International Journal of Occupational Safety and Ergonomics
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tose20

Paradigms and Safety Requirements for a New Generation of Workplace Equipment

Tadeusz Missala[a]
[a] Industrial Institute for Automation and Measurements PIAP, Poland
Published online: 08 Jan 2015.

International Journal of Occupational Safety and Ergonomics (*JOSE*) 2014, Vol. 20, No. 2, 249–256

Paradigms and Safety Requirements for a New Generation of Workplace Equipment

Tadeusz Missala

Industrial Institute for Automation and Measurements PIAP, Poland

A workplace in the manufacturing industry consists of not only stationary equipment (e.g., machining centres, fixed robots) but also mobile equipment (e.g., automated guided vehicles, mobile robots), with both kinds co-operating directly with workers. Workplace equipment should not only be safe, it should also not generate fear or anxiety; still better if it should inspire calm and confidence. In view of robot laws, this article presents selected examples of robot–human co-operation, reviews safety requirements and safety functions developed to date. It also proposes a package of selected new safety functions, necessary to fulfil this paradigm. It also suggests and presents examples of actions that can make the workplace a human-friendly environment and presents examples of such actions.

safety requirements workplace   industrial robots   mobile robots

1. INTRODUCTION

Fast progress in control science and robotics opens new possibilities in manufacturing, introducing simultaneously new occupational safety and health problems. Solving these problems and creating a sufficiently safe workplace, or even a safe working environment, is a great challenge and great social responsibility of scientists and engineers. The discussion on this subject is taking place now on various technical fora (e.g., McDermott [1]).

My intention is to share my thoughts with specialists in occupational safety, using human–robot workspace as an example.

At the beginning of the 1970s, a new manufacturing tool, a robot, initiated a manufacturing and workplace revolution. This revolution has had two phases. First, industrial robots were introduced; they were stationary and separated from humans. Now, there are autonomous mobile robots: stationary and mobile robots are working together with humans. This phase is at our doors [2].

Inevitably, any industrial activity may cause harm to humans and the natural environment. Our goal is to decrease that possibility to an insignificant minimum.

Risk, a product of the possibility of harm and the severity of its consequences, is a measure of discomfort at work. The smaller the risk, the greater the safety. Safety comfort is defined as tolerable risk, the maximum level of risk that can be socially and financially accepted. Reaching tolerable risk requires hazard and risk analysis, defining the safety functions, and establishing and realizing their integrity levels.

2. SAFETY CONCEPT AND MEASURES

2.1. As Low As Reasonably Practicable (ALARP)

The concepts of ALARP and tolerable risk are the general risk assessment principles presented in Standard No. IEC 61511-3:2004 [3]. It is one particular principle which can be applied to determine the tolerable risk and safety integrity levels (SIL). It is not, in itself, a method for determining SIL. Standard No. IEC 61508-5:2010 [4] and

Correspondence should be sent to Tadeusz Missala, Industrial Institute for Automation and Measurements PIAP, Al. Jerozolimskie 202, 02-486 Warszawa, Poland. E-mail: tmissala@piap.pl.

Missala [5] presented corresponding methods. In the case of real devices, systems or workplaces, the following three situations are possible: I = risk is so great that it is rejected altogether, the object of analysis should be redesigned; III = risk is, or has been made, insignificant, no activities are required; or II = risk is between I and III and is reduced to a tolerable level (Figure 1).

With respect to risk class II, the ALARP principle recommends that risk should be reduced as far as reasonably practicable, or to a level which is as low as reasonably practicable (hence, ALARP). This level of risk is considered to be the same as tolerable.

