Resilience Engineering approach to safety assessment: an application of FRAM for the MSAW system.

Luigi Macchi, Erik Hollnagel, Jörg Leonhard

Resilience Engineering Approach to Safety Assessment: An Application of FRAM for the MSAW system

Luigi Macchi[1], Erik Hollnagel[1] and Jörg Leonhard[2]
(1) MINES ParisTech
Crisis and Risk Research Centre (CRC), 06904 Sophia Antipolis Cedex, France
(2) Deutsche Flugsicherung, GmbH
Safety Management/VY, 63225 Langen, Germany

Abstract

This paper describes a safety assessment study of the Minimum Safety Altitude Warning system (MSAW) using resilience engineering principles. The purpose of the MSAW system is to alert Air Traffic Controller (ATCO) of potential Controlled Flight Into Terrain and Controlled Flight Into Obstacles with sufficient warning time for appropriate instructions to be issued to pilot. The first step of the safety assessment is to identify and describe the MSAW functions by means of the Functional Resonance Analysis Method (FRAM). The impact of the introduction of MSAW in the Air Traffic Management (ATM) system is evaluated by incorporating the MSAW functions into an existing FRAM model of ATCO activities. The resulting FRAM model is then used to evaluate two scenarios to identify possible risks emerging from the introduction of MSAW. Risk identification is based on the evaluation of functions' performance variability and on the occurrence of unexpected combinations. The advantages of this approach are discussed in the conclusion of the paper.

Introduction

The introduction in the Air Traffic Management system of a safety net device such as the Minimum Safety Altitude Warning system (MSAW), must be preceded by a safety assessment. The MSAW has been here used as case study for the application of the Functional Resonance Analysis Method (FRAM) to identify emergent risks due to the combination of variability of normal performance. A detailed description of the FRAM can be found in, e.g., Hollnagel (2004), Woltjer et al. (2007), or Macchi et al. (2008).

The Deutsche Flugsicherung (DFS) MSAW System requirements document (Version 2.1 issued 11.01.2007) states that MSAW is a safety function that "under normal circumstances, allows the ATCO to conduct his tasks with MSAW operating in the background and not disturbing ATC process." MSAW, being normally transparent to the controller, has the objective to prevent a "serious situation from developing into a catastrophic one in case of loss of terrain awareness." In more detail, MSAW has the objective to alert ATCOs of a potential Controlled Flight Into Terrain (CFIT) and Controlled Flight Into Obstacle (CFIO) and serious approach path deviations. Alerts have to be provided with sufficient time to allow ATCOs to respond.

The MSAW has the functionality to monitor:

1. General Terrain;
2. Minimum Radar Vectoring Altitudes;
3. Approach Path.

This paper describes the safety assessment of the Approach Path Monitoring functionality of MSAW. This functionality must alert ATCO in case of an aircraft that deviates, or is predicted to deviate, from the approach path of a runway.

System functions

In order to perform a safety assessment with FRAM it is necessary to identify and characterise MSAW specific functions and how they are coupled to other ATM functions (e.g., Monitoring, Planning, etc.). The detailed characterisation of the functions uses the six aspects (Input, Output, Preconditions, Resources, Time and Control) defined by the FRAM guidelines (Hollnagel, 2004). In the current analysis, the functions were grouped into the three categories of ATM functions, MSAW related functions, and Organisational functions.

ATM functions

The ATM functions represent what the ATM system does to achieve its objective, i.e., assure a safe and efficient air traffic flow in a given airspace. Twelve functions (Table 1) have been identified in collaboration with Air Traffic Controllers (ATCOs) and safety experts.

Table 1– ATM functions

1	PROVIDE MET DATA	Provide to CWP QNH, wind speed and direction, heavy rain etc. Technical function performed by IDVS/omega system.
2	PROVIDE FLIGHT & RADAR DATA	Provide CWP flights call sing, flight level, aircraft typology, aircraft vectoring, route information etc. Technical function performed by P1/ATCAS system.
3	DISPLAY DATA CWP	Display data on Controller Working Position
4	MONITORING	Monitor traffic situation and anticipate traffic development. This function consists in building and updating a mental picture of traffic situation, as well as search for potential conflicts.
5	PLANNING	Develop a control plan to anticipate conflicts and manage traffic flow.
6	STRIP MARKING	Mark the issued clearances on paper or electronic strip
7	COORDINATION	Coordinate with adjacent sectors on desired flights level, vectoring, route, airplanes reported problems etc. This function is performed by the planning controller to support executive controller activity
8	UPDATE FDPS	Update data processing system with respect to issued clearances.
9	PILOT-ATCO COMMUNICATION	Communication, initiated by pilots, to establish radio contact or to request information or clearances to controller
10	SECTOR-SECTOR COMMUNICATION	Radio telecommunication between adjacent sectors to initiate the coordination function.
11	ISSUE CLEARANCE TO PILOT	Issue clearances to pilots via radio communication system or data link.
12	UPDATE MET DATA	Manually update Meteorological data if technical system temporally fails and some data are missing

