The Impact of Different Media on Safety and Usability of Interactive ATC Applications

Fabio Paternò[1], Carmen Santoro[1], and Sophie Tahmassebi [2]

[1] CNUCE-C.N.R., Via S. Maria 36, 56126, Pisa, Italy
{F.Paterno, C.Santoro}@cnuce.cnr.it
[2] Centre d'Etudes de la Navigation Aérienne, Avenue Édouard Belin 7,
31055 Toulouse Cedex, France
tahmasse@cenatoulouse.dgac.fr

Abstract. This paper identifies and discusses a set of criteria relevant to assess the impact of using different media in the design of user interfaces for safety-critical systems. An evaluation of different options concerning the allocation of such media during the design of an application in the Air Traffic Control domain is shown to illustrate and clarify our approach. Particular attention is paid on how different choices in allocating tasks among air traffic controllers affect usability and safety of operators' interactions.

1 Introduction

In spite of increasing development and availability of new communication technologies, little work has been dedicated to analyse more deeply the concepts which drive the choice and use of interaction media in the design of user interfaces for safety-critical systems. To this end we believe that, instead of completely relying on late empirical testing, it can be useful to perform an evaluation of different media and task allocation choices [1] according to appropriate criteria, to discard meaningless possibilities and to focus on problematic parts of the design.

In current applications the co-existence of more than one technology is getting more and more common, so there is a need to deeply understand nature and constraints of each medium and its appropriateness with respect to the user tasks and environments to evaluate which technology provides the best support.

The issue of allocating media is getting particularly demanding in current safety-critical systems where many studies have shown that accidents have been often caused by human error [2]. In such systems two contrasting trends seem to exist at the same time: on the one hand the 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 because its impact (especially in terms of safety and usability) is not always known and in the worst case it may threaten human life. An example of the latter issue is given by applications in a highly cooperative system [3] as the Air Traffic Control (ATC) area, where many problems have still to be solved. Number and duration of delays show that ATC systems are not always able to cope with passengers' demand; the growing air traffic increases the possibility of accidents; several incidents occurred because of the undesired effects of

M. Felici, K. Kanoun, A. Pasquini (Eds.): SAFECOMP'99, LNCS 1698, pp. 89-102, 1999

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 [4] or to provide them with an augmented reality environment [5] 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, the increases in air traffic have begun to highlight the potential bottleneck of radio channels which can become saturated during high levels of traffic, thus several solutions are going to be envisaged. Datalink (a technology allowing electronic exchanges of data [6]) is a solution that seems to overcome the main limitations of traditional communication systems. However, adding this technology in the system impels to understand its impact on User Interface (UI) design issues.

In the next sections, we introduce our approach giving at first a general overview of ATC system in terms of tasks [7] [8] that controllers have to support, with special care to media and tools provided by both VHF and datalink technologies. Then we select two design options on how to allocate interaction media to different users, defining the criteria we found relevant to estimate advantages and disadvantages of each considered option. Finally an assessment of the two choices is given according to the selected criteria. The discussion is focused on a case study in the ATC domain, however, the method proposed can be applied to other interactive safety critical systems where the interactive part has to be redesigned to support new requirements.

2 The Current ATC System Based on Vocal Communication

In this section we roughly describe the controllers' tasks during the en-route phase in the current French ATC system (other countries may present slight differences).

The civil airspace is divided into various control centres and, within each centre there are basically two controllers: the *executive* controller, who is due to maintain appropriate separation between aircraft in the sector, and to hold communications with pilots; and the *strategic* controller, who is in charge of co-ordinating transfer of aircraft from sector to sector with other strategic colleagues.

