International Journal of Occupational Safety and Ergonomics (*JOSE*) 2004, Vol. 10, No. 2, 129–136

An Analysis of Accidents Caused by Improper Functioning of Machine Control Systems

Marek Dźwiarek

Central Institute for Labour Protection – National Research Institute, Warsaw, Poland

The scope of this study covers events resulting from improper functioning of machine control systems. An accident model providing a basis for formulating a checklist for accident analysis has been developed. Data about 700 accidents were collected. An analysis has proved that in the group of accidents caused by improper functioning of machine control systems, serious accidents happened much more frequently as compared to the group of accidents with no relation to the control system. The reasons for the majority of incidents caused by improper performance of safety functions consist in the errors made by designers. In view of that, incorrect behaviour of a worker should be treated as a normal event instead of a deviation causing an accident.

accident analysis safety-related control system of machinery functional safety

1. INTRODUCTION

Accidents at work involve excessive costs, social and economic. The fact that improving the effectiveness of accident prevention should nowadays be intensified, for both moral and economic reasons, is commonly accepted. The effectiveness of accident prevention is stimulated by the quality of information about the causes and circumstances of accidents at work. They exert a decisive influence on the assessment of the risk posed by hazards causing accidents as well as ways of eliminating or reducing it. For that reason, information about incidents is very important, too, since after analysing them it is possible to assess the effectiveness of preventive means. That is why research has been undertaken on accident causes as well as an analysis of phenomena leading to accidents.

Due to advanced computer techniques available on the market there is an increasing number of accidents at work which are caused by unpredictable functioning of machine control systems. Improper functioning of machine control systems results in an inappropriate operation of a machine, which may consist in, e.g., changing the parameters of working motion or improper signalling of the machine working state. As a result, the requirements of production quality will not be satisfied or defective elements will be produced, which will definitely involve addition production costs. Much more risky, however, are possible unpredictable movements of the machine as well as involuntary speed changes, unexpected starts or no stops when there should be one, ejection of mobile elements or machined parts, etc. Such phenomena emerge when improper functioning of machine control systems causes loss of safety function responsible for preventing effects like that. Such behaviour of the machine may cause an accident at work involving much more serious results, leading to the loss of health or even life of the operator. Therefore, this study aims at determining typical phenomena causing accidents of this type.

2. METHODOLOGY OF THE STUDY

So far there have been no detailed investigations into accidents caused by disturbances in machine control systems performing safety functions. In the literature only the results of investigations conducted on a very limited scale are available

This publication has been prepared on the basis of the results of a task carried out as part of the commissioned research project PCZ 16-21 "A System of Analysing Accidents in the Working Environment for Prevention Purposes".

Correspondence and requests for offprints should be sent to Marek Dźwiarek, Central Institute for Labour Protection – National Research Institute, ul. Czerniakowska 16, 00-701 Warszawa, Poland. E-mail: <madzw@ciop.waw.pl>.

[1, 2, 3]. Some information can be found in papers devoted to a general analysis of accidents [4, 5]. The information, however, consists only in the conclusion that such accidents happen and constitute a specified percentage of all accidents at work.

Malm's report [3] discusses several accidents caused by machine control systems being damaged or by improper implementation of safety functions. The analyses of accident causes, which were carried out, showed that machine control systems functioned properly; the structural defects, however, were not indicated. The design solutions were not analysed either. The conclusions were limited to some recommendations concerning the need to avoid such events by means of applying proper work organization schemes.

The scope of the study covers events resulting from improper functioning of machine control systems. To ensure proper extraction of data on such accidents from all the information on accidents that has been collected therefore becomes crucially important. Proper identification of the faults of control systems which may cause accidents requires a detailed analysis of the events that have taken place. Therefore, for the causes of accidents to be identified properly, it is necessary to establish co-operation between experts from research institutes and employees of industrial plants. The only way experts can assess an accident properly and identify its cause is to make the information about the accident available at an early stage. Therefore, a group of correspondents, consisting of employees of industrial plants, was organized to inform the experts about events as soon as possible. The information was then forwarded to the relevant experts. In co-operation with the correspondents they analysed thoroughly the accident, even at the scene, if necessary. The available databases on accidents were created mainly for statistical purposes and to determine social and economic consequences of accidents. The research consisted of the following stages:

1. Organizing a network of co-operating employees of industrial plants, drawing up an inquiry sheet for initial assessment of the causes, circumstances and consequences of accidents or incidents.
2. Collecting from industrial co-operators information about events. Initial assessment of the events, after extracting those interesting in view of their causes, as well as their thorough analysis.
3. Drawing conclusions and providing recommendations for an effective prevention of accidents.