MSAW related functions

In order to evaluate the impact of the MSAW introduction on the ATM system it is necessary to integrate MSAW related functions with ATM functions. Based on participation in the official safety assessment workshop for MSAW, as well as several interactions with

controllers, the following four functions have been identified (Table 2). The first function is performed by the technical system that computes and generates alerts on the base of the predicted aircraft paths and on the implemented logic. The three other functions require the intervention of humans to enable or disable the transmission of alerts to the Controller Working Position and define the airspace volumes and SSR codes for which alerts (if calculated) are not transmitted.

Table 2 – MSAW functions

1	GENERATE MSAW ALERT	Generate alerts (General Terrain Monitoring, Approach Path Monitoring, Minimum Radar Vectoring Altitude) using predicted aircraft paths and MSAW prediction logic.
2	ENABLE MSAW ALERT	When MSAW is not enabled, the alert generation process continues, but alert transmission will be suppressed
3	DEFINE ALERT INHIBIT AIR SPACE VOLUMES	Define specified airspace volumes to inhibit the transmission of MSAW alerts
4	DEFINE ALERT INHIBIT SSR CODES	Define individual or list of SSR codes to inhibit the transmission of MSAW alerts.

Organisational functions

The FRAM assumes that performance variability to a large extent is determined by the context or the work environment, and also that the context can be unstable or changing. Indeed, it is possible to consider the context as the outcome of other functions (physical, social, organisational, economical, etc.) in the environment where the work takes place, hence subject to organisational control.

To provide the basis for the identification of organisational functions, the set of Common Performance Conditions proposed by Hollnagel (1998) was combined with recent research on evaluation of safety-critical organisation (Reiman and Oedewald, 2009). An initial list was complied and compared against others from the organisational literature (e.g., Reason, 2008; Weick & Sutcliffe, 2007; Hopkins; 2008) and then refined for the specific case. The identified organisational functions are summarised in Table 3 and shown relative to the corresponding Common Performance Condition.

Table 3 – Mapping CPCs into Organisational functions

Common Performance Conditions	**Function**	**Description**
Availability of resources, number of goals and conflict resolution, available time	MANAGE RESOURCES	Organizational function: provide and manage economical, technical and human resources to allow system functioning
Training and experience	MANAGE COMPETENCE	Organizational function: provide operators with required competences and knowledge for system operation. This includes technical, safety competence and deference to expertise.
Access to procedures and methods	MANAGE PROCEDURES	Organizational function: design, update, distribute procedures to support operational activity
Crew collaboration and quality	MANAGE TEAMWORK	Organizational function: manage teamwork to assure a desired quality in team collaboration

Common Performance Conditions	Function	Description
HMI and operational support, conditions of work	MANAGE WORKING CONDITIONS	Organizational function: manage the conditions (e.g. HMI, ergonomic aspects, noise, lightening etc) in which the work is carried out

The FRAM model

The function identification leads to the FRAM model of the ATM system (Figure 1). The model is composed of the three types of functions presented above:

- ATM functions,
- Organisational functions (thick lined functions in the figure) and
- MSAW functions (in grey in the figure).

Notice that the functions in the model are not linked *a priori*. The links between them are generated according to the analysed scenario. The following describes a scenario that was developed to demonstrate the safety assessment. A set of instantiations (i.e., the way in which functions are coupled under given conditions) of the model is then presented. The instantiations, together with the evaluation of the performance variability, are the basis for the risk identification.

