Safety Science 50 (2012) 1888–1897

Contents lists available at SciVerse ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Safety certification requirements for domestic robots

Eleftheria Mitka, Antonios Gasteratos *, Nikolaos Kyriakoulis, Spyridon G. Mouroutsos

School of Engineering, Democritus University of Thrace, Vas. Sophias 12, Xanthi 671 00, Greece

ARTICLE INFO

Article history:
Received 5 December 2011
Received in revised form 5 April 2012
Accepted 10 May 2012
Available online 7 June 2012

Keywords:
Standardization
Domestic robots
Requirements
Systemic method

ABSTRACT

Domestic robotics is a growing sector with the potential for a large number of commercial applications. Robotics technologies have been successfully applied in industrial production lines, yet, for them to be successful in a dynamic household environment the need for increased reliability, robustness and other special capabilities become paramount. We are not far from the time when people will live and interact with robots and, thus, safety becoming the fundamental issue to observe. Robot designers should produce safe products for humans no matter what failure, malfunction or mishandle may occur. Thus, respective safety procedures ought to be applied to domestic robots as well. The most critical challenge is to preserve safety of humans without forfeiting a single token of the efficiency required to perform any task. In this technical communication, the authors address the need for safety regulations in domestic robotics and, while they do not intend to replace any current robot safety standards or guidelines, the proposed work may serve as a supplement to the standards. Since specific safety standards for domestic robots are not available, we propose that their safety verification should be carried out on the base of well-applied standards that developed in other areas and discussed here. The communication in hand provides the ground upon which a standard on domestic robots can be built. Moreover, it proposes a systemic approach that explicitly relates the system and user requirements to a list of safety problems, in order to achieve an adequate level of safety in domestic robotics.

1. Introduction

The necessity for safety in robotics technology has already been referred to by Asimov as early as 1942. Nevertheless, researchers have already identified that just the Asimov's three laws are not adequate to cope with robot behavior. Present-day industrial robotics standards lay out instructions for robots and their operational environment. The new ISO 10218-1 (2011) and ISO 10218-2 (2011) standards delineate the requirements with the view to reduce, as far as possible, critical hazards. The trade-off between advanced technical attributes and the pertinent absolute safety requirements is an issue standardization project teams need to consider, due to the emerging nature of this technology. Moreover, robotics technology is expanding from industrial to household applications, creating thus new kind of robots, such as robotic companions, logistic robots, robots for surveillance and intervention, and edutainment robots. Robots of the aforementioned types, shall be able to provide services to make humans' daily life much easier; with typical tasks including medical treatment of patients in the privacy of their own homes, transportation of patients or people with disabilities to hospitals and public places, protection of residents and people's belongings, children education, social companionship to elders, etc.

Traditionally, guards and interlocks have been used to protect people working with robots. However, such isolation safety practice can lead to new unhealthy restrictions in operations and usage. Safety of industrial robots has been a matter of concern in standards for years and this has resulted in regulations that keep users and robots apart; making well defined operations, such as programming, teaching and repair more difficult. Access to industrial robots is restricted by fixed and movable guards on the base of ISO 14120 (2002), through interlocks and other safety devices. Generally speaking, the principle of "stopping or separating", as applied to industrial environments, is unsuitable for home; since human–robot interactions constitute basic functions of any domestic robot. It should also be pointed out that, compared to their industrial relatives, service robots are usually smaller, less powerful and with enhanced mobility and autonomy. However, the basic guidelines of preparation for standardization, the methodologies for safety of machinery, as well as the international standard for robotics (ISO 10218-1, 2011) providing rules for robot-human interactions, should also be made applicable to domestic robots. Every manufacturer should follow the basic instructions summarized in the general principle of safety of machinery (ISO/IEC Guide 50, 1999) including the basic safety standards, the principle of risk assessment (ISO 14121, 1999), inherent safety principle for design (ISO 12100, 2010) and safe

* Corresponding author. Tel.: +30 2541079359; fax: +30 2541079331.
E-mail addresses: em3933@ee.duth.gr (E. Mitka), agaster@pme.duth.gr (A. Gasteratos), nkyriako@pme.duth.gr (N. Kyriakoulis), sgmour@ee.duth.gr (S.G. Mouroutsos).

0925-7535/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ssci.2012.05.009

features according to ISO 13857 (2008). The safety organization should examine the effectiveness of the methods used by the designer in order to reduce hazards to those corresponding to the Reasonable Alternative Design (RAD) standard. It may then justify the residual hazards by applying the ALARP (As Low As Reasonably Practicable) test, adopted in the standard of the risk management of medical devices, (ISO 14971, 2000). Moreover, the organization needs to consider the cost of installation of safety devices against their utility, since commercialization of domestic robots demands a low budget strategy. In this regard, the right balance between cost/benefit and hazard reduction to as low as a level as possible needs to be established; i.e. where the risks (R) are balanced against utility (U) of the device. If U > R, the manufacturer avoids the liability for a harmful incident. The absolute measure of severity states that the Head Injury Criterion (HIC) should be less than 200, according to intrinsic safety with regards to head acceleration hazards, when the maximum static force to be applied on objects equals 1 N (Wassink and Stramigioli, 2007).

Nowadays, as personal care and service robots tend to invade in every day life, there is a necessity to produce relative international standards. Thereupon, ISO establish ISO TC 184 Technical Committee that has the responsibility for developing standards on automation systems and integration. Moreover, one Subcommittee called SC2 that deals with robots and robotic devices has also been established. The scope of SC2 is the standardization of manipulating robots and robotic devices (except for toys and military ones). SC2 is developing a group of novel and/or revised standards in order to incorporate aspects of industrial robotics to personal care and domestic service ones. Standardization efforts of SC2 are carried out by four active working groups including: WG7 on developing safety requirements concerning non-medical personal care robots and WG8 on developing service robots standards. In WG8, the standards currently under construction are carried out concerning the most urgent areas such as software, coordinate system, modularity, performance criteria, safety assurance, user interface and characteristics of mobile robots (Seungbin and Gurvinder, 2009). The first standard to be updated is ISO 8373 (2007) that covers a vocabulary of terms and definitions used in robotics standards. The new ISO 10218-1 (2011) and ISO 10218-2 (2011) standards in conjunction with new standards developed for personal care service robots that are being established by WG7, touch existing robotic domains and extended them to novel domains such as the domestic robotics (Harper et al., 2009). Yet, due to the lack of the existence of international standards for such an emerging domain, the respective standard organizations in South Korea and Japan defined their own safety standards with aim to assist the rapid development of viable global markets in these conceivable future applications. These efforts support standards of vocabulary of terms and definitions along with relevant technical standards. Owing to the absence of certification in the domain and with aim to increase commercialization, utilization and acceptance of domestic robots by the society, the establishing of international standards should incorporate terminology from any national respective effort such as the South Korean standards KS B 6937 (KS B 6937, 2006) and B 6938 (KS B 6938, 2006) and Japanese ones JIS B0134 (JIS B0134, 1998) and B0185–0187 (JIS B0185, 6, 7, 2002, 2003, 2005 respectively). Moreover, among Korean Standards there are six safety related standards: KS B 6935 (KS B 6935, 2006), KS B 6936 (KS B 6936, 2006), KS B 6960 (KS B 6960, 2007), KS B 6961 (KS B 6961, 2007), KS B 6962 (KS B 6962, 2007) and KS B 6966 (KS B 6966, 2008) and performance standards related to service robots such as KS B 6960 (KS B 6960, 2007) or household robots KS B 6934 (KS B 6934, 2006).