A checklist was developed to facilitate the process of identifying accident causes properly. This checklist made it possible to recognize and classify adequately an event as early as at the stage of its primary assessment. The checklist as well as the procedure of identifying the causes of accidents were developed on the basis of a model of an accident or dangerous event that indicated the phenomena affecting its course. The models that were employed to date resulted in limiting the analysis to the conclusion that a technical factor had caused an accident, without taking into consideration the phenomena that might occur due to improper functioning of control systems. A hypothesis of the model including particular possible faults that cause an improper performance of safety functions has been formulated on the basis of the requirements given in standards on machine control systems.

3. A MODEL OF ACCIDENTS CAUSED BY IMPROPER PERFORMANCE OF SAFETY FUNCTIONS

Investigations aiming at formulation of accident models have been conducted for many years. They have concentrated on proper identification of the most important phenomena that emerge in the course of accident. The models available to date differ in both their level of detail and scope of applicability. More general models allow a less detailed analysis of phenomena.

3.1. Most Common Models of Accidents

A model produced by H. Heinrich as early as in the 1930s [6] is the simplest example. Since the accident is represented as a series of consecutive events, it is a sequence model. Various more detailed models [7] have been based of that model. The STEP model [6] is a sequence model, too. A basic drawback of sequence models consists in the fact that when using them only the phenomena emerging directly in the course of an accident can be analysed. Therefore, they show all the most important factors arising during the event, avoiding however, indicating accident causes that emerged earlier. These factors exerted their influence before the accident happened, in this way making it possible for the phenomena to follow. Since first of all mistakes made by designers of machines and workstations were analysed, the sequence model was not suitable for that purpose.

A relatively large group of accident models comprises those based on the analysis of human behaviour under stress. A model of the effect of the social environment on safety at work developed by R. Studenski or the Smille model [7] are examples, as are Glendon and Hale's [8] model of human behaviour in danger and many other ones. In these models, however, the scope of the effect of the technical factor is not satisfactory in view of our needs, therefore the models are also not detailed enough to be applied to an analysis of accidents caused by improper performance of safety functions.

Many other models have also been proposed in the literature. However, they concentrate on the phenomena occurring when operating a machine. The assumption that the main causes of accidents are generated in the vicinity of machines lies behind those models. Even when a possible machine fault is introduced, a detailed analysis concentrates on the precautions taken by the machine operator to prevent accidents caused by an improper machine operation. The analysis of machine properties, especially of possible faults in the design of its control system is almost completely neglected. It is therefore obvious that the models currently available are not suitable for the analysis of improper performance of the safety function treated as a cause of an accident.

3.2. Accident Model Developed

The safety requirements formulated in regulations and standards on machine control systems have created a basis for developing the proposed model of accidents caused by improper safety function performance. A machine constructed in a way that complies with the standards should not involve an unacceptable risk, i.e., in the course of its operation there should not be any accidents caused by the properties of the machine. However, since accidents of that kind do happen, some mistakes must be made in the course of its design or operation. The most typical deviations from safety requirements, which cause accidents, should therefore be identified.

Safety functions can be implemented into the system by both the manufacturer and the user of the machine. A proper implementation of safety functions consists of the following stages:

- Identification of hazards and definition of safety functions;
- Determination—on the basis of risk analysis—of resistance to fault category of safety functions, complying with Standard No. ISO 13849-1:1996 [9];
- Design, construction and validation of devices appropriate for the assumed function and its resistance to fault;
- Development of a user's manual, including the maintenance scheme and necessary service operations.

Those stages can be distinguished in the course of implementing a function into a machine when it is performed either by the designer or by the user. The machine user should additionally provide:

- Training courses for machine operators;
- Instructions on occupational safety;
- Proper supervision of the operation of the machine;

- Procedures for routine checks, maintenance and repairs;
- Supervision and documentation of changes introduced into the system.

Improper functioning of the control system may be caused by improper actions performed at any stage of the life of the machine. They may negatively affect the performance of the safety function after the following events:

- Random failures of elements of the control system;
- Machine problems due to extreme environmental impacts (interferences of supply voltage and electromagnetic interference are especially important here);
- Undertaking, by the operator, actions that do not comply with the user's manual and with instructions on a safe work and, additionally, that have not been predicted by the designer of the safety function.

