ANNALS of Faculty Engineering Hunedoara
– International Journal of Engineering
Tome XIII [2015] – Fascicule 3 [August]
ISSN: 1584-2673 [CD-Rom; online]
a free-access multidisciplinary publication of the Faculty of Engineering Hunedoara

[1.] Péter PAUSITS, [2.] Gábor SZÖGI, [3.] Gábor FŐDI

SAFETY CONSIDERATIONS FOR ROBOTS FUNCTIONING IN DIVIDED WORKSPACE

[1-3.] Óbuda University, Doctoral School on Safety and Security Sciences, HUNGARY

Abstract: Owing to the continuous large-scale development of robots predictive statistics suggest that by 2020 there is going to be on average one robot per household. Due to its physical size and power it could be a potential source of serious threat for people in the same space, be they an operator, a person being served, or a patient waiting for surgery. Rapidly developing devices are not always accompanied by the adequate safety regulations. However, in the future these regulations are going to be indispensable for without them the developments are going to be uncoordinated and during the implementing the financial interests are going to overtake safety interests and risk reduction. However, contrary to an industrial robot that is only threatened by economic and moral disadvantages, we, humans are threatened by away bigger risk: the loss of life. Therefore several regulations should be created to reduce risk and to keep the developments within the confines of security. For this, the creation of forward-looking international standardization and moderation are necessary and should be applied by each developer, manufacturer and user in the severest way.
Keywords: medical robot, divided workspace, secure human-machine relationship, sensors

1. INTRODUCTION

During the development of the world there has always been a need for production equipment and production methods. After the emergence of guilds and manufactories the increment of human factors appeared on every field. The steam engine created by James Watt is a highlighted milestone on the path to the Industrial Revolution of the 18th century, being the first device ever to generate kinetic energy several times higher than human force can. A new unit of measurement, the watt has simultaneously been introduced to the SI, as the unit of performance. From then on more and more efficient ways to apply this generated kinetic energy have started rapidly developing. The fact that the primary field of utilization had become the industrial production has led to the outburst of the Industrial Revolution. From then on the development of industrial machine tools and processing units has begun at a pace never before seen. The development of production equipment reached the point in the 19th century where the kinetic energy generated by steam machines was insufficient. This caused the appearance of several developments using a different propellant, such as Nikolas August Otto's Otto engine patented in 1876, being the first internal combustion four-stroke engine. The appearance of this new form on energy caused the development to skyrocket, for the Otto engine was able to produce a significantly bigger amount of energy than the steam engine. The demand for the dynamo, the device to generate electrical energy appeared simultaneously. Several experiments regarding this device have already been conducted at that time. Ányos Jedlik was able to transform kinetic energy to electrical energy in 1861but this technology was patented by Ernst Werner von Siemens in 1866. Electrical energy has the advantage over any other kind of energy of being easily regulable and economically transportable from the producer to the user. This advantage was quickly recognized in the field of industrial applications. Long term and extensive developments conducted by John von Neumann followed in 1952 and the first computer was created that could utilize electrical energy to store data. The working principle of this computer, called von Neumann's principle is still used to date. The developments of the last 60 years prove that regulation, control, production, processing, and data storage require electrical energy.

Robots gained special attention during the developments since electrical energy has been usable as kinetic energy or for data storage. They are considered the realization of artificial intelligence and the way to overcome the disadvantages of the human factors and the electromechanical machines used to increase energy. This increased energy used to cause severe accidents in the early days for there had not been elaborate safety standards or directives regarding the application of robots. Currently robots are primarily used in an industrial environment with the most modern safety regulations that during standard operation exclude the possibility of even the smallest injuries. Robots are currently able to execute industrial operations alone or under surveillance of operators, so there is no need for them to come in contact with humans. By the exclusion of divided workspace the possibility of personal injury can be reduced to the absolute minimum. This act can prevent human injury, an economically inexpressible

damage. However, there still is a possibility of the robot damaging itself, but this can only be deducted as an economic damage. But the further development of automation becomes limited if the workspace can't be divided by humans and robots. Several researches regarding medical and service robots have been conducted for nearly 30 years. These researches include the application of divided workspace, for in the case of a medical robot there is no way to avoid coming in physical contact with a patient or an operator. Researches dedicated to making divided workspace as secure as it possibly can be have consequently become more frequent.

