Evaluating safety and usability of ATM systems

Patrizia Marti, Paola Lanzi, Francesco Pucci

University of Siena
Department of Communication Science
Via dei Termini 6
I-53100 Siena, Italy

Deep Blue s.r.l.
Via Basento 52 D
00198 Rome, Italy
contact@dblue.it

[marti/lanzi/pucci@media.unisi.it]

Summary

In the paper we present methodologies and results of the validation carried out within the ITI project, an innovative user interface for the En-Route and Approach Controller Working Positions for the new Ciampino ACC. The project developed as a co-operation between the Italian National Administration ENAV S.p.A. (Ente Nazionale Assistenza al Volo) and the Eurocontrol Experimental Centre (Bretigny, France). The validation was based on the idea that critical situations are not due only to the availability of a certain information during the task execution but to the way in which different components in the process (software applications, organisational and cultural aspects, the physical layout, human operators) are balanced and interact to avoid or provoke breakdowns in the activity. The validation methodology we adopted allows to pro-actively assess which aspects of the system may impair or enhance safety after the introduction of new artefacts in the work setting.

Introduction

Evaluation of safety critical systems is a composite and articulated activity. Thanks to the availability of advanced technological tools, operators can demand routine tasks to the system and to concentrate on higher level mental operations. Therefore the activity of these operators evolves towards a flexible and context dependent process, where the knowledge that is daily produced is used to face new incoming situations. Indeed critical situations are not due only to the availability of a certain information in the execution of a procedure but to the way in which different components in the process (software applications, organisational and cultural aspects, the physical layout, human operators) are balanced and interact to avoid or provoke breakdowns in the activity. For this reason, the evaluation of complex safety critical systems requires an in depth analysis of the socio-technical context of the work, in order to assess the role that each component plays in the process. In this paper we present the experience we made evaluating an innovative user interface for the En-Route and Approach Controller Working Positions for the new Ciampino ACC. In the project we evaluated the following aspects: 1) *technical usability*, that is the perceptual and physical aspects of the human computer interface such as display formatting as well as anthropometric characteristics of the object being worked with; 2) *domain suitability*, that refers to the appropriateness of the content of information and display representations; 3) *user-acceptability*, that is the ease of use and suitability of the system for supporting cognitive task requirements; 4) *safety,* that is the systematic assessment of the components at stake in a process (software applications, organisational and cultural aspects, physical layout, human operators) and their interactions.

Usability aspects of the interface were evaluated applying user-centred methodologies, including heuristic evaluation and cognitive walkthrough. Heuristic evaluation covers issues related to the effectiveness and efficiency and can be used to guide a design decision or to critique a decision that has already been made.

Cognitive walkthrough covers issues related to the effectiveness of the system, highlighting problems of action executions and feedback interpretation with respect to a specific goal. These methodologies were mainly used to evaluate technical usability and domain suitability.

In the paper, we will concentrate on the other two dimensions of the validation, that is user acceptability and safety, highlighting features and potential of a novel approach named CRIA, Critical Interaction Analysis. The approach is inspired by the SHEL model (Edwards, 1972) as a general analysis framework and founds its theoretical basis on the Distributed Cognition theory (Hutchins, 1995). This theory has been developed within the Cognitive Science community, for studying the mediation role of external artefacts in human activity. It re-elaborates the long lasting thesis that human cognition is mediated by artefacts (rules, tools, representations), which are both internal and external to the mind. The ability of the human mind in processing symbolic information is strongly bounded by the difficulties in carrying out a complex reasoning without the aid of tools. The most powerful forms of thinking take place in interaction with tools, to overcome the limitations of the human mind. Thus, the knowledge for human cognitive activity is not located exclusively in the brain, but rather it is distributed among the brain and the cognitive artefacts employed to carry out the activity. Cognitive artefacts are those tools able to represent, store and process information.

The SHEL method has been specially developed to study the human factor in complex working environments. The particular version of the model we developed and refined, studies how the knowledge is distributed between humans and tools such as computer, rules, procedures, hardware, and how this knowledge is activated and used for a specific activity.

In the following, we will briefly describe the ITI project, a novel strip-less user interface for air traffic control. Afterwards we will present the details of the CRIA method, then will illustrate the way in which it was applied to ITI and finally we will discuss the benefits of the approach through the analysis of exemplar outcomes.

