International Journal of KONBIN, 1(3), 2007
ISSN 1642-9311

RELATIONS BETWEEN SAFETY AND SECURITY IN TECHNICAL SYSTEMS

RELACJE MIĘDZY POJĘCIAMI BEZPIECZNOŚCI I BEZPIECZEŃSTWA W UKŁADACH TECHNICZNYCH

SMALKO Zbigniew

Air Force Institute of Technology
Instytut Techniczny Wojsk Lotniczyh,
PL 01– 494 Warszawa, Poland

E-mail: zbigniew.smalko@itwl.pl

Abstract. The subject of this paper deals with the relationship between safety and security of the man - machine system. In the above system a man can act both as a decision - maker and operator. His desired psychophysical efficiency lies in the undertaking the correct decisions as well as in the skilful machine control and operating.

Keywords: safety, reliability, technical systems

Streszczenie. Przedmiotem referatu są relacje między pojęciami bezpieczeństwa i bezpieczności w układzie człowiek – maszyna. Człowiek może występować w takim układzie jako decydent i operator. Jego pożądana sprawność psychofizyczna polega na umiejętności podejmowania słusznych decyzji oraz na sprawnym sterowaniu i operowaniu maszyną.

Słowa kluczowe: bezpieczeństwo, niezawodność, systemy techniczne

1. Introduction

The subject of this paper deals with the relationship between safety and security in the *man - machine* system. A man can act in the above system both as a decision - maker and operator. His desired *psychophysical efficiency* lies in the undertaking the correct decisions as well as in the skilful machine control and operating.

In the set: *man - machine - surroundings*, the realization of definite working tasks takes place. The realization is the result of the following sequence of operations: the man has an effect on the machine; the machine has an effect on surroundings to receive the desired reaction of surroundings (processing, movement, etc.). The positive result of the above activity we will recognize as done by man, *supported by the machine*, together with the *desirable environment reaction*. It is desirable, that the influence of the man and his machine on the surroundings, are *effective and harmless*.

In practice the circumstances of the task realization of the man - machine - surroundings system *are not always favourable* to the safe task performance, because the following events can occur:

- the returnable, undesirable, *harmful for the man reactions, coming from the machine e.g.: vibrations, noise*, can accompany the positive man influence on the machine,
- the assumed positive machine influence on surroundings can accompany undesirable *return* reactions coming from surroundings, which are *harmful for machine, surroundings and the men, e.g.: conflicts and collisions with elements belonging to surroundings in micro* –

1. Wprowadzenie

Przedmiotem referatu układu są relacje między pojęciami bezpieczności i bezpieczeństwa w układzie *człowiek – maszyna.* Człowiek może występować w takim układzie jako *decydent i operator*. Jego pożądana *sprawność psychofizyczna* polega na umiejętności podejmowania słusznych decyzji oraz na sprawnym sterowaniu i operowaniu maszyną.

W układzie: *człowiek- maszyna- otoczenie*, ma miejsce realizacja określonych zadań roboczych. Odbywa się ona w wyniku następującej sekwencji działań: człowiek oddziałuje na maszynę, która z kolei, oddziałuje na otoczenie w celu otrzymania pożądanej reakcji otoczenia (przetworzenia, przemieszczenia itp.). Pozytywny wynik omówionych wyżej działań uznajemy za wykonanie zadania przez człowieka, *wspomaganego przez maszynę* przy *pożądanej reakcji środowiska*. Wskazane jest, przy tym, aby oddziaływania człowieka i jego maszyny na otoczenie były *efektywne i nieszkodliwe*.

