Safety of robots in a neighborhood of the people and the new law of robotics

Tadeusz Missala

Industrial Research Institute for Automation and Measurements PIAP

Abstract: Interoperability between robots and humans is becoming more and more frequent. One of significant problems is to keep safety. Selected problems of safety in case of industrial robot applications as well as by personal care application for human are presented.

Keywords: robots safety, industrial robots, personal robots

1. Introduction

Last years of robotics development lead to situations, in which the near or direct cooperation between people and robots is more and more frequent. The report [1] elaborated for EU Commission confirms that this trend is dominating and long-lasting.

There is possible to indentify the following blocks of situation, robots enter cooperation with people:
- industry applications – materials and elements handling, as well as elements workmanship,
- non-medical care (domestic, shopping etc.) applications,
- medical applications – care and surgery,
- war, police, antiterrorist etc. applications.

The two first groups of above mentioned situations will be considered.

2. General remarks

2.1. Introduction

As a robot is an electrical driven machine, requirements of Machine Directive [2], Low Voltage Directive [3] and EMC Directive [4] shall be applied. The main requirement of these legislation acts is to provide the suitable safety for people and the natural environment. This is achieved in some steps, according to safety strategy, as follows (terms according [12]):
- inherent safety design [5],
- hazards identification, e.g. by HAZOP studies [13],
- safety functions definition [6, 7],
- risk assessment, e.g. graph method [6, 13] or table method [7],
- safety requirements for safety functions definition [6, 7],
- risk reduction by safety functions realization.

The main difference between classic work of robots, e.g. material handling, welding and the work in a neighborhood of the people, both industrial and care robots, is the latter cannot be protected be means of barriers, guards and other external means of protection. They must be safe by mean of realization of safety functions. Such a system of protection is a purpose of the functional safety techniques [11].

2.2. General concept of risk reduction

The most general risk assessment principle is the ALARP principle (As Low As Reasonably Practicable) and tolerable risk concepts [13].

ALARP is one particular principle which can be applied during the determination of tolerable risk and safety integrity levels. It is not, in itself, a method for determining safety integrity levels. Corresponding methods are presented, for example, in IEC 61508-5 [13] and also in [15].

In case of real devices or systems three situations are possible:

a) the risk is so huge that it is refused altogether; or
b) the risk is, or has been made, so small as to be insignificant; or
c) the risk falls decreases between the two states specified in items a) and b) above and has been reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction.

With respect to item c), the ALARP principle recommends that risks should be reduced "so far as is reasonably practicable," or to a level which is "As Low As Reasonably Practicable" (ALARP).

If a risk falls between the two extremes (that is, the unacceptable region and broadly acceptable region) and the ALARP principle has been applied, then the resulting risk is the tolerable risk for that specific application. According to this approach, a risk is considered to fall into one of three regions classified as "unacceptable", "tolerable" or "broadly acceptable" (see fig. 1).

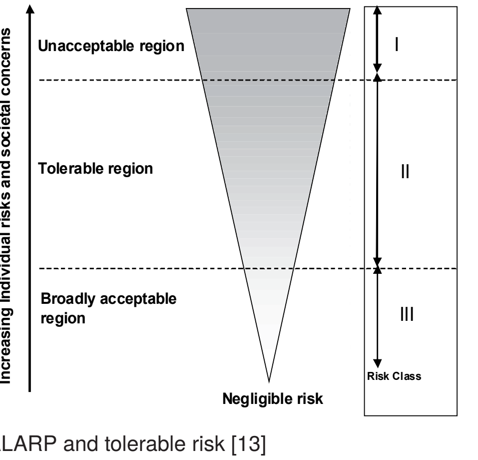

Fig. 1. ALARP and tolerable risk [13]
Rys. 1. ALARP i ryzyko tolerowalne [13]

Above a certain level, a risk is regarded as unacceptable. Such a risk cannot be justified in any ordinary circumstances. If such a risk exists it should be reduced so that it falls in either the "tolerable" or "broadly acceptable" regions, or the associated hazard has to be eliminated.

