The MEFISTO Project

ESPRIT Reactive LTR 24963 Project

Title of Document:	The impact of different media on safety and usability of interactive ATC applications
Author(s):	Paternò, F., Santoro, C., Tahmassebi, S.
Affiliation(s):	CNUCE-C.N.R., CENA
Date of Document:	Mar 3 1999
Mefisto Project Document:	WP 1-15
Distribution:	INTERNAL
Keyword List:	Safety, Usability
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: The impact of different media on safety and usability of interactive ATC applications	**Id Number: WP 1-15**

Abstract

In this report a set of criteria relevant to assess the impact of using different media in the design of user interfaces for safety-critical systems is proposed and discussed. An evaluation of different options concerning such media during the design of an interactive and cooperative application in the Air Traffic Control domain area is shown to illustrate and clarify our approach. Particular attention has been paid on how different choices in the allocation of tasks among air traffic controllers and the modalities of their performance affect usability and safety of operators' interactions.

Title: The impact of different media on safety and usability of interactive ATC applications	**Id Number: WP 1-15**

Table of Contents

1. Introduction

In spite of increasing development and availability of new communication technologies and tools, little work has been dedicated to analyse more deeply the concepts which drive the choice and use of interaction media when the design of user interfaces for safety-critical systems is considered. To this end we believe that, instead of trusting only late empirical testing to define the most appropriate way of working, it can be useful to perform an evaluation on different media and task allocation choices **[Leathley97]** according to appropriate criteria to discard meaningless possibilities and to focus on problematic parts of the design.

As in current applications the co-existence of more than one technology is getting more and more common there is a need for a deeper understanding of nature and constraints of each media used and their appropriateness with respect to the environment where the media is supposed to be used, for better evaluating which technology provides the best support for a task in a specific context.

Besides, the media allocation issue is getting more demanding especially in current safety-critical systems where many studies have shown that accidents often are caused by a human error [Hollnagel93]. In these systems two contrasting trends seem to exist at the same time: on the one hand (the general belief that) the more advanced technology used, the better in terms of performance and reliability; on the other hand the indisputable reluctance and difficulty to introduce a new technology in these systems because their impact (especially in terms of safety and usability) is not always known and at worst it may threaten human life.

An example of the latter issue is given by applications in a highly cooperative system [Paternò98b] as the Air Traffic Control (ATC) area, where many problems are still to be solved. The number and duration of delays show that ATC system and the airports are not always able to cope with passengers' demand, the growing air traffic increases the possibility of accidents and several air traffic control incidents have occurred because of the undesired effects of operators' interactions or the lack of efficiency in current systems, requiring more sophisticated techniques for its management. Previous attempts have tried to introduce more advanced user interfaces for the controllers [Chatty96] or to provide them an augmented reality environment [Mackay98] to make faster and more natural their activity, but unfortunately these approaches are remained at a prototype's stage and have not been followed by real utilisation.

Furthermore, keeping in mind that currently most communications between controller and pilot are carried out by means of VHF technology, the increases in air traffic have begun to stress that the real bottleneck stays just in the radio channels used in today's controller-pilots ATC communications, which can become soon saturated during high levels of air traffic, therefore several solutions are going to be envisaged. One of the most innovative solutions is the introduction of a new means of communication between controllers and pilots: the data link. In strict sense, datalink means "terminals together with interconnecting circuits permitting the transmission of data between the terminals" **[EUROCONTROL]** . Thus, with a data link application, the controller is provided with the capability to issue altitude assignments, lateral deviation, route changes and clearances, speed assignments, radio frequency assignments and various requests for information and the pilot is provided with the capability to respond to messages, to request clearances and information, to report information and to declare/rescind an emergency.

The introduction of this new communication technology seems to overcome the main limitations suffered by the traditional system even though its effects are not well understood and there is still a lot of work to do in order to identify the most effective user interface design.

In the next sections, we firstly introduce our approach and give a general overview of ATC system in terms of tasks [Diaper89] [Paternò98a] that have to be supported with special attention to media and tools provided by both VHF and datalink technologies. Then we analyse two possible different allocations of media in the environment considered and we define the evaluation criteria that we plan to consider. Finally an evaluation of the different media allocation options is given according to the previous criteria.

2. Our Approach

The continuos improvement of interaction and communication technologies often raises the problem of understanding whether the introduction of such technologies can reduce the level of safety related to the possible user interactions. The case study that we show in this report is an example of this type of problems that can raise also in other application areas. The overall goal is to obtain user interfaces supporting safe interactions without loosing in terms of usability. Indeed often usability requires the possibility to support a flexible environment, however this has to be carefully designed in order to avoid to introduce the possibility to get into hazardous states.

Our approach is based on the use of task models that describe the activities that should be performed by both users and applications in reaching the overall goals. We start with the tasks supported by the current technology (in our example, voice-based Air traffic control) [Paternò98]. Then we provide criteria to evaluate different options for designing new applications supporting new technologies such as data link communication. The criteria considered are fair allocation of work among controllers, conflicts on shared objects, possibility of hazardous situations and time of task performance. The analysis of possible hazardous states is performed by using an extension of a HAZOP technique applied to the possible activities to perform while interacting with the considered application.

More specifically we have analysed two different design options concerning on how to allocate the interaction media to the two controllers co-operating in a station, advantages and drawbacks of each of them are discussed using the set of criteria that we propose.

3. The current ATC system: A brief Overview

Before describing our analysis it can be useful to provide the reader with a short overview of the main features of the current (French) ATC system, describing roughly the controller tasks during the en-route phase (other countries may have a slightly different system). Our intention is not to detail all the controller activities but only to give an idea of the major tasks they have to do and particularly to identify the different communication media they have to use both in the current system and in a future system where the availability of datalink technology in addition to radiotelephony communications is envisaged.

