Nienaruszalność bezpieczeństwa przegubowych konstrukcji robotów

Tadeusz Missala[1]

Streszczenie

Roboty wprowadzają liczne zagrożenia do środowiska pracy i środowiska naturalnego. Kategoria zagrożeń (od niewielkich do katastrofalnych) zależy od rodzaju czynności wykonywanych przez robot. Zwrócono uwagę na różnice między robotami przemysłowymi i robotami obsługowymi. Na tle zasad określania poziomu ryzyka tolerowanego przeanalizowano nienaruszalność bezpieczeństwa typowego rozwiązania robota 5-cio osiowego i wykazano, że jest ona zbyt mała. Przedstawiono analizę wykazującą możliwość osiągnięcia poziomu SIL 3, wystarczająco wysokiego do zastosowań związanych z bezpieczeństwem.

1. WPROWADZENIE

Co to jest robot bezpieczny ?

Klasyczne prawo Asimova formułuje to następująco: **Robot nie ma prawa uczynić krzywdy człowiekowi.**

To wymaga rozszerzenia: nie uczyni krzywdy ani człowiekowi, ani procesowi, który wykonuje lub obsługuje, ani środowisku naturalnemu, np. przez spowodowanie szkód ekologicznych wynikających z uszkodzenia urządzeń procesowych, ani nie spowoduje strat materialnych wynikających z odszkodowań za wypadki z ludźmi i/lub kar za straty ekologizne i/lub strat z powodu przerwy w produkcji.

W tym kontekście należy rozpatrzyć różne rodzaje robotów i różne sytuacje, w których one pracują.

1.1. Robot przemysłowy

Są tu dwie sytuacje: przy normalnej pracy robot nie współpracuje z człowiekiem lub z nim współpracuje.

W sytuacji pierwszej mogłoby się wydawać, że stanowisko robota wystarczy odgrodzić barierami, mechanicznymi lub optoelektronicznymi, aby uzyskać bezpieczeństwo (brak zagrożeń). Jednakże należy brać pod uwagę prace wykonywane przez personel specjalistyczny: programowanie, serwis, naprawy, przy których wejście w strefę pracy robota jest konieczne. Ponadto zawsze istnieje

[1] Przemysłowy Instytut Automatyki i Pomiarów, 02-486 Warszawa, Al. Jerozolimskie 202. tmissala@piap.pl, www.piap.pl

kontakt robota z procesem i urządzeniami realizującymi proces lub mu poddawanymi. Czym innym będzie, gdy wskutek złego zadziałania robota wypadną kartony lub skrzynki z piwem, a zupełnie czym innym gdy rozbiją się butle z fosgenem. Samo zabezpieczenie barierą nie rozwiązuje problemu, są potrzebne inne środki ograniczania ryzyka.

1.2. Robot obsługowy

Z założenia robot obsługowy kontaktuje się z człowiekiem i to z osobą niepełnosprawną. Nie tylko musi być dla niej przyjazny w czasie normalnej obsługi, ale przede wszystkiem musi być dla niej bezpieczny. Reakcja człowieka na nienormalne zachowanie robota może być spóźniona lub całkowicie niemożliwa.

Bezpieczne funkcjonowanie robota w najbliższym otoczeniu człowieka jest sprawą zasadniczą. W referacie rozwinięto tezy przedstawione na poprzedniej Krajowej Konferencji Robotyki [4].

Rozpatruje się problem uzyskania wystarczającego zmniejszenia ryzyka wynikającego z pracy robota.