TABLE 1. Sample Interpretation of Risk Classes [2]

Risk Class	Interpretation
I	intolerable risk
II	undesirable risk, and tolerable only if risk reduction is impractical or if the costs are grossly disproportionate to the improvement gained
III	negligible risk

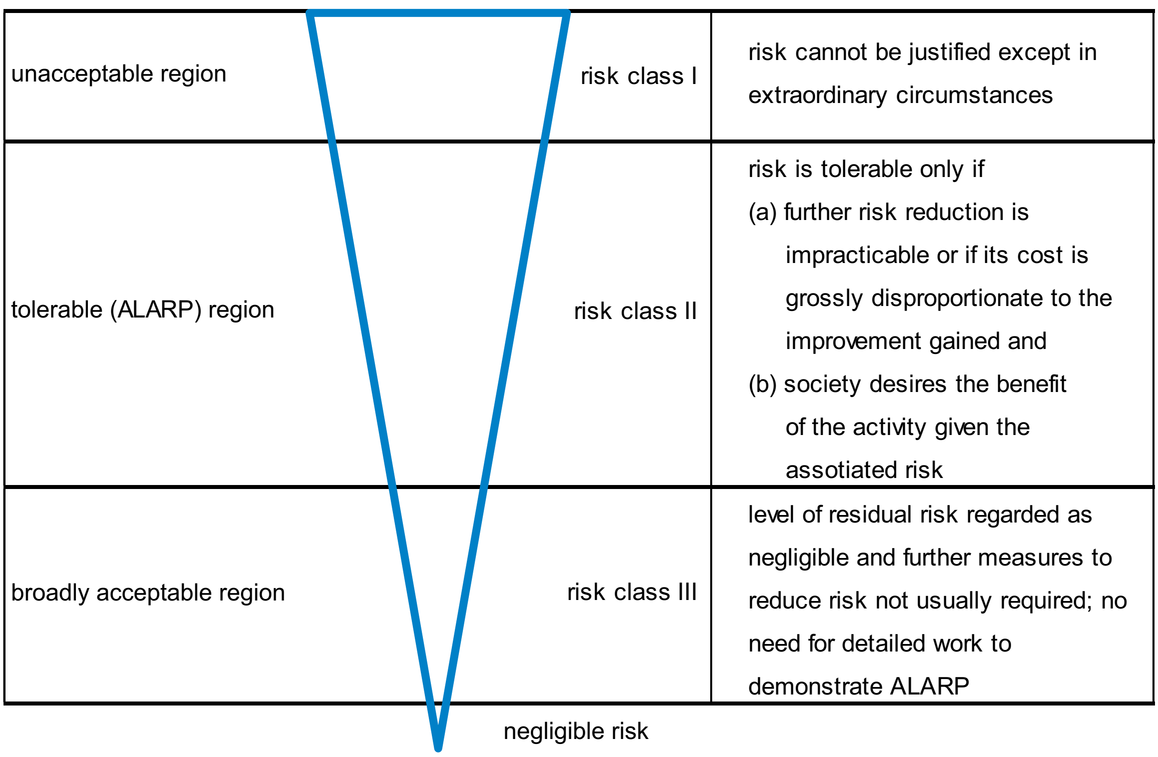

Figure 1. ALARP (as low as reasonably practicable) and tolerable risk [2].

TABLE 2. Sample Risk Classification of Incidents [2]

	Risk Class (Consequence)			
Probability	**Catastrophic**	**Critical**	**Marginal**	**Negligible**
Likely	I	I	I	II
Probable	I	I	II	II
Possible	I	II	II	II
Remote	II	II	II	III
Improbable	II	III	III	III
Incredible	II	III	III	III

Notes. I = unacceptable region, II = tolerable (as low as reasonably practicable, ALARP) region, III = broadly acceptable region.

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. When using the ALARP principle, care should be taken to ensure that all assumptions are justified and documented.

It is necessary to define three regions of Figure 1 in terms of the probability and consequence of an incident. Table 1 shows sample interpretations of the three risk classes. Table 2 interprets each risk class with the concept of ALARP.

Having determined a tolerable risk target, it is possible to determine SIL of safety functions.

2.2. Safety Integrity Requirements

Depending on the identified risk level, safety functions at various integrity levels should be applied. SIL is defined with probabilistic measures [6] and four SIL are introduced [7]. Tables 3–4 provide corresponding data.