W rzeczywistości okoliczności, w jakich może się znaleźć układ: człowiek -maszyna -otoczenie, *nie zawsze sprzyjają bezpiecznemu* wykonaniu zadania, ponieważ:

- z założenia pozytywnym oddziaływaniom człowieka na maszynę mogą towarzyszyć uboczne niepożądane, *szkodliwe dla niego, zwrotne reakcje maszyny np. wibracje, hałas;*
- z założenia pozytywnym oddziaływaniom maszyny na otoczenie mogą towarzyszyć uboczne i niepożądane *wtórne* reakcje otoczenia - szkodliwe *dla niej samej, dla otoczenia oraz dla człowieka, np. konflikty i kolizje z elementami środowiska* w skali mikro oraz/lub w skali makro w wyniku zderzenia z innymi obiektami technicznymi oraz/

and macro - scales as a result of collisions with other technical objects and/or formations of nature,
– the assumed positive, return influence of surroundings on the machine can accompany the undesirable *influence on the man*.

The described factors, together or separately, cause the unfavourable changes in technical states of elements of the man - machine system. The unfavourable task realization circumstances are mostly identified with hazards affecting the man and machine. They are coming both from external forcing factors (environmental, atmospheric) and internal influence factors (of fatigue, wear and ageing character).

2. Hazards of the man-machine system

It is possible to distinguish the following technical states in the *menaced man-machine-surroundings system*: fit for use, partial fit for use, partial unfit for use, critical unfit for use and total unfit for use.

The *fit for use technical state* of the system is characterized with *lack of damages* and with the acceptable operation state of the system, the operator feels safe and the object acts correctly performing the task. The prevention and counteraction of the machine degradation depends on: *technical services, losses completing, system technical state monitoring and user (operator) insurance from incidents, damages and losses results.* The system movement to the partial fit for use technical state we identify as the fault tolerable system.

The *partial fit for use technical state* is characterized with *tolerable faults*, no cross the acceptable operation state of the system,

lub wytworami natury,
– z założenia pozytywnym wtórnym oddziaływaniom otoczenia na maszynę mogą towarzyszyć niepożądane *oddziaływania na człowieka.*

Czynniki te, łącznie lub oddzielnie, powodują niekorzystne zmiany stanów elementów układu: człowiek – maszyna. Okoliczności niesprzyjające wykonaniu zadania utożsamiane są z narażeniami, stwarzającymi zagrożenie dla człowieka i maszyny. Pochodzą one zarówno od zewnętrznych czynników wymuszających (środowiskowych, atmosferycznych) jak i wewnętrznych czynników wymuszających (zmęczeniowych, zużyciowych i starzeniowych).

2. Narażenia układu człowiek - maszyna

W z*agrożonym układzie człowiek - maszyna -otoczenie*, można wyróżnić następujące stany: zdatności, częściowej zdatności, częściowej niezdatności, krytycznej niezdatności i szkodowości.

Stan Zdatności charakteryzuje się *brakiem uszkodzeń*, dopuszczalnym stanem technicznym, operator czuje się bezpieczny a obiekt działa poprawnie wykonując zadanie. Zapobieganie i przeciwdziałanie degradacji maszyny polega na: *obsługach technicznych, uzupełnianiu ubytków, monitoringu stanu, ubezpieczeniu użytkownika (operatora) od następstw wypadków, szkód i strat.* Przejście do stanu częściowej zdatności utożsamiamy z tolerowalnym uszkodzeniem.

Stan Częściowej Zdatności charakteryzuje się *tolerowalnymi uszkodzeniami*, nieprzekroczonym stanem dopuszczalnym, operator odczuwa lekkie zagrożenie i maszyna jeszcze działa poprawnie

the operator feels light threat and machine can still correctly execute the ordered task.

The destructive process of the system has been started. The prevention and counteraction of the machine degradation depends on *self-acting decomposition of surpluses*. The system movement to the *partial unfit for use* technical state we identify as the partial fault intolerable.

The system *partial unfit for use technical state* is characterized with *intolerable partial damages*, the acceptable operation state of system is exceeded and limiting level is reached, the operator feels threatened and machine is not correctly executing the ordered task. It is possible to identify the first symptoms of the process of damages and losses, moreover the threats are occurring and accident is possible. The system movement to the *critical unfit for use technical state* is identified as the *critical fault*.