The civil airspace is divided into various control centers and, within each centre, it is divided among sectors through horizontal and vertical division (geographical sectors). Two controllers operate in one working position (even though, depending on the traffic, an assistant can help on the position):

- the *executive* controller, who is in charge of maintaining the appropriate separation between aircraft and holding the voice frequency, in other words in the current system only the executive controller speaks to the pilots.
- the *strategic* controller, who is in charge of co-ordinating, on the one hand the entrance of the aircraft into the sector with the strategic controller of the previous sector, and on the other hand the exit of the aircraft with the strategic controller of the next sector.

In addition, some « background » tasks have to be added for both controllers which correspond to surveillance tasks. So we can identify three kinds of communications (the related numbers refer to those in Figure 1):

1. Between strategic and executive controllers of the same sector, (for example vocal and "elbow" communications, that is pointing the radar with fingers to capture colleague's attention)
2. Between strategic controllers of two neighbouring sectors involved in a flight sector exchange (by means of phone communications)
3. Between the executive controller of each sector and pilots currently in the sector (thanks to radio communications)

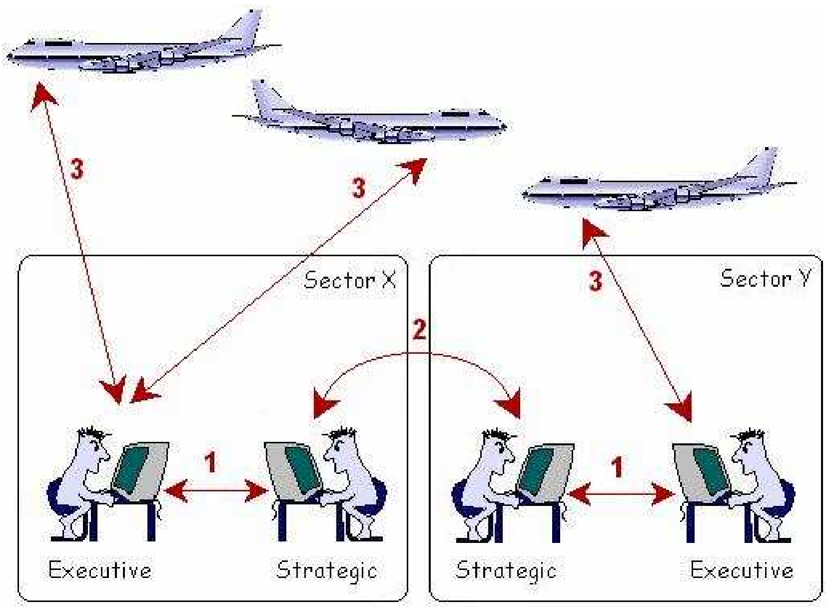

Figure 1: The communications occurring between en-route controllers

Looking more deeply in the environment of a single working position (see Figure 2), controllers are provided with two radar screens, where the aircraft radar tracks, the airways, and the sector limits are displayed, a radio used by the executive controller to communicate with all pilots in the sector, a telephone used by the strategic controller to keep in touch with other strategic controllers of neighbouring sectors, and a Touch Input Device (TID) which allows controllers to update in the ground system some flight data such as the time, level and track (these updates are normally performed by the strategic controller because the executive controller is generally busy).

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 call-sign, aircraft type) but also flight information on the planned route of the aircraft. All the data printed in a flight strip are manually updated by the controller with a pencil. The controller can also update the ground system via the Touch Input Device (TID), but these updates are limited: at a given time the ground system has not the latest up-to-date information for each flight.

The main goal of this application is safety and regularity of flights: safety means that minimum separation are respected between aircraft; regularity means that the flights follow as much as possible the initial flight plans.

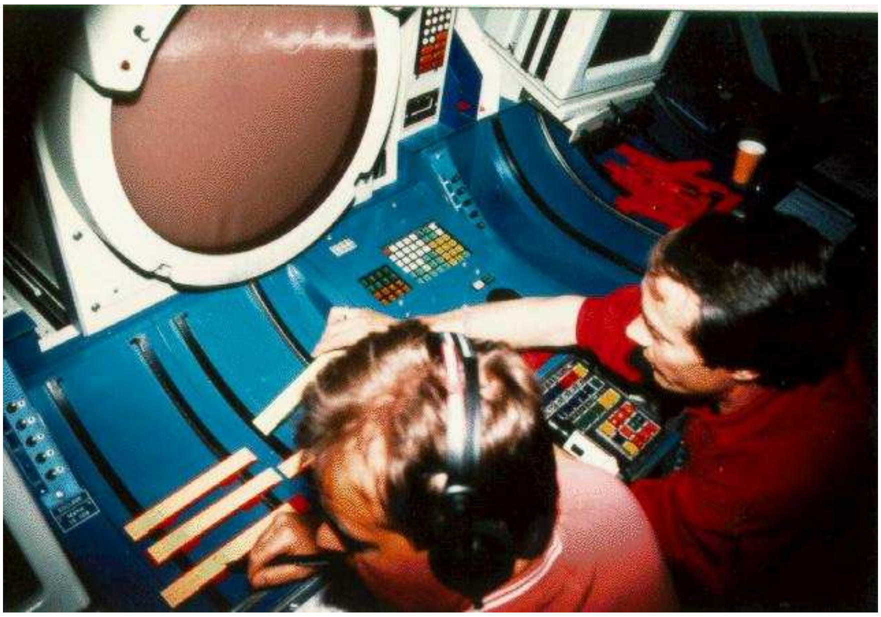

Figure 2 : The controller working position

Today, most of air/ground communications are conducted by voice over Very High Frequency (VHF) or High Frequency (HF) radio channels. The frequency of each sector is dynamically assigned and it is known to all the pilots who are currently in the sector and who have to tune in to it for communicating with the controller. Since only one speaker (controller or pilot) can broadcast over this frequency at a time, and there are *many* pilots and *one* executive controller, the resulting communication has an asymmetrical nature because all the pilots are in competition for speaking with the controller. This kind of "sharing" obviously penalises the pilots since sometimes they have to wait because the frequency at the moment is busy.