The required SIL for each safety function is determined on the basis of the results of risk analysis. If risk is analysed with quantitative methods [3, 4], the requirement is defined as the probability of dangerous failure per hour. If risk is analysed with qualitative methods [3], the result is defined as SIL.

TABLE 3. Safety Integrity Levels (SIL): Target Failure Measures for Safety Function Operating in High Demand or Continuous Mode of Operation [2]

SIL	Probability of Dangerous Failure per Hour
4	$\geq 10^{-9}$–$<10^{-8}$
3	$\geq 10^{-8}$–$<10^{-7}$
2	$\geq 10^{-7}$–$<10^{-6}$
1	$\geq 10^{-6}$–$<10^{-5}$

3. DEFINITION OF HUMAN–ROBOT WORKSPACE: FIRST PHASE IN ROBOTICS

3.1. Introduction

The point of this first phase in the world of stationary industrial robots is to separate working robots from the human. Access the robot zone is permitted for programmers and maintenance personnel only and entering is possible when a robot is working in the service mode, e.g., all velocities are reduced to about one quarter of their full scale. When a robot is working in the automatic mode, the work zone is separated with barriers, fences, controlled doors, light curtains, laser scanners and other safety measures, appropriate for preventing humans from entering the dangerous zone. Activating any safety device causes an emergency stop of the robot.

The main applications developed for robots were painting, cutting (with gas and plasma); welding (with gas and an electric arc); some kinds of automated assembly; packing; positioning on platforms, trucks and palettes; and handling objects. These applications are currently in use and will continue to be used in future. Asimov's first law of robotics[1], i.e., "A robot may not injure a human being or, through inaction, allow a human being to come to harm" is a necessary and sufficient condition of safe work in those applications.

Many studies considered safety problems related to such installations. Karwowski, Rahimi and Mihaly compared a Kentucky-based appliance manufacturer before and after computer automation of the assembly process [8]. The number of dangerous accidents during one-year pre- and post-automation was compared, following the American National Standards Institute (ANSI) classification of the

TABLE 4. Relationship Between Residual Error Rate of Transmission Protocols and Safety Integrity Level (SIL) [5]

SIL	Probability of Dangerous Failure per Hour	Maximum Permissible Residual Error Rate
4	$\geq 10^{-11}$–$<10^{-10}$	$\geq 10^{-11}$–$<10^{-10}$
3	$\geq 10^{-10}$–$<10^{-9}$	$\geq 10^{-10}$–$<10^{-9}$
2	$\geq 10^{-9}$–$<10^{-8}$	$\geq 10^{-9}$–$<10^{-8}$
1	$\geq 10^{-8}$–$<10^{-7}$	$\geq 10^{-8}$–$<10^{-7}$

[1] http://en.wikipedia.org/wiki/Three_Laws_of_Robotics

nature of injury. Rachimi and Karwowski reviewed critical issues in robot–human interaction and proposed studies of human aspects of the design of robotic systems [9]. Karwowski and Rachimi investigated the influence of robot speed and its unpredictable motions on safety in a robotic plant [10]. Karwowski, Rahimi, Parsaei, et al. discussed the effectiveness of simulation techniques for robot safety training, showing robot-related accidents [11]. Zurada, Karwowski and Graham reviewed problems related to sensory integration and management of uncertainty in robot safety systems [12].

Taking another point of view, Kosiński, Grabowski and Siemiątkowska suggested a neural safety system of two cameras to recognize a hazardous situation and prevent accidents in robotic plants [13].

In his numerous publications, Missala tackled various aspects of safety in robotic plants: system aspects of safety [14]; risk assessment conducted with layer of protection analysis (LOPA) [15]; functional safety, especially safety integrity of robots considered as safety-related systems (surgery robots [16], turn-wrist robots [17] and walking robots [18]); and an integrated manufacturing system [19].