In Kabe et al. (2010) seven service robots were approved according to the general safety principles of machinery. In another approach, (Kulic and Croft, 2006) presents a method for ensuring human–robot interaction based on danger factors and simulated experiments. Nagamachi (1986) attempted to analyze, through experiments and actual data of real accidents, human–robot unsafe conditions in industrial applications, which were due to intrinsic limitations in human perception, decision making and action taking, with the use of a Fault Tree Analysis. Furthermore, the "principle of separating" robot from human operators is no longer tenable as robots move from the state of separation to that of coexistence (Etherton and Sneckenberger, 1990). In this paper we make an attempt to codify safety regulations in domestic robots. Unlike previous literature endeavors applicable specifically to the safety of other categories of robots (e.g. in industry, Corrales et al., 2011; in construction, Lee et al., 2011; in medical applications, Fei et al., 2001), our paper emphasizes the need for an innovative certification procedure for domestic robots with the view to test the validity of the applied measures and to also provide supplementary guidelines to the existing standards and methods on such an emerging technology. We survey well-established standards developed in other areas, such as electrical appliances safety or software quality, and we reflect on their applicability to domestic robots. The robot must be safe to operate in dynamic environments in close proximity to humans and, in order to achieve this safely, its hardware and software should be properly integrated. Software reliability is essential in a domestic robot since any loss in control, in what is essentially a complicated computer-based safety–critical system, can lead to dangerous actions with catastrophic consequences. It cannot be overemphasized that the designer of such systems needs to always keep in mind the problems associated with debugging large computer programs (Wyrobek et al., 2008). It is important, therefore, to be able to recognize and identify potentially hazardous conditions in the operation of a robot at an early stage. Defining the procedure to determine the circumstances under which the robot may cause injuries and performing a hazard analysis is essential. Safety test methods include a system simulation following a risk analysis (such as fault tree analysis (FTA), risk tree, network logic, preliminary hazard, energy barrier, task analysis, subsystem analysis, failure mode and effects analysis). These quantitative techniques make use of probability theory to estimate relevant hazards (Rahimi, 1986; Jiang and Cheng, 1990). Moreover, a stochastic process based on probability theory could be implemented to a certain degree in the field of internal safety devices.

2. Design requirements and protective measures

2.1. System, technical and safety requirements

The American National Institute of Standards and Technology (NIST) has identified three safety zones for working robots (Kilmer, 1982), with Level 1 safety zone defined as the area outside the accessible working area of the robot, Level 2 zone as the accessible workspace area of the robot (excluding a small area surrounding the robot itself) and Level 3 as the zone in the immediate vicinity of the robot. Fig. 1 depicts the concept of dividing the space around the robot into the respective safety zones. Apart from maintaining a safe distance for humans, further measures should still be considered the safe use of robots. However, in the cases of domestic robots use, keeping humans far from robots appears to be impossible. Thus it is clear that safety of humans under conditions of close proximity should be given proper consideration. Building robots according to existing national standards can lead to reduced risk levels and ensure adequate levels of reliability and safety. Robots to be operated in Europe should conform to the European Committee directives and carry the CE marking approval (European Community, 2000).

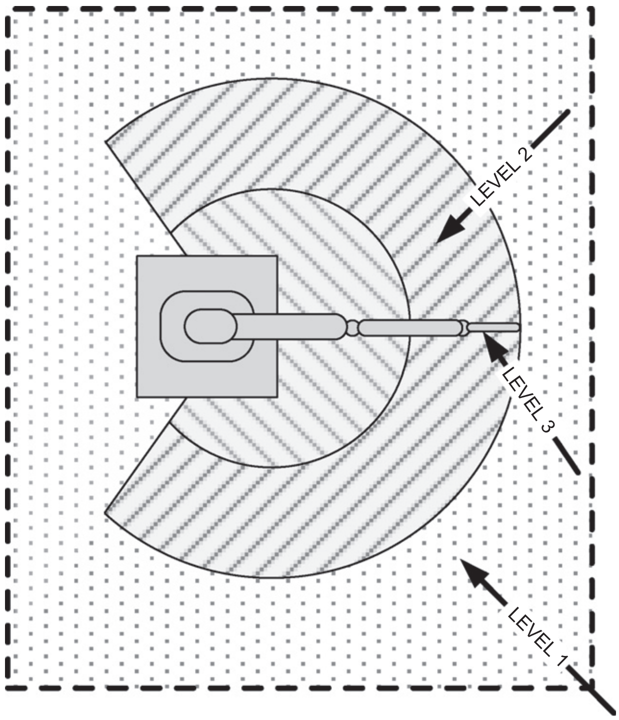

Fig. 1. The three safety region levels identified by NIST.

Delving into the realm of a safe robot constructing, all system and safety requirements should be given due consideration, from the beginning of the process. A system may be considered safe when it meets the basic safety standards defined by the national directives and regulations and safety targets are fulfilled. Every system operating in proximity to humans has to comply with specific safety requirements for accident avoidance. The safety requirements may vary according to the application the system is designed for; e.g. the high level safety requirements for a rehabilitation robot could be: (i) no collisions and (ii) user command execution without putting the patient's life in danger. Apart from the high level safety requirement that can be described verbally, for a system to be safe, its parts should also meet the existing safety standards. In the previous example of the rehabilitation robot this means that any mechanical or electrical part of the robot ought to be appropriately certified. Thus, the robot is safe if and only if during its operation there are no collisions, the user commands are executed precisely, its parts are certified and they follow the national directives. If these requirements are not fulfilled then the system cannot be considered safe in any case. The national directives concern the harmonization of the products limited to some essential requirements. The products that are placed on the market and put into service are only those that fulfill these essential requirements.

