# SAFETY ANALYSIS AND INTEGRATION FOR ROBOTIC SYSTEMS - APPLICATION TO A MEDICAL ROBOT FOR TELE-ECHOGRAPHY

J. GUIOCHET*, B. TONDU and C. BARON

Abstract : *Today, as many new application areas for robotic systems emerge, safety is becoming critical. Indeed, service robots, including medical robots, share their working area or have a close interaction with humans. This paper presents a deductive method for safety analysis and integration. This method uses well-known analysis techniques for computer control systems and includes the use of a formal language (Unified Modeling Language) to combine safety analysis with the development process. Each step of the analysis will be presented with a case study of a robot for tele-echography.*

Keywords : *Robot Safety, UML, Medical robot, Tele-Echography.*

## Introduction

Today, as many new application areas for robotic systems emerge, safety is becoming critical. Indeed, service robots, including medical robots, share their working area or have a close interaction with humans. Safety, which already was an important concern for industrial robots [1] is now the major preoccupation. The term "robot safety" may be interpreted as the prevention of damage to the robot itself and its environment, particularly the human component. This

*LESIA, Electrical and CS Eng. Dpt., INSA, 135 Av. de Rangueil, 31077 Toulouse cedex4 France; email : guiochet@insa-tlse.fr

article presents a deductive method for the safety analysis and integration of a robotic system. This method uses well-known analysis techniques for computer control systems but includes the use of a formal language (Unified Modeling Language) to combine safety analysis with the development process. Human factors are presented in the first section, where the contribution of this field to safety is developed. A second section discusses about the assessment of hazards and risks of the whole system. The third section presents the use of assessment methods such as Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) which identify potential unit errors resulting in hazards. The fourth section is about the choices of corrective measures guided by the previous steps. Finally the paper concludes with a discussion about how the steps of this safety analysis follow from each other. Each step of the analysis will be presented with a case study of a system for robotic tele-echography, TER [2]. 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.

# 1. Human Factors for Service Robotics

The term "human factors" may be defined as the discipline that studies the relationship between technology and the human. Most of the studies of this field are combined with cognitive sciences (such as psychology, philosophy, neuroscience, etc.) and are usually made during system analysis. The goals of such studies are to improve safety, quality and production. In order to elaborate a safer design of systems, we just consider a small part of this wide field. A first step is to analyze human performance and interactions with the system to find ergonomic solutions. This identification of interactions leads us to define safety requirements.

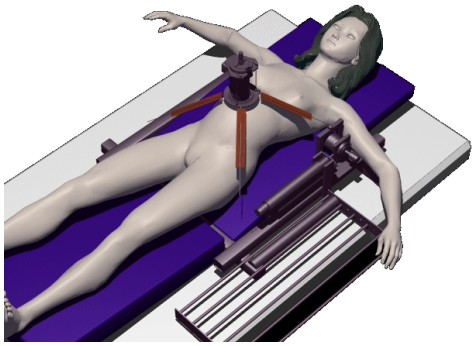

**Figure 1 :** *TER slave robot architecture*

The description of the global scenario (without the robot) allows the analysis of human actions during the examination. Then all the interactions between actors during the robot activity and all the environmental conditions (temperature, illumination, pressure, weight and height of the robot, contacts, etc.) have to be analyzed. This analysis leads to the choice of a parallel structure (Cf. fig.1). The main safety criteria were to limit the work envelope and limit the collisions (which are well-known with robot arms). The difficulty to model the work space (the patient's body), leads to the choice of a compliant slave robot, with an actuation by intrinsically compliant artificial muscles [3]. Position and force information are transmitted bi-directionally. Live visual and audio data are also transmitted in both directions. It is also planned (partly to avoid psychological troubles of the patient) to implement "chat", between the operator and the expert.