2. BEZPIECZEŃSTWO A RYZYKO

2.1. Definicje [1]

W dalszym ciągu referatu będą stosowane poniższe definicje:

szkoda

fizyczny uraz lub pogorszenie stanu zdrowia ludzi, tak bezpośrednie jak i pośrednie, wynikające ze szkody w majątku lub w środowisku

zagrożenie

potencjalne źródło szkody

UWAGA – Termin obejmuje niebezpieczeństwo krótkotrwałe oraz oddziałujące długotrwale (na przykład wydzielanie substancji toksycznych).

sytuacja zagrożenia

sytuacja, w której osoba jest narażona na zagrożenie (-a)

zdarzenie zagrażające

sytuacja zagrażająca, której wynikiem jest szkoda

ryzyko

kombinacja prawdopodobieństwa wystąpienia szkody i ciężkości tej szkody

ryzyko tolerowane

ryzyko, które jest akceptowane w określonym kontekście opartym na aktualnych wartościach społecznych

ryzyko resztkowe

ryzyko pozostające po zastosowaniu środków bezpieczeństwa

bezpieczeństwo

niewystępowanie ryzyka nieakceptowanego

bezpieczeństwo funkcjonalne
część bezpieczeństwa całkowitego odnosząca się do obiektu i jego systemu sterowania, która zależy od prawidłowego działania systemów E/E/PE związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innych technikach i zewnętrznych środków do zmniejszania ryzyka

nienaruszalność bezpieczeństwa
prawdopodobieństwo, że system związany z bezpieczeństwem wykona w sposób zadowalający wymagane funkcje bezpieczeństwa, we wszystkich określonych warunkach i w określonym przedziale czasu

stan bezpieczny
stan obiektu, charakteryzujący się osiągnięciem bezpieczeństwa

dające się racjonalnie przewidzieć użycie niewłaściwe
użycie wyrobu, procesu lub usługi w warunkach lub do celów nie zamierzonych przez dostawcę, które mogą się jednak zdarzyć w powiązaniu ze zwyczajowym zachowaniem się człowieka względem wyrobu, procesu lub usługi

2.2. Ryzyko robota (obiektu) a ryzyko tolerowane

Każde urządzenie techniczne i każdy proces wytwórczy mogą być zaprojektowane starannie z punktu widzenia bezpieczeństwa lub też nie. Dlatego pierwszym krokiem jest ocena zagrożeń i ryzyka, jakie niesie rozpotrywane urządzenie techniczne tak przy pracy normalnej, jak i w dającym się racjonalnie przewidzieć użyciu niewłasciwym

Robot jest źródłem zagrożeń wynikających z jego ruchów manipulacyjnych, utrzymywania przedmiotów w chwytaku oraz ruchów komunikacyjnych (przejeżdzanie z jednego miejsca na inne). Każde nieprawidłowe wykonanie dowolnej czynności może wywołać sytuację zagrażającą.

Może być różny poziom ryzyka tolerowanego, który wynika m. in. z:

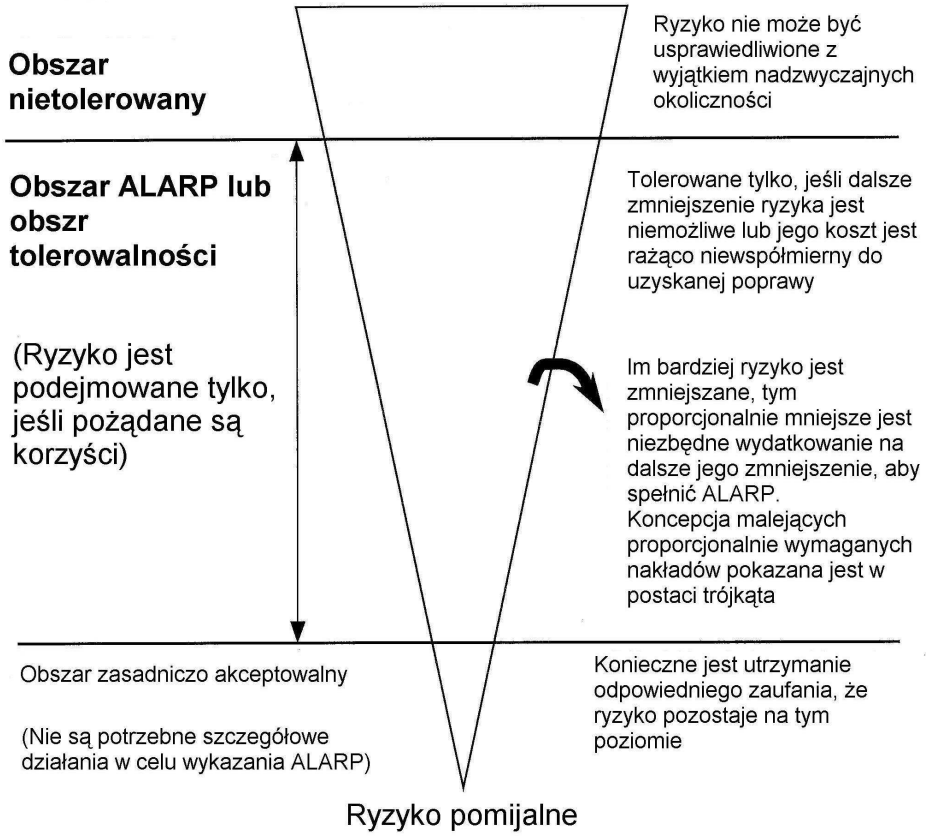
- rodzaju wykonywanych czynności;
- rodzaju przedmiotów manipulowanych;
- obowiązujących przepisów; BHP, ochrony środowiska, ochrony przed awariami przemysłowymi, ochrony przeciwwybuchowej;
- konsekwencji i kosztów awarii wywołanej przez robota;
- stanowiska firm ubezpieczycielskich.

