HAL
open science

Applying Existing Standards to a Medical Rehabilitation Robot: Limits and Challenges

Jérémie Guiochet, Quynh Anh Do Hoang, Mohamed Kaâniche, David Powell

To cite this version:

Jérémie Guiochet, Quynh Anh Do Hoang, Mohamed Kaâniche, David Powell. Applying Existing Standards to a Medical Rehabilitation Robot: Limits and Challenges. Workshop FW5: Safety in Human-Robot Coexistence & Interaction: How can Standardization and Research benefit from each other?, IEEE/RSJ Intern. Conference Intelligent Robots and Systems (IROS2012), Oct 2012, Vilamoura, Portugal. hal-01282195

HAL Id: hal-01282195

https://hal.science/hal-01282195v1

Submitted on 8 Mar 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Applying Existing Standards to a Medical Rehabilitation Robot: Limits and Challenges

Jérémie Guiochet [1,2], Quynh Anh Do Hoang [1,2], Mohamed Kaâniche [1,2] and David Powell[1,2]

***Abstract*— Considering the new threats in medical robotics due to increasing complexity and autonomy, and the absence of dedicated standards, we present in this paper how we carried safety analyses for a rehabilitation robot. We combine several standards and research works for a safe design and to construct a safety case for regulatory bodies. We point out some challenges for standardization and future research.**

***Index Terms*— Robot safety, rehabilitation robot, walking assistant, safety standards, risk analysis, safety case, GSN**

I. Introduction

While removing fences around industrial robots, developers were at first working on functions of innovative applications (service or advanced robots) without considering safety. This phenomenon is now counterbalanced by the increasing demand of users and researchers to take those robots out of the laboratories and into real-life situations. It is now mandatory that such systems should be trusted both by users and regulatory bodies. As complexity and autonomy of robots increase, new threats appear. Two main issues stand out: how to design a safe robot? and how to construct an argument that the robot is indeed safe? For many domains, both issues are treated by directly applying standards that give guidelines on how to design a system (usually in the form of checklists), and give the assurance to regulatory bodies that the system is safe. In the domain of service robotics, and more particularly in medical robotics, there is no single standard that addresses all issues. In this paper, we present how we applied several standards to the development of a medical rehabilitation robot, and what we had to develop when standards were inapplicable. We first present the robot in Section II, and how standards have been applied in section III. Sections IV and V present the challenges for standardization and our conclusion.

II. The rehabilitation robot MIRAS

MIRAS [23] (Multimodal Interactive Robot for Assistance in Strolling), is an assistive robot for standing up, sitting down and walking, and also capable of health-state monitoring of the patients. It is designed to be used in elderly care centers by people suffering from gait and orientation problems where a classic wheeled walker (or "rollator"), such as in Figure 1(a), is not sufficient for patient autonomy. The robotic rollator is composed of a mobile base and a moving handlebar (Figure 1) and is equipped with several sensors to detect physiological parameters and the posture of the patient. It can also autonomously move when the patient summons it with a movement of his/her hand ("hello" function).

III. Application of standards and safety argumentation

In the European Community, the only requirement for certification is to be compliant with EC directives. The application of ISO-standards is not mandatory, but it is of course a strong argument when requesting certification. It is also sometimes a mandatory requirement expressed by customers.

A. Machinery or Medical Device European Directives

At the top level of standardization, the European Council defines directives, defines high level requirements for certification of systems. In the MIRAS project, the robotics constructor, Robosoft[1], was used to applying the Machinery Directive 2006/42/EC [1] for all its service robots when no standard was applicable (e.g., for autonomous vehicles). Nevertheless, after discussions with the French medical regulatory body (ANSM[2]), it was required that the system be classified as a Class IIa Medical Device, as defined in the Directive on Medical Devices [2], and it was highly recommended that a request for authorization for clinical trials be sent to this agency. This procedure focusses on protecting the patient and not on how the tests are carried out. A first impact of this choice, is that standards on non-medical robots such as ISO10218 [11] and ISO 13482:2012 [16] do not apply to our system. All ISO standards about Medical Device can then be applied. We focus on this paper on the most interesting ones for our application (for instance we do not study standards about electrical equipment (IEC60601-X) that could be applied).