Furthermore, clear system requirements are also important, since they contain the specifications of the equally important subsystems. Thus, an ample definition of the system requirements leads to an easier integration of all subsystems. The system requirements are not limited to the technical requirements, but also encompass the ones concerning safety (which, of course, determine the boundaries of the technical requirements). It is true that safety requirements depend on the technical ones and that should also enfold the national directives and standards. However, as Protagoras said, "*man is the measure of all things*", suggesting an element of variability according to user's requirements. That is to say, it would indeed be hard, but not impossible, to specify universal requirements, where all possible applications of the specified system need to be taken into account. Besides the technical parts of the final system, reliability testing occurs for the software parts: grouping data into clusters of homogeneous failure intensities provides better reliability assessment. The final system must pass reliability tests, at both the hardware and software level, before proceeding to manufacture and eventual release to the market.

2.2. Safety requirements for domestic robots

In this section we will assess the safety issues regarding to domestic robots, thus, we should start with a definition of this robotics category. That said, notwithstanding the plethora of definitions for robots used industry (e.g. ISO/FDIS 8373, 2012; OSHA, 1999), there is hardly any source to provide an analytical counterpart for domestic usage. According to ISO/FDIS 8373(2012), "*a manipulating industrial robot is an automatically controlled, reprogrammable, multipurpose, manipulator programmable in three or more axes, which may be either fixed in place or mobile for use in industrial automation applications*". The robot includes the manipulator (including actuators) and the control system (hardware and software). Moreover, according to the Definition 1.2 (ISO standard 8373, No. 2.14): a robotic system is a "*system comprising robot, end-effector, any equipment, devices, or sensors required for the robot to perform its task, and any communication interface that is operating and monitoring the robot, equipment, or sensors, as far as these peripheral, devices are supervised by the robot control system*". Another useful definition is 1.3 (ISO standard 8373, No. 2.15) where robotics is the "*practice of designing, building, and applying robots*". On the other hand, robots for residential use are those automation apparatuses, which are considered capable of successfully taking over chores in a household environment inhabited by groups of people. They may complete a wide variety of tasks such as vacuum cleaning, fetch and carry tasks, ironing clothes, and window cleaning. Thus, a domestic robot is a robot used in a domestic environment (Crowley, 1989).

The successful introduction of safe household robots for use in a diverse number of tasks represents a major challenge. In fact, the so familiar household surroundings constitute an most chaotic environment; full of non-stationary objects, including different groups of entities, making it hard to evaluate the safety of such systems without any standardization benchmark. Here, we believe it is crucial to put forward a comprehensive and systematic overview of corrective or preventive measures, based on robotic safety guidelines and standards, in order to provide a safety checklist throughout the design, manufacture, commissioning and operation stages of robot use. These safety criteria intend to minimize the chance of an accident and provide the necessary protection to users.

With the aim to sustain the ultimate objective of this study, i.e. putting forward an innovative, systematic and complete method that combines worldwide well-tried, existing principles with a new concept concerning specific human–robot interaction issues, the flowchart in Fig. 2 is used to articulate a general safety approach for domestic robots. On the top of the flowchart the guidelines involved in the procedure of risk assessment are set out. We take the view that if residual risks are diminished to a tolerable level in terms of the ALARP region and if RAD and existing standards are implemented, then there is no need to elaborate further the risk assessment. Otherwise, the next step is the fulfillment of our key element, the proposed robotic safety checklist, described later in this section. If this step is bypassed, then more preventive features are required to achieve risk reduction. The next step in this iterative certification procedure, introduces the reduction of the design and construction of machinery hazards bellow a certain acceptable level. Next, a check is made as to whether the system complies with the general principles of inherent safety design.

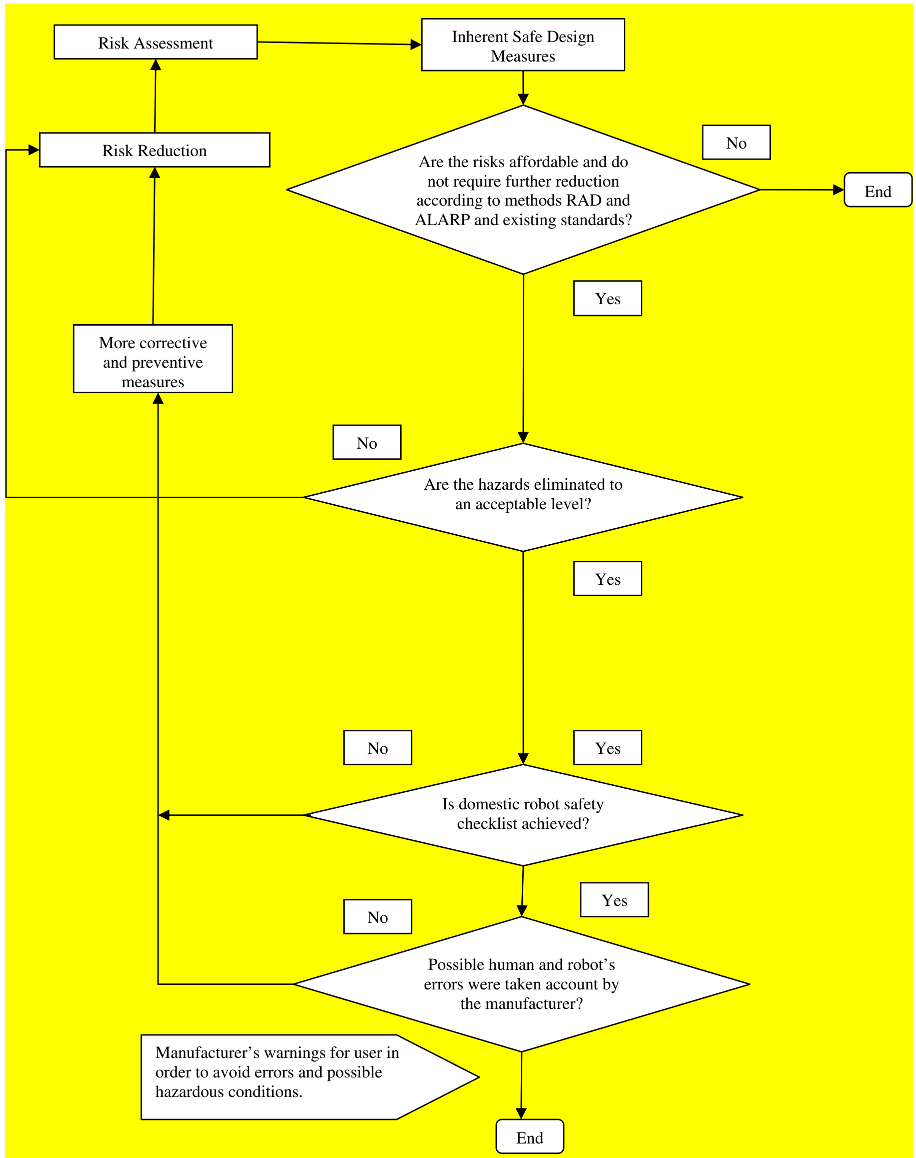

Fig. 2. A safety approach concerning applied methods and our proposed concept.