A socio-technical approach to system validation

The ITI Interface integrates basic features to support the controller's job. It is based on the EATCHIP Basic (i.e. SYSCO) and Advanced Functions (i.e. Safety Nets (SNET), Monitoring Aids (MONA)) specifically oriented to support some of the current controller's tasks. In validating ITI, we adopted an approach that systematically assesses the components at stake in a process (software applications, organisational and cultural aspects, physical layout, human operators) and their interactions. The assessment is based on the idea that a criticality is a wrong distribution of resources among the components. The method allows to pro-actively assess which aspects of the system may impair or enhance safety after the introduction of new artefacts in the work setting.

This method is inspired by the well known SHEL model, developed by Elwyn Edwards (1972). The model describes the behaviour of interactive systems with special regard to human factors issues. SHEL is an acronym for Software, Hardware, Environment, and Liveware. Software refers not just to computer software but to the rules, procedures, practices that define the way in which the different components of the system interact among themselves and with the external environment. Hardware is used to refer to any physical and non-human component of the system such as vehicles, tools, manuals, signs and so on. Liveware refers to any human components of the system in the relational and communicational aspects. Environment refers to the socio-cultural and organisational environment in which the different components of the process interact.

The SHEL model concentrates on the interfaces among people and all system components including other Liveware resources. The important point about SHEL is that it offers a system view where humans cannot be considered as isolated from the other system components. This view is consistent with recent theoretical work in cognitive psychology including Distributed Cognition (Hutchins, 1995) and Activity Theory (Nardi, 1996) but is grounded in simple concepts that can be understood by system designers without this theoretical background. In particular, Activity Theory assumes that human behaviour is not a set of disembodies cognitive acts (e.g. decision making, classification, remembering). Rather conscious activity takes place in everyday practice and it is inextricably embedded in a social matrix of which every person is an organic part. In this respect the unit of analysis to take into account is wide and articulated. It consists of a subject (individual or group), an object or motive, artefacts (or tools) and socio-cultural rules and norms. Hence human activity should be considered as a socially and culturally organised ensemble where artefacts play a critical role in mediating human activity.

Inspired by Distributed Cognition and Activity Theory, the CRIA method elaborates the SHEL model offering an operational approach to real time simulation and data analysis.

Complexity and real time simulations

In general terms, we can consider complexity as the condition that concerns the nature and consequences of interactions and non *linearities* of systems with many different agents. These systems are too rich and varied to understand in simple, mechanistic or linear ways. We can understand many parts of them but the larger and more intricately related phenomena can only be understood by principles and patterns and not predicted in detail. In human organisations, complexity plays an interesting role since it deals with dynamic and emergent patterns of behaviour, innovation and change, learning and adaptation.

ATC is an example of complex system: even if controllers' tasks are structured and well documented, the activity itself produces adaptations that make the tasks less stable (from personal strategies of task execution to serious violation of procedures). Tasks assigned to controllers can be performed in different ways, and the performance is very dependent on the specific configuration the "human-machine system" acquires (external environment, individual capabilities, confidence, procedures, history of the interaction, status of the system). More in detail in ATC can be considered a complex system since the cognitive properties of the whole can differ radically from the cognitive properties of the individuals who perform the activity.

One issue for the validation of new concepts and procedures in such complex systems is the simulation of the complexity of the context. Real time simulations represent a way to conduct relevant validation steps. In a real time simulation the ATC support tool is fed with real data previously stored (e.g. radar and other ATC data), but the context of interaction has to be recreated including, as much as possible, the richness of potential interactions between hardware, software and liveware components. In this respect, one of the desirable effect of real time simulation is the representation of how the system can be "naturally" subjected to the full variability of input data and situations that may occur in the real world. There is a need to reproduce a real environment in realistic scenarios.

A fundamental challenge is therefore how to represent the context of work practice (both current practice and envisioned future work practice) in order that the simulation may be linked to safety issues.

Our approach with CRIA is to consider not only the actions of "users", but also the contexts in which these actions take place and in which systems and devices are used. The literature on accident, incident, and near misses occurred in safety critical systems suggests that the usability of a control system and its ability to tolerate variances are strictly related to an adequate distribution of knowledge and the consequent correct interaction and co-operation between humans and tools. In order to simulate and analyse these interactions, it is necessary to adequately represent the context and to have a high level analysis capability. In this respect, task analysis is not adequate since it tends to focus on fine granularity on specific human tasks, and is weak in analysing high level communication tasks and co-operative activities.