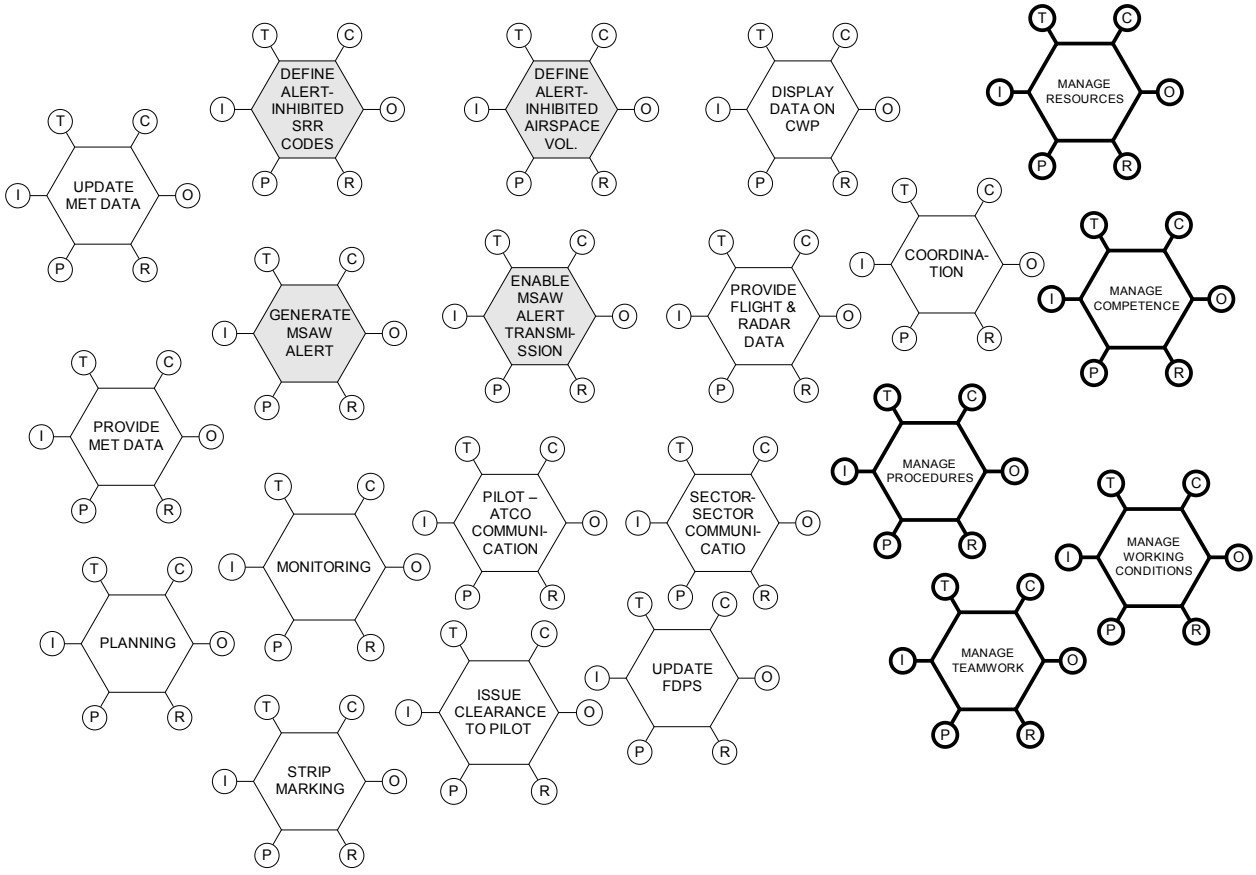

Figure 1 – The FRAM model of the socio-technical system

Approach landing scenario

The scenario used to assess the introduction of MSAW in the ATM system is a Landing approach at the Stuttgart airport (Germany). The airport and air traffic characteristics suggest that a scenario with two approaching aircraft is realistic. Interviews and field observations performed at DFS control centre in Langen showed how controllers would interact with the two flying pilots to direct them towards the Final Approach Fix point in the most efficient way. The following clearances will be issued:

1. Aircraft #1 identified, proceed direct to DLS 512, descend altitude 5000 FT-QNH 1027
2. Aircraft #2 identified, descend FL60, proceed direct to DLS 512
3. Aircraft #1 descend altitude 4000 FT, turn right heading 230, cleared ILS25
4. Aircraft #2 descend altitude 4000 FT-QNH 1027, turn left heading 210, cleared ILS25
5. Aircraft #1 contact tower
6. Aircraft #2 contact tower

Figure 2 shows the arrival chart of Stuttgart airport and the paths aircraft would follow according to issued clearances (dotted lines).

