System Performances under Automation Degradation (SPAD)

E. Hollnagel[3], C. Martinie[1], P. Palanque[1], A. Pasquini[2], M. Ragosta[1,2], E. Rigaud[3], S. Silvagni[2]

[1] University Paul Sabatier,
CS-IRIT
118, route de Narbonne
31062 Toulouse Cedex 9
{martinie, palanque, ragosta}@irit.fr

[2] DeepBlue Srl
Piazza Buenos Aires 20,
00198 Roma - Italy
{alberto.pasquini,
sara.silvagni}@dblue.it

[3] ARMINES
Rue Claude Daunesse, B.P. 207
06904 Sophia Antipolis
erik.hollnagel@mines-paristech.fr
Eric.Rigaud@mines-paristech.fr

Foreword **- This paper describes a project that is part of SESAR Workpackage E, which is addressing long-term and innovative research. The project was started early 2011 so this description is limited to an outline of the project objectives augmented by some early findings.**

Abstract **- Increased automation is one of the main changes foreseen by SESAR in ATM. This will pose new challenges including possible automation degradation. The premise for the SPAD project is that degradation of systems automation is unavoidable due either to internal (e.g. human, software or system failure) or external (e.g. weather, strikes, malicious behaviors) events (or both). There is thus a need to understand, monitor and manage how automation degradation of a single system may propagate to the overall ATM system, and to define ways to confine and absorb degradation problems, with and without human contribution. There is also a need to estimate the implications of degradations for the overall ATM system performances. These aspects will be investigated by SPAD, which has the following aims: 1) understanding, modelling and estimating the propagation of automation degradation in ATM; 2) estimating the consequences of automation degradation on ATM performances; 3) supporting an effective intervention for the containment of automation degradation. This paper presents the early findings by the SPAD project after 6 months of work and presents the investigations that will be carried out in the next months.**

Keywords - automation, resilience, degradation, models, ATM.

I. PROBLEM DESCRIPTION AND OBJECTIVES

The continuing increase of traffic demand and new business challenges will bring the current ATM system to its capacity limits by 2013-2015. An overall productivity improvement is therefore urgently needed and the paths to this have been outlined by SESAR in the "ATM Target concept". As foreseen by SESAR, a common enabler to meet the new capacity and efficiency demands is an increase of automation to support, and in some long term case even replace, tasks currently performed by humans. Human operators will be able in this way to manage a higher number of tasks and will shift their roles toward more strategic ones. Some of the keys to the future Concept for the ATM system are a drastic reduction of controllers' task load trough increased automation in conflict detection and resolution, as well as higher levels of automation for data gathering and management.

Higher levels of automation reduce system flexibility, which is a key feature to deal with non-standard or unexpected events, cf., the so called "Planning vs. Flexibility paradox". Indeed a system which has been carefully planned, standardised, and automated is unable to respond to non-standard and unplanned events such as technical failures. In addition to the difficulty of specifying, implementing and testing such automated systems the decrease in flexibility may make the ATM system more sensitive to degradation problems.

There is a need to understand how automation degradation will propagate in SESAR scenarios, where the number of interconnections will significantly increase. The increased coupling of the ATM systems makes it harder to identify and isolate failures when they occur, and to detect minor malfunctions before they propagate to the whole system. While many studies have focused on automation and automation classification and [8]established an automation taxonomy, little is known about automation degradation, how it propagates in a complex system, and what the links are between degradation and system performances. This knowledge gap must be filled to cope with the challenges in the SESAR future of ATM.

The aims of SPAD project are accordingly:

- To understand, model and estimate the propagation of automation degradation in ATM, and to evaluate the associated consequences on ATM performances.
- To validate the above results on a large ATM system with high degree of automation.
- To develop a demonstration prototype for monitoring degradation and estimating its propagation and the related reduction of performances in a large ATM system with high degree of automation.

SPAD will follow two complementary paths to reach these objectives. The first will build models that support abstraction and multiple views on the problem. The second will exploit simulation through both user and system testing via multilevel scenarios. These two aspects will be presented through a generic description of the approach in section III and exemplified in section IV.

II. EXPECTED OUTCOME, CONTRIBUTION TO ATM AND CONNECTION WITH RELATED WORK

The concrete outcome of the project will be:

- The identification of a set of key performance indicators that can be used for the assessment of the evolution of the performances fluctuations.
- A federation of models that can describe automation degradation propagation and its effects on ATM performances. In terms of concrete application we will deliver instantiations of the federation of models for each of the systems studied in the project.
- A validation report with the evaluation of the performance of the federation of models and recommendations for further improvements useful for researchers investigating the same subject.
- A prototype for monitoring automation degradation based on predefined scenarios. The predictive ability of the model federation will be used to forecast performances evolutions. These predictions will be compared to observed from the prototype. Using this we will be able to estimate degradation propagation and its effect on ATM performances. In addition, by using performance indicators that relate to system functions, the federation of models embedded in the prototype will enable the identification of possible interventions, either to sustain performance at an appropriate level or to ensure a graceful degradation.