The importance of the context of use for design and evaluation of interactive systems has been the subject of considerable research in both the HCI and the CSCW literature (Nardi 1996, Hutchins 1995).
Carroll (1995) was perhaps amongst the first to question the task as the appropriate unit of analysis. He introduced the concept of the task artefact cycle, arguing that the introduction of technology into a work setting changes the nature of the tasks in that setting. For Carroll this was followed by a turn to scenario-based design where scenarios as representations of work were intended to capture rich aspects of the context of work that could be not captured by task representations alone. Although the notion of the context is in theoretical terms recognised, there is little consensus on what the contents of such representations of context should be.

The CRIA method provides a clear theoretical contribution and an operational approach to how to represent the complexity of the context in real time simulations and how to analyse data with the objective of system validation and pro-active safety assessment.

The application of the CRIA method

The CRIA method develops in the following three phases:

1 - Preparation of test material

- Identification of the basic Software (S), Hardware (H), Liveware (L) components that may affect the use of the new system. This phase of the method, as the following one, is carried out through an accurate activity analysis based on observation in the real operational context and the analysis of official documents on operational procedures.
- From the activity analysis a set of safety issues related to the current activity are identified. The safety issues are macro validation objectives that have to be reflected in the scenarios during the real time simulations. They will be elaborated later in the process to fit the validation context (operational conditions, actors involved, implementation details). In ITI, a set of safety issues were identified, related to information visibility, consistency and integration of the information needed to perform the activity; conflict detection, coordination/transfer, hand-over procedure, monitoring. All these issues were emerged during the observation of controllers at

work (using an older system than ITI) and from the ITI system specifications.

- Scenario building. Scenarios are built to represent, in realistic situations, potential critical interactions among H,S,L components. Indeed the validation does not aim to sequentially test each single procedure as standing alone, but to create a simulated realistic operational context, in which non linear interactions among components could emerge. Scenarios are representations of possible configurations of work processes. They are an interpretation and a reconstruction of the work processes observed in the real operational context. For this reason, scenarios focus on some aspects or features of the process and neglect some others. In this respect scenarios are fundamentally different from simple "traffic samples". They do not include only number and typology of traffic in a given unit of time but are realistic situations where process breakdown may occur (occurrences of exceptional circumstances, ambiguous procedures, controllers' errors, communication misunderstandings). They are realistic since resulted from the analysis of the current work activity. It is important to point out that scenarios represent information coming from different sources (activity observations, documents, interviews, story telling) and different people with different knowledge and views (controllers, domain experts, human factors experts, developers).

In ITI scenarios were built in the following steps:

1- matching safety issues and ITI applications. We verified that the selected scenarios matched the identified safety issues and highlighted which ITI applications could impact on these safety issues.
2- trying out scenarios on the simulation platform.
3- identifying the SHEL components of each scenario (H: all the applications implemented in ITI; S: all procedures needed to the process development; L: the actors involved in the simulation, couples of planner and executive Controllers, plus pseudo-pilots). This step allows provides the framework for data analysis.
4- envisioning interactions among components. For each scenario we tried to identify which interactions between the operator and the other system components (L, S, H) could be safety critical using the ITI applications.
5- structuring scenario for test sessions to plan a complete and meaningful test. Elements of the structure included: rationale, estimated temporal duration, actors, goal (the objective of the scenario that the evaluators had to reach), initial condition (status of the interface), operational context, ITI applications involved, other external supports available to the controller.
6- Preparation of the CRIA Question Table,.that is a list of the CRIA Question Table, that is a list of questions related to the coupling of H,S,L components of the selected scenarios. These questions are administered to the controllers after the real time simulation, during debriefing sessions that have the purpose to analyse specific accounts of the tests that may remain unclear in a later analysis. Examples of the CRIA Question Table are: L-H "Do the controllers use the SIL?"; "Is the SIL an appropriate tool to provide information not contained in the label? L-S "Does the system support the controllers in applying the procedure of horizontal co-ordination?" L-L "Do the controllers co-ordinate before transferring an a/c?" (If yes) " Do they use the electronic co-ordination or the telephone?".

