

Integration of functional, cognitive and quality requirements

A railways case study

Massimo Felici, Mark-Alexander Sujan, Maria Wimmer

Abstract

The paper shows a SHEL oriented requirements engineering approach, which has been applied in a case study dealing with the definition of the requirements for a new railways traffic control system. The SHEL model provides an integrated view by considering any productive process or activity performed by a combination of Hardware, Software and Liveware resources within a specific environment. A set of SHEL oriented requirements describes the different views on a complex system. The requirements are grouped into three main classes of requirements, namely, functional, cognitive and quality requirements. The paper points out the issue of integrating different types of requirements.

1. Introduction

Requirements engineering [17, 22] approaches still focus on the information technology to be designed. However, complex systems consist of various resources with different characteristics. Several studies [2, 3, 8] point out that the automation of work, introducing new information technology within a productive environment, may lead to serious dependability problems and often results in non-effective use of new systems. Accidents involving complex technology are often caused by a combination of organisational, managerial and technical factors [14]. Literature on accidents, incidents and near misses in safety-critical systems [13, 15] stresses that both the weaknesses and the strengths of a system are in the interaction among resources.

Recent research [18, 20] in requirements engineering encourages the adoption of hybrid methodologies already early in the design process. The relationships among resources interacting / co-operating in a productive process need further clarification in order to obtain an integrated requirements engineering approach.

The paper points out the issues of integrating different types of requirements, which are defined over software, hardware and liveware resources. The SHEL model [4] provides an integrated view over software, hardware and liveware resources supporting an integrated requirements engineering approach (Section 2). Section 3 shows a railways case study in which we have applied the integrated approach. Section 4 discusses functional, cognitive and quality requirements and presents a template to integrate the different types of requirements. Furthermore, insights from eliciting requirements and integrating diverging views for the case study are presented. Finally, our conclusions and further work are presented in Section 5.

2. A SHEL oriented requirements engineering approach

The SHEL model [4] supports a systemic view defining any productive process as performed by a combination of Hardware (e.g., any material tool used in the process execution), Software (e.g., procedures, rules, practices, etc.) and Liveware (e.g., end-users, stakeholders, etc.) resources embedded in a given Environment (e.g., socio-cultural, political, etc.). The knowledge required to perform a specific process can be considered as being distributed among the system resources. Thus, a productive process may be regarded as an instantiation of the SHEL model for a specific process execution. The systemic view of the SHEL model encourages the definition of requirements not just for the system to be designed

(hardware and software), but also for those aspects (e.g., procedures, practices, human roles, interaction, help in breakdown-situations, etc.) related to Liveware resources. Therefore, SHEL oriented requirements represent a trade-off among Hardware, Software and Liveware resources in a given Environment. Further discussion of the SHEL concept can be found in [16, 23].

