# Resilience Management Problem in ATM Systems as a Shortest Path Problem

## A proposal for definition of an ATM system resilience metric through an optimal scheduling strategy for the re-allocation of the system tasks

F. Gargiulo, D. Pascarella
Soft Computing Dept.
CIRA, Italian Aerospace Research Center
Capua, Italy
f.gargiulo@cira.it

A Errico, V. Di Vito, E. Filippone
Air Traffic Management Dept.
CIRA, Italian Aerospace Research Center
Capua, Italy

***Abstract*—As a preliminary study about the methodology for resilience management problem in ATM systems, this paper identifies the key aspects that should be taken into account in the formal definition of the problem. It provides an overview of the definitions and concepts related to resilience in ATM systems. Finally, the paper introduces a proposal of a definition of a resilience metric for an ATM system and formally states the resilience management problem as an optimization problem. The latter aims at finding an optimal scheduling strategy for the re-allocation of system tasks. The paper also inspects the nature of the proposed metric, highlights the constraints of the problem and makes a comparison with other approaches.**

***Keywords-component; resilience engineering; resilience management problem; resilience metric; ATM systems; key performance indicators;key performance areas***

## I. INTRODUCTION

An approach to Resilience Engineering in ATM is the high level objective of the SAFECORAM project. The approach proposed in this project eventually deals with the re-allocation of tasks between residual resources of the system after a disturbances, in order to minimize the loss of global performance. Improving the resilience of the system is then translated in a minimization of performance decay in presence of failures, emergency conditions, disrupts of the ATM system. The description of the idea as a whole is presented in [17].

In the present paper, the selection of the optimization methodology better suited to support the resilience engineering problem as approached in SAFECORAM is discussed, with an introduction to the state-of-the-art of methodologies suitable for application.

Considering that ATM is an open system, its operation is constantly perturbed by disturbances. These disturbances may interact with each other, potentially creating a cascade of adverse events, that may span over different spatial and time scales. The adverse ATM events may have different nature and impact ([1],[2]): they may pass without any discomfort for passengers, they may result in a small passenger discomfort or they may arise a discomfort that is out of any proportion. In the latter case, there are two categories of events:

- catastrophic accidents involving one or more aircrafts;
- events that push the dynamics of the ATM far away from its point of operation and dramatically affect the performance of the system.

These events are rare and exceptional in ATM, but they have large economy and safety impacts, so they have triggered several studies about what can be learned from them in order to improve the air transportation system by means of safety analysis. However, another source of learning is formed by the human operators that have experience in handling situations that are not fully covered by procedures because of the intractability of the system. This means that human operators may learn not only from rare catastrophic events, but from a larger set of events. The decoupled usage of safety analyses of catastrophic events and of human performances has led to an ultra-safe ATM, but with a conflicting safety in respect to capacity, economy and environment requirements. Moreover, it is difficult or even impossible to establish the resilience role in realizing these high safety levels: currently, there is only a qualitative understating of ATM resilience and no quantitative results exist, so we are not able to assess whether an ATM system design is more or less resilient then another ATM system design ([1],[2]). The only way to escape from this situation is a systematic implementation of resilience in ATM in SESAR and NextGen programs.

## II. RESILIENCE DEFINITIONS AND RELATED CONCEPTS IN ATM SYSTEMS

A few scientific papers and books have been progressively published on resilience, covering different research domains. A detailed description is supplied in [2]. The meanings and the interpretations of resilience may be summarized in three different forms.

The first form is *engineering resilience*. As specified in [18], this form corresponds to the more traditional definition of resilience and focuses on efficiency, constancy and predictability. It concentrates on stability near an equilibrium steady state, on the resistance to disturbance and on the speed of return to the equilibrium. Here, resilience is the time required for a system or the ability of a system or the capability of a substance to return to an equilibrium steady state [19]. This view is coherent with the definition of [20] and represents a foundation for economic theory, too.

The second form is *ecological resilience*. As specified in [18], this form focuses on persistence, change and unpredictability. It concentrates on disturbances that can flip a system into another behavior space (i.e., into another equilibrium state). Here, resilience is defined as the ability of a system to absorb a disturbance, whilst essentially retaining the same function, structure, identity and feedbacks. This view is compliant with the definition of Holling [21].

The first two forms of resilience address contrasting aspects. Engineering resilience tends to stability, whereas ecological resilience tends to robustness. Indeed, engineering resilience does not prevent the transition to another equilibrium state for the system and requires only the persistence of the system structure. From a safety-oriented perspective, engineering resilience focuses on maintaining efficiency of a function and ecological resilience focuses on maintaining existence of a function

This paper refers to the third form, an interpretation of resilience named *resilience engineering*. This is a term that has emerged in conjunction with resilience as regards the development of resilient systems. Resilience engineering has been introduced in [3] as *"a paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success"*. It is intended as a sub-discipline in the area of safety or performance analysis and it is especially directed to socio-technical systems. Here, the stress is on the ability to deal with the unexpected in order to achieve a more flexible approach for the compliance with safety and reliability objectives. Moreover, as stated in [4], *"resilience engineering is concerned with building systems that are resilient to change"*. Thus, resilience engineering aims at the design of systems that are able to continue to work even when faced with adverse situations (both anticipated and unanticipated) by possibly taking advantage of human endeavors.

