Grant Agreement number:288899

Project acronym: Robot-Era

Project title: Implementation and integration of advanced Robotic systems and intelligent Environments in real scenarios for ageing population

Funding scheme: Large-scale integrating project (IP)

Call identifier: FP7-ICT-2011.7

Challenge: 5 – ICT for Health, Ageing Well, Inclusion and Governance

Objective: ICT-2011.5.4 ICT for Ageing and Wellbeing

Project website address:www.robot-era.eu

D7.2
Guidelines for integrating hardware and middleware solutions for dependability of Robot-Era services

Due date of deliverable: 31/10/2012
Actual submission date: 07/02/2013

Start date of project: 01/01/2012 Duration: 48 months

Organisation name of lead contractor for this deliverable: SSSA
Deliverable author: Massimo Filippi, Filippo Cavallo, Christian Martin, Giancarlo Teti, Alessandro Di Nuovo, Franz Broz and Daniel Duma

Version:1.8

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Service)	
RE	Restricted to a group specified by the consortium (including the Commission Service)	
CO	Confidential, only for members of the consortium (including the Commission Service)	

Document History

Version	Date	Author	Summary of Main Changes
1.0	23-02-2012	Filippo Cavallo (SSSA)	First version of the template for Robot-Era Deliverables
1.1	19-11-2012	Massimo Filippi (SSSA)	Structure of the document; Introduction, Section 2 and inputs on the other sections.
1.2	04-12-2012	Massimo Filippi and Filippo Cavallo (SSSA)	Minor revisions
1.3	07-12-2012	Christian Martin (MLAB)	Contributions on Domestic and Condominium Robots (Sections 3.1 and 3.2)
1.4	03-01-2013	Massimo Filippi (SSSA)	Minor revisions
1.5	10-01-2013	Giancarlo Teti (RT)	Contribution on Outdoor Robot (Section 3.3)
1.6	15-01-2013	Alessandro Di Nuovo, Franz Broz and Daniel Duma (UOP)	Contribution on dependability on the user interaction of Condominium Robot (Section 3.2.1)
1.7	06-02-2013	Annes Bistry (UHAM)	Contribution on Robotic Arm for Manipulation (Section 3.1.1)
1.8	**07-02-2013**	**Massimo Filippi (SSSA)**	**Final submitted version**

Table of Contents

Executive summary

This Deliverable introduces the dependability of Robot-Era system and services. The term "dependability" is a system concept that integrates such attributes as reliability, availability, safety, confidentiality, integrity, and maintainability. The goals behind the concept of dependability are the abilities of a system to deliver a service that can justifiably be trusted, and to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the user.

Since in the Robot-Era project different robotic platforms and devicesare installed in different environments (public and private spaces, living labs and residential sites), it's crucial to focus and enhancing all the dependabilityaspects, in order to assure a high level of safety and availability.

First and foremost, service robotics requires that dependable robot systems be deployed to operate in human-inhabited environments. Second, service robots must fulfill their tasks with adequate performance and robustness in dynamic and unpredictable environments. For mobile robots, the safety requirement is particularly relevant, since the robot actively engages the environment and hence bears full responsibility in case of hard contact with people or objects.

The standard definition of dependability, provided by Laprie, is conceived in particular for computer systems, and it's not completely suitable for the service robotics. We propose a new definition of dependability, extending the concept toward new attributes and considering two main different blocks, technical and human factors.

Dependability must be obtained for each single component of a robot and for the whole system, which, designed to fulfill a certain task, might be more than just a sum of its components.

In the Robot-Era project, the dependability of the servicesdepends on each robots and the Ambient Intelligence. In this work we define and analyze all dependability attributes in a modular approach, for each component of the overall system, first of all the three robotic platforms (domestic, condominium and outdoor robots) and the Ambient Intelligence.

In the section 3 the dependability of the tree robotic platforms is described, with particular attention to the safety attribute, and in the section 4 is described an evaluation of the robot-Era AmI. The architectures and technical aspects discussed in this document are intentionally not described in depth. Each Robot-Era robot platform is discussed in Deliverables D4.1, D5.1 and D6.1, respectively.

In the last section, for each attribute of dependability, we propose a list of variables and metrics in order to evaluate and quantify the dependability of Robot-Era services, during the experimental loops.

1 Introduction

Dependability, defined as the property of a system by which it can be "depended on" or "trusted on", is the combination of a number of factors, such as safety, robustness and reliability, weighted by specific working environment [1-2].

The term "dependability" is a system concept that integrates such attributes as reliability, availability, safety, confidentiality, integrity, and maintainability. The goals behind the concept of dependability are the abilities of a system to deliver a service that can justifiably be trusted, and to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the user(s) [3].

The service delivered by a system is its behavior as it is perceivedby its user(s); a user is another system (physical, human) that interacts with the former at the serviceinterface. The function of a system is what the system is intended to do, and is described by thefunctional specification.

In 1985, Laprie defined dependability "as the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers. The service delivered by a system is its behavior as it is perceptible by its user…" [4].

Furthermore, Laprie provides a scheme of dependability components, such as impairments, affecting dependability, means, for pursuing dependable systems, and attributes, composing dependability, as shown in the dependability tree in Figure 1.

Depending on the specific application context, more emphasis has to be put on each of the attributes included in the concept of dependability.

A systematic exposition of the concepts of dependability consists of three parts: the threats to, theattributes of, and the means by which dependability is attained, as shown in Figure 1.

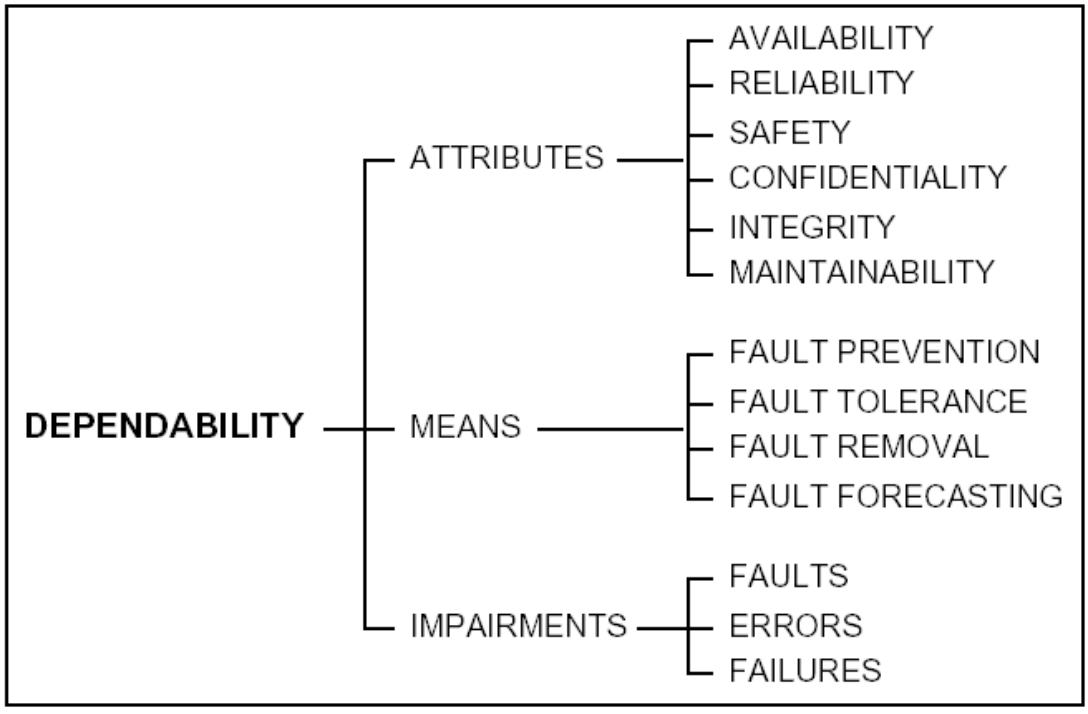

Figure 1. The dependability tree (Laprie)

So, dependability is an integrative concept that encompasses the following basic attributes:

- Availability: readiness for correct service;
- Reliability: continuity of correct service;
- Safety: absence of catastrophic consequences on the user(s) and the environment;
- Confidentiality: absence of unauthorized disclosure of information;
- Integrity: absence of improper system state alterations;
- Maintainability: ability to undergo repairs and modifications.

Several other dependability attributes have been defined that are either combinations or specializations of the six basic attributes listed above. Security is the concurrent existence of availability for authorized users only, confidentiality, and integrity with 'improper' taken as meaning 'unauthorized'. The availability is always required, although at different levels, but the other components may or may not be required, depending on the application [5].