2- Run the test

Each test is developed in three main phases. In the following we describe the testing phase of ITI:

<u>Warming up</u>

The session started with a brief explanation of the simulation schedule and its objectives. Before starting the evaluation, the controllers were asked to familiarise with ITI even if they were already been trained in a previous pilot session.

<u>Scenarios execution</u>

The controllers received the scenario objective on a paper sheet. They were requested to execute the scenario simulating as much as possible the real operational conditions.

During the simulation the activity of controllers was observed and video recorded applying ethnographic methods of data collection. The objective of using ethnography to activity analysis is to understand the social context of the real work settings in which the activity takes place. The key benefit that ethnography offers to design and evaluation is a rich and detailed description of the complex features of the work setting. In ATM for example, what ethnography especially provides is a throughout insight into the subtleties involved in the work and in the routine interactions among members of the team work. In some way, ethnography is an alternative approach to analytical methodologies like task analysis (Kirwan and Ainsworth, 1992) and workflow. Indeed these methodologies do not focus on the social dimension of the work organisation, but aim at modelling more abstract and normative structure of tasks. The vital moment-by-moment mutual checking of "what is going on" by the various members of the team is missed in task analytic approaches to describe the work.

This kind of analysis is based on video and audio recording of the situation and notes taken by the observer. The use of audio and video analysis is not obvious (Hutchins, 1995). Some aspects of the setting are usually lost in the video and audio. The camera angle leaves some parts of the environment obscured, for example. However the data that can be collected are extremely rich. Once the situation has been recorded and transcribed, the data are interpreted by the analyst. In order to avoid misinterpretations, the transcriptions and the related interpretations are discussed with controllers for a final check.

Post test: retrospective comments, focus group with the user.

After each scenario, the controllers were involved in a debriefing session based on the video recording of the test. The controllers were asked to freely comment their performance even if the designers drove the discussion on the assessment of safety issues. At the end of the debriefing the CRIA Question Table was filled out. The technique of Focus group allowed to obtain a wide variety of views from a range of people (controllers coming from different operational realities, system developers) who might have different but equally relevant perspectives about the use and the impact of the system. Moreover, due to the freeform nature of focus group, unexpected viewpoints were identified which may be otherwise overlooked if a more structured approach, such as questionnaire methodology, is taken alone. On the basis of video recordings, controllers were mainly asked to:

- discuss about the performance of the system (accuracy, representation, reliability etc.) also by asking explanations to the system developers;
- reason about their activity with the information provided by the new system;
- make a comparison among the activity carried out with or without the support of the system.

3- Data analysis

The data emerged from test sessions, controllers' retrospective comments and focus group were analysed to evaluate the impact of ITI on safety issues and to proactively evaluate the possible occurrence of new safety issues due to the introduction of the ITI interface in the current operational context. The findings of the analysis were based on answers to the CRIA Question Table, the discussion of safety issues with controllers and the observation of the activity during the simulation. They were reported in a document and summarised in different matrixes that highlight critical interactions among SHEL components and pro-active safety assessment (see Figure 2 below). In the following we provide an extract of the outcomes and an example of the matrix containing observed critical interaction and pro-active safety assessment.

Outcomes

This section describes one example of process (in this case the execution of two procedures) where breakdowns have been observed at different levels during the test. It also describes how the projection of such breakdowns onto other resources of the process allowed us to proactively assess critical interactions that could reasonably arise under similar conditions.

The ITI interface is an innovative system with a new basic HMI characterised by three main features: a full strip-less environment, the possibility to perform electronic co-ordinations and the introduction of advanced functions like SNET and MONA. Although the operational concepts of these functionality are the real strength of the design philosophy, however sometimes the effectiveness of such concepts is reduced by the way in which they have been designed in the system (data presentation, interaction mechanisms).

The following extract mostly concerns the strip-less philosophy and the enhancement of labels representing aircraft (a/c) in the ITI interface, with a particular emphasis on the electronic coordination and the transfer-assume procedure. The simulation allowed to observe and analyse design defects that impact on usability and safety and to proactively identify critical interactions that could arise in the process under analysis even if not directly observed during the test.

