The MEFISTO Project

ESPRIT Reactive LTR 24963 Project

Title of Document:	A method for the comparison of design options for allocating communication media in a cooperative and safety-critical context
Author(s):	Fields, B., Paternò, F., Santoro, C., Tahmassebi, S.
Affiliation(s):	University of York, CNUCE-C.N.R., CENA
Date of Document:	Oct, 02, 1999
Mefisto Project Document:	WP 1-16
Distribution:	INTERNAL
Keyword List:	Communication media, deviation, cooperation, mutual awareness
Version:	Draft

MEFISTO Partners:

CNUCE, Pisa, Italy

Alenia, Rome, Italy

Dept. of Computer Science, University of York, United Kingdom

DRA, Malvern, United Kingdom

Universitè Toulouse 1, Toulouse, France

CENA/Sofréavia, Toulouse, France

Associates Partners: University of Siena, Italy — ENAV, Rome, Italy

Title: A method for the comparison of design options for allocating communication media in a cooperative and safety-critical context	**Id Number:** WP 1-16

Abstract

In this paper we present the MECHA method for evaluating and comparing design options for communication media that pays particular attention to how they support cooperation in an interactive safety-critical system. The comparison is performed using three sets of criteria based on: task performance, analysis of user deviations and consequent hazards, and coordination. We illustrate the method by applying it to the design of how to allow access to new communication technology in an Air Traffic Control environment.

Title: A method for the comparison of design options for allocating communication media in a cooperative and safety-critical context	**Id Number:** WP 1-16

Table of Contents

Title: A method for the comparison of design options for allocating communication media in a cooperative and safety-critical context	**Id Number:** WP 1-16

Title: A method for the comparison of design options for allocating communication media in a cooperative and safety-critical context	**Id Number:** WP 1-16

1. Abstract

In this paper we present the MECHA method for evaluating and comparing design options for communication media that pays particular attention to how they support cooperation in an interactive safety-critical system. The comparison is performed using three sets of criteria based on: task performance, analysis of user deviations and consequent hazards, and coordination. We illustrate the method by applying it to the design of how to allow access to new communication technology in an Air Traffic Control environment.

2. Introduction

Design issues concerned with media allocation are becoming increasingly critical as technology becomes more diverse and more pervasive. *Media allocation* refers to decisions about the access that actors in a system have to different communication media. This is of particular significance in safety-critical systems where many studies have shown that accidents often are caused by a human error, whose likelihood may be increased by poor design (Reason 1990). For instance, Hollnagel surveys literature citing human error as a causal factor in as many as 80% of safety related incidents across a range of high-technology industrial sectors (Hollnagel 1993).

In such "high consequence" systems two contradictory tendencies seem to co-exist. On the one hand is a widely held belief that the deployment of advanced technology can lead, by automating inefficient and error prone tasks, to improvements in both performance and safety. On the other hand is the reluctance to introduce a new technology because of uncertainty about the impact of piecemeal technical changes (for instance on usability), and the consequent effect on safety and human life. In this regard we believe that, instead of trusting only to empirical testing in later phases of the development lifecycle, it is vital to perform evaluations of different user interface proposals and task allocation choices early in the design process.

An area where this kind of tension arises is Air Traffic Control (ATC), a highly interconnected cooperative system, where many problems have still to be solved. Huge increases in air traffic have meant that the existing systems are beginning to find it difficult to cope. The results are not only delays for the travelling public, but also concern about the risks of near misses and other incidents. Previous attempts have been made to develop alternative user interfaces for controllers (Chatty and Lecoanet 1996) or to augment the existing environment by the use of novel interaction techniques (Mackay et al 1998). However, despite much research effort, this work has remained at a prototype stage and has not been deployed in the field.

One of the problems facing the ATC system at the moment arises because currently most communication between controller and pilot is carried out by VHF radio, a medium of limited bandwidth that is fast becoming a bottleneck for ATC. This limitation, together with the known failure modes of voice communications (mis-heard communications are one of the most commonly reported ATC problems), can have serious safety implications. One solution that has been proposed is the introduction of *data link* communications, a technology allowing asynchronous exchanges of digital data containing messages coded according to a predefined syntax. This technology seems to overcome some of the main limitations suffered by the traditional system, but its implications for the work of

controllers and the safety of the overall system are not fully understood. It is this understanding that MECHA (Method for Evaluation of Cooperation, Hazards and Allocation) seems to improve with regard to specific design choices.

Safety, as many authors have observed, is not a property of individual tasks or actions, but of the interrelationships and interconnections between parts of a system. Perrow, for instance, identifies the complexity of a system and the coupling between its parts as significant factors in the genesis of accidents (Perrow 1984). What is often referred to as "human error" cannot be seen simply as a result of failures in human information processing; technology and technical change in a work system can create contexts that shape the way actions — erroneous or otherwise — take place (see Woods et al 1994). MECHA therefore supports the investigation of competing different design proposals in terms of how they might encourage or discourage various type of failure, how design and allocation decisions may tend to mitigate the effects of failure, and the ways the technology contributes to the detection and repair of failures. In the context of this work, we are particularly interested in safety issues in the communication between users of *a collaborative system*. Air traffic control work involves the co-ordination of activities and reconciliation of interests of pilots, the controllers working within a sector, and the controllers of other sectors, as well as many other agents and agencies. Although Symon et al. (1996) argue that a number of conflicts may exist in such work (between formal constructs and the work goals, or between the goals themselves), and that the term "collaboration" may be misleading.

It must be emphasised that technology changes inevitably lead to changes in the tasks of individual actors in the system (see, for example, Carroll and Rosson's (Carroll and Rosson 1992) discussion of the "task-artefact cycle). In particular, any device may provide support, automate tasks, or solve problems for some aspects of a person's activity. At the same time, the introduction of technology may have the effect of transforming tasks, creating new demands and placing additional requirements on the humans in the system.

Finally, a need for a structured analysis has arisen from the consideration that only ethnographic approaches are not sufficient to provide the information required from system designers and developers (Bentley et al, 1992) as such approaches tend to provide many details without sufficient indications about priorities among them thus making difficult the work of designers who have often to take decisions about what aspects are more relevant. Our method can be applied to a wide range of systems, not only to those that are safety critical. However, some aspects of the method, such as the analysis of deviations and hazards, are particularly targeted at systems where safety is a prime concern.

Taking these factors into account, the purpose of this paper is twofold:

- to present MECHA, a Method for Evaluation of Cooperation, Hazards and Allocation. The method aims to understand and analyse the impact of new communication technology in a safety context, and the different ways of assimilating it into the existing working practices;
- to apply the method to a real application, in this case en-route air traffic control, an area that is currently subject to various pressures and technological innovations. We discuss only a part of the domain, though the method can be applied much more widely. We consider a scenario and we will use it as a means to evaluate various design options.

In Section 0 we introduce the method, and then Sections 0 describes case study in general terms, and provides a scenario to give a concrete example of possible problems, activities and issues in the current system (Section 0). Then we propose two different ways to allocate the data-link and flight information to the controllers in a sector, and thereby allocate the main tasks between them (Sections 0 and 0). It is these compositions of task, technology and scenario that will be examined using MECHA.

For each design option (the current system and the two envisioned ways to access data link), the analysis of hazardous states is conducted using a method (Paternò et al. 1999), based on existing hazard analysis techniques (MOD 1996). In addition, a checklist-based inspection of the design options is carried out to make comparisons between them. The criteria for making comparisons are based on implications that design choices have for the tasks of individuals, for how they prevent or mitigate possible deviations in user behaviour, and for the coordination of the activities of several collaborating individuals.

3. The proposed method

Our work aims to bridge between a social view of collaborative activity and the work of designers of real systems who require systematic methods able to evaluate design choices. To this end the methods we propose support the analysis and comparison of a set of design options. In the specific case study considered in this paper they are: the current system, and other two options that differ in the way that new communication technology is used. The options differ in terms of how the tasks are performed and allocated, and on the choice of the artefacts and representations that are appropriate to support such tasks. These differences are highlighted by describing scenarios that allow the analyst to focus on a specific case of use. The scenarios are introduced in the technical context of the current system. Subsequently, the scenarios are modified in the other two cases. For sake of brevity in the paper we consider only one scenario. In a safety-critical context scenarios should be selected so as to focus on activities that can bring the system in a hazardous state.

In order to capture the main elements to analyse and how they differ in the considered cases, each option is characterised by the specific media and representations that they provide for controllers, the specific ways that tasks are performed and allocated, and the scenario of use considered. The comparison of the design possibilities will be guided by a collection of criteria that involve usability aspects (such as task efficiency, and coordination and mutual awareness) and safety aspects (such analysis of users' deviations and their impact).

