ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1986

Seria: GÓRNICTWO, z. 143 Nr kol. 883

1st International Conference - Reliability and Durability
of Machines and Machinery Systems in Maning
1986 JUNE 16-18 SZCZYRK, POLAND

Jerzy JAŹWIŃSKI

Airforce Technical Institute
Warsaw, Poland

Krystyna WAŻYŃSKA-FIOK

Warsaw Technical Universety
Warsaw, Poland

PROBLEMS OF RELIABILITY AND SAFETY IN TECHNICAL SYSTEMS

Summary. Problems of safety in technical systems are for understandable reason very important. These problems are of special importance among others, in transport systems and in mining systems.

In the field of transport during last years theoretical and practical works dealing with technical systems safety in reliability aspects have been done. The main ideas of these works have rather universal character and it seems they may be adopted to the technical systems in other fields.

In the paper the basic concepts and definitions as well as basic models concerning safety reliability have been presented. Mathematical relations between reliability indices and safety indices have been proposed.

Problems of designing and construction of equipment and systems with higher safety reliability have been discussed and guidelines for designers have been formulated.

1. INTRODUCTION

During last years it may be observed the tendency to isolate from the general reliability theory, problems connected with systems safety. This part of theory can be called reliability of system safety. These problems are connected with taking into account effects of failures.

In the most of technical systems, the failures can be divided into two groups. The first group causes the dangerous situation, the second one - only less efficient functioning of the system. As may be seen the results of failures are not equivalent. In the first case we can speak about unreliability of safety, and in the second one about unreliability of efficiency of these systems.

The system safety problems are now in area of interests of both theoreticians and practicians on various fields all over the world.

We can observe it aspecially in such specific fields as for example air space, nuclear physics, transportation, fire-fighting, mining, where the probability of direct impendancy over system's safety is very big. In the world there are two Systems Safety Society: in USA and in France. These Societies organize (one year in USA, next year in France) international conferences. In Poland actually the Systems Safety Group in the fraime of Polish Cybernetic Society (Affiliated by Polish Academy of Sciences) has been established. The aim of this Group is concerning Polish scientific center which is engaged in this subject matter.

2. BASIC DEFINITIONS

The reliability is now a well developped field of science and has many worked out concepts and definitions, which are presented in large literature and normative publications. In this paper we shall mention only most important of them, and our own, which we are using. All the definitions are of normative character:

R - system reliability - probability of fulfilling requirements;

Q - system unreliability - probability of the system failure;

R_B - safety reliability - probability of fulfilling requirements from the point of view of safety, i.e. of non-occurrence of the safety unreliability;

Q_B - safety unreliability - probability of occurrence of an event causing a dangerous situation;

Q_S - efficiency unreliability - probability of occurrence of an event causing an unefficient functioning.

All these concepts deal a definite time and definite exploitation conditions.

3. MATHEMATICAL MODEL OF THE "MAN-MACHINE" SYSTEM

Let us consider an object, which is composed of technical part and operator's part.

The technical part of system can work correctly (state A) or fails (state $\bar{A}$). The probabilities P of these events we denote by $R = P(A)$ and $Q = P(\bar{A}) = 1 - R$, respectively.

In process of exploitation of the object impendancy over safety does not occur or occurs. We denote these events by B and $\bar{B}$, respectively.

There may exist four distinct situations, probabilities of occurrence of which are given by the relations:

$$P(B/A) = 1 - q_B = r_B \tag{1}$$

$$P(\bar{B}/A) = q_B \tag{2}$$

$$P(B/\bar{A}) = q_S = 1 - \bar{q}_B \tag{3}$$

$$P(\bar{B}/\bar{A}) = 1 - q_S = \bar{q}_B \tag{4}$$

In above relations:

r_B - is a probability of non-occurrence of impendancy over safety if the object works correctly;

q_B - is a probability of occurrence of impandancy over safety if the object works correctly;

q_S - is a probability of non-occurrence of impendancy over safety if the object fails;

$\bar{q}_B$ - is a probability of occurrence of impendancy over safety if the object fails.