An ATM system is a socio-technical system that is driven by economic interests of the participating stakeholder. Hence, it is performance-oriented. Moreover, the resilience framework shall intuitively address the ability of the ATM system to reduce both the magnitude and the duration of the deviation from targeted system performance levels. As a consequence, a set of *key performance indicators (KPI)* for the ATM domain shall have to be rigorously established in order to include all the relevant performance dimensions. According to ICAO [5], KPIs are quantitative indicators of current/past performance, expected future performance (estimated as part of forecasting and performance modelling), as well as actual progress in achieving performance. They may be directly measured or they may be calculated from supporting metrics.

KPIs are grouped into *key performance areas (KPA)*. ICAO defines KPAs as *"a way of categorizing performance subjects related to high-level ambitions and expectations"* [5]. ICAO has defined eleven KPAs: safety, security, environmental impact, cost effectiveness, capacity, flight efficiency, flexibility, predictability, access and equity, participation and collaboration, interoperability.

The *current state* of an ATM system is defined by the current values of its performance indicators.

A *disturbance* is a phenomenon, factor or process, either internal or external, which may cause a stress in a system. It is relative to the specified reference state and considered system. It is categorized and quantified by type, frequency, intensity and duration.

A *stress* is the state of a system caused by a disturbance which differs from the reference state and is characterized by deviation from this reference condition. A stress can be: *survival*, if the system can respond by perturbation without modification to change the current state or *lethal*, if the system cannot or should not respond by perturbation to change the current state and has to be modified.

A *perturbation* is the response of a system to the possible or current significant undesirable changes of the state of the system caused by a disturbance. Perturbation aims at preventing the state changes and/or at minimizing the deviation of the current values from the reference values of performance indicators. If the stress is unavoidable, but survival, perturbation can be: *transient*, if it enables a temporary deviation which becomes zero over time, with return to the reference state; or *permanent*, if the deviation becomes fixed over time, leading to a state that is different from the reference state.

Several definitions of resilience have been introduced, with more qualitative statements than quantitative (analytical) formulations having been suggested. Indeed, as pointed out in [6], although resilience is becoming an essential component of systems and enterprises, there is currently a lack of standardization for a quantitative definition and a measurement of resilience. For example, Woods has asserted that "*we can only measure the potential for resilience but not resilience itself*" [3]. However, some of the aspects of resilience are measurable. These quantifiable aspects are more technical in nature and they are related to reliability, safety and capacity parameters [7].

The absence of a global quantitative definition of resilience is a significant limit for resilience applications: we cannot monitor the resilience of a system and we cannot assess whether a system A is more resilient than a system B (functionally equivalent to A). A quantitative measure of resilience is essential in order to investigate and improve resilience. In the following, we firstly examine the aspects and

attributes that a quantitative resilience measure should involve. Thereafter, we review some of the main resilience metrics that have been proposed so far.

### A. *Resilience Attributes*

Reference [8] outlines the following "4 Rs" properties for the resiliency of a generic system:

- *robustness:* strength, or the ability of elements, systems, and other units of analysis to withstand a given level of stress or demand without suffering degradation or loss of function;
- *redundancy:* the extent to which elements, systems, or other units of analysis exist that are substitutable, i.e., capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality;
- *resourcefulness:* the ability to identify problems, establish priorities, and mobilize resources when conditions exist that threaten to disrupt some element, system, or other unit of analysis; resourcefulness can be further conceptualized as consisting of the ability to apply material (i.e., monetary, physical, technological, and informational) and human resources to meet established priorities and achieve goals;
- *rapidity:* the ability to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

Reference [9] suggests the following key properties for resilience:

- resilience is an ability to respond to disruption through recovery;
- the response may be measured in terms of its magnitude, and its temporal and spatial extent;
- the magnitude may be expressed with respect to system performance targets.

In addition, a view of three capacities of resilience is presented for complex networks (but it may be related to a generic system). These three capacities are:

- *absorptive capacity*, to withstand disruptions;
- *adaptive capacity*, to accommodate flows through alternative paths into the network;
- *restorative capacity*, to quickly recover from a disruptive event at minimum cost.

Therefore, resilience is interpreted as the ability of a complex network to retain performance during and after disruptions and their ability to return to the normal state of operation quickly after disruptions.