The system *critical unfit for use technical state* is characterized with *critical faults*, the acceptable operation state of the system is exceed and critical level is reached, the harmful factors are acting on the operator and machine is not correctly executing ordered task or is a subject of stoppage (stops to act and to execute task). It is possible to identify early symptoms of the process of damages and losses. The prevention and counteraction of the machine degradation depends on *slowing down and interruptions of the process of damages and losses formation*, as well as on *the surroundings alarming*. The system movement to the total *unfit for use* technical state we identify as the machine destruction and people injuring.

The system *total unfit for use technical state* is characterized with *extensive destructions, damages and losses*, the

wykonując zlecone zadanie, natomiast zaczynają występować zarodki procesu powstawania szkód i strat. Zapobieganie i przeciwdziałanie degradacji maszyny polega na *samoczynnym rozchodowaniu resursów i nadmiarów.* Przejście do stanu *częściowej niezdatności* utożsamiamy z nietolerowalnym częściowym uszkodzeniem.

Stan Częściowej Niezdatności charakteryzuje się *nietolerowalnymi częściowymi uszkodzeniami,* jest przekroczony stan dopuszczalny i osiągnięty zostaje stan graniczny, operator czuje się zagrożony, obiekt działa niepoprawnie, wykonanie zadania jest wątpliwe, występują symptomy procesu powstawania szkód i strat, a także występują zagrożenia i przewidywany jest wypadek. Przejście do stanu *krytycznej niezdatności* utożsamiamy z *krytycznym uszkodzeniem.*

Stan Krytycznej Niezdatności charakteryzuje się *krytycznymi uszkodzeniami,* przekroczony zostaje stan graniczny i osiągnięty zostaje stan krytyczny, operator jest poddawany szkodliwym oddziaływaniom, obiekt działa niepoprawnie lub przestaje działać i wykonywać zadanie, ma miejsce proces powstawania szkód i strat. Zapobieganie i przeciwdziałanie dalszej degradacji maszyny polega na *spowalnianiu i przerywaniu procesu powstawania szkód* i strat oraz na *alarmowaniu środowiska*. Przejście do stanu *szkodowości* utożsamiane jest ze zniszczeniem maszyny i poszkodowaniem ludzi.

Stan Szkodowości charakteryzuje się *rozległymi zniszczeniami, szkodami* i *stratami*, przekroczony zostaje stan krytyczny, operator jest poszkodowany a obiekt jest zniszczony, maszyna traci właściwości użytkowe i przerywa

critical level of the technical state of the system is over crossed, the operator is injured and machine loses the operation features and the realization of the task is not possible. There are considerable damages and losses observed. The prevention and counteraction of the men - machine system degradation depends on actuating the *rescue system,* as well as *medical and technical emergency services*. The system return to fit for use technical state depends on renovation (or interchange) of the total machine, the medical help, neutralisation of human harm and compensation of the losses.

The specially significant states and properties of the human – machine system are: safety and excess strength. Safety is a particular *state of man – machine – surroundings system*. Whereas security is a particular *attribute of man – machine system*. To perform more detail analysis of it is necessary to explain no less then two basic concepts: hazard and risk.

2.1. Hazard definition

Hazard is understood as a premise of the occurrence of a critical event in the uncertainty circumstances. *The critical events* are the *critical fault of the machine and/or erroneous decisions made by the operator*, which can cause failure and accidents with undesirable effects in the form of fatalities, environment degradation, property loss and financial losses and also causes the different civil-legal consequences for the decision makers and operators.

