event trees are often used in ATM safety assessments. It was concluded that the basic model construct in such trees, being an event or condition, is so generic that it can in principle represent almost any hazard (or source of performance variability). However, these trees cannot well represent the large numbers of possible combinations of conditions and dynamic event occurrences. Therefore, it is not possible to systematically evaluate dynamically dependent events and conditions, and the obtained insight in safety and resilience is often limited.
- STAMP uses mathematical constructs based on system dynamics to describe interactions and dynamics between organizational processes and their effect on safety from a top level perspective. This focus means that model constructs are lacking for a considerable number of the ATM hazards that relate to pilots, controllers, technical systems and their interactions.
- FRAM uses hexagons to describe functions, characterizations of variability of the functions and diagrams of relations between functions as a basis for qualitative reasoning about the spread of performance variability in an interconnected system. In this way a broad psychological perspective is attained on human performance contributions to attaining resilience in complex systems. Current FRAM methods do not yet include means to systematically evaluate the impact of interactions between functions and performance variability of the functions.
- Multi-agent dynamic risk modelling for ATM includes several modelling constructs to systematically describe the interactions of humans and technical systems in ATM scenarios, and to systematically include sources of performance variability in these models. It was shown in ATM safety assessments, that such modelling provides accident risk results as well as insight in the contribution of humans, technical systems and associated hazards to these accident risk levels.

In conclusion, these methods cover a variety of ways to address performance variability in ATM scenarios. To systematically analyse the risk of and resilience in ATM scenarios, we consider that multi-agent dynamic risk modelling has most potential. Since human performance variability should be well covered in such modelling, the link with the psychological perspective adhered in FRAM needs to be well addressed in subsequent steps in the MAREA project. In the MAREA project it is foreseen to develop a broader set of model constructs in WP2. Bases for this development are the hazards that are not or partly covered by current multi-agent DRM constructs and the manifestations of performance variability found in the interviews with pilots and controllers.

DISCLAIMER

The views expressed in this research paper are those of the authors. The paper does not purport to represent views or policies of NLR, Eurocontrol or SJU.

REFERENCES

[1] Eurocontrol. A white paper on Resilience Engineering for ATM. September 2009

[2] Hollnagel E, Woods DD, Leveson N. Resilience engineering: Concepts and precepts. Ashgate, Aldershot, England, 2006

[3] FAA/Eurocontrol AP15. Human performance in air traffic management safety: A white paper. Eurocontrol, August 2010

[4] Hollnagel E, Nemeth CP, Dekker S. Resilience Engineering Perspectives, Volume 1: Remaining sensitive to the possibility of failure. Ashgate, Aldershot, England, 2008

[5] Nemeth CP, Hollnagel E, Dekker S. Resilience Engineering Perspectives, Volume 2: Preparation and restoration. Ashgate, Aldershot, England, 2009

[6] Hollnagel E. Barriers and accident prevention. Ashgate, England, 2004

[7] Woltjer R, Hollnagel E. Functional modeling for risk assessment of automation in a changing air traffic management environment. Fourth International Conference Working on Safety, Crete, Greece, 2008

[8] Woltjer R. Functional modeling of constraint management in aviation safety and command and control. PhD Thesis Linköping University, no. 1249, 2009

[9] Macchi L, Hollnagel E, Leonhard J. Resilience engineering approach to safety assessment: An application of FRAM for the MSAW system. Mines ParisTech, hal-00572933, version 1, 2 March 2011

[10] ComplexWorld Team. D3.5 Complex ATM white paper. Issue 1, 15 July 2011

[11] De Jong HH. Guidelines for the identification of hazards: How to make unimaginable hazards imaginable, National Aerospace laboratory NLR, report NLR-CR-2004-094, March 2004

[12] Stroeve SH, Everdij MHC, Blom HAP. E.02.10-MAREA-D1.2-Hazards in ATM: model constructs, coverage and human responses, October 2011

[13] Leveson NG. A new accident model for engineering safer systems, Safety Science, Vol. 42, pp. 237-270, 2004

[14] Forrester JW. Industrial dynamics. Pegasus Communications, Waltham (MA), USA, 1961

[15] Leveson NG. Engineering a safer world: Systems thinking applied to safety. http://sunnyday.mit.edu/safer-world/safer-world.pdf, 2009

[16] Blom HAP, Bakker GJ, Blanker PJG, Daams J, Everdij MHC, Klompstra MB. Accident risk assessment for advanced air traffic management. In: Donohue GL and Zellweger AG (eds.), Air Transport Systems Engineering, AIAA, pp. 463-480, 2001

[17] Stroeve SH, Blom HAP, Bakker GJ. Systemic accident risk assessment in air traffic by Monte Carlo simulation. Safety Science 47:238-449, 2009

[18] Everdij MHC, Klompstra MB, Blom HAP, Klein Obbink B. 'Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets', H.A.P. Blom, J. Lygeros (eds.), Stochastic hybrid systems: Theory and safety critical applications, Springer, 2006, pp. 325-350, 2006

[19] Endsley MR. Towards a theory of situation awareness in dynamic systems. Human Factors, 37(1): 32-64, 1995

[20] Stroeve SH, Blom HAP, Van der Park M, Multi-agent situation awareness error evolution in accident risk modelling. Proceedings 5th USA/Europe Air Traffic Management R&D Seminar, Budapest, Hungary, 23-27 June 2003

[21] Blom HAP, Stroeve SH. Multi-agent situation awareness error evolution in air traffic. Proceedings 6th Probabilistic Safety Assessment and Management Conference, Berlin, Germany, 2004

[22] Hollnagel E. Human Reliability analysis, context and control. Academic press, London, 1993

[23] Everdij MHC, Stroeve SH. 'Feasibility study on Dynamic Risk Modelling for ATM Applications', Final report for Eurocontrol, March 2009, NLR-CR-2008-512

[24] Stroeve SH, Blom HAP, Bakker GJ. Contrasting safety assessment of a runway incursion scenario by event trees and agent-based dynamic risk modelling. Ninth USA/Europe ATM R&D Seminar, Berlin, June 2011