Przejście od ryzyka robota do ryzyka tolerowanego dobrze ilustruje zasada ALARP (As Low As Rational Practicable), którą zilustrowano na rysunku 1. W tablicy 1 przedstawiono przykłady klasyfikacji ryzyka wypadków

- klasa ryzyka I odpowiada obszarowi nieakceptowanemu;
- klasy ryzyka II i III odpowiadają obszarowi ALARP, z tym, że klasa ryzyka II odpowiada tylko wewnętrznej części obszaru ALARP;
- klasa ryzyka IV odpowiada obszarowi zasadniczo akceptowanemu.

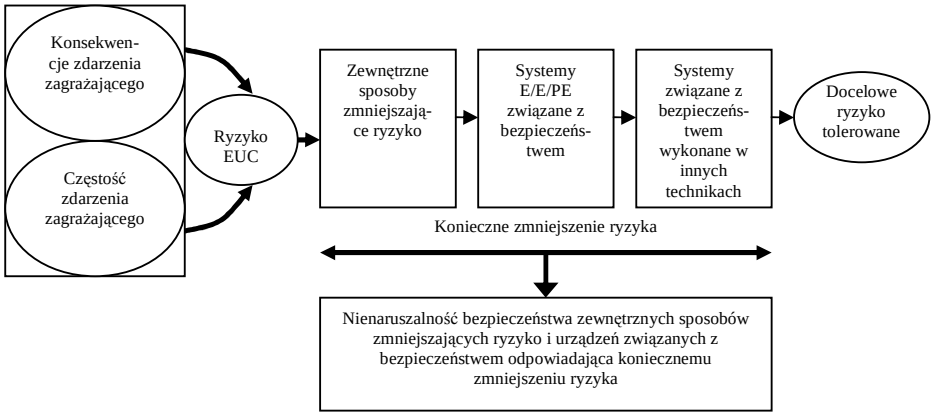
Tab. 1. Przykład klasyfikacji ryzyka wypadków [1]

Częstość	Konsekwencje			
	Katastrofalne	**Krytyczne**	**Niewielkie**	**Pomijalne**
Częsty	I	I	I	II
Prawdopodobny	I	I	II	III
Sporadyczny	I	II	III	III
Mało prawdopodobny	II	III	III	IV
Nieprawdopodobny	III	III	IV	IV
Niewiarygodny	IV	IV	IV	IV



Rys. 1. Schemat metody ALARP [1]

Sposób postępowania w obszarze zmiejszania ryzyka zilustrowano na rysunku 2.