The real hazard is created by the *external and internal forcing factors*, which after exceeding the permissible limits can cause the different kinds of *critical events* and *undesirable effects* following them. The consequences of the above can be the critical events which obstruct the desirable

wykonanie zadania, a stąd występują znaczne szkody i straty. Zapobieganie i przeciwdziałanie dalszej degradacji układu człowiek-maszyna polega na uruchomieniu *systemu ratowniczego* oraz *pomocy medycznej i technicznej*. Powrót do *stanu zdatności* może polegać na całkowitej odnowie(wymianie) maszyny, na leczeniu i neutralizacji szkód ludzkich i odszkodowaniu strat materialnych.

Do szczególnie istotnych stanów i właściwości układu: człowiek- maszyna zaliczymy: bezpieczeństwo i bezpieczność. Bezpieczeństwem nazywamy wyróżniony stan układu: człowiek-maszyna- otoczenie. Natomiast bezpiecznością – nazywamy wyróżnioną właściwość układu człowiek - maszyna. Bezpieczeństwo dokładniej analizowane wymaga wyjaśnienia nie mniej niż dwóch podstawowych pojęć *zagrożenia i ryzyka.*

2.1. Określenie zagrożenia

Zagrożenie rozumiane jest jako przesłanka wystąpienia krytycznego zdarzenia w warunkach niepewności. *Krytycznymi zdarzeniami* nazywamy *krytyczne uszkodzenia maszyny oraz/lub podjecie błędnych działań przez operatora*, które mogą spowodować awarie i wypadki, z możliwymi niepożądanymi skutkami, w postaci ludzkich szkód, degradacji środowiska naturalnego i utraty mienia, oraz strat finansowych. A także przynosić różnego rodzaju cywilno prawne konsekwencje dla decydentów i operatorów.

Rzeczywiste zagrożeni*e* stwarzają *zewnętrzne i wewnętrzne czynniki wymuszające*, które po przekroczeniu dopuszczalnych granic oddziaływania mogą spowodować różnego rodzaju *krytyczne zdarzenia a* w ślad za nimi *niepożądane konsekwencje.*

functioning of the system, causing failures and accidents.

The first kind of hazard is the possibility of *exceeding the permissible limits of influence* of the external and internal factors (including the human factor). The consequences can be the critical events enabling the effective and safe action of the system causing failures *and accidents*. The second kind of hazard are the expected returnable results of the critical events – *losses, harms and legal consequences* bearded by people and also *harm* to environment and objects of techno-sphere.

Hazard due to its nature exists independently on our lack of sense and knowledge of the current machine condition and atmospheric phenomena. With regards to the above we identify the *self- revealing, possible to be revile and impossible to be revealed*.

2.2. Risk definition

Risk is the qualitatively or quantitatively expressed readiness to suffer the consequences of particular decisions, made in the uncertainty circumstances.

The *consequences* of critical events are *rational and irrational, numerical and qualitative*. There are different scales of the relevance and seriousness of the incurred losses and damages made. There are also the rules regulating conventional penalties for breach of commitments. The consequences of some immeasurable damages and losses are the conventional civil law and financial penalties. In this way it is possible to classify the consequences of critical events from the law and financial point of view.

Usually *risk* is quantified as a combination of *probability or frequency* of critical event occurrence and the adequate *measure of*

Zagrożenie pierwszego rodzaju *stanowi możliwość* przekroczenia dopuszczalnych granic oddziaływania*, przez zewnętrzne i wewnętrzne czynniki wymuszające(w tym przez czynnik ludzki). Konsekwencją tego mogą być krytyczne zdarzenia, które uniemożliwiają poprawne i bezpieczne funkcjonowanie układu powodujące* awarie i wypadki. *Zagrożenie drugiego rodzaju* stanowią *spodziewane wtórne skutki* krytycznych zdarzeń takie jak – *szkody, straty i konsekwencje prawne* ponoszone przez ludzi a także *szkody* wyrządzane środowisku naturalnemu i obiektom technosfery.