3.1 Criteria for comparison

A collection of criteria that can be used in making comparisons between the different design and task allocation options has been identified. The aim is not to provide specific measurable parameters that can distinguish in a quantitative way between the options, but instead to suggest criteria that form a framework in which we may explore what the differences between the options are.

The reasons for this more qualitative approach is that evaluation of interactive systems is more economically carried out earlier in the development lifecycle, where re-design in response to identified problems is more feasible, as several authors (eg., John and Kieras 1996) have pointed out. Besides, the scope of MECHA is broader than a number of other HCI evaluation techniques (such as Heuristic Evaluation (Nilesen, 1993)), that focus on specific aspects of a user interface design, since it deals also with cooperation and hazards thus allowing designers to obtain a global evaluations of the impact of using different communication technologies.

The process of comparing competing design alternatives will be a two phase one. In the first phase, we envisage how a scenario will be "played out" given a particular configuration of technology, task, and responsibilities. In the second phase, we begin to ask questions that allow us to make hypotheses about some of the problems with the allocation of tasks and functions that might arise. In order to carry out this second, evaluative phase, we will assess the technology and its usage according to three sets of criteria. The enquiry will be scoped and contextualised by considering the tasks, actions and processes demanded by a particular scenario.

3.2 Implications for individual tasks and task allocation

We can identify three main types of difference between the current system and "augmented" systems where data-link is available:

- *Change of task allocation between the human and the machine*: for example, in datalink environment, the update of the ground system (containing flight information) is no longer performed manually by the controller, but in an automatic way by the system.
- *Change of task allocation between human operators:* because both controllers can communicate with pilots as well, by means of datalink functionality.
- *Change of objects manipulated by task and change of representations used to support tasks*: for example, in the new system the information contained in flight paper strips can be electronically provided.

Furthermore, a number of factors relating to the way tasks are carried out must be considered when making comparisons between the design options. For instance, technological changes can have the effect of transforming control tasks into vigilance and monitoring tasks at which people are often less effective (cf. Hopkin 1988). Similarly, design and task allocation decisions can have a significant impact on the workload of individuals and the range of responses to workload demands that are available to participants.

3.3 Hazards and deviations

This collection of criteria are particularly important for interactive safety-critical systems, and involve studying the different failure and hazard characteristics of different design options. We use an inspection technique to go systematically through the actions that are required from participants, and consider ways in which failures might arise during a scenario, what the effect of failures might be, and what safeguards and defences exist in the system. Since an objective of the current work is to explore the impact of different arrangements of communication technology, a special emphasis will be placed on communicative actions.

The particular questions we will seek answers to are: what are the potential hazards that can arise as consequences of deviations, failures in communication, or erroneous actions in the scenario? Are there factors that tend to encourage mis-communication, erroneous action, or faulty assessments? What recommendations concerning the user interface design can be provided to mitigate possible hazardous states and their effects?

This type of analysis will be performed with the help of *guidewords* (see MOD 1996, Leathley 1997, Burns and Pitblado 1993 for related techniques). A *guideword* is a word or phrase that expresses and defines a specific type of *deviation*. Guidewords have been found to be a useful tool to stimulate discussion as part of an inspection process about possible *causes* and *consequences* in deviations of user interactions. Mechanisms that aid the *detection* or *indication* of any hazards are also examined and the results are recorded. We have found it useful to investigate the deviations associated with the following guidewords:

- *None*, the task has not been performed or it has been performed but it has not produced any result;
- *Other than*, the task has been performed using the wrong data or producing wrong data;
- *Ill-timed*, the task has been performed at the wrong time.

In an analysis, these guidewords can be further refined. For example, *Other than* could be further refined into *Less*, *More*, or *Different* indicating situations where less, more or different information has been used in the tasks. Likewise *Ill-timed* can be refined into *Early* or *Late* implying that the task is performed too early or too late.

The basic idea is that for each option we consider the main tasks and the possible deviations that can occur in the performance of the task. Interpreting the guidewords in relation to a task allows the analyst systematically to generate ways the task could potentially go wrong, as a starting point for further discussion and investigation. This analysis may generate suggestions for how to guard against such deviations and recommendations about user interface designs that might either reduce the likelihood of the deviation, or support detection and recovery.

3.4 Co-ordination of activities and mutual awareness

The concept of “articulation work” and the means by which the activities of individuals are coordinated are a complex topic. For current purposes, we focus on one aspect, namely, the way in which technology changes (such as the introduction of datalink) have an impact on the kinds of coordination that are necessary and possible. More specifically, the two questions we will be asking about the design alternatives are:

- What coordinations are needed so that the tasks of the two controllers are brought into step? The answer to this question will typically be dependent on the particular roles, responsibilities, and tasks of the individuals involved.
- How such coordinations will be supported by the available mechanisms? The answers to this question are likely to be dependent on the detail of the technologies and artefacts that mediate the tasks of individuals and communications between them.

4. A case study in Air Traffic Control

4.1 The ATC domain

The principal objectives of the air traffic control system are generally stated as the achievement of safe and expeditious flow of traffic through airspace. In this case, safety is interpreted as meaning that separations standards, for the minimum safe distance between aircraft should be respected. The goal of expedition means that, so long as safety is preserved, the flow of traffic through the airspace should be maximised.

Civil airspace is partitioned, by horizontal and vertical divisions, into a number of geographical regions known as *sectors*. Typically, in an air traffic control centre (we refer to the French organisation), aircraft within a sector are managed by two air traffic controllers, who work closely together, but individually have rather different roles and concerns. The *executive* controller is able to contact aircraft using VHF radio, and is directly responsible for making short-term decisions and maintaining the appropriate separation distance between aircraft. The *strategic* controller, on the other hand, has longer term concerns and co-ordinates with strategic controllers in adjacent sectors to agree flight parameters (particularly the altitude) of aircraft entering and leaving the sector, so that their passage between sectors happens in a safe and orderly manner.

Negotiations between sectors concerning aircraft are always handled by the relevant strategic controllers and take place on the telephone. Both controllers must monitor the evolving traffic situation and identify possible conflicts or problems. It is the executive controller, who is responsible for deciding on how to solve a problem.

4.2 The scenario

At the heart of the analysis will be a scenario in which the functioning of each of the designs will be considered. The purpose of using a scenario will be to enable the analyst to envision how a particular technological configuration will affect the attempt to solve specific problems in a specific context. The same scenario will be used to consider each of the three design possibilities, but is described here in the context of the first: the current ATC system. In later sections, the differences for each of the technological variants will be described.

We structure the description of scenarios around a “template” that has been used previously as part of a scenario-based error analysis technique (Fields et al 1997). The template provides sections for describing the *agents* who play a part in the scenario, the physical *situation* and *environment* that generates problems for the

agents, the *tasks* to be carried out, *systems* and devices that are present, and the *actions* that take place as the scenario unfolds.

Agents

The scenario is centred on the activity of a single sector, and therefore an executive and a strategic controller are involved. Two other agents are also important: the pilots of aircraft in the sector (in particular BAW1234 and AZA5678), and the strategic controller of an adjacent sector. These five agents will be referred to as **strategic**, **executive**, **BAW1234**, **AZA5678**, and **adjacent strategic** respectively.

Situation and Environment

The activity takes place in an en-route sector in which two airways, A and B, intersect. A third airway also intersects A. The sector has boundaries with other en-route sectors. The two aircraft in question, BAW 1234 and AZA 5678, are flying along routes as shown in Figure 1. As indicated in the figure, both aircraft are at (and have been cleared to) Flight Level 290 (FL290). The problem faced by the controllers is the potential conflict between these two aircraft at the intersection of the two airways.

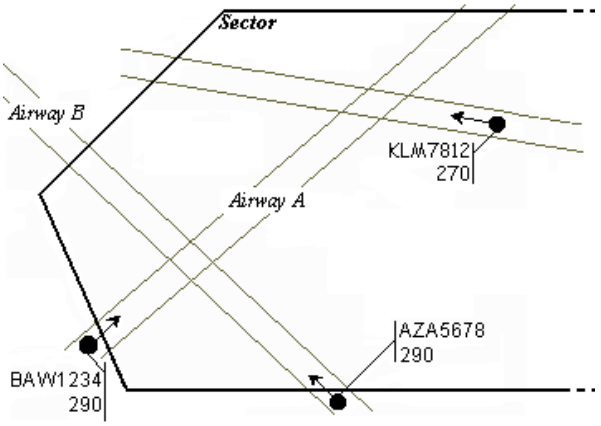

Figure 1: Intersecting airways in an en-route sector

A third flight, KLM7812, may generate a potential conflict depending on the solution to the first conflict. We assume that the controller is unable to make the aircraft change direction or speed to solve the conflict; instead, vertical separation will be achieved.