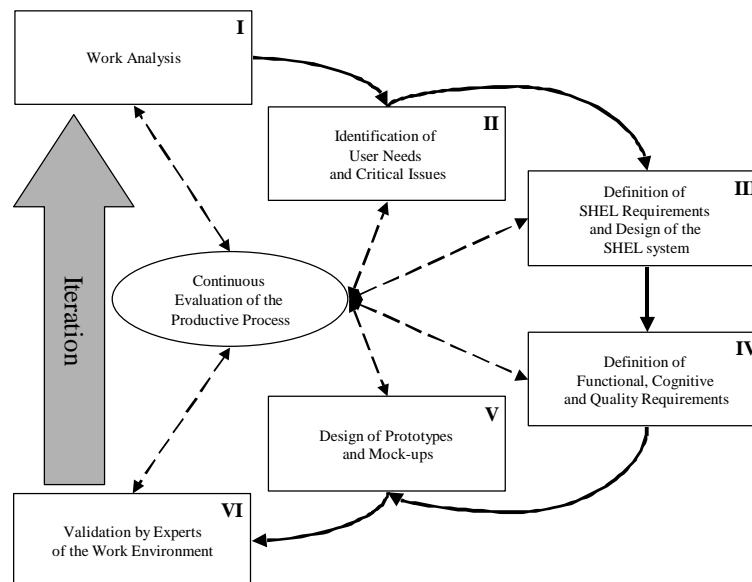


Figure 1: The phases of the process adopted for defining requirements

Figure 1 shows a SHEL oriented approach for the definition of requirements. The first step is a profound analysis of the work system of the specific environment. The knowledge required to perform a productive process, both in normal and abnormal conditions, is captured. The work analysis studies the way in which the productive process is performed taking into account the process itself and all the resources that contribute and interact in the process execution. The analysis uses different counterbalancing techniques of knowledge gathering, including observations, interviews, ethnography, heuristic analysis methods, video recording, checklists etc. Representative models of processes, tools supporting the process performance, objects in the work processes, interactions, social and work practices, formal procedures, critical issues, and human skills and behaviour are produced to describe the existing work system with its critical issues and weaknesses. Reports and models for knowledge representation are e.g. scenarios, narrative descriptions, templates and other task models. The generation of these reports and representative models involves a continuous iteration of analysis, modelling, and evaluation by the users until a satisfactory common understanding of the work system has been reached. In the analysis scenarios are an important instrument to underline current weaknesses in certain problem situations, to communicate with end-users and get feedback from them and to link critical issues to user needs and later on to requirements. An overview of different potential applications of scenarios can be found in [7, 19].

As soon as enough information is collected by the work analysis the focus changes to the weaknesses of the actual system by eliciting critical issues due to the knowledge distribution among the SHEL resources and their interaction. The results are organised in terms of the critical issues and user needs represented according to the SHEL model, which is also used to link critical issues within the productive processes, with functional, cognitive and quality requirements. The outcome of the second phase also provides a basis for alternative design

considerations taken later on in the engineering process. In our understanding designing or re-engineering a system implies a redistribution of knowledge, which includes also dynamic task allocation and job design. The underlying idea of the second phase is to figure out suitable knowledge distributions, which enable an effective use of the resources in order to perform the specific productive process. The basic assumption is that there are no exclusive combinations of the three principal SHEL resources to shape a specific process, hence the same process can be performed using different possible combinations of the Hardware, Software and Liveware resources. Already early in the design process, this can be reflected by alternative design solutions represented by various prototypes and design models.

In the third phase of the process all the collected information contributes to defining the requirements and architecture of the system according to the SHEL model. The SHEL requirements and architecture of the system represent the starting point for defining functional, cognitive and quality requirements, which is the fourth phase of the process. It is discussed in detail in section five. The phase of specifying the system requirements is followed by a design phase, where the requirements are mapped into design patterns represented in prototypes, mock-ups, design models, scenarios etc. The last phase of one iteration cycle in the SHEL oriented requirements engineering approach is the validation by the domain experts. The activity concerns a proof of the projected system in the real world, where system compliance with the requirements is evaluated, and where the requirements and the projected system are validated in the real system environment.

The holistic approach employs a continuous evaluation and verification of the analysis results, requirements and alternative design solutions during the whole design phase. Some influence due to the introduction of a new system within a productive process can be predicted, but the real impact can only be evaluated during testing and application in practice. The use of prototypes [1, 9] together with user involvement are effective instruments to validate possible modifications before the final implementation. Simulation using mock-ups and prototypes together with a set of pre-defined scenarios [5, 21] ease the communication and feedback with the users in order to improve and validate the requirements and to anticipate bad design solutions or impacts to the environment. Various architectural solutions and implementations are evaluated with the user by refining the prototypes and repeating the analysis and design parts in an iterative way. Evaluation takes into account directly measurable criteria such as performance (e.g., number of trains dispatched, maintenance work completed) and also criteria such as usability, cognitive workload and level of cognitive support.

3. A railways case study

The case study consists of a railways traffic control (RTC) system for which the requirements have been defined in co-operation with the Italian National Railways (Ferrovie dello Stato - FS). The system is to support the dynamic rescheduling of the railways resources (e.g., train paths, vehicles, maintenance units, etc.) by human agents in case of unplanned events. The planning activity as currently conducted by FS is divided into seasonal time-table planning, contingency planning to take into account special short term demands, and real-time planning to react to unforeseen events. The project focuses on the real-time planning on a particular line of the Italian railways network which can be characterised by the need for high responsiveness, rapid decision taking and the existence of multiple conflicting targets. Important requirements for the RTC system to be developed during the project are:

- ?? increased quality of service (e.g., rescheduling the rail resources via real-time planning in the case of disturbances, providing customer information, managing breakdown situations)
- ?? more efficient use of infrastructure, personnel and rolling stock

?? dynamic management of transport resources.