Below that level a risk is considered to be "tolerable".

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

In order to apply the ALARP principle, it is necessary to define the three regions of fig. 1 in terms of the probability and consequence of an incident. To take into account ALARP concepts, the matching of a consequence with a tolerable frequency can be done through risk classes. Tab. 1 is an example showing three risk classes (I, II, III) for a number of consequences and frequencies. Tab. 2 interprets each of the risk classes using the concept of ALARP. That is, the descriptions for each of the four risk classes are based on fig. 3. The risks within these risk class definitions are the risks that are present when risk reduction measures have been put in place. With respect to fig. 1, the risk classes are as follows:

- risk class I is in the unacceptable region;
- risk class II is in the ALARP region;
- risk class III is in the broadly acceptable region.

Having determined the tolerable risk target, it is possible then to determine the safety integrity levels of safety instrumented functions.

Tab. 1. Example of risk classification of incidents [13]

Tab. 1. Przykład klasyfikacji ryzyka zdarzeń

Probability	Risk class			
	Catastrophic consequence	Critical consequence	Marginal consequence	Negligible consequence
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

Tab. 2. Example of interpretation of risk classes [13]

Tab. 2. Przykład interpretacji klas ryzyka [13]

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Negligible risk

2.3. Safety integrity requirements

Dependent of identified risk level, the safety functions of various integrity levels shall be applied. The integrity levels are defined by means of probabilistic measures [11] and four levels (SIL) are introduced. The above presented tables provide the corresponding data.

Tab. 3. Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation [11, 15]

Tab. 3. Poziomy nienaruszalności bezpieczeństwa: docelowe miary uszkodzeń funkcji bezpieczeństwa [11, 15]

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Tab. 4. Relationship of residual error rate of transmission protocols to SIL level [15]

Tab. 4. Relacja błędu szczątkowego protokołu transmisyjnego do poziomu SIL [15]

Applicable for safety functions up to SIL	Probability of a dangerous failure per hour for the functional safety communication system	Maximum permissible residual error rate for the functional safety communication system
4	$\geq 10^{-11}$ to < 10-10	$\geq 10^{-11}$ to $< 10^{-10}$
3	$\geq 10^{-10}$ to < 10-9	$\geq 10^{-10}$ to $< 10^{-9}$
2	$\geq 10^{-9}$ to < 10-8	$\geq 10^{-9}$ to $< 10^{-8}$
1	$\geq 10^{-8}$ to < 10-7	$\geq 10^{-8}$ to $< 10^{-7}$

3. The world of industrial robots

The main feature of industrial robot world is the system separation human and robots; the work zones of industrial robots are, as principle, strictly protected against people entrance. Access to the work zone is restricted for the specialist personnel only: programming and servicing personnel. In such application the first Asimov law of robotics [17]: "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 safety work. The safety function required by the safety standard [8, 9] are listed in table 5.

The example of industrial robotic system is presented on fig. 2.

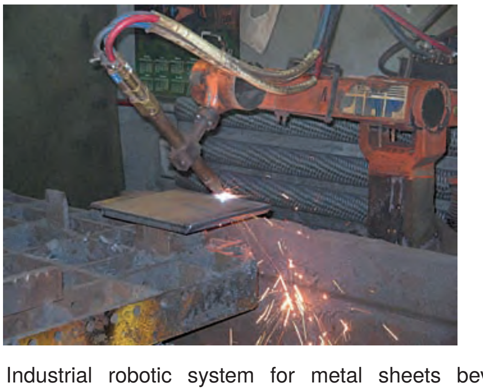

Fig. 2. Industrial robotic system for metal sheets bevelling [www.piap.pl]

Rys. 2. Przemysłowe stanowisko zrobotyzowane do ukosowania blach

Tab. 5. Safety functions of industrial robots
Tab. 5. Funkcje bezpieczeństwa robotów przemysłowych