In this paper the security issues of a complex robot cell is going to be presented from an electronic and mechanical point of view, and also from the point of view of its software. Security regulations and their application regarding robots used in the industry, dangers of the divided workspace, and the risks of the human factors are also going to be presented.

2. SECURITY ANALYSIS

Due to the development and the accidents that had occurred in the past security analysis is getting a bigger attention, especially risk analysis. It was recognized, that applying risk analysis from the very beginnings can prevent a number of accidents, be it personal injury or economical or moral damage. However the task of risk analysis has to be taken into consideration from the elaboration of the process to during the designing, the production, the set-up to the usage itself. Owing to this, several risk assessment procedures that apply mainly mathematical probability theory and statistical calculations have been worked out. We can safely say that risk can never be reduced to zero but we have to take every possible step to reduce the chance of accidents to the absolute minimum.

We have to set up a model during risk analysis that presents the actual machine, the situation, the environment and the relation with the staff in the most realistic possible way.

3. APPLIED MODELING METHODS

3.1. Preliminary danger analysis

This method is expedient when the developments regard a machine or an environment about which there's not much experimental information available. This occurs mostly during the designing of experimental or developmental machines, and gets a highlighted role during the creation of the concept and designing. The possible risky situations, sources of danger and the extent to which these dangers are damaging to the health can usually be presented on a tree graph. Then the risky situations are evaluated based on the extent of their dangerousness. A method is created for every single risky situation to presumably reduce the extent of danger.

3.2. Error tree analysis

The goal of the analysis is to examine every possible accident in depth and to explore every single step that can lead to that accident. During this process all circumstances, and environmental and human factors are taken into consideration and the process is completely traced back to the smallest of initial problems. On every level where risk can occur it is evaluated and reduced to the smallest extent the possibilities allow. It is known that the occurrence of an accident is almost never triggered by a single factor but rather consecutive errors. Primarily because these singular events can be foreseen and therefore prevented. Risk is generally caused by a sequence of related and unplanned happenings. The error tree analysis seeks to solve the problem as early as possible to decrease to risk of occurrence.

3.3. "What if…" analysis

This method is useful in the case of low complexity systems that have only two levels of error. It's also useful to determine trivial risks in the case of more complex systems. Already developed security systems can be revised for possible errors using this analysis. E.g. "What if a wire in the security electrical circuit breaks?" This way every subtask is analyzable. In case the analysis is unsuccessful or the criteria of the occurrence too complex a different risk analysis method is recommended.

3.4. HAZOP (Hazard and Operability Studies) analysis

The HAZOP analysis is a particularly complex method that applies experts for every field involved. The links between these fields are defined and used as starting points for further exploration of possible accidents and risks. The extent to which these fields are linked to the risk is defined and the possible errors are explored. In case the probability of the occurrence can't be reduced to almost zero, the experts will suggest a measure together to increase safety.

3.5. Event tree analysis

This method is similar to the error tree analysis as it explores consecutive events. Only this time the starting point is the trigger event and every process started by a new event is recorded and presented to show the interdependence in an obvious way. This way the possible consequences of the occurrence of an initially neglected small event become apparent. The chain of events that can lead to a severe accident can this way be revealed.

3.6. Failure mode and effects analysis

During this analysis the each element's frequency of failure and the probable consequences are collected. Analyses of this type are regularly reviewed considering the experiences. The other name for these analyses is FMEA (failure mode and effects analysis). The FMEA reveals the ideal frequency of maintenance and replacement of components. In the case of this analysis every error is managed independently.

3.7. MOSAR (Method Organised for Systematic Analysis for Risk) analysis

The MOSAR analysis involves the review of the effectiveness of the existing risk reducing analyses. The interaction between subsystems is explored. After the analysis of risks the acceptability of risks is evaluated and then suggestions are made to better the prevention.

4. SYSTEM DESIGN METHODOLOGY

A number of researches and developments were conducted to create a methodology that could be a guide during the development of a robot from the conception to the manufacturing and the maintenance. The most advanced system methodology to date is hazard identification and safety insurance control (HISIC). HISIC proposes that during the development of a robot a team of experts of several fields should work together keeping the basic principles in mind. HISIC has seven basic principles. By the application of these principles the development, the design, the employment and the maintenance of the robot will get enough attention from every aspect.