The final instruction checks the occurrence of errors by humans and robots and strongly recommends that the manufacturer should use warning signals in order to enhance human protection. It is essential that no inacceptable risk remain in a safe system, i.e. the risk should not exceed an affordable level. So, corrective and preventive measures have to be followed iteratively until the hazard is diminished to an acceptable level.

In the following paragraphs (Sections 2.2.1-2.2.13) we have kept a structure similar to a standard a manufacturer should follow in order to assure the safety of robotic products. Descriptions points out the requirements against and guidelines on the safety issues on the specific case of robots for domestic use. Moreover, and with an aim to readers further understanding, we accompanied these recommendations by two real examples, in order to illustrate the various stages of the evaluation of the risks or certification. The two chosen examples are the SONY AIBO[1] (Fig. 3a) and Friendly Robotics Robomow (Fig. 3b), which as being a robot pet and a robot lawnmower, respectively, they exhibit totally diverging characteristics in the application domain, the mode of use, the safety level, the way of movement, etc.

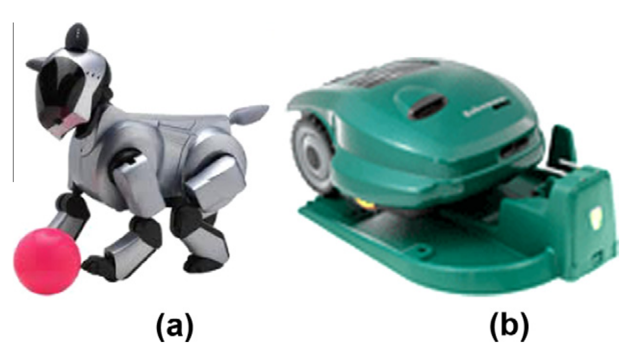

Fig. 3. The two real examples of domestic robots, chosen to illustrate the various stages of the evaluation of the risks or certification: (a) SONY AIBO and (b) Friendly Robotics Robomow [the images are adopted from the web-sites of the respective companies: http://www.sony.com and http://www.robomow.com/].

[1] The authors have chosen to present AIBO here, due to the fact that many people are familiarized with this robotic pet, notwithstanding that SONY Corporation has ceased its production.

2.2.1. Recommendation for mechanical strength

1. Means for releasing stored energy when robot is stopped shall be provided. Stored energy can be dangerous due to potential overshoot action on switching on. Pressure release valve shall be incorporated in robot design. The normal fuse valve, which is built-in the system, shall continue to operate before dangerous pressure is reached (as in industrial robots).
2. Safety features shall continue to be active, so that the robot will halt when necessary to protect people. Otherwise a person might be crushed between the robot and another object, person or the wall.
   Safety features, in case of AIBO (SONY Corporation, 2004), such as battery pack (lock indicator, unlock hole, insertion slot, release lever), mode indicator, AC adaption conversion pack, safety switch of "memory stick", pin for removing AIBO's extremities, over-current monitoring protection and tilt sensors should be active to eliminate dangerous conditions.
   Safety features, in case of Robomow (Friendly Robotics Acquisition Ltd., 2009), such as child guard/safety guard, lift sensor, sensor equipped bumpers, sealed batteries, perimeter switch, automatic departure warning alert shall continue to be active in order to protect residents under all emergency circumstances.
3. Dynamic brakes for the case of software crash or failure of power supply shall be provided. When software shuts down robots may follow arbitrary trajectories and run into a person or another personal asset (Jiang and Cheng, 1990).

2.2.2. Requirement of electrical safety

1. Hoses and cables shall be embedded inside the body of the robot. Otherwise residents could be injured by contact to them (as in industrial robots).
   To prevent shock hazard and injuries of persons, in case of AIBO, parents or guardians shall not open the cabinet, in order to avoid damaging cords, blades or housing.
   To prevent human health, in case of Robomow, residents shall not open the mower's covering hood with aim to avoid damaging internal electrical components.

2. The use of adequate insulation, cable cross-sections, panel covers shall prevent an electrical shock.
   In the case of AIBO, or any robot performing on batteries, there exist electrical hazards, such as fire, electric shock or chemical burn hazard in case that battery is mistreated and explosion hazard, if the battery is incorrectly placed.

3. The robot electrical equipment shall follow the appropriate instructions of the relevant requirements (IEC 60204-1, 2005).

2.2.3. Recommendation for software quality

1. Settings in order to maintain backup power for robots bearing RAM shall be checked, so that all data shall not be erased if there is a power failure causing a malfunction.
2. Robot with operating units shall use only ROM to prevent from changing the operating program.
3. A restart procedure shall be made available to operate after an emergency stop. In case of an improper restart, program and data could be saved on disk incorrectly which might affect the ability of the robot to perform specific safety critical tasks, as well as user's ability to manipulate it (as in industrial robots).
4. Restarting the robot by resetting a single switch shall not be possible. A more detailed restart procedure shall be provided to prevent any hazardous movements or similar situations. The objective of this instruction is that a simple restart method shall not be possible to deal with any arbitrary situation and, thus, a person may accidentally press a simple restart button with an improper or disoriented robot's start-up most probable leading to a hazard.
5. A built-in electronic hardware control system and/or safety operational software shall be selected to force the robot to shut itself down in an emergency, so that to prevent harmful accidents or property damaging.
6. The software implementing the safety rules on the robot, shall be completely isolated from the rest of the software operating the robot, in the sense that it cannot be affected by malfunctions caused by any other operating reason.
7. The software architecture should be built in such a manner so that safety is hierarchically above any other operation. Therefore, any detailed operation shall refer to the software implementing the safety rules.
8. A well-defined, built-in, self-checking safety software shall not result in a failure to shut itself down (as in industrial robots).
9. An expert, system-based malfunction diagnostics software shall be provided in order to determine malfunction causes. The absence of a comprehensive procedure may encourage random guessing rather than actually determining the true problem.
10. Robot motion simulator in 2-D or 3-D shall be provided to simulate robot operation under accident occurrence conditions. Since mismatches between the real and the virtual world may always occur, simulation data shall be tested on the real robots.
11. The robot shall have easily accessible safety commands and functions, so that the user shall be able to stop the robot in an emergency or shut down the power/software.
12. The software of the robot should bear a self-checking program that manages suspicious movements. Unless such a program exists, the user shall not be able to reach a control to stop a disoriented robot in proper time (as in industrial robots).
13. Online tutorials and help menus shall contain the appropriate instructions, so that users shall have direct access to information on how to operate the robot and with a good understanding of how the robot shall execute its task. It is strongly recommended, wherever possible, that the robot itself downloads the updated instructions and presents them to its user.
    In case of AIBO, the manufacturer should provide easy-accessed online software tutorials with aim to explain to the user the safety instructions about managing the wireless LAN function, the images/videos taken by the robot, the daily schedule, the connection with a PC or a mobile communication device, the remote control, the autonomous and the rest mode, respectively. This robotic pet shall be able to download any updated menu and provide them to the user.
    In case of Robomow, the manufacturer shall provide an operational video explaining the various type of modes available, namely deep sleep, manual, automatic, max, preset time, edge, eco and the safety practices that need to be followed.
14. The reliability of the software shall be thoroughly tested.
15. The settings for the recovery procedure shall be tested, as they are critical to putting the robot back to normal operation after a failure. Care shall be taken to make the user aware of any malfunction. Furthermore, a back-up power system shall be initiated by software, if needed (Jiang and Cheng, 1990).