Those events, especially when a few of them coincide, may results in an accident. Therefore, they are direct accident causes. The fact that those events could have happened results directly from the machine designer's or user's prior errors. However, commitment of those errors does not imply that accidents occur immediately.

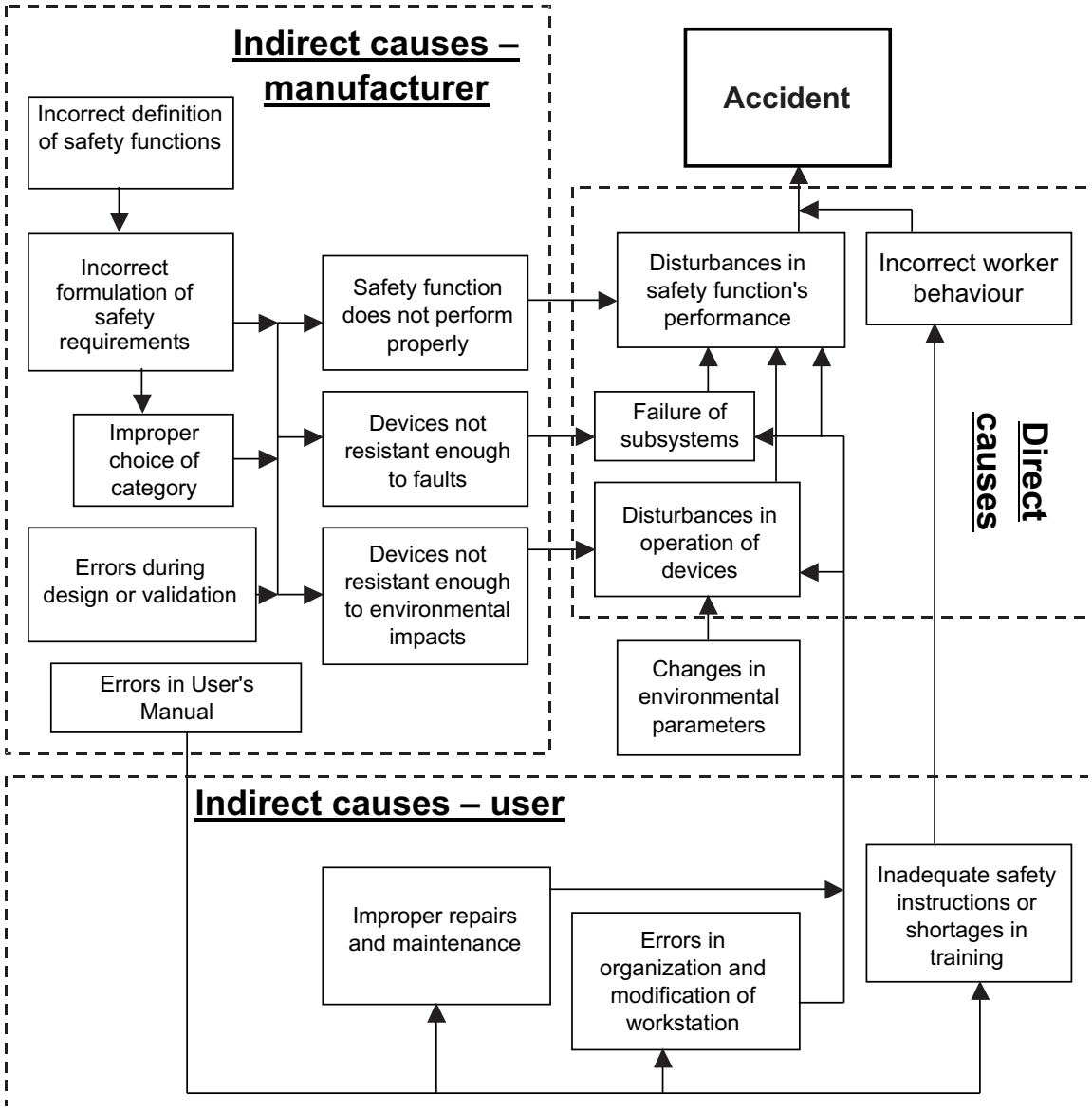

Figure 1. Model of an accident caused by disturbances in the performance of safety functions.

