Marek Dźwiarek

Bezpieczeństwo funkcjonalne systemów sterowania maszynami

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy

CIOP PIB

Bezpieczeństwo funkcjonalne systemów sterowania maszynami

Marek Dźwiarek

Bezpieczeństwo funkcjonalne systemów sterowania maszynami

Warszawa 2012

Dyrektor Centralnego Instytutu Ochrony Pracy
– Państwowego Instytutu Badawczego
prof. dr hab. med. Danuta Koradecka

Niniejsze opracowanie zostało przygotowane na podstawie rezultatów projektów w zakresie badań naukowych i prac rozwojowych, w tym w ramach programów wieloletnich pn. „Dostosowywanie warunków pracy w Polsce do standardów Unii Europejskiej" oraz „Poprawa bezpieczeństwa i warunków pracy" wykonanych w latach 2002-2010, koordynowanych przez Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy

Opiniodawca
prof. dr hab. Kazimierz Lebecki

Autor
dr inż. Marek Dźwiarek
Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy

Projekt okładki
Anna Antoniszewska

ISBN 978-83-7373-126-4

CIOP PIB

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy
ul. Czerniakowska 16, 00-701 Warszawa
tel. (48-22) 623 36 98, fax (48-22) 623 36 93, www.ciop.pl

Pragnę złożyć serdeczne podziękowanie wszystkim, którzy przyczynili się do powstania tego opracowania.

Szczególne słowa podziękowania kieruję do ***Pani prof. dr hab. med. Danuty Koradeckiej*** za twórcze inspirowanie i wielką życzliwość dla moich naukowych dążeń oraz umożliwienie mi wykonania w Centralnym Instytucie Ochrony Pracy – Państwowym Instytucie Badawczym wszystkich prac badawczych będących podstawą tej książki.

Najserdeczniejsze podziękowania składam mojej żonie, Ewie, która wspierała mnie przez te wszystkie lata. Bez jej codziennego wsparcia, życzliwości i poświęcenia nie byłoby możliwe osiągnięcie tego, do czego dążyłem.