### B. *Main Resilience Metrics*

Several quantitative metrics and analytical frameworks have been proposed for resilience measurement. References [6] and [10] provide a survey about resilience measurement methodologies from a wide range of disciplines. Generally speaking, resilience metrics may be divided in [11]:

- *attribute-focused metrics*, which typically consists of indices that rely on subjective assessments;
- *data-based indicators*, which quantify system attributes that are asserted to contribute to resilience;
- *performance-based methods*, which measure the consequences of system disruptions and the impact that system attributes have on mitigating those consequences.

In particular, performance-based methods do not quantify attributes that impact on the system functioning; on the contrary, they directly measure the system outputs during the recovery period. As an example, most resilience metrics for transportation networks are categorized as performance-based methods because they measure the flows across the network during recovery (meant as restorative) activities.

The common framework underlying performance-based approaches employs a system performance metric F(·) as a basis for the resilience computation. This is a time-dependent function, which represents the system delivery function or figure-of-merit. $F(\cdot)$ has a nominal value $F_0$. The system operates at this level until a disruption occurs at time $t_0$, which causes a degradation in the performance $F_0$ to some level $F_{min}$ at time $t_1$. At this point, recovery starts and likely improves the performance $F(\cdot)$. When the system achieves a targeted performance level (not necessarily $F_0$), recovery is completed (Fig. 1). Obviously, resilience is quantifiable only if $F(\cdot)$ is quantifiable.

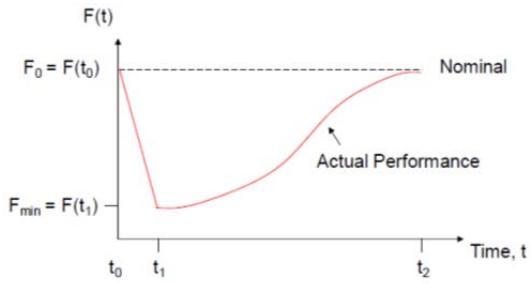


Figura 1. Generic concept of disruption and recovery for resilience performance-based metrics [11].

Fig. 1 is representative of a performance function for which increasing values are considered better. In case that decreasing values are preferable, $G(\cdot) = F^{-1}(\cdot)$ should be considered. Multiple options usually exist for sequencing recovery activities, which may have different costs, may imply different targeted level of performance and may require different times to recovery (Fig. 2). A resilience performance-based metric should generically take into account these three aspects.

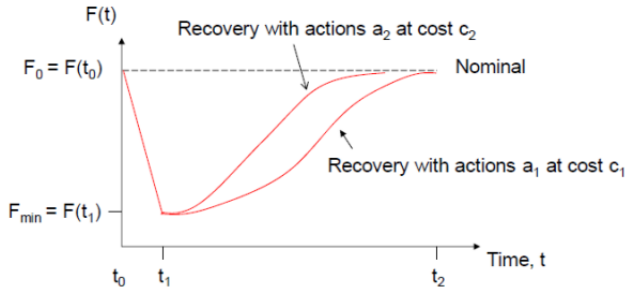


Figura 2. Different recovery strategies for resilience performance-based metrics [11].

## III. RESILIENCE MANAGEMENT IN SAFECORAM

This section reports the SAFECORAM proposal to cope with the problem of resilience management in an ATM system. It starts with the description of a *scenario* and formalizes the resilience management framework as an optimization problem through the definition of the concepts of *flows* and *flows distance*.

### A. Definition of Scenario

A scenario represents the set of a nominal and non-nominal situations affecting the ATM system, with the aim of stimulating alternative behaviors of the system to be evaluated from the resilience point of view in order to select the best reaction to the considered situation. A scenario is described through the specification of following information:

- *Summary*: it is a summary description of the scenario in order to emphasize the affected flight phase/phases and the considered non-nominal stimulus/stimuli on the ATM system;
- *Preconditions/Settings*: it specifies the general framework of the considered scenario (for instance, type of affected vehicles, traffic conditions, weather conditions, etc.);
- *Main flow*: it specifies the evolution of the considered scenario in the nominal situation and it outlines the nominal roles of the involved actors and systems (according to the applicable nominal procedures) at high level;
- *Failures and/or disturbances*: it describes the failures and/or disturbances considered to impact the nominal evolution (main flow) of the examined scenario and their impact on the affected actors/systems;
- *Alternative flows*: it individuates and develops the possible evolutions of the reference non-nominal scenario in order to emphasize the degrees of freedom of the involved actors/systems and the resulting outcomes, in terms of alternative flows originating from the different reactions of the ATM system to the considered perturbations; every alternative flow identifies an allocation strategy of the tasks between the system components.
- *Involved actors, systems (agents) and procedures*: it summarizes the roles and possible alternative behaviors of the affected actors and systems in the framework of the considered non-nominal scenario; this summary description is focused only on the specific expected behavior in non-nominal conditions.
- *Involved KPAs and KPIs*: it preliminarily (qualitatively) identifies the KPAs (and implicitly the related KPIs) affected in the considered scenario, based on the expected impact of the considered non-nominal events on the main flow and based on the expected possible outcomes in terms of alternative flows.