Item	Description of safety function	SIL
1	Holding brake function	1
2	Safety-related control system performance	2
3	Emergency stop	2
4	Protective stop	2
5	Speed reduction control	2
6	Initialization of motion at full speed from pendant control	2
7	Enabling function	2
8	Unattended motion prevention	2
9	Unexpected start of the robot	2
10	Safe reduction of speed, while collaborating with a human	2
11	Robot arm position monitoring, while collaborates with a human	2
12	Limitation of power 80 W and force 150 N on the robot arm, while cooperates with a human	2
13	Limiting of robot arm movement, other as mechanical	2
14	Programmable limitation of span of robot movement	1 or 2 or 3
15	Safety functions of safety-related control system	2

Nowadays, this world is becoming more complicate – the direct cooperation between people and industrial robot is often needed and is taking place by full speed of robot arm. It is a question, the above mentioned safety function will have sufficient integrity level, in my opinion it could be to low. The suitable risk assessment shall do a response.

4. The world of non-medical personal care robots

4.1. General remarks and a new law of robotics

The world of personal care robots shall be fundamental different from industrial robot world. The first I have written about it in the publication [16]. Now it is time to enlarge those considerations.

The care robots act, one can say live in the same world as people; the worlds of people and robots are approaching to one complex world.

It will be a world of people aged, fully or partially disabled, children, domestic animals, care and/or servicing robots, living and acting together in apartments, shops, hotels, streets, parks etc. Robots will be companions, carers, servants, transport means etc.

In such circumstances, in such a world, the Asimov laws or robotics are insufficient. It is need, a new law to formulation: "Robotum homini amicus est – Robot is a human friend"

What does it mean?

Between others:

- Robot shall be as safe as technically possible – each and all faults and failures lead to stop of movements or to go to fully safe position on fully safe trajectory;
- All movement shall be slow, smooth and calm; any sudden movement isn't acceptable;
- Communication between human and robot shall have place by voice, eye contact, gesticulation;
- Robot shall understand and express same feelings, e.g. approval, refusal, happiness (gay), sadness (sorrow);
- Human shall construe the robot as a nice companion.

There are leading many project and works to realize above mentioned thesis, also in Poland. As some examples can serve the project of "social robots" [18–21].

4.2. Safety problems

4.2.1. Introduction

The safety problems of non-industrial robots are actually the object of international standardization works. Am September 2011 was distributed the final DIS ISO 13482 [10], that is dealing with this problem.

The scope of the standard is personal care robots defined as:

Personal care robot – service robot that allows physical contact with humans for the purpose of aiding actions or performing actions that contribute directly towards improvement in the quality of live of individuals, excluding medical applications.

The above mentioned International Standard is containing the requirements for three groups of non-industry robots:

- mobile servant robot – personal care robot that is capable of moving freely to perform an intended task and/or handling objects (with or without a manipulator);
- physical assistant robot – personal care robot that assists a person to perform required tasks, to provide supplementation or augmentation capabilities. A physical assistant robot is designed to bring the functionality of a weak person or an elderly person, to that which can be performed by an ablebodies person, as well as to augment the performance of an ablebodied user;
- person carrier robot – personal care robot with the purpose of transporting humans to a different location by means of autonomous navigation, guidance and locomotion.

The proposed safety functions of these robots, defined on the basis of suitable risk assessment done in the standard, will be presented below. The guidance for design the safety functions and verify their SIL are e.g. in [6, 7, 22, 23].

4.2.2. Safety functions of mobile servant robots

The safety functions of mobile servant robots are collected in [10] into two groups:

- home servant robots, that purpose is to perform a variety of domestic tasks autonomously;

Fig. 3. Humanoid Wakamaru manufactured by Mitsubishi [www.boston.com]
Rys. 3. Robot Wakamaru produkcji Mitsubishi

– public guide robots, which purpose is to provide information and entertainment in public places.