III. PROPOSED APPROACH

We consider ATM as a Large Scale Socio-Technical System that combines its resources and capabilities in order to achieve a common goal. Modelling of systems of systems is complex for several reasons: the need to consider multiple levels and domains; the overall complexity and the variety of component systems; the level of uncertainty that remains in their behaviour and interactions.

One approach to study such systems has been to combine models offering different perspectives of the system under study and analysing them at different levels of granularity. A widely used approach following this philosophy is UML [10] exploiting nine different models/notations for describing data intensive software. More recently SysML [7]has been designed in order to introduce a broader (system oriented) perspective to UML resulting in the addition of other models (e.g. a model for describing requirements that was not present in UML).

This approach is relevant for SPAD since we do not need a homomorphy of the ATM system. Since we intend to study the propagation of automation degradation and the related influences on performances, our interest will be limited to only a few aspects of the ATM system. At the level of the single component system where the degradation starts, we will focus on the core and critical functions of the system. At the integration level, when we consider this system in the context of other systems, our interest shifts to the interactions between the systems and the links to overall performances. For this reason we do not intend to develop a large scale stand-alone model but will rather focus on a limited number of essential specific aspects of the systems, using upgraded versions of existing models combined in federation. Each model will focus on a specific characteristic (e.g. functional aspects, interactions and propagation, human behavior and its interaction with the system) and represent a part of the whole ATM system with variable levels of granularity (from coarse to fine) depending on the interest of the analysis. An example of the areas covered by different models is shown in **Figure 1**.

Figure 1 shows the three main views that will be adopted in SPAD. The first one called “Behavioral oriented model” represents behavioral information at the ATC position. It explicitly deals with the operators’ activities and how their activities are made available to the other systems by means of communication channels. The second view is called “Functional oriented model” and includes both the autonomous functions of the position but also the connected equipment of the related aircrafts. The figure explicitly refers to UAV but other aircrafts are also considered. The last view is call “interaction oriented model” and brings in the broader perspective of systems of systems.

Federation of Models - We plan to adopt a federation of models to guarantee that interaction between models are meaningful at both conceptual and technical level. In particular, our federation will address:

- Information exchange mechanisms that ensures the capability to exchange information between federated models during the analysis;
- Compatibility of the representations to ensure federated models will have meaningful and compatible information exchange about the entities;
- Environmental representation to ensure federated models will have a shared and correlated environment.

To achieve these objectives the federation of models shall be able to work at different levels of abstractions from the single system till the top system of systems level. At the system level we need an articulated model of what is required for the system to carry out its operations, to monitor and measure automation degradation and its containment including the possible contribution of humans to resilience. When considering this system in integration with other systems we need a model of interaction and coupling between the different systems, to understand and measure degradation propagation and the link with the overall performances. The basic set of models of the federation has been already identified (e.g. TROPOS [1] or [2] and FRAM [6]) and the selection will be finalised during the initial phases of the project and refined using the case studies (see later in this Section). Indeed, 6 months into the project other models are now considered (see

section IV) even though their fit to the objectives is still investigated.

Adapting the Models with the Case Studies - Models are based on abstractions, idealization, and assumptions. In order to get trustworthy results from these models they shall be adjusted to the reference system. We plan to use scenarios from several reference systems having different levels of automation and different implementation perspectives. The initial systems considered were:

- An Arrival Manager (AMAN), which is a ground based planning tool that suggests to the air traffic controller an optimal arrival sequence of aircraft and providing support in establishing the optimal aircraft approach routes.
- An Airborne Spacing Sequencing and Merging (ASPA-S&M) with a full Flight Management System (FMS) integrated solution assisting the pilot. This is a set of systems supporting the flight crew to guarantee a time or distance based spacing from designated aircraft as requested by the air traffic controller.
- An Unmanned Aerial System (UAS) for automated self-separation of Unmanned Aerial Vehicles (UAV), ensuring that each UAV can reach the desired destination with the optimal route without conflict with other aircraft or UAV and without human intervention.

For each case study we will develop three scenarios of growing degradation severity. For example, for the UAS we considered the following possible degradations:

- one of the UAV has sporadic communication problems delaying its transmission and then affecting the consensus mechanism for determining the optimal trajectories;
- one of the UAV does not follow the trajectory assigned to it;
- one of the UAV does not collaborate at all. It does not follow the trajectory assigned to it and does not transmit its position.

This design requires nine scenarios with all the possible combinations of low, medium and high automation and low, medium and high degradation severity. For each scenario we will have to analyse the effects of automation degradation, how this can propagate, and the effect on the local and overall ATM performances. Scenarios will be reviewed and refined in collaboration with operational experts. Applying the models in federation on these scenarios we will evaluate their ability to model adequately the situation, adjust their performances, integrate them with other models if necessary, and calibrate them.