TABLE 5. Safety Functions of Industrial Robots [20, 21]

Safety Function	SIL
Safety-related control system	2
Emergency stop	2
Protective stop	2
Speed reduction control	2
Initiation of motion at full speed from pendant control	2
Enabling function	2
Prevented unattended motion	2
Prevented unexpected start of robot	2
Speed reduced to safe, while robot co-operates with human	2
Robot arm position monitoring, while robot co-operates with human	2
Up to 80 W and 150 N imposed on robot arm, robot co-operates with human	2
Limited robot arm movements, other than mechanical	2
Programmable limited span of robot movement	1/2/3
Other safety functions of safety-related control system	2

Notes. SIL = safety integrity level.

3.2. Current Safety Requirements

The newly established Standards No. ISO 10218-1:2011 [20] and ISO 10218-2:2011 [21] present safety requirements for stationary industrial robots. Table 5 lists the safety functions these standards define. Those standards result from long-standing standardization work and can be considered as sufficient for stationary industrial robotic applications.

4. MOBILE AND OTHER NONSTATIONARY ROBOT WORLD OF TODAY [2]

The past 20 years have resulted in many designs and realizations of nonstationary robots for many purposes or as cybernetic toys. A list of such robots is always incomplete as new designs arrive almost daily:

- humanoid robots [22]: some for nonconventional use, e.g., in astronautics [23] to help astronauts aboard the International Space Station;
- android robots: numerous corporations develop software for them, e.g., ST-Ericsson [24], Linaro [25], The Astonishing Tribe (TAT) [26]);
- personal care–mobile servant robots [22]: they are capable of moving freely to perform tasks and/or handle objects; they can be divided into home servant and public guide robots;
- personal care–physical assistant robots (exoskeleton robots) [27]: they assist a person in performing tasks, supplement or augment capabilities, bring functionality of a frail or elderly person to that of an able-bodied person, and augment the performance of able-bodied users;
- personal care–person carrier robots (transport robots, e.g., segway [3], robotic lifts and transfer

[2] This section does not discuss military, antiterrorist, surgical or invasion medical robots.

[3] http://www.segway.com/

wheelchairs with an onboard arm): they transport humans to different locations by means of autonomous navigation, guidance and locomotion;
- medical robots for diagnostics, e.g., for diagnosing neural diseases [28];
- medical robots for rehabilitation;

For such applications, Missala formulated a new paradigm: "A robot is a human's friend" [2]. In other words, a robot should be safe, i.e., the probability of dangerous failure should be extremely low. A robot's behaviour should inspire sufficient confidence: "A robot is watching me and its movements will not hurt me".

A humanoid female robot is an example of such a solution. The HRP-4C female humanoid robot, developed by Kawada Industries and the National Institute of Advanced Industrial Science and Technology in Japan, moves like a human, understands commands via voice recognition, and sings using a voice synthesizer.

TABLE 6. Safety Functions of Public Guide Servant Robots

Safety Function	SIL
Holding function of brakes	1
Speed limit	2
Control to bring motion to safe stop and ensure safe disembarking	2
Fixed/movable guards around wheels	2
Power deactivated if terminal is detected open	1
Outer cover	1
High-friction tyres	1

Notes. SIL = safety integrity level.

TABLE 7. Safety Functions of Physical Assistant Robots (Exoskeleton Walker Robots)

Safety Function	SIL
Cushioned sharp edges	1
Emergency stop	1
Speed limit and safety-related speed control	1
Electric current limit	1
Safeguard against fire	3
Charged activation control	2

Notes. SIL = safety integrity level.

Tables 6–9 present safety requirements for personal care robots developed on the basis of Draft Standard No. ISO/DIS 13482:2012, which has not been transformed into a standard. No safety standards for medical robots have been published yet; Directive 93/42/EEC is a unique document in this area [29].

TABLE 8. Safety Functions of Personal Transport Robots

Safety Function	SIL
Speed limit and safety-related speed control	2
Fixed/movable guards around wheels	2
Imposed limits and control to avoid sudden acceleration	1
Controlled stop during embarkation/ disembarkation	1
Antivandalism measures (key or password start)	2
Active mobility balance control	2
Charging power activated only when motion is activated	1
Displayed charging status	1
Heat dissipation	1
Secondary independent brake control to bring motion to safe stop and ensure safe disembarking	2

Notes. SIL = safety integrity level.