Integrity is a prerequisite for availability, reliability and safety, but may not be so for confidentiality(for instance attacks via covert channels or passive listening can lead to a loss of confidentiality,without impairing integrity).

The definition given for integrity (absence of improper system statealterations) extends the usual definition as follows:

- when a system implements an authorizationpolicy, 'improper' encompasses 'unauthorized';
- 'improper alterations' encompass actions resultingin preventing (correct) upgrades of information;
- 'system state' encompasses hardware modificationsor damages.

The definition given for maintainability goes beyond corrective and preventivemaintenance, and encompasses the forms of maintenance aimed at adapting or perfecting the system.

Security has not been introduced as a single attribute of dependability. This is in agreement with theusual definitions of security, which view it as a composite notion, namely the combination of:

- confidentiality (the prevention of the unauthorized disclosure of information),
- integrity (theprevention of the unauthorized amendment or deletion of information),
- availability (theprevention of the unauthorized withholding of information).

A single definition for security couldbe: the absence of unauthorized access to, or handling of, system state.

Besides the attributes defined at the beginning of the section, and discussed above, other, secondary,attributes can be defined. An example of specializing secondary attribute is robustness, i.e.dependability with respect to external faults, that characterizes a system reaction to a specific class offaults.

The property of a system to be available, reliable, safe or secure is to be intended in relative, probabilistic sense and not in absolute, deterministic sense, due to unavoidable, presence of occurrence of faults.

The process of designing dependable systems answering the specific application requirements is quite complex and needs to follow a methodical highly structured approach based on three main activities: specification, design, evaluation (design paradigm) [6].

A system may fail either because it does not comply with the specification, or because the specificationdid not adequately describe its function. An error is that part of the system

state that may cause asubsequent failure: a failure occurs when an error reaches the service interface and alters the service. Afault is the adjudged or hypothesized cause of an error. A fault is active when it produces an error;otherwise it is dormant.

Impairments can affect a system and cause a drop in dependability, their definitions are the following:

- **Fault**: *defect in a system.*
  The presence of a fault in a system may or may not lead to a failure, for instance although a system may contain a fault its input and state conditions may never cause this fault to be executed so that an error occurs and thus never exhibits as a failure.

- **Error**: *discrepancy between the intended behavior of a system and its actual behavior.*
  Errors occur at runtime when some part of the system enters an unexpected state due to the activation of a fault. Since errors are generated from invalid states they are hard to observe without special mechanisms, such as debuggers.

- **Failure**: *instance in time when a system displays behavior that is contrary to its specification.*
  An error may not necessarily cause a failure, for instance an exception may be thrown by a system but this may be caught and handled using fault tolerance techniques so the overall operation of the system will conform to specification

The development of a dependable system calls for the combined utilization of a set of four techniques:

- **Fault prevention**: *how to prevent the occurrence or introduction of faults*.
  It can be achieved by quality control techniques acting during the design and manufacturing of hardware and software, such as structured programming, information hiding and modularization for software and rigorous design rules for hardware.

- **Fault tolerance**: *how to deliver correct service in the presence of faults*.
  It is generally implemented by error detection and subsequent system recovery.Error detection originates an error signal or message within the system. An error that is present butnot detected is a latent error.
  Recovery transforms a system state that contains one or more errors and (possibly) faults into a statewithout detected errors and faults that can be activated again. Recovery consists of error handling andfault handling. Error handling eliminates errors from the system state.Fault handling prevents located faults from being activated again.

- **Fault removal**: *how to reduce the number or severity of faults*.
  It can be performed both in the development phase, thorough the section of verification, diagnosis and correction, and in the operational life of a system, through corrective and preventive maintenance.

- **Fault forecasting**: *how to estimate the present number, the future incidence, and the likely consequences of faults*.

The specification phase is very delicate as it determines the weight that each of the four techniques suggested in the development of dependable systems (fault prevention, fault tolerance, fault removal and fault forecasting) has in their combined utilization.

The alternation of correct-incorrect service delivery is quantified to define reliability, availability andmaintainability as measures of dependability:

- reliability: a measure of the continuous delivery of correct service, or, equivalently, of the time to failure;
- availability: a measure of the delivery of correct service with respect to the alternation of correctand incorrect service;
- maintainability: a measure of the time to service restoration since the last failure occurrence, orequivalently, measure of the continuous delivery of incorrect service;
- safety is an extension of reliability: when the state of correct service and the states of incorrectservice due to non-catastrophic failure are grouped into a safe state (in the sense of being free fromcatastrophic damage, not from danger), safety is a measure of continuous safeness, or equivalently,of the time to catastrophic failure; safety is thus reliability with respect to catastrophic failures.

Generally, a system delivers several services, and there often are two or more modes of service quality,e.g. ranging from full capacity to emergency service. These modes distinguish less and less completeservice deliveries. Performance-related measures of dependability are usually subsumed into the notionof performability.

The experience has shown that the design of dependable systems requires the balanced use of both fault tolerance and fault avoidance techniques [6].

Particularly, fault tolerance is nowadays applied to a number of application fields such as long-life, delayed-maintenance, high availability and commercial applications and even safety-critical applications (e.g. flight control, nuclear plant monitoring, railway signaling), which require a high degree of confidence on the correct and safe operation of the system in order to prevent loss of life or damage to expensive machinery [7].

The property of fault tolerance is achieved through the use of redundancy in the hardware and software domains. In hardware, the redundancy can be easily realized by replicating a single design multiple times depending on the desired fault tolerance capability.

Software redundancy consists of the creation of two or more 'independent' versions of a piece of software, in order to ensure that design faults in one version do not cause system failures (design diversity)[8].

Design diversity is now adopted in some industrials sectors like aerospace and rail transportation where software solutions are going to be used in safety-critical functions. However convenience in the use of software redundancy is still under analysis, as the independence or better the negative correlation among the failures caused by redundant solutions must be ensured.

Anyway, the use of either hardware or software multi-channel design reveals in practical applications as an effective mean to increase the dependability of a system, with a larger or smaller weight depending on the level of safety-criticism of the application.
Moreover, the concept of multi-channel system is no more than the reproduction of the natural redundancy employed in human activities.
For instance, the same concept of redundancy as index of safety is used in the airlines, when a co-pilot is joined to the pilot in order to have a backup solution in emergency situations, or even in surgery, when two or three surgeons work together in difficult operations.

2 Dependability for Service Robotics

Respect to the elements analyzed by Laprie with regards to computer systems, shown in the previous section, robotics slightly moves the focus, from some less relevant elements to some additional ones.

Ingrand et al. proposed an architecture for dependable robotics system, by analyzing the additional requirements imposed by robotics and by taking into account the different levels of organization of the software modules [9].

Following the methodological approach of the design paradigm, their analysis of the specific field of robotics points out the fundamental requirements for the design of a dependable robot dealing with:

- The *programmability* of the robot system for accomplishing different tasks in different situations.
- The *autonomy* and *adaptability* of the system, in order to carry out the tasks, to modify and adapt the system behavior in accordance with the environmental changes as perceived by the sensors.
- The *reactivity*, meaning that the robot is able to safely face with the bounds and obstacles met on its path and eventually to continue its activity.
- The *consistent behavior*, by witch its actions are always aimed at pursuing the objectives of its tasks.
- The *robustness* to the variable types of contingencies.
- The *extensibility*, eventually, i.e. the learning capability allowing to extend the robot functionalities, by implementing behaviors of learning by imitation or by teaching.

All these properties should be involved in the design at the level of global system, including the robot, the environment, the application requirements and the user, as they acquire a different priority and require different solutions according to the features of the global system.
Within robotics, service robotics poses additional critical issues related to the close interaction of robots with humans and the environment, and to the need for human's trust on robot behavior.
Modern robotics is addressing many new areas of application that require safe and effective physical and cognitive interaction with humans. Consequently, robot dependability is becoming an area that is rapidly gaining direct interest from many research group worldwide.
Since our society largely depends on infrastructures that are controlled by embedded information systems, the dependability concept has been widely employed for these kinds of systems. Although service and personal robots are supposed to become an important part in our future society, dependability aspects have been almost constantly neglected by researchers. However, dependability concepts are needed especially for these types of robots because they are intended to operate in unpredictable and unsupervised environments and in close proximity to, or in direct contact with, people who are not necessarily interested in them, or, even worse, who try to harm them by disabling sensors or playing tricks on them.

Dependability is one of the main issues in the development of service robots. Dependability involves physical safety on one side and operating robustness (consisting of availability, reliability, and maintainability) on the other.
Service robots in real environments impose requirements that are incomparably higher than demands made on the capabilities of industrial robots.