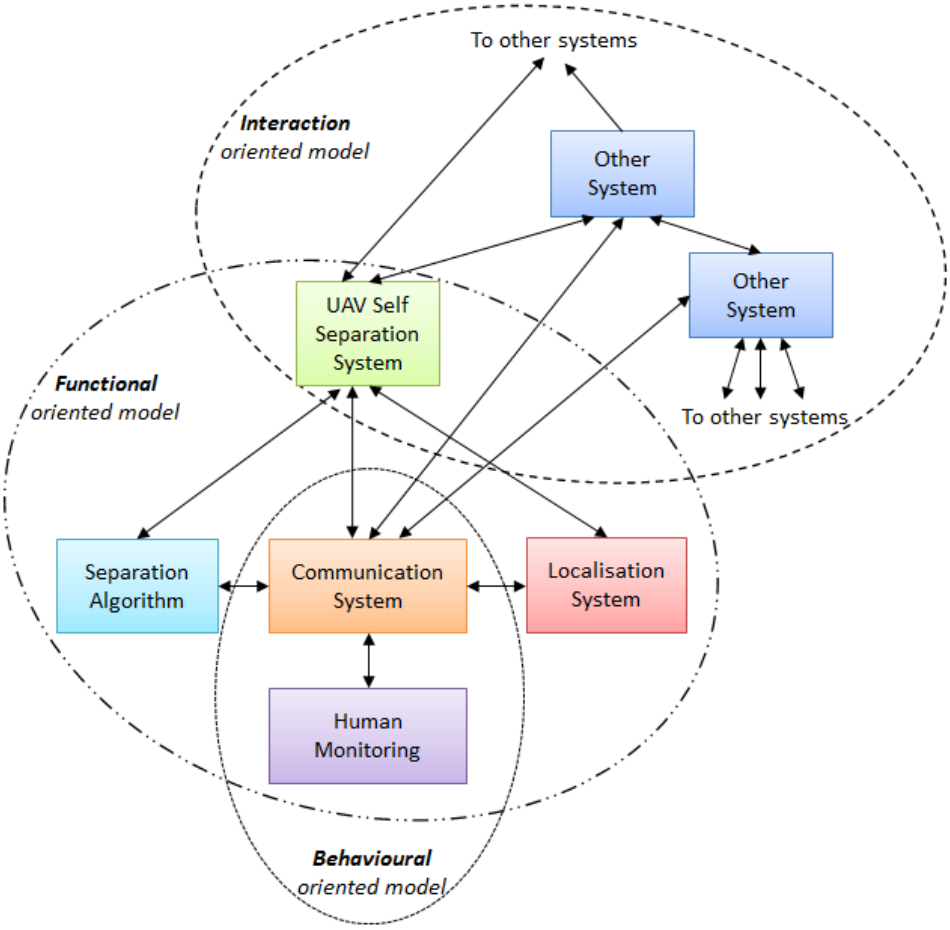

Figure 1. Various models and their contribution as a federation to the understanding of impact of degradations

The first two case studies keep the human operator in the loop and will thus be used to model the potential human role in the containment of the degradation propagation.

At current stage of the project these case studies are being reconsidered in the light of the objectives of the projects. The number of case studies may be reduced to allow more depth in the study of the scenarios that remain.

Validating Models – This section presents (using as an example the UAV case study) how models and simulation will be integrated in the project. We will be able to animate the Unmanned Aerial System (the third of the case studies) through an integrated set of simulators. These can simulate and represent the behaviour of each UAV; their separation algorithms; their communication, and localisation devices. Simulators will also show real traffic using an ADS-B ground station, and merge within it the simulated UAV. Using these simulators we will be able to reproduce a significant portion of airspace with both UAV and piloted aircraft. UAV operation will be completely automated with human intervening only in case of system degradation to activate predefined containment and recovery strategies. The initial version of these simulators will be provided by the European project ARCA [11] in the framework of a scientific collaboration between SPAD and ARCA. Simulators will be adapted to be used as test-bed for the federation of models, developed in the first part of the project.

Through evaluation runs at different levels of degradation severity we will evaluate the following abilities of the Federation:

- Ability to describe properly the degradation propagation
- Ability to take into account containment and recovery strategies (limited to a pre-defined set only)
- Ability to estimate the degradation effect on the overall system operational performances (limited to capacity and flexibility)

A validation report will report the results together with recommendations and all the practical indication to refine the Federation and the constituent models on the basis of the simulation outcome and of the related analysis.

Developing the simulator - The set of simulators produced in ARCA will be adapted to our project and completed with a tool to monitor and measure degradation and estimate its propagation and reduction of performances in the UAS system. The tool will also identify opportunities for effective countermeasures, responses, and early warnings, which can be used as a basis for possible reconfigurations.

This tool will exploit the prediction ability of our federation of models. The federation of models will be executed having as input data from the ARCA simulators regarding the operational conditions. In cases of degradation the models will provide information about its possible evolution and propagation, and estimate the influences this degradation will have on system performance. The functional modelling will also be used to identify opportunities for possible countermeasures and responses, and early warnings to be used as basis for reconfiguration.