The seven basic principles are the following:

- Definitions and requirements
- Hazard identification (HI)
- Safety insurance control (SIC)
- Safety critical limits
- Monitoring and control
- Verification and validation
- System log and documentation

The adequate application of these basic principles allows the risks occurring during the employment of robots to be reduced. Risk can be reduced to the absolute minimum if the operator recognizes the hazard and reacts in time. The role of robots does not just stop at the operation they were meant to execute. They help the operator recognize and prevent the stochastically and deterministically occurring dangers at once. If the monitoring system's sampling time and reaction time are making it capable of preventing hazards or reducing the damage to the absolute minimum, reaction time can be reduced to its fraction. HISIC provides a method to realize this process in an adequate quality and time.

4.1. Complex robot cell

A complex robot cell, be it industrial, surgical or service robot, is composed of several principal components isolated from each other from the point of view of safety. For this and to create the most reliable and hazard free product many different experts are required during the process of development. The three main fields are electronics, mechanics and software. These fields have very small intersections with each other when it comes to safety. In the following the way to reduce the intersections and to reduce the hazard of accident will be presented.

Naturally, these separate fields are cooperating because it's required to execute the desired operation. The lack of cooperation can also be a source of hazard.

4.2. Electronics

Since the appearance of electricity the presence of electrical signal has always been essential in automated processes. Software is able to manage the properties of an electrical signal as data and actuators are able to create kinetic and other kinds of energies in a regulated way based on data transported by electrical signal. Earlier, production equipment functioning solely by mechanical principles did exist, e.g. punch cards used to store data mechanically. But today we could not imagine executive equipment that is not software controlled or that is not electrical.

The existence of a homogeneous system requires data received from environmental and internal characteristics to be transformed into electrical signal. Naturally, as a consequence of the development electrical signal can be split into different modifications, because analog amplitude modulated and frequency modulated signals and digital PWM (Pulse Width Modulation) signal are electrical signals too. Nonetheless computers with an operating principle based on von Neumann's principle can only manage and binary signals (Fig. 1.) and forward binary data.

The central processing unit, depending on how advanced or complex is it, can be a 4-8-16-32-64 bit CPU. This is of top importance from the point of view of the management of inputs and outputs. But the majority of detectors (Fig. 2.) transform the measured signal into analog signal and actuators transform analog signal into kinetic and other kinds of energies.

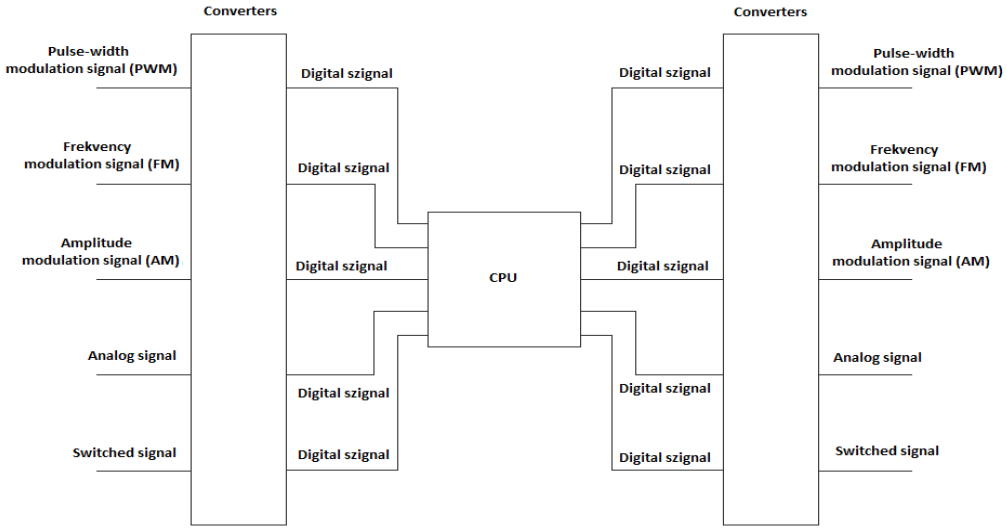

Figure 1. Digital signal

Type of detector	Measured property	Working principle, output signal
PT 100, PT 1000 thermometers	Temperature	Voltage change triggered by change in resistance depending on temperature. Tension measured between output points appears in the form of analog signal.
Incremental encoder	Position	The displacing dial generates a series of impulses with the help of photo electronics. The extent of the displacement can be calculated by the amount of impulses. The output signal appears in the form of square wave where the number of rising edges is relevant.
Incremental encoder	Angular velocity	The displacing dial generates a frequency modulated signal with the help of photo electronics. The frequency of the signal is directly proportional to the angular velocity in every instant.
Inductive-, capacitive- and mechanical switch	Presence	Depending of the measuring principle output voltage will appear in the output of the single switches. The output signal of the switches is called switched voltage.