Task Context

We can now enumerate the tasks that controllers have to perform in the current environment. We use a level of "task granularity" chosen pragmatically to allow us to discuss and reason about the pros and cons of each arrangement. The list of

tasks is:

- *Detect problem.* The controller *identifies* a possible conflict in the current air traffic situation
- *Inform Controller.* One controller informs the other that a problem has been detected or something has to be done
- *Handle First Contact*. The task of replying to the first communication from a pilot who has just entered the sector
- *Solve problem*. The executive's cognitive process of *finding a solution* to solve a conflict or to achieve a more expeditious flow of traffic
- *Send Clearance.* The executive's task of sending instructions to aircraft for managing the traffic in the sector
- *Update Strip.* The executive annotates the flight strips to keep the "history" of the air traffic evolutions in the sector
- *Update ground system*. Both controllers — generally the strategic— are in charge of updating data in the ground system
- *Negotiate transfer parameters*. The strategic controllers have to negotiate about the best transfer flight parameters of the flights which are going to change sector
- *Monitor radar.* The controller checks the information provided by the radar
- *Handle Last Contact.* The executive sends to pilot the new frequency

In this scenario, the conflict between the two aircraft is detected by the strategic controller. A strategy for avoiding the conflict (by altering the altitude of one aircraft) is devised by the executive who issues a new clearance to the relevant aircraft. The strategic controller is responsible for seeking agreement for a revised co-ordination with the appropriate adjacent sectors, and at the same time, may respond to requests from other strategic controllers.

System Context

In this option we assume a technological context similar to that found in ATC centres today.

Actions

After having fixed the transfer parameters of the two flights with the strategic controllers of previous and next sectors, the strategic controller detects the potential for conflict using flight progress strips. This involves comparing flight levels and estimated times of arrival for the two aircraft at the point at which the airways intersect. At this stage, both aircraft are still outside the sector considered

(Figure 1). The strategic controller then informs the executive (who will devise a strategy for avoiding the conflict) and at the same time moves the strip into the correct position in the strip rack, within reach of the executive.

After few minutes, BAW1234 enters the sector and the first contact is received from the pilot of BAW1234 via the VHF radio ("Bordeaux control, Speedbird 1234, level 290, good morning"). Similarly, AZA5678 announces its arrival into the sector. On the basis of information previously supplied by the strategic controller, the executive is able to decide how to avoid the conflict. In this particular scenario, the executive decides to solve the conflict by increasing the altitude of BAW1234 (see Figure 2-a). This vertical separation will also avoid a conflict with flight KLM7812 that is travelling on the third airway. Therefore, the executive controller issues the clearance, which is then acknowledged by the pilot in question:

Executive: Speedbird 1234 CLIMB TO flight level 330

BAW 1234: Speedbird 1234 CLIMBING TO flight level 330

The executive then annotates the paper strip to indicate that the clearance has been given and the aircraft is climbing (see Figure 2-b), and starts to monitor on the radar if the flight actually performs the instruction. As this instruction affects the previously agreed Transfer Flight Level (TFL), at which the aircraft will make the transition between the current sector and the next one, some re-negotiation will be needed. The strategic controller, on hearing the communication between the executive and pilot, recognises the need to contact the neighbouring strategic controller to confirm whether the revised transfer flight level is acceptable.

The adjacent strategic controller, however, is unable to accept the revised altitude of BAW1234 as the TFL. An agreement between strategic controllers is reached on the original TFL: 290. The strategic controller now informs the executive verbally, and subsequently updates the flight progress strip to reflect this change.

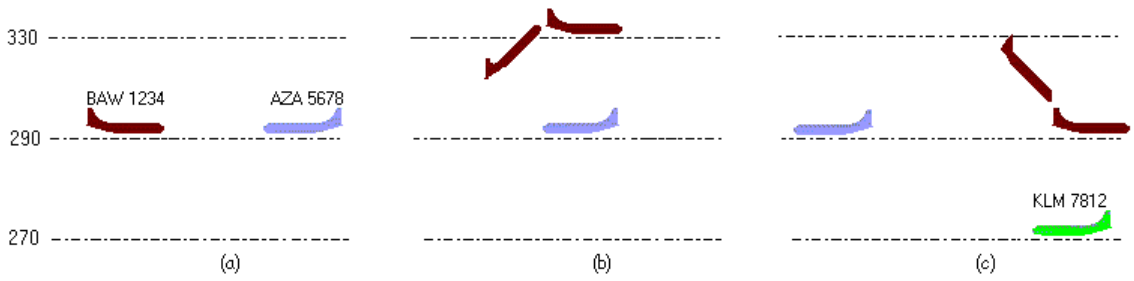

Figure 2: The different flight phases in the scenario

Therefore another exchange between the executive and pilot will be needed to transmit the new transfer flight level to the pilot of BAW1234. This must occur sufficiently far in advance to allow the aircraft to make the descent before

changing sector, and crucially, it must occur after BAW1234 has crossed airway B (see Figure 2-c):

Executive: Speedbird 1234 DESCEND TO flight level 290

BAW 1234: Speedbird 1234 DESCENDING TO flight level 290

The executive then updates the strip and one of the controllers updates the ground system (so that an updated flight strip can be printed in the next sector). Afterwards, the executive performs the "last contact" by informing BAW 1234 of the frequency on which the controller of the next sector must be contacted. Then BAW1234 switches to the new frequency and is able to communicate with the executive controller of the new sector. BAW1234 is no longer under the control of the current executive, who can remove the associated flight progress strip from the rack and discard it.

4.3 The three options considered

In our case study, three design options are analysed and compared. These are the current ATC system, and other two options that differ in the way that new communication technology is used. The two new options both use datalink (in different ways) and replace the paper strips with other electronic artefacts. This has an impact on how the tasks are performed and allocated, and on the choice of the representations that are appropriate to support such tasks.

In order to capture the main elements to analyse and how they differ in the three cases, each option is characterised by the specific media and representations that they provide for controllers, the specific ways that tasks are performed and allocated, and the scenario of use considered. In the end, we selected three main options for detailed consideration:

- the current system, supported by only VHF communication;
- a system with data link communication available only to the executive controller, and electronic flight strips. We have access to a user interface and air traffic control simulator, DRUIDES, developed at CENA, supporting this kind of datalink configuration;
- an envisioned system with data link communication available to both controllers: the executive is to send messages to pilots related to the aircraft's passage through the sector, and the strategic controller engages in communications with other strategic controllers concerned with changes of sector. We have access to a user interface prototype related to this option.

It is useful to explain why we selected these options for evaluation. We wanted to consider a small number of options that allowed us to address the main design issues. The key distinction between the new variants is that one aims to replicate existing communication patterns and support them with the new datalink

technology in order to overcome the reported bottleneck of overloaded radio channels. So, it permits an investigation of the properties of the communication medium, without altering the division of labour between controllers. The other one aims, instead, to change the allocation of communication tasks among controllers, taking advantage of the possibilities of the new technology and using different software artefacts to support controllers' tasks. It investigates whether it is possible to optimise the allocation of data-link to both controllers with a different allocation of tasks. The task of managing aircraft when they change sector becomes the responsibility of the strategic controller, and is connected with the task of negotiating about transfer parameters.

5. Option 1: The current system

5.1 The system and its usage

The system

Figure 3: The current air traffic control position

Looking at the environment of a single working position (see Figure 3), we see a complex array of devices and information artefacts. Controllers are provided with two radar screens, where the radar "tracks" (indicating the location of aircraft, the airways, and the sector limits) are displayed. A VHF radio is provided for use by the executive controller to communicate with pilots in the sector (this possibility is available also for the strategic only for emergency cases). Telephones allow the strategic controller to keep in touch with other strategic controllers of neighbouring sectors. A Touch Input Device (TID) allows both controllers to update the ground-based computer system to reflect changes to flight data (such as the time, flight level and track), following control decisions and instructions to aircraft to change these quantities although the strategic controller is normally in charge of performing these updates. Thus, in the current system three kinds of communications exist:

1. Between strategic and executive controllers of the same sector, (for example voice and "elbow" communications to attract attention)
2. Between the strategic controllers of neighbouring sectors involved in a flight sector exchange (by means of phone communications)
3. Between the executive controller and pilots of aircraft in the related sector (by means of VHF radio)