In addition, both controllers perform "in background" surveillance tasks. Thus, three kinds of communications can be distinguished (numbers refer to those in Fig. 1):

1. Between strategic and executive controllers of the same sector, (for example vocal and "elbow" communications to attract attention);
2. Between strategic controllers of two neighbouring sectors involved in a flight sector exchange (phone communications);
3. Between the executive controller of each sector and pilots currently in the sector (radio communications);

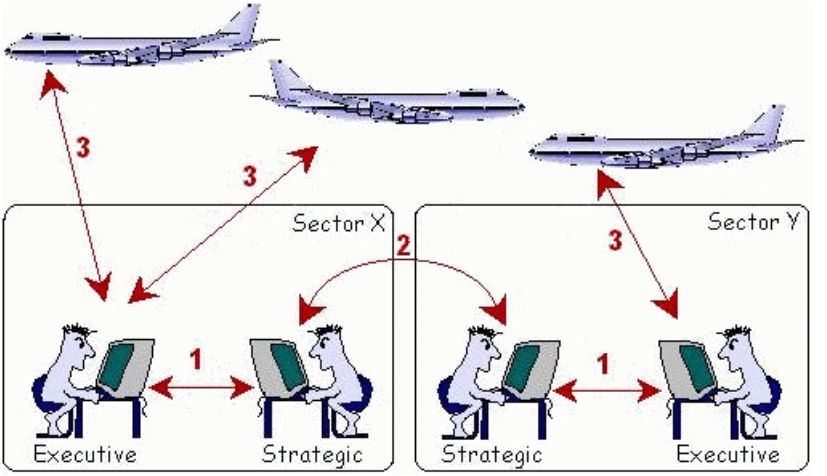

Fig. 1. The communications occurring between en-route controllers

Today, most of air/ground communications are conducted by voice over Very High Frequency (VHF) radio channels. At any time *many* pilots are in competition for speaking with *one* controller as only one speaker (controller or pilot) can broadcast over the radio, so the resulting "sharing" especially penalises pilots who sometimes have to wait because the frequency is kept busy by another communication.

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

Thus, the main advantage of the current R/T (Radio/Telephony) is that it allows rapid communications between pilots and controller being voice the most natural medium of human communication. Besides, an R/T message contains not only the message itself, but also some subjective information (stress, emotion, anger, humour, courtesy) which are relevant to pilots and controllers. However, the process of communicating by voice is prone to human error, because its transient nature might easily introduce mis-understandings and confusions. In addition communications exchanged through radio channels are generally concise (following the standard aeronautical phraseology) in order not to long occupy the frequency so they can not be considered really "natural" communications. Thus, the main limitations suffered by the current R/T channels can be either:

- *Technical,* channel congestion, limited range, simultaneous transmissions on the same frequency, amplitude modulation susceptible to weather interference or
- *Human,* mis-understandings due either to the poor quality of the communication, or transient nature of voice, difficulties to understand a non native language or accent, workload, confusion due to the party line effect.

In order to overcome most limitations of the current system, different alternatives have been proposed. One of the most promising is the adoption of datalink as additional medium of communication between controller and pilot, and we address the UI-related issues in the following sections.

3 Towards the New System

The current system seems to have reached limits of its capability and to be really short of efficient solutions, so increasing interest has been devoting to the possibility that conventional radio communications can be *augmented* with a new communication media called datalink, which electronically transfers digital messages to computer on the ground and in the aircraft. Initial considerations on human factors have already suggested that it could increase controllers' efficiency in the management of traffic and reduce potential communication errors, anyway special care has to be paid on its impact on the system, particularly in terms of variations to how controllers perform their tasks.

With regard to the latter point, three main differences are identified moving from the current system to an "augmented" one where both media are available:

1. *Change of task allocation between human and machine*: for instance, in datalink environment some tasks become automatically performed (e.g. the update of the ground system);
2. *Change of task allocation between human operators:* for example strategic-pilots datalink communications can occur as well;
3. *Change of artefacts manipulated by interaction tasks*: electronic flight strips are an example of "new" artefacts that can affect how tasks are performed.

More generally, these changes should carefully be analysed whenever a new application, supporting different interaction techniques and media, is designed. Furthermore, a number of factors related to how 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 [9]. 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.

4 Supported Tasks

In this section we define more precisely activities that have to be performed by controllers in en-route ATC applications, using a task “granularity" refined enough to reason about pros and cons of each arrangement. In the following table the identified tasks (together with domain objects manipulated by) are listed.