Marek Dźwiarek

Spis treści

Rozdział 1

Wprowadzenie

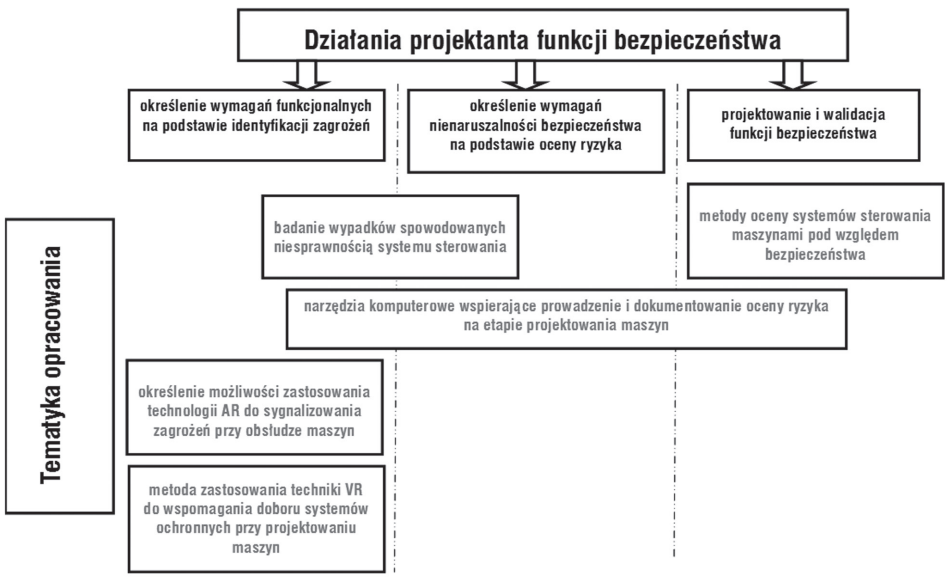
1.1. Wstęp

Nowoczesnym technologiom zawdzięczamy coraz bardziej wydajne i uniwersalne maszyny. Zwłaszcza zastosowanie komputerów i złożonych układów elektronicznych umożliwiło znaczne zwiększenie skuteczności i jednocześnie zmniejszenie ceny systemów sterowania maszynami. Dlatego też układy programowalne można napotkać zarówno w odbiorniku telewizyjnym czy samochodzie, jak i w obrabiarce, robocie przemysłowym, a także w systemach nadzorujących pracę elektrowni atomowych i przebieg złożonych procesów chemicznych. Uszkodzenie systemu programowalnego pracującego w odbiorniku telewizyjnym wiąże się jedynie z niewielkimi kosztami ponoszonymi przez użytkownika, natomiast niewłaściwe działanie systemu sterowania napędem w pojazdach czy systemu sterowania obrabiarką może być przyczyną tragicznego w skutkach wypadku. Defekt sterownika kontrolującego pracę urządzenia ochronnego stosowanego do maszyn szczególnie niebezpiecznych prawie zawsze kończy się ciężkim wypadkiem. W większości typowych sytuacji błędy projektanta, których skutkiem jest niewłaściwe realizowanie założonych funkcji maszyny, ujawniają się dopiero w sytuacjach szczególnych, odbiegających od zwykłych warunków pracy urządzenia. Sytuacji takich nie można uniknąć poprzez działania zapobiegawcze na stanowisku pracy. Jedyną metodą jest zapewnienie, żeby podczas projektowania urządzenia uniknięto błędów i zastosowano właściwe rozwiązania konstrukcyjne. W procesie projektowania systemów bezpieczeństwa powinno się więc uwzględniać zjawiska występujące w warunkach defektu systemu, a projektant powinien stosować odpowiednio skuteczne środki zapobiegające związanym z tymi defektami sytuacjom niebezpiecznym.

Tak więc projektant systemu bezpieczeństwa musi zagwarantować spełnienie dwu celów, jakimi są:

– wytworzenie systemu umożliwiającego maszynie realizację założonych funkcji, z uwzględnieniem wymagań bezpieczeństwa
– zbudowanie systemu, który funkcjonuje w warunkach defektu w przewidywalny sposób i z określoną niezawodnością przez cały cykl życia maszyny.

Obecnie dostępnych jest wiele opracowań dotyczących odporności systemów sterowania na defekty. Są to jednak prace ukierunkowane na problematykę odnoszącą się do systemów o dużej złożoności, działających w warunkach występowania znacznego ryzyka związanego z możliwością śmierci dużej grupy osób lub katastrofy przemysłowej. Ogólne zasady bezpieczeństwa funkcjonalnego systemów technicznych o dużym poziomie zagrożenia omówił Kosmowski (2006). W Polsce badania w tym zakresie prowadzone są np. w Głównym Instytucie Górnictwa. Problematykę bezpieczeństwa funkcjonalnego systemów przeznaczonych do pracy w atmosferze wybuchowej, a zwłaszcza w górnictwie, przedstawili Lebecki i Rosmus (2007a, 2007b). Kwestie bezpieczeństwa funkcjonalnego w sektorze przemysłu procesowego omawiał Markowski (2006), a tematykę bezpieczeństwa funkcjonalnego zintegrowanych systemów wytwarzania podjął także Missala (2010). Niniejsze opracowanie jest poświęcone bezpieczeństwu funkcjonalnemu systemów sterowania maszynami, a zwłaszcza działaniom podejmowanym przez ich projektantów.



Rys. 1.1. Wzajemna korelacja tematyki opracowania i różnych aspektów projektowania systemów bezpieczeństwa do maszyn

Założenia funkcjonalne do systemów bezpieczeństwa powinny być formułowane na podstawie identyfikacji zagrożeń występujących przy maszynie. Natomiast wymagania dotyczące pewności realizacji tych funkcji są uzależnione od poziomu ryzyka, które należy redukować. Niniejsze opracowanie dotyczy zarówno problematyki wspomagania formułowania założeń funkcjonalnych, jak i kwestii określania wymaganej pewności realizacji funkcji bezpieczeństwa, a następnie jej zapewnienia w procesie projektowania systemu. Korelację tematyki tego opracowania i różnych aspektów projektowania systemów bezpieczeństwa do maszyn pokazano na rys. 1.1.