Since our models will be either relatively simple because they are related to single systems (e.g. Tropos), or based on a few simple principles and recursive (e.g. FRAM), they will be quite easy to implement by software. This tool will represent the implementation in a prototype of the SPAD approach, demonstrating how it can be used in real systems for monitoring and estimating degradation propagation and reduction of performances and to facilitate an effective intervention in the degradation lifecycle.

Iç. FIRST RESULTS

The progresses in the project after 6 months are described in this section. As we are still in the early stages we may reconsider current results according to the project evolution.

The scenarios that will be used have been detailed and refined especially in the context of the AMAN case study (presented below). Several models have been tested on that same case study (TROPOS, FRAM, HAMSTERS) and is also presented.

Detailed description of scenarios

In the future of ATM the increase of automation requires the investigation of new challenges including those related to possible degradations. The aim of the SPAD project is to study the propagation of automation degradation from a single system to the overall ATM system and the ability to confine and absorb the effects. An additional objective is to evaluate the descriptive capabilities of existing models, to see whether various models can consistent and complementary, and ultimately to suggest possible solutions to improve Air Traffic Management. The SPAD project will propose several case studies and each of which will take into account different scenarios with growing levels of the impact of the degradation of automation.

In line with the aim of evaluating the impact of degradations of automation at different levels (low, medium and high) and of comparing the different levels between them, we propose a supplementary scenario, called "*nominal scenario*" with no degradation. This will be the baseline for the comparison of the impact of automation degradation. This comparison will use the set of key performance indicators that is still under identification and validation.

The nominal scenario contains a simplified representation of the ATM world with a restricted number of airports, aircraft, ACC and TMA, pilots and controllers. In addition, we take into account a restricted number of tools and ATM functions to facilitate the investigation of the propagation of automation degradation. However, the remaining functions are chosen carefully in order for the results to remain representative.

As shown in **Figure 2**, the nominal scenario contains four airports (called A, B, C and D), each composed of one Tower (TWR) and a series of structures for aircraft approaches and departure. Air Traffic is controlled by two Area Control Centers (called ACC1 and ACC2) responsible for controlling aircraft en-route in a particular volume of airspace (sector) at high altitudes and in between airport approaches and departures

.

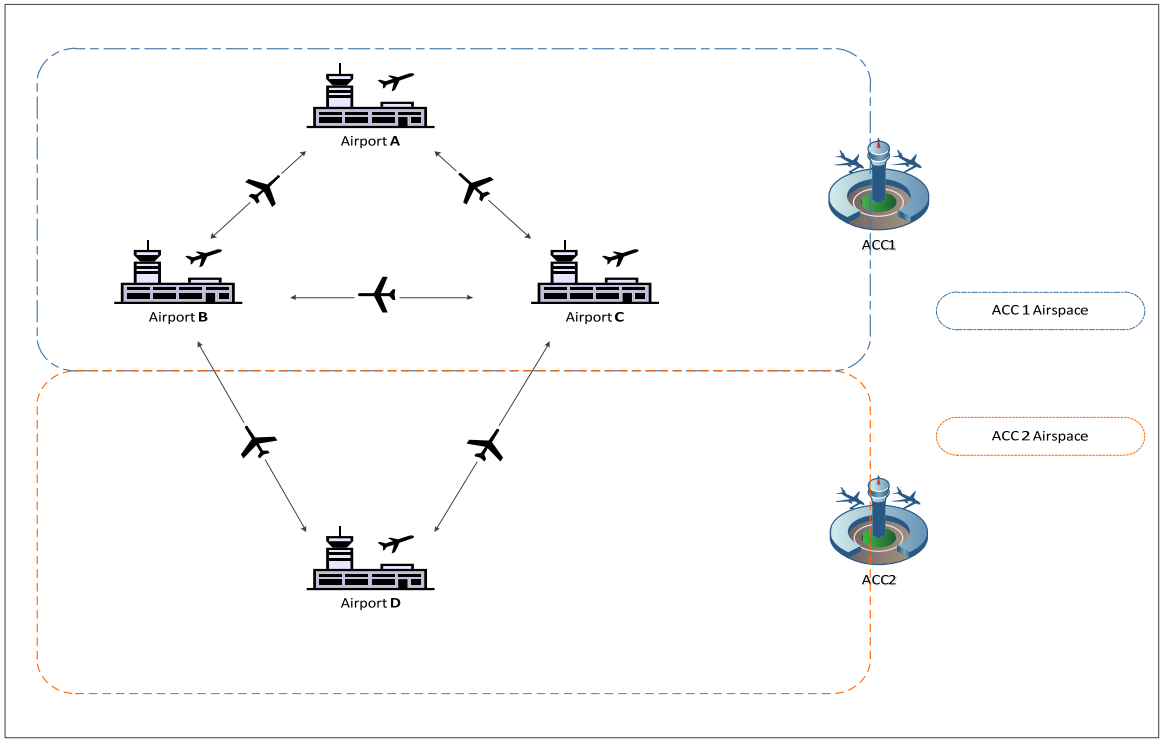

Figure 2. Structures involved in the scenario

Each element incorporates some specific instrumentation for the management of the information flow and provides particular roles for its controlling and supervision. While independent they all concur to achieve the same goal: a safe air traffic management as close as possible to the expected schedule.