Zagrożenie ze względu na swoją naturę istnieje niezależnie od braku naszej świadomości i wiedzy o aktualnym stanie maszyny i zjawiskach atmosferycznych. W związku z tym rozróżniamy zagrożenia *samoujawniające sie, ujawnialne i nieujawnialne.*

2.2. Określenie ryzyka

Ryzykiem nazywamy jakościowo lub ilościowo wyrażoną gotowość poniesienia konsekwencji określonych decyzji, podejmowanych w warunkach niepewności.

Konsekwencje krytycznych zdarzeń są *wymierne i niewymierne, liczbowe i jakościowe*. Stosowane są różne skale istotności i ciężkości ponoszonych strat i wyrządzanych szkód. Jak również istnieją przepisy regulujące wysokość kar umownych za niedotrzymanie zobowiązań.Następstwem niektórych niewymiernych szkód i strat, są umownie wymierne kary cywilno prawne i finansowe. W ten sposób daje się na ogół kwantyfikować konsekwencje krytycznych zdarzeń od strony prawnej i finansowej.

Ryzyko jest na ogół liczbowo wyrażane przez *kombinację prawdopodobieństwa lub częstości* wystąpienia krytycznego

losses, damages or other consequences with numerical evaluation. The qualitative *risk* is connected with the damage or failure of assumed as priceless and unique formations of nature, products of technology, culture and art. The applied decisions making is connected with the possibility of *making error* in the assessment of the dangerous situation development.

The formal estimation of the *permissible level of risk* requires the knowledge of the *frequency* of a particular kind of critical events together with the possibly assigned consequences. This kind of data basis is very useful for planning the preventive tasks in safety systems. However the dynamical assessment of risk level is dependent on the possibility of the estimation of the *expected remaining time* to the critical event from the time instant of its symptoms occurrence. It is necessary to undertake the effective safety measures and rescue action arrangements. This kind of data basis is useful for prevention tasks planning in rescue and advisory expert systems.

2.3. Safety definition

Safety is the state of the system: man, machines and surroundings, in which its elements are not threatening each other. They are also passively and actively adopted for avoiding and neutralization of hazards, which occurrence, due to their character is unavoidable. Unsafety is the state of the system, in which no less than one element threatens no less than one of the other elements of this set. Therefore there is one kind of safety and there are many kinds of unsafety (hazards).

Hazard prevention depends on the particular degree of the possibility of the *expected time to the critical event* estimation, that means the time remaining

zdarzenia oraz odpowiedniej *miary strat, szkód oraz innych konsekwencji* dających się wyrazić liczbowo. *Ryzyko* określane jakościowo odnosi się do zniszczenia lub uszkodzenia, uznawanych za bezcenne, niepowtarzalnych wytworów natury, techniki, kultury i sztuki. Podejmowanie użytkowych decyzji wiąże się z *możliwością popełnienia błędu* w ocenie dalszego rozwoju niebezpiecznej sytuacji.

Formalne oszacowanie *dopuszczalnego poziomu ryzyka* wymaga znajomości *częstości* pojawiania się określonego rodzaju krytycznych zdarzeń wraz z dającymi sie im przypisać konsekwencjami. Tego rodzaju bazy danych są przydatne do planowania przedsięwzięć profilaktycznych w systemach bezpieczeństwa. Natomiast dynamiczna ocena poziomu ryzyka zależy od możliwości oszacowania *pozostałego oczekiwanego czasu* do wystąpienia krytycznego zdarzenia od chwili pojawienia się jego symptomów. Jest to niezbędne do podjęcia skutecznych środków bezpieczeństwa, opuszczenia strefy zagrożonej i przygotowania akcji ratunkowej. Tego rodzaju bazy danych są przydatne do planowania przedsięwzięć profilaktycznych w systemach ratownictwa oraz w doradczych systemach ekspertowych.