First and foremost, service robotics requires that dependable robot systems be deployed to operate in human-inhabited environments. Second, service robots must fulfill their tasks with adequate performance and robustness in dynamic and unpredictable environments. For mobile robots, the safety requirement is particularly relevant, since the robot actively engages the environment and hence bears full responsibility in case of hard contact with people or objects [10].
Dependability must be obtained for each single component of a robot and for the whole system, which, designed to fulfill a certain task, might be more than just a sum of its components. In order to prevent faults efficiently, modular and structured systems are mostly preferable. They enable the testing of each component separately. However, fault prevention alone does not lead to dependability; fault tolerance and error recovery should be considered as additional means[11].
From a general viewpoint, three main research areas on service robot dependability can be considered:

- Mechanical design, compliant systems, safe design, sensing control and monitoring while interacting with humans.
- Software and systems integration and encompasses error detection, diagnosis and recovery, V&V (verification and validation) techniques, testing and controller synthesis.
- Decisional autonomy, network of robots and their high level interactions with humans; this area is the least explored so far it yet offers paramount machine intelligence challenges.

Bischoff et al. [3] proposed guidelines for the design of dependable robotic assistants. In their analysis, the most general design rule to keep in mind is that a robot system exists for one reason: to provide value to its users. Therefore, before specifying any system requirement, or determining the hardware platform or development processes, one has to answer the question whether a planned feature contributes to the system's ability to provide value to the user. All design decisions should be made with this general rule in mind. Furthermore, the dependability of a robot is not something that can be added on after the robot has been designed and built. Rather, it must be designed into the robot from the very beginning and, specifically, Bischoff et al. claim that it emerges from the following design principles:

- learning from nature how to design reliable, robust and safe systems;
- providing natural and intuitive communication and interaction between the robot and its environment;
- designing for maintainability;
- caring for a simple, systematic and tidy design;
- optimizing system performance through field tests with novice users.

Although several, if not all, of these design principles might be considered "common sense" for robotics engineers, they have definitely not been explicitly formulated before and are not followed by a large part of the research community. We strongly believe that future robotic assistants could benefit from applying these design principles.

Our study of dependability for service robotics has highlighted that one important guideline to enhancing dependability of service robots is the modular approach: to separate the complete system into physically and functionally distinct units, for an easy and cost effective maintenance, easy removal and replacement of single modules.

The great advantage of this modular approach is that it allows us to design, develop, test and improve system components alone, or even to buy them directly off the shelf, before integrating them into a complex system.

If the components themselves are failsafe and need little or no maintenance at all, overall system maintainability is greatly increased.

Strictly modular design where all modules have standardized, homogeneous mechanical and electrical interfaces is considered as most important. If these modules are connected via powerful communication links they can be nearly arbitrarily configured and adapted to changing requirements. This concept of modularity should be pursued both for the construction of the robot body and its sensors, and for the structure of the information processing system.

In the service robotics, fundamental aspects for the user's safety are the localization and navigation of the mobile robots.

For mobile robots, one of the major safety hazard is the possibility of the robot losing its position. This could lead to the robot leaving its assigned operation area, falling down stairs and hurting people, or damaging its environment. Physical safety can only be guaranteed if the robot knows its position (fault prevention) and is able to recover position loss as quickly as possible (fault recovery).

In order to dependably navigate in environments populated by people, the navigation system of an interactive robot assistant must be capable of dealing with dynamic environments. It must guarantee that people will not be hurt nor objects damaged at any time. In order to specify the requirements for a dependable navigation system, the different possibilities of implementing a mobile robot's navigation system must be analyzed. Furthermore, the degree of dependability must be evaluated for each solution.

2.1 Our proposal of dependability for Service Robotics

Our study has shown that the dependability is a very complex concept, that integrates different attributes and aspects.

The definition of dependability provided by Laprie, is the most general and used, but it was conceived in particular for computer systems.

In our opinion, for the service robotics this definition is not completely suitable, at least it's not suffice.

We propose a new definition of dependability concept, more suitable for service robotics, in order to consider all the aspects and main properties.

That is, it includes the traditional dependability attributes of availability, reliability, etc, included in the Laprie's model, and it extends the concept toward new attributes, integrating them in the tree model.

We believe that these attributes need to be re-interpreted to some extent to take into account the characteristics of service robotics.

In accordance to our analysis, we propose the new dependability concept, shown in Figure 2.

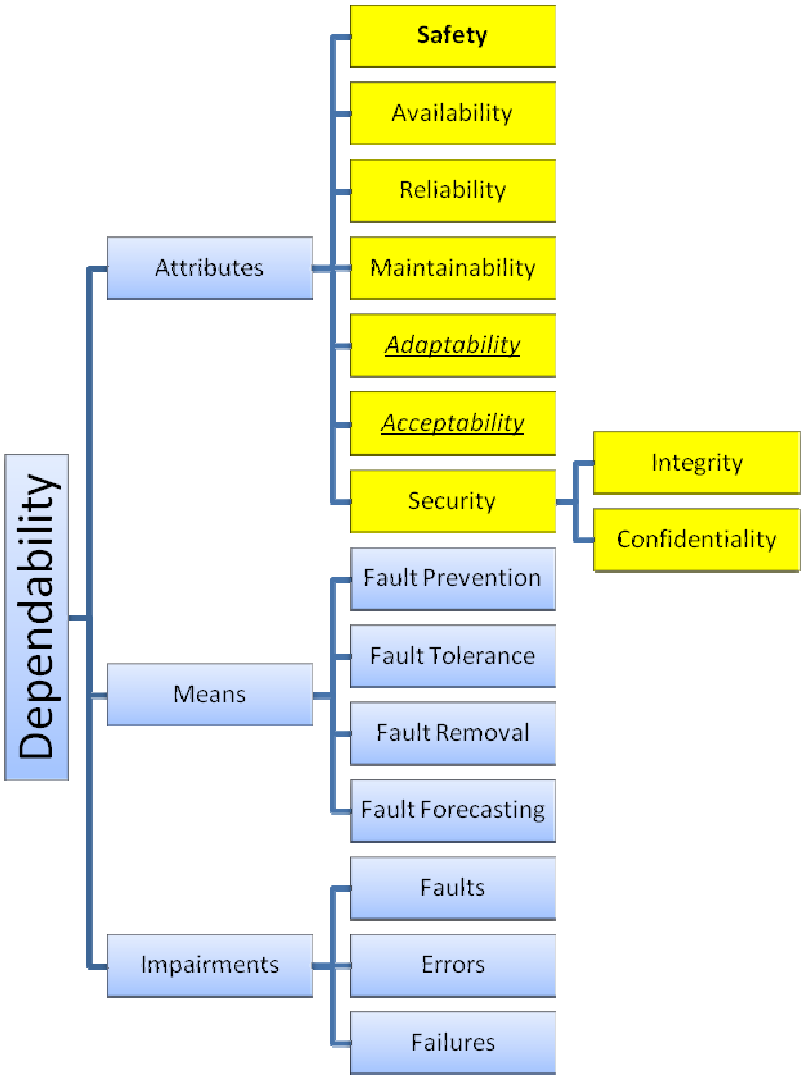

Figure 2. New dependability concept for service robotics

The attributes of dependability are the following:

- **Safety**: absence of catastrophic consequences on the user(s) and the environment; the main aspects of this attribute include safe navigation, so localization, and safe human-robot interaction; the safety has to be always ensured both in indoor and in outdoor environments.

- **Availability**: readiness of system for providing correct services to the user(s).The degree to which a system is in a specified operable and committable state at the start of a service, when the service is called for at an unknown, i.e., a random, time. Simply put, availability is the proportion of time a system is in a functioning condition. This is often described as a mission capable rate.The ratio of the total time a functional unit is capable of being used during a given interval to the length of the interval.

  Availability of a system is typically measured as a factor of its reliability - as reliability increases, so does availability. However, no system can guarantee 100% reliability; and

as such, no system can assure 100% availability. Further, reliability engineering and maintainability involve processes designed to optimize availability under a set of constraints, such as time and cost-effectiveness.

- **Reliability**: continuity of correct service; the ability of a system or component to perform its required functions under stated conditions for a specified period of time.