Rys. 2. Ryzyko i nienaruszalność bezpieczeństwa [1]

3. ANALIZA ROBOTA

3.1. Ustalanie wymagań bezpieczeństwa

Poziom wymagań bezpieczeństwa będzie różny zależnie od zastosowania, z którym będzie związana klasa ryzyka (patrz tablica 1). Przyjęto wyrażanie poziomu wymagań bezpieczeństwa w kategoriach:

- zapewnianych funkcji bezpieczeństwa;
- nienaruszalnosci bezpieczeństwa tych funkcji.

Funkcjami bezpieczeństwa są:

- wszystkie funkcje związane z realizacją ruchu robota (roboty obsługowe), ochrona programistów i personelu obsługującego lub współpracującego z robotem;
- funkcje zakazu dostępu do obszaru pracy robota.

Poziom nienaruszalności bezpieczeństwa (SIL) jest zdefiniowany w przypadku robota (rodzaj pracy ciągły), intensywnością uszkodzeń niebezpiecznych na godzib\nę według tablicy 2 [1].

Tab. 2. Poziomy nienaruszalności bezpieczeństwa: docelowe miary uszkodzeń funkcji bezpieczeństwa działających w rodzaju pracy na częste przywołanie lub ciągłym

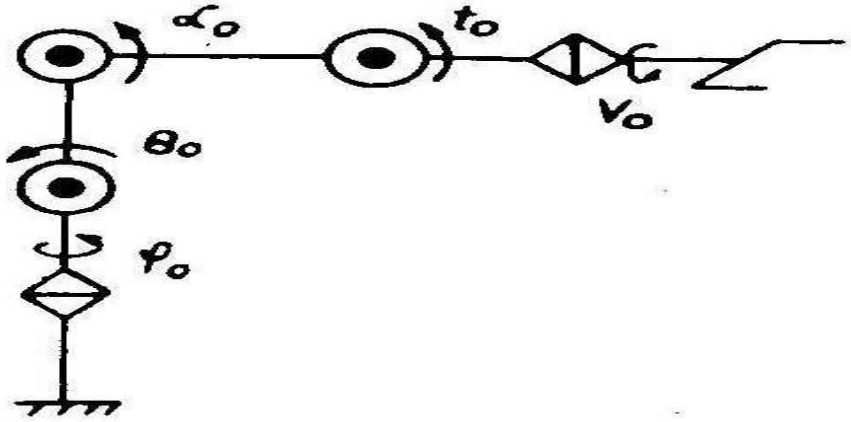
Poziom nienaruszalności bezpieczeństwa	**Rodzaj pracy na częste przywołanie lub ciągły** (Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę)
4	od $\geq 10^{-9}$ do $< 10^{-8}$
3	od $\geq 10^{-8}$ do $< 10^{-7}$
2	od $\geq 10^{-7}$ do $< 10^{-6}$
1	od $\geq 10^{-6}$ do $< 10^{-5}$

Do wstępnego ustalenia wymagań bezpieczeństwa robota pracującego w gnieździe produkcyjnym można posłużyć się jedną z metod opublikowanych w [1,2], na przykład metodą jakościową – grafem ryzyka. Wynikiem będzie wymagany poziom nienaruszalności bezpieczeństwa SIL

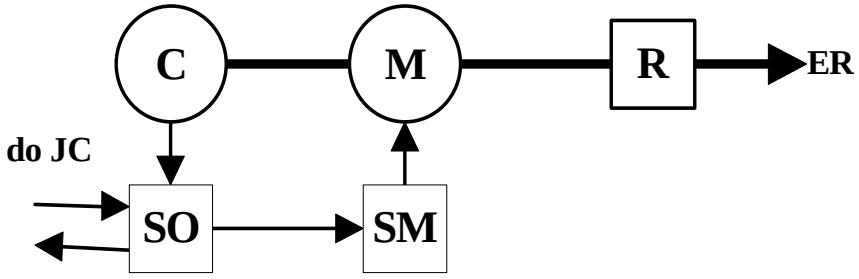
3.2. Ocena SIL robota bez wprowadzania zabezpieczeń (poziom rysyka procesu z rys. 2)

Rozpatruje się łańcuch funkcjonalny realizacji ruchów manipulacyjnych robota. Przykładowy schemat kinematyczny robota przegubowego przedstawiono na rysunku 3 [3].