2.3. Określenie bezpieczeństwa

Bezpieczeństwem nazywamy stan układu: ludzie, maszyny i urządzenia oraz otoczenie, w którym jego składniki wzajemnie sobie nie zagrażają. A także są biernie i czynnie przysposobione do unikania i neutralizacji zagrożeń, których ze względu na przypadkowość ich występowania uniknąć się nie udaje.

Niebezpieczeństwem nazywamy stan układu, w którym nie mniej niż jeden ze składników zagraża nie mniej niż jednemu

for the tasks averting, neutralizing and eliminating the hazard, on the possessed excesses and protections and on the different types of actions allowing to tolerate the consequences of critical events as well as on the faultless decision-maker - operator decisions to start the machine and propriety of steering the machine, taking into account the changes of machine and surroundings states.

The possibility of making the *second kid of mistake* is very important in the assessment of the threat situation which lies in *assuming the existing hazard as non-existed* and incorrect permission for further performance of the task. These kinds of human error contribute to unnecessary damages and losses.

The individual sense of safety follows from the personal acceptance of the predicted consequences of existing hazards. It is an expression of the subjective valuation of the accepted risk of critical events occurrence and efficiency of applied safeguards. It is necessary to notice that all other principles of establishing permissible social, regional and world wide hazards are also subjective.

From the *legal point of view* the assessment of the dangerous situation lies in the statement of the possibility to obey the rules in the scope of the psychophysical behaviour of the operator (decision – maker) and the regulations in the scope of reaching the permissible values of operational parameters of the machines and devices and also in insurance against civil responsibility.

From the *financial point of v*iew it lies in the statement of the possibility to divide risk between contractors and the possibility of insuring the property and people in the danger zone.

innemu składnikowi tego układu. Stąd ma miejsce jednego rodzaju bezpieczeństwo i wiele rodzajów niebezpieczeństw.

Zażegnanie *niebezpieczeństwa* zależy w określonym stopniu zarówno od stopnia nasilenia zagrożeń jak i od *pozostałego oczekiwanego czasu do wystąpienia krytycznego zdarzenia*, czyli czasu pozostającego na wykonanie przedsięwzięć oddalających, neutralizujących i likwidujących zagrożenia, od posiadania nadmiarów i zabezpieczeń a także od różnego rodzaju przedsięwzięć umożliwiających tolerowanie następstw krytycznych zdarzeń, jak również od bezbłędności decydenta –operatora podczas podejmowania decyzji o uruchomieniu maszyny i poprawności sterowania maszyną – z uwzględnieniem zmian stanu technicznego maszyny i stanu otoczenia. Przy ocenie rozwoju niebezpiecznej sytuacji ważna rolę odgrywa możliwość popełnienia *błędu drugiego rodzaju* polegającego na *uznaniu istniejącego zagrożenia za nieistniejące a* tym samym niewłaściwego zezwolenia na dalszą realizację zadania. Tego rodzaju błąd przyczynia się do powstania niepotrzebnych szkód i strat. Indywidualne poczucie bezpieczeństwa *wynika z osobistej akceptacji spodziewanych konsekwencji istniejących zagrożeń. Jest ono wyrazem subiektywnego wartościowania akceptowalnego ryzyka wystąpienia krytycznych zdarzeń oraz skuteczności zastosowanych zabezpieczeń. Należy zauważyć, ze również sa subiektywne wszelkie inne zasady ustalenia dopuszczalnego społecznego, regionalnego i światowego ryzyka.*

Uznanie sytuacji za bezpieczną *z prawnego punktu widzenia* polega na stwierdzeniu możliwości przestrzegania przepisów w zakresie psychofizycznych zachowań operatora (decydenta) oraz uregulowań

Safety of man – machine – surroundings system depends on:

- *errorless decisions* with regards to risk management,
- *menacing hazard intensity* in dependence on influence factors,
- *efficiency of preventive actions*, averting, neutralizing and eliminating the hazard
- *the remaining expected time* to the critical event,
- *relevance of consequences* of expected critical events,
- *efficiency of rescue actions* decreasing the results and consequences of critical events,
- *range of insurance* allowing to tolerate legal and financial consequences of critical events.