However, the "party line" (the fact that on a given frequency a pilot can listen to all messages exchanged on that frequency —even the messages not addressed to him) has proved to be useful because the pilots are able to check about the information exchanged avoiding possible misunderstandings of vocal communications, and to build their own mental traffic representation. In addition, the party line contributes to enhance pilots situation awareness, in that pilots listening to controllers' communications with other a/c (aircraft) can obtain advance knowledge of events and situations that can affect their flight (i.e. traffic congestion, delay report, weather conditions). In this way they can perform a better decision-making process, and eventually anticipate future controller's instructions offering to do some actions to speed up the sector traffic management, thus improving the global efficiency and safety of system.

The main advantage of the current R/T (radio telephony) is that it is a rapid means of communication between pilots and controllers being voice the most natural means of human communication: an R/T message contains not only the message itself, but also some subjective information (such as stress, emotion, anger, humour, courtesy) being relevant to pilots and controllers. However, the process of communicating clearances or information by voice is prone to human error, because its transient nature might easily introduce mis-understandings and confusions: thus, the main limitations of the current R/T can be either

- *technical* (channel congestion, limited range, simultaneous transmissions on the same frequency, amplitude modulation susceptible to weather interference) or
- *human* (miscomprehension, due to either the poor quality of the communication, or transient nature of voice, or difficulties to understand a non native language (accents), or workload, or confusion due to the party line effect). In addition, recall that in order not to occupy for a long time the frequency, the communications exchanged through radio channels are generally concise (following the standard aeronautical phraseology), so they can not be considered in strict sense “natural” communications.

To overcome most limitations of the current system, different alternatives have been proposed. One solution is the reduction of the spacing between each aeronautical frequency channel, however this solution cannot be a long term solution because firstly the traffic will still continue to increase (and then the congestion of the frequencies will appear again) and secondly, as a given frequency is associated to a given sector, the increase of the number of frequencies will imply the increase of the number of ATC sectors and the size reduction of the sectors; in these conditions, the pilots will have to change very often the active ATC frequency on-board and a lot of air /ground communications will be devoted to the transfer between sectors. Thus, as the current system seems to have already reached the limits of its capability and to be really short of efficient solutions, there is an increasing interest to analyse the possibility that conventional radio communications can be augmented with a new communication media called datalink. The datalink system electronically transfers digital messages to computer screen displays located on the ground and in the aircraft, and initial human factors considerations have already suggested that this approach can increase the efficiency with which the air traffic controllers operate and the airspace is managed, and reduce pilot communication errors.

4. Task Supported

Now we can start to identify the tasks that controllers have to perform in en-route ATC applications. For the time being, we use a kind of "task granularity" refined enough to discuss and reason about pros and cons of each arrangement. In the following table we list the tasks we consider together with the domain or logical objects which are manipulated by each of them.

Task	Explanation	Domain objects
Monitoring Radar	The controllers have to monitor continuously the radar to prevents conflicts and solve problems in handling the traffic in the sector	Flight traffic
Negotiation about Transfer Parameters	The strategic controllers have to negotiate about the best transfer flight parameters of the flights which are going to change sector	Flight level
Annotate Strips	The controllers annotate the flight strips to keep the "history" of the air traffic evolutions in the sector	Flight level, Route, Speed, Destination
Update Ground System	Both controllers —but generally only the strategic controller— are in charge of updating the data in the ground system which contains information on the flights' plan to allow printing of updated flight strips.	Flight level, Route, Speed, Destination
Detect Problem	The task of *identifying* a possible conflict in the current air traffic situation	Flight traffic in terms of routes, flight level, lack of separation
Solve Problem	The cognitive process of *finding the best solution* to solve a conflict or to give more regularity to the traffic flow	Current and foreseen air traffic
Send Clearance to Pilot	The "most important" communications with pilots, namely orders and clearances	Flight plan, clearance
Send Information to Pilot	In some sense the "less important" communications with pilots, e.g. weather information, delay reports	Basic information
Handle First Contact	The task of replying to the first communication of a pilot who is just entered in the sector	Flight identifier, Frequency

Handle Last Contact	The task of communicating the frequency of the new sector to a pilot who is going to leave the current sector	Frequency
Inform Other Controller of Problem	The communication task performed by a controller to inform his/her colleague of a problem enhancing mutual knowledge of traffic situation	Conflicts, conflicts' solutions

Table 1: The Controllers' Tasks

These tasks have to be *performed by* (*at least*) *one of the two controllers* in each of the three options that we are going to study, and you can notice that in the above table we did not specify *who* actually performs a task because the problem of an optimal allocation of tasks among the controllers and its impact on the user interface design will be discussed in the next sections.

5. Changes in task performance with the introduction of datalink

It is important to remark that data link environment does not mean ‘no voice’ environment. An air-ground data link environment means an environment where two media of air/ground communication exist : the data link and the voice. Therefore all the high-level tasks previously described are still valid. The difference is that voice communication will be reduced and new (data link) communication will be available, producing a new environment where both technologies are present. This will modify how the tasks mentioned will be performed.