Na łańcuch realizacji ruchów manipulacyjnych robota składają sie ruchy jego trzech głównych osi (φ, Θ, α) dwóch osi powiązanych z chwytakiem (t, v) oraz zamykanie i otwieranie chwytaka. Podstawowa architektura osi jest typu 1oo1 i została przedstawiona na rys. 4.

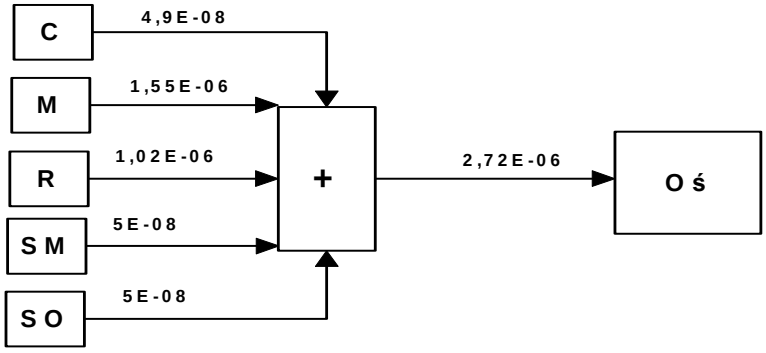


Rys. 3. Schemat kinematyczny robota



Rys. 4. Schemat blokowy osi robota
C – czyjnik położenia, M – silnik, R – przekłasnia (reduktor), SO – sterownik osi, SM – sterownik silnika; JC – jednostka centralna robota, ER – element mechaniczny robota

Z analiz wykonanych przez autora i przedstawionych w [3 - 7] wynika, że stosując dobre elementy handlowe, których dystrybuantę uszkodzeń można przybliżyć rozkładem normalnym uciętym i które można uznać za nienaprawialne w okresie gwarantowanej trwałości, nienaruszalność bezpieczeństwa architektury z rys. 4 można zobrazować modelem niezawodności przedstawionym na rys. 5 [9].



Rys. 5. Model niezawodnościowy osi robota
Oznaczenia jak na rys.4. Liczby podaja intensywności uszkodzeń na godzinę

Intensywności uszkodzeń podane na rys. 5 pochodzą z następujacych źródeł:

- czujnika położenia, silnika i przekładni z [6] po przeliczeniu na prawdopodobienstwo wyznaczenia trwałości wynikające z rozkładu normalnego [7] tj. 0,9592,
- sterowników z [1] w założeniu, że są one typu "fail-safe" o SIL 3.

W realizacji ruchu manipulacyjnego biorą udział wszystkie osie, a więc w modelu niezawodnościowym ich intensywności uszkodzeń sie dodają. Intensywność uszkodzeń robota przy pominęciu jednostki centralnej) będzie więc:

$$\lambda_{robota} = 5 \times \lambda_{osi} = 5 \times 2{,}72 \times 10^{-6} = 1{,}36 \times 10^{-5},$$

to jest poniżej SIL 1.

Takie rozwiązanie jest mozliwe do zaakceptowania co najwyżej w robotach przemysłowych, nie jest akceptowane w robotach obsługowych i medycznych.

3.3. Drogi zmiejszania ryzyka

Z rys. 5 widać, że elementami wnoszącymi najwiekszą intensywność uszkodzeń są silnik i przekładnia (udział 94,5 %). Ponieważ nie można zastosować rozwiązań nadmiarowych, przeto pozostaje diagnostyka i próby okresowe.

Jak wynika z danych zawartych w [1], w architekturze 1oo1, przy intensywności własnej uszkodzeń $\lambda = 1{,}0 \times 10^{-7}$ tj. takiej jak podana na rys. 5, pokryciu diagnostycznym DC = 90%, MTTR równym 8 h i 6-cio miesięcznym odstępie prób okresowych otrzymuje się wynikową intensywność uszkodzeń na poziomie

$\lambda = 5{,}0 \times 10^{-9}$.