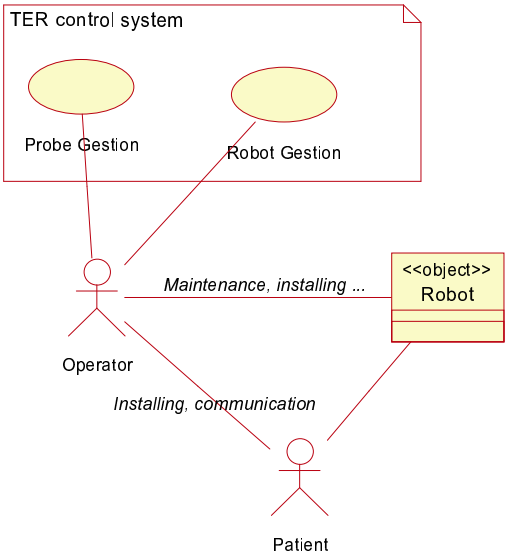


**Figure 2 :** *Example of Use Case Diagram*

A second step is the interpretation of "human errors" (a failure of a human to do a specified action, which results in undesirable outcomes). We proposed to use one of UML (Unified Modeling Language [4]) specification models, the Use Case Diagram (Cf fig.2), to guide this analysis. For each human actor, all the interactions are modelled with a single link. Based on all those links and their specifications, errors an actor can make are determined (with questionnaire, simulations, database or laboratory work). If errors can be classified and their causes identified, then it is possible to propose solutions (this area of research is very well detailed in Reason's book [5]). For example, in our system, the "operator" can fail in installing the patient (positioning) and then provoke abnormal robot movements which can hurt the patient. It can be due to a

| HAZARDS | | |
|---|---|---|
| Physical | Mechanical | Robot pressure on the patient too high, friction on patient body, collision, the robot falls on the patient |
| | Electrical | Electrocution, static electricity |
| Chemical | Toxic air (from artificial muscles), toxic gel (from echography gel) | |

**Table 1 :** *Example of Hazard assessment*

lack of training, a bad examination table, etc. The goal of this analysis is to find ergonomic solutions, specially for interfaces that decrease human errors. But not all the identified human errors can be analyzed, so these data have to be integrated in the FTA step (mentioned later), to determine exactly their consequences and their implications in the system safety. The next phase is to determine the whole system hazards.

## 2. Hazard and risk assessment

A hazard can be defined as a scenario that results from an unwanted transfer or blockage of energy or material, which results in damage to persons, objects or processes. The aim of this step is to make an inventory of all the hazards of the system, estimate their severity and their probability of occurrence, and then calculate the associated risk (defined as the product of those two factors). For each application domain, norms usually guide the assessments. In our study we choose four levels of severity: catastrophic (death or total destruction), hazardous (injury), moderate (inconvenience), minor (defect just noticed). A matrix is usually used to calculate the hazard risk level depending on those four levels and on the hazard probability. Results can be presented in tables, with an extra box for comments or ideas for solutions. All the hazards can be classified (Cf. table 1) according to their energy source (mechanical, electrical, climatic, etc.).

This assessment help designers to analyze the main risks and consider the general risk level of the system. First, the highest risks can be treated, reduced and then reassessed. This

analysis cannot be exhaustive, and the hazard table is completed during the following steps.

# 3. Analytical methods

Analytical methods imply to use dependability concepts applied to robotics. We proposed to use the terminology of [6] At this step of analysis first models of the system should have been made. Fault prevention, increasing safety, is provided by formal specification, conception method and patterns. The UML semantic provides some rules and guidelines in order to decrease the risk of errors. We have chosen to use both FMEA (Failure Modes and Effects Analysis) and FTA (Failure Tree Analysis), because they are very expressive and complementary . They are also widely used in robotics [7, 8, 9].