Table 1. The Controllers' tasks

Task	Explanation	Domain objects
Monitoring Radar	Controllers have to check continuously the information provided by the radar	Flight traffic
Negotiation about Transfer Parameters	The strategic controllers have to negotiate about the best transfer flight parameters of flights which are going to change sector	Flight level
Annotate Strips	The controllers annotate flight strips to keep the "history" of traffic evolutions in the sector	Flight level, Route, Speed, Destination
Update Ground System	Both controllers —but generally only the strategic—update the ground-based computer system to reflect changes to flight data.	Flight level, Route, Speed, Destination
Detect Problem	The controller *identifies* a possible conflict in the current air traffic situation	Routes, flight level, lack of separation
Solve Problem	The cognitive process of *finding a solution* to solve a conflict or to give more regularity to the traffic flow	Current and foreseen air traffic
Send Clearance to Pilot	The task of sending instructions to aircraft	Flight plan, clearance
Send Information to Pilot	The task of sending information to aircraft	Weather information, delay reports
Handle First Contact	The task of replying to the first communication from a pilot who has just entered in the sector	Flight identifier, Frequency
Handle Last Contact	The task of sending the frequency to communicate with the controller of the next sector	Frequency
Inform Other Controller of Problem	One controller informs the other that something has been detected or something has to be done	Conflicts, conflicts’ solutions

Note that in the table above we do not specify *which controller* actually performs a specific task, as the analysis of how to allocate tasks among the controllers (and the impact on the user interface design) is putting off until next sections.

5 Changes in Task Performance with the Introduction of DataLink

Fig. 2 shows 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 the 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.

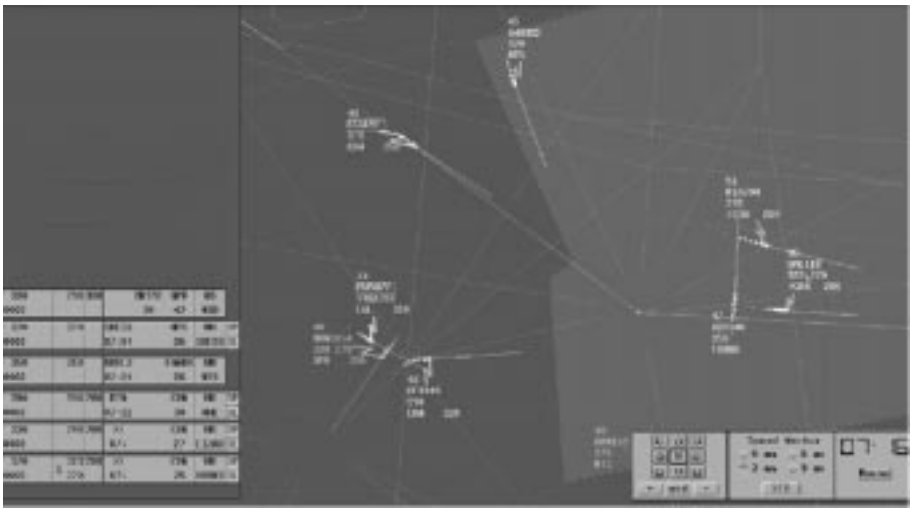

Fig. 2. An Example of Controller's User Interface in a Datalink Environment

In the current system, when the controller receives the affirmative answer from pilot s/he looks for the correspondent callsign on the radar screen, finds the associated strip in the rack, annotates it and updates the ground system. This activity is quite demanding as the information is "spread" over different supports (radar, paper flight strips), needing a high eye/hand co-ordination ability from the controller to blend them. The latter issue is an important safety concern, being assured that every information source which causes diversion of controller's attention focus is highly undesirable and should be avoided as much as possible.

In the new environment, first of all the controller is alleviated from keeping trace of traffic evolutions in the ground system as it is automatically performed. In addition, even if s/he does not have to annotate but just read the strip (to check conformance with a/c current position on the radar), now both pieces of information are on the screen, reducing necessary eyes' movements and resulting controller's fatigue.

6 The Analysed Options for Media and Task Allocation

In the following sections, we consider different options of allocating media and tasks 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 potential conflicts in accessing to shared objects and number of possible hazardous situations.