Ta wartość zostanie przyjęta do rozważeń końcowych. Pokrycie diagnostyczne, o którym mowa wyżej można uzyskać między innymi przez:

- wprowadzenie procedury okresowego pomiaru prądów pobieranych przez silniki w stanie jałowym i bez forsowania prądu,
- wprowadzenie czujników i układu pomiaru hałasu pracujących silników i reduktorów i porównywanie z danymi wzorcowymi,
- wykorzystanie odkształceń sygnału wyjściowego rezolwera do nadzorowania pracy serwomechanizmu [8],
- staranny przegląd podczas prób okresowych.

Niezależnie od powyższego można uzyskać dalsze obniżenie ryzyka stosując redundancje po stronie pomiaru położenia. Wprowadzenie jej jest możliwe, np. przez stosowanie klasycznego rozwiązania z prądnicą tachometryczną i całkowanie jej sygnału. Zastosowanie architektury 1oo2 [1,9] da znaczne ograniczenie intensywności uszkodzeń niebezpiecznych. Za [1] wprowadza sie oznaczenia:

PFH_s – prawdopodobienswo uszkodzenia na godzine grupy nadmiarowej czujników;

β - udział uszkodzeń o wspólnej przyczynie w uszkodzeniach niewykrytych przez testy diagnostyczne (tu $\beta = 0{,}02$),

β_D - udział uszkodzeń o wspólnej przyczynie w uszkodzeniach wykrytych przez testy diagnostyczne (tu $\beta_D = 0{,}01$),

λ_D – intensywność uszkodzeń niebezpiecznych na godzinę, równa połowie całkowitej intensywności uszkodzeń λ, (tu $\lambda = 4{,}9 \times 10^{-8}$, $\lambda_D = 2{,}45 \times 10^{-8}$),

λ_{DD} – intensywność uszkodzeń niebezpiecznych wykrytych przez testy diagnostyczne.

λ_{DU} – intensywność uszkodzeń niebezpiecznych niewykrytych przez testy diagnostyczne,

DC – pokrycie diagnostyczne (przyjęto $DC = 0{,}6$)

T_1 – odstęp prób okresowych (przyjęto 6 miesięcy, tj. $T_1 = 4380$ h),

$MTTR$ – średni czas do naprawy (tu $MTTR = 8$ h)

t_{CE} – średni równoważny czas niedyspozyczyjności kanału przy architekturze 1oo1, 1oo2, 2oo2 i 2oo3 (w godzinach)

Wg [1] jest:

$$PFH_s = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} + + \beta_D \lambda_{DD} + \beta \lambda_{DU},$$

$$\lambda_{DU} = \frac{\lambda}{2}(1-DC) = 0{,}98 \times 10^{-8},$$

$$\lambda_{DD} = \frac{\lambda}{2} DC = 1{,}47 \times 10^{-8},$$

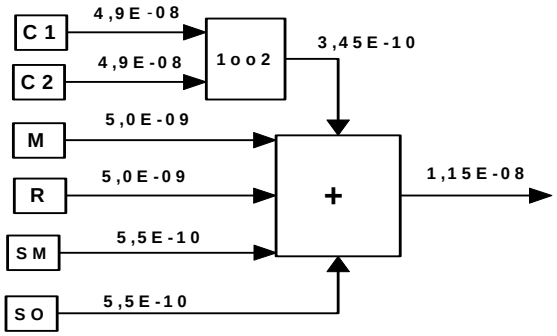
$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR,$$

$$t_{CE} = 0{,}4(2190+8) + 0{,}6\times 0{,}8 = 884\,,$$

$$PFH_s = 2(0{,}98\times 1{,}47 + 0{,}98\times 0{,}98)^2 \times 10^{-16} \times 884$$

$$+ 0{,}01\times 1{,}47\times 10^{-8} + 0{,}02\times 0{,}98\times 10^{-8} = 3{,}45\times 10^{-10}\,.$$

Wykorzystując wykonane obliczenia otrzymuje się zmodyfikowany model niezawodnościowy osi robota przedstawiony na rys. 6.