TABLE 9. Safety Functions of Robotic Lifts and Transfer Wheelchairs With Onboard Arm

Safety Function	SIL
Speed limit	2
Mobility balance control	2
Intelligent/mechanical braking	2
Seat belt control	2
Control to bring motion to safe stop and ensure safe disembarking	2
Control/intelligent braking to bring motion to safe stop	2
Fixed/movable guards around wheels	2
Control to avoid sudden acceleration	1
Controlled stop during embarkation/ disembarkation	1
Enclosed electrical terminals, power deactivated if terminal is open	1
Heat dissipation	1
Shock absorption	2
Noncontact obstacle detection	2
Antivandalism measures (key start)	2

Notes. SIL = safety integrity level.

5. DEFINITION OF HUMAN–ROBOT WORKSPACE: EXPECTED PHASE IN ROBOTICS

5.1. Characteristics

The characteristic feature of the second phase is common use, apart from classic industrial, mobile, intelligent robots capable of performing autonomous complicated transportation and work tasks. In their report developed for the European Commission, Forge and Blackman confirmed that this trend was dominating and long-lasting [30].

A robot should assist, help and support humans. This leads to a general transformation of the working environment and work habits. Robots and humans will work together in close vicinity. Industrial stationary and mobile robots will co-operate with humans in manufacturing. The goal is to reach friendly co-operation between robots and humans. Therefore, military, police, anti-terrorist and medical applications will not be considered here.

Future, reasonably foreseeable manufacturing functions of industrial mobile robots may include

- individual transport for humans, e.g., segway;
- transport of materials (development of automated guided vehicles tending towards autonomous pick-up transport devices);
- transport and tool handling;
- support for humans in manipulating assembled parts, including heavy ones;
- manual work [31], thus replacing humans in uncomfortable situations;
- transport of machine tools between warehouses and the workplace;
- operation of computer-controlled machine tools, thus replacing operators in uncomfortable situations;
- inspection of tanks and other places difficult to access.

The external appearance of robots can vary; they can look like humans, pushcarts, trucks or trolleys.

5.2. Safety in a Workplace With Mobile Industrial Robots

As has been said, the manufacturing world is increasingly complicated: direct co-operation between humans and industrial robots, stationary and mobile, is often necessary, taking place at a not very low speed of the robot arm. It is a question then if the aforementioned safety functions are sufficient and if their required integrity level meets the paradigm of human-friendliness. In this author's opinion, the present situation is not satisfactory.

Tables 10–11 propose some safety functions. The safety functions in Table 11 are especially

TABLE 10. Safety Functions of Industrial Robots to Be Used in the Vicinity of Humans

Safety Function	SIL
Speed limit circuit	2/3
Mobility balance control	2
Intelligent/mechanical braking	2/3
Control/ intelligent braking to bring motion to safe stop	2
Fixed/movable guards around wheels	2
Control to avoid sudden acceleration	1
Safe stop control during embarkation/ disembarkation	1
Enclosed electrical terminals, power deactivated if terminal is open	1
Heat dissipation	1
Shock absorption	2
Emergency stop	2/3

Notes. SIL = safety integrity level; SIL 2 or 3 depends on the results of risk assessment.

TABLE 11. Human-Friendly Safety Functions of Industrial Robots to Be Used in the Vicinity of Humans

Safety Function	SIL
Safety distance when bypassing human	2/3
Limited speed when bypassing human	2/3
Limited speed when approaching human	2/3
Signal when human approaches robot	2
Signal of good intentions when approaching human	2
Reaction to voice signals/commands from human	3
Reaction to gesture signals/commands from human	3
Antivandalism hardware	3
Antivandalism software	3
Wireless emergency stop	2/3

Notes. SIL= safety integrity level; SIL 2 or 3 depends on the results of risk assessment.

interesting: their intention is to create a working environment that workers find friendly and understandable. To find out if those safety functions are sufficient, suitable risk assessment and an analysis of human behaviour are necessary.