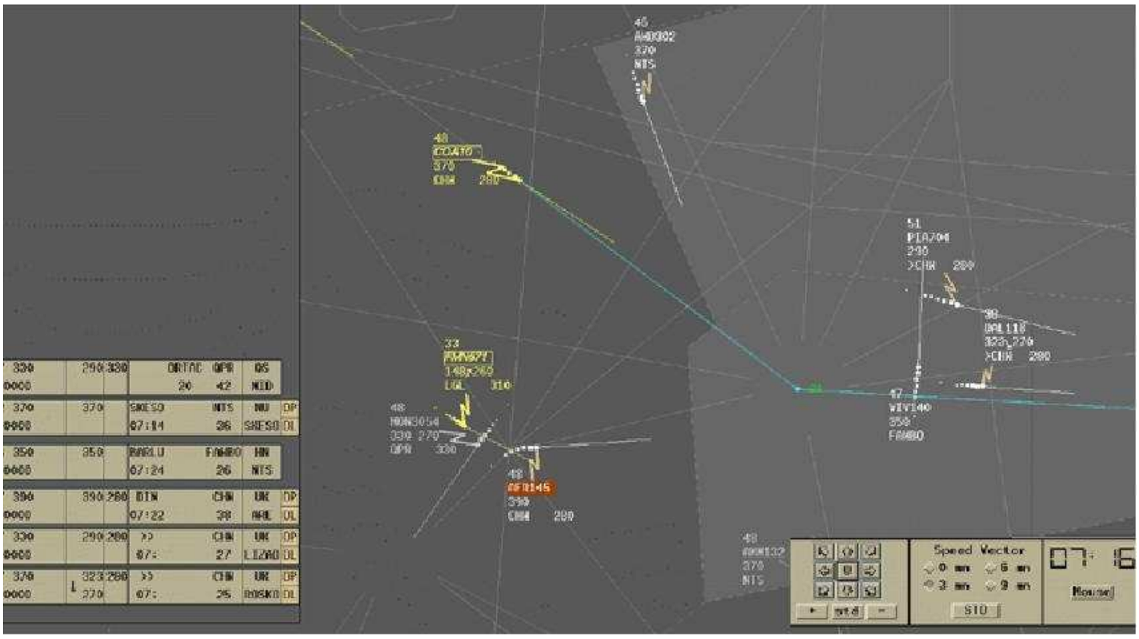

Figure 3: An Example of Controller's User Interface in a Datalink Environment

We can identify three main differences passing from the current system to the "augmented" system where both media are available:

1. *Change of task allocation between the human and the machine*: for example, in datalink environment, the update of the ground system is no longer performed manually by the controller, but in an automatic way by the system;
2. *Change of task allocation between human operators:* because the strategic can communicate with pilots as well, by means of datalink functionality;

3. *Change of artefacts manipulated by interaction tasks*: this can have an impact on how tasks are performed and, consequently, on usability and safety aspects. An example of new artefacts in the new system is that the flight strips can be electronically provided in addition to traditional paper strips.

In Figure 3 we show an example of user interface for en-route controllers in a datalink environment: in the window, the radar data blocks of aircraft currently in the sector are recognisable, together with their associated electronic strips listed and displayed on the left-bottom part of window. The controller is allowed to send instructions to an a/c either from the associated electronic strip or from its radar data block via a pop-up menu. Once the pilot replies with a positive answer ("Wilco" message), the ground system is automatically updated.

In the current system the same instruction would have been transmitted via voice with the additional task for the controller to update the ground system after having received the positive pilot's operational answer. More precisely, when the controller receives the Wilco from pilot, firstly s/he has to identify him, then retrieve the correspondent callsign on the radar screen, find the associated strip in the rack, annotate it and update the ground system within ten minutes before the a/c leaves the sector. Therefore this task is revealed rather demanding because the information is spread and displayed over different sources, needing a high eye/hand co-ordination ability from the controller to blend them; in addition, it might 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. In the new environment the controller is alleviated from this task since keeping track of traffic evolutions in the ground system is performed in an automatic way.

In addition, even if the controller does not have to annotate but just read the strip for integrating this information with the a/c current position on the radar, now both pieces of information are on the screen and then the necessary eyes' movements and the resulting controller's fatigue is reduced.

Anyhow, further improvements can be underlined in the datalink user interface prototype shown in Figure 3 too: for example, several trials at CENA emphasised that the electronic strips' table was rarely used by the controllers who often failed to monitor the system consequently. In fact, asynchronous events and especially visual alarms go unnoticed: when something was going wrong in the datalink exchange the related warnings were mainly shown in the strip table (see Figure 4-a), which was not used, even though a warning indication in red was also available on the radar data block (see Figure 4-b), but it was not sufficient enough to get the controller attention on time.

(a) (b)

Figure 4: A Warning Message in the Datalink Environment

6. The analysed options for media and tasks allocation

In the following sections, we consider possible different options on media and tasks allocation between executive and strategic controllers as far as it concerns the communications controller-pilot(s). Each option will be evaluated on the basis of several criteria, ranging from the time of task performance, the balancing of the workload among controllers, to the potential conflicts in accessing to shared objects and the number of possible hazardous situations.

Before going forward into the proper analysis, it is better to define more precisely the hypothesis that we are going to consider:

H1. The negotiations needed to possibly modify some sector change parameters are always handled by the strategic controllers of each sector involved in the change;

H2. For each sector, both the controllers have to monitor the traffic situation and to identify possible conflicts or problems, but only the executive controller is in charge of deciding what the best solution is to solve a problem.

It is important to note that these hypothesis affect the possible (reasonable) assumptions because they can generate further constraints deriving from humans senses knowledge. In the environment considered, the direct consequence of the first hypothesis (the strategic controller has to negotiate by telephone with the strategic controllers of the neighbouring sectors) is that the strategic has always to put attention to information going from an *audio* source (the telephone). Thus the opportunity of allocating in a "dedicated" way only one audio media to each controller arises (the telephone to the strategic, the radio to the executive), and the necessity of discarding all the assumptions where the strategic controller has to communicate with pilots on the frequency as well. In fact, if the strategic is already busy on the telephone with another colleague s/he cannot perform equally well (or equally quickly) the critical task of hearing and replying to pilots that would want to speak with him/her on the frequency.