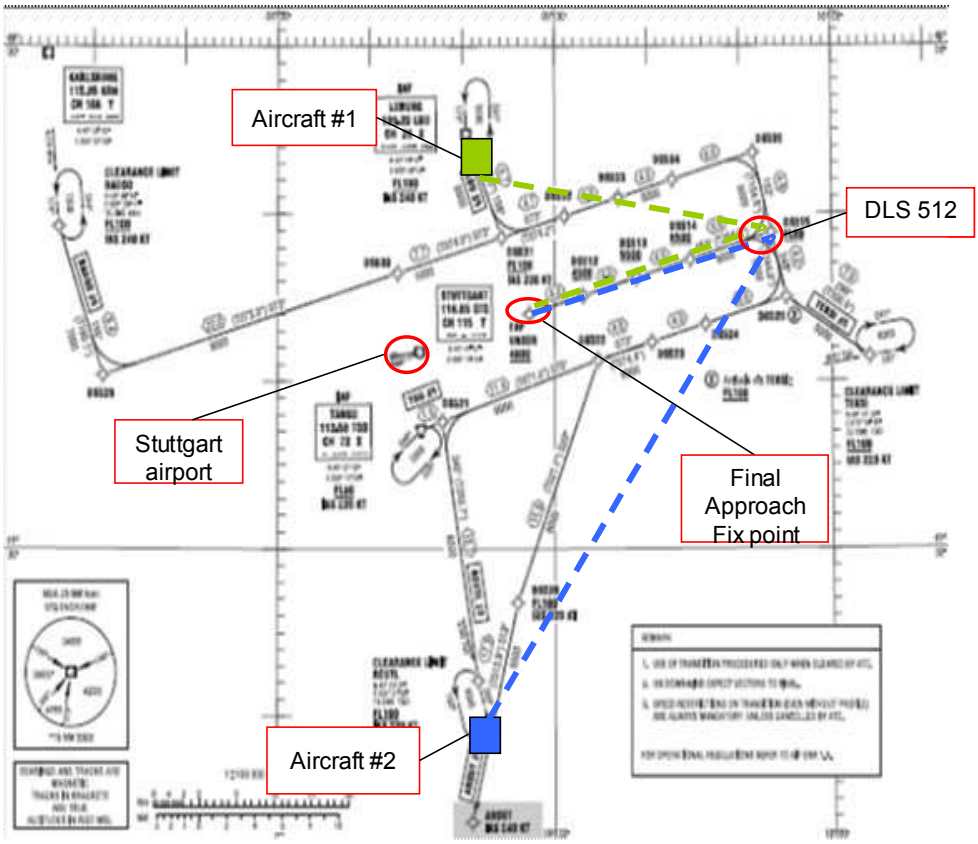

Figure 2- Approach landing scenario at Stuttgart airport

Evaluation of variability of normal performance

In the FRAM, the identification of risks is based on the evaluation of the variability of normal performance and in its potential non-linear combination (so called functional resonance effect). It is therefore necessary first to assess performance variability. To begin with it is

recognised that the functions of a socio-technical system have different characteristics that conveniently may be described by one of the three MTO categories: Human (M), Technology (T), and Organisation (O). These three categories describe functions of a different nature and with characteristic differences in performance variability.

- Human functions will typically be quite variable because people must adjust their performance to current working conditions (resources and demands, cf., Hollnagel, 2009). Human performance can vary on a short term basis, but may also have a dampening effect.
- Technological functions that depend mainly on the technology implemented in the system are in less subject to variability since they are designed to be stable, reliable, and predictable. For the purpose of this study the technological functions are assumed to be properly designed, implemented and maintained and variability is therefore not expected. Technical functions, however, do not have the possibility to dampen performance variability.
- Organisational functions are subject to a different kind of variability, relative to the human functions. The nature or organisational functions makes these less variables than human functions – or rather their variability has a delayed effect on the human functions. A typical example could be the production and updating of procedures. However, since the aim of this safety assessment was the evaluation of the human contribution to system safety, organisational functions were considered stable for the scenario.

The following presents how performance variability for human functions could manifest itself (i.e., what the outputs of variable functions could be) and proposes a rule to assess performance variability. The application of the rule to the instantiations of the model supports the identification of emergent risks.

Human functions: Assessment of performance variability

The above presented set of organisational functions was introduced to account for the context effect on human performance. In this way the model and the method are both composed of homogeneous elements, namely functions and their aspects. The advantage of this is the possibility to assess performance variability by using a set of elements that can be described in a common way.

In order to assess performance variability it is necessary to characterise the aspects for all the functions. Each aspect could be characterised in terms of the precision and timing with which it is produced.

In terms of precision, an aspect can be:

- Precise;
- Acceptable;
- Imprecise.

In terms of time, an aspect can be:

- Too early;
- On-time;
- Too late.

In FRAM, the output of an upstream function may be used by a downstream function as Input or Precondition or Control or Resource. The timing of the output from an upstream function may affect the available time for the downstream functions to be performed, i.e., it may increase or decrease temporal pressure, which in turn may have an impact on the precision

and timing of their output. It is possible to represent the quality of possible outputs combining the precision and the timing characteristic as shown in Table 4.