Rys.6. Zmodyfikowany model niezawodnościowy osi robota
Oznaczenia jak poprzednio

W powyższym modelu przyjęto, że sterownik osi i sterownik silnika są jednostkami o architekturze 1oo2, co upoważniło do przyjęcia intensywności uszkodzeń niebezpiecznych na poziomie $5{,}5\times 10^{-10}$. Jeśli taką samą niezawodność przypisać jednostce centralnej, to intensywność uszkodzeń całego robota będzie:

$$\lambda_{robota} = 5\times 1{,}15\times 10^{-8} + 5{,}5\times 10^{-10} = 5{,}805\times 10^{-8}\,,$$

co odpowiada poziomowi SIL 3, akceptowanemu w odniesieniu do robotów obsługowych i medycznych[4].

4. KONKLUZJA

Z przedstawionych rozważań wynika, że stosując odpowiednie techniki diagnostyczne i architektury nadmiarowe można zwiększyć nienaruszalność bezpieczeństwa robota z poziomu niekwalifikującego do stosowania w instalacjach związanych z bezpieczeństwem do poziomu SIL 3, akceptowanego w takich zastosowaniach.

LITERATURA

[1] PN-EN 61508-1: *Bezpieczeństwo funkcjonalne elektrycznych /elektronicznych /programowalnych elektronicznych systemów związanych z bezpieczeństwem – Części 1-7.*
[2] PN-EN 61511: 2005(U) – *Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora procesów przemysłowych – Części 1-3*.
[3] T. Missala. Robot positioning error due to resolver's errors. In: 33. International Wissenschaftlichen Kollokwium T.H. Ilmenau, *Vortragreihe „Technische Kybernetik/Automatisierungstechnik"*, Ilmenau-GDR, October 1988, s. 229-232.
[4]T. Missala. Robot jako system związany z bezpieczeństwem. In: *Postępy robotyki. Przemysłowe i medyczne systemy robotyczne.* Red. K. Tchoń. Warszawa, WKŁ, 2005.
[5] T. Missala. Errors of the servomechanism velocity measurement realized by signal scanning of the displacement transducers. In: *Prace Krajowego Kongresu Metrologii KKM'98*, t. 3, Gdańsk - Poland, June 1988, s. 385-393.
[6] T. Missala. Mechatronics Elements in Safety-Related Circuits. In: *Mechatronics 2004 Warsaw University of Technology, Faculty of Mechatronics and Brno University of Technology, Faculty of Mechanical Engineering*, Elektronika, 2004 r., No 8-9, s.183 – 185.
[7] T. Missala. Metodologia oceny nienaruszalności bezpieczeństwa elementów o ustalonej trwałości. In: *Materiały Konferencji Automation'2006*, s. 111 - 118, Warszawa – Poland, 2006 r.
[8] T. Missala. Diagnostyka serwomechanizmu na podstawie sygnału wyjściowego rezolwera. In; *Prace XV Międzynarodowego Sympozjum „Mikromaszyny i Serwonapędy"*, Białowieża - Poland, Wrzesień 2006 r. (w druku).
[9]M. Śliwiński. *Metody analizy systemów sterowania i zabezpieczeń z uwzględnieniem kryteriów bezpieczeństwa funkcjonalnego.* Rozprawa doktorska, Politechnika Gdańska, Gdańsk 2006 r.

SAFETY INTEGRITY OF TURN-WRIST ROBOT CONSTRUCTIONS

Robots introduce many hazard situations into labor and natural environment Hazard cathegory (from little to catastrophic) depends from the activities carried out by the robot. The attantion was turned on thedifferences between industrial robots an servicing robots. On the ground of the tolerable risk level determination principles, the safety integrity of the typical 5-axis robot was assessed and was demonstrated that it is too low. The analysis was performed and it is shown, the diadnostic and redundant architectures give the possibility to achieve the level SIL 3, sufficient for safety-related applications.