Another possibility we considered initially was that the executive had to support the vocal communications, leaving the strategic controller to manage the datalink communications with pilots. But it was rejected because it created a situation hardly governable. For example, under this assumption, every communication to a datalink-equipped aircraft could be initiated by both controllers (because also voice communication is possible for datalink-equipped a/c), and it could happen that the pilot answers to a controller's request using a different modality (thus communicating with another controller), causing the existence of "mixed" communications that seemed to be rather dangerous.

We started our analysis with three main options which are graphically summarised with the following tables:

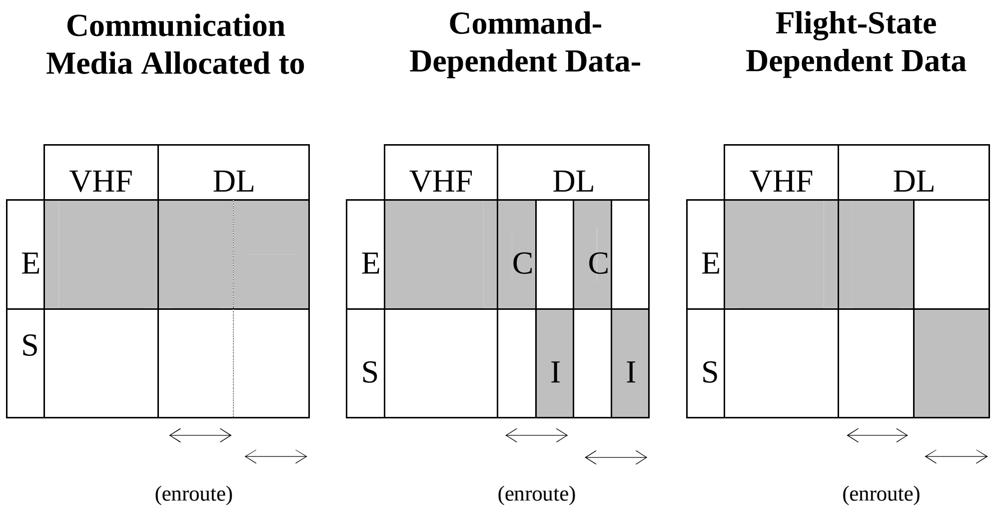

Figure 5 : A Tabular Overview of the Three Options Initially Considered

In order to reason about the different selected options, each table was split into two rows —one for each controller, executive (E) and strategic (S)— and into two columns —one of each media used for controller-pilot communications, voice (VHF) and datalink (DL). In addition the "DL" column was divided into two sections: the «ch.sect.» section (the communications needed to manage a sector change, namely the pilot's first contact, the controller's last contact and the consequent answers to these communications) and the «enroute» section (that refers to all the other tasks that have to be managed during the en-route phase). Each of these sections was split in turn into two subsections, clearance (C) and information (I), to distinguish the kind of communication that is referred.

In the first option (see the first table in Figure 5), we suppose that the executive controller has to support both vocal and datalink communications with pilots then the whole row associated to him/her is shaded, whereas in the second and the third tables the datalink communications are handled by both the controllers, with different arrangements.

We decided to discard the second option because was really a small variation of the first one as the changes are rather minimal as well as their effects on the way to interact with the application.

7. Criteria for evaluation

Evaluation methods applicable at a late design step are generally more expensive than methods that can be used at earlier stages (evaluation costs increase as the design process progresses). Designers can reduce the amount of user testing by discovering problem early in the design process, thus reducing the number of design iterations [John96]. Concerning the media allocation issue, discovering usability and safety problems as soon as possible in the design process involves checking the design against several criteria that can be decisive to evaluate the strength and weakness of each choice.

Currently, there is a lack of general agreement about the aspects that should be taken into account in allocating media and guidelines that should evaluate this allocation process. Traditional approaches consider only the nature of information (transience, urgency), the technical characteristics of the media used to (its constraints and limitations) and, of course the overall performance of the system.

However, from our point of view, a more complete analysis can not leave out of consideration other aspects that put the human in a more central role, especially in safety-critical systems where it is really crucial to prevent incorrect user interactions, whose effects can threaten human life. These incorrect behaviours are not necessarily totally wrong actions but also right actions performed at the wrong time: especially in the ATC system, controllers are very sensitive concerning the "right time" to perform actions, as a too late action on traffic might transform a fairly difficult problem into a very difficult one. To make sure that controllers do not miss the right time for delivering a control instruction, they have to monitor very frequently the exact position of the aircraft, until it enters the right place, and they have to remember it continually, switching from time to time on the different situations. This makes the memory management a very demanding task for the controller and obviously this mechanism is very costly.

So it is clear that in this environment the emphasis is mainly on the human, rather than the machine and the system, making relevant interactive aspects such as the tasks performed by the human, his/her workload, the skills requested to perform their activities and the possible hazardous situations that can arise because of human incorrect action or behaviour.

Finally, the criteria that we found relevant for such system are:

1. *Fair allocation of work between the controllers*: although this parameter is difficult to estimate from a quantitative point of view, we tried not to have completely unbalanced allocation of the controllers' activities between the two operators.

2. *The possible hazardous situations*, being this aspect really critical in this safety-critical system. A useful aid to analyse in a more structured way all the possible hazardous situations caused by "deviations from design intent" in the interactions between system components, is provided by the application of a HAZOP-like method [McDermid94] [Burns93] . An example of application of this technique is shown in the next sections.
3. *Conflicts on shared objects between controllers*: the maximum sharing possible between the controllers would be desiderable in order to minimise the possible inconsistencies between the views of the two controllers and to maximise their concurrent activities. It is evident that higher the sharing, higher the accuracy with which the interface should be designed to avoid that concurrent accesses not well designed might create conflict situations.
4. *The time of task performance:* improvements to the overall system's performance derive mainly from improvements to controllers' tasks performance, thus it is really important to identify bottlenecks and defeats in controllers' activity and make up for them as much as possible in order to increase the global efficiency.