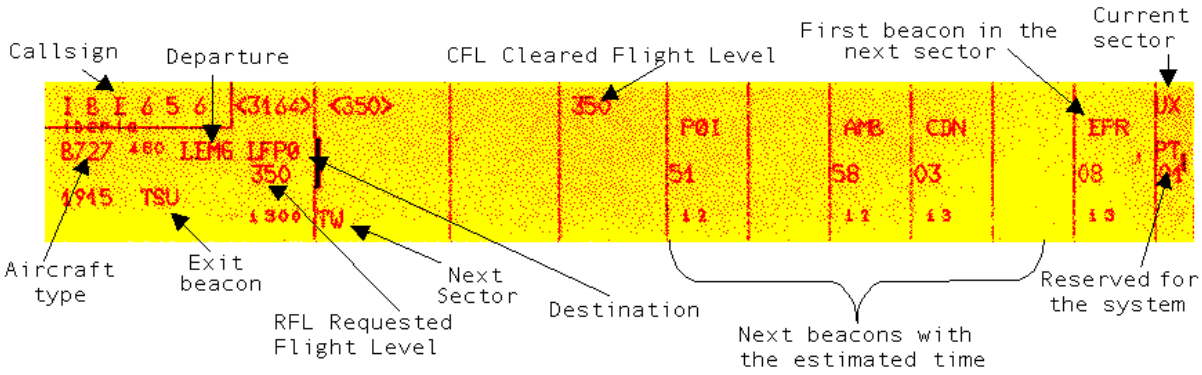

Figure 4: Example of paper strip

The controllers on a working position have also some flight paper strips printed "in real time" and delivered to a given control position about ten minutes before the flight enters the sector handled by that position. There is one strip per aircraft: the strip gives general information on the aircraft (identifier or callsign, aircraft type) (see Figure 4) but also flight information on the planned route of the aircraft. All the data printed on a flight strip are manually "updated" by the controller using a pen.

The scenario

Table 1 summarises the actions performed when the scenario occurs in the current technological setting, as described at greater length in Section 0.

1 **Strategic determines the possibility of conflict** and **alerts the executive**.
2. BAW1234 enters into the sector with the VHF message: "Bordeaux control, Speedbird 1234, level 290, good morning**".**
3. **Executive solves conflict** detected by strategic **sending the clearance:** "CLIMB TO 330"
4. **Acknowledgement received** from BAW1234 signalling that BAW1234 starts to climb. **Paper strips and ground system annotated manually.**
5. **Strategic overhears communication** and **recognises need for re-negotiation** of TFL
6. **Strategic contacts adjacent strategic controller**.
7. **Agreement reached** on TFL 290.
8. the **strategic informs executive** that the executive has to send a new clearance for the TFL290
9. the **executive sends the clearance:** "DESCEND TO 290"
10. **Acknowledgement received** from BAW1234. Paper strips and ground system annotated manually.
11. **Last contact** from executive: "Speedbird 1234 CONTACT Marseille control 135.85, GOODBYE" followed by pilot's reply.
12. **Paper strip removed**

Table 1: Scenario actions for option 1

5.2 Evaluating the design

5.2.1 Implications for Task performance

Table 2 shows how tasks are allocated between agents in the current ATC system. In this option we can note that there is no computerised support from the system for performing the main tasks identified and there are various tasks that can be performed by both controllers. Similar tables will be provided for the other options to highlight how tasks and their allocation is modified within them (for example, in some cases some functions will be carried out by the system). Some of the differences will arise as a consequence of the introduction of data link. For example, in the third option we will have a "change flight data" task instead of "update strip" because the third option is a stripless environment.

Strategic	***Executive***	***System***
Monitor Radar	Monitor Radar	
Negotiate Transfer Parameters		
Update Strip	Update Strip	
Update Ground System	Update Ground System	
Detect Problem	Detect Problem	
	Solve Problem	
	Send VHF Clearances	
	Handle First Contact	
	Handle VHF Last Contact	
Inform Controller		

Table 2: Task allocation in option 1

The main limitations of the current system are especially highlighted in situations of high traffic. Traffic increases are managed and controlled (and consequently the increase of conflicts to be prevented, detected and solved) largely by the executive, although the strategic constantly pays attention to monitor both the executive's activity and the traffic situation.

There are problems in situations of very high traffic because the executive remains the only agent in charge of making problem solving decisions and communicating them by means of radio communications without automatic decision support. Therefore, the greater the number of aircraft in the sector, the harder the executive's task, and bigger his/her workload in coordinating all the activities needed to ensure traffic safety and regularity. Besides, with a bigger workload the executive is much more prone to introduce errors and omissions in performing his/her task. In addition, congested radio channels increase the possibility of misunderstanding due to simultaneous communications requiring to repeat the

communication, and in the worst case, force the speaker to wait until the frequency is available again, making harder the task of communicating a message.

If we analyse the type of controllers' tasks we note that they are different in:

a) *Number of tasks*: the executive has to support all the communications with pilots and, at the same time, must respond to and solve problems as they appear in real time. The strategic controller, apart from the task of monitoring the system, has only to negotiate with other strategic controllers the flights' transfer parameters and to update the ground system for all the vocal communications that occur between the executive and pilots currently crossing the sector;

b) In addition, the executive's work is more demanding, because of *time constraints and deadlines.* The executive must often solve problems and make decisions before problems develop, whereas the temporal requirements on when the strategic controller updates the ground system, and so on, can be rather less stringent. Therefore, in contrast to the executive controller, the strategic controller can "organise" the work with a degree of flexibility.

c) The *type of skill requested*, because for example the task of resolving an unforeseeable conflict quickly in the traffic flow is obviously more demanding compared to the strategic controller's work of updating the ground system (that is a "routine" task above all).

The above considerations highlight that the executive controller is engaged in supporting heavier activity than the strategic (in terms of tasks, constraints on them and skill requested) which results in an imbalance in the allocation of work between the two controllers.

Regarding the representation of data in the current system the primary sources of information are the radar and the flight strips. In the current system, paper strips are available. When we analyse such strips we should not concentrate only on the information contained in the strips, but also in the type of interaction that a specific representational form allows tosupport the users' tasks. For example, paper flight strips are generally considered by controllers to be an extremely flexible tool, supporting both visual and tactile memory (Bentley et al. 1992). Additionally, the ability to easily rearrange and reorder strips in the strip bay depending on different criteria can play a crucial role in conflict detection and decision making.

Besides, recall that the strip offers a useful means of communication between the strategic and the executive controllers. The two controllers can work simultaneously on the strip board, annotating, moving and pointing at strips (for example the particular position where the strategic puts a strip in the strip bay is used to communicate a different level of urgency with which the executive has to put attention to it). In this way the communication between controllers is made

effective, reducing the need for explicit verbal communications in an acoustically busy environment. In addition, on the one hand the task of writing on paper strips can be an important means by which the controller's mental "picture" of the traffic situation is updated and reinforced. On the other hand, however, strips are sometimes seen simply as a distraction from looking at the radar screen. The same can be said of the task — generally carried out by the strategic controller — of manually updating the ground system: it reduces the time available for more important jobs.

The main controllers' task of avoiding, detecting and resolving conflicts results from a repeated cycle of looking at the aircraft representation on the radar and the associated flight strip in the strips' bay. Thus in the current system, especially in high traffic situations, the continuous activity of doing it (moving the eyes from two different artefacts — the radar and strips' bay — and coordinating the information from these sources) should not be overlooked in any assessment of controller workload.

5.2.2 Hazards and deviations

In the case of giving a clearance in a voice only environment (for example, "Speedbird 1234 climb to flight level 330") if we consider the "*none"* deviation it can indicate either that the controller has not sent the clearance or that it was sent but not received.

If the executive does not send a clearance there can be a number of possible explanations. As we saw in the scenario description, clearances can be the result of various activities: a conflict is detected, communicated to the executive, then a solution is identified by the executive, and translated into possible clearances. Each of these phases has the potential to fail. For example the possible conflict can remain undetected, or it may be detected, but the strategic is interrupted before informing the executive and the conflict is subsequently forgotten.

In this option the problem the pilot failing to hear the clearance could arise if other tasks on the flightdeck distract the pilots. It may take some time before the controller realises that the communication has failed. As the reader can see this analysis of deviations can be represented by tables structured as that below that give the analyst or designer a means of recording the justification or rationale for decisions that have been made. In the table we consider the task of sending the "last contact" instruction.