The RTC system concerns the control and reactive management of the train movements within a certain control zone. The FS have a heterogeneous infrastructure and information technology support. There exist mainly three work environments where the control process is carried out by different systems. In the first one the work is carried out by a quasi manual RTC system, in which the train positions are graphically registered by hand on a specific paper table. The oral communication is the principal means of interaction even during emergencies. It takes place by face-to-face interaction, microphone or telephone. In the second environment the operator works with more technical instruments providing an automatic monitoring system for the railways traffic. In the third environment the control system allows the operator to act directly on the line by switching junctions and setting protection signals of stations. In this case, stations can also be unmanned, and so the stations are managed remotely.

During normal activities, the control operator observes the train movements and computes the deviations of the real data from the planned time schedule. The assessment of the deviations is based on the gravity of the deviations, formal rules, operator's experience and on other environmental factors. The overall goal of the operator's work is to make decisions for rearranging the productive resources and objects based on their assessment of deviations in order to avoid or minimise inconveniences or even incidents that may lead to economical damage or harm to humans. In order to react appropriately, especially in emergency cases, the operators need to have in any moment an understanding of the dynamic system. They use several artefacts for keeping the necessary knowledge alongside.

The operator has the supervisory control of the objects in use in their control zone as far as the movement is concerned. Yet, the direct responsibility and management of the different resources (e.g. humans, or machines) is assigned to other departments as defined in the organisational structure of the FS. Hence, the operator has to collaborate and co-ordinate with colleagues of other departments. Further characteristics of the operator's work are economical and safety related criticality, high dynamism and little predictability, unforeseen or unpredictable events that trigger and require quick decision-making, involvement of many objects, need of sufficient knowledge, skills and experiences, consideration of decisions in the context, varying workload.

Notice that the control process involves hardware, software and liveware resources. As changes are implemented to perform the control process, the knowledge distribution changes among the resources in the overall system environment. Over time the availability, adaptability and flexibility of the resources within the environment affect the control process. Improving the overall system requires therefore a careful consideration and re-distribution of knowledge among the resources as well as an effective design of the interactions. Requirements may not only be defined for functionality of the resources in isolation, but also for their interaction, for breakdown or non-availability. As human operators represent a crucial resource in the control process special focus needs to be placed on cognitive requirements supporting user needs especially in critical situations. Moreover, the complex interrelations among the resources require careful consideration and necessitate the definition of quality requirements (e.g., reliability) for the control system.

4. Integration of functional, cognitive and quality requirements

The section describes shortly the functional, cognitive and quality requirements defined for the case study as well as the attempt of integrating them by the means of the SHEL model. Figure 2 shows a SHEL-oriented architecture representing system aspects as well as work aspects. The SHEL-oriented architecture emphasises the boundary of the system and its interaction with other systems or human agents.

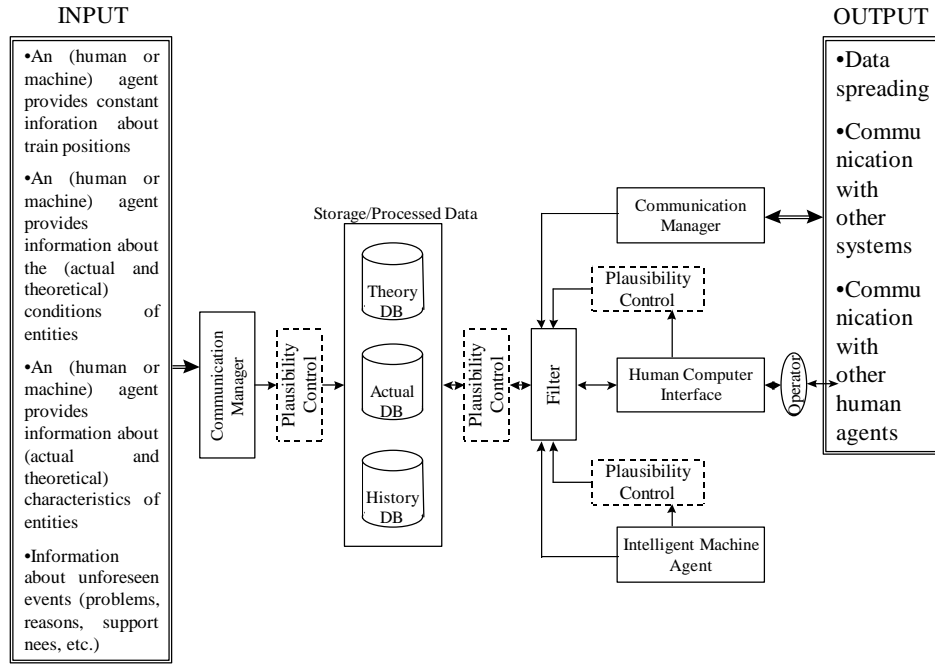


Figure 2: A SHEL-oriented architecture

4.1. Functional requirements

Functional requirements describe the functionality each system component needs to contribute to achieve the process goals. From the knowledge distribution point of view this means describing the process knowledge allocated to a specific system resource according to the SHEL model. In addition, ‘interaction’ requirements describe the interaction among system components.