8. Evaluation

Now we start to analyse each option to evaluate their pros and cons according to the criteria above identified.

8.1 Case 1: Both communication media allocated to the executive

In the Table 2 we divided the tasks with respect to the human operator who performs them under the first option: thus, for example, in the executive's column we list all the tasks that the executive controller is expected to perform when all communication media are allocated to him/her.

Strategic	***Executive***
Monitor Radar	**Monitor Radar**
Negotiate transfer parameters	
Annotate Strips	**Annotate Strips**
Update Ground System	**Update Ground System**
Detect Problem	**Detect Problem**
	Solve Problem
	Send Clearance to Pilot
	Send Information to Pilot
	Handle First Contact
	Handle Last Contact
Inform Controller of Problem	

Table 2: Task Allocation with Communication Media Allocated to the Executive

From the Table 2 you can see that there are four tasks (highlighted in bold) which appear in both executive and strategic columns, thus it seems to be some "redundancy" in the system. Actually, two of them (namely the *Monitor Radar* task and the *Detect Problem* task) are really performed in a parallel way because both controllers are always in charge of monitoring the traffic flow and eventually detect problems (it is reasonable because of the high safety criticality level of these tasks). The *Update Ground System* is normally performed by the strategic because the executive is generally busy (of course, we are referring to updates concerning non-datalink equipped a/c, otherwise those are performed in an automatic way). In the case of the *Annotate Strips* task for each strip generated by the system, the strategic is the first controller that analyses it (when the correspondent flight is not entered yet in his/her sector, and s/he has to negotiate the flight transfer parameters with other strategic controllers and annotate consequently the strip). Once s/he has modified the strip, the executive controller starts to use it when s/he receives the first contact from the pilot (s/he annotates it to keep track of the flight evolution within the sector). When the flight associated to the strip is still in the sector, the strategic controller could have to annotate again the strip, because of a negotiation with the strategic controller of the sector which the flight is going to enter into (this is a situation of "strip sharing" between the strategic and the executive controller). Now we try to estimate this first option according to the criteria above defined.

8.1.1 Hazardous situation

In the below table, we show an example of HAZOP study analysing the impact of the possible deviations in the executive's task of communicating to a pilot (using datalink messages and under the assumptions of the first case) the new frequency that he has to use for the VHF communications with executive controller of the next sector. The procedure for identifying such deviations (excursions of a value outside its normal operating envelope) from the design intent is facilitated by the application of a number of *guidewords* which refer a specific type of deviation. The results of the analysis will be recorded in a tabular form containing the following elements: *task*, indicating the activity which is being analysed; *guideword*, indicating the type of deviation which is considered; *deviation*, indicating the specific problem detected or how the guideword is interpreted in the context of the task; *cause*, indicating hypotheses about the ways in which how the problem might arise; *consequence*, indicating the possible effects of the deviation for the system as a whole; *protection*, indicating how (within the current design) it is possible to protect from the deviation; *recommendations*, indications for an improved design in order to prevent the deviation.

Just to give an example of how a HAZOP analysis works, in the Table 3 we consider the "*Other Than*" guideword applied to *Handle Last Contact* task, indicating that the controller's last contact sent to a pilot results to be different from that intended: different because either wrong flight has been selected, or a wrong frequency has been sent, or the pilot has mis-read the correct message. Of course, for the same communication other guidewords can be examined (e.g. *None*: no communication occurs; *Early*: the communication occurs too early, *Late*: the communication occurs after the right time, and so on).

Task: Handle Last Contact			**Guideword: Other Than**	
Deviation	**Cause**	**Consequence**	**Protection**	**Recommendations**
1. Executive allocates wrong frequency in communication	Executive holds faulty belief about correct frequency (e.g., a mistake about which sector a/c will be entering, or about what the correct frequency for that sector is) Intention problem	(i) Valid frequency : the pilot contacts the wrong controller when he performs a R/T communication (ii)Invalid frequency: the pilot tries to tune in to a non-existent frequency when he performs a R/T communication	Valid (but wrong) frequency and invalid frequency are detected by the executive controller of the new sector checking the first contact's message from the pilot	Ensure the user interface provides controllers with representations of associations between sectors and frequencies immediate to be interpreted Ensure that the strategic controller can have an adequate feedback of the actions' effects performed by the executive in order to be aware of them and able to check
	Executive knows frequency, but makes a slip Action problem			Design user interface which prevents from slips
2. Executive uses incorrect callsign	... as a result of a mistake … Intention problem	The new frequency is given to the wrong flight	If the pilot is still far from the sector boundary he could look for a double-check from the executive	The application should warn that a flight far from the sector boundary has been selected Ensure a feedback of the actions' effects on the strategic controller's user interface
	... or a slip. Action problem			Design user interface which prevents from slips
3. Wrong frequency received	Pilot mis-reads frequency , because of inattention, poor video quality, or being biased by a preconception. Perception problem Or Understanding problem	(i)Valid frequency: the pilot contacts the wrong controller when he performs a R/T communication (ii)Invalid frequency: the pilot tries to tune in to a non-existent frequency when he performs a R/T communication	Valid (but wrong) frequency and invalid frequency are detected by the executive controller of the new sector checking the first contact's message from the pilot	The application should detect automatically that a wrong frequency is used and inform the old controller in order to send again the right frequency

Table 3: An Example of table derived from a HAZOP analysis

Analysing the Table 3, one possible hazardous situation that could appear using datalink messages to communicate the new frequency to a pilot is when the controller makes a mistake in identifying the a/c callsign on his/her interface (case 2.) and then s/he sends the command to a wrong flight. In addition, even if the controller is good at identifying and pointing with mouse the right a/c, s/he has to select the right command and the appropriate parameters: another possible deviation is not to select the right frequency value (case 1.). In order to avoid (reduce at least) possible errors in performing these tasks the user interface should be designed in such a way to bound properly the range of possible values, to ensure that it never stays in an "undefined" mode —for example the controller has selected the command and the parameters but s/he actually forgets to send the instruction. The user interface should take care either of avoiding these situations at all (for example by means of modal windows) or warning properly the controller about them. The last possible hazardous situation examined (case 3.) is on the pilot's side: a correct order is displayed on his/her interface, but probably s/he was not good at correctly reading it, so s/he is going to use a wrong frequency to communicate via radio with controller.