- **Maintainability**: ability to undergo repairs and modifications. In engineering, maintainability is the ease with which a product can be maintained in order to: isolate defects or their cause, correct defects or their cause, meet new requirementsmake future maintenance easier, or cope with a changed environment

- **Acceptability**: a system that is not acceptable to users will simply not be used. In our opinion the acceptability is a primary feature of a service robot. Therefore, it is essential that system characteristics that affect its acceptability, such as the human-robot interface, the system learnability and the aesthetics, are considered in the design process.
  One aspect, related to the acceptability, that we can consider is the fitness for purpose. It is taken for granted in most of the dependability literature but, socio-technical system failures regularly arise because a computer-based system is not fit for the purpose for which it was designed and users of the system have had to adapt their operational processes to accommodate the system's inadequacies. When the purpose of a system is to cope with disability, users may simply not have this option and the system may simply be unused.

- **Adaptability**: within the home both the environment and the users of the systems change. This is particularly true for elderly, or disabled, people whose capabilities tend to decline as they age. Therefore, if system dependability is not to degrade, then it must be able to evolve over time, generally without interventions from the system's designers. Moreover, also the outdoor environment is highly variable, many factors could change their conditions, so the robot platforms have to recognize these environmental changes, modify and adapt the system behavior in accordance.

- **Security**: is a composite of **confidentiality**, the absence of unauthorized disclosure of information, and **integrity**, the absence of improper system state alterations.
  It's important to specify the difference between safety and security: the term 'safety' indicates purely physical safety, for users and environment, while 'security' indicates only the absence of intrusions, of unauthorized access to, or handling of, system state.

As these definitions suggested, only availability and reliability are quantifiable by direct measurements, while the other attributes are more subjective.

For instance, the primary attribute, safety, cannot be measured directly via metrics but is a subjective assessment that requires judgmental information to be applied to give a level of confidence; reliability can be measured as failures over time.
In order to have a quantifiable measure of safety, we could consider this attribute as an extension of reliability and availability: when the state of correct service and the states of incorrectservice due to non-catastrophic failure are grouped into a safe state (in the sense of being free fromcatastrophic damage, not from danger), safety is a measure of continuous safeness, or equivalently,of the time to catastrophic failure; safety is thus reliability with respect to catastrophic failures.

Our final proposal is to divide the dependability attributes into two different blocks (see Figure 3):

- → **Technical Factors**: this block includes the standard attributes and the adaptability, all related to technical aspects.
- → **Human Factors**: this block includes the acceptability and the customizability attributes, strictly related to human factors, to the users.

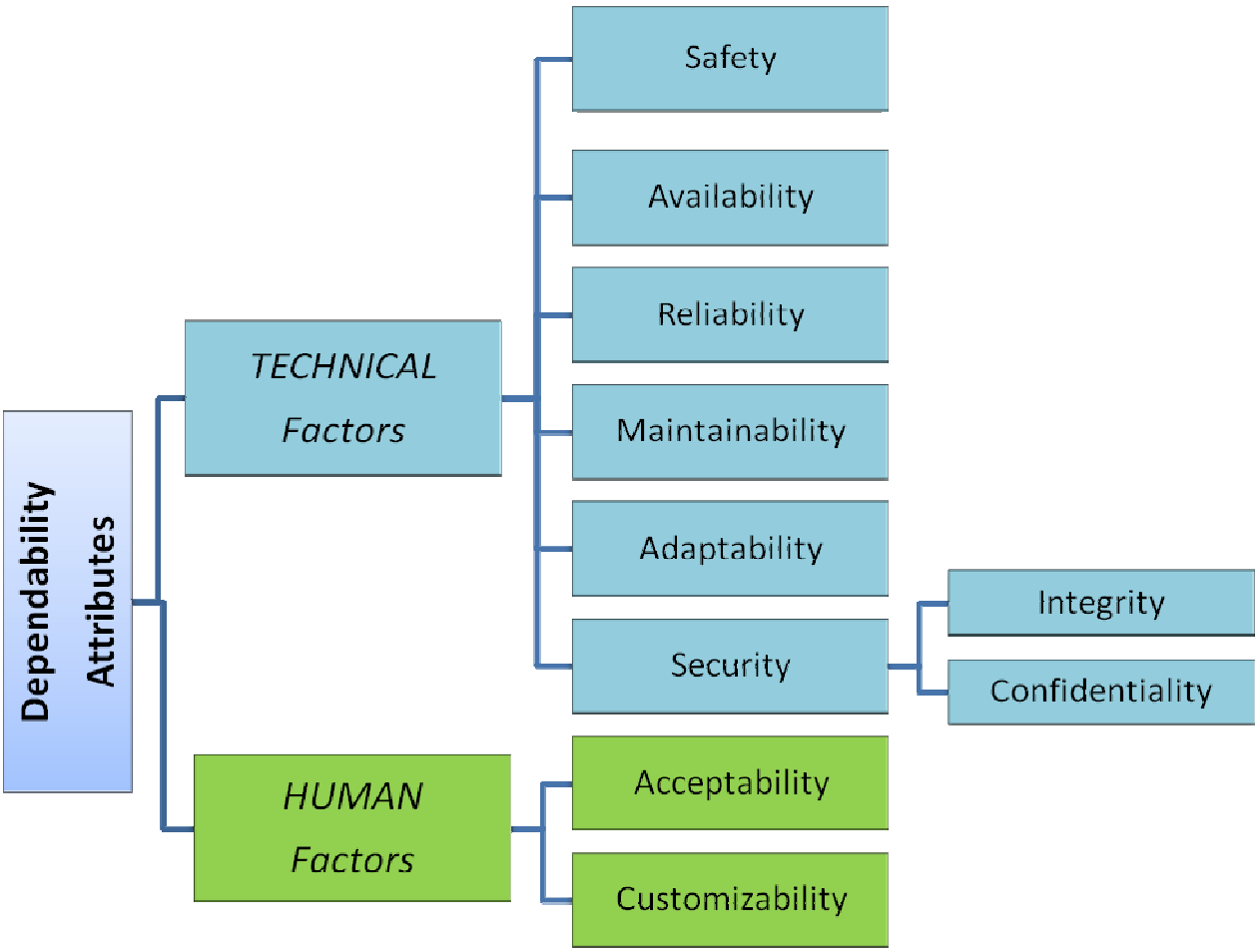

Figure 3. Our proposal of dependability attributes

In our proposal, we would increase the importance of the user in the dependability assessment, we consider the perception of the dependability attributes, particularly the acceptability, from the point of view of the user.

In the Human Factors section, another attribute we propose is the **customizability**, the ability for system to be changed by the user.

We have to highlight important considerations about the **acceptability**'s attribute. In our analysis we adopt the approach defined by Aquilano et al. [14].

This innovative approach is suitable to evaluate assistive technologies, not properly service robots. So we adopt a conveniently modified version of this approach, suited for service robotics. This innovative approach to evaluate assistive technologies is aimed at evaluating if the devices features and specifications match addressed actual needs of disabled people. In this framework, user acceptability of a device is defined as the degree of user predisposition to carry out daily activities using the intended device as the result of his/her diverse perceptions on the following set of characteristics: usability (sum of effectiveness, efficiency and satisfaction), utility, aesthetics, impact on daily habits, obtrusiveness, safety, portability and comfort (see Figure 4).

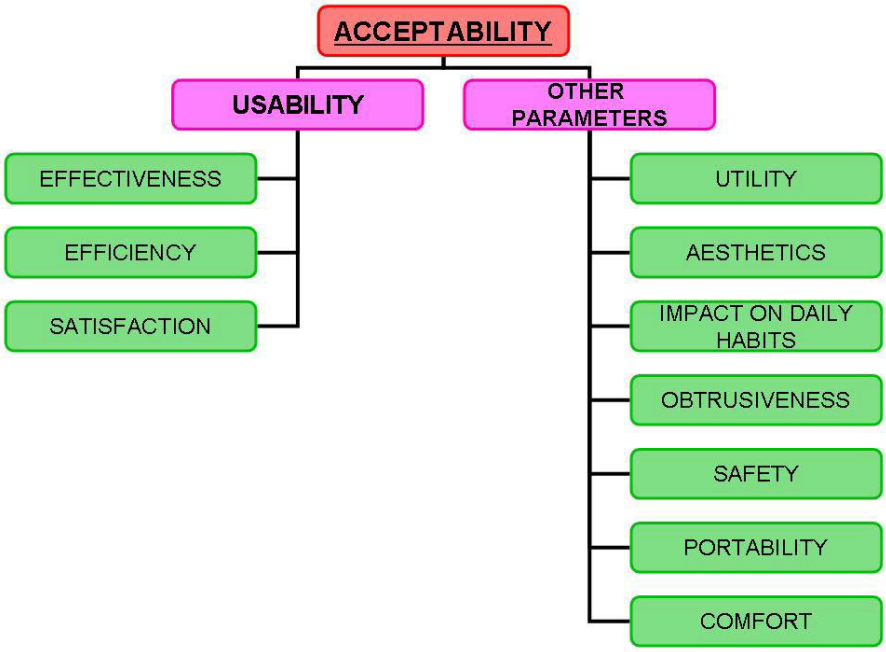

Figure 4. Schematic drawing of general requirements of assistive technologies acceptability

Aquilano et al. provided a protocol that aims at determining objective and quantitative parameters that represent information directly traceable by means of numerical values. An overall acceptability level can be obtained by those parameters that make possible a simple and effective quantitative analysis and trade off among different devices designed to fulfill the same functionality.