In general, functional requirements are extracted from an exhaustive analysis of the existing work environment with elicitation of critical issues and weaknesses of the current knowledge distribution among the SHEL resources. Moreover, the definition of the overall system architecture and the specification of general system requirements give a frame for detailing specific functionality in the assigned system component. Other sources bypassing the functional requirements specification are expert knowledge from the different members participating in the design team [11], technological advancements influencing the projected system, as well as overall project goals driving the organisation to change the existing system (table 2 shows an examples of the functional requirements for the RTC case study).

A continuous evaluation and verification of the functional requirements during the whole design phase is important. Thereby, early design solutions in form of prototypes and mock-ups together with scenarios can help to validate the defined functional requirements and to anticipate bad design solutions or impacts on remaining system components. Continuous evaluation of requirements and design solutions is strongly recommended.

4.2. Cognitive requirements

Cognitive requirements are non-functional requirements, which derive from the psychological demands of the humans working within the system. These are frequently neglected and often have led to incidents or system under-utilisation. It is generally agreed that humans are an essential part in the operation of complex systems, because they are better able to handle unforeseen events than machines are. However, frequently they are considered as part of the environment of a computer system to be designed, rather than part of the system itself. This fails to take into account the importance of the interaction of the humans and the

various artefacts. More promising is the Distributed Cognition approach [10], which maintains that a complex system is composed of humans, hardware artefacts, procedures and rules. The knowledge is distributed over all the components of the complex system. Cognition cannot be understood by analysing or observing the human in isolation, but rather by analysing the complex socio-technical system as a cognitive entity. This allows understanding that work processes are performed by a dynamic combination of the different system resources (HW/SW/LW).

The conception of distributed cognition leads to a variety of new, cognitive requirements, which the system has to meet. Since the knowledge required to perform a process is distributed over the components, a generic cognitive requirement is that the required knowledge for a human to react to unforeseen events needs to be available to him/her. Examples of cognitive requirements are "Status of the support system should be obvious at all times", or "Train path monitoring should be done such that data is available after possible support system breakdown". The cognitive, non-functional requirements will map eventually onto functional requirements, some of which may be implemented by a dynamic function allocation scheme, e.g. "All functions offered by the support system concerning the selection of train paths need to be executable also manually", or "All functions offered by the support system need to offer a facility to switch them on or off". Another example (not implemented by dynamic function allocation), with respect to the above non-functional requirement is "Train path monitoring should be done redundantly on a permanent hardware medium". Such a redundant distribution of knowledge allows performing the process even after the breakdown of some of the involved resources.

4.3. Quality Requirements

The quality requirements for the control system have been extensively discussed in [6]. The software architecture for the control system consists of three main components (four with the operator), the System Monitor, the Man Machine Interface, and the Decision Support System. Each component has a different task, hence different quality requirements.

According the standard ISO 9126 [12], the quality model consists of a set of important quality characteristics for the final product. Quality subcharacteristics and attributes refine the quality model. Attributes are directly measurable software properties that quantify the quality subcharacteristics. Quality characteristics and subcharacteristics can be internal or external representing respectively the design view and the end-user view. Internal quality attributes are measurable properties of the software product on its development process that influence the final product quality. The internal attributes are related to one or more external quality characteristics of the quality model according to the quality view that is suitable for the specific project.

A set of quantitative targets identify specific boundaries on the internal quality attributes, which are also used to monitor the project progress. Once a product is undergoing final testing or has been released to a limited user population, it is necessary to measure the actual quality achievement. Thus the measures over the external quality attributes are compared with the foreseen targets to confirm that the software product meets the requirements. These requirements, usually referred to as quality requirements, describe the user needs and are quantified in terms of values (targets) for specific external attributes.