As a strip-less system, the entry and exit flight levels in ITI can be coordinated directly through the a/c label. This label allows controllers to perform their activity concentrating right on the radar tracks, without shifting their attention to peripheral windows or external tools. In the following we describe the execution of the coordination procedure as it was performed during the test. This procedure is applied when a controller proposes an exit (or entry) flight level and the controller of the adjacent sector counter-proposes a different value.

The system is designed to allow controllers to manage both proposal and counterproposal in a rapid and effective way. This often encourages controllers to coordinate flights in advance and to start several coordination procedures quite at the same time, without waiting for the coordination to be solved. Often during the simulation, controllers maintained several open co-ordinations at the same time (both incoming and outgoing), but they could hardly realise the arrival of a counter-proposal from an adjacent sector. The reason is the appearance and position of proposed and counter-proposed values that are displayed on the label in the same way (same position, same font of the digits, and same colour). Figures 1A and 1B contain two screen shots of a proposed value together with a counter-proposed value.

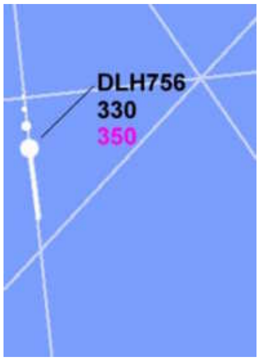

Figure 1A: Proposal

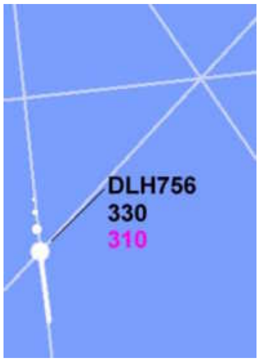

Figure 1B: Counterproposal

The activity became critical when the executive controller tried to close a coordination to transfer the a/c to the following sector without succeeding. The value he proposed to the following controller had not been accepted and the second controller counter-proposed a new one. Therefore the system was waiting for a reaction to the counter-proposal and in the meantime the first controller did not have any control on the label. At this point he asked the planner controller what was going on. Neither the planner controller was able to diagnose the problem, so in turn he called by phone the planner controller of the following sector asking for closing the coordination. At this point, the breakdown was revealed since the second planner explained that a new value had been counter-proposed and never accepted. The problem was solved but the time needed to accomplish the procedure was so long to vanish the benefits of the electronic coordination. This breakdown was originated by a L-H critical interaction and propagated to L-L interaction. The breakdown could indeed be avoided using other tools available on the interface.

On the top of the interface there are the Coordination IN and OUT windows that help to discriminate between an outgoing coordination proposal and an incoming counterproposal. These windows list all incoming and outgoing coordination messages and it is possible to disambiguate the meaning of the magenta value in the a/c label by simply checking whether the coordination message is present in the IN or OUT window.

Why didn't the controllers use this tool? Actually they misunderstood the meaning of the Coordination IN and OUT. Instead of considering the windows as lists of incoming and outgoing coordination messages, controllers interpreted them as lists of "inbound" and "outbound" flights. This is a mental model developed by the use of tools like the paper strips or SIL (sorted inbound list, a kind of electronic strip-board) that stimulate the controllers to reason in terms of inbound and outbound a/c whilst the ITI system "reasons" in terms of messages IN and OUT. The formulation of the wrong mental model produces two critical interactions: a L-H interaction due to the bad design of the Coordination windows (their name "Coordination In" and "Coordination Out" can be easily misinterpreted); a L-S critical interaction, due to the praxis of the controllers to use the SIL to monitor incoming traffic. In currently operational systems the SIL contains flights that are double sorted by entry points and estimated time of arrival. In ITI the SIL is sorted only by time of arrival. This is a severe limitation for controllers who did not appreciate this functionality and therefore did not use it very much during the simulations.

The misinterpretation of the co-ordination in and out was due to the fact that controllers considered them as particular instances of the SIL, containing only flights with open co-ordination.

In other words the misinterpretation of Co-ordination Windows was biased by their previous negative experience with the SIL therefore this knowledge was applied also to other similar objects of the interface.

The example described above provides a first insight of the richness of interactions and outcomes we collected during the real time simulation. Data analysis was conducted in a systematic way analysing the procedures carried out during the scenarios in terms of SHEL components and taking note of the observed breakdowns. These were in turn propagated from observed procedures to the whole process under investigation (e.g. from the co-ordination procedure to the complete process including monitoring and transfer of control), providing a set of recommendations on potential breakdowns that could occur if the ITI interface would be operational in the current ATC context. The results of the analysis were reported in form of matrixes as sketched in Figure 2 below.