## 3.1. Failure Modes and Effects Analysis (FMEA)

FMEA is a method used for the identification of potential errors (failure modes) of the examined object (system, segment, software/hardware unit) in order to define and classify their effects (failures) with regard to criticality (also called Failure Modes, Effects and Criticality Analysis). This is to prevent faults (causes of failure) and thus weak points in the design which might result in danger to or loss of the system or persons. Secondly, the FMEA is also to furnish results for corrective measures, and for the determination of operating and application conditions of the system. Each failure mode (the way the component fails) is analyzed, and effects on the system are assessed. This analysis should lead to hazards previously identified. If this is not the case, new hazards have to be added to the data of the previous step and the risks have to be assessed. Those two steps are complementary, the first considers the global system whereas the second analyzes system unit failures that could lead to hazards. Different models are necessary to perform this study, and each designer has to provide models from his domain: electronic, electrical, computer and mechanical. Figure 3 illustrates a part of the electronic components of the TER controller with a "Deployment Diagram". Electric parts can also be integrated in this diagram. For software units, a "Component Diagram" is suit-

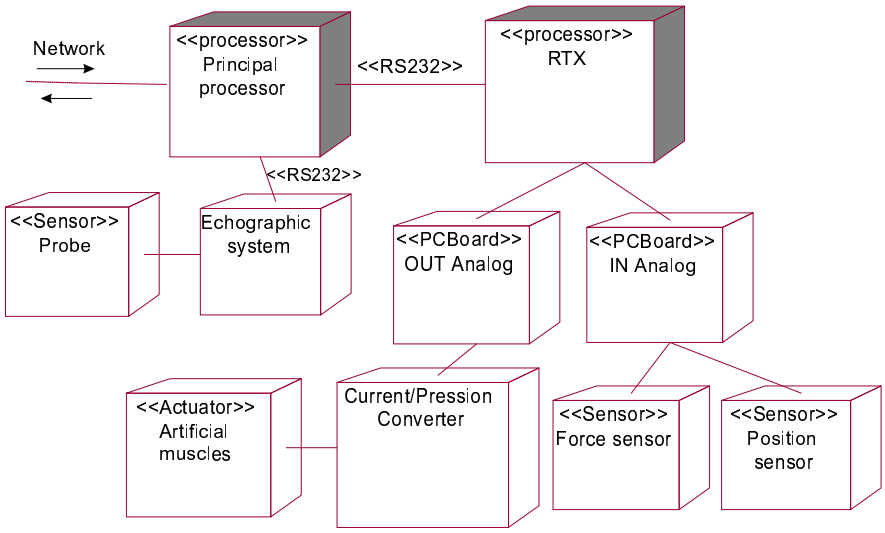


**Figure 3 :** *Deployment diagram of the TER slave controller*

able. The mechanical part can be modelled with an "Object Diagram". The database resulting from the FMEA can be modified at any time in the process and is directly used in the FTA.

## 3.2. Fault Tree Analysis (FTA)

FTA synthesizes data from FMEA and takes into account the combinations of events leading to hazards (identified during the hazard and risk assessment). It is a top-down approach to failure analysis starting with an undesirable event called a *top event*, and then determining how this top event can be caused by individual or combined lower level failures or events. Whereas in the FMEA it was important to distinguish different domains, in FTA, failures and events from different fields are combined. Logical relations between them are represented by logic symbols (AND and OR gates). In a safety analysis, the top event is a hazard that must have been foreseen and thus identified by the previous techniques. FTA can be quantitative, indeed if all the failure probabilities can be assessed then the frequency of the top-event can be calculated (usually for electronics), but in most cases it is impossible, and a qualitative analysis is done. First, a tree can be just represented with the failure interactions, and second, events (including human errors) and protection mechanisms can be integrated. The goal of the qualitative analysis is to find the *minimal cut sets* (relationship between the top event and