6. CONCLUSION

An overview of present and future working environments leads to the conclusion that a new look at safety functions is necessary. Table 11 presents the first proposal of how this problem can be solved: it opens a discussion.

REFERENCES

1. McDermott TJ. Responsibility & integrity a must in manufacturing. DesignNews. 2012. Retrieved February 11, 2014, from: http://www.designnews.com/author.asp?section_id=1365&doc_id=237257.
2. Missala T. Safety of robots in a neighborhood of the people and the new law of robotics. Pomiary Automatyka Robotyka PAR. 2012;(1):48–52. Retrieved February 11, 2014, from: https://www.par.pl/2012/PAR_01_2012_Missala_48_53.pdf.
3. International Electrotechnical Commission (IEC). Functional safety—safety instrumented systems for the process industry sector—part 3: guidance for the determination of the required safety integrity levels (Standard No. IEC 61511-3:2004). Geneva, Switzerland: IEC; 2004.
4. International Electrotechnical Commission (IEC). Functional safety of electrical/electronic/programmable electronic safety related systems—part 5: examples of methods for the determination of safety integrity levels (Standard No. IEC 61508-5:2010). Geneva, Switzerland: IEC; 2010.
5. Missala T. Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa [An analysis of the requirements and methods of proceeding in assessing risk and determining the required level of of safety integrity]. Warszawa, Poland: Oficyna Wydawnicza Przemysłowego Instytutu Automatyki i Pomiarów; 2009.
6. International Electrotechnical Commission (IEC). Functional safety of electrical/electronic/programmable electronic safety related systems—part 1: general requirements (Standard No. IEC 61508-1:2010). Geneva, Switzerland: IEC; 2010.
7. International Electrotechnical Commission (IEC). Functional safety of electrical/electronic/programmable electronic safety related systems—part 4: definitions and abbreviations (Standard No. IEC 61508-4:2010). Geneva, Switzerland: IEC; 2010.
8. Karwowski W, Rahimi M, Mihaly T. Effects of computerized automation and robotics on safety performance of a manufacturing plant. Journal of Occupational Accidents. 1988;10(3):217–33.
9. Rahimi M, Karwowski W. A research paradigm in human-robot interaction. Int J Ind Ergon. 1990;5(1):59–71.
10. Karwowski W. Rahimi M. Worker selection of safe speed and idle condition in simulated monitoring of two industrial robots. Ergonomics. 1991;34(5):531–46.
11. Karwowski W, Rahimi M, Parsaei H, Amarnath BR, Pongpatanasuegsa N. The effect of simulated accident on worker safety behavior around industrial robots. Int J Ind Ergon. 1991;7(3):229–39.
12. Zurada J, Karwowski W, Graham JH. Sensory integration and management of uncertainty in robot safety systems: a review. International Journal of Computer-Integrated Manufacturing. 1998;11(3):262–73.
13. Kosiński RA, Grabowski A, Siemiątkowska B. Dwukamerowy, neuronowy system bezpieczeństwa do wykrywania sytuacji niebezpiecznych na zautomatyzowanych stanowiskach pracy [Two cameras neural safety system for the advanced recognition of danger situations on automated works stands]. In: Materials of Conference AUTOMATION. Warszawa, Poland: PIAP; 2006. p. 119–27.
14. Missala T. Bezpieczeństwo robotów przemysłowych. Aspekty systemowe [Safety of industrial robots. System aspects]. Prace Naukowe Instytutu Cybernetyki Technicznej Politechniki Wrocławskiej. Konferencje. 1993;(41):374–80.

