UML based risk analysis - Application to a medical robot

J. Guiochet
GRIMM-ISYCOM/LESIA, University of Toulouse II, France
C. Baron
LESIA, INSA Toulouse, France

ABSTRACT

Medical robots can perform complex tasks and share their working area with humans. Therefore, they belong to safety critical systems. In nowadays development process, safety is often managed by the way of dependability techniques. We propose a new global approach, based on the risk concept in order to guide designers along the safety analysis of such complex systems. Safety depends on risk management activity, which core is risk analysis. This one consists in three steps : system definition, hazard identification and risk estimation. We first propose the use of UML (Unified Modeling Language) as the description language. Then, for the next steps, interactions of UML and risk analysis techniques such as FMECA (Failure Mode, Effects and Criticality Analysis) are studied. As an illustration of its potentiality, the proposed approach has been applied to the case study of a system for robotic tele-echography (ultrasound scan examination).

1. INTRODUCTION

Today, as many new application areas for robotic systems emerge, including medical robots, safety is becoming critical [2]. Robots can have a close interaction with patients and medical specialists. In this context, for medical robots as Robodoc (ISS, Inc., USA) safety is the essential requirement for commercialization [1]. Safety, defined for industrial robots as the prevention of damage to the robot itself and its environment, and particularly the human component [3], can now be defined as the property of a medical robot to be "free from unacceptable risk" [8]. Therefore it is necessary to reduce the risk to an acceptable level with a complete risk management activity (see the norm [7]). Those activities are based on a system model. UML (Unified Modelling Language) notation is now a standard in system and software engineering. We have also chosen this language for its expression power. In this article we present a new approach of risk analysis integrating UML notation (section 2.). This approach have been successfully applied to the

development of a medical robot for tele-echography (section 3.).

2. UML BASED RISK ANALYSIS

As illustrated on the right part of the figure 1 (from the norm [7]), risk management is composed of different activities: risk analysis, risk evaluation and risk reduction. In this article we focus on risk analysis which consists in three steps : system definition, hazard identification and risk estimation (the risk is calculated based on damage severity and probability). The description of those activities can be found in a more generic norm: the Guide 51 [8]. The first step of a risk analysis concerns the definition and the descriptions of the system, its boundaries and the intended use. This step is particularly linked with requirements analysis and human factors integration and on its main activities: the function allocation and the task analysis. For both of those activities, UML diagrams as *use case* and *sequence* diagrams are useful as shown in a previous work [6]. Those diagrams help designers in defining non ambiguous and consistent activities of each actor. They also permit to create a link between the risk analysis and the development process. Those reasons led us to choose the first step of the risk analysis which is "system use and intended use description in UML" as shown on figure 1.

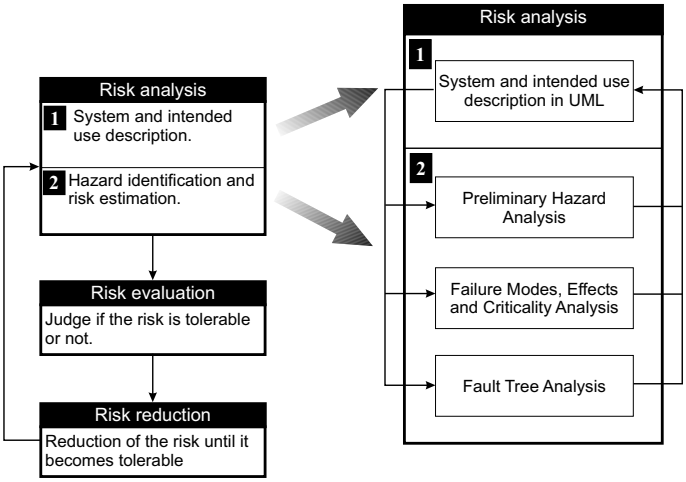

Figure 1 : UML based risk analysis in the risk management activity

The second step of risk analysis is the hazard identification which can be done with analytical methods. In a schematic view, a system use can be represented as in figure 2. *External environment* is represented as a *stick-man* because it acts as an actor for the subsystem. On this diagram, only control flow is represented and not the data flow. Based on this notation, five main hazards can be identified: harmful perturbations from external environment (message *perturb*), bad uses which are usually human errors (message *use*), subsystem failures (message *react*), combination of those hazardous phenomena and combination of interactions which are not identified as failures but that can nevertheless lead to a hazard.

Based on this hazard list we have chosen to use three analytical methods. First, PHA (Preliminary Hazard Analysis) is a participatory method which can be applied in the early step of the process development. A group of designers, users, domain specialist met together to determine main hazards. This can lead to identified the five hazards presented above. Second, FMECA (Failure Mode, Effects and Criticality Analysis), which is a method used for the identification of potential errors of the examined object, permits to analyze the first three points of our hazard list. Last, Fault Tree Analysis (FTA) is well adapted for the two last hazards of the list and can complete the FMECA in an advanced design. For those three methods, UML models developed previously are used to perform the analysis as illustrated in figure 1.