B. Rollator and wheelchair standards

One characteristic of the robot is that it is designed to replace, and increase efficiency of, a classic rollator (walking frame with wheels). In this case, a classic rollator standard, the ISO 11199-2:2005 [12], exists but many parts cannot be applied to the robotic rollator. For instance, many tests are specified for the 2 types of brakes, on the handles during strolling, and a general test for parking the device. In the case of the robotic rollator, there are no handle brakes since the targeted profile of patients do not have the ability to use

[1]CNRS, LAAS, 7 av. du colonel Roche, F-31400 Toulouse, France {name}@laas.fr
[2]Univ. Toulouse, LAAS, F-31400, Toulouse, France

[1]http://www.robosoft.com
[2]French national agency for safety of medicine and health products, http://ansm.sante.fr/

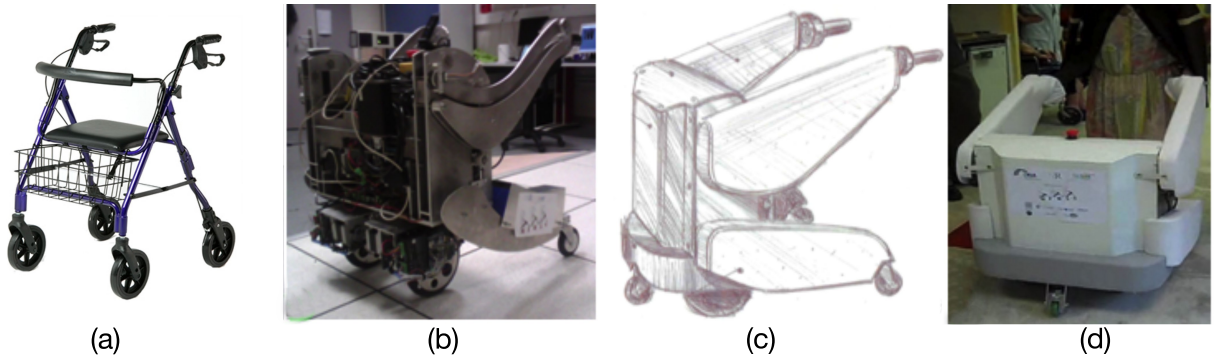

Fig. 1. (a) Classic "Rollator", (b) MIRAS experimental robot, (c) Design with packaging (d) Prototype during clinical investigation

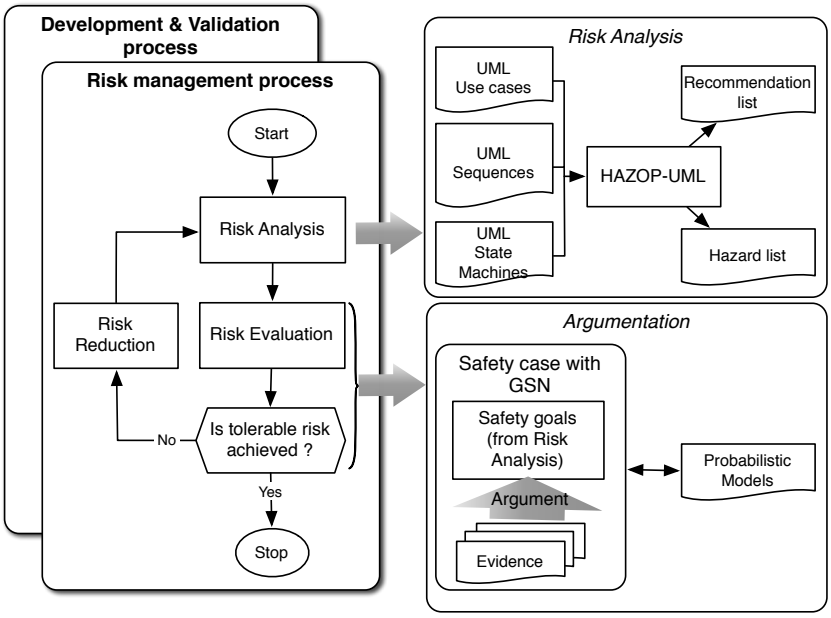

Fig. 2. Risk management and safety case in our safety analysis process

brakes. The robot moves only if a force is applied on the handles. Nevertheless, we selected all guidelines and tests that were applicable to MIRAS (e.g., stability tests), which correspond to about 40% of the standard. The wheelchair standard, ISO 7176-5:2008 [15] was also considered, but only to define robot dimensions that are compatible with a hospital environment.