The connections between the structures can be *direct* (i.e. Airport A is directly connected with Airports B and C) or *indirect* (i. e. Airport A is indirectly connected with Airport D because the air traffic flow and the information are mediated by the other two airports). So we can consider different levels of the impact of the degradation of automation:

1. **confined degradation**: the degradation affects only the structure or the system where the malfunctioning has taken place (i.e. Airport A, in the picture before),
2. **average degradation**: the degradation affects other systems directly connected to the one in which the malfunctioning has taken place (i.e. from Airport A to the airports directly connected with it as the Airport B and Airport C)
3. **extended degradation**: the degradation affects all the structures or the systems, directly and indirectly connected with the system where the malfunctioning was originated (i.e. in the previous picture it affects also the remote connection with Airport D).

This produces three scenarios with growing levels of the impact of the degradation of automation.

Preliminary study of candidate models

1) TROPOS

This is a goal–oriented model. Figure 3 illustrates an example of TROPOS applied to the first case study of the SPAD project, the AMAN system. In Figure 3:

- AMAN computes the arrival sequence
- Only COO can approve and manually modify the arrival sequence if needed
- The arrival sequence is displayed in CWP monitor
- TCC supports COO in verification of the sequence
- AMAN monitors and applies separation criteria
- AMAN generates advisories based on approved sequence.

To better understand the model and the picture, some notions typically used in TROPOS need to be explained:

- ✓ **AND decomposition**: a goal can be decomposed in to several subgoals, meaning that top goal can be satisfied if all subgoals are achieved.
- ✓ **Te**: *Trust of Execution* relationship between two actors indicates the belief of one truster that a trustee is able to achieve a goal, execute a plan, or deliver a resource.
- ✓ **De**: *Delegation of Execution* relationship between two actors indicates that one delegater delegates to a delegatee the achievement of a goal or execution of a plan.

We can see that there are some **De** and **Te** to AMAN and COO that at the beginning were goals or subgoals of TCC like *"Arrival sequence creation"* and its subgoals *"Manual update the sequence"* or *"Verification and application of separation criteria"*. While they are on TCC side, they are executed or by the AMAN system or by the COO.