The machine during construction of which errors were committed may operate properly for many years until a special coincidence reveals those hidden design or organization faults. Therefore, they are indirect accident causes. Figure 1 illustrates an accident model with the aforementioned phenomena. This model shows how direct causes result from specific indirect causes. Therefore, starting from the block "Accidents" and going through successive blocks of indirect causes, one can indicate basic sources of a series of events causing accidents. This makes identification of all the accident causes possible and it indicates the most appropriate preventing measures.

This model provides a basis for formulating a checklist for accident analysis.

4. RESULTS OF ACCIDENT ANALYSIS

An important aspect of the study consisted in gathering as much information as possible about accidents and incidents related to improper functioning of machine control systems. To this end the following activities were undertaken:

1. A group of respondents was established in factories. They were appointed to collect information about events and to provide their preliminary classification.
2. A questionnaire was forwarded to factories together with a request to supply the authors of the study with information about accidents that were caused by the operation of a machine.
3. Co-operation with the National Labour Inspectorate was established.
4. Co-operation with staff dealing with occupational safety and health was also established, in factories that register incidents to gather information about such events.

The questionnaire was designed to make preliminary classification of accidents according to their causes possible. There were about 100 questions in the questionnaire relating to those main features of a machine that might cause an accident. The questions were grouped in over 20 main groups. A negative answer to a main question meant that the accident causes did not belong to that group, there was therefore no need to answer more detailed questions. Only a positive answer to a main question required detailed information in terms of answering detailed questions. Thus the questionnaire was easy to fill in.

The enterprises, where the questionnaire was administered, were chosen from a random sample developed by the Central Statistical Office (GUS). They were factories representative of Polish industry sampled from a group examined by GUS on the national level taking into consideration both the fields of activity and the number of employees. The factories which answered the questionnaire (20%) revealed practically the same structure as the whole sampled group of factories. As a result 837 factories were examined.

Mainly large and medium factories filled in the questionnaires. Information collected in co-operation with the National Labour Inspectorate concerned mainly accidents that happened in small factories.

As a result data about 700 accidents—with different causes—that took place in 1996–2002 were collected. Information was gathered from both the questionnaires and respondents. The accident reports were grouped according to the causes indicated in questionnaires and then forwarded to the experts in various (relevant) fields for further detailed analysis. Thus experts checked if the questionnaires had been filled in correctly. As a result, 144 accidents caused by the operation of of a machine were identified, with 54 of them caused by improper functioning of machine control systems.

Those accidents constituted 36% of all accidents that took place when a machine was operated (see Figure 2). In the analysis, the following classification of the severity of

accidents was introduced in accordance with Standard No. ISO 13849-1:1996 [9]:

- Slight (normally reversible) injuries: this group comprises all types of brushing, lacerations without complications, contusions, etc.;
- Severe (normally irreversible) injuries: this group comprises all kinds of amputations and death.

caused by sudden events independent of the human activity were definitely of secondary importance. On the basis of the analysis carried out, these authors could determine the following main incorrect activities undertaken by the operator, which lead to the accident:

- Inadequate response to a sudden event,
- Employment of working procedures that do not satisfy safety requirements,
- Attempts at defeating safety systems.

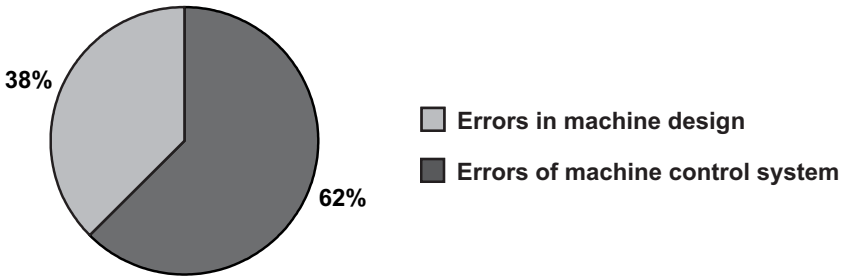

Figure 2. Accidents caused by improper functioning of the control system in relation to all accidents at machines.