C. Risk management standards and safety case construction

All safety standards now have a common basis for risk management which is the ISO Guide 51 [18][3]. This standard is then developed in a generic one, the ISO31000:2009 [14], and also included in several domains, from industrial machines (ISO12100:2010 [13]) to medical devices (ISO14971:2006 [17]). We aimed to be 100% compliant with this standard.

Risk management is the overall activity aimed at achieving a tolerable level of risk (see left-hand part of Figure 2). It is actually rare to carry out a complete and reliable estimation of risks. Indeed, data about failure rates is often incomplete due to the novelty of innovative technologies, new software functions for perception for instance, and there is little or no data on robot-human interaction errors. Nevertheless, we developed an approach based on this process [21], [22], [7], [6], combining UML (Unified Modeling Language) [24] and HAZOP (Hazard Operability) [9] in order to identify hazards (see left-hand part of Figure 2).

We have experienced that UML diagrams, used to describe the system and human-robot interactions, were easily understandable by non UML experts coming from the robotics and medical domains. Several use cases and scenarios were developed in concert with the domain experts and the resulting models then served as the basis of a deviation analysis using an adapted version of HAZOP. This led to 397 possible deviations classified in 16 hazard classes. Both UML modeling *per se* and the HAZOP analysis gave rise to general recommendations to enhance safety. Recommendations were fed back to the system developers at the user level (e.g., a

[3]Note that a new one dedicated to safety concepts for medical devices has recently been published, ISO Guide 63:2012 [19]

Severity Levels	
Level	**Description**
Catastrophic	Leads to patient's death
Critical	Leads to permanant deficiency or an injury putting in jeopardy patient's life
Serious	Leads to an injury (a) requiring intervention of health professionnal or (b) causing patient's loss of confidence in the system (with possible psychological impact)
Minor	Leads to a temporary injury (a) not requiring intervention of health professionnal or (b) causing medical staff to have less confidence in the system
Negligible	Causes annoyance or inconvenience

Fig. 3. Severity levels in MIRAS

Likelihood levels	
Level	**Occurrence frequency**
Extremely Frequent	~ once a week
Frequent	~ once in a month
Probable	~ once every 6 months
Occasional	~ once a year
Remote	~ once every 10 years
Improbable	~ once every 100 years
Incredible	less than once every 100 years

Fig. 4. Frequency of occurrence levels in MIRAS

new procedure for sitting on a chair), the specification level (e.g., the first prototype did not include an integrated seat), and the design level (e.g., a heartbeat mechanism to regularly check the state of the robot and send an alarm to the medical staff in case of robot malfunction).

By definition, risk estimation should consist in estimating the severity and probability of occurrence of each potential harm. For that, analysts need to use probabilistic or ordinal scales. Some standards define such scales as examples, but there are none for robotic systems used in medical applications. Hence we collaborated with the doctors of three hospitals involved in the MIRAS project to establish a severity ranking scale that is suitable for the application context of the assistive robot considered in our study. For severity ranking, we first adapted a scale presented in ISO14971 [17], and asked the doctors to estimate the severity level of the identified hazards. This led to a redefinition of levels as presented in Figure 3, adding an important dimension with respect to other such tables: the loss of confidence in the robot. Even if this is not directly related to safety, the psychological impact on the patients and the medical staff is of great importance.

The second dimension of risk, frequency, was addressed at the same time as risk acceptance levels. We proceeded as follows: we defined three levels of acceptance according to the ALARP principle (which states that risk must be reduced to a level that is As Low As Reasonably Practicable) [8]: *unacceptable* (risk cannot be justified except in extraordinary circumstances), *tolerable* (tolerable only if further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained) or *acceptable* (negligible risk). Then we asked doctors from 3 different hospitals to assess for each hazard, at which frequency (according to the scale defined in Figure 4) the investigated hazard could be considered acceptable, tolerable or unacceptable.

This led us to define precisely both likelihood levels and risk levels. The result is presented in Figure 5 (the HN numbers appearing in this figure will be explained later).