1.2. Wykorzystanie systemów sterowania w procesie redukcji ryzyka

Podstawową definicję maszyny podano w dyrektywie maszynowej 2006/42/WE. Mówi ona, że maszyną jest:

a) zespół wyposażony lub który można wyposażyć w mechanizm napędowy inny niż bezpośrednio wykorzystujący siłę mięśni ludzkich lub zwierzęcych, składający się ze sprzężonych części lub elementów, z których przynajmniej jedna jest ruchoma, połączonych w całość mającą konkretne zastosowanie,

b) zespół, o którym mowa w lit. a, bez elementów przeznaczonych do jego podłączenia w miejscu pracy lub do podłączenia do źródeł energii i napędu,

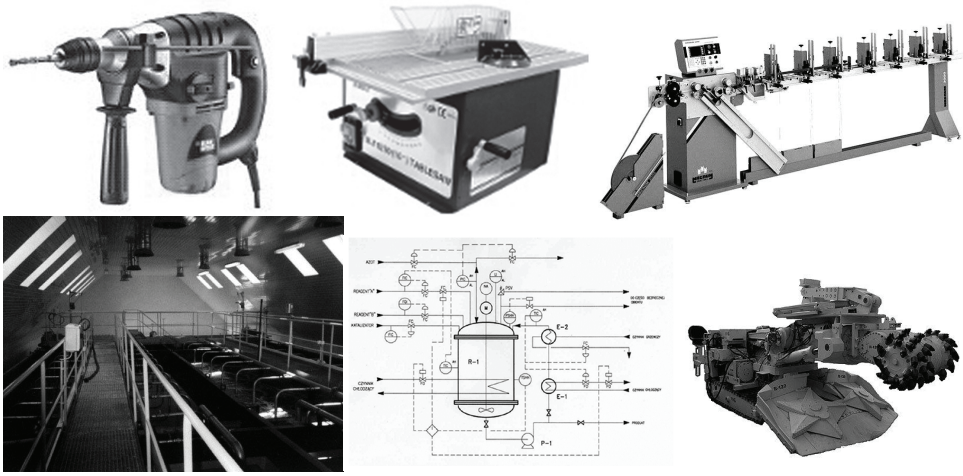
c) zespół, o którym mowa w lit. a i b, gotowy do zainstalowania i zdolny do funkcjonowania jedynie po zamontowaniu na środkach transportu lub zainstalowaniu w budynku lub na konstrukcji,

d) zespoły maszyn, o których mowa w lit. a – c, lub maszyny nieukończone, które w celu osiągnięcia określonego efektu końcowego zostały zestawione i są sterowane w taki sposób, że działają jako zintegrowana całość,

e) zespół sprzężonych części lub elementów, z których przynajmniej jeden jest ruchomy, połączonych w całość, przeznaczony do podnoszenia ładunków, którego jedynym źródłem mocy jest bezpośrednie wykorzystanie siły mięśni ludzkich.

Definicja ta obejmuje bardzo szeroką gamę urządzeń, poczynając od najprostszych elektronarzędzi, po złożone zautomatyzowane systemy wytwórcze. Na rys. 1.2 pokazano wybrane przykłady maszyn:

– elektronarzędzie
– pilarkę stołową
– automat montażowy
– zespół maszyn oczyszczających ścieki
– mieszalnik substancji niebezpiecznych w procesie chemicznym
– kombajn chodnikowy.



Rys. 1.2. Przykłady maszyn

Przykłady te pokazują, jak wielka jest różnorodność maszyn i jak bardzo zróżnicowana może być ich konstrukcja. Dotyczy to także systemów sterowania tymi maszynami. W przypadku elektronarzędzia system sterowania składa się z kilku elementów elektromechanicznych. Pilarka stołowa i automat montażowy są sterowane z użyciem sterowników PLC (sterowniki programowalne). Natomiast systemy sterowania zespołem maszyn lub złożoną maszyną, jaką jest kombajn chodnikowy, to są komputery o dużej mocy obliczeniowej. Projektant maszyny, bez względu na jej złożoność, zawsze powinien zapewnić, że będzie ona przystosowana do obsługi bez stwarzania zagrożeń dla operatora.

Ogólna strategia zmniejszania ryzyka przy obsłudze maszyn jest przedstawiona w normie PN-EN ISO 12100:2011. Strategia ta zakłada, że zagrożenie istniejące w maszynie prędzej lub później spowoduje powstanie szkody, jeżeli nie zostanie zastosowany odpowiedni środek bezpieczeństwa. Środki bezpieczeństwa są kombinacją środków zastosowanych przez projektanta i użytkownika, przy czym środki wprowadzone na etapie projektowania uważa się za bardziej skuteczne od tych, które wprowadza użytkownik.