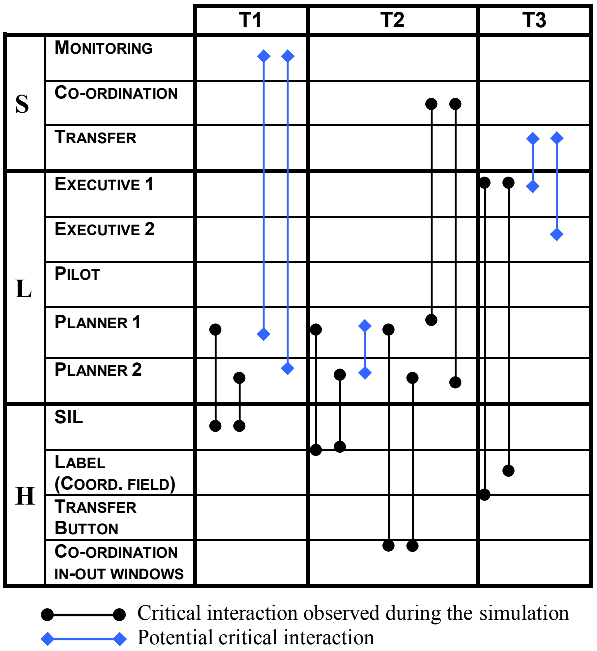

Figure 2: Example of data analysis

In particular, Figure 2 reports the analysis performed on the process "transfer of control" composed of three different procedures: monitor, co-ordination and transfer. This process was tested through one or more scenarios in the real time simulation. On the left column S, H, L components of the process are represented.

In the first row T1, T2 and T3 refer to the steps necessary to manage a flight that ideally crosses sector 1 (managed by planner 1 and executive 1) and then enters the adjacent sector 2 (managed by planner 2 and executive 2). T1, T2 and T3 are related to monitoring, co-ordination and transfer of control procedures respectively. These procedures when combined together constitute the process of transfer of control, one of the most delicate processes of ATM.
From left to right, the table shows a critical L-H interaction concerning the already mentioned problems related to the use of the SIL. It involves planners of both sectors. Even if not directly observed during the simulation, this critical interaction can be expected to affect the monitoring procedure. Indeed since in ITI the flights are sorted in the SIL by estimated time of arrival in the sector (the entry point and the time of arrival to the point are not represented in the SIL), in order to correctly carry out the monitoring procedure, the planner should consult the label of each aircraft involved in the process, keeping in mind relevant information and comparing them to efficiently manage the traffic. The lack of an appropriate external representation for executing the procedure is compensated by the planner with a resulting increase of cognitive effort for his/her activity.

The second column contains other critical L-H interactions. One of these concerns the already mentioned problem related to the way co-ordination proposals and counter-proposals are implemented and represented in ITI (see Figures 1A and 1B).
The other concerns the misinterpretation of the Co-ordination In and Out Windows.
This is a typical example of propagated criticality. As a matter of fact the caption "Co-ordination in" and "Co-ordination out" may be misleading. But probably this defect would have been less critical if proposals and counter-proposals had been more distinguishable on the radar screen and/or the SIL had been better organised.
As consequence of these L-H critical interactions two more L-S critical interactions emerge (also represented in the second column), consisting in the breakdown of the co-ordination procedure.
Moreover a L-L critical interaction is expected to involve the planners, who could misinterpret the situation as happened during the simulation.

Further L-H critical interactions are represented in the third column. They both involve the executive controller[1].
The first problem consists in the fact that the transfer function is not available in case of flights with open-co-ordinations. In other words the transfer procedure is stuck until the co-ordination procedure is concluded.
The second is strictly related to the first one: the co-ordination cannot be interrupted or cancelled by the controller who is waiting for the answer. Only the other can do it, accepting the value proposed, counter-proposing another value or rejecting the co-ordination.
In a real operational context these L-H critical interactions are expected to affect the L-S interaction in the transfer of control procedure.

As general conclusion, the example proposed puts in evidence how different critical interactions, occurring in different times and involving different resources may combine together provoking the breakdown on the whole process of transfer of control.