Task: Handle last contact		**Guideword: None**		
Deviation	**Cause**	**Consequence**	**Protection**	**Recommendations**

No message is sent by the controller	Controller fails to recognise the need for giving a new frequency (e.g. mistake dues to failing to note aircraft location or proximity to sector boundary) Perception problem	No new frequency received by pilot — aircraft may enter the sector without having contacted the new controller	(i) If aircraft enters next sector without making a call, the next controller will call the current one. (ii) Pilot calls ATC	Provide an indication when aircraft within threshold distance of sector boundary Such an indication would persist until electronic system updated
	Controller recognises need, but fails to send message (e.g. memory lapse or high workload-induced slip) Action problem			
No message is received	Pilot fails to perceive message (e.g. inattention, high workload) Perception problem		(i) Controller expects answer; lack of it may prompt a second call. (ii) Pilot calls ATC	If there is no answer within some time limit an alarm message (e.g. an audible signal) could be automatically activated
	Total failure of communication technology			

Table 3: Example of analysis of deviations based on guidewords

An "*other than"* deviation with the voice communication can be interpreted as meaning that, for some reason, the controller either sends the wrong information (wrong clearance, wrong parameter or both), or sends right information but it is incorrectly perceived by the pilot, or the wrong pilot is contacted.

Wrong information can be given for various reasons. For example, a relevant environmental factor may not have been taken into account. In this scenario, a third aircraft, KLM7812, is also in the sector, and the solution proposed can generate another conflict later on. Also, the *type* of solution may be correct but some of its details may not be. For example, the flight level chosen may not be appropriate for the direction of travel. Similar problems in a VHF-only environment can happen also because there is a lack of automatic tool support for making decisions. Thus all the support available for controllers, paper strips and radar information, require considerable cognitive effort. The pilot may misperceive or misinterpret the controller's command for various reasons, both linguistic and contextual.

Ill-timed communication is one that occurs either too early or too late. If the controller communicates a solution too early s/he can generate new problems other than solving the current one. For example, changing the flight level too early can generate a conflict with a flight that originally was not in conflict with that under consideration. Various reasons exist for a communication being late, most obviously, either controller may be busy with other duties. Another possibility is

that when the executive needs to communicate the radio channel is already "occupied" by another pilot. Indeed, another problem can be derived from limitations of audio communication. Since only one speaker can broadcast over the frequency at a time, the resulting communication has an asymmetrical nature (*one* speaker, *many* hearers). As all the pilots compete for the use of this resource, such sharing can be seen as penalising pilots.

5.2.3 Mutual awareness and cooperation

In the scenario we are considering here there are three main points at which the streams of activity in which the executive and strategic controllers are engaged in must be brought together and coordinated. The first of these points of coordination occurs when the strategic controller determines that a conflict is likely to occur, and informs the executive controller (step 1 in the scenario). This is a very explicit form of coordination between the two streams of activity.

The second point of coordination is that the strategic controller must know about the conflict-avoiding clearance the executive has issued ("*climb to flight level 330*" — steps 3, 4, and 5 in the scenario) so as to know that negotiation with the controller of the adjacent sector is necessary.

The third point of contact is that the executive must know the outcome of the negotiation between the two strategic controllers, so as to be able to pass the appropriate clearance to the aircraft (step 8).

Having identified what coordinations are required for the tasks on individuals to be carried out successfully, we can now begin to look at how they take place. In other words, what "coordination protocols" (Schmidt and Simone 1996) exist and how they are achieved.

In this situation, where VHF radio is the only form of communication between the ground and the air, communications between pilots and the executive are public, in the sense that they are audible in the control room, and may be overheard by the strategic controller. The communication between the strategic controller and controllers of adjacent sectors, on the other hand, is conducted through a medium with different properties: the telephone. One property is that conversations conducted using it are private and the executive is not party to them (at best, only one half of the conversation is made public in the control room).

The second coordination can therefore be accomplished in two ways: firstly, by the strategic controller monitoring the talk on the VHF channel and responding when necessary, or secondly, by explicit action on the part of the executive. This explicit notification can take place in a number of ways (speech, writing on flight progress strips, nudging and pointing). In practice, all these mechanisms are used, and the choice depends on a number of factors, such as the level of ambient noise in the control room, and the other tasks that are being carried out concurrently.

The third coordination is more constrained in how it can take place: since the communications between sectors cannot be overheard the strategic controller must, in the case where a re-negotiation of a new transfer flight level occurs, inform the executive explicitly.

On first sight, this constraint on the third sort of coordination may seem like a deficit, a lack of flexibility of coordinative mechanisms. However, this asymmetric arrangement (where, by monitoring, the strategic controller can gain an awareness of the tasks of the executive, but not vice versa) is entirely consistent with the idea that a "protective cocoon" is constructed within which the executive controller works (Hughes et al. 1992). The status of the executive's work is rendered public by the nature of the VHF channel, creating an awareness, whereas no such facility exists for the maintenance of a mutual awareness of the strategic controllers work.

This will tend to have an impact on the nature of the division of labour that exists between the controllers. The strategic controller is able to "help out" in times of busyness (a clear connection between coordination and safety). Flexible arrangements such as this are made possible by the public nature of some of the communication media. Our own observations at a current air traffic control centre have identified a number of routine situations where the "shared space" of VHF transmissions permits just such an arrangement. The strategic controller is able to appropriate some of the tasks normally carried out by the executive (for instance, those connected with flight progress strip management).

6. Option 2: Data link for the executive controller

6.1 The system and its usage

6.1.1 The system

In this option the main differences with respect to the current system are in terms of system context and actions. With datalink functionality available we have a fully electronic environment in which some of the current technology (radar displays, paper flight progress strips) is replaced completely. Figure 5 provides an example of possible user interface layout. Electronic flight strips are on the bottom left side whereas on the right side there is a representation of the current traffic in the air sector. There is also the possibility to display on the controller's interface the graphic trajectory of each aircraft currently in the sector. Radio and phone are still present.

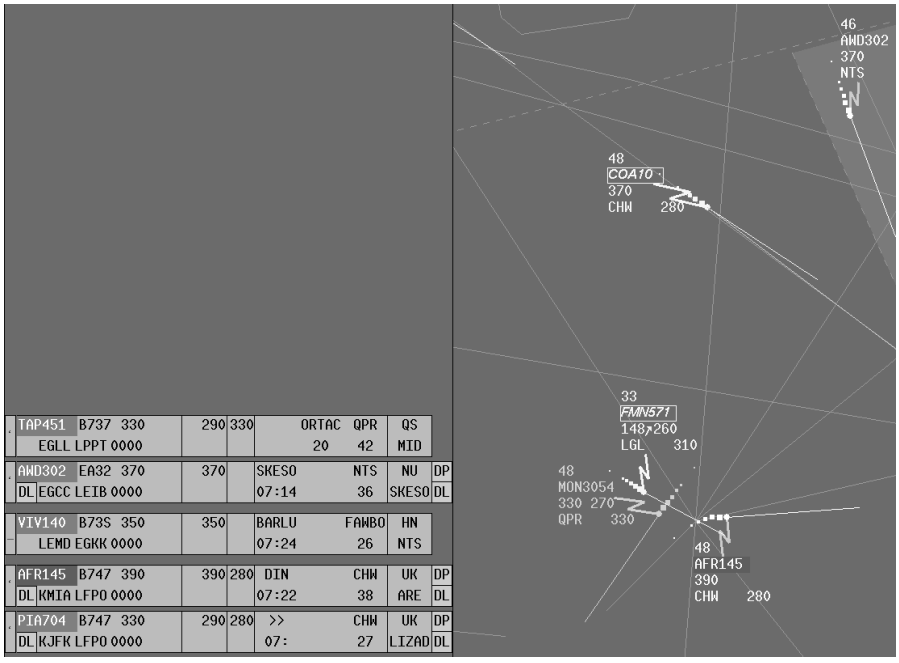

Figure 5: a data link user interface with electronic strips

6.1.2 The scenario

In the following listing we highlight the differences with respect to the scenario associated with the current system, assuming that the all communication is performed by data-link. Data link communications are “point-to-point” so in the instructions below the pilot will not be specified.

1. **Strategic determines the possibility of conflict** and **alerts the executive**
2. BAW1234 enters into the sector **sending the DL message:** "MONITORING Bordeaux control 120.5". The executive replies only if the frequency is wrong => no executive DL answer in our scenario
3. Executive **solves conflict** detected by strategic **sending the datalink clearance** (CLIMB TO 330)
4. WILCO received (via datalink) from BAW1234 signalling that BAW1234 starts to climb => **electronic strips and ground system automatically updated**
5. Executive with voice comm. **makes strategic aware of need of re-negotiation** on TFL
6. **Strategic contacts adjacent strategic controller**
7. **Agreement reached** on TFL 290.
8. the **strategic informs executive** via voice that the executive has to send a new clearance for the TFL290
9. the **executive sends the clearance via datalink** (DESCEND TO 290)
10. **WILCO received** via datalink from BAW1234 => **electronic strips and ground system automatically updated**
11. **Last contact** from executive - MONITOR Marseille 135.85 to BAW1234 and pilot's reply (both via datalink).
12. **Electronic strip disappears** from controllers' view

Table 4: Scenario actions for option 2

6.2 Evaluating the design

6.2.1 Implications for task performance

Table 5 shows how the task allocation is performed in this option. By interacting with the electronic strip the same interaction can perform two tasks: update strip and update ground system. In this context the executive controller has still a larger workload than the strategic controller. The previous factors a)-c) (introduced in paragraph 4.2.1) are still valid in this case, but the executive's problems can be worse because of the need to pay attention on two different sources of information (concerning the communications with pilots).