The probability of non-occurrence of impendancy over safety is given by:

$$R_B = q_S + (1 - q_B - q_S)R \tag{5}$$

It may be proved, that the correlation coefficient for the events of non-occurrence of failure (A) and of non-occurrence of impendancy over safety ($\bar{B}$) is given by formula:

$$\rho_{AB} = \sqrt{\frac{R(1-R)}{R_B(1-R_B)}}\,\frac{dR_B}{dR} \tag{6}$$

in which:

$$\frac{dR_B}{dR} = 1 - q_B - q_S \tag{7}$$

The formulae (5), (6) and (7) determine the relation between the reliability R and the safety R_B.

For analysis of the problems of the object safety the following relations are useful:

$$R_B = q_S + (\bar{q}_B - q_B)\, R = q_S + (r_B - q_S)\, R = Qq_S + Rr_B \tag{8}$$

$$Q_B = 1 - R_B = Rq_B + Q\bar{q}_B = Q - Q_S + Rq_B \tag{9}$$

$$Q_S = Q - Q_B + Rq_B \tag{10}$$

where:

Q_B - is the unreliability of safety;

Q_S - is the unreliability of efficiency.

Let us analyze the above relations from the point of view of influence of various factors on the safety reliability R_B.

- Safety reliability R_B increases with increase of reliability R, if:

  a) $\bar{q}_B > q_B$, $r_B > q_S$, $q_B + q_S < 1$, $\rho_{AB} > 0$

  b) in a special case: $q_B = 0$, $\bar{q}_B > 0$, $\rho_{AB} > 0$

- Safety reliability R_B decreases with increase of reliability R, if:

  a) $\bar{q}_B < q_B$, $r_B < q_S$, $q_B + q_S > 1$, $\rho_{AB} < 0$

  b) in a special case: $\bar{q}_B = 0$, $q_B > 0$, $\rho_{AB} < 0$

- Safety reliability R_B is independent on reliability R, it:

  a) $\bar{q}_B = q_B$, $r_B = q_S$, $q_B + q_S = 1$, $\rho_{AB} = 0$

  b) in a special case: $q_B = \bar{q}_B = 0$, $\rho_{AB} = 0$

- Safety unreliability Q_B may be diminished by increasing of efficiency unreliability Q_S.

4. RECOMMENDATIONS TO CONSTRUCTORS

From the presented above analysis the following recommendations to constructors designing objects with large safety reliability may be formulated:

(i) In the process of object construction one ought to obtain the approaching zero value of conditional probability q_B of occurrence of impendancy over safety under the condition that the object works correctly. It may be reached by choise of such a construction of the object, for which it is practically impossible for an operator to make in expoloitation any error causing impendancy over safety. As an example, it should

be nearly impossible to make a false identification of the actual state of the object (because it may leads to making of unproper control operation) or to touch any of the object's parts being in motion or under the high voltage.

(ii) If the condition $q_B \approx o$ is fulfilled, the safety reliability R_B is practically proportional to the object reliability R. It means, that it is possible to obtain increase of safety by the increse of object reliability (relation 8). The larger reliability may be obtained by enlarging of reliability of object elements or by choise of the object structure with reliability surplus. The most commonly used types of surplus are structural, functional and time surplus.

(iii) The safety reliability R_B may be enlarged by enlarging of conditional probability q_S of occurrence of efficiency unreliability if the object fails. The probability q_S depends on the safety structure of the object. We distinguish the safety structure without surplus (each object failure causes the unreliability of safety) and with surplus (some of failures cause unreliability of safety, other failures cause only unreliability of efficiency). One ought to enlarge the efficiency unreliability Q_S not changing the object unreliability Q. The reliability structure with surplus is in many cases equivqlent to safety structure with surplus. The reliability structure without surplus is in most cases the structure with surplus from the point of view of safety, because not each failure causes unreliability of safety. The most common forms of safety surplus are functional and time surplus.