Figure 2. Types of detectors and their working principle

Electronics are responsible for transforming communication into a homogenous system. It provides computers and actuators with authentic data in real time.

Thus the first small intersection is the communication on the adequate level. Every single signal conversion will inevitably cause a minimal loss of data and time delay. Thus it is of tom importance to make the least amount of conversions between the occurring environmental property and the data reaching the software. During the design the conversions have to be reviewed to find the omittable or replaceable ones.

The particularities of the detectors part of the subtasks of electronics. A number of environmental and internal characteristics exist that can influence the safe operation of a robot. These characteristics can be:

- temperature
- humidity
- light
- presence
- position
- direction of displacement
- velocity
- pressure

There are a number of detectors with different working principles to measure the single characteristics. Optical systems/sensors are the latest sensors. These sensors perform complex measurements in real time, therefore the time delay is minimal. We are able to measure temperature, light, presence, position, direction of displacement and velocity with optical systems if the sampling time is sufficient. However, every property requires a specific detector to maintain a safe data collection. But the most effective way of

preventing the malfunction of a detector is by redundant sensors with different working principles. The electrical signals they emit are evaluated by a software program, as a decision-making unit.

To sum it up, from an electrical point of view the intersection is the establishment of a homogenous system and the detectors. To resolve this intersection and reduce the hazard, simplification and redundancy are the answer.

4.3. Mechanics

The reason why the raison d'être of robots cannot be questioned is because they are able to resolve the disadvantages of the human factors and increase the human-made energy to sufficient level for the execution of a process. An industrial robot is able to displace several tons of mass if necessary, unlike people. Furthermore, a surgical robot is able to perform the most precise incisions without a shaky hand, or reach places unreachable for the human hand. Also, a robot is able to work in a dangerous environment that is potentially hazardous for the human health. However, during the designing process the selection of the adequate actuator and adequate scaling of the mechanical loading require special attention.

Actuators primarily apply precision DC electric to move robots, or in some cases hydraulic motors, but the latter is not characteristic for surgical or service robots for their controllability is insufficient. In the case of surgical robots precision is critical. Thus, when choosing the actuator the application of a special servo motor is required. The majority of servo motors are PWM operated and are also detectors, so they are able to provide data of their position in real time.

Another small intersection of mechanics is stability. Therefore robotic arms have to be designed to be able to execute twice the physical operation they have to operate. Furthermore, in a divided workspace robots are exposed to external stochastic impacts. It's impermissible for the robot to be moved out of its operational position because of such effects. Therefore, the body of the robot has to be designed in a way that it can resist possible external physical impacts and manage to stay stable.

Thus, risk originating from the mechanical unit can only be reduced if the prescribed maintenance, the selection of actuators and mechanical design are made to perform twice as well at carrying capacity and operating time as they will have to. Unfortunately, redundancy is not feasible in the case of mechanical risk reduction.

4.4. Software

With the advanced technology of today computers are indispensable when using any kind of electrical device. Be it detectors, actuators, or communication. Actually, every electrical device that contains a programmable microcontroller or microprocessor is a computer. Accordingly, these devices execute a targeted task but they have a program memory and they run a machine code. In addition, every complex robot system has a central controlling computer that makes decisions and regulates actuators based on data from the detectors' electrical signals. Its task is to synchronize their operation and perform controls that reduce risk. Thus software is the part of the robot that assumes that mechanics, electronics and commination works adequately and error-free, and if it detects an error, it instructs risk reducing measures. If the software program can't eliminate a problem sufficiently, it will have to decide about shutting the robot down. The software program running in every programmable component of a robot has to be completely stable, run time errors are not permissible. Thus, a robot has to go through several tests before set-up, and the methods presented earlier have to be applied to reduce hazard. One very important property a software program has to possess is the ability to override or correct obviously irregular orders from the operators. [10] Creating this ability is of top importance during the development of the software program. However, operators have to be able to intervene in case of an error. The most trivial way of doing so is by pushing the emergency button that stops the functioning of the robot.