Strategic	***Executive***	***System***
Monitor Radar	Monitor Radar	
Negotiate Transfer Parameters		
Update Strip	Update Strip	Update Strip
		Update Ground System
Detect Problem	Detect Problem	
	Solve Problem	
	Send (VHF & DL) Clearance to Pilot	
	Handle VHF First Contact or Datalink Monitoring	
	Handle (VHF & DL) Last Contact	
Inform Controller	Inform Controller	

Table 5: Task allocation in option 2

In fact, in the current system (first option) an upper limit is placed on number of communications that can be received from pilots by the sequential nature of radio technology. Data-link, on the other hand, has no such limitation (or rather, it has different limitations) and capacity of the technology can increase beyond that of the executive, especially in situations of heavy traffic. Consequently, evaluating in a comparative way the strategic and the executive's workload, the imbalance is even more evident. The above considerations allow us to say that in this option there is the most **unbalanced allocation of work** between the executive and the strategic controller.

It is worth noting that providing the executive controller of another media of communication allows him/her to improve the task performance whenever s/he is able to perform concurrently more activities using different senses (audio/visual) and overcome the problem of congested radio channels.

In addition, even though in this option another media of communication is provided together with the radio channel especially in high traffic situations the increase in communication availability is not exploited enough. This is because the executive remains still the interactive system's bottleneck being the only agent in charge of supporting the communications with pilots (**low performance with high traffic**).

In this option, we suppose an electronic environment available to controllers: the flight progress strips are electronically provided and are visualised as a part of the controller's user interface. This can be a useful improvement because we observed that in the first option the information was spread and displayed over different sources, needing a high eye co-ordination ability from the controller to blend them. In addition, it may affect the global system safety since every information source which causes diversion of controller’s focus of attention is highly undesirable and should be avoided as much as possible.

Under this option the controller is a bit more alleviated from this task since keeping track of traffic evolutions in the ground system is performed in an automatic way and the same is valid for the update of strips (of course, as far as it concerns the datalink communications), so the controller could reply sooner to pilots' requests (in Druides was also possible to send clearances by selecting flights on the radar screen).

In addition, the simultaneous presence of aircraft representation and the associated flight strip on the same support allows to easily implement an automatic mechanism to link the two representations to each other: whenever the controller points an aircraft data block, the correspondent electronic strip is simultaneously highlighted (flashing) and vice versa. In this way the aforementioned problem for

the controllers to scan the strip bay (or the radar) in search of a particular aircraft is eliminated and the resulting controller's fatigue is reduced, although eye movements (from strips to aircraft representations) are still required.

6.2.2 Hazards and deviations

The introduction of data link can solve some problems generated by voice communications. For example there is no longer the problem that a communication is not sent because the frequency is busy, although it is worth noting that not all communications between pilot and controller are supported with the same effectiveness with datalink messages compared to the equivalent -often faster and more natural- radio communications. On the other side, the datalink messages seem to better support long clearances, when may be very useful to check visually a long message before sending it out, rather than only mentally verify and then repeat it aloud (as in the current system), so decreasing the possibility of mistakes sending them.

However, datalink messages also introduce some possible concerns: with *none* deviation the problem of perception from the receiver side may increase because a voice message can attract the attention of the receiver (either pilot or controller) more than a message that appears in a user interface already full of indicators that have to be visually checked. To this end in electronic strip environments it is important the use of techniques suitable to highlight arrival of new information.

In addition, a good user interface should prevent from the possibility that the sender of a datalink message (i.e. the controller) leaves the system in a state where s/he edits the message but then s/he is distracted by some other problems and, consequently, s/he forgets to perform the action that triggers the sending of such a message. Besides, in a data-link environment some feedback highlighting that a clearance has been sent but the related wilco has not yet been provided from the pilot can be provided to help the controller to remember the state of the ongoing communication.

In a graphical user interface for a data-link communication there can be some problems belonging to the *other than* deviation: problems related to the typical slips that can occur with such user interfaces, thus it is important that they are designed so as to prevent these possibilities. For example, among the classical interaction's techniques, the menus are an example of how a user interface can decrease (but unfortunately not eliminate) the possibility of introducing wrong input parameters (so reducing the possibility that an "other than" deviation could occur in this system), just because the data are selected from an available range of values. On the other hand, note that in order to select an item in a menu, a controller has to click in a zone which can be very small, so it can cause that s/he has to put really attention to this action, subtracting his/her visual attention to other tasks (monitor the traffic): this feature can be considered a drawback

compared to the current system where the controller was able to watch radar simultaneously to sending a radio clearance, and a potential increase to system's hazards.

Ill-timed communication cannot occur for the limitations typical of the voice communication. Moreover in a data-link user interface it is easy to highlight flights that are within a certain threshold from the sector's limits so as to remember that the related clearances should be provided or some graphical elements that show how the selected flights should evolve so as to better detect possible conflicts. However, the use of more information on the screen associated with the flight position can decrease the readability when the flights considered are close each other thus requiring more time to detect information useful for the controllers' activities and slowing down the ability to send clearances.

6.2.3 Mutual awareness and cooperation

The same coordination requirements exist in this case as in the VHF regime: the executive must be informed of the existence of a potential conflict; the strategic controller must be aware of clearances that the executive issues; and the executive must be aware of the results of cross-sector negotiations. Some superficial differences between this situation and the current system exist at the level of tasks. For instance, the automatic updating of the ground system and the presence of electronic flight progress strips means that it is no longer necessary for the flight progress strip to be manipulated and removed manually. What are different in more important ways, however, are the mechanisms by which coordination may take place.

Several observations can be made about the mechanisms by which coordination may be achieved in this case:

- In contrast to the VHF only case, there are fewer "public" mechanisms to support co-ordination.
- However, the more sophisticated environment does contain some cues for coordination. For instance, the fact that an aircraft has been assumed (by action on the part of the executive) is indicated directly in the display (the colour of the aircraft symbol). Thus providing a kind of "computational coordination mechanism" (to use the terminology of Schmidt and Simone 1996).
- Problems of visual, computer mediated coordinations: cf. the Druides experience, where alarms (not coordination mechanisms, as it happens) went unnoticed by controllers (COURTEIX-Kherouf 1998).

This arrangement of communication media has a number of implications for the coordinations that must take place. The first and third coordinations are relatively unchanged from the VHF case, and still require an explicit action on the part of the strategic controller to notify the executive. The second point of coordination is

different in this case, compared to the previous one. It is no longer possible that the activities of the two controllers can be coordinated by the strategic controller "listening in" to talk on the VHF channel. Some more explicit means of communicating will be necessary (such as the executive notifying the strategic controller when the clearance has been issued).

One further implication of this is that the technology may tend to limit the kind of opportunistic intervention and "helping out" that is made possible in the current system, through shared representations and media (such as the VHF channel) that allow controllers to gain an awareness on one another's work. Such flexible working appears to make the system more robust by allowing, to some extent, at least, "workload peaks" to be smoothed out, and the division of labour to be flexibly renegotiated in response to changing circumstances. An implication for design is that if such flexible working is deemed desirable, then additional measures will have to be taken to permit the levels of mutual awareness that are needed to support it, by compensating for what the replacement of voice by datalink has tended to diminish.

7. Option 3: Datalink for both controllers

7.1 The system and its usage

In this option we consider an environment with more electronic support. We thus consider the possibility that both controllers, in different circumstances can send clearances by data link, and the electronic strips are replaced with enriched flight labels. The motivation for such enriched flight labels is to improve some limitations found with electronic strips. For example, several trials at CENA emphasised that the electronic strip table was rarely used by controllers, who often failed to monitor the system consequently (COURTEIX-Kherouf 1998). In fact, asynchronous events and especially visual alarms went unnoticed: when something was going wrong in the datalink exchange the related warnings were mainly shown in the strip table, which was not used, even though a warning indication in red was also available on the radar data block, but it was not sufficient enough to get the controller attention in time.