If the above recommendations are fulfilled, it may be stated using relation (9), that the safety unreliability reaches minimum for the minimal values of object unreliability Q and conditional probability q_B of safety unreliability of correctly working object and for the maximal value of object efficiency unreliability Q_S.

5. THE EXPLOITATION PROBLEMS OF "MAN-MACHINE" SYSTEM SAFETY RELIABILITY

In the "man-machine" system in exploitation, very important are two time intervals, denoted T_W and T_D. The time interval T_W represents time needed by the operator for realization control operation. The time interval T_D represents time, which operator has to his disposal to make the control operation. The time intervals T_W and T_D are random variables of cumulative distribution functions $F_W(t)$, $F_D(t)$ and density functions $f_W(t)$, $f_D(t)$. The control task is made with a fixed time limit when $T_W \leq T_D$. In many cases too late realization of control task causes the danger situations.

The random variables T_W and T_D are correlated. When the operator has to his disposal sufficiently long time he works quietly and among random variables T_W and T_D we do not observe clearly stochastic relations. When T_W is close to T_D, then diminishing of the time T_D causes subsequent diminishing of the time T_W; we can observe an occurrence the psychical mobilization of operator and among random variables T_W, T_D stochastic relations exist. Correlation factor has large positive value. When the time T_D is too short, an operator's demobilization can occure an increase of realization time T_W, and among random variables T_W, T_D the character of stochastic relation is changed; the correlation factor has negative value.

Operator during realization of the task is influence by the stress. Very important form of stress is the time stress. The way of influence of the time stress on an operator shall be presented on the example of changes of stochastic relations between task realization time T_W and disposable time T_D.

In work [5] as a measure of the time stress, function

$$S = \frac{E[T_W]}{T_D} = \frac{\bar{T}_W}{T_D} \tag{11}$$

was proposed.

According to (11) the time stress is the random variable; realization of this variable we denoted S^*. From relation (11) results, that time stress is real situation. During realization of definite controlling task, operator estimates mean time $\bar{T}_W$ of task realization on the base of his experience. The disposable time depends on external factors and is unknown to operator; on operator each time influences realization of the random variable T_D.

In work [5] it is shown, that there exist such a limit value M of time stress (characterising an operator) that for realization of stress S^* we can write:

a) $S^* < 1$ - random variables T_W and T_D are stochastically independent. Disposable time has no influence on task realization time.

b) $1 \leq S^* < M$ - between random variables T_W and T_D are stochastic dependances. These dependances are of such type that with decrease of disposable time, task realization time also decrease, i.e. the stress influence has a mobilizing character.

c) $M \leq S^* < M + 1$ - between random variables T_W and T_D are stochastically dependances. These dependances are of such type, that with decrease of disposable time, task realization time increases, i.e. stress influences on operator in demobilizing manner.

d) $S^* > M + 1$ - stress influence on an operator is of destructive type, i.e. operator can be unable to realize the task.

In the work [5] it was shown that for "typical" operator limited value of stress M is 2,3. For "still" operator M = 1,9-2,2. For "energic" operator M = 2,4-2,8.

The safety reliability measure of "man-machine" system is probability of punctual realization the task:

$$R_B = P(T_W \leq T_D) \tag{12}$$

Probability R_B in general case may be obtained from relation:

$$R_B = \int_0^\infty \int_{\tau_D}^\infty f_{WD}(\tau_D, \tau_W) d\tau_D d\tau_W \tag{13}$$

or

$$R_B = \int_0^\infty \int_{\tau_D}^\infty f_{W/D}(\tau_W, \tau_D) f_D(\tau_D) d\tau_D d\tau_W \tag{14}$$

where:

f_{WD}, $f_{W/D}$ - are respectively cumulative and conditional probability density function random variables T_W adn T_D.