Before going forward into the proper analysis, it is better to define the hypothesis that we are going to keep unchanged for both options. First of all, the co-existence of different information sources of audio type (telephone, radio), peculiar constraints related to its own transient nature, and the high level of safety-criticality connected to communications exchanged through them, claims the need of allocating in a "dedicated" way only one audio medium to each controller (telephone to strategic, radio to executive). In this way all the assumptions where the strategic controller has to communicate with pilots on the frequency as well are discarded: in fact, if the strategic is already busy on the telephone with another colleague in order to negotiate some sector's change parameters, 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. In addition, as in every safety critical system the decision-making process is a decisive point we decided that both controllers have to monitor the traffic situation, but only the executive is in charge of deciding what the best solution is to solve a problem and act upon consequently. Initially, we started considering the three options graphically summarised in Fig. 3:

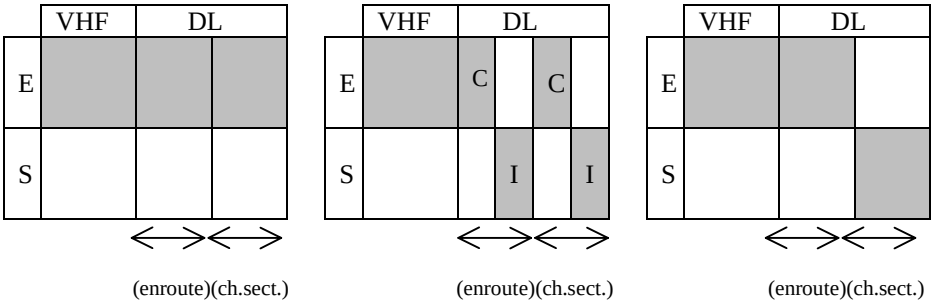

Fig. 3. A tabular overview of the three different options

Each table in Fig. 3 is split into two rows —one for each controller, executive (E) and strategic (S) and two columns —one of each media used for controller-pilot communications, voice (VHF) and datalink (DL). In addition the "DL" column is divided in two sections: the "ch.sect." section (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 (all the other tasks that have to be carried out during the en-route phase). In one case the DL section is split in turn into two subsections, clearance (C) and information (I), to distinguish the kind of messages that can be transmitted.

As you can see from the first table in Fig. 3, under the first option we suppose the executive controller handling 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 datalink communications are handled by both the controllers, with different arrangements. For the purposes of our analysis, we decided to discard the second option because it is 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 Integrated Evaluation of Usability and Safety

Currently, there is a lack of general agreement about the aspects that should be taken into account in allocating media, as well as guidelines that should evaluate this allocation process. Traditional approaches consider only the nature of information (e.g. urgency), the technical characteristics of the used media (constraints and limitations) and, of course the overall performance of the system. However, especially in safety-critical systems a more complete analysis has to focus a little more on the role of the human in order to prevent incorrect user interactions that can threaten human life. These incorrect behaviours are not necessarily totally wrong actions but also right actions performed at the wrong time: particularly in the ATC system, controllers are very sensitive concerning the "right time" to perform actions, as a too late action might transform a fairly difficult problem into a very difficult one. In order not to miss the right time for delivering an instruction, controllers monitor exact positions of aircraft, continuously refreshing them until the right moment arrives, switching from time to time on different situations in traffic, and this activity is a quite demanding task for them.

As in this environment the emphasis is mainly on the human, (rather than the machine and the system), interactive aspects such as tasks performed by the human, his/her workload, skills requested and possible hazardous situations that can arise because of incorrect human action or behaviour become key points. Finally, we selected the following criteria:

1. *Fair allocation of work between operators*: although this parameter is difficult to estimate from a quantitative point of view, we tried not to have completely unbalanced allocation of controllers' activities between the two operators.
2. *Possible hazardous situations*, as this aspect is really crucial in every safety-critical system. We use a HAZOP-like method [10][11] to analyse possible hazardous situations caused by "deviations from design intent" in the interactions between system components.
3. *Conflicts on shared objects between operators*: the maximum sharing between the controllers is desirable to minimise inconsistencies between the views of the two controllers and to maximise their concurrent activities. Higher the sharing, higher the accuracy with which the interface should be designed to avoid that (not well designed) concurrent accesses might cause conflict situations.
4. *Time of task performance:* improvements to the overall system's performance derive mainly from improvements to controllers' tasks performance, thus it is essential to identify bottlenecks and defeats in controllers' activity making up for them as much as possible.