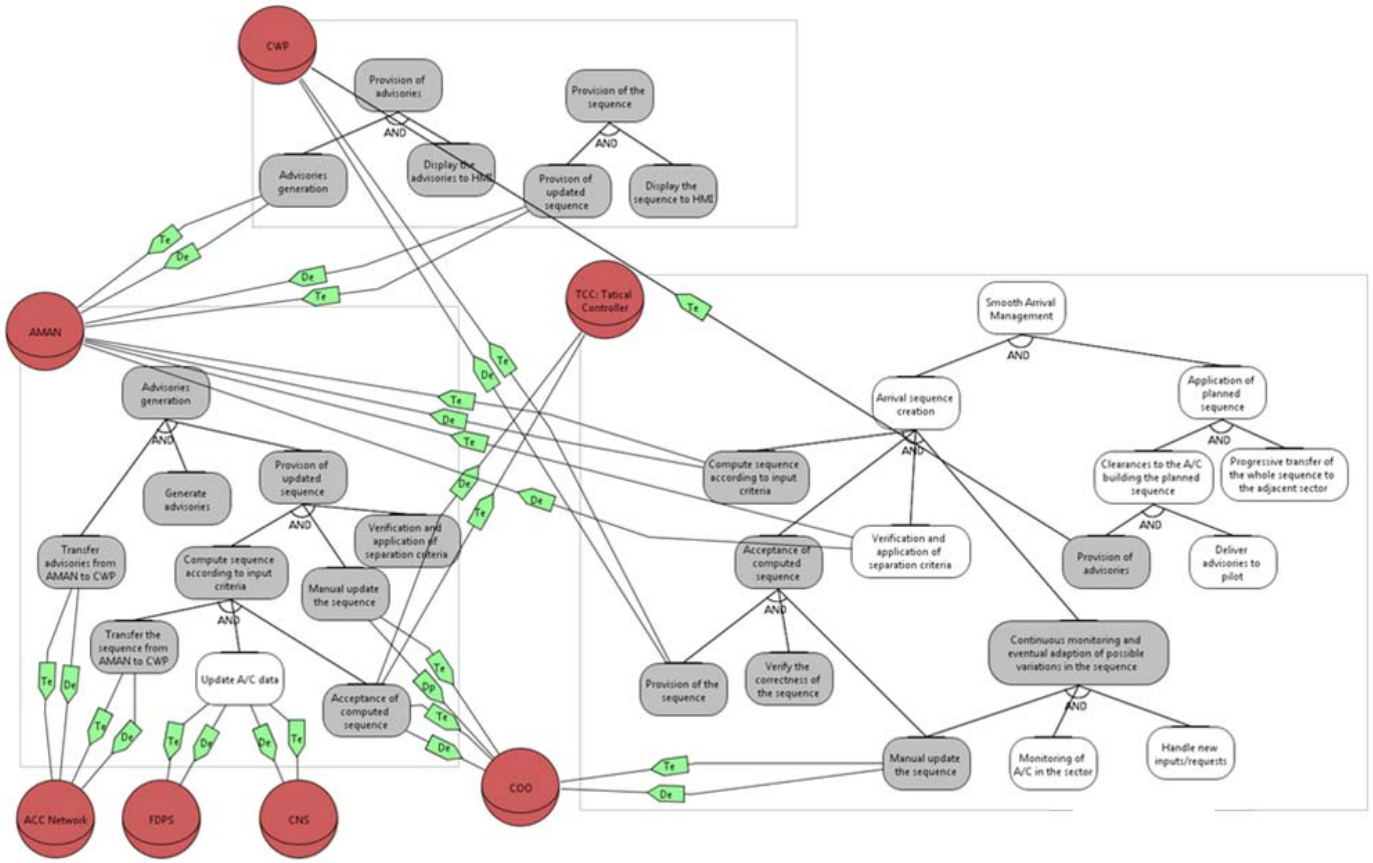

Figure 3. A TROPOS representation of advanced version of AMAN

1) FRAM

The FRAM is based on four principles [6]:

1) the equivalence of success and failures because these last ones represent the adjustments necessary to cope with the under specification found in complex real-world classifications,

2) the principle of approximate adjustments because to get anything done people must adjust their performance to the current conditions; since resources and time are finite, such adjustment will inevitably be approximate,

3) the principle of emergence, both failures and normal performance are emergent phenomena: neither can be attributed to or explained simply by referring to the (mal)functions of specific components or parts,

4) the principle of functional resonance substitutes the traditional cause- – effect relationship. The resonance explains how disproportionate large consequences can arise from seemingly small variations in performance and conditions.

A socio technical system is represented by a set of connected function. **Figure** 4 shows the graphical representation of a FRAM functions.

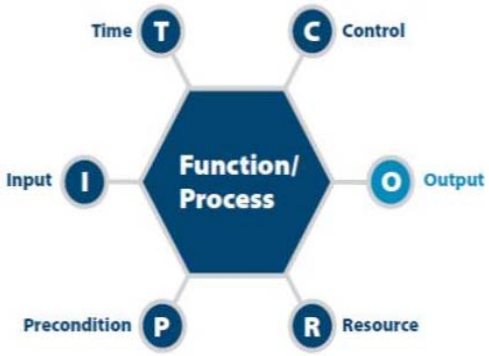

Figure 4. The six aspects of a FRAM function

Figure 5 shows the use of FRAM to part of the AMAN case study, namely the three functions needed to process aircrafts from their arrival in the airspace managed by AMAN (left-hand side of the Figure). It ends by producing an advisory of arrival sequence list (SEQ_LIST) and timing information (TTL/TTG) representing respectively Time To Land and Time To Gate information.