For the evaluation metrics and benchmarks for Robot-Era services, from the point of view of acceptability and usability, we refer to deliverable D2.5"First report on the evaluation metricsand benchmarks for Robot-Eraservices".

3 Dependability of the Robot-Era robot platforms

In this section we consider and evaluate the dependability aspects of the Robot-Era system. The hardware solutions will target the robotic platforms (extra hardware designed to be integrated with various platforms) and different solutions for enhancing dependability of each robot will be analyzed and experimentally tested.
The proposed solutions for controlling human-robot physical interaction will intervene first at robot level, where major attention will be devoted to the critical issue of safely managing the transition between two control strategies when the robot switches from one function/service to another one. Secondly, it will be devoted at system level in order to:

- allow cooperation among robots, in addition to human-robot interaction;
- provide each robot with the capability of selecting or reconfiguring the control strategy when they are;
- cooperating, thus always allowing achieving the target performance also in case of failure;
- provide each robot with predictive sensory information whenever sensory delays due to heavy processing times should affect the control system operations.

The dependability of the Robot-Era services depends on each specific robot and device. It's important to define and analyse dependability aspects in a modular approach, for each component of the overall system.

Robot-Era includes three types of robotic platforms: domestic robots, condominium robots, and outdoor robots. Although these platforms will differ both in hardware and software, the Robot-Era consortium agreed that they should share a similar abstract architecture. In the following sections, the dependability of each robot platform is described and analysed.

3.1 Domestic Robot

Dependability of the platform

The domestic robot is based on the commercial robot platform SCITOS G5 from MLAB. The technical details of the platform are described in deliverable D4.1.

The SCITOS platform has a CE sign (*Certificate of Conformity*), which was approved by the "TÜV Thüringen". The SCITOS A5 with robot head, touch display and integrated charger was successfully tested in 2009 according the rules DIN EN 60335-1 (VDE 0700 part 1) 2007-02 and DIN EN 60204-1 (VDE 0113 part 1) 2007-06. Based on these tests and the CE sign, that the SCITOS A5 platform can be used in public environments without necessary presence of an human operator. The safety hazards are listed and described in the operational manual of the SCITOS platform. Due to all this things, the **safety** of the platform is given.

Since the platform has a modular designed, the **maintainability** can be guaranteed. If one component fails it can be replaced by an identical one without replacing the whole robot.

All hardware components are using an integrated CAN bus for communication. The CAN bus comes from the automotive industry and provides a very reliable and fast communication between microcontrollers.

The battery and the power supply system are monitored by a battery management unit. If an over current or another critical error in the power supply is detected, the whole system can be shut down automatically to prevent dangerous situations.

The SCITOS platform is used in many different applications in public environments, industrial areas and in research institutes. Therefore the platform is well tested approved and the **reliability** of the platform is given.

Dependability and safety of the navigation system

For navigation of the mobile robot, the navigation software CogniDrive from MetraLabs will be used. For more details, please refer to the deliverables D2.4 and D4.1. Although CogniDrive is very robust and approved in many different application, driving more than 15.000km, a real safety according a *Safety Integrity Level* (SIL) cannot be achieved, since the navigation software runs on a standard PC. To the knowledge of the authors, it is almost impossible to fulfil the requirements of SIL on a standard PC. Therefore, the SCITOS platform contains a SIL certified laser range finder and a bumper system.

The SIL certified laser range finder Sick S300 allows to define a safety field. As soon as something (a human being or an obstacle) are detected within the safety area, the motors of the robot can be stopped or the maximum velocity can be reduced to a level, at which a possible collision with a human would not cause injuries. These behaviours are realized in the hardware (i.e. in the motor controller) of the robot to achieve the required safety. Furthermore, the bumper of the robot fulfils two important aspects. If an obstacle or human being was not detected by the laser range finder (e.g., if the objects is below the scanning plane), a contact with the bumper will bring the robot to an immediate stop. Additionally, the bumper is made of flexible rubber, which is able to absorb a part of the kinetic energy in case of a collision.

For all technical details refer to Deliverable D4.1: "Domestic robot platform specification".

3.1.1 Robotic Arm for Manipulation

Dependability of the Hardware

The selection of the manipulator hardware has been made in order to assure reliability, dependability and safety. The Jaco-Arm from Kinova (see Figure 5) is a lightweight robot arm designed to work closely next to humans.

The arm has been evaluated in several clinical studies where it was mounted on wheelchair platforms and assisted disabled people in their daily life.

Due to the lightweight design the risk of injury or damage due to collision is minimized. The operation speed is selected as an optimal trade-off between safety of operation and performance. The use of carbon fibre has several advantages: durability, stability and minimizing the risk of injury in the unlikely event of a collision.

In addition to that the slim design ensures high user acceptability. As the robot arm is a commercially available product, aspects like certification, compliance to local rules, maintainability and reliability will be ensured by the vendor.

For more technical details,and the explanation about the choice of this manipulator, refer to Deliverable D4.1: "Domestic robot platform specification".

Figure 5. Kinova Jaco Arm

Dependability of the Software

Within our software framework several measures are taken to achieve reliability and safety. The first measure is to use multimodal sensor systems. We fuse sensor data of traditional high resolution vision systems and depth cameras in order to generate precise and robust sensory data. Sensory data will be analysed by multiple algorithms in order to decrease the risk of malfunction. The complete trajectory of the robot arm will be planned and analyzed according to object affordances and possible obstacles, ensuring a collision-free execution of the manipulation task.

Each autonomously planned action needs to be confirmed by the user in order to ensure the highest possible reliability.

Integration of user interrupt

Although all possible technical measures have been taken we plan to add an additional security layer by integrating a switch for the user to stop manipulation. The user will always be the highest authority and should always be able to overrule the decision of the robot. This software stop-button needs to be easily visible and accessible by the user. As control will be performed from a different system that is connected by a wireless connection that may fail, regular polling of the state and auto-stop on connection problems will be implemented.

Software Maintainability

The developed software will be integrated into the ROS framework. This way it is possible to easily monitor and debug the function of each module. Due to the extendibility the software system can be adapted to varied requirements. This way most parts of the software can be re-used in different contexts.

3.2 Condominium Robot

Since the condominium robot is also based on a SCITOS G5 platform using the CogniDrive navigation software, the same aspects as described in section 3.1 for the domestic robot can be applied here.

For all technical details refer to Deliverable D5.1: "Condominium robot platform specification".

3.2.1 Dependability of the user interaction

The dependability of the user interface depends on the three main interaction modalities:

1) Web based interfaces and mobile devices

The web based server-client architecture will allow remote control though mobile devices like tablets and mobile phones. Information from the robot or the ambient environment will also be made available to the user through this interface. The **availability** of the service will be guaranteed with the on-board touchscreen, which will mainly function as an on-robot "backup" interface for maintenance, error reporting and basic I/O functions. That touchscreen will allow interaction with a single platform when the wireless signal is down. A good quality wireless signal will be required in order to guarantee the **reliability** of the services. Therefore reliability will depend on the reliability of the hardware used as well as the software. For this reason a central computer server with redundant hardware and automatic backup solutions will be employed to host main software (e.g. web interfaces, speech recognition, ambient intelligence). Thus we will adapt standard hardware/software solutions, i.e. commercially available mobile devices and computer platforms produced by renewed brands, equipped with a maintained operating system such as the Ubuntu Long Term Support version. This will also guarantee the **maintainability** of the hardware/software system that can be done by any technician/ customer support
The design of the software, that implements the interfaces will guarantee the **adaptability** and **customizability** of the system to a single user's needs and expectations and to particular services. Furthermore, even if the interaction with the internet must be reduced to the strictly necessary, security issues will arise when the server is connected with the internet. To this end, strong **security** standards (ISO 27002) will be adopted to design the system and protect the user data from malicious software and external intrusion. Finally the **acceptability** of the user interface system will be studied and developed according to the guidelines of Work Package 2.