Tables 6 and 7 are presenting these functions. On fig. 3 the example of servant robot is presented.

Tab. 6. Safety functions of home servant robots
Tab. 6. Funkcje bezpieczeństwa robotów usługowych domowych

Item	Description of safety function	SIL
1	Use fixe/movable guards to prevent inserting a body part	2
2	Monitor the torque inside the arm drives	2
3	Monitor and restrict velocity of the arm	2
4	Detect human body parts in the workspace	2
5	Monitor force and way during grasping and check for plausibility	2
6	Monitor and restrict loads that may be lifted	1
7	Restrict dynamic forces when the arm is moved	1
8	Move the mobile base to stabilize the robot after dynamic forces occurred	2
9	Using robust algorithms and plausibility checks to ensure that the right object is grasped	<1
10	Monitor grasping force to ensure correct clamping force	1
11	Use grasp planning to clamp only at solid surfaces	<1

Tab. 7. Safety functions of public guide servant robots
Tab. 7. Funkcje bezpieczeństwa robotów usługowych przeznaczonych do prac publicznych

Item	Description of safety function	SIL
1	Use speed limit circuit	2
2	Control to bring mobility to a safe stop and induce a passenger to safely disembark from the mobility	2
3	Use fixe/movable guards around wheels	2
4	Deactivate electric power if terminal is detected open	1
6	Outer covering	1
7	Use of high-friction tyres	1

4.2.3. Safety functions of physical assistant robots (exoskeleton walker robots)

The safety functions of physical assistant robots form in [10] one group. They are collected in tab. 8.

Tab. 8. Safety functions of physical assistant robots (exoskeleton walker robots)
Tab. 8. Funkcje bezpieczeństwa robotów asystujących fizycznie (egzoszkielety do chodzenia)

Item	Description of safety function	SIL
1	Cushioning on sharp edges	1
2	Emergency stop	1
3	Speed restriction and safety-related speed control	1
4	Current limitation of motors	1
5	Safeguarding against burn (fire)	3
6	Charging activation control	2

4.2.4. Safety functions of personal carrier robots

The safety functions of personal transport robots are collected in [10] into two groups:
– personal transport robots;
– robotic lift and transfer wheelchairs with on-board arm.

Tab. 9. Safety functions of personal transport robots
Tab. 9. Funkcje bezpieczeństwa robotów do transportu osobistego

Item	Description of safety function	SIL
1	Speed restriction and safety-related speed control	2
2	Use fixe/movable guards around wheels	2
3	Physical restriction and control to avoid sudden acceleration	1
4	Controlled stop (active stability) control during embarkation/disembarkation	1
5	Use anti-vandalism circuitry (key or password start)	2
6	Active mobility balance control	2
7	Activation of charging power only when the mobility is connected	1
8	Indication of charging status on the mobility display	1
9	Heat dissipation mechanism (heat sinks, air flows with fan control)	1
10	Secondary independent brake control to bring mobility a controlled stop and induce a passenger to safety disembark from the mobility	2

Tab. 10. Safety functions of robotic lift and transfer wheelchairs with onboard arm
Tab. 10. Funkcje bezpieczeństwa wind robotycznych i jezdnych wózków inwalidzkich z zamontowaną poręczą

Item	Description of safety function	SIL
1	Use of speed limit circuit	2
2	Use of mobility balance control	2
3	Use of intelligent braking circuit or mechanical design	2
4	Seat belt worn by user	2
5	Control to bring mobility to a safe stop and induce a passenger to safely disembark from the robot	2
6	Control and/or intelligent braking to bring mobility a safe stop	2
7	Use fixe/movable guards around wheels	2
8	Control to avoid sudden acceleration	1
9	Safe stop control during embarkation/disembarkation	1
10	Mobility balance control	1
11	Enclose all electrical terminals and deactivate electrical power if terminal id detected open	1
12	Heat dissipation mechanism (heat sinks, air flows with fan control)	1
13	Shock absorbing mechanism	2
14	Non-contact obstacle detection	2
15	Use anti-vandalism circuitry (key start)	2

Fig. 4. Toyota Personal Transport Assistance Robot "Winglet" [www.youtube.com]
Rys. 4. Osobisty asystujący robot transportowy Toyota "Winglet"

Tables 9 and 10 are presenting these functions. On the fig. 4 an example of personal transport robot is presented.