Table 1 shows the internal reliability defined for the system monitor of the case study together with the target values for the attributes. We do not describe all of the quality model for the sake of brevity. In order to identify the quality characteristics and to define the quality requirements for the project, the work analysis was quite useful. Work analysis results allow to better understand the integration of the system into the work environment. It is possible to analyse deeply the work performed by the operator and the system. The user viewpoint has

been used to refine the characteristics of the quality model. The quality requirements are based on the system aspects pointed out from the user.

Table 1: internal reliability and target values for the System Monitor

System Component	Quality Characteristic	Quality Subcharacteristic	Quality Subsubcharacteristic	Attribute	Target
System Monitor	Reliability	Estimated Reliability		Mean time between failures	? 1*10E3 hours
		Correctness		Module fault density	? 10 faults per module
		Test Accuracy	Test Coverage	Function coverage	= 100 %
				Branch coverage	? 70%
		System Evolution Trend		Trend of module modification	to be defined on first changes
				Trend of requirement modification	to be defined on first changes

4.4. Requirements integration

The section shows all the issues that we encountered for integrating the different types of requirements of the case study. Integration of functional, cognitive and quality requirements is no easy task. The discussions we had during the project were characterised from the different viewpoints each of us had – biased from our background discipline. We took into account separately functional, cognitive and quality requirements. Hence, the first phase of the work was to encounter the different types of requirements as described above. During these discussions it was also important to realise and accept the different viewpoints on system characteristics the others had developed. Finally, our discussions aimed to identify a suitable way for integrating soundly and reasonably our work.

Table 2: An example of a classification of SHEL requirements and types of requirements

SHEL Requirements		SHEL Space Resources				Type of Requirements		
Function ID	Description	S	H	L	SHL	F	C	Q
1	Provide Information				*	*	*	
1.1	Reliable Information		*	*			*	*
1.2	Required Information	*	*	*		*	*	*
1.2.1	Characteristics of Trains		*			*		
1.2.2	Characteristics of Tracks		*			*		
1.2.3	Characteristics of Stations		*			*		
1.3	When it is required – to have it at any time	*	*	*		*	*	*
1.3.1	As quickly as possible	*	*				*	*
1.3.2	Long term (as feedback)	*	*			*		
1.3.3	Constant/permanently available information	*	*	*		*	*	
1.4	Adaptive information, when it is needed	*	*				*	
1.5	Adaptive – how to display	*	*				*	
1.6	Provide feedback from actual status of the entities involved in the system	*	*	*		*	*	
1.6.1	For theoretical planning	*				*		
1.6.2	For decision making (from history of movements)	*	*	*		*	*	
1.7	Visualise deviation from actual to theoretical	*				*		*

Table 2 shows an example of the SHEL requirements classified in terms of type of resources¹ (i.e., Software, Hardware and Liveware) and type of requirements (i.e., Functional, Cognitive and Quality). The requirements are the result of the work analysis and the synthesis of user needs. The SHEL view and the classification of requirements provide a holistic design perspective, which is useful not only for designing the control system, but also for defining new activities and procedures that need to be designed together with the new system.

The following points summarise our experiences and lessons learnt for integrating functional, cognitive and quality requirements:

- ?? Classical requirements engineering approaches do not support the integration of different types of requirements.
- ?? Most of the requirements engineering approaches focus on the process of defining requirements without taking into account specific product aspects.
- ?? The attempt of integrating different methodologies (e.g., work analysis and software quality) dealing separately with functional, cognitive and quality requirements resulted to be costly.
- ?? The relation between different types of requirements (e.g., function-cognitive, quality-cognitive and functional-quality) is not clear.
- ?? The different types of requirements represent redundancies, which may increase inconsistencies. An effective representation of integrated requirements can improve the ability of assessing the completeness and the correctness.
- ?? An effective representation of integrated requirements could improve the ability of managing changes in the requirements. The origins of requirements evolution are due to the different stakeholders involved in the development process. Hence any change in the specific environment will affect requirements. Managing integrated requirements could become an effective way for obtaining change tolerant processes and requirements.

5. Conclusions and further work

The paper points out a set of issues to integrate different types of requirements, which have been defined by a systemic requirements engineering process taking into account a holistic view of the system. The identified issues represent a check list for comparing requirements engineering approaches. Currently most of the methods in requirements engineering do not support all the features required for an integrated methodology. Moreover, the set of issues for integrating requirements represents a work plan suggesting possible research directions and updates for requirements engineering methodologies. We strongly suggest to tackle all the issues identified in order to obtain integrated requirements specifications fitting the holistic expectations.