2) Speech synthesis and recognition

The **availability** of both automatic speech recognition (ASR) and speech synthesis/text-to-speech (TTS) depends on the wireless connection between the robots and a remote server. The system will be designed in such a way that at least ASR will be provided from a server that is external to the robots and which is accessed via a wireless connection. The physical location of this server will depend, and it is even possible for this service to be delivered "on-demand" via the internet by a third party. Therefore, the availability of this service will depend on server uptime (for which backup systems might be required as mentioned above) and the availability of a reliable point-to-point connection, perhaps over an external network, i.e. the Internet.
The **reliability** of state-of-the-art ASR systems is never 100%, i.e. speech recognition may fail to recognise words or whole sentences, and it can misunderstand words. The degree of

this is dependent on a high number of variables, like speaker gender and age and quality of the sound setup. Metrics for measuring ASR performance, like Word Error Rate (WER, the amount of words that were wrongly recognised), are unique to every trained model, of which we will need to employ one per language. These metrics will be obtained during the project in test scenarios and they will be determined by the final choice of ASR software, hardware and interaction setup (microphones), together with the specific language used, and no doubt there will be a high individual speaker variation.
The **availability** and **reliability** of TTS is likely to be higher, as it is less demanding on resources and can more easily be provided from the robot platform, with the caveat that the robot platform itself can fail. Also, it cannot "fail" in the way ASR can. The text to be read out loud is known, there is no ambiguity or uncertainty, although the **acceptability** of TTS will depend on the quality of the voices and the user's profile.
ASR systems can adapt to their users' speech, potentially improving recognition accuracy (decreasing WER) and the technology for this is widely fielded. The **acceptability** of such a system can then be expected to increase over time. On the other hand, concatenative TTS of the type that will be used offers little in the way of **customizability**, with the exception of being able to programmatically control voice pitch, speed and to a certain degree intonation.

3) Other modalities

The use of nonverbal communication modalities in addition to the speech and web-based interfaces should increase the overall **reliability** of the robot interface by providing feedback about the robot's task understanding to the user. These should also increase the robot's **acceptability** by making interactions with the robot more natural and intuitive. Unlike the web and speech interfaces, these modalities will be **available** to the user only when the user is co-located with the robot and able to see it. Some motions, such as pointing, cannot be supported on all platforms due to differences in the robots' hardware configurations. However, all platforms will have body motion and head-based gestures (looking and nodding) available. Because these actions will be performed while communicating about tasks, the **reliability** of their correct performance will be dependent on the reliability of supporting aspects of the robot's cognitive architecture, such as the robot's ability to locate the user or an object in the environment. For navigation, findings from the study of proxemics in HRI should be used to design the robot's speed and path of approach towards the user in order to increase **acceptability**. Because these modalities serve as an additional channel of information alongside the web-based and speech-based interface, how and how frequently nonverbal communication modalities are used can be adaptedto the preferences of individual users in order to increase the robots' **customizability**.

3.3 Outdoor Robot

In this section are analysed all the technical aspects of the Outdoor Robot, related to its dependability, hardware and software factors that guarantee and enhance safety and the other attributes of dependability.

Safety requirements for the outdoor robot have been done in compliance with the new international *standard ISO/DIS 13482* "Robots and robotic devices – Safety requirements for non-industrial robots – Non medical personal care robot". All the safety hazards are described more in details in section 5 of Deliverable D6.1. Basically, safety for the outdoor robot is related to mechanisms and procedures to avoid dangerous situation that can cause damages to human beings, to the environment and to the robot itself.
Primarily to guarantee safety the robot must not harm people and animals and other things in the urban environment, such as cars, urban furniture, etc. Second, robot should avoid dangerous situation i.e. stairs, gaps, sidewalk, etc. that can causes damages to itself and people.

For this purpose the robot will be equipped with many sensors for obstacle detection and in particular of a laser scanner, a set of ultrasound sensors and a 3D camera. The idea is to create a safe bubble around the robot (see Figure 6). The laser (Hokuyo UTM-30LX)is positioned in the front of the robot, it has a beam of 270° and can detect obstacle on a plane of height 35 cm from the ground. Minimum distance is about 20 cm, maximum distance is 30m. Laser will be used primarily for navigation and to detect obstacles in front of the robot. A 3D camera (Asus Xtion Pro) is mounted on the front of the robot pointing down with an inclination of about 45° and is used to detect obstacles below 35 centimetres such as stairs, gaps and sidewalk. A ultrasound sensor with a large beam will be placed on the front part of the robot to detect any obstacle above the height of 35 cm in front of the robot that cannot be detected with the laser. Finally, 3 ultrasound sensors with a reduced beam will be placed on the back of the robot to detect obstacles on the back.

Figure 6. The obstacle detection sensors and their detection space.

A second factor that may damage or cause injuries to human beings is the bin of the robot, in particular during the phases of opening and closing. During the opening phase the bin can hit people present on the back of the robot: to prevent or reduce the risk the robot warns with vocal messages about this operation, moreover the opening speed is slow to reduce the force of impact in the event of a collision. On the other hand, during the closing phase accidentally might happen that a part of the human body, such as an arm or a hand of the

user, remains stuck in the bin. To reduce the riskthe robot warns with vocal messagesabout this operation, the closing speed is reduced and the force applied by the motors has been tuned so that a human being can always counteract the bin motion.

Concerning the outdoor walking support service the outdoor robot should provide a physical support to the user to realize the walk arm in arm. This support consists in a hand and forearm support that is placed on the left side of the robot (see D6.1 for more details). At the end of the support in correspondence of the user hand a joystick is placed for guiding the robot. Dangerous situations mightarise since the robot and the user are very closeont to each other: robot movements might unbalance the user who can fall down or the robot can hit the user during the motion. To reduce the risk of unbalancing and impact, the robot moves slowly and the speed and motion of the robot will be always controlled by the user with the joystick. As soon as the user leaves the joystick the robot stop immediately its motion. Furthermore, the user is always on the side of the robot while the robot moves mostly forward avoiding the risk of collision. It should be also taken into account that the user restsits arm on the support and is not linked to it, therefore at any time he can leave the robot.

Finally, in case of any dangerous situation caused by the robot two emergency buttons are placed on the robot to stop immediately its motion.

The **maintainability** is mainly guaranteed by the modular architecture of the robot: the core part of the robot is the supervisor system or main controller that manages all the robot's components and communicates with the other electronics control boards using the CAN bus as a communication channel (see Figure 7). Each electronics control boards has been provided with self-diagnosis mechanisms and failures are communicated through the CAN bus. The main controller is responsible of detecting and signalling anomalous situations to the user and to the operators. If a component fails or does not respond over the CAN bus the main controller stops immediately the robot operations. Moreover, thanks to this modular architecture, failed components can be easily replaced with new one.

Concerning the power, the battery level is constantly monitored by one of the electronic boards and is communicated over the CAN bus to the main controller. Moreover, the power board prevent the "switch on" of the robot when the battery level is below a certain predefined threshold (22.7 VDC) and switches off the robot when the battery level is below a second predefined threshold (20 VDC).

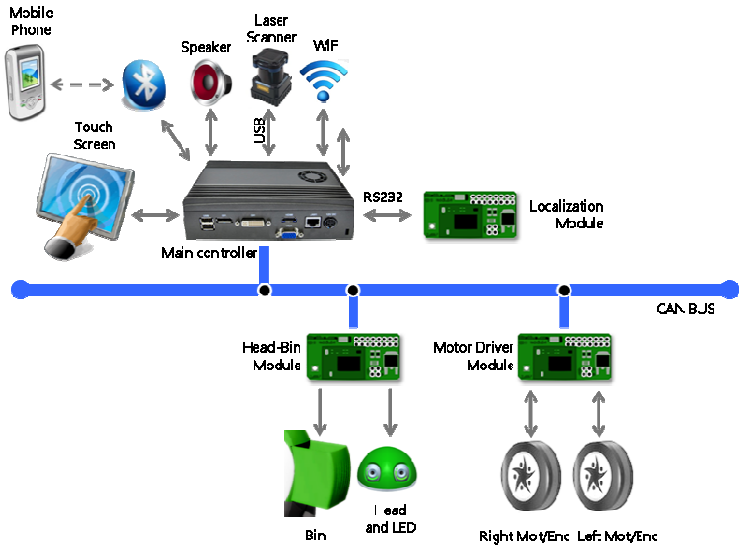

Figure7. The Outdoor Robot Architecture.