Even if the description of the scenarios it is not exhaustive in terms of enumeration and exploitation of all the possible alternative flows emerging from the considered non-nominal situation (being the full spectrum of possibilities intrinsically unpredictable), there are enough information to demonstrate that the proposed approach for resilience management can provide the evaluation of the best choices to be taken in order to optimize the reaction to the examined perturbations.

### B. SAFECORAM Resilience Loss Metric

The term flow refers to the flows listed both in Main flow and *Alternative flows* sections in each scenario. Then, a flow is simply a set of tasks that must be executed in order to reach a terminal condition. From this point of view, actors are less important, because we put the focus on the tasks (meant as functions performed by the actors) and the propaedeutic order between them.

Resilience will be expressed as a function of the ATM system performances and, as a consequence, the statement of the resilience management problem within SAFECORAM project has to address a performance-based metric for resilience. As prescribed by the SESAR Performance Framework [12], the ATM system performances are related to specific KPAs and a KPI represents a quantitative measure for each specific area. Among all KPAs selected from SESAR Performance Framework, the KPAs are taken into account within SAFECORAM project [13] are: *Safety*, *Efficiency*, *Capacity* and *Environment*.

A detailed description of these KPAs can be found in [5]. In order to describe a general approach, suppose that there are $n$ KPAs, named $\{A_1, \dots, A_n\}$. For example, $A_1$ may represent Safety, $A_2$ the Efficiency, etc. Suppose that the $k$-th KPA is related to a set of KPIs, named:

$$\left\{KPI_1^{(A_k)}, \dots, KPI_{m_k}^{(A_k)}\right\} \quad (1)$$

Where $m_k$ is the number of KPIs that are associated to $A_k$. We group all the KPIs into the following set:

$$\Theta = \left\{KPI_1^{(A_1)}, \dots, KPI_{m_1}^{(A_1)}, \dots, KPI_n^{(A_n)}, \dots, KPI_{m_n}^{(A_n)}\right\} \quad (2)$$

Where $m = m_1 + \cdots + m_n$ denotes the total number of KPIs. From the performance point of view, each task $T_{i,j}$ may be also associated to a tuple $\left(k_{i,j}^{(1)}, \dots, k_{i,j}^{(m)}\right)$, wherein $k_{i,j}^{(t)}$

represents the "contribution" of (the execution of) $T_{i,j}$ in the evaluation of the *t*-th KPI in Θ. For example, suppose that in a flow there is an actor $C_1$ that has two tasks $T_{1,1}$ and $T_{1,2}$. In this case, the KPIs are:

$$KPI_1^{(A_1)} = f\left(k_{1,1}^{(1)}, k_{1,2}^{(1)}\right) \quad (3)$$

$$KPI_1^{(A_2)} = g\left(k_{1,1}^{(2)}, k_{1,2}^{(2)}\right) \quad (4)$$

Where $f(x,y)$ e $g(x,y)$ are functions that should be determined in accordance with the domain experts.

The **flow state** (both nominal and non-nominal) is the set of the values of its KPIs, that is, the state of a flow $F(S)$ is the following tuple:

$$F(S) = \langle KPI_1^{(A_1)}, \dots, KPI_{m_1}^{(A_1)}, \dots, KPI_n^{(A_n)}, \dots, KPI_{m_n}^{(A_n)} \rangle \quad (5)$$

$F(S)$ is a quantitative indicator of the global performance achieved by the ATM system if it executes the flow $S$ into the considered scenario.

The definition of the flow state let us to approach to the resilience management problem as a single objective optimization problem. In fact, the measurement of the flow state provides us of a way to compare flows respect to only one parameter, the flow state indeed. Therefore, in the following, the discussion is about the selection of the flow that optimize the resilience using flows state only.

Without the definition of the flow state, two flows can be compared with respect to each KPIs. Of course, a flow $S_1$ can outperform the flow $S_2$ with respect some KPIs and $S_2$ can be better of $S_1$ with respect the others KPIs. In this multi-objective optimization point of view, could happen that there is not a flow that outperforms (that is, *dominates*) all others flows, but perhaps a subset only. In this case, the output of the an optimization algorithm would be a set of candidate solutions, named for instance $P$. $P$ would contain the dominating flows, (the Pareto front) and it holds that for every flow do not belong to $P$ there exists a flow in P that outperform it. Eventually, the optimization algorithm would prompt to the user to select the flow among them belonging to $P$. Each flow in $P$ can be considered as a tradeoff and the optimization algorithm does not have a rule to determine which is the best tradeoff, then it delegates the choice to the user.