7.1.1 The system

In this option the strategic controller can use data link technology in the flight transfer phase. This means both frequency-related clearances and clearances related to change of flight parameters during such a phase. In order to better support the understanding of when a flight is under the control of the strategic we recommend the possibility to graphically represent in the sector the area pertinent to the change sector activities.

All the interaction with system functionality are supported through the radar labels, as the ability to operate directly on an item in the current focus of attention is really important for the controller: in some sense the radar data block becomes a multi-line label that replaces the flight strip. Note that, in order not to clutter the screen, the information permanently displayed on these labels is kept to a minimum, allowing at the same time the controller to expand it (moving and clicking the mouse onto it) when s/he has to up-link some instructions or collect aircraft information.

So, in this improved system the flight parameters of aircraft currently in the sector are displayed “on demand” by controller when necessary, leaving on the screen only a minimal kernel of the most relevant information (the “standard” label, see

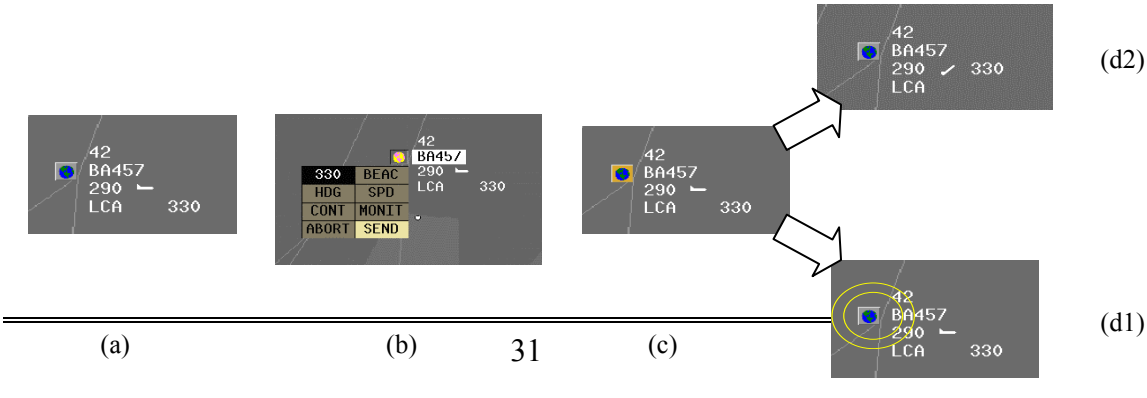

Figure 6-a). In Figure 6 we show an example of session when the controller wants to send to pilot the instruction of changing the flight level parameter: moving the cursor onto the radar label, the label is expanded, it is possible to select the CFL instruction, the requested new flight level (330 in our example, see Figure 6-b), and then either to abort or to send it; when the clearance is sent to the aircraft the symbol beside the callsign has a special colour to indicate that the Wilco has not been received yet (see Figure 6-c). When the "Wilco" is received (Figure 6-d_2), the symbol returns to the normal colour and the icon of the aircraft changes to indicate that it is actually climbing. Another possibility is that the pilot is unable to perform the instruction: in this case, an error symbol beside the callsign is displayed in a warning colour (Figure 6-d_1). In such a way, the improvement is that for each aircraft currently in the sector, the attention of controllers is focussed only to its (multi-line) label, which allows them to performs their activities to send clearances to pilot, to collect flights parameters, etc., and the attention is no longer divided between the representations of aircraft on radar and the associated flight strip.

Figure 6: An enriched flight label

7.1.2 The scenario

With respect to the previous option the difference is in terms of actions. Suppose that the strategic controller has to support all the activities necessary during the "change of sector" (CS phase) phase, leaving the normal en-route phase (ER phase) to the executive. Under this option it becomes really important to define precisely both when the datalink control passes from the strategic to executive and vice versa (to know when a flight is under the control of the executive and when the flight is under the control of the strategic) and in which flight phase (CS or

ER) BAW 1234 should firstly climb and then descend: we assume that the first clearance (climb) has to be sent when the BAW 1234 is into its ER phase, and the second clearance (descend) has to be sent while BAW 1234 is into its CS phase.

1. **Strategic determines the possibility of conflict** and **alerts the executive**
2. The ground **receives the datalink message** when BAW1234 enters into the sector: "MONITORING 120.5". No strategic's reply.
3. Executive **solves conflict** detected by strategic sending the datalink clearance (CLIMB TO 330)
4. **WILCO received** from BAW1234 => **ground system automatically updated**
5. Executive makes strategic aware of need of re-negotiation on TFL
6. **Strategic contacts adjacent strategic controller**
7. **Agreement reached** on TFL 290.

8. The strategic **sends the datalink clearance** (DESCEND TO 290)
9. WILCO received via datalink from BAW1234 => **enriched flight labels and ground system automatically updated (change flight data)**
10. Last contact from strategic (MONITOR Marseille 135.85) to BAW1234 and pilot's reply (via datalink).

Table 6: Scenario actions for option 3

7.2 Evaluating the design

7.2.1 Task performance

The workload between controllers is more distributed, both in terms of number of tasks and in terms of type of task: in fact under this option the strategic controller has a more direct role in making decisions and controlling the traffic as far as it concerns the flights in their "changing sector" phases, resulting much more involved in the overall controllers' activity of managing and controlling the traffic. As shown in Table 7 the task *Update strip* disappears to be replaced with a *Change flight data* task as there are no more strips in this environment.

Strategic	***Executive***	***System***
Monitor Radar	Monitor Radar	
Negotiate Transfer Parameters		
Change flight data	Change flight data	Change flight data
		Update Ground System
Detect Problem	Detect Problem	
Solve Problem	Solve Problem	
	Send VHF Clearance to Pilot	
Send DL Clearance to Pilot (only during change sector)	Send DL Clearance to Pilot (only during en route)	
	Handle VHF First Contact	
Monitoring Frequency		
Handle DL Last Contact		
	Handle VHF Last Contact	
Inform Controller		

Table 7: Task allocation in option 3

In fact, whereas in the other cases the strategic had to perform all "routine" activities, now his/her activity can have a direct impact on the general system speed-up, as all flights going into the sector or leaving the sector have to communicate with the strategic controller.

On the one hand this can result in less work for the executive, and in a real "parallelism" by allowing clearances to be sent pilots (in different flights phases) by both controllers, overcoming most limitations of the previous options. On the other hand, the need for mutual awareness and coordination between the

controllers becomes more acute.

As a matter of fact, a "stripless environment" actually gives controllers more time to watch the display, even though controllers have to spend some time for the additional activities related to mouse selection of enriched labels to display the data that in the other options are permanently displayed. The problem of linking the aircraft representation with the information normally included in the flight strip is addressed by this design. However, this raises additional questions about how well particular tasks (for example the task of comparing values associated to two or more aircraft in order to avoid conflicts) could be performed under this option. Further improvements could be imagined: for example the possibility to send specific clearances in a graphical manner rather than in a textual way, for example selecting on the screen the next beacons rather than textually editing them.

7.2.2 Hazards and deviations

In this option possible deviations with respect to the expected behaviour can be originated when the flight is in a position very close to the change sector phase so as both controllers can believe that it is under the other controller's responsibility. This requires a user interface mechanism highlighting in which of the two phases the flight is (for example adding an internal border to the sector indicating when the flight enters in the area requiring change sector clearances).

Having a controller dedicated to the handling of the change sector phase with data link commands decreases the possibility that the related clearances are sent too early or too late (or they are not sent at all). However, there may still be some problems when several flights are transferring, and one of them requires cross-sector negotiation by the strategic controller, thus distracting the strategic from sending the clearances concerning the other flights.

In the *other than* deviation case we can imagine the possibility that the controller identifies a good logical solution but it supplies incorrect parameters. For example, the controller may attempt to use flight level that is reserved for flights travelling in the opposite direction. It is important to include in the user interface some support for avoiding such situations, for example disabling the possibility to give to a flight a flight level associated with the opposite direction. This can be done exploiting the more electronic support foreseen in this option.

7.2.3 Mutual awareness and cooperation

Many of the coordination issues of the previous case are relevant here: the executive makes tactical decisions (of which the strategic controller should be aware) and the strategic controller manages cross-sector negotiations (the results of which the executive needs to know about).

The most significant change from the previous two cases is that the strategic controller now carries out an action that was previously carried out by the executive (arranging for the handover of the aircraft to the next sector). This might have the effect of changing the executive's workload and improving the balance of work between the two controllers. It also changes coordination requirements: it is no longer required that the strategic communicates the change sector flight parameters to the executive and the executive controller must become aware of when the aircraft is no longer under his control because is in the area under the control of the strategic. Several mechanisms exist to facilitate this kind of coordination, the most obvious being the colour coding used to indicate the status of aircraft.