Reliability is probably the most important factor affecting dependability of outdoor robot. Previous experiments carried out with DustCart in 2010 for two months in the historical city centre of Peccioli where the robot was installed to provide a real service to the citizens, showed some limits and drawbacks of the system. These drawbacks can be summarised in the following points:

- the stiffness of the base caused the robot performance to degrade in case of road disconnections and/or slippery situations: in these cases the wheels could lose the contact or could slide with/on the ground thus affecting encoder measurements with a consequent error in the computation of odometry.
- Odometry, GPS and beaconing system were not robust enough: the deterioration of GPS signal due to obstructions caused by buildings, the obstruction of beacons caused by people, cars, etc. and the errors in the computation of odometry caused often the robot to get lost.
- The sensors for obstacle detection didn't allow to detect dangerous situations common to urban environment such as steps, sidewalks, stairs and other.

All these factors had impact on system reliability which was almost poor. To increase system reliability of outdoor robot the system has been improved in its main weak components: new mobile base, localization system and obstacle detection systems have been developed and new navigation software has been adopted.

The mobile base has been improved mechanically in order to provide a more robust system for navigating in urban environment: the introduction of suspensions improves drastically the adaptability of the robot to deal with road disconnections. A new commercial localization system by Trimble (Applanix AP10 GNSS-Inertial System) has been integratedand provides position and orientation in outdoor environment with optimal accuracy and robustness. As reported in the previous paragraph also the obstacle detection system has been improved to detect common dangerous situation in urban environment and finally, the navigation software has been upgraded and the well consolidated navigation stack of ROS has been integrated. Increase of performance of the system will be evaluated in the experimental loop to measure improvements of system reliability.

Availabilityof outdoor robot basically depends on the number of available robot to carry out the Robot-Era services. We can consider two options:a robot for each user and a set of robot for a set of users. In the first option the robot is basically immediately available to accomplish a service required by the user. Of course, the robot is not available for further services until the end of a previous service. In the second scenario, a set of users share a set of robots: availability primarily depends on the use of resources shared by the users and is strongly related to the cost. More robots means more availability but higher cost, on the contrary, less robots means less availability and less cost. Thus, availability is a matter of cost/benefit ratio.

As reported in the previous sections **acceptability**is a combination of many factors and in case of Robot-Era is evaluated at service level. For this parameter see Deliverable D2.5: "Evaluation metrics and benchmarks for Robot-Era services.

Adaptability is probably the most complex factor of dependability to be achieved for outdoor robot because urban environment is highly variable, more than a domestic environment: in fact urban environment is highly populated by people, animals, vehicles, bikes, etc. that move in an unpredictable manner around the robot. The system has been provided with many sensors (laser, ultrasounds, 3D camera) and navigation algorithms to detect and react properly to these situations. A second aspect concerns adaptability to the

user: this aspect has been taken into consideration especially for the walk arm in arm task.In fact, the hand and forearm support can be adapted in position and height according to user preference and physical characteristics. The hand and forearm support can be mounted both on left side and right side of the robot and its height can change between 95 and 110 cm (see Figure 8) depending on the height of the user.

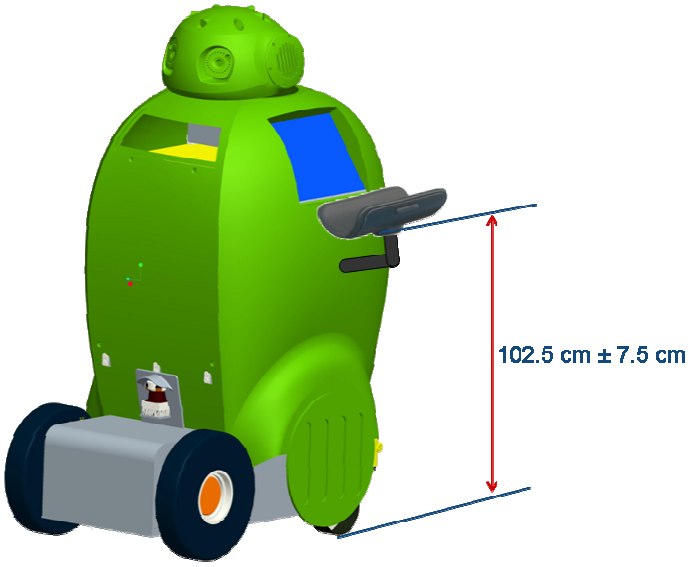

Figure 8.Changeable height of hand and forearm support.

Security is probably of less importance for outdoor robot and it's achieved mainly by avoiding unauthorized access to the robot. For the walk arm in arm task the user is close to the robot, thus other persons cannot use the robot without the authorization of its user. For the garbage collection and disposal task the robot is completely autonomous during the task and does not require and does not allow interaction with other people which therefore cannot use the system. Finally, for the shopping tasks people at the shops will be provided by the Robot-Era main supervisor with a password that will be entered on the touch screen to start the interaction with the robot in order to open the robot container and put in the goods. Other type of unauthorized access, such as access throughout the network will be solved at network protocol that level.

4 Dependability of the Robot-Era AmI

Ambient Assisted Living (AAL) investigates the development of systems involving the use of different types of sensors, which monitor activities and vital signs of lonely elderly people in order to detect emergency situations or deviations from desirable medical patterns.
AAL solutions need to provide high accuracy and proactive responses, "perceiving" lonely elderly people in their household environment through various sensors and carrying out appropriate actions under the control of the underlying software.
Dependability in the AAL domain is a critical requirement, since poor system availability, reliability, safety, or integrity may cause inappropriate emergency assistance to potentially have fatal consequences.
For domestic systems, we need to consider the dependability of the socio-technical system as a whole where the system includes the user, the home environment and the installed assistive technology [12].
In the AAL domain, there are few case studies and experiment reports. It is still difficult to do verification and validation of AAL systems in real scenarios due to their complexity and the unavailability of reference implementations. So we need first to find ways to quantitatively assess the architecture of AAL systems for dependability.
To accomplish that we must express dependability in terms of relevant domain properties and identify critical components that may require special design attention and project resource allocation [13].
For distributed systems, the security is a very interesting property, it's an important attribute of dependability, probably the most important. It becomes more relevant for the case of AmI environments. This is due to some of the characteristics of these environments, for example, intermittent connections of both, users and devices within the system; or the heterogeneity of the devices simultaneously connected. Thus, dependability should be an essential requirement for AmI systems.

In the Robot-Era project, key principles of AAL will be adopted in designing innovative solutions that can improve overall dependability of the Robot-Era services. Particular care will be devoted in the configuration of the sensors to be added to the environment and/or on the robot in order to keep an acceptable level of safety and adaptability and at the same time low computational burden, high robustness and reliability of these systems.
The main objective is to control that AmI is able to recognize all critical situations and activate alarms and assistance processes, with an efficient priority management.
Performing this type of analysis we could test the *priority management* of the AmI.
In fact, in the Robot-Era project, we will develop an AmI infrastructure, and the corresponding high-level services, that satisfy specific requirements for providing context-aware assistance. Specifically it should provide:

- A context awareness service, by which the information dynamically collected by the robots and devices is pulled together and different facets of the current "context" are inferred.

- A response generation service, by which adequate responses are enacted by the recognition of a given context (e.g., hazard situations) or by explicit request by the user.

- A self-configuration service, by which the relevant robots and devices that have to perform a given task and/or to collect some given information are automatically identified, connected and activated in the appropriate way.

A possible test we could implement is to simulate a critical situation, for example the fall of the elderly, and analyse the information stream at the different levels (see Figure 9):

- The wearable device detects the fall from data sensors.
- It sends the information to the PDA, through BT communication.
- The PDA sends the information to the PEIS-middleware.
- […]
- The AmI recognizes the critical situations and sends alarms.