In the following discussion, the former approach is adopted therefore the output of the optimization algorithm will be a unique flows.

Now, it needs an order relation amongst the whole states of the flows of a same scenario in order to establish if a flow $S_1$ is better or worse than a flow $S_2$ with respect to their states, i.e., their key performances. For this reason, a *flow distance* function $d$ is introduced. If Ω is the set of all the flows of the same scenario, a function $d: \Omega \longrightarrow \mathbb{R}$ is a flow distance if it has the well-known distance properties*: non-negativity, identity of indiscernibles*, *symmetry* and *triangle inequality*.

A flow distance represents a quantitative measure of the similarity between two flows of a scenario and it should be related to the flow states for our purposes. Two flows $S_1$ and $S_2$ are similar and their distance $d(S_1, S_2)$ is low if their states $F(S_1)$ and $F(S_2)$ (i.e., their global ATM performances) are close.

Even if the user do not chooses a flow in a set of candidate solutions P as would be in the case of a multi-objective optimization approach, through the definition of a flow distance the user indirectly provide the optimization algorithm of a rule by means select the best flow.

Based on the previous considerations, we define the resilience metric in the following way. Let $S_0$ be the nominal flow of a scenario 𝕊, that is, the main flow of 𝕊. Let $S_i$ be an alternative flow of the same scenario 𝕊 of $S_0$. The *SAFECORAM resilience loss metric* $RL_{\mathbb{S}}(S_i)$ in the scenario 𝕊 of the ATM system is:

$$RL_{\mathbb{S}}(S_i) = d(S_0, S_i) \quad (6)$$

This metric is a function of the selected scenario 𝕊 (and its nominal flow): this dependence is strictly related to the scenario-based approach in SAFECORAM project [12]. Moreover, it is a function of the alternative flow that has been triggered within 𝕊.

The metric in (6) is a resilience loss metric because the more similar are the performed alternative flow $S_i$ and the nominal flow $S_0$, the lower is $RL_{\mathbb{S}}(S_i)$. In this way, the proposed metric confirms that the ATM system is more resilient if the chosen alternative flow is more similar to the nominal flow, i.e., if their states (and so their global performances) are closer.

Several characterizations of the SAFECORAM resilience loss metric may be provided according to the nature of the flow distance index. For examples, in order to illustrate the approach suppose that:

$$KPI_1^{(A_i)} \in [0,1], \quad i = 1,2,3,4 \quad (7)$$

Where a value close to 1 of the KPI indicates "good" performance and a value close to 0 represents "poor" performance.

The values of the four KPIs in every flow $S$ of the scenario 𝕊 may be drawn on a bi-dimensional Cartesian coordinate system (Fig. 3).

In Fig. 3, we denote with $\{KPI_1, KPI_2, KPI_3, KPI_4\}$ the set of the four KPIs and with $\{KPI_1(S), KPI_2(S), KPI_3(S), KPI_4(S)\}$ the set of the KPIs values for the flow $S$. $R(S)$ is the area of the quadrangle with vertices $\{KPI_1(S), KPI_2(S), KPI_3(S), KPI_4(S)\}$ and can be seen as a "state area" or a "global performance area" of the ATM system for the flow $S$.

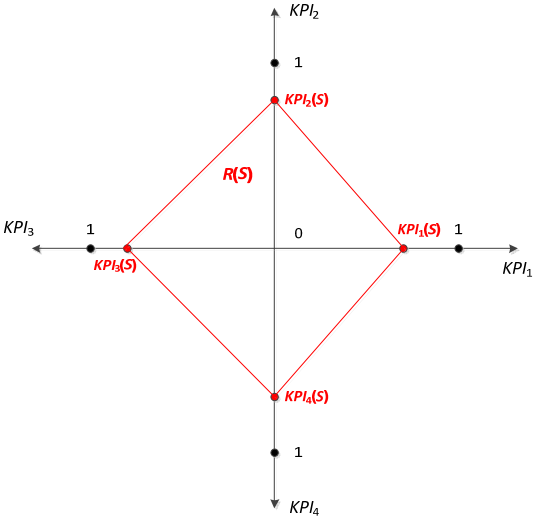


Figura 3. Bi-dimensional graphical representation of the KPIs of a flow.

In this case, an intuitive definition of the flow distance between the flows $S_1$ and $S_2$ is:

$$d(S_1, S_2) = |R(S_1) - R(S_2)| \tag{8}$$

It is not difficult to verify that it is a well-defined distance function. Hence, according to (8), two flows are similar if they entail similar global performance area.