It is worthwhile to stress that the aim of identifying such criteria 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.

8 Evaluation

This section is devoted to evaluate pros and cons of each option according to the aforementioned criteria.

8.1 Case 1: Both Communication Media Allocated to the Executive

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

Table 2. Task allocation with communication media allocated to the executive

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	

In Table 2 four tasks (highlighted in bold) appear in both executive and strategic columns, seeming that some "redundancy" occurs 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 possibly detect problems (it is reasonable because of the high level of safety criticality of such tasks). The *Update Ground System* is normally performed by the strategic because the executive is generally too busy (of course, we refer to updates concerning non-datalink equipped a/c, otherwise they are automatically performed).

As far as it concerns the *Annotate Strips* task for each strip generated by the system, once the strategic possibly modifies the strip, s/he passes it to the executive controller who starts to use it when s/he receives the first contact from the pilot (annotating 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 the strip again, because of a negotiation with the strategic controller of the sector which the flight is going to enter (this is a situation of "strip sharing" between the strategic and the executive controller).

8.1.1 Hazardous Situation

In the method that we have developed [12] based on the HAZOP approach, the procedure for identifying “deviations” (excursions of a value outside its normal operating envelope) from the design intent is performed by applying a number of *guidewords* referring to a specific type of deviation. The results of the analysis is recorded in a tabular form with the following elements: *task* the activity which is being analysed), *guideword* (the type of considered deviation), *deviation* (the specific detected problem or how the guideword is interpreted in the context of the task), *cause* (hypotheses on how the problem might arise), *consequence* (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* (suggestions for an improved design).

Just to give an example of how it works, in this section we examine possible deviations in the executive’s task of communicating the frequency of next controller to a pilot (using datalink messages and under the assumptions of the first option).We consider the "*Other Than*" guideword applied to *Handle Last Contact* task, indicating that the controller's last contact sent to a pilot (with a datalink message) 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 could be examined as well (e.g. *None*: no communication occurs; *Early*: the communication occurs too early, *Late*: the communication occurs after the right time, and so on).

With this type of analysis, one 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 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 to select a wrong frequency value. In order to avoid (reduce at least) possible errors performing these tasks the user interface should be designed in such a way to bound properly the range of possible values, to ensure that UI 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: τhe 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.

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 the strategic with a proper feedback of executive’s actions as far as it concerns the (silent) datalink communications. This feedback —differently from the VHF communications easily heard by the strategic as s/he stays very close to the executive— has to explicitly be provided on the strategic controller's user interface and carefully designed. On the other hand, the executive handles different media and tools to manage the traffic, increasing the possibility of incorrect interactions using them: thus, the likelihood that hazardous situations occur is **high**.

8.1.2 Possible Conflicts Derived from Shared Objects

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 while the associated flight is still in the sector (and then under the control of the executive). The level of sharing is **low**.

8.1.3 Fair Allocation of Work

The executive controller has a bigger workload compared to the strategic's, because of many factors:

1. *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 (for datalink-equipped planes the update of the system is performed in an automatic way).
2. In addition, the executive's work is more stressful, because of more pressing *time constraints* which are, as the task of resolving problems and communicating with pilots have to be performed as soon as possible. On the contrary, the strategic can "organise" his/her work more freely than the executive colleague can: for instance, s/he 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).
3. 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 considerations above allow us to state that under this option there is an **unfair allocation of work** between the executive and the strategic controller.

8.1.4 Time of Task Performance

Consider the actions needed to perform a VHF communication from a controller to a pilot: first of all, as his/her communication is heard by all the pilots currently in the sector, s/he has to identify the flight with which s/he wants to communicate, so s/he at 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 concerned pilot has to read-back the instruction to declare that s/he is going (or not) to execute the order, possibly starting to do it.