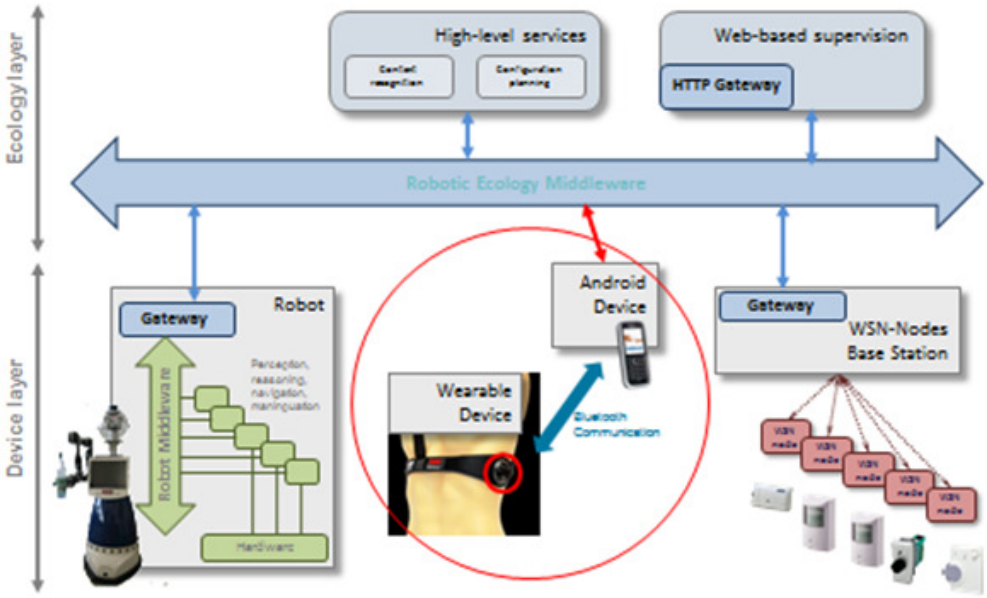

Figure 9. Schematic example

For an accurate description of sensors and AmI infrastructure of the Robot-Era system see Deliverable D3.1: "Report on the implementation of the AmI infrastructure modules".

For the description of the Robot-Era middleware (PEIS-middleware) see Deliverable D7.1: "Analysis and definition of interoperability aspects".

5 Dependability Assessment of the Robot-Era Services

Our proposal is to evaluate the dependability's attributes for each of Robot-Era services, during the experimental phases.

As the definitions suggested, only availability and reliability are quantifiable by direct measurements, while the other attributes are more subjective.

In the following table (Table 1), for each attribute of dependability, we propose a list of variables and factors that we could evaluate in order to quantify the dependability of Robot-Era services, during the experimental loops.

Table 1. Assessment of Dependability Attributes

Dependability Attributes	Variables
Safety	– Robot **Localization** - Robots position is always known? - Localization techniques and error estimation - Does robots leave their assigned operation area? – Robot **Navigation** - Obstacle avoidance, no hurts to people or environment! - Limited speed - Paths evaluation - Robot stops in a safe way if necessary – Physical Human-Robot Interaction →Safe manipulation(robotic arm of DomesticRobot) – Physical Interaction between two robots. – Ability of the Control Center to supervise and guarantee safety for people, robots and public environment.
Availability	– Measurement of proportion of time the system is in a functioning condition during the time duration of the task. – Measurement of the system's readiness (time between the user request and the real start of the service).
Reliability	– Time measurement of continuity of correct service. – Measurement of the necessary time to complete the tasks and the overall services.

	– Evaluation of failure of robots to perform operations. → We could consider Safety as an extension of reliability: when the state of correct service and the states of incorrect service due to non-catastrophic failure are grouped into a safe state (in the sense of being free from catastrophic damage, not from danger), safety is a measure of continuous safeness, or equivalently, of the time to catastrophic failure; safety is thus reliability with respect to catastrophic failures!
Acceptability	– For this attribute see Deliverable D2.5: "Evaluation metrics and benchmarks for Robot-Era services".
Security	– Evaluation of the security level of data and information of users and services; no intrusions of unauthorized people. – Availability of services for only authorized people. – Absence of intrusions, of unauthorized access to, or handling of, system state. – Actions must be taken to prevent unauthorized use of controls (password, antivandalism method such as fingerprint recognition, key cards, etch).

6 Conclusions

This work has introduced the dependability aspects ofsystem and services of the Robot-Era project. The term "dependability" is a system concept that integrates such attributes as reliability, availability, safety, confidentiality, integrity, and maintainability. The goals behind the concept of dependability are the abilities of a system to deliver a service that can justifiably be trusted, and to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the user.
Since in the Robot-Era project different robot platforms and devicesare installed in different environments (public and private spaces, living labs and residential sites), it's crucial to focus and enhancing all the dependabilityaspects in order to assure a high level of safety and availability.

All participating partners in the project have discussed the requirements and properties of the robot platforms and the whole Robot-Era system in terms of dependability.
First and foremost, the Robot-Era project requires that dependable robot systems be deployed to operate in human-inhabited environments. Second, service robots must fulfill their tasks with adequate performance and robustness in dynamic and unpredictable environments. For these mobile robot platforms, the safety requirement is particularly relevant, since the robots actively engage the environment and hence bears full responsibility in case of hard contact with people or objects.

The classical definition of dependability, provided by Laprie, was conceived in particular for computer systems, and it's not completely suitable for the service robotics. So wehave proposed a new definition of dependability, extending the concept toward new attributes and considering two main different blocks, technical and human factors.

Dependability must be obtained for each single robot platform and for the whole system, which, designed to fulfill specific tasks, might be more than just a sum of its components. In particular, the most relevant attribute of dependability in the Robot-Era system is safety, that is the absence of catastrophic consequences on the users and the environment; the main aspects of this attribute include safe navigation, so localization, and safe human-robot interaction.

TheSCITOS platform (domestic and condominium robots) has a CE sign (*Certificate of Conformity*). The SCITOS A5 with robot head, touch display and integrated charger was successfully tested in 2009. Based on these tests and the CE sign, that the SCITOS A5 platform can be used in public environments without necessary presence of an human operator. Due to all this things, the safety of the platform is given.

For the outdoor robot safetyrequirements have been done in compliance with the new international *standard ISO/DIS 13482* "Robots and robotic devices – Safety requirements for non-industrial robots – Non medical personal care robot".

The attribute of maintainability is mainly guaranteed by the modular architecture of the robotic platforms. Also the other attributes of dependability are described in this work for the robotic platforms and the AmI.The architectures discussed in this work are intentionally abstract. Each concrete Robot-Era robot platform is discussed in Deliverables D4.1, D5.1 and D6.1 respectively, while the AmI and the middleware are discussed in Deliverables D3.1 and D7.2.

In the section 5, we have proposed different variables and factors in order to evaluate and quantify the dependability's attributes for the Robot-Era services, during the experimental phases.

References

[1] J.C. Laprie, "Dependability: Basic Concepts and Terminology" (Springer-Verlag, 1992).

[2] A. Avizienis, J.C. Laprie, "Dependable computing: from concepts to design diversity", *Proceedings of the IEEE*, vol. 74, no. 5, May 1986, pp. 629-638.

[3] R. Bischoff and V.Graefe, "Design Principles for Dependable Robotic Assistants," *International Journal of Humanoid Robotics* Vol. 1, No. 1 (2004) 95–125.

[4] J.C. Laprie, "Dependable Computing: Concepts, Limits, Challenges," *25th IEEE International Symposium on Fault-Tolerant Computing*, Pasadena, California, USA, June 27-30, 1995, Special Issue, pp. 42-54.

[5] A. Avizienis, J.-C. Laprie, and B. Randell, "Fundamental concepts of computer system dependability," in *Proc. IARP/IEEE-RAS Workshop on Robot Dependability*, Seoul, Korea, 2001, pp. I-1.

[6] A. Avizienis, "Building dependable systems: How to keep up with complexity," Proc. IEEE, 1995.

[7] J.C. Laprie, "Dependable computing and fault tolerance: concepts and terminology", *Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing (FTCS-15)*, Ann Arbor, Michigan, June 1985, pp. 2-11.

[8] A. Avizienis, J.C. Laprie, "Dependable computing: from concepts to design diversity", *Proceedings of the IEEE*, vol. 74, no. 5, May 1986, pp. 629-638.

[9] F. Ingrand, R. Chatila, R. Alami, "An Architecture for Dependable Autonomous Robots, " 0-7803-7241-7/01/$10.00(c)2001IEEE.

[10] S. Caselli, F. Monica, and M. Reggiani, "YARA: A Software Framework Enhancing Service Robot Dependability," *Proceedings of the 2005 IEEE International Conference on Robotics and Automation Barcelona*, Spain, April 2005.

[11] B. Graf, M. Hans, and R.D.Schraft, "Mobile Robot Assistants," Issues for Dependable Operation in Direct Cooperation with Humans, IEEE Robotics & Automation Magazine, June 2004, 1070-9932/04/$20.00©2004 IEEE.

[12] G. Dewsbury, I. Sommerville, K. Clarke and M. Rouncefield, "A Dependability Model for Domestic Systems,".

[13] G.N. Rodrigues, V. Alves and R. Franklin, "Dependability Analysis in the Ambient Assisted Living Domain: an Exploratory Case Study,"2010 Fourth Brazilian Symposium on Software Components, Architectures and Reuse.

[14] M. Aquilano, C. Salatino and M.C. Carrozza, "Assistive Technology: a New Approach to Evaluation," *10thIEEE International Conference on Rehabilitation Robotics (ICORR)*, 2007.