For the purposes of our analysis it is meaningful to analyse the different role that each controller plays under these assumptions: the strategic controller's role is mainly devoted to support the executive's work, checking and monitoring his/her activity, therefore the need of providing to the strategic a proper feedback of executive's actions as far as it concerns the datalink communications. This feedback —differently from the VHF communications that are easily heard by the strategic because s/he stays very close to the executive— has to explicitly be provided on the strategic controller's user interface and carefully be designed. On the other hand, the executive has to handle different media and tools to manage the traffic, thus increasing the possibility of incorrect interactions using them: therefore the likelihood that hazardous situations occur is **high**.

8.1.2 Possible conflicts derived from shared options

Under this assumption the controllers have to manage really different tasks and actually they have to share only the strips and only if the strategic controller wants to update a flight parameter decided after a negotiation with other strategic controllers while the associated flight is still in the sector (and then under the control of the executive who could have to update other parameters in the same strip depending on his/her decisions). The level of sharing is **low**.

8.1.3 Fair allocation of work

It is clear that the executive controller has a bigger workload compared to the strategic controller's, because of many factors:

a) *Number of tasks*: the executive has to support all the communications with pilots and, at the same time, s/he has to think of the best solution to the problems as they unpredictably appear. The strategic controller has to negotiate with other strategic controllers and s/he has to update the ground system for all the non-datalink equipped planes in the sector (this task is further reduced if there are many datalink-equipped planes in the sector, for which the update of the system is performed in an automatic way).

b) In addition, the executive's work is more stressful, because of *time constraints* more pressing, as the task of problem resolution and the task of communicating with pilots have to be performed as soon as possible, whereas the strategic does not have to update the system each time s/he receives a positive answer from a pilot, but it is enough that s/he updates the system until ten minutes before the flight crosses the sector boundaries, so that an updated strip is printed in the other sector, then s/he can "organise" his/her work more freely than the executive colleague.

c) The *type of skill requested*, because the task of quickly resolving an unforeseeable conflict 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 allow us to state that there is an **unfair allocation of work** between the executive and the strategic controller.

8.1.4 Time of task performance

Consider which are the actions needed to perform a VHF communication from a controller to a pilot: first of all, because his/her communication is heard by all the pilots currently in the sector, s/he has to identify precisely the flight with which s/he wants to communicate, so s/he first reads the a/c identification and then s/he sends to the pilot the proper order, clearance or information (following the aeronautical phraseology). The pilot involved has to read-back the instruction to declare that s/he is going to execute the order and then s/he starts to do it.

Consider now a communication performed by the controller using datalink technology. The datalink technology allows controllers to have point-to-point communications, so first of all the controller has to identify on his/her interface the right a/c representation. Once s/he has identified the right a/c, s/he has to point it with the mouse and then select the menu that allows him/her to use the datalink capabilities. Then s/he can select the right command and (if requested) the appropriate parameters and s/he can send the instruction. The pilot's system sends to the controller's system the acknowledgement that the message is ready to be displayed on the pilot's interface, and then the pilot replies with a "*Wilco"* message to indicate that s/he is able to perform the order.

Keeping in mind that every datalink communication is always delayed because of normal transmission delays, for each controller-pilot session there are two delays to add (one for sending a request and another one for the answer to it). In terms of controller-pilot communications, the VHF technology allows to gain shorter performance times being definitely more immediate.

However, being the executive controller to support all the communications with pilots, especially in high traffic situations the global time needed to support them could make worse just because of the executive's bottleneck who can fulfil only one pilot request at a time (**low performance with high traffic**).

8.2 Case 2: the flight-state dependent datalink allocation

In this situation, all datalink-equipped a/c have to interact with both controllers, depending on the different flight phases: with strategic controller when the flight changes the sector, otherwise with the executive. In the below table we summarise the tasks' arrangement:

Strategic	***Executive***
Monitor Radar	**Monitor Radar**
Negotiate transfer parameters	
Annotate Strips	**Annotate Strips**
Update Ground System	**Update Ground System**
Detect Problem	**Detect Problem**
	Solve Problem
	Send Clearance to Pilot
	Send Information to Pilot
Handle First Contact	
Handle Last Contact	
Inform Controller of Problem	

Table 4: Task allocation in the Flight-State dependent datalink allocation

8.2.1 Hazardous situation

In this option the strategic controller can send order to pilots, so it is possible his/her orders can conflict to executive's, leading to possible hazardous situations.

For example, the flight level requested for an a/c by the strategic controller could be different from that expected by the executive controller (and vice versa), so a dangerous situation may arise when the flight's control passes from one controller to the other one.

As far as it concerns the HAZOP analysis on the task examined in the previous section (send the new frequency to a pilot approaching to change the sector) the issues listed in the HAZOP Table 3 continue to be valid with the exception of exchanging the executive's role with the strategic's: in fact, in this case the strategic is in charge of sending datalink messages to pilots approaching to change sector (*Handle First Contact* and *Handle Last Contact* tasks in Table 4).