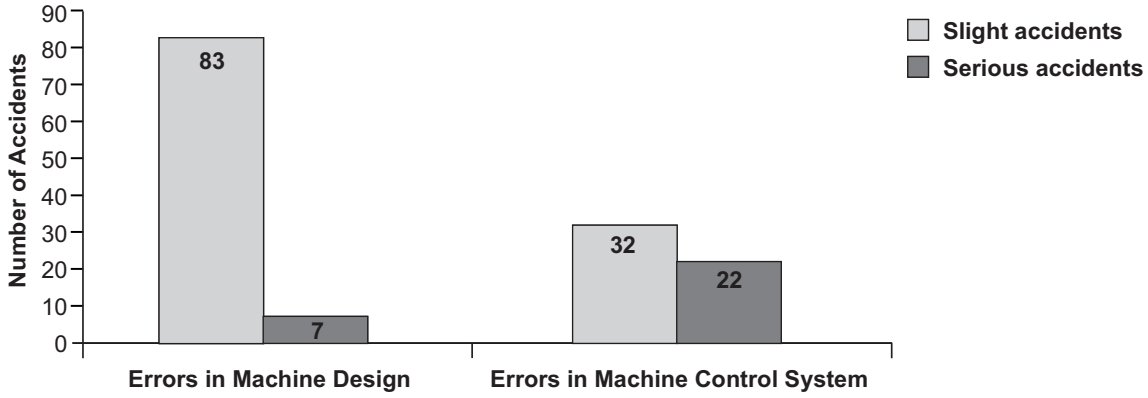

Figure 3. Severity of accidents.

Figure 3 illustrates the results of accident analysis in view of their severity: serious accidents caused by improper functioning of machine control systems happened much more frequently (41%) as compared to the group of accidents with no relation to the control system (7%). Those results proved that machine control systems were very important.

It should be emphasized that in all the analysed accidents the events were connected with incorrect behaviour of the workers. The accidents

Those activities may be undertaken spontaneously, but sometimes also on purpose. However, in a substantial majority of cases the operator's incorrect behaviour results from a sudden unpredictable situation caused by improper machine operation.

According to the basic safety principles a machine should be designed in a way that there are no hazards in the course of its normal operation as well as during predictable incorrect operation. That means that the designer should

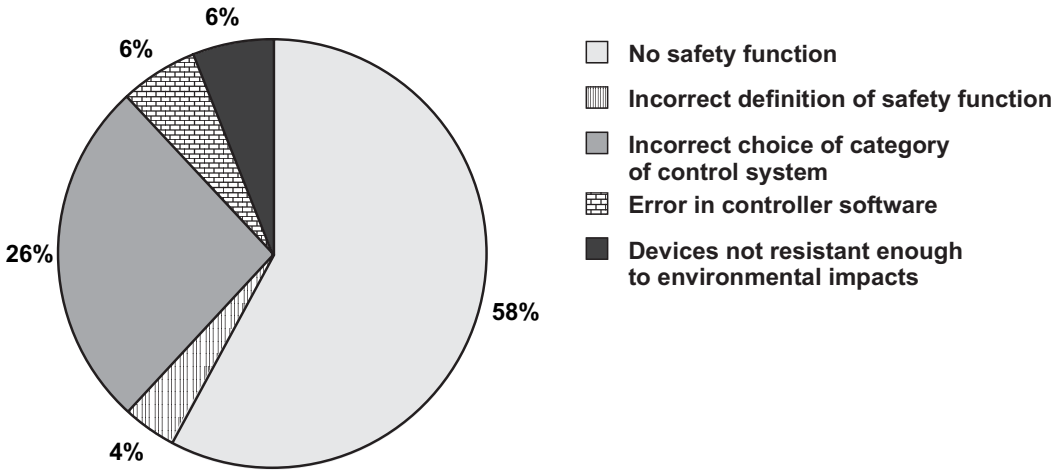

Figure 4. Frequency of different causes of accidents caused by improper functioning of the control system.

use structures that prevent purposeful incorrect operation of the machine. Therefore, if the operator employs improper working procedures intentionally causing an accident, the event should be considered as a result of errors in machine design.