2.4. Security definition

The security when is more detailed analyzed, as the property of man - machine – surroundings system is described by the set of the five concepts: *active emergency , passive emergency, harmlessness, redundancy, protectiveness.*

Active emergency is understood as a property of man - machine – surroundings system describing the adaptation of steering system and man to fast manoeuvring, changes of machine acceleration, velocity of movement and stopping, to act harmlessly and to avoid collisions with surroundings.

Passive emergency resistance is understood as a property of the machine which describes its ability to protect the operator, crew, passengers and cargo against the external consequences and the efficient protection against internal hazards.

Harmlessness is understood as a property describing the man – machine system from the point of clipping the hazardous impact

w zakresie osiągania dopuszczalnych wartości eksploatacyjnych parametrów maszyn i urzadzeń a także na dokonaniu ubezpieczenia od odpowiedzialności cywilnej. Uznanie sytuacji za bezpieczną *z finansowego punktu widzenia* polega na stwierdzeniu możliwości podziału ryzyka na kontrahentów oraz możliwości ubezpieczenia przez decydenta posiadanego mienia i ludzi znajdujących w strefie zagrożenia.

Bezpieczeństwo układu człowiek – maszyna -otoczenie, zależy od:

– *bezbłędności decyzji* dotyczących zarządzania ryzykiem,
– *nasilenia zagrożeń* od czynników wymuszających,
– *skuteczności przedsięwzięć profilaktycznych* oddalających, neutralizujących i likwidujących zagrożenia,
– *pozostałego oczekiwanego czasu* do przekroczenia dopuszczalnych granic przez czynniki wymuszające,
– *istotności konsekwencji* od spodziewanych krytycznych zdarzeń,
– *skuteczności przedsięwzięć ratowniczych* zmniejszających skutki i konsekwencje następstw krytycznych zdarzeń,
– *zakresu ubezpieczeń* umożliwiających tolerowanie prawnych i finansowych skutków krytycznych zdarzeń.

2.4. Określenie bezpieczności

Bezpieczność jest właściwością układu człowiek-maszyna polegającą na zapewnieniu wyjścia ze strefy zagrożenia manewrem oraz/lub zapewnieniu niezbędnych nadmiarów i odporności na szkodliwe wymuszenia wewnętrzne i zewnętrzne. Bezpieczność dokładniej analizowana, jako właściwość układu: człowiek-maszyna-otoczenie, opisywana jest zbiorem pieciu pojęć: niezagrażalności, ochranialności, nieszkodliwości, nadmiarowości, zabezpieczalności.

of the machine at the nature surroundings.

Redundancy is understood as a property describing the man – machine system elements reserve, which makes possible to tolerate the machine damages and man mistakes, as a result of creation of the excesses: structural, functional, time and informational.

Protectiveness is understood as a property of the machine - surroundings system which describes the warning and blocking subsystems of the machine – surroundings system making impossible the access to the system by an unauthorized persons and/or persons improperly operating the object.

3. Concluded remarks

The random evolution of a dangerous situation proceeds in practice independently of our own will. However the counteraction of the further progress of the dangerous situation are determined and placed in time.

The sequence of the applied main concepts is as follows - we identify threats and their consequences, we assess the chances of the undesirable effects of critical events occurrence, we estimate the risk of decision making and on that basis we state the safety of the system. We make the corrections of the evaluation, taking into account the available safety measures and security features of the operator and machine.

The presented paper should be considered as a disputable attempt to precise the concepts connected with the widely understood safety of the human-machine-surroundings system.