References

- [1] Budde, R., "Approaches to Prototyping", Springer Verlag, Berlin, 1994.
- [2] Clegg, C.W., Warr, P.B., Green, T.R.G., Monk, A., Kemp, N.J., Allison, G., Landsdale, M. "People and Computers: How to Evaluate your Company's new Technology", Ellis Horwood, Chichester, 1989.
- [3] Eason, K.D., "Information Technology and Organisational Change", Taylor and Francis, London, 1988.
- [4] Edwards, E., "Man and machine: Systems for Safety", Proceedings of British Airline Pilots Associations Technical Symposium, British Airline Pilots Associations, London, 1972, pp. 21-36.

¹ Requirements classified as SHL are those which involve all the SHEL resources. The classification depends on the granularity of the representation of requirements.

- [5] Erickson, T., "Notes on Design Practice: Stories and Prototypes as Catalysts for Communication", In *Scenario-based design: envisioning work and technology in system development*, John M. Carroll (ed.): John Wiley & Sons, 1995.
- [6] Felici, M., Pasquini, A., De Panfilis, S., "Software Quality in User-Centred Design", *Proceedings of ESCOM-ENCRESS 98*, Rome, Italy, 27-29 May 1998, pp. 239-247.
- [7] Filippidou, D., "Designing with Scenarios: A Critical Review of Current Research and Practice", In *Requirements Engineering*, vol. 3 (1):1-22, 1998.
- [8] Hornby, P., Clegg, C.W., Robson, J.I., MacLaren, C.R.R., Richardson, S.C.S., O'Brien, P., "Human and Organisational Issues in Information Systems Development", *Behaviour & Information Technology*, vol. 11 (3), 1992, 160-174.
- [9] Houde, S., Hill, C., "What do Prototypes Prototype?", In *Handbook of Human-Computer Interaction* (2nd ed.), M. Helander, T. Landauer, and P. Prabhu (eds.): Elsevier Science B.V., Amsterdam, 1997
- [10] Hutchins, E., "Cognition in the Wild", MIT Press, 1995.
- [11] ISO/DIS 13407, "Human-centred design processes for interactive systems". ISO, 1999.
- [12] ISO/IEC 9126, "Information Technology – Software Quality Characteristics and Metrics" .
- [13] Kletz, T., "Lessons from Disaster", Gulf Publishing Company, Houston, 1993.
- [14] Leveson, N., "Safeware", Addison Wesley, Readings, MA, 1995.
- [15] Perrow, C., "Normal Accident: Living with High-Risk Technologies", Basic Book, New York, 1984.
- [16] Rizzo, A., Pasquini, A., Di Nucci, P., Bagnara, S., "ShelFS: Managing critical issues through experience feedback in railways", In *Human Factors and Ergonomics in Manufacturing*, vol 9 (in press).
- [17] Sommerville, I., Sawyer, P., "Requirements Engineering: A Good Practice Guide", John Wiley & Sons, 1997.
- [18] Sommerville, I. Sawyer, P., "Viewpoints: principles, problems and a practical approach to requirements engineering", *Annals of Software Engineering*, pp. 101-130, 1997.
- [19] Sutcliffe, A., "Scenario-Based Requirements Analysis", In *Requirements Engineering*, 3(1):48-65, 1998.
- [20] Viller, S., Sommerville, I., "Social analysis in the requirements engineering process: from ethnography to method, Technical Report CSEG/14/1998, Lancaster University, 1998.
- [21] Weidenhaupt, K., Pohl, K., Jarke, M., Haumer, P., "Scenarios in System Development: Current Practice", *IEEE Software*, vol. 15 (2): 34-45, 1998.
- [22] Wieggers, K.E., "Software Requirements", Microsoft Press, 1999.
- [23] Wimmer, M., Rizzo, A., Sujan, M., "A Holistic Design Concept to Improve Safety Related Control Systems", *Proceedings of International Conference on Computer Safety, Reliability and Security (Safecom'99)*, LNCS 1698, Springer Verlag, 1999.

Acknowledgement

We are grateful to Alberto Pasquini (ENEA, Italy) and Antonio Rizzo (University of Siena, Italy) as well as some people of the OLOS Network (Human Capital and Mobility Programme of the European Community 3rd Framework Programme) for their support, supervision and comments to this work and our attempt to integrate software, hardware and human aspects in requirements engineering. A special thank goes to the Italian National Railways (FS), who provided the case study and allowed us to interact with system operators spending their time.