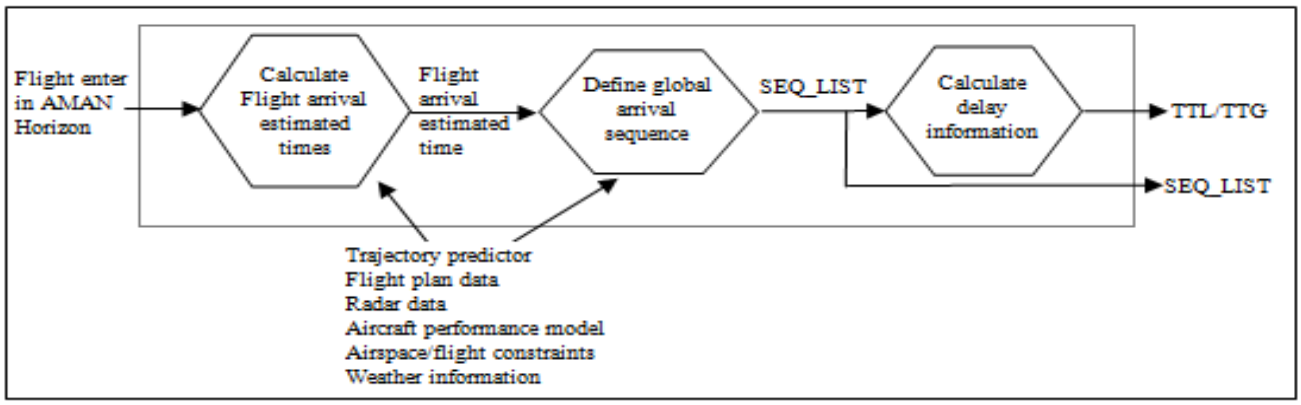

Figure 5. FRAM model of the internal functioning of AMAN

2) HAMSTERS

HAMSTERS[1] (**H**uman-centered **A**ssessment and **M**odeling to **S**upport **T**ask **E**ngineering for **R**esilient **S**ystems), is inspired by existing notations, in particular Concur Task Trees (CTT) and has been intended to remain compatible with this at the users level. Indeed both can be considered as hierarchical and graphical models representing relationship between tasks by means of operators (see Table 2). However, HAMSTERS involves extensions such as conditions associated to task executions, data flow across task models etc. extending its expression power beyond the one of CTT. HAMSTERS is publicly available, featuring a task simulator and providing a dedicated API for observing editing and simulation events.

TABLE 1. Tasks types in HAMSTERS

Task type	Icons in HAMSTERS task model
Abstract Task	Abstract task
System Task	System task
User Tasks	User task, Cognitive task, Perceptive task, Motor task
Interactive Tasks	Interactive task, Input task, Output task, InputOutput task

As presented in Table 1, the elements of task models in HAMSTERS include:

- ***Abstract task***: a task that involves sub tasks of any types.
- ***System function***: a function performed only by the system.
- ***User task***: a generic task describing a user activity. It can be specialized (from left to right on Table 1) as Cognitive task (e.g. comparing value, remembering information), Perceptual task (e.g. reading some information) or Motor task (e.g. pressing a button).
- ***Interactive task***: a task describing an interaction between the user and the system. It can be refined (from left to right on Table 1) into Input task when the users provide input to the system, Output task when the system provides an output to the user and InputOutput task (both but in an atomic way).

As for CTT, each task in HAMSTERS can be *iterative*, *optional* or *both* (as graphically shown in the following figure).

Figure 6. Icons of Optional, Iterative and both iterative and optional tasks

An *iterative* task can be executed one or several times but can be interrupted or suspended by another task. An *optional* task does not necessarily need to be executed. Again, as in CTT temporal relationship between tasks is represented by means of operators as described by the following table.

In HAMSTERS, the notion of object represents the elements of the world manipulated by tasks. HAMSTERS offers constructs for representing the information flow between tasks.

TABLE 2. Illustration of the operator type within HAMSTERS

Operator type	Sym-bol	Description
Enable	>>	ENABLE operator allows its tasks and/or task group and/or operator groups to execute one after the other, from left to right.
Concur-rent	|||	CONCURRENT operator allows tasks and/or tasks belonging to task groups and/or operator groups to execute "at the same time" in any order.
Choice	[]	CHOICE operator allows the user to select the first available task to execute among each available sub-branch. When a task is executed, HAMSTERS disables all the other branches that don't contain the executed task.
Disable	[>	DISABLE operator shall deactivate the execution of the first branch when a task is executed on the second branch. DISABLE operator shall have 2 and only 2 branches.
Suspend-resume	|>	SUSPEND-RESUME operator suspends the execution of the first task or branch when task is executed on the second branch.

Figure 7 describes the tasks (using HAMSTERS notation) that have to be performed by the Sequence Manager (SEQ_MAN) to achieve the "Manage and supervise the AMAN system" goal. To reach this main goal he/she has to accomplish several subgoals (*"Monitor the advisories"*

[1] http://www.irit.fr/recherches/ICS/softwares/hamsters/index.html

"Supervise the SEQ_LIST" "Take into account the requests of the EXE_TMA") at the same time ("|||"operator). These subgoals are iterative and abstract tasks can be decomposed into additional abstract and cognitive tasks as shown for the "Supervise the SEQ_LIST" subgoal (to fit the image in a limited space the other subgoals were collected with the FOLD function that is represented by a plus sign "[+]" in the lower left of each subgoals). The tasks that are performed by the SEQ_MAN to achieve the "Modify the SEQ_LIST" subgoal consist in checking the sequence list ("*Check the SEQ_LIST*" output task) and then, in sequence (">>" operator), *"Decide to switch the position of the aircraft"* cognitive task, *"Modify the SEQ_LIST"* and to complete this series of tasks *"Inform the EXE_TMA about the change"* which is an user task.