Message	Failure mode (error)	Cause	Effects a. Same level b. Upper level c. System level	Risk			Possible detection means: (on line) a. Failure mode b. Effects	Potential solutions: : a. Prevention b. Protection c. Other actions d. Remarks
				Severity	Probability	Risk		
Control movements (parameters)	Bad parameters	Master site failure or link failure	Unwanted movement	1	P	H	Parameters coherence verification (digital filter)	a. Use of a standard protocol b. Ignore value, set the controller in waiting state

Figure 4 : A failure mode analysis of the message *Control movements*

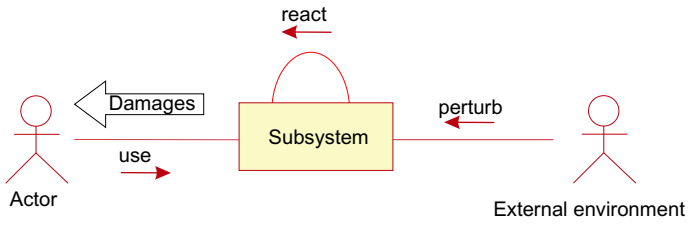

Figure 2 : Main interactions during a subsystem use

UML use cases have been used to complete tables during PHA to understand the context of potential accident and which actors were exposed. Considering that damages appear into a system because of its dynamics we focus on message exchanges which are the core elements of dynamics. Going on the notion of *Message* in UML, we presented some models of errors related to this concept and we have used them in the FMECA tables. A more complete study is presented in [5]. Interactions between FTA Technique and UML are still studied but some diagrams as object diagram can be the base of fault trees.

Those methods used with object-oriented development led to propose solutions to reduce the risk which are mainly: re-design, new requirements, modification of the use.

3. APPLICATION ON TER

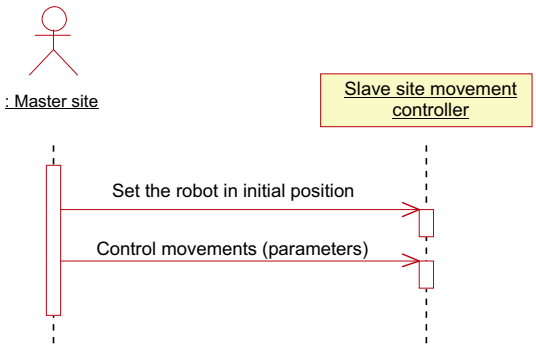

Figure 3 : UML sequence diagram

This approach have been successfully applied to a case study of a system for Robotic Tele-Echography (TER)[9]. TER is a tele-robotic system designed and developed by a French consortium composed of universities, hospitals and industrial companies. The slave robot is tele-operated by an expert clinician who remotely performs the ultrasound scan examination. A virtual probe is mounted on the master interface device. The real probe is placed on the slave robot end-effector. A complete study of safety is presented in [4]. As instance, a simplified sequence diagram is given on figure 3.. Based on this diagram we perform an analysis of one message of this interaction with a FMECA table presented on figure 4. Then, from this analysis, one can propose a solution for this failure mode by the modification of the system UML diagrams. The solution we propose consists in temporarily changing the robot controller state. This can then be modeled with a state diagram.

4. CONCLUSION

Medical robots belong today to safety critical systems. Therefore, their development process must include a risk management activity. Risk analysis is described in medical and generic norms as the core of this activity. The approach we have develop consists to use UML diagrams for the main steps of risk analysis. For the first step, system definition, UML help designers and analysts to identify the use, the boundaries of the the system, the actors and their load of work. Those points are fundamental for the next step: the hazard identification and the risk estimation. For the hazard identification activity it is possible to use UML diagrams with well-known techniques as PHA, FMECA or FTA. This approach permits to have homogeneous models between development process and risk analysis process. This also leads to produce documentation useful for tracability. Indeed, in UML, requirements models are completed during the development and produce the design models. This approach have been applied successfully to the development of a medical robot and will be experimented again in other service robots.

References

[1] 93/42/EEC. Council directive of the 14th of june 1993 concerning medical devices. Journal officiel des Communautés européennes (JOCE) N°L169, 1993.

[2] B. Davies. Safety of medical robots. *ICAR'93*, pages 311–313, 1993.

[3] B.S. Dhillon. *Robot Reliability and Safety*. Springer-Verlag, 1991.

[4] J. Guiochet. *Safety management of service robot systems - UML approach based on system risk analysis (in french)*. PhD thesis, Institut National des Sciences Appliquées de Toulouse, 2003.

[5] J. Guiochet and C. Baron. UML based FMECA in risk analysis. In *Proc. of the European Simulation and Modelling Conference ESMc2003, Naples, Italy*, October 2003. to be published.

[6] J. Guiochet, B. Tondu, and C. Baron. Integration of UML in human factors analysis for safety of a medical robot for tele-echography. In *Proc. of the IEEE/RSJ International Conference on Intelligent Robots and Systems, Intelligent Robots and Systems for Human Security, Health, and Prosperty IROS 2003*, October 2003. accepted.

[7] ISO 14971. Medical devices - Application of risk management to medical devices. International Organization for Standardization, 2000.

[8] ISO/IEC Guide 51. Safety aspects - Guidelines for their inclusion in standards. International Organization for Standardization, 1999.

[9] A. Vilchis, P. Cinquin, J. Troccaz, A. Guerraz, B. Hennion, F. Pellissier, P. Thorel, F. Courreges, A. Gourdon, G. Poisson, P. Vieyres, P. Caron, O. Mérigeaux, L. Urbain, C. Daimo, S. Lavallée, P. Arbeille, M. Althuser, J-M. Ayoubi, B. Tondu, and S. Ippolito. TER: a system for Robotic Tele-Echography. *Lectures Notes in Computer Science, Medical Image Computing and Computer-Assisted Intervention (MICCAI'01)*, pages 326–334, 2001.