Another scalar real-valued formulation for the flow distance between the flows $S_1$ and $S_2$ of a scenario $\mathbb{S}$ is:

$$\begin{aligned} d(S_1, S_2) = {} & a_{1,1} \left| KPI_1^{(A_1)}(S_1) - KPI_1^{(A_1)}(S_2) \right| + \cdots \\ & + a_{1,m_1} \left| KPI_{m_1}^{(A_1)}(S_1) - KPI_{m_1}^{(A_1)}(S_2) \right| \\ & + \cdots \\ & + a_{n,1} \left| KPI_1^{(A_n)}(S_1) - KPI_1^{(A_n)}(S_2) \right| \\ & + \cdots \\ & + a_{n,m_n} \left| KPI_{m_n}^{(A_n)}(S_1) - KPI_{m_n}^{(A_1)}(S_2) \right| \end{aligned} \tag{9}$$

Wherein the terms $a_{i,j}$ are real-value coefficients. Therefore, the distance index in (9) is a linear combination of the deviations amongst the KPIs of the compared flows. It is a valid distance function because the single deviations amongst the KPIs are distance indexes and a linear combination of distance indexes is a distance index.

If we suppose that $a_{i,j} = 1, \forall i, j$, then two flows $S_1$ and $S_2$ are more similar if their related quadrangles in Fig. 3 are "superimposable", i.e., the single vertices pairs:

$$\begin{gathered} \left(KPI_1(S_1), KPI_1(S_2)\right) \\ \left(KPI_2(S_1), KPI_2(S_2)\right) \\ \left(KPI_3(S_1), KPI_3(S_2)\right) \\ \left(KPI_4(S_1), KPI_4(S_2)\right) \end{gathered}$$

are closer among each other.

Note that, as already stated in [12], the SAFECORAM resilience loss metric is time-independent.

The previous examples highlight a family of adoptable resilience loss metrics for SAFECORAM approach. One or more metrics will be definitively finalized and employed for the design of the methodology concerning resilience management in ATM.

### C. Statement of the Resilience Management Problem

In accordance with the definitions of the previous paragraphs, if a disturbance (or equivalently a failure) $\delta$ occurs in the nominal flow $S_0$ of the scenario $\mathbb{S}$ of the reference ATM system, a perturbation[1] is required in order to cope with the disturbance and its related stress[2]. Then, a set of alternative flows $\Gamma^{(\mathbb{S},\delta)} = \{S_1, \ldots, S_k\}$ may be executed in order to reach the same terminal condition of $S_0$.

Hence, the set of alternative flows $\Gamma^{(\mathbb{S},\delta)}$ strictly depends on the occurred disturbance $\delta$ in $\mathbb{S}$. Here, we assume that the disturbance $\delta$ is unique in $\mathbb{S}$ in accordance with [14]. As a consequence, the set of alternative flows is a function of only the scenario $\mathbb{S}$, namely, $\Gamma^{(\mathbb{S},\delta)} = \Gamma^{(\mathbb{S})}$.

The set $\Gamma^{(\mathbb{S})}$ can be modelled as a *DAG (Directed Acyclic Graph)*. This is a directed graph with no directed cycles, that is, it is formed by a set of vertices and directed edges with each edge connecting one vertex to another such that there is no way to start at a vertex $v$ and follow a sequence of edges that eventually loops back to $v$ again. We denote the DAG with $G = \langle \mathrm{V}, \mathrm{E} \rangle$, where V is the set the set of vertices and E is the set of edges. Every vertex $v \in \mathrm{V}$ corresponds to a single task $T_{i,j}$ and an edge $(u, v) \in \mathrm{E}$ – with $u, v \in \mathrm{V}$ – states that the task $u$ must be executed before the task $v$ starts. Hence, the edges represent the precedence relations of the alternative flows of $\mathbb{S}$, that is, of the equivalent DAG $G$.

Also assume that there are a starting vertex $v_{start}$ and a ending vertex $v_{end}$. The starting vertex conventionally represents a null task and also depicts the triggering condition (the disturbance $\delta$) of the set of alternative flows $\Gamma^{(\mathbb{S})}$. When all tasks/vertices are executed, then the scenario $\mathbb{S}$ finishes. In other words, $\mathbb{S}$ terminates successfully when $v_{end}$ is completed. The vertex $v_{end}$ is also named **terminal condition** of $\mathbb{S}$.

Thereby, an alternative flow $S_l \in \Gamma^{(\mathbb{S})}$ is a route (a sequence of vertices, i.e., of tasks) from $v_{start}$ to $v_{end}$ (Fig. 4).

In Fig. 4, every edge is labelled with the tuple $\left(k_{i,j}^{(1)}, \ldots, k_{i,j}^{(m)}\right)$, which represents the contribution of the destination vertex (task) $T_{i,j}$ in the evaluation of the KPIs.

[1] As regards resilience management, we suppose that the stress is survival and the perturbation is transient In this way, we deal with resilience (and not robustness) actions.
[2] The stress typically implies a decrease in one or more KPIs.