Table 4- Human functions: output characterisation

		Temporal characteristics		
		Too early	On time	Too late
Precision	Precise	A: Output to down-stream functions is precise but too early	B: Output to down-stream functions is precise with the right timing	C: Output to down-stream functions is precise but delayed, reducing available time
	Acceptable	D: Output to down-stream functions is acceptable but too early	E: Output to down-stream functions is acceptable with the right timing	F: Output to down-stream functions is acceptable but delayed, reducing available time
	Imprecise	G: Output to down-stream functions is imprecise and too early	H: Output to down-stream functions is imprecise but correctly timed	I: Output to down-stream functions is imprecise as well as delayed, reducing available time

Table 4 can be used to assess the potential for performance variability induced by the combination of all the incoming aspects for a given function and consequently the likely quality of its output. The effect on performance variability of the aspects could be presented as follow (Figure 3):

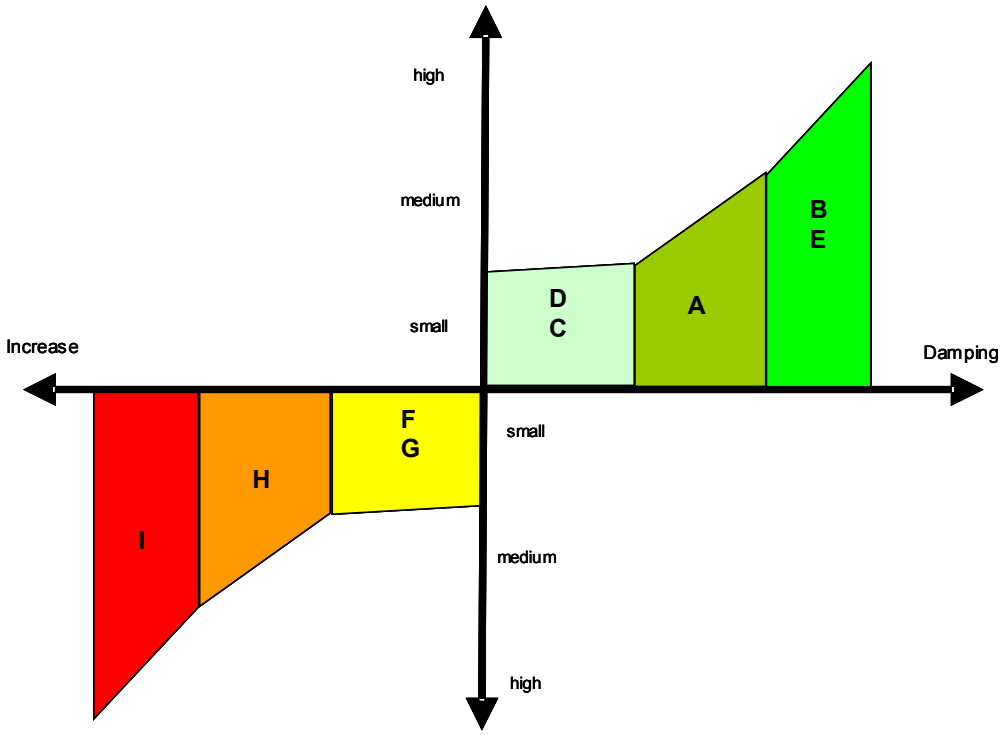

Figure 3- Aspect's quality effect on Performance variability

For the time being a quite simple rule (method) could be proposed:

The median of the quality of the aspects is the quality of the output.

Risks identification results

The risk identification for the scenario is based on a 'paper and pencil' simulation. It is used to illustrate how the proposed methodology can be applied to a real safety assessment case, although such an application certainly will be more intricate. The presented scenario could be instantiated in the model leading to a set of sequence of instantiations representing the temporal development of the scenario. Note that the analysis of the consequences of performance variability is based on the contents of the FRAM model rather than on the graphical rendering. The latter can be useful for communication, but is not essential for the method as such.

In order to apply the method to the identification of potential emergent risks, a further set of assumptions has to be made:

1. Organisational functions produce precise outputs, therefore the context for Human functions performance is acceptable and the organisational functions therefore do not induce variability;
2. The MSAW function 'Generate MSAW alert' during the scenario triggers an alert (for Aircraft #1) during the development of the scenario. The remaining technological functions are properly designed and implemented their outputs are therefore correct and no variability is induced;
3. The MSAW function 'Enable MSAW alert transmission' is performed imprecisely (Output characterised as **H** in Table 4);
4. 'Issue clearance to pilot' function is performed earlier than expected when the clearance *Aircraft #1 descend altitude 4000 FT, turn right heading 230, cleared ILS2* is issued (Output characterised as **D** in Table 4);

5. The remaining functions are performed with acceptable precision and timing (Output characterised as **E** in Table 4).

It is now possible to present the instantiations, to apply the methodology, and to draw preliminary conclusions. In the diagrams that follow, dotted lines represent the output of organisational functions, i.e., the context. Only relevant functions are represented in the instantiations.