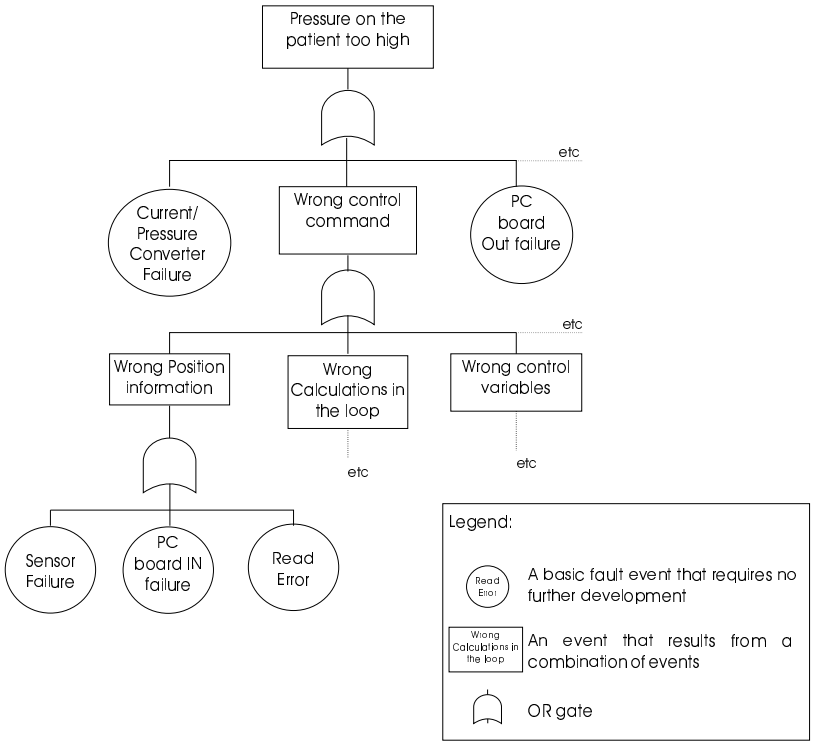


**Figure 4 :** *Example of FTA for the TER slave application*

the primary events) which represent the basic events that will cause the top event and which cannot be reduced in number. Figure 4 shows a part of the fault tree for the top event "robot pressure on the patient too high".

# 4. Choices of safety measures

All the corrective measures proposed during the previous steps have to be considered in this step. We propose a list of different points that should be considered:

1. Definition of the ideal behavior of the system and its fail-safe states (using UML State Diagram). Choices of putting the system in a fail state must be later introduced in the "solutions" column of the FMEA tables. It is also directly linked with the error messages transmitted to the Human-Machine Interface.