8. Summary and lessons learnt

In our study we have seen how the MECHA method can be used to analyse and evaluate the impact of the introduction of new technology in a safety-critical context. The method is based on aspects, such as task allocation and performance, analysis of deviations and cooperation mechanisms that can be useful to analyse not only safety-critical applications. However some aspects, such as analysis of deviations and suggestions for preventing them or mitigating their effects are particularly important in this type of applications where in some cases the effects of deviations cannot be undone and can have catastrophic effects.

Besides, we have seen how safety-critical applications are interactive, real-time applications where users (controllers in our case study) should be ready to detect deviations and manage them so as to avoid further problems. As controllers can perform some other activities, in some cases by cooperating with other controllers, this can prevent them from detecting such deviations. In this possible concurrent activities lies the root of many safety issues. Such a concurrency often allows more efficient and flexible performing of tasks so the problem is not to limit it but to design environments able to effectively and safely support it.

Table 8 summarises some of the findings for each of the three design options that have been discussed in the previous sections.

	Hazards and deviations	**Task performance**	**Mutual awareness and cooperation mechanisms**
Only VHF	Considerable (due to executive's bottleneck)	Low with high traffic (mainly due to combined bottleneck of VHF media available only to executive)	*From exec to* strategic: implicit (for VHF communications with pilots); *From* strategic *to exec*: always explicit (for phone communications with other strategic)
D.L. for executive	Fewer hazards or deviations related to misunderstanding of VHF communications (due to availability of DL)	Low with high traffic: the executive's bottleneck still remains, improvements in media communications (DL is added to VHF)	*From exec to strategic*: need for explicit mechanisms (for datalink communications with pilots) *From* strategic *to exec*: need for explicit mechanisms (for phone communications with other strategics)
D.L. for both	Low (if both controllers are aware of *when* each flight is under the control of *which controller*)	Improvements of global performance: two media -VHF and DL- available (for communications with pilots) to *both* controllers	*From exec to strategic and from* strategic *to exec:* Need for explicit mechanisms for all datalink communications with pilots

Table 8: Summary of design options

In our analysis we have indicated a useful tendency to obtain artefacts that allow *users to better integrate information concerning a specific logical object.* While paper strips require a strong effort to integrate information that is on them with that provided from the radar, electronic strips decrease such a effort and enriched labels further improve this integration.

We have seen how a combined analysis of the tasks carried out by the user and of the possible deviations provide information to define how tasks should be performed to improve their performance and understand the impact of possible deviations in the considered system. This analysis can not leave out of consideration the specific environment (in terms of single or multi-agents, different media and artefacts, several object representations, etc.) where the tasks are performed, and in this sense a comparative analysis amongst current and envisaged systems can give useful information to highlight for example which arrangement allow to get a better performance of which tasks (hardly ever one system is the "best" in absolute terms).

The systematic analysis of deviations gives useful suggestions for improving the design. For example, it is possible to better identify when an action from the controllers is required and to suggest introduction of warning messages and the level of intensity of the relative alarm messages so as *limiting the impact derived from possible deviations from expected behaviour* that we found with our analysis.

The current system has successfully been used for many years. However it is now going to change because it is inadequate to address the external conditions that are changed (such as the strong increase of air traffic). Indeed, radio communication has some limitations that are more evident when there is a need to carry out several communications concurrently.

However the long practise of controllers with it has consolidated *a set of coordination mechanisms that are well recognised and sufficiently reliable*. It is thus important that this level of coordination and robustness be preserved in future and possibly even improved. Although increased automation does not always improve usability (Bainbridge 1983), the introduction of more electronic support can lead to a *decrease in the workload* of controllers because of the possible automation of some tasks (for example whenever a command is accepted by the pilot the system is automatically updated). It is also possible to introduce functionality to automatically identify information useful for *supporting decision making*.

9. Conclusions and future work

The user interface design is a complex process, which has to consider several different aspects, especially when intended for a cooperative and interactive safety-critical application as in the air traffic control example considered in the paper. When such safety critical applications are analysed, both usability and safety aspects have to be carefully considered in an integrated way.

We have presented a method based on the use of three types of criteria (implications on task performance, analysis of deviations, and coordination) and its application to the en-route air traffic control by considering three options in the use of communication media.

Taking into account the analysis developed, whose results are summarised in the previous sections, we plan to modify the Druides prototype for supporting en-route air traffic control with data link support. Further work on developing tool support for the proposed method is also foreseen. In this case the purpose will be to provide scenarios and task model to the tool and then the tool should help the designer to identify design options and effective solutions.

10. References

Bainbridge, L. (1983) Ironies of Automation. *Automatica* 19, 775-779.

Bentley R., Hughes J., Randall D., Rodden T., Sawyer P., Shapiro D., Sommerville I., (1992) Ethographically-informed systems design for air traffic control, *Proceedings CSCW'92*, pp.123-129.

Burns, D.J. and Pitblado, R.M. (1993) A Modified HAZOP Methodology For Safety Critical System Assessment. *Directions in Safety Critical Systems — Proceedings of the Safety-Critical Systems Symposium*, Bristol, 1993, Springer-Verlag.

Chatty, S., Lecoanet, P. (1996) Pen Computing for Air Traffic Control, in *Proceedings of CHI'96*, April 13-18, 1996 Vancouver, British Columbia, Canada.

Carroll J., Rosson M.B., (1992) Getting Around the task-artifact cycle: how to make claims and design by scenario, *ACM Transactions on Information Systems,* 10, pp.181-212.

Courteix-Kherouf., S. (1998) Complementary Use of Data Link and Voice Frequency communication between Pilots and Air Traffic Controllers in a simulated Environment. *Proceedings HCI-Aero'98*.

Fields, R.E., Harrison, M.D. and Wright, P.C. (1997). *THEA: Human Error Analysis for Requirements Definition.* University of York, Department of Computer Science, Technical Report YCS-97-294. http://www.cs.york.ac.uk/~bob/papers.html

Hughes, A., Randall, D. and Shapiro, D. *Faltering from ethnography to design*. CSCW'92, the Fourth Conference on Computer Supported Cooperative Work, New York, ACM Press.

Hopkin, V.D. (1988) Air Traffic Control. In E. L. Wiener and D. C. Nagel, Eds. *Human Factors in Aviation*. Academic Press, 1988. Pages 639-663.

Hopkin, V.D., (1995) Human Factors in Air Traffic Control, Taylor & Francis, London.

Hollnagel, E. (1993) *Human Reliability Analysis — Context and Control.* Academic Press.

John, B.E., Kieras, D.E. (1996) Using GOMS for User Interface Design and Evaluation: Which Technique?, *ACM Transaction on Computer-Human Interaction*, Vol. 3, No. 4, December 1996, 287-319.

Leathley, B.A., (1997) HAZOP Approach to Allocation of Function in Safety Critical Systems, In *ALLFN'97, Proceedings of the 1st International Conference on Allocation of Functions*., Galway, Ireland, IEA Press.

Mackay, W.E., Fayard, A.L., Frobert, L., Médini, L. (1998) Reinventing the familiar: exploring an augmented reality design space for air traffic control, in Proceedings of CHI'98, April 18-23, 1998, Los Angeles, CA USA.

MOD (1996) HAZOP Studies of Systems Containing Programmable Electronics. UK Ministry of Defence, Interim Def Stan 00-58 Issue 1.

Nielsen J. (1993). *Usability Engineering*. Boston: Academic Press.

Paternò, F., Santoro, C., Tahmassebi, S. (1998) Formal Models for Cooperative Tasks: Concepts and an Application for En-Route Air Traffic Control. In Proceedings DSV-IS '98, Springer Verlag, U.K.

Paternò, F., Santoro, C., Fields, B., (1999) Analysing User Deviations in Interactive Safety-Critical Applications, Proceedings DSV-IS'99.

Perrow, C. (1984) *Normal Accidents: Living With High Risk Technologies.* Basic Books.

Reason, J., (1990) *Human Error*, Cambridge University Press.

Schmidt, K. and Simone, C. (1996) Coordination Mechanisms: Towards a Conceptual Foundation of CSCW Systems Design. *Computer Supported Cooperative Work: The Journal of Collaborative Computing* **5**(2/3): 155-200.

Symon, G., Long, K. and Ellis, J. (1996) The Coordination of Work Activities: Cooperation and Conflict in a Hospital Context. *Computer Supported Collaborative Work: The Journal of Collaborative Computing* **5**: 1-31.

Woods, D.D., Johannesen, L.J., Cook, R.I. and Sarter, N.B. (1994) *Behind Human Error: Cognitive Systems, Computers and Hindsight.* CSERIAC, State-of-the-Art Report SOAR 94-01.