Landing approach scenario - First instantiation

The first instantiation (Figure 4) represents the starting point for the 'paper and pencil' simulation. Due to the above mentioned assumptions, no risks emerge from this instantiation. Although the inaccurate enabling of MSAW alert transmission introduces potential performance variability in the system, the potential variability is not triggered because there is no need of an MSAW alert at the time.

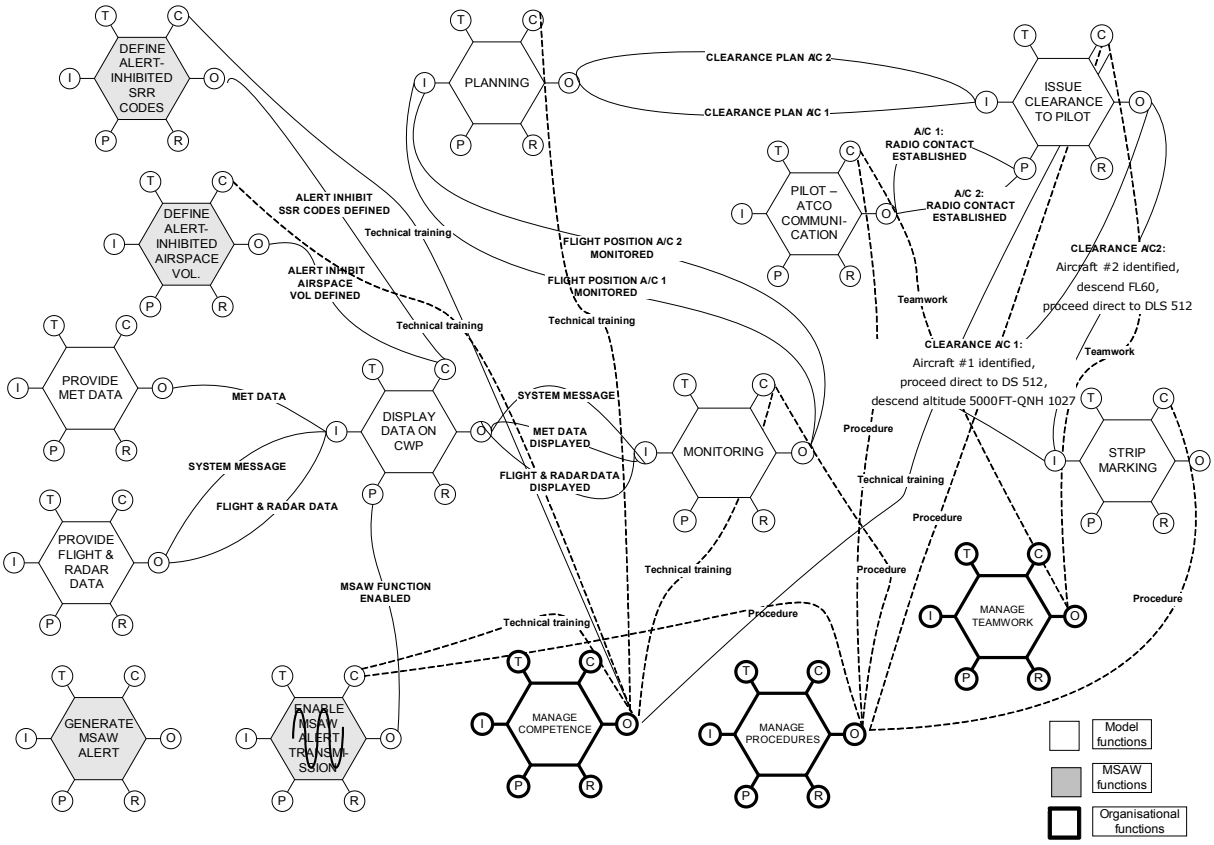

Figure 4- Scenario – First instantiation

Landing approach scenario- Second instantiation

The second instantiation for the scenario represents the temporal evolution of the situation. After the first instantiation the two aircraft have been instructed to proceed directly towards DLS512. During this instantiation, two additional clearances are issued to the pilots. As assumed, the clearance *Aircraft #1 descend altitude 4000 FT, turn right heading 230, cleared ILS2* is issued too early (Output **D**).