As presented before, the answer to the question "is tolerable risk achieved" should be based on a formal demonstration or at least a well-structured argumentation. Using such a matrix was easy for the clinical investigations procedure. Indeed, we reduce functionalities of the robot, and change the context of use, i.e., all patients are supervised by a medical expert and a robot expert is standing by ready to press the emergency stop. Without detailing the argumentation we were able to demonstrate that for each risk the level was tolerable or acceptable. Hazards identified in Figure 6, presented in the new paragraph, are noted HNx in Figure 5. For the analysis of the system for its final use, it is quite impossible to estimate the right frequency of all the risks. This matrix is thus not useful to answer the question of residual risk. For this reason, we propose to use an argumentation process, supported by evidence, to justify that an acceptable level of risk has been achieved. The question "Is tolerable risk achieved?" in the risk management process is supported by a structured argumentation, also called a Safety Case [3], [5] (see right-hand part of Figure 2). The argumentation with a safety case can be carried out using the Goal Structuring Notation (GSN) [20].

A first goal to be assessed was to compare the assistive robot to a classic rollator (also called frame walker). If the robot shows higher performance from the safety perspective compared to a traditional robot, the project would be considered successful. Hence, we have set as top-goal G1 the claim that: "The MIRAS robot is at least as safe as a classical rollator" (Figure 6). This goal is broken down into sub-goals through two strategies: we argue safety claims with respect to, on one hand, risks induced by the robot technology and, on the other hand, risks that are equally relevant to a classic rollator.

In our case, we had 16 subgoals stated as "Hazard HNx has been addressed". Then, for all subgoals, we identified various pieces of evidence according to the sub-goal to be solved: test results, estimation of fault detection coverage and compensation efficiency, proof of correct implementation of code, failure rate of physical components, compliance with standards, etc. We identified a total of 44 pieces of evidence to be collected.

D. Software Standards

Software failures in our system could be an important source of hazardous situations. Due to the difficulty of quantifying software failure rate for critical applications [4], it is not possible to estimate the probability of a risk to judge whether or not it is acceptable. The general approach in many standards is thus to specify some methods and techniques used to develop the software, that, when applied correctly, increase the level of confidence that can be attributed to the software. The medical software standard [10], suggests

Severity \ Frequency	Incredible	Improbable	Remote	Occasional	Probable	Frequent	Extremely Frequent
Catastrophic							
Critical							
Serious			HN8 HN9				
Minor			HN11	HN6			
Negligible			HN3	HN5	HN13 HN12 HN7	HN1	

Acceptable Tolerable Not acceptable

Fig. 5. Elicited risk acceptability matrix, with hazard numbers for prototype clinical investigations