We assume that $\overline{T}_{W/D}$ and $\sigma_{W/D}$ are given by:

$$\overline{T}_{W/D} = \begin{cases} a_1 \dfrac{\overline{T}_W}{S^*} & S^* \in [1, M) \\ a_1 \overline{T}_W S^* + a_1(1 - M)\overline{T}_W & S^* \in [M, M+1) \\ 2 a_1 \overline{T}_W & S^* \in [M+1, \infty) \end{cases} \tag{15}$$

$$\sigma_{W/D} = \begin{cases} \dfrac{a_2 \sigma_W}{S^*} & S^* \in [1, M) \\ a_2(2 S^* + 1 - 2M)\sigma_W & S^* \in [M, M+1) \\ 3 a_2 \sigma_W & S^* \in [M+1, \infty) \end{cases} \tag{16}$$

These relations are illustrated on figure 1. The factors a_1 and a_2 characterize operator qualifications. In practice $a_1 = a_2 = 0,7-1,3$, and for average operator $a = 1$.

6. CONCLUSION

It seems that the model presented in clause 3 can be needed already at the object project stage in order to attain increase of its safety reliability.

We can also observe that in "man-machine" system in exploitation, complicated stochastic relations exist between control task realization time and disposable time.

In practice both these quantities are interdependent stochastic random variables, because operator's predispositions are variable dependent on hour in a day and on lenght of duration realization of the task.

The considerations presented in this paper have been made for transport systems but they have universal character and it seems that can be needed in various fields of technology.

REFERENCES

[1] Gulina O.M., Ostrejkowskij W.A.: Analiticzeskoje zawisimosti dla ocenki nadieżnosti s uczotom korrelacji mieżdu nagruzkoj i niesuszczej sposobnosti obiekta. "Nadieżnost'i kontrol kaczestwa" 2, 1981.

[2] Jaźwiński J.: Psychologiczne problemy bezpieczeństwa pracy z uwzględnieniem problemów niezawodności. Materiały Kolokwium "Niezawodność systemu "obiekt techniczny - człowiek". Wisła 1984.

[3] Jaźwiński J., Ważyńska-Fiok K.: Design of constructions with large safety reliability. Proceedings 4-th Conference on Mechanical Aspects of Electronic Design, "Constronic `84", Budapest 1984.

[4] Jaźwiński J., Ważyńska-Fiok K.: Symulacyjne badania niezawodności i bezpieczeństwa układu "operator - obiekt techniczny". Materiały IV Konferencji "Nauka i praktyka w transporcie". Politechnika Warszawska, Instytut Transportu, Warszawa 1985.

[5] Siegel A.J., Wolf J. Jay,: Man - machine simulation models, psychosocial and performance interaction. John Willey and Sons, Inc. New York.

Recenzent: Doc. dr hab. inż. Jerzy FRĄCZEK

Wpłynęło do Redakcji: luty 1986 r.