Niezagrażalność (bezpieczność czynna), rozumiana jest jako właściwość układu człowiek maszyna opisująca przysposobienie układu sterowniczego i podatności człowieka do szybkiego manewrowania, zmiany przyśpieszeń, prędkości przemieszczania i hamowania maszyny, celem bezszkodowego działania i unikania kolizji z otoczeniem.

Ochranialność (bezpieczność bierna), rozumiana jest jako właściwość maszyny opisująca jej przysposobienie do ochrony operatora, załogi, pasażerów i ładunków przed skutkami zewnętrznych i wewnętrznych narażeń.

Nieszkodliwość rozumiana jest jako właściwość układu: człowiek maszyna opisująca jego przysposobienie do ograniczenia szkodliwego oddziaływania maszyny na środowisko naturalne.

Nadmiarowość rozumiana jest jako właściwość opisująca rezerwowanie elementów układu: człowiek - maszyna, które stwarza możliwość tolerancji uszkodzeń maszyny i błędów człowieka, w wyniku stworzenia w nim nadmiarów: strukturalnych, funkcjonalnych, czasowych i informacyjnych.

Zabezpieczalność rozumiana jest jako właściwość układu: maszyna-otoczenie opisująca system ostrzegawczy i blokujący układu uniemożliwiający użytkowanie maszyny przez osoby nieuprawnione oraz/lub przez osoby nieumiejętnie operujące obiektem.

3. Uwagi końcowe

Tak, więc sekwencja stosowania głównych pojęć przebiega następująco identyfikujemy zagrożenia i ich konsekwencje, oceniamy szanse wystąpienia niepożądanych następstw krytycznych zdarzeń.

References/ Literatura

1. Avizienis J., Larie G., Randel B. *Fundamental Concepts of Dependability*. Newcastle University, Report no. CS-TR-739, Newcastle, October 2000.
2. Jazwiński J., Borgoń J.: *Niezawodność eksploatacyjna i bezpieczeństwo lotów*. WKIŁ, Warszawa, 1989.
3. Mazur M.: *Terminologia techniczna*. WNT, Warszawa, 1961.
4. PN-77/N-04010, *Wybór wskaźników niezawodności*. PKNMiJ 1977.
5. Puszkin W.G.: *Probliema Nadeżnotsi*. Izdatelstwo Nauka, Moskwa, 1971.
6. Smalko Z.: *Pięć podstawowych pojęć w technice*. Komitet Naukoznawstwa PAN, Warszawa, 1987.
7. Smalko Z.: *Charakterystyki poleglisci układu człowiek - maszyna - otoczenie*. Materiały Szkoły Niezawodności PAN, Wydawnictwo ITE , Radom, 2007.

Oszacowujemy ryzyko podjęcia określonych decyzji i na tej podstawie orzekamy bezpieczeństwo układu.

Dokonujemy korekty tej oceny uwzględniając dostępne środki bezpieczeństwa uwzględniając właściwości bezpiecznościowe operatora i maszyny. Losowy rozwój sytuacji niebezpiecznej w zasadzie przebiega niezależnie od naszej woli. Natomiast przeciwdziałania dalszemu rozwojowi niebezpiecznej sytuacji są zdeterminowane i umiejscowione w czasie.

Niniejsze opracowanie należy traktować jako dyskusyjną próbę uściślenia pojęć związanych z szeroko rozumianym bezpieczeństwem układu człowiek-maszyna-otoczenie.

Prof. dr hab. inż. Zbigniew SMALKO, professor of the Air Force Institute of Technology, Warszawa, as well as the University of Technology, Faculty of Transport. Specialist in reliability safety and maintainability of technical transport systems, operation problems of transport systems and devices. Author and co-author of more then 200 scientific publications. Member of: Polish Academy of Science (PAN) – Transport Committee, PTBiN, ERN SAFERLENET, ETNiŚT; Editor in Chief of Archives of Transport, Chair of Winter Schools of Reliability PAN. Organisator and member of several scientific and programme committees of international and national conferences and symposiums