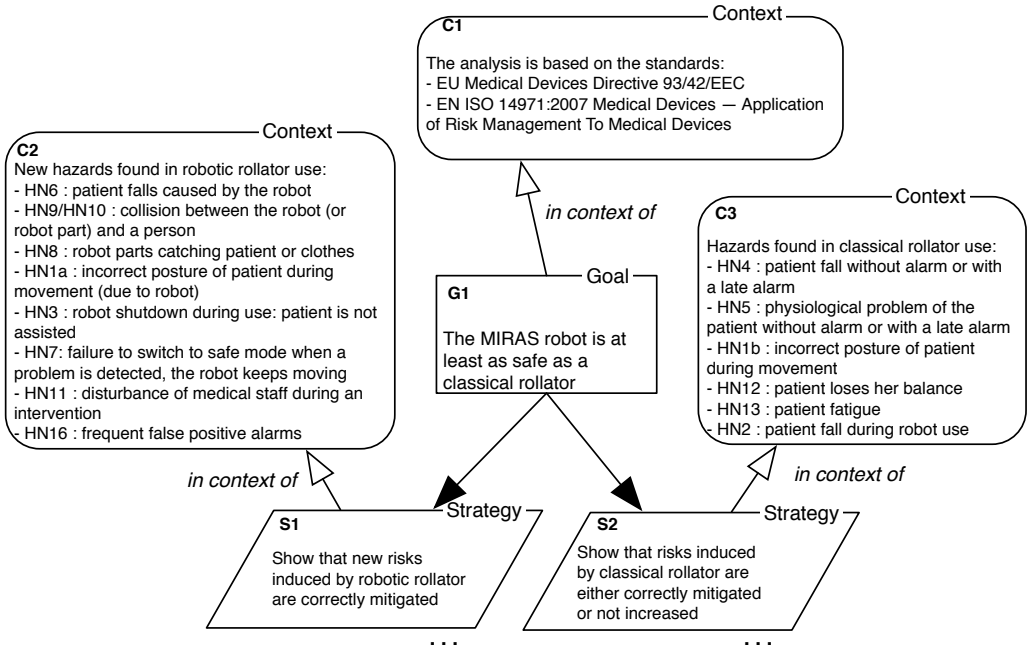

Fig. 6. The High Level Goal Structure of MIRAS robot

a severity ranking system based on patient injuries that can induce a failure of the software with three levels: A (No injury or damage to health), B (Non-serious injury is possible) and C (Death or serious injury is possible). As the standard prescribes neither a process model nor particular software engineering methods to accomplish the normative requirements, we defined a mapping between this severity ranking and the Safety Integrity Level (SIL) of IEC 61508 [8] (Figure 8), which is a very thorough catalogue and categorization of software methods and techniques. Four levels are defined in this standard (1 to 4, the highest being for the most critical software), but in the context of the assistive robot, it seems reasonable to consider that the highest SIL should not exceed SIL3, the highest direct harm being a patient fall (and not death). This helped us to select techniques for software development, depending on the level of the risk concerned by the software component.

Class	Description
A	No injury or damage to health is possible
B	Non-serious injury is possible
C	Death or serious injury is possible

Fig. 7. Severity ranking from IEC 62304

Severity	Class by IEC 62304	SIL by IEC 61508
Catastrophic	C	3
Critical	B	2
Serious	B	2
Minor	A	1
Negligible	A	0

Fig. 8. Relations between IEC 61508 and IEC 62304

IV. Challenges

Standardization for medical rehabilitation robots

There is no standard for rehabilitation robots as a medical device. Such a standard, as for other domains of service robotics, should include risk analysis methods, examples of ranked levels for severity and frequencies, general safety requirements, as well as measures, tests, safeguards, checklists, etc.

Clinical trials as part of the development process

It would also be interesting to have a standardized way to integrate clinical trials in the development of rehabilitation robots. During the MIRAS project, several prototypes were designed, and each time the clinical trials gave rise to numerous important modifications.

Building a safety case

As in other safety critical domains, a safety case is needed. This could be formalized in a standard. Research is needed on the notion of uncertainties which are inherent part of risk analysis and in the establishment of safety case. In the same way as residual risk, which should be estimated and evaluated as acceptable, residual uncertainties in the safety case should be identified, estimated and evaluated to be judged as acceptable or not.

Social and political issue

In many countries (including France), part of the cost of a Medical Device is supported by national health insurance. Knowing that the price of a rehabilitation robot could be rather high, there could be an impact on whether or not to define some such robot as a medical device. In turn, this could impact the scope of future standards and their adaption in national standards.

V. Conclusion

Even if it was not mandatory, we explored which ISO-standards where applicable in the development of the MIRAS robot. Once this system was defined as a medical device according to the EC directive, the only standard fully applicable was the risk management one (ISO14971) as presented in Figure 9. All other standards were used as a knowledge base for defining robot dimensions, stability requirements, tests, software analysis and development techniques. Of course, this is not satisfactory for robot designers and manufacturers, who are interested in communicating about a complete compliance with standards. This led us also to point out some challenges for standardization and research. We are now working on the problem of dealing with uncertainties in safety cases for autonomous systems, which is a critical issue for certification. As an example, for a critical application, IEC61508 does not recommend the use of artificial intelligence techniques, which shows the low level of confidence accorded to autonomy software by regulatory bodies.

Standard number	Domain	Estimated Applicability to MIRAS
93/42/EEC - Medical Devices Council Directive	Medical	100%
ISO 14971:2007 - Risk management	Medical	100%
ISO 11199-2:2005 - Rollators	Medical	40%
ISO 62304:2006 - Medical Software	Medical	20%
IEC 61508ed2:2010 - Safety of Electrical/Electronic/Programmable Electronic	Generic	5%
2006/42/CE - Machinery Council Directive	Generic	N/A
ISO10218:2011 - Safety of industrial robots	Robotics	N/A
ISO 13482:2012 - Safety of personal care robots	Robotics	N/A

Fig. 9. Application of standards in the MIRAS project

Acknowledgements

This work was partially supported by MIRAS, a project funded under the TecSan (Technologies for Healthcare) program of the French National Research Agency (ANR) and SAPHARI, a project funded under the 7th Framework Program of the European Union.