Accidents caused by the control system were then analysed from the viewpoint of their causes. The results are shown in Figure 4. It is clear that lack of safety functions is the most common cause (58%). That means the accident might have been prevented if the designer had used a proper safety function. Lack of functions like guard position control and presence sensing in a dangerous zone is most frequent. According to the model presented in Figure 1, this type of causes should be considered as a special kind of an incorrect definition of a safety function. Another group comprises accidents caused by random failure of a safety-related element of the control system due to either an improper choice of the category of control system or inadequate fulfilling of the category requirements. Accidents of this type account for 26% of all accidents. Other accident causes, i.e., errors made in defining safety functions (the definition of safety function does not predict all possible events, 4%), errors made in the course of design (errors in the control system software, 6%), and inadequate resistance to environmental impacts (climate factors, interferences in power supply, of both electric and pneumatic type, 6%) constituted a considerably smaller percentage of all accidents. Therefore, the analyses carried out proved that the reasons for the majority of incidents caused by improper performance of safety functions consist in designers' errors.

5. CONCLUSIONS

This study has proved that accidents caused by improper functioning of machine control systems pose a serious problem. The in-depth analyses that have been carried allow one to conclude that they constitute a percentage of all accidents caused by the operation of a machine that cannot be neglected. Additionally, it should be emphasized that the results of such accidents with usually much more serious as compared to accidents from other causes. Therefore, a thorough analysis of such accidents is crucially important so that planning adequate protective measures is possible. One should have in mind, however, that not only a direct accident cause should be indicated and removed but the main indirect cause should also be identified since such accidents can be avoided in future only when this cause is removed as well. The produced model of accidents caused by improper functioning of the control system can be helpful in executing this task. The theoretical model that was developed on the basis of standard requirements was then verified in the course of the

study. The verification has proved that it can be useful in a complete and proper identification of all accident causes as well as in a detection of sources of improper functioning. The model can be successfully applied to further analyses of accidents as a tool for helping people making the analysis and drawing conclusions. That can be performed both by means of filling the checklist following the model as well as graphical visualisation.

The analyses carried out have proved that a machine operator's incorrect behaviour is a very important factor in a series of events that cause an accident.

Workers' incorrect behaviour can be avoided by means of intensifying supervision and training courses. It is, however, obvious that this approach cannot be a fully reliable means since it is impossible to totally eliminate human errors that are an element in an event sequence that leads to an accident. One should therefore concentrate on technical measures that could neutralize workers' errors. The analyses carried out have proved that the main causes of all the accidents consist in machine designers' errors. The control system designed in a proper way should be resistant to operators' errors. Thus, a worker's incorrect behaviour should be treated as a normal event instead of a deviation causing an accident. A machine operator's incorrect behaviour results from disturbances in the performance of the system; it is not their cause [10]. This is the only way in which the operator's errors should be treated in the course of accident analysis. It makes it possible to properly identify the true accident causes and to plan adequate preventive measures.

REFERENCES

1. Belisle J, Laurin JA. Analyse des causes d'un accident survenu une machine de coulée. In: Safety of industrial automated systems. Proceedings of the conference. Montréal, Canada: Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST); 1999. p. 6–10.
2. Edwards R. Experience gained from accidents associated with complex electronic technology. In: 2nd International Conference: Safety of industrial automated systems. Sankt Augustin, Germany: Berufsgenossenschaftliches Institut für Arbeitssicherheit (BIA); 2001, p. 39–44.
3. Malm T. Safety aspects in automation of paper roll handling. In: 2nd International Conference: Safety of industrial automated systems. Sankt Augustin, Germany: Berufsgenossenschaftliches Institut für Arbeitssicherheit (BIA); 2001, p. 51–8.
4. Harms-Ringdahl L. Safety analysis. Principles and practice in occupational safety. London, UK: Elsevier; 1993.
5. MaTSU. Employers incident analysis 1991–1998 (Offshore Technology Report OTO 2000 002). Health and Safety Executive; 2000. Retrieved April 13, 2004, from: http://www.hse.gov.uk/research/otohtm/2000/index.htm
6. Heinrich HW. Industrial accidents prevention. New York, NY, USA: McGraw- Hill; 1959.
7. Studenski R. Teorie przyczynowości wypadkowej i ich empiryczna weryfikacja (Prace Głównego Instytutu Górnictwa). Katowice, Poland: Główny Instytut Górnictwa; 1986.
8. Hale AR, Hale M. A review of industrial accident research. London, UK: Her Majesty's Safety Office; 1971.
9. International Organization for Standardization. Safety of machinery—safety-related parts of control systems—part 1: general principles for design (Standard No. ISO 13849-1:1996). Geneva, Switzerland: Author; 1996.
10. Dekker SWA. Accidents are normal and human error does not exist: a new look at the creation of occupational safety. JOSE 2003;9(2):211–8.