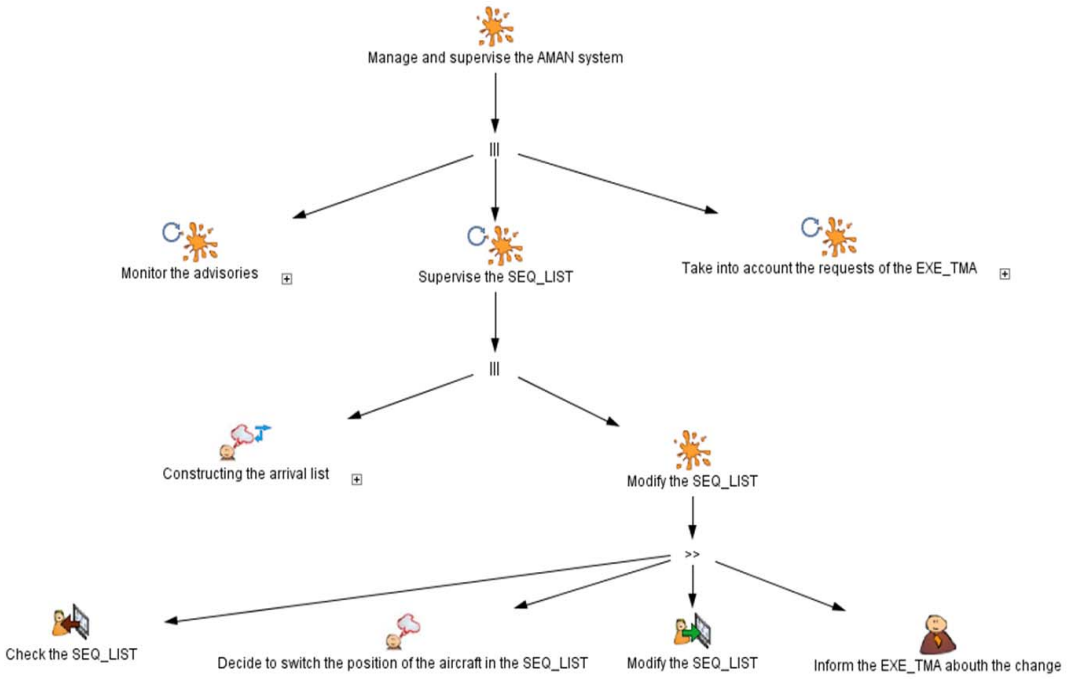

Figure 7. Task model of the Manage and Supervise the AMAN system by the SEQ_MAN

Publications on preliminary results

The early results of the projects have already been published in conference. How to use tasks models to describe and assess automation level has been presented in [4] while a federation of two low level models (tasks and interactive systems) has been used to demonstrate their potential for describing various automation levels [5].

ACKNOWLEDGMENTS

This work has been partly funded by R&T CNES Tortuga R-S08/BS-0003-029, by EUROCONTROL research network HALA! on Higher Automation Levels in Aviation and by the SPAD project.

REFERENCES

[1] Asnar Y.D.W., M. Felici, F. Massacci, A. Tedeschi, and A. Yautsiukhin. Quantitative Assessment for Organisational Security & Dependability, Second International Conference on Dependability (DEPEND 09), Athens, Greece, June 18-23, 2009.

[2] Giorgini, P.; Kolp, M.; Mylopoulos, J.; Pistore, M. The Tropos Methodology: an overview. Methodologies And Software Engineering For Agent Systems, (2004)

[3] Hadar, I; Reinhartz-Berger, I; Kuflik, T.; Perini, A.; Ricca, F.; Susi, A. An empirical study of Requirements Model understanding: Use Case vs. Tropos models, 25th ACM Symposium on Applied Computing , (2010)

[4] Martinie C., Palanque P., Eric Barboni, Martina Ragosta. Task-Model Based Assessment of Automation Levels: Application to Space Ground Segments (regular paper). IEEE international Conference on Systems Man and Cybernetics, (IEEE SMC 2011), Anchorage, Alaska, IEEE, 15-18th October 2011.

[5] Martinie C., Palanque P., Barboni E., Winckler M., Ragosta M., Alberto Pasquini, Paola Lanzi. Formal Tasks and Systems Models as a Tool for Specifying and Assessing Automation Designs (regular paper). 1st international Conference on Application and Theory of Automation in Command and Control Systems, (ATACCS 2011) Barcelona, Spain, May 2011, ACM DL.

[6] Macchi L., E. Hollnagel, and J. Leonhard. Resilience Engineering Approach to Safety Assessment: An Application of FRAM for the MSAW system. Proceedings of Eurocontrol Safety R&D Seminar, Munich, October 21-22, 2009.

[7] OMG Systems Modeling Language (OMG SysML™), version 1.2 June 2010, http://www.omg.org/spec/SysML/1.2/

[8] Parasuraman R., T.B. Sheridan, and C.D. Wickens, "A model for types and levels of human interaction with automation." IEEE trans. on systems, man, and cybernetics., vol. 30, May. 2000, pp. 286-297.

[9] Paterno, F., Mancini, C. & Meniconi, S. ConcurTaskTrees: A Diagrammatic Notation for Specifying Task Models. In: Proc. of Interact'97. Chapman & Hall (1997), 362-369.

[10] Rational Software Corporation. UML Notation Guide. 1.1 ed.1997.

[11] Taurino D., A. Tedeschi, A. Sanchez, A. Flores, R. Sysala, P. Suchanek, V. Nanni and S. Taraglio. Adaptive Routing and Conflict Management for Unmanned Aircraft Vehicles, Procs of the IASTED International Conference on Robotics and Applications, ACTA Press, 2010