2.2.4. Initial start-up test

1. The manufacturer should take the necessary measures to inform the user that regular tests on all safety protections need to be performed. Detailed instructions on how to perform these tests shall be provided.

   In the user's guide, the user of AIBO is informed that he should periodically check the AC adapter to avoid fire hazards, the receiving antenna for interference, the shield of interface cable for damaging, the lithium-Ion battery for leading, the enclosure for opening and the external flexible cord for damaging.

   The manual of Robomow informs the buyer, that periodically he ought to inspect blades for foreign material or debris, to clean base-station with a damp cloth, to confirm good contacts between base-station wires and contacts, to confirm that power supply is plugged at main power receptacle and that the coiled cord is properly placed in the holder, to check the reliable connection of the power cable with the wire connector and to confirm good contacts in the end of the green and the red wires.
2. Emergency stops shall execute the proper stop function. In particular, wiring, communication devices, sensors, electrical and utility connections, program bugs, speed mode; plugs should meet the performance criteria.

2.2.5. The requirement of emergency stop switch

1. The installation of stop and restart buttons shall be regularly looked after. An alarm realized by means of a stop button an/or an audible alert and/or a visual cue and/or an auditory cue and/or an occasional verbal exclamation, shall be installed. The user shall be informed about secondary stop procedures and the process to lead to start position.
2. The restart position shall be tested for its proper performance (as in industrial robots).
3. An emergency stop shall be installed and verified that remains functional preventing any dangerous function (Jiang and Cheng, 1990).

   Robomow is already equipped with an emergency stop switch on the manual controller in order to block its mowing path.

2.2.6. Recommendation for the sensory devices

1. Check thoroughly the safety performance and force level of tactile and proximity sensors and also check if the safety-related sensors are sensitive enough to detect small objects (in case of domestic service robots).
2. Check thoroughly all the sensors for malfunctions. Faulty sensors could damage the product or hurt people.

   AIBO's sensors such as integrated sensors (infrared, distance, acceleration, vibration) and input sensors (head, back, chin, paw) shall be checked thoroughly by the manufacturer for possible malfunctions.

   Robomow's sensors such as lift, rain, bumper, touch-sensitive shall be tested for improper function, prior to its disposal to the market.
3. Screen the privacy of the robot user by restraining the respective sensing abilities of the robot, especially when it is equipped with privacy sensitive sensors, such as cameras or microphones (Denning et al., 2009).
4. Consider the need that the robot should be able to operate (or shut down) safely with one or more of its sensors inoperative (Jenkins, 1993).

2.2.7. Recommendation for measuring the static performance

1. Take account of the results against manufacturer's specifications because results may differ or robot could function improperly due to inadequate design (Jiang and Cheng, 1990).

   Manufacturer should check if AIBO is functioning properly according to its own technical specifications. Functions that should be checked are the Wi-Fi, the operating light, the volume control switch, the game mode, the clinic mode, the house sitting mode and the energy station function.

   Manufacturer shall check Robomow's functions such as the manual shut off (equipment mounted and remote), the base-station control zone, the two step operator presence control, the manual controller panel and the manual drive speed control.

2.2.8. Recommendation for measuring the dynamic performance

1. Post-manufacture check of the full scale system, about its maximum, minimum, optimal speed and settings, start/end points, path, process (as in industrial robots).
2. The reliability of sensors shall be tested under dynamic conditions and safety features shall be provided to avoid a malfunction.
3. Control parameter settings shall be corrected according to manufacturing specifications while the robot remains stationary and safety information shall be provided to the user (Jiang and Cheng, 1990).

2.2.9. Malfunction

1. A specified checking procedure shall be selected to determine the cause of a malfunction.
2. A caution note shall be included in the user manual that only authorized personnel, having the necessary technical expertise and skill, should work on correcting a robot's malfunction. An emergency button shall be provided for unaware users when malfunction occurs, since unqualified users may get injured.

   User's manual of AIBO contains a warning, which legibly states that all malfunctions should be inspected by the nearest authorized agents.

   Robomow's user's manual indicates that every maintenance, service, replacement or inspection of worn or damaged parts should be carried out by service experts.

   Moreover, Robomow is equipped with an emergency stop switch on the manual controller. Pressing this emergency button blocks any hazardous movement, the rotation of sharp blades and mower's wheels within seconds.

1. Dimensions of implements such as plates, glasses or kitchen equipment should be considered when selecting a robot with grippers and plan well how these objects might be handled.
2. Objects shall be correctly oriented and gripped by the robot so that users should be able to stop the operation if the object is mishandled. Provide a sensing device to aware the robot of the mishandled object and equip the robot with an indicator, such as a loud noise, to alert residents that an object is mishandled.

2.2.10. Training

1. Providing that the robot bears parts that might be harmful, e.g. blades, picks, etc., then specific responsibilities concerning for the respective safety procedures shall be assigned to an adult user.

2. Full legible instructions shall be provided from the manufacturer in user's instruction manual in accordance to the particular robot model with all possible dangers related to the robot.
3. Any user responsible for the safety of the robot shall be trained appropriately, prior to operating the robot, and shall be aware of the dangers and precautions to be taken. In the special case of a robot bearing harmful parts a special, visible and legible sign shall be place on the robot by the manufacturer warning any user.
4. A training schedule on safety shall be established from the trained user to all who might come in contact with the robot and live in the house. We strongly recommend that the resident should firstly give dramatic representation on the hazards of using the robot and secondly inform correctly others with the necessary precautions (Bonney and Yong, 1985).

   AIBO's user should inform the unfamiliar residents about any fire, electrical or explosion hazards or chemical burn that might be caused by an improper handling of the device.

   Robomow's user should inform unaware residents about any inflammation, electrical, overheating, cutting or tripping hazards that might be caused by improper handling of the device or the rotation of sharp blades, or by thrown objects.
5. Warning signs shall be established to protect residents who may consider that they can ceaselessly be reckless with the operating robot, condition to the robot embedding harmful parts.