Conclusions

[1] For the sake of synthesis Figure 2 mentions only the executive of sector 1, since he is the transferee of the imagined flight. The same analysis can be extended to the executives of the other managed sectors.

The CRIA methodology provides a powerful framework for safety assessment. Its main assumptions can be resumed in the following statements:

- Each resource in a process is a stakeholder of knowledge needed to perform the process.
- The modification of a resource changes the interaction among SHEL components (i.e., the introduction of new tools in a work setting).
- Criticality is a wrong distribution of the resources among the components.
- Breakdown is a rupture in the interaction between the components.
- Any process can be executed with a different allocation of resources.
- Dynamic and complex system environments require flexible allocation of resources for process execution in order to deal with breakdowns of components and unpredictable situations.

Furthermore, CRIA allows also to proactively assess problems and critical interactions that are not observed during the simulation. Indeed simulation scenarios focus on specific accounts of activities and some critical interactions may not emerge during the observation. The CRIA analysis goes beyond the very observed activity allowing to proactively assess the impact of the new tools on the entire process even if not directly observed. Indeed if we project an observed critical interaction to the development of the entire procedure, we can discover that the tools, in the current implementation, could put at risk also the interaction between other components of the process.

In conclusion, the methodology we presented was successfully tried out in different contexts of safety critical applications (Rizzo et al, 2000). The application described in this paper confirms its potential to a pro-active evaluation of the impact of new technological tools in real operational settings. In particular the method offers the following advantages:

- it allows to systematically detect critical interactions about system components and to infer new ones;
- it allows to overcome the limitation of scenarios that represent categories of single events;
- it provides the knowledge necessary to specify requirements and re-design defects. Indeed the method clearly detects at what level the problem occurs and which interactions among system components should be redesigned to solve it.

References

Carroll, J.M. (Ed.), (1995). Scenario-based design: envisioning work and technology in system development. New York: Wiley.

Edwards, E., 1972, Man and machine: Systems for safety, Proceedings of British Airline Pilots Associations Technical Symposium (British Airline Pilots Associations, London), pp. 21-36.

Rizzo, A., Pasquini A., Di Nucci, P., Bagnara, S. (2000) SHELFS: Managing critical issues through experience feedback in railways. Human Factors and Ergonomics in Manufacturing, 10, 83-98.

Hutchins, E. (1995). *Cognition in the Wild.* MIT Press.

Kirwan, B. & Ainsworth, L.K., (1992) *A Guide to Task Analysis*. Taylor & Francis, London.

Nardi, B. (Ed) (1996). *Context and Consciousness: Activity Theory and Human-Computer Interaction* Cambridge: MIT Press.

Author Biographies

Patrizia Marti.

Patrizia Marti is lecturer in Educational Technologies at the Communication Science Department of the University of Siena (Italy) where she made research in the areas of nomadic systems, educational technologies and safety critical systems. Her current research interests are interaction design and human factors in safety critical applications. In 2001, she co-founded Deep Blue s.r.l., a consultancy firm based in Rome (Italy) composed of a multidisciplinary team of specialists in human factors, cognitve psychology, interaction design, and software engineering. Deep Blue s.r.l. operates in the area of design, development and validation of complex systems in strict collaboration with Eurocontrol Experimental Centre (Bretigny, France) and ENAV S.p.A. (the Italian Aviation Authority).

Paola Lanzi

Degree in Communication Science at the University of Siena, Italy. Since August 2000 she collaborated with the Multimedia Communication Laboratory of the University of Siena working on international projects for the evaluation of safety critical applications and nomadic systems for art and entertainment. From 2001, she works as human factors expert for Deep Blue s.r.l. in particular the analysis and validation of ATM systems. Her research area includes user studies, distributed cognition, real time simulations.

Francesco Pucci.
Degree in Communication Science at the University of Siena, Italy, with a thesis in Human-Computer Interaction. Since 1999 he worked as a free-lance consultant for Butera e Partners (Rome-Milan, Italy) and as HCI researcher at the Multimedia Communication Lab of the University of Siena (Italy). Involved in several international research projects, his areas of interest include interactive systems for education and cultural heritage, and activity analysis and validation of complex systems. From 2001, he works as interaction designer for Deep Blue s.r.l. in particular developing innovative concepts for ATM.