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, pointing it with the mouse and then selecting menu allowing him/her to use the datalink capabilities. Then s/he selects the right command and (if requested) the appropriate parameters and s/he sends 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, but only when the pilot looks at the message and replies with a "*Wilco"* message it means that s/he is able to perform the order.

Considering how a communication is supported by using datalink technology keep in mind that every datalink communication is always delayed because of normal transmission delays, so the VHF technology allows to gain shorter performance times being definitely more immediate. However, being the executive controller due to keep all the communications with pilots, especially in high traffic situations the global time needed to support them could get worse just because of the executive's bottleneck who can fulfil only one pilot's request at a time (**low performance with high traffic**).

8.2 Case 2: The Flight-State Dependent Data-Link Allocation

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

Table 3. Task allocation in the flight-state dependent datalink allocation

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	

8.2.1 Hazardous Situations

In this option the strategic controller can send order to pilots, so it is possible that 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, so a dangerous situation could arise when the flight's control passes from one controller to the other one.

Along the lines of our analysis of the task examined in the previous section (send the new frequency to a pilot) all the issues continue to be valid with the exception of exchanging the executive's role with the strategic's one, being now the latter controller in charge of sending datalink messages to pilots approaching to change sector (*Handle First Contact* and *Handle Last Contact* tasks in Table 3).

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 part of datalink communications. Thus, the coordination and mutual awareness between the two controllers has to be 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). In addition, the strategic

controller's activity of checking and supporting the executives work could get less effective. Therefore, under this option **controllers' mutual awareness and cross-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. It can happen that both controllers want to perform an action on the same a/c as they both can access to 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 the right 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 more distributed, either in terms of number of tasks, as in terms of type of task: 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 global system, as all flights going into the sector or leaving the sector have to communicate with him/her. Under high traffic situations it could happen that some flights perform the first contact but the strategic could be already occupied in other matters, so in this case 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's performance (often depending on the controllers' skills in anticipating conflicts) can benefit from an executive controller a bit more focussed on the flow in the sector because has been freed from several routine's communications (such first/last contact often are), so s/he can spend more time monitoring system, allowing him/her to 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 badly-designed user interface that does not take into account the need of 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 paper we discuss how different media can affect —in terms of safety and usability— the work of human operators in this type of applications. Besides, we show how the proposed criteria can be applied in the Air Traffic Control field.

The proposed approach starts from the assertion that the user 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 paper (although the same issues can be applied to other areas). In this case the high co-operation requested between different users claims that possible changes in users' way of working have to be carefully analysed before introducing them in the system, as 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 involved human agents 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: in our experience this qualitative evaluation can provide useful guidelines to assess pros and cons of each option.

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

References

1. Leathley, B.A., HAZOP Approach to Allocation of Function in Safety Critical Systems, in Proc. Of the 1st International Conference on Allocation of Functions
2. Hollnagel E., Human Reliability Analysis, Academic Press, 1993
3. 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*, pp.71-86, Springer Verlag, Abingdon, U.K., June 1998.
4. Chatty, S., Lecoanet, P., Pen Computing for Air Traffic Control, in Proceedings of CHI'96, April 13-18, 1996 Vancouver, British Columbia, Canada
5. 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
6. 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
7. Diaper, D., Task Analysis for Human-Computer Interaction, Chichester: Ellis Horwood.
8. Paternò, F., A Model-based approach to the design and evaualuation of interactive application, Springer-Verlag, 1999.
9. Hopkin, V.D. Air Traffic Control. In E. L. Wiener and D. C. Nagel, Eds. *Human Factors in Aviation*. Academic Press, 1988. Pages 639-663.
10. 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
11. Burns, D.J. and Pitblado, R.M. A Modified HAZOP Methodology For Safety Critical System Assessment. F. Redmill and T. Anderson, Ed. Directions in Safety Critical Systems —Proceedings of the Safety-Critical Systems Symposium, 1993, Springer-Verlag
12. Fields, B., Paternò, F.,.Santoro, C, Analysing User Deviations in Interactive Safety-critical Applications, Proceedings DSV-IS'99, Springer Verlag, June'99, Braga, June'99