2.2.11. Structural components of the robot's content

1. A back-up procedure shall be established to halt the robot in case of: (i) software or hardware failure; (ii) violation of safety rules; (iii) lost of control or moving in an erratic manner and (iv) human error (as in industrial robots).
2. Safety measures at points of collision shall be added (in case of domestic robots with moving parts).
3. An emergency stop in case of robotic companion or humanoid robot, that the robot is out of control and may need to be shut off quickly. In case of pressing this button, at any time during normal operation, the robot has to stop within seconds. The emergency stop shall be accessible and recognizable (IEC 60204-1, 10.3.2: 2005, 10.7.1; ISO 13850).
4. An appropriate danger sign for electrical shock shall be generated if needed.
5. Make sure stops will not create a pinch point and equip the robot with built-in pressure – sensitive safety switch, which is activated in case that the robot exceeds its functional limits due to: (i) poor user judgment, (ii) mechanical failure or (iii) bug in programming.
6. Any material used to build up the robot shall be checked for deficiencies.

   All the material used to built AIBO's body, energy station, energy station pole, AC adapter, battery pack, pink ball, AIBOne and AIBO card shall be tested for deficiencies.

   All the material used to built Robomow's body, charger, base-station, perimeter wire, manual controller and power pack shall be checked for deficiencies.
7. The robot should not cause interference with any other electronic device.
8. Adequate electrical protection shall be provided against electrical surge such as regulators, filters, proper ground circuit.
9. The robot shall be equipped with a specific audio or visual signal, easily recognizable by everyone, to let people know whether it is on or off. Use a frequency that is not within the range of noise frequencies, in case of an audio signal.

2.2.12. Operation stage

1. Control access of unaware residents or guests because robot may pin unknowledgeable pets or people. The device can only be used by people who know how to operate it and who have read and fully understood the entire manual.
2. Take measures that the user will report any abnormal or disoriented operational condition observed.

   The safety switches and any sensor embedded in AIBO shall be tested under dynamic conditions and verified that they are in a proper working condition.

   The manufacturer should inform the buyer of Robomow system that he/she should keep all guards, shields, switches, safety devices and sensors in place. The user is not supposed to operate the robot if any parts are damaged or inoperable.
3. A visual checkout procedure shall be developed and implemented.
4. The designer should take into account the fact that objects will be dropped and liquids will be spilled upon the robot, eventually.
5. The developer shall consider that "owner's operational manual" may not be read thoroughly from the user. Supplementary material shall be included, such as video instruction. Operations instruction shall be able to be given to the user by the robot itself (e.g. by online material, downloaded by the robot itself).
6. The installation of the robots and its charging-station shall follow legible instructions and shall not require more than 1 h.
7. In case that domestic robot's function requires battery charging, the charging station shall be positioned according to the following rules:
   - It shall be placed on compact, flat and stable surface with good drainage, on level ground, preferably in a wide span area of the house.
   - Make sure that water or other liquids is not directed inside the charging station.
   - The entrance of the charging station shall be positioned so that the robot can enter.
   - The charging-station shall be well fastened to the ground away from explosive and/or flammable environments.

     AIBO's energy station shall not be placed on hot or wet surfaces or near devices that might cause interference.

     Robomow's charger station shall not be placed in sites subject to vibration and away from concrete, incline or hard surfaces and preferable at the largest area of the lawn surface. The lawn surface should be leveled with the base-station.
8. Except for replacement of not well-maintained or worn out tools, the device shall not require routine or extraordinary maintenance more than once a year.
9. The device shall not be subject to interferences such as high ambient noise, radio transmissions, unshielded computers, infrared remote controllers and magnetic fields.
10. Any internal malfunction shall be detected and the robot shall continue to operate, condition to the malfunction does not affect the safety rules.
11. The robot shall be capable of operating autonomously. Otherwise restricted control shall be operated through a remote controller.
12. Depending on the operation of the robot, it shall be as compact as possible with minimum size and weight, in order to maneuver into the house.
13. The preferable human robot interaction would be by natural language and/or vision.

14. The operational area shall be well defined and operational contingencies detected shall be eliminated (Jenkins, 1993). Such operational contingencies include: inability to determine location in the house; obstacles within its path; inoperative sensors; not accessible charging station; inability to follow user's commands; inability to follow the tasking path; charging station not charging; sensor failure; high temperature of an actuator or a motor; low battery, and so on.
15. An operative mechanism shall be applied, such as a lifting or rollover sensor, in order to reduce the chance of theft.
16. Nonwaterproof robots shall be prevented from washing with high-pressurized liquids and shall be prevented from being turned over in water, partially or completely.

2.2.13. Requirement of shape safety

1. Check again that there are no jagged edges, corners, sharp edges or picks as in case a corner sticks out of the robot might result in a hazard. Nevertheless, the robot shall be manufactured with smooth upper cover surface (ISO 12100-2, 4.2.1, 2003).
   Any material on AIBO or the supplied accessories shall be checked for jagged edges, corners, sharp edges or picks.
   Any material on Robomow or the supplied accessories shall be tested for corners that sticking out the covering hood because there might alert for potential hazard.

2. Any material used to build up the robot shall not contain carcinogenic, allergenic or toxic substances above the allowable limits.
3. The actuation mechanism of the robot shall be protected. The respective covers shall be kept in good condition (as in industrial robots).

3. Information for the user

In addition to the design requirements in Section 2.2, every manufacturer should make users aware they ought to follow the following instructions:

1. Plan well that the floor is flat. Otherwise, fill in any holes and remove objects such as extension cords, clothing items and books that block the path of the robot. In addition, obstacles types may include: stable (walls, stairs), changeable (doors), static (cabinets), floating (chairs, tables) and moving (residents, pets, guests, infants). It is proposed to operate the robot at scheduled times every day.
2. Children must not ride upon, misuse or attack the robot. In particular, the user should pay extra attention to infants because they are inattentive and extremely vulnerable. Moreover, pets shall be protected from sitting on the robot or disturbing its task.
3. User should set up a list of instructions concerning the task of the robot in a visible place in the house.
4. Do not contact the robot during its operation.
5. Prevent humans from throwing objects to the robot while it operates.
6. Ensure that all residents are well out of range of the robot motion when turning on the power.
7. Make sure that any accompanying sensor is placed away from light, microwaves, magnetic fields, heat or sound (Jenkins, 1993).
8. In addition, user must carefully read the instructions and fully understand them in order to prevent harmful injuries and pay extra attention to the symbols that appear on the robot and the manual; their shape and color are important for safety. We insist that the user should make adjustments according to the procedures described in the manual and in no case should he make any adjustments that are not expressly indicated (Jiang and Cheng, 1990).
9. Prevent residents, pets, children and guests from coming in contact with an operating robot.
10. Establish a regular routine to check the quality of the robot.
11. Check the indicators of the sensors regularly (Jiang and Cheng, 1990).
12. The power supply-transmitter shall be placed according to the following guidelines:
    - In a well-ventilated place without atmospheric pollution and heavy sunlight.
    - Preferably indoors.
    - If you place it outdoors, ensure it is protected in a well-ventilated housing to prevent water and humidity.
    - Draw carefully the cord from the charging station to the power supply transmitter. Do not shorten or lengthen it.
    - Allow permission to the power supply-transmitter unit only to aware residents.
13. If the robot is operating in close proximity to another one (by the same or a different manufacturer), then you should make adjustments so that the frequencies of the two robotic devices do not interfere with each other.
14. The environmental constraints such as heat, noise, chemicals and fire shall be under control. Furthermore, noise level shall be kept to a minimum limit. The air openings of the power supply unit shall be wiped out of residuals. An appropriate signaling shall be required if any environmental or electrical condition is violated. Robot shall be protected from heat or fire (Jenkins, 1993).

4. Risk assessment and risk reduction

4.1. Environmental constraints

The operational environment of a domestic robot shall not be affected by any living being such as residents, guests, parents, children, infants, the elderly, people with mental and physical impairments, and pets. Moreover, it should not be affected by an unstructured and chaotic environment. The constraints imposed by a household are definitely reasonable. Albeit, rooms are placed and created randomly, they are connected by different doors: specific outdoors or openings drive outside or into wardrobes and lockers. Further constrains are imposed by ladders, chimneys, various types of floor textures and hardness. Forgotten objects may be specifically and dynamically located, delicate and probably priceless and lighting conditions varies from absolute darkness to ablaze.

4.2. Risk assessment

The risk of a hazard is calculated as the product of two factors, as follows: risk = "probability" $\times$ "severity", where "probability" is the likelihood to occur a hazard and "severity" is the seriousness of the hazard, respectively. Thus, apart from setting a risk limit, a maximum severity must also be set, ensuring that the robot is not capable of causing undesired severities. In a nutshell, the functional safety should be in consistence with a detailed and briefed description of the hazards that indicate the maximum permissible risk level and severity.

5. Intrinsic safety

The concept of an intrinsically safe design aims to produce such morphologies that prevent an unpredictable injury to robot's users. Thus, intrinsic safety is dictated by the industrial design, whereas the study on software/hardware combination should reduce the probability of occurrence of possible harmful injuries (Wassink and Stramigioli, 2007).

6. List of factors that cause safety problems to domestic robots

The necessity for a comprehensive study of factors and hazards that cause safety problems in domestic environments by robots is emergent. Based on previous standards and studies, basic risks related to accidents caused by domestic robots are listed. The following classification attributes the factors into human error and robot's errors. Since more studies are accomplished, more factors could be added in the classification that follows. We note that a few of these errors may not be categorized in one list or another. The fundamental scope of this separation is to point out the *way* that a safety expert has to consider further, in order to determine the causes of problems or malfunctions (Rahimi, 1986; ISO 10218-1, 2011; Jiang and Cheng, 1990).

Error due to human factor involves faulty instructions to residents or misuse of the device.

- The operational task of the robot is unknown to the resident.
- User performing change of a part.
- User is unaware of the programmed movement of the robot.
- Curious unaware guest come close to the robot.
- User's programming fault.
- Lack of acquaintance with the relevant equipment of the device.
- The user is reckless.

Errors due to robot factor involve factors that may lead to software malfunctions. These are specifically: defective adjustments, poor logic design, improper implementation, support software design or failure, erroneous pointer, memory allocation, call, stack and unexpected timing. The software malfunction might result to any of the following:

- Robot system failures (mechanical, electrical...).
- Unintentional robot movement.
- Expected and unpredictable stops and starts of robot.
- Failure to stop.
- Grippers deficiencies.
- Human–robot environment (chemical, thermal conditions).
- Unreliability of existing safety devices.
- High speed of robot. The robot shall be prevented from moving at high speed (Bonney and Yong, 1985).
- Improper initial robot start-up procedures.
- Blocking of servos.
- Precision efficiency, deterioration.
- Faults of tools or mishandle of household objects.
- Fault in data transmission.
- Intentional deactivation of safety devices.

7. List of identified hazards towards machinery

On top of the measures taken by the manufacturer to avoid the risk of hazards that domestic robots might cause to the user, the product should also be evaluated against the following list of possible dangers:

- Mechanical Hazard (Crushing, Shearing, Cutting or severing, Entanglement, Impact, High pressure fluid injection, Shape, Acceleration/deceleration, inadequate mechanical strengths, Mass and velocity, Potential elements or elastic elements) (Bonney and Yong, 1985).
- Electrical Hazard (Contacts of persons with live parts, Breakdown, Leakage current, Electrostatic phenomena, Thermal radiation).
- Hazard generated by vibration (White-finger disease, Neurological, osteo-articular disorders).
- Hazard generated by radiation (electromagnetic fields, infra-red light, visible light and ultra-violet, light Laser radiation, X and γ rays, α and β rays, electron or ion beams, neutrons, ionizing or non-ionizing radiation).
- Thermal Hazard (Burns and scalds).
- Hazards generated by neglecting ergonomic principles in machine (physiological and psycho-physiological effects, human errors).
- Slipping, tripping and falling hazards. Trapping points can be caused by the movement of household objects (Bonney and Yong, 1985).
- Hazard generated by materials and substances (ingestion, inhalation of fluids, gases, mists, fumes, fibers, dusts or aerosols harmful toxic, corrosive, teratogenic, carcinogenic, mutagenic, irritant or sensitizing effect, biological hazards).
- Environmental Hazards (temperature, wind, snow, lightning, vapor, explosive or flammable atmospheres) (ISO 12100-1, -2, 2003).

8. Summary

In this paper, we reviewed standards and safety features related to the design of domestic robots, from the point of view of safe performance. We summarized and made references to fundamental issues such as risk assessment, intrinsic safety, safety of machinery, factors and hazards and their relevance to robotic products. As the domestic robot industry is forecast to expand rapidly in the near future, with highly sophisticated commercial robots in home use, standardization work needs to be stepped-up. The paper concludes with a method that can be considered as a fundamental step towards any certification procedure, which is an important process for effective commercialization. Finally, we feel that this procedure will meet manufacturers' and users' requirements with aim to guaranty the safety of this emerging technology, in terms of general public acceptance to domestic robotics.