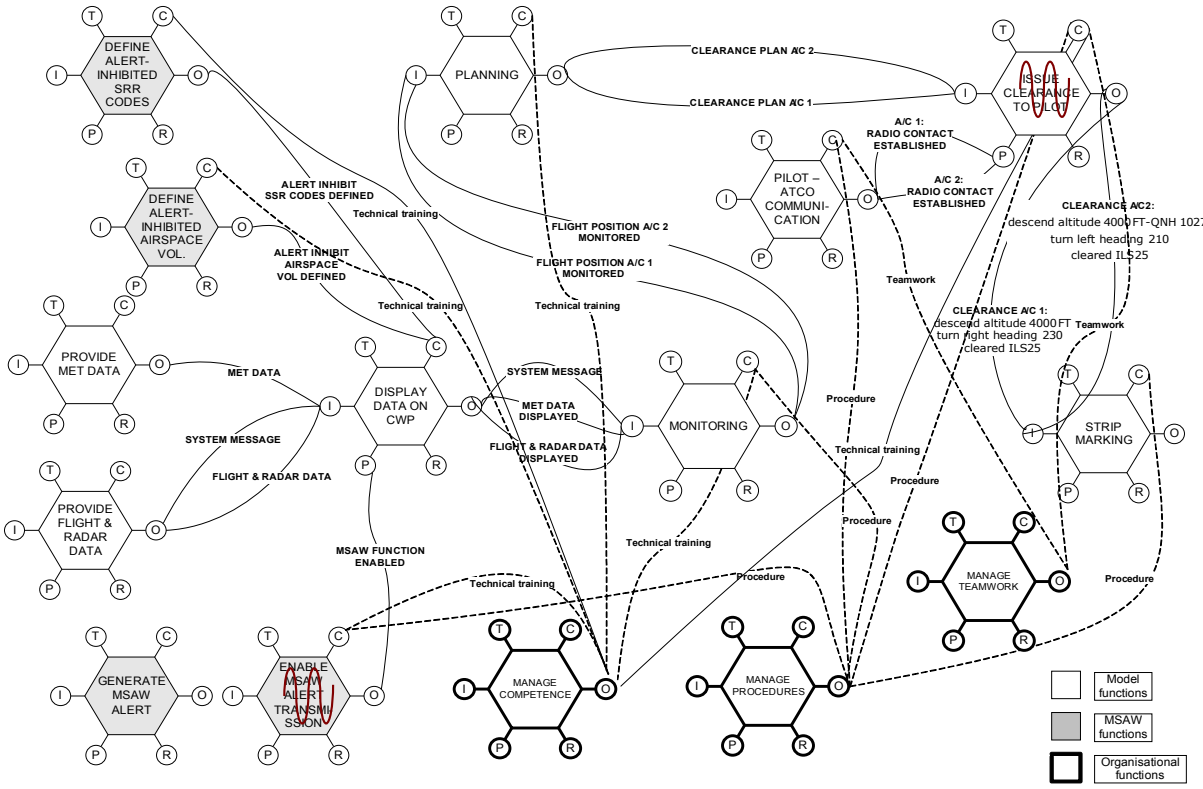

Figure 5- Scenario - Second instantiation

Landing approach scenario – Third instantiation

In addition, an alert is calculated but not displayed on CWP (as assumed) since Preconditions are not satisfied.

The Monitoring function therefore receives:

- Acceptable precision and correctly timed output from the Provide Met. Data (Output **E**);
- Acceptable precision but premature flight data for A/C #1 (Output **D**);
- Imprecise but correctly timed data from the MSAW functions (Output **H**).

Its output therefore is still acceptable but no longer on time (Output **F**), since it is reasonable to consider ATCO will detect the dangerous situation for Aircraft #1 later than if supported by MSAW.