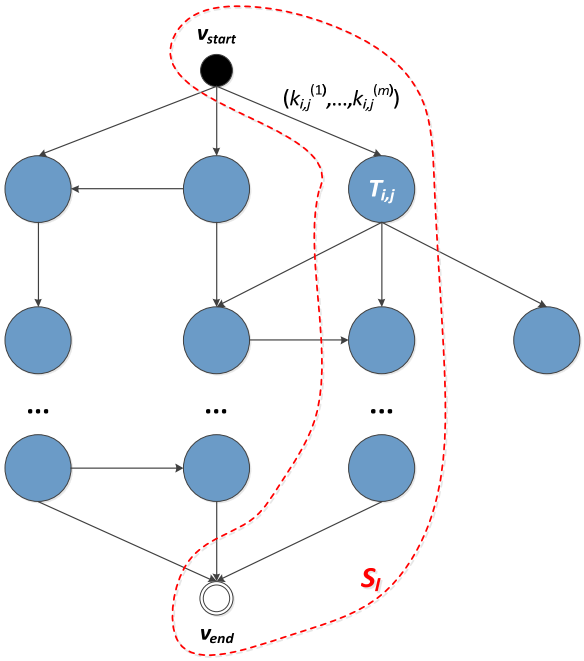


Figura 4. Directed acyclic graph for the set of alternative flows of a scenario.

At the end of the alternative flow $S_l$, the KPIs are evaluated and their values represent the current state $F(S_l)$ of the flow $S_l$, i.e., its current global performance.

Given a flow distance function $d(\cdot)$, we define the **resilience management problem** as the following optimization problem:

$$S_{opt} = \arg\min_{S_l \in \Gamma^{(\mathbb{S})}} RL_{\mathbb{S}}(S_l) = \arg\min_{S_l \in \Gamma^{(\mathbb{S})}} d(S_0, S_l) \qquad (10)$$

This problem consists in scheduling the best alternative flow $S_{opt}$ in the scenario $\mathbb{S}$ as the alternative flow in $\mathbb{S}$ that has the minimum resilience loss (i.e., the flow distance) with respect to the nominal flow $S_0$. The formulation of the problem (10) is independent from the definition of the flow distance.

Note that this problem is also a constrained optimization problem, wherein the constraints are represented by the precedence relations of the alternative flows, i.e., by the set of edges of the DAG $G$ that is associated to the set $\Gamma^{(\mathbb{S})}$ of alternative flows. Hence, the problem (10) is equivalent to find the optimal route from $v_{start}$ to $v_{end}$ in the DAG $G$ of $\Gamma^{(\mathbb{S})}$ (Fig. 4), namely, the route that minimizes the resilience loss metric $RL_{\mathbb{S}}(\cdot)$. From this point of view, every edge of $G$ has a crossing cost, which is related to the tuple $\left(k_{i,j}^{(1)}, \ldots, k_{i,j}^{(m)}\right)$ of its destination task $T_{i,j}$. This cost represents the increase in $RL_{\mathbb{S}}(\cdot)$ if the edge is crossed, i.e., if the task $T_{i,j}$ is performed.

This methodological approach assumes that the crossing cost of an edge depends only on the destination task, whereas it does not depend on the starting vertex. Indeed, the contribution of the task $T_{i,j}$ to the KPIs evaluation depends only on $T_{i,j}$ and it does not depend on the past evolution of the flow, i.e., the traversed sequence of tasks to reach $T_{i,j}$. Anyway, without loss of generality, the methodological approach would be the same even if this assumption was not true. In this case, the crossing cost of an edge would depend both on its starting vertex (the previous task) and on its destination vertex (the current task).

Moreover, the problem (10) refers to the ability of the ATM system to lead itself towards to the most similar state with respect to the reference state (the state of the main flow), that is, towards the target performance level $F(S_0)$. Hence, the formulated problem mainly refers to the definition of resilience as the ability to get back to the global performance level of the system by means of recovery actions. Here, the term recovery means a reallocation strategy of the tasks performed by the system components (as identified by the alternative flow) and does not mean restore (i.e., it does not deal with repairing actions of the failed components).

## IV. Conclusions and Future Works

The SAFECORAM proposal for resilience management addresses the following aspects of resilience:

- the third phase (recovery) of resilience pointed out in [15]
- the adaptive capacity in [9]
- the flexibility property [16] and some of its heuristics.

Other attributes (avoidance, survival, absorptive capacity, restorative capacity, etc.) are not considered.

In the end, a resilience optimization problem has been stated in [10], too. This problem aims at selecting an optimal recovery strategy that minimizes the resilience metric, that is, a combination of systemic impact and total recovery effort. So, the cost of the recovery action is from a restorative point of view (i.e., it is a repairing action). On the contrary, in the SAFECORAM proposal, the cost of the optimal recovery strategy is from an adaptive point of view, namely, it is a tasks reallocation strategy that is coded by the best alternative flow.