It is worth noting that under this option the roles of the two controllers are more balanced (the strategic controller is not only a help for the executive controller), but s/he plays an active role in the sector traffic management, looking after a part of datalink communications. Thus, the coordination and mutual awareness between the two controllers needs to be more augmented with respect to the previous option (because for example the strategic has to exactly know at what time the handover of a flight has to be performed with the executive and so does the executive), although the monitoring activity of the strategic controller towards the executive controller’s activity could get more effective.

Therefore, under this option **controllers' mutual awareness and checking are the most critical conditions for obtaining a low number of hazardous situations**.

8.2.2 Possible conflicts derived from shared objects

Under this option the aspect of "shared objects" is a bit more critical. Note for example that it can happen that when both controllers try to perform an action on the same a/c (it is possible because both controllers have to handle datalink-equipped a/c in different moments, then they have to access to the appropriate tools), thus it is relevant to take care of the incorrect behaviours that could occur if the actions are not well serialised. A good user interface highlighting when it is time to pass the control from the executive controller to the strategic and vice versa, (e.g. avoiding that the strategic decides to send a "last contact" instruction to a pilot whereas at the same time the executive controller wants to have other communications with the same a/c) should limit the number of conflicts that is **potentially high**.

8.2.3 Fair allocation of work

The workload between controllers is a bit more distributed, either in terms of number of tasks (a bit more equally distributed between the controllers), as in terms in type of task (skill requested, time pressure constraints): in fact, while 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, as all flights going into the sector or leaving the sector have to communicate with the strategic controller. Under high traffic situations it can happen that some flights perform the first contact but the strategic is already occupied in handling other first/last contact, or in communications with other strategic controllers, so in this case even the strategic can feel heavier his/her activity. The allocation of work seems to be **fair**.

8.2.4 Time of task performance

In this case the overall system performance often depending on the controllers' skills in anticipating conflicts in the sector can benefit from an executive controller a bit more focussed on the flow in the sector because has been freed by several routine's communications such first/last contact often are, s/he spends more time monitoring situation, thus s/he can be more ready to reply to pilots in order to prevent/solve conflicts.

Of course, all these advantages can be exploited only if other co-ordination problems between the strategic controller and the executive controller are not added because of a bad-designed user interface that does not take into account the need of a mutual knowledge and awareness between controllers. Therefore, under this option**, if conflicts are resolved, the best performance is reached**.

9. Conclusions and Future work

In this report we have discussed how different media can affect —in terms of safety and usability, two concepts related to interactive safety critical applications— the work of human operators in this type of applications. Besides, we have shown how the criteria proposed can be applied to a case study in the Air Traffic Control field.

The proposed approach starts from the assertion that the interface design is a complex process, which has to consider several different aspects, especially when intended for a safety-critical application as in the air traffic control example considered in the report (although the same issues can be applied to other areas). In this case the high cooperation requested between different users claims that possible changes in users' way of working have to be carefully analysed before introducing them in the system, because the effects of erroneous users' interactions can be easily propagated within such system with critical consequences.

Therefore, our work represents an attempt to structure all various aspects into a more organic approach which starts identifying the possible options in allocating media and tasks, analysing the resulting changes of environment, artefacts, and interactions between the different human agents involved and between the human and the system. The next step is to evaluate the options according to different criteria that we found relevant in the assumed environment: although this qualitative evaluation can not be easily carried out, it can provide useful guidelines to assess pros and cons of each option.

According to the analysis developed, we plan to modify a new system prototype for supporting en-route air traffic control with data link support that should better satisfy the safety and usability criteria than the current system. Further work on formal reasoning about safety and usability properties of this multi-users environment, with the support of model-checking techniques, is also foreseen.

10. References

[Burns93] Burns, D.J. and Pitblado, R.M. *A Modified HAZOP Methodology For Safety Critical System Assessment*. Directions in Proc. of the Safety-Critical Systems Symposium, Bristol, 1993, Springer-Verlag

[Chatty96] Chatty, S., Lecoanet, P., *Pen Computing for Air Traffic Control*, in Proceedings of CHI'96, April 13-18, 1996 Vancouver, British Columbia, Canada

[Diaper89] Diaper, D., *Task Analysis for Human-Computer Interaction*, Chichester: Ellis Horwood, 1989

[EUROCONTROL] *Operational Requirements for Air Traffic Management (ATM) Air/Ground Communications Services, Appendix A: Glossary and Abbreviations*. Available from http://www.eurocontrol.be/projects/eatchip/odiac/document/apa_10.doc

[Hollnagel93] Human Reliability Analysis – Context and Control, Academic Press, 1993.

[John96] John, B.E., Kieras, D.E., *Using GOMS for User Interface Design and Evaluation: Which Technique?*, ACM Transaction on Computer-Human Interaction, Vol. 3, No. 4, December 1996, 287-319

[Leathley97] Leathley, B.A., *HAZOP Approach to Allocation of Function in Safety Critical Systems*, in Proc. Of the 1st International Conference on Allocation of Functions

[Leveson95] Leveson, N.G., *System Safety and Computers*, Addison-Wesley Publishing Company, 1995.

[Mackay98] Mackay, W.E., Fayard, A.L., Frobert, L., Médini, L., *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

[McDermid94] McDermid, J.A. and Pumfrey, D.J. *A Development of Hazard Analysis to aid Software Design*. Proc. COMPASS'94, *IEEE Press*. ftp://ftp.cs.york.ac.uk/ hise_reports/safety/develop.ps.Z

[Paternò98a] Paternò, F. *The contribution of a formal approach to task modelling: the ConcurTaskTrees example*, Proceedings of Task Analysis 1998 - State of the Art in Europe, Schaerding, June 1998.

[Paternò98b] Paternò, F., Santoro, C., Tahmassebi, S. *Formal Models for Cooperative Tasks: Concepts and an Application for En-Route Air Traffic Control*. In *Proc. DSV-IS '98*, Abingdon, U.K., June 1998.

[Reason90] Reason, J., *Human Error*, Cambridge University Press, 1990.