15. Missala T. Ocena ryzyka w gnieździe zrobotyzowanym—propozycja postępowania [Safety assessment for a robotized plant—proposal of proceeding]. Prace Naukowe Instytutu Cybernetyki Technicznej Politechniki Wrocławskiej. Konferencje. 2001;(46):345–52.
16. Missala T. Robot jako system związany z bezpieczeństwem [Robot as a safety-related system]. In: Tchoń K, editor. Postępy robotyki: przemysłowe i medyczne systemy robotyczne [Progress in robotics: industrial and medical robotic systems]. Warszawa, Poland: Wydawnictwa Komunikacji i Łączności; 2005. p. 183–91.
17. Missala T. Nienaruszalność bezpieczeństwa przegubowych konstrukcji robotów [Safety integrity of turn-wrist robot construction]. In: Tchoń K, editor. Postępy robotyki: systemy i współdziałanie robotów [Progress in robotics: systems and co-operation of robots]. Warszawa, Poland: Wydawnictwa Komunikacji i Łączności; 2006. p. 139–48.
18. Missala T. Nienaruszalność bezpieczeństwa robotów kroczących—analiza wstępna [Safety integrity of walking robots—preliminary analysis]. In: Thoń K, Zieliński C, editors. Problemy robotyki [Problems of robotics]. Politechnika Warszawska—Prace Naukowe—Elektronika (No. 166). Warszawa Poland: Oficyna Wydawnicza Politechniki Warszawskiej; 2008. p. 597–606.
19. Missala T. Bezpieczeństwo funkcjonalne zintegrowanego systemu wytwarzania [Functional safety of integrated manufacturing system]. In: Thoń K, Zieliński C, editors. Problemy robotyki [Problems of robotics]. Politechnika Warszawska—Prace Naukowe—Elektronika (No. 175). Warszawa Poland: Oficyna Wydawnicza Politechniki Warszawskiej; 2010. p. 275–84.
20. International Organization for Standardization (ISO). Robots and robotic devices—safety requirements for industrial robots—part 1: robots (Standard No. ISO 10218-1:2011). Geneva, Switzerland: ISO; 2011.
21. International Organization for Standardization (ISO). Robots and robotic devices—safety requirements for industrial robots—part 2: robot systems and integration (Standard No. ISO 10218-2:2011). Geneva, Switzerland: ISO; 2011.
22. Murray C. Slideshow: humanoid robots get real. DesignNews. 2011. Retrieved February 11, 2014, from: http://www.designnews.com/document.asp?doc_id=233766.
23. Montalbano E. NASA explores humanoid robot design. DesignNews. 2012. Retrieved February 11, 2014, from: http://www.designnews.com/document.asp?doc_id=243445.
24. Happich J. ST-Ericsson launches a low-cost and compact Android-ready platform. EE Times. 2010. Retrieved February 11, 2014, from: http://www.eetimes.com/document.asp?doc_id=1270515.
25. Clarke P. Accelerated Android 4.0 available on ARM development boards. EE Times. 2011. Retrieved February 11, 2014, from: http://www.eetimes.com/document.asp?doc_id=1260844.
26. Johansson D. Android platforms—four tips for UI development. EE Times. 2008. Retrieved February 11, 2014, from: http://www.eetimes.com/document.asp?doc_id=1275158.
27. Beciri D. Cyberdyne HAL-5—exoskeleton robot. RobAid beta. 2009. Retrieved February 11, 2014, from: http://www.robaid.com/bionics/cyberdyne-hal-5-exoskeleton-robot.htm.
28. Neural recordings: robot reveals the inner workings of brain cells. 2012. Retrieved February 11, 2014, from: http://www.gtresearchnews.gatech.edu/robot-brain-recording/.
29. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices. OJ. 1993;L169:1–43. Retrieved February 11, 2014, from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF.
30. Forge S, Blackman C. A helping hand for Europe: the competitive outlook for the EU robotics industry. Seville, Spain: European Commission, Joint Research Centre; 2009. Retrieved February 11, 2014, from: http://ftp.jrc.es/EURdoc/JRC61539.pdf.
31. Murray C. GM's Robo-glove mimics human hand. DesignNews. 2012. Retrieved February 11, 2014, from: http://www.designnews.com/document.asp?doc_id=240915.