According to our proposal manufacturers wishing to verify the safety of their prospective domestic robotic products should follow the following steps:

1. Submit the necessary papers, according to the requirements of safety guidelines, to the safety commission.
2. The commission sets-up a safety committee comprising safety scientists as a third party.
3. The safety committee carries out an assessment with the view to approve the placement of the product in the personal robotics market whilst checking the following issues that we have analyzed above:
   - Design requirements and protective measures.
   - Information made available to the user.
   - Risk assessment and risk reduction.
   - Intrinsic safety.
   - List of factors that cause safety problems to domestic robots.
   - List of identified hazards towards machinery.
4. Based on the examination report of the safety committee, the safety commission determines a final statement and issues a judgment report to verify the adequacy for safety of the manufacturer's product.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.ssci.2012.05.009.

References

Bonney, M.C., Yong, D., 1985. Robot Safety. International Manufacturing Technology. IFS Publications Ltd., UK.

Corrales, J.A., Candelas, F.A., Torres, F., 2011. Safe human–robot interaction based on dynamic sphere-swept line bounding volumes. Robotics and Computer-Integrated Manufacturing 27, 177–185.

Crowley, J., 1989. Planning and execution of tasks for a domestic robot. Robotics and Autonomous Systems 5 (3), 257–272.

Denning, T., Matuszec, C., Koscher, K., Smith, J.R., Kohno, T., 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th International Conference on Ubiquitous, Computing, pp. 105–114.

Etherton, J., Sneckenberger, J.E., 1990. A robot safety experiment varying robot speed and contrast with human decision cost. Applied Ergonomics 21 (3), 231–236.

European Community, 2000. Guide to the implementation of directives based on the new approach and the global approach.

Fei, B., Ng, W.S., Chauhan, S., Kwoh, C.K., 2001. The safety issues of medical robotics. Reliability Engineering and System Safety, 183–192.

Friendly Robotics Acquisition Ltd., 2009. Robomow operating and safety manual. <http://www.robomow.com/pdf/2010/rl_manual_en.pdf>.

Harper, C., Dogramadzi, S., Tokhi, O., 2009. Developments in vocabulary standardisation for robots and robotic devices. In: Proceedings of the Twelfth International Conference on Climbing and Walking Robots and the Support Technologies for Mobile Machines, Istanbul, Turkey.

IEC 60204-1, 2005. 10.7.1 Devices for emergency stop shall be readily accessible.

ISO 10218-1, 2011. Robots for industrial environments – safety requirements – Part I: robot.

ISO 10218-2, 2011. Robots and robotic devices. Safety requirements for industrial robots. Part 2: robot systems and integration.

ISO 12100, 2010. Safety of machinery—general principles for design, risk assessment and risk reduction.

ISO 12100-1, -2, 2003. Safety of machinery – basic concepts, general principles for design.

ISO 13857, 2008. Safety of machinery—safety distances to prevent danger zones being reached by the upper limbs.

ISO 14120, 2002. Safety of machinery—guards—general requirements for the design and construction of fixed and movable guards.

ISO 14121. 1999. Safety of machinery – principles of risk assessment.

ISO 14971, 2000. Medical devices – application of risk management to medical devices.

ISO Standard, ISO 8373, 2007(E). Manipulating industrial robots – vocabulary.

ISO/FDIS 8373, 2012. Robots and robotic devices – vocabulary. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=55890>.

ISO/IEC Guide 50, 1999. Safety aspects – guidelines for their inclusion in standards.

Jenkins, F., 1993. Practical requirements for a domestic vacuum-cleaning robot. Technical Report.

Jiang, B., Cheng, O., 1990. A procedure analysis for robot system safety. International Journal of Industrial Ergonomics, 95–117 (Industrial Engineering Department, Auburn University, AL 36849, USA).

Japanese Standard, JIS B0134, 1998. Manipulating industrial robots – vocabulary.

Japanese Standard, JIS B0185, 2002. Intelligent robots – vocabulary.

Japanese Standard, JIS B0186, 2003. Mobile robots – vocabulary.

Japanese Standard, JIS B0187, 2005. Service robots – vocabulary.

Kabe, T., Tanaka, K., Hiroyoso, I., Sugimoto, N., 2010. Consideration on safety for emerging technology – case studies of seven service robots. Safety Science 48, 296–301.

Kilmer, R., 1982. Safety sensor systems for industrial robots. In: Proceedings of the Robots VI Conference and Exposition. Society of Manufacturing Engineers (SME), MI, pp. 479-491.

Korean Standard, KS B 6934, 2006. Performance measure methods for household cleaning robots.

Korean Standard, KS B 6935, 2006. Service robots – safety guidelines.

Korean Standard, KS B 6936, 2006. Service robots – safety instructions.

Korean Standard, KS B 6937, 2006. Service robots – vocabulary – Part 1. Classification & general terms.

Korean Standard, KS B 6938. Service robots – vocabulary – Part 2. Mobility and intelligence.

Korean Standard, KS B 6960, 2007. Service robots – safety requirements – electrical aspects.

Korean Standard, KS B 6961, 2007. Service robots – test methods for mechanical strength – Part 1. Load test.

Korean Standard, KS B 6962, 2007. Service robots – test methods for mechanical strength – Part 2. Fall and distortion test.

Korean Standard, KS B 6966, 2008. Service robots – safety requirements for shape.

Kulic, D., Croft, E., 2006. Real-time safety for human–robot interaction. Robotics and Autonomous Systems 54, 1–12.

Lee, S., Yu, S., Choi, J., Han, C., 2011. A methodology to quantitatively evaluate the safety of a glazing robot. Applied Ergonomics 42, 445–454.

Nagamachi, M., 1986. Human factors of industrial robots and robot safety management in Japan. Applied Ergonomics 17 (1), 9–18.

OSHA Technical Manual (OTM), 1999. Industrial robots and robot system safety, section IV (Chapter 4). <http://www.osha.gov/dts/osta/otm/otm_iv/otm_iv_4.html>.

Rahimi, M., 1986. Systems safety for robots: an energy barrier analysis. Journal of Occupational Accidents, 127–138.

Seungbin, M., Gurvinder, S.V., 2009. Survey on ISO standards for industrial and service robots. In: Proceedings of the ICROS-SICE International Joint Conference, Japan.

SONY Corporation, 2004. ERS-7M2 Entertainment Robot AIBO: user's guide (basic). <http://www.aiai.ed.ac.uk/project/aibo/documents/ERS-7M2/AIBO-Basic-Manual.pdf>.

Wassink, M., Stramigioli, S., 2007. Towards a novel safety norm for domestic robotics. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, USA.

Wyrobek, K., Berger, E., Van der Loos, M., Salisbury, K., 2008. Towards a personal robotics development platform: rationale and design of an intrinsically safe personal robot. In: IEEE International Conference on Robotics and Automation Pasadena, CA, USA.