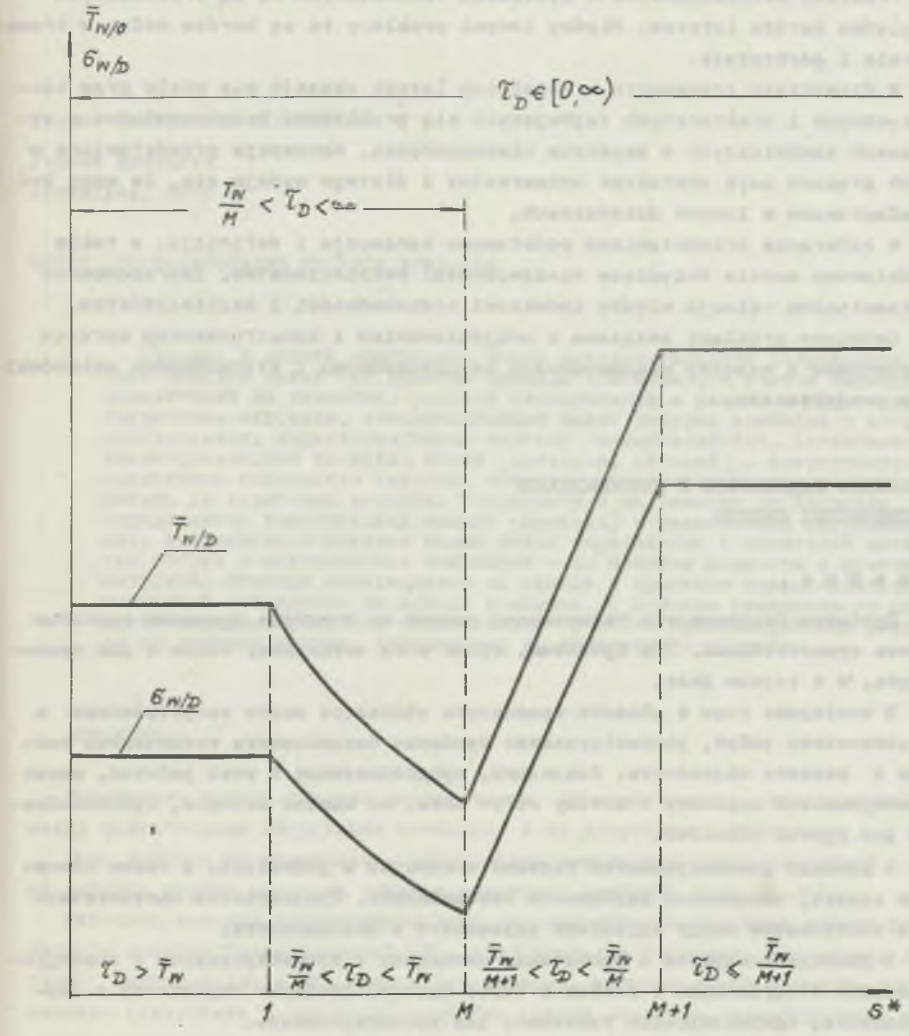

Fig. 1. Relations $T_{W/D}(S)$, $\sigma_{W/D}(S)$

Rys. 1. Zależności $T_{W/D}(S)$, $\sigma_{W/D}(S)$

PROBLEMY NIEZAWODNOŚCI I BEZPIECZEŃSTWA
W SYSTEMACH TECHNICZNYCH

S t r e s z c z e n i e

Problemy bezpieczeństwa w systemach technicznych są ze zrozumiałych względów bardzo istotne. Między innymi problemy te są bardzo ważne w transporcie i górnictwie.

W dziedzinie transportu w ostatnich latach ukazało się wiele prac teoretycznych i praktycznych zajmujących się problemami bezpieczeństwa w systemach technicznych w aspekcie niezawodności. Koncepcje przedstawione w tych pracach mają charakter uniwersalny i dlatego wydaje się, że mogą być zaadaptowane w innych dziedzinach.

W referacie przedstawiono podstawowe koncepcje i definicje, a także podstawowe modele dotyczące niezawodności bezpieczeństwa. Zaproponowano matematyczne relacje między indeksami niezawodności i bezpieczeństwa.

Omówiono problemy związane z projektowaniem i konstruowaniem sprzętu i systemów o wyższej niezawodności bezpieczeństwa i sformułowano wskazówki dla projektantów.

ПРОБЛЕМЫ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ
ТЕХНИЧЕСКИХ СИСТЕМ

Р е з ю м е

Проблемы безопасности технических систем по понятным причинам являются очень существенными. Эти проблемы, кроме всех остальных, важны и для транспорта, и в горном деле.

В последние годы в области транспорта появилось много теоретических и практических работ, рассматривающих проблемы безопасности технических систем в аспекте надежности. Концепции, представленные в этих работах, имеют универсальный характер и потому могут быть, по мнению авторов, приспособлены для других областей.

В докладе рассматриваются главные концепции и дефиниции, а также основные модели, касающиеся надёжности безопасности. Предлагается математическое соотношение между индексами надежности и безопасности.

В докладе говорится о проблемах, связанных с проектированием и конструированием оборудования и систем с более высокой степенью надёжности и безопасности, сформулированы указания, для проектировщиков.