5. Conclusions

The proposal of solving of safety-related problems concerned to new robot applications – non-medical care personal robots are presented, on basis of a suitable standard draft.

Bibliography

1. Forge S., Blachman C.: *A helping Hand for Europe: The competitive Outlook for the EU robotic Industry*, JRC European Commission, 2009.
2. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), OJ of EU L157/24 from 9.6 2006.
3. Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits (codified version), OJ of EU L 374/10 from 27.12.2006.
4. Directive 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC, OJ of EU L 390/24 from 31.12.2004.
5. EN ISO 12100:2010, Safety of machinery – General principles for design – Risk assessment and risk reduction (ISO 12100:2010).
6. EN ISO 13849-1:2008, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (ISO 13849-1:2006).
7. EN 62061: 2005, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.
8. EN-ISO 10218-1:2011, Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots (ISO10218-1:2011).
9. ISO/DIS 10218-2, Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration (ISO 10218-2:2011).
10. ISO/DIS 14842, Robots and robotic devices – Safety requirements for non-industrial robots – Non-medical personal care robot.
11. EN 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements.
12. EN 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations.
13. EN 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety related systems – Part 5: Examples of methods for the determination of safety integrity levels.
14. EN 61882:2001, Hazard and operability studies (HAZOP studies) – Application guide.
15. Missala T.: *Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa*, Oficyna Wydawnicza Przemysłowego Instytutu Automatyki i Pomiarów PIAP, Warszawa 2009.
16. Missala T.: *Robot jako system związany z bezpieczeństwem,* [w:] Tchoń K. (red.): *Postępy robotyki – Przemysłowe i medyczne systemy robotyczne*, 183–191, WKŁ, Warszawa 2005.
17. www.wikipedia.org/wiki/Three_Laws_of_Robotics.
18. Tchoń K.: *Roboty i interaktywni towarzysze życia – projekt europejski LIREC*, prezentacja na sesji Foresight ARP, Wrocław 2010.
19. Sydor K., Arent K.: *FROGIT: społecznie interaktywny robot do badań HRI z dziećmi młodszymi*, [w:] Problemy robotyki, t. I, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2010, 173–184.
20. Budziński R., Kędzierski J., Weselak B.: *Głowa robota społecznego Samuel – konstrukcja*, [w:] *Problemy robotyki*, t. I, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2010, 185–194.
21. Granosik G., Stanuch M., Wojtowicz K.: *Oprogramowanie robota społecznego Telson*, [w:] *Problemy robotyki*, t. I, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2010, 195–206.
22. EN 61078: 2006, Analysis techniques for dependability – Reliability blocks diagram and Boolean methods.
23. EN 61165: 2006, Application of Markov techniques. ■

Bezpieczeństwo robotów w sąsiedztwie ludzi i nowe prawo robotyki

Streszczenie: Współpraca ludzi z robotami jest coraz częstsza. Jednym z istotnych problemów jest utrzymanie bezpieczeństwa. Przedstawiono wybrane zagadnienia bezpieczeństwa w przypadku przemysłowych zastosowań robotów, a także zastosowań robotów do osobistej opieki nad ludźmi.

Słowa kluczowe: bezpieczeństwo robotów, roboty przemysłowe, roboty osobiste

Tadeusz Missala, PhD, Full Prof.

After 10 years of work in industry and 7 years work in high education schools, from 1967 is working in Industrial Research Institute for Automation and Measurement PIAP, to 1988 as head of department of Electrical Automation and now as head of Certification Body.

e-mail: tmissala@piap.pl