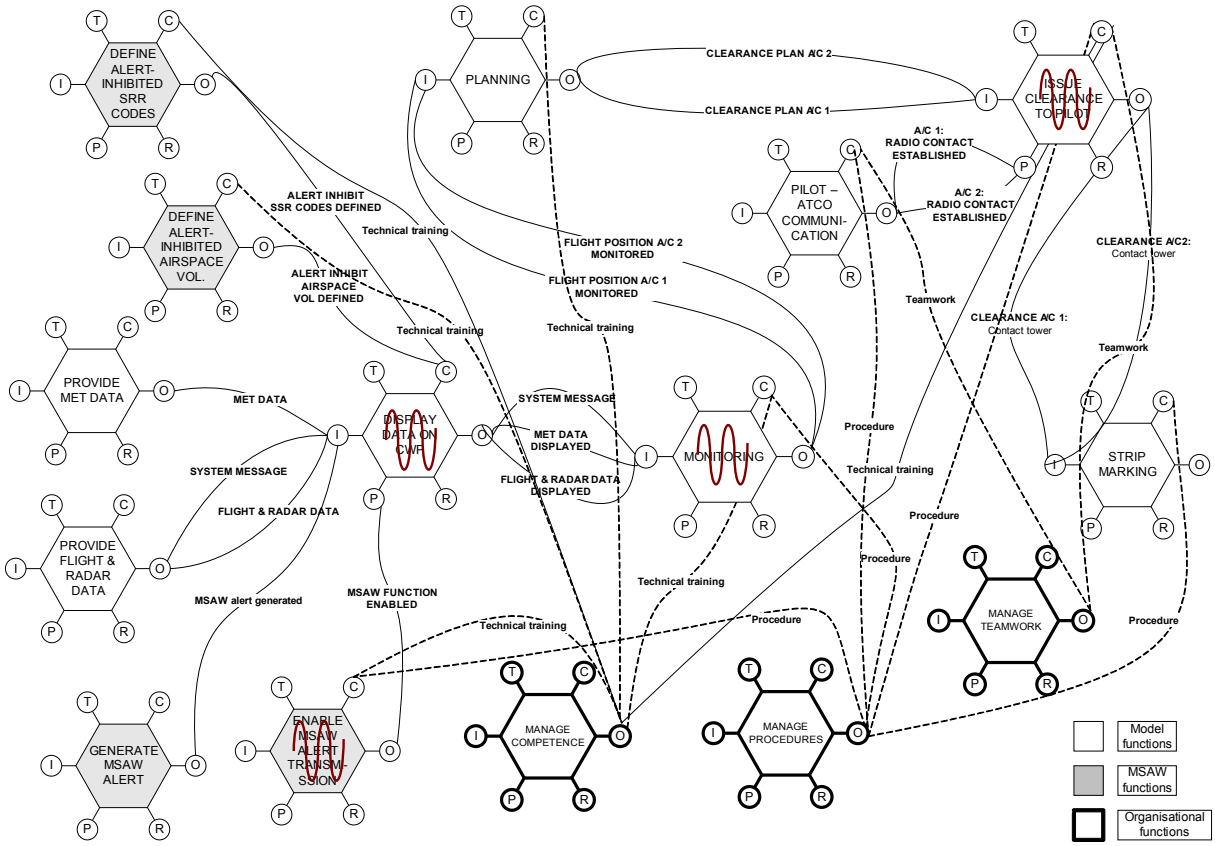

Figure 6- Scenario - Third instantiation

The application of the proposed methodology to a simplified example has shown the possibility for identification of emergent risks due to the interaction of the variability of normal performance induced by the 'Issue clearance to pilot' and 'Enable MSAW alert transmission' functions. Given the above assumptions, this variability may affect the Monitoring function in such a way that that it is performed with acceptable precision but later than expected.

Conclusion

This paper has presented the application of the Functional Resonance Analysis Method to perform a safety assessment study for the Minimum Safe Altitude Warning system. The introduction of a safety net system in the ATM domain requires the evaluation of its potential impact in safety terms. Adopting a resilience engineering approach, the FRAM and the proposed methodology have been applied to look for risks due to the combination of variability of normal performance rather than to system failures or breakdowns. The Landing approach scenario illustrated how an inappropriate enabling of the alert transmission in combination with a 'trivial' anticipation of a clearance could result in a degraded performance of the monitoring function. This result, within the limitations of the example, nevertheless shows the added value of a resilience engineering approach when evaluating the potential impact of the introduction of new equipments in the ATM domain.

Acknowledgements

We are grateful to the air traffic controllers at DFS and to Ivonne Herrera for their availability, the useful discussions and the support they have always been ready to provide.

References

Hollnagel, E. (1998). *Cognitive reliability and error analysis method*. Elsevier.

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, UK: Ashgate Publishing

Hollnagel, E. (2009). *The ETTO principle: Why things that go right sometimes go wrong*. Aldershot, UK: Ashgate Publishing.

Hopkins, A., 2008. *Failure to learn: the BP Texas City refinery disaster*. CCC Australia Limited

Macchi, L., Hollnagel, E., Leonhardt, J. (2008). *A systemic approach to HRA: A FRAM modelling of Control Over Flight activity*. EUROCONTROL Safety R&D seminar. 22-24 October, 2008, Southampton, UK.

Reason, J., 2008. *The human contribution: Unsafe acts, accidents and heroic recoveries*. Aldershot, UK: Ashgate Publishing.

Reiman, T., Oedewald, P., 2009. *Evaluating safety critical organizations – emphasis on the nuclear industry*. Report number 2009:12. Swedish Radiation Safety Authority. http://www.stralsakerhetsmyndigheten.se

Weick, K. E., Sutcliffe, K.M., 2007. *Managing the unexpected: Resilient performance in an age of uncertainty*. Jossey-Bass, San Francisco, CA.

Woltjer, R. and Hollnagel, E.(2007). *The Alaska airlines flight 261 accident: a systemic analysis of functional resonance*. Proceedings of the 2007(14th) International Symposium on Aviation Psychology, April 23-26, Dayton, OH.