Software is responsible for the adequate management of communicational protocols. Usually such complex systems use system buses between components, but direst connections also exist. During the selection of the system bus two characteristics that depend on the distance applied, have to be considered: data transfer rate and reliability. The number of devices the system bus can maintain commutation between is among the criteria of the systems. The following comparison presents the characteristics of the most frequently used system buses (Fig. 3.).

Name	Data transfer rate (kbit/s)	Maximum number of communication devices (pcs)	Maximum length of wire (m)
CAN Bus	50-1000	64	40-1000
Profi Bus	9,6-12000	32	100-1200
LIN Bus	20	16	40
LonWorks	78-1250	32385 (127)	125-2200
Inter Bus	500	4096	200-13000
P-Net Bus	76,8	125	1200

Figure 3. Characteristics in the case of twisted pair cables

5. SUMMARY

This paper concludes that risk analysis is of top importance during the development of each system. Risk factors have to be taken into consideration from the creation of the concept and solutions for risk factor have to be sought from the very beginnings. The

more complex a system is, the bigger the hazard of health damage or economical disadvantages. The necessity of components in the robots desired to be developed, such as the central control device, the adequate communication, actuators, and sensors can be concluded. These components pose many risks and from the point of view of safety, a number of small intersections can be found and have to be resolved to reduce risk. Following the risk reduction of the single components, the expected level of cooperation of the components on connection points is necessary. Next to minimal hazards, complex robot sells have to operate with an expected level of safety. Divided workspace becomes riskier than isolated workspace due to the human factors. As long as a robot operates in an isolated space, human injury cannot occur next to normal operating mode, thus, due to safety regulations, robots immediately stop if a strange object or person enters the workspace, so personal injury is impossible. However, in divided workspace the human-machine physical contact, accidental or intended, is inevitable. Thus risk reduction has to be done taking stochastic and deterministic physical contact into consideration to prevent permanent injuries, or injuries harmful to health of the operators or served people.

References

[1.] http://www.kvaser.com/about-can/can-standards/linbus/ (date: 23 April 2015)
[2.] http://www.freescale.com/files/microcontrollers/doc/reports_presentations/LINOVERVIEWPRESENT.ppt (date: 23 April 2015)
[3.] Balázs Novák – Comparison of fieldbus system buses (Terepi buszrendszerek összehasonlítása)
[4.] Dr Gábor Csutorás – The science of safety (Biztonságtudomány)
[5.] L. Schreiter, D. Bresolin, M. Capiluppi, J. Raczkowsky, P. Fiorini és H. Woern, „Application of Contract-based verification techniques for Hybrid Automata to Surgical Robotic Systems", 2014 European Control Conference (ECC), p. 2310-2315
[6.] T. Kerezovic, G. Sziebig, B. Solvang és T. Latinovic, „Human Safety in Robot Applications – Review of Safety Trends", 11th International conference on accomplishments in Electrical and Mechanical Engineering and Information Technnology (DEMI 2013), p. 1031-1039
[7.] Jiajie Yu, Yingqiang Wang, Youping Li, Xianglian Li, Cuicui Li és Jiantong Shen, „The Safety and effectiveness of Da Vinci surgical system compared with open surgery and laparoscopic surgery: a rapid assessment", Journal of Evidence-based Medicine 7., vol. 2014. p. 121-134
[8.] P. Kazanzides, Y. Kouskoulas, A. Deguet és Z. Shao, „Proving the Correctness of Concurrent Robot Software", 2012 IEEE International Conference on Robotics and Automation, p. 4718-4723
[9.] Min Yang Jung, Russell H. Taylor és P. Kazanzides, „Safety Design View: A Conceptual Framework for Systematic Understanding of Safety Features of Medical Robot Systems", 2014 IEEE International Conference on Robotics and Automation, p. 1883-1888
[10.] Rajnai Zoltán-Bleier Attila: Structural problems in the fixed communication systems of the Hungarian Army, In: Fekete Károly (Szerk), Kommunikáció 2009., Budapest, 346 p, ISBN 978 963 7060 70 0

ANNALS of Faculty Engineering Hunedoara
– International Journal of Engineering