2. Choices of the start and stop procedures (modelled with an "Activity Diagram").

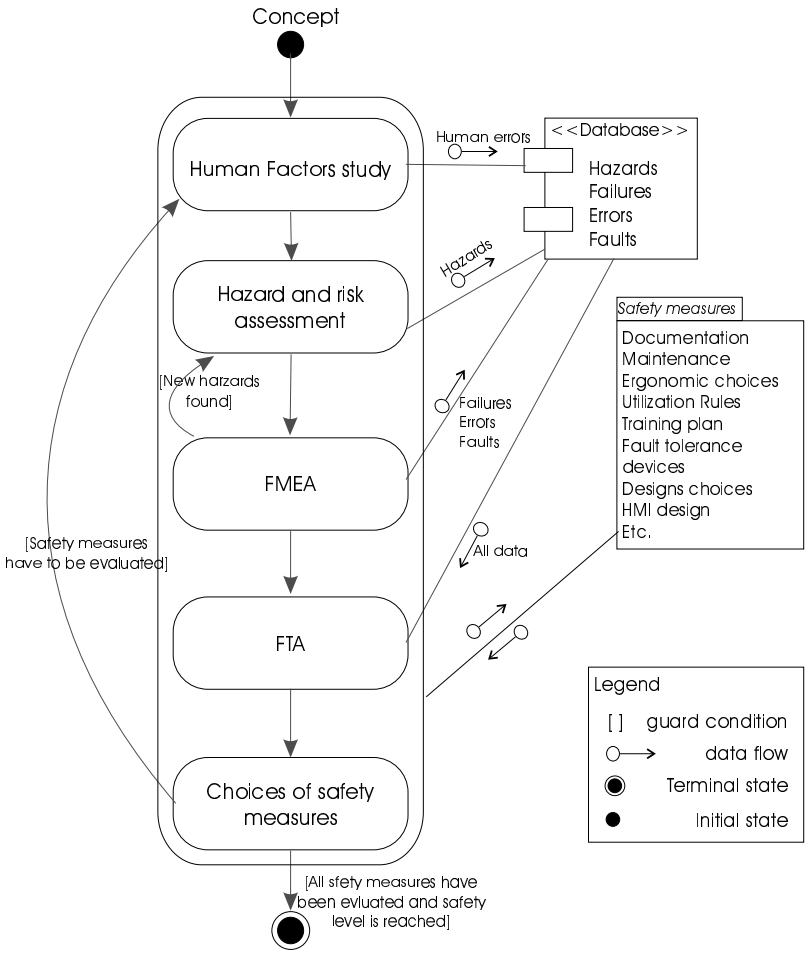


**Figure 5 :** *Safety process*

3. Choices for direct design means (modifications, fault tolerant mechanisms, etc.), indirect (as protections) and descriptive measures (use restriction, use redefinition, etc.).

4. Considerations on the Human-Machine Interface design (specially for the error message queue [10]).

5. Choice of measures different from design ones (maintenance, documentation, training plan, etc.).

Then each measure has to be evaluated with the previous steps, going back to the first analysis, to evaluate whether the safety measures are coherent with human factors. Then it is important to assess if the new introduced measures can be a source of hazards. The specification models of new mechanisms are used in the FMEA and the FTA, to identify the

unit failures. How the steps interact is represented in figure 5. During the process phases, database are made, and they furnish at the end a complete safety documentation.

# Conclusion

A lot of techniques for safety analysis are already known and experimented in various engineering domains (aerospace, electronics, and nuclear industries). Service robotics is also a field where safety has became critical. And nowadays, robot control complexity requires the utilization of software engineering techniques. This is the reason why we think that a safety process has to be mixed with a classical development process, using the same language. We have chosen the object oriented language UML for its fault prevention characteristics (exposed in a comparison with a top-down functional decomposition in [11]), and for its expression power in the robotics field [12]. This process can be used at the very beginning of the development to help to choose safety measures, but can be reused at any moment. Analytical methods, which we based on the UML system models, first permit fault removal and fault forecasting. Secondly, fault tolerance mechanisms can be introduced. The final point of this process lies in the direct use of the design documentation to evaluate the safety of the system. A first application on the design of a Tele-Echography Robot (TER) has shown that this process help in the choice of good safety measures, and furnish an evaluation of safety level. In a next application, an anthropomorphic arm actuated by artificial muscles, we will experiment the complete association between the controller development (in UML) and the safety process.

# References

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

[2] 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)*, 2001.

[3] B. Tondu and P. Lopez, "Modeling and control of McKibben artificial muscle robot actuators", *IEEE Control Systems*, vol. 20, no. 2, pp. 15–38, 2000.

[4] G. Booch, J. Rumbaugh, and I. Jacobson, *Unified Modeling Language Users Guide*, Addison Wesley Longman, 1999.

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

[6] J-C. Laprie, *Dependability: Basic concepts and terminology in English, French, German, Italian and Japanese*, vol. 5 of *Dependable Computing and Fault Tolerance*, Springer-Verlag, Austria, 1992.

[7] B.S. Dhillon and A.R.M. Fashandi, "Safety and reliability assessment techniques in robotics", *Robotica*, vol. 15, pp. 701–708, 1997.

[8] K. Khodabandehloo, "Analyses of robot systems using fault and event trees: case studies", *Reliability Engineering and System Safety*, vol. 53, pp. 247–264, 1996.

[9] I. Walker and J. Cavallero, "Failure mode analysis for a hazardous waste clean-up manipulator", *Reliability Engineering and System Safety*, vol. 53, pp. 277–290, 1996.

[10] N.G. Leveson, *Safeware - System safety and computers*, Addison-Wesley, Univesity of Washington, 1995.

[11] L. Caroll, B. Tondu, C. Baron, and J.C. Geffroy, "Comparison of two significant development methods applied to the design of real-time robot controllers", *IEEE International Conference on Systems, Man and Cybernetics (SMC'98)*, pp. 3394–3399, October 1998.

[12] L. Carroll, *Vers la maîtrise du développement d'un contrôleur temps réel sûr de fonctionnement pour les robots manipulateurs*, PhD thesis, Institut National des Sciences Appliquées de Toulouse, 1999.