References

[1] 2006/42/EC: Directive 2006/42/ec of the european parliament and of the council of 17 may 2006 on machinery. Journal Officiel des Communautés Européennes (JOCE) NL157 (2006)

[2] 93/42/EEC: Council directive of the 14th of june 1993 concerning medical devices. Journal Officiel des Communautés Européennes (JOCE) NL169 (1993)

[3] Bishop, P., Bloomfield, R.: A methodology for safety case development. In: Safety-Critical Systems Symposium,Birmingham, UK (1998)

[4] Butler, R.W., Finelli, G.B.: The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software. IEEE Transactions on Software Engineering 19(1), 3–12 (1993)

[5] DefStan00-56: Defence standard 00-56 issue 4: Safety management requirements for defence systems. Ministry of Defence, UK (2007)

[6] Do Hoang, Q.A., Guiochet, J., Kaaniche, M., Powell, D.: Human-robot interactions: model-based risk analysis and safety case construction. In: Embedded Real Time Software and Systems (ERTS2012), Toulouse, France (2012)

[7] Guiochet, J., Martin-Guillerez, D., Powell, D.: Experience with model-based user-centered risk assessment for service robots. In: IEEE International Symposium on High-Assurance Systems Engineering (HASE2010). pp. 104–113. IEEE Computer Society, San Jose, CA, USA (2010)

[8] IEC61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission (Ed 2, April 2010)

[9] IEC61882: Hazard and operability studies (HAZOP studies) – Application guide. International Electrotechnical Commission (2001)

[10] IEC62304: Medical device software - software life cycle processes. International Organization for Standardization (2006)

[11] ISO10218: Robots and robotic devices ? safety requirements for industrial robots. International Organization for Standardization (2011)

[12] ISO11199-2:2005: Walking aids manipulated by both arms – requirements and test methods – part 2: Rollators. International Standard Organisation (2005)

[13] ISO12100: Safety of machinery – general principles for design – risk assessment and risk reduction. International Organization for Standardization (2010)

[14] ISO31000: Risk management - Principles and guidelines. International Organization for Standardization (2009)

[15] ISO7176-5: Wheelchairs – part 5: Determination of dimensions, mass and manoeuvring space. International Organization for Standardization (2008)

[16] ISODIS13482: Robots and robotic devices – Safety requirements for non-industrial robots – Non-medical personal care robot. International Organization for Standardization (2012)
[17] ISO/FDIS14971:2006: Medical devices - Application of risk management to medical devices. International Standard Organisation (2006)
[18] ISO/IEC-Guide51: Safety aspects - Guidelines for their inclusion in standards. International Organization for Standardization (1999)
[19] ISO/IEC-Guide63:2012: Guide to the development and inclusion of safety aspects in international standards for medical devices. International Organization for Standardization (2012)
[20] Kelly, T.P.: Arguing Safety – A Systematic Approach to Managing Safety Cases. Ph.D. thesis, University of York (1998)
[21] Martin-Guillerez, D., Guiochet, J., Powell, D.: Experience with a model-based safety analysis process for an autonomous service robot. In: IARP Workshop on Technical Challenges for Dependable Robots in Human Environments (DRHE 2010), Toulouse, France. pp. 1–8 (2010)
[22] Martin-Guillerez, D., Guiochet, J., Powell, D., Zanon, C.: UML-based method for risk analysis of human-robot interaction. In: International Workshop on Software Engineering for Resilient Systems (SERENE2010), London, UK (2010)
[23] MIRAS: Multimodal Interactive Robot for Assistance in Strolling. Project supported by the French ANR (National Research Agency) under the TecSan (Healthcare Technologies) Program (ANR-08-TECS-009-04), http://www.miraswalker.com/index.php/en
[24] OMG-UML2: OMG Unified Modeling Language (OMG UML), Superstructure, V2.1.2. Object Management Group, formal/2007-11-02 (2007)