Future works will cope with the implementation of a set of flow distances, other than those ones suggested in this paper, and a set of scenarios in order to test the proposed approach. The goal of the experimental phase is the detection of one or more flow distances (or a combination of them) that best fit the intuitive concept of resilience engineering in ATM systems. The main concern related to this objective is the assessment of how the proposed solutions are satisfactory from the user point of view.

## Acknowledgment

This work is co-financed by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Programme. Opinions expressed in this work reflect the authors' views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

## REFERENCES


[1] CW Members. “ComplexWorld Position Paper”. Deliverable D23.2, December 2012, SESAR Project ComplexWorld (E-01.01). 2012

[2] R. Francis, “Analysis of Resilience in Manmade and Natural Systems”. Deliverable D1.1, February 2013, FP7 Project Resilience 2050, 2013

[3] E. Hollnagel, D. Woods, and N. G. Leveson,. “Resilience Engineering: Concepts and Precepts”, edited by Ashgate, Aldershot, UK, 2006.

[4] G. Baxter, “Resilience Engineering”. In: Socio-Technical Systems Engineering Handbook (Chapter 6), University of St Andrews. http://archive.cs.st-andrews.ac.uk/STSE-Handbook/, 2011

[5] ICAO. “Manual on Global Performance of the Air Navigation System”. Doc 9883, 2009.

[6] D. Henry, and J. E. Ramirez-Marquez,. “Generic Metrics and Quantitative Approaches for System Resilience as a Function of Time”. In: Reliability Engineering and System Safety, 99, pp. 114-122, 2012.

[7] S. Jackson,. “Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions”, edited by Wiley, 2009.

[8] M. Bruneau, S. Chang, E. Eguchi, G. Lee, T. O’ Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, and D. von Winterfeldt,. “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities”. In: Earthquake Spectra, 19, 2003.

[9] A. Cook, S. Cristòbal, P. Förster, and G. Tanner,. “ComplexityCosts – Update on the State of the Art”. Deliverable M04, Edition 01.00.00, February 2014, SESAR Project ComplexityCosts (E.02.21), 2014.

[10] E. D. Vugrin, D. E. Warren, M. A. Ehlen, and R. C. Camphouse,. “A framework for assessing the resilience of infrastructure and economic systems”. In: Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering, edited by Springer-Verlag, 2010, pp.77-116. 2010.

[11] E. D. Vugrin, M. A. Turnquist, and N. J. K. Brown,. “Optimal Recovery Sequencing for Enhanced Resilience and Service Restoration in Transportation Networks”. In: International Journal of System of Systems Engineering, 2014.

[12] V. Di Vito, and E. Filippone,. “Automation level baseline assumption for the definition of ATM scenarios”. Deliverable D1.1, Edition 01.00.00, October 2013, SAFECORAM Project (E.02.21), 2013.

[13] A. Errico and P. Caruso,. “Failure Emergency Scenarios: analysis approach”. Deliverable D2.1, Edition 01.00.00, October 2013, SAFECORAM Project (E.02.21), 2014.

[14] V. Di Vito, G. Torrano, A. Errico and E. Filippone,. “Study Reference Scenarios”. Deliverable D1.2, Edition 01.00.00, April 2014, SAFECORAM Project (E.02.21), 2014.

[15] R.Westrum,. “A Typology of Resilience Situations”. In: Resilience Engineering: Concepts and Precepts, pp. 55-65, edited by Ashgate, Aldershot, UK, 2006.

[16] D. Woods,. “Essential Characteristics of Resilience”. In: Resilience Engineering: Concepts and Precepts (Chapter 2), edited by Ashgate, Aldershot, UK, 2006.

[17] Errico, A., Torrano, G., Di Vito, Caruso, P., Cuciniello, G., Filippone, E. “Scenarios design and analysis of non-nominal conditions to suppport resilience engineering in ATM”, *Submitted for acc. To* SESAR Innovation Days ’14- Madrid, 25-27 November 2014.

[18] C. S. Holling,. “Engineering Resilience versus Ecological Resilience”. In: Engineering within Ecological Constraints, National Academy Press, Washington D.C., USA, pp. 31-44, 1996.

[19] O. Gluchshenko and P. Foerster,. “Performanced Based Approach to Investigate Resilience and Robustness of an ATM System”. In: Proceedings of Tenth USA/Europe Air Traffic Management Research and Development Seminar (ATM2013), Chicago, Usa, 2013.

[20] R. M. Hoffman,. “A Generalised Concept of Resilience”. In: Textile Research Journal, 18(3): 141-148, 1948.

[21] C. S. Holling,. “Resilience and Stability of Ecological Systems”. In: Annual Review of Ecology and Systematics, 1973:4, pp. 1-23, 1973.

[22]