Projektant maszyny, przystępując do opracowania projektu, powinien zapoznać się z doświadczeniami użytkowników podobnych maszyn i – jeśli to możliwe – uzyskać opinie potencjalnych użytkowników nowego projektu, a następnie podjąć działania w następującej kolejności:

– określić ograniczenia i użytkowanie zgodne z przeznaczeniem
– zidentyfikować zagrożenia i związane z nimi sytuacje zagrożenia
– oszacować ryzyko dla każdego zidentyfikowanego zagrożenia i sytuacji zagrożenia

– ocenić ryzyko i podjąć decyzję, czy jest potrzebne jego zmniejszenie
– wyeliminować zagrożenie lub zmniejszyć ryzyko związane z zagrożeniem, stosując odpowiednie środki bezpieczeństwa.

Działania te wpisują się w iteracyjny proces oceny i redukcji ryzyka. Po wyeliminowaniu zagrożenia, np. przez zmianę technologii wytwarzania, należy spróbować ponownie zidentyfikować zagrożenia i związane z nimi sytuacje zagrożenia, aby się przekonać, że działania eliminujące jeden rodzaj zagrożenia nie stały się przyczyną wystąpienia innych zagrożeń. Po zastosowaniu środka bezpieczeństwa należy ponownie ocenić ryzyko związane z daną sytuacją zagrożenia i sprawdzić, czy zostało ono obniżone do poziomu społecznie akceptowalnego. Jeżeli ten poziom nie został osiągnięty, to należy zadecydować o zastosowaniu dodatkowych środków bezpieczeństwa lub zmianie dotychczas proponowanych rozwiązań na inne. W każdym z tych przypadków należy dokonywać ponownej oceny ryzyka i powtarzać te kroki iteracyjnie z możliwie najlepszym wykorzystaniem dostępnej techniki aż do momentu, gdy dla wszystkich zidentyfikowanych zagrożeń i sytuacji zagrożenia zostaną znalezione rozwiązania obniżające ryzyko do akceptowalnego poziomu.

Należy zauważyć, że społecznie akceptowalny poziom ryzyka wynika z jednej strony ze społecznych oczekiwań co do warunków wykonywania pracy, a z drugiej z możliwości technicznych i organizacyjnych oraz kosztów wprowadzania nowych lub bardziej zaawansowanych i złożonych środków bezpieczeństwa. Społecznie akceptowalny poziom ryzyka systematycznie ulega obniżeniu, co prowadzi do tworzenia coraz bezpieczniejszego środowiska pracy. Jest to możliwe w wyniku stale dokonującego się postępu technicznego i wprowadzania nowych metod organizacji pracy.

W iteracyjnym procesie zapewniania bezpieczeństwa użytkowania maszyny przy wyborze odpowiednich środków bezpieczeństwa konieczne jest zachowanie następującej kolejności osiągania celów:

– bezpieczeństwo użytkowania maszyny we wszystkich fazach jej życia
– zdolność maszyny do realizacji swoich funkcji
– użyteczność maszyny w procesach wytwórczych
– koszty wykonania, eksploatacji i demontażu (złomowania) maszyny.

Aby zapewnić trwałe bezpieczeństwo użytkowania maszyny, ważne jest zastosowanie środków bezpieczeństwa, które nie utrudniają i nie przeszkadzają w użytkowaniu maszyny zgodnie z jej przeznaczeniem.

Wykorzystanie środków bezpieczeństwa opartych na metodach sterowania jest jedną z kilku podstawowych możliwości zapewnienia bezpieczeństwa użytkowania maszyny, choć nie priorytetową (Dźwiarek, Strawiński, 2008). W pierwszej kolejności należy – poprzez zastosowanie rozwiązań konstrukcyjnych bezpiecznych samych w sobie – maksymalnie zredukować liczbę występujących zagrożeń i sytuacji zagrożenia. Następnie trzeba ograniczyć przebywanie osób w strefach zagrożenia

lub sięganie do tych stref w możliwie największym, racjonalnie uzasadnionym stopniu. Można to osiągnąć przez stosowanie odpowiednio skutecznych, stałych obudów, osłon lub przegród, mechanizację i automatyzację czynności produkcyjnych oraz umieszczanie stanowisk sterowania w odpowiednim oddaleniu od stref zagrożenia. Dopiero po wyczerpaniu tych możliwości należy sięgnąć po inne środki bezpieczeństwa, w tym oparte na metodach sterowania.

Środki bezpieczeństwa oparte na metodach sterowania zastosowane jako wyposażenie maszyny, realizujące zaplanowane funkcje bezpieczeństwa, są stosowane w trzech podstawowych grupach zagrożeń:

- wynikających z niewłaściwego zadziałania maszyny związanego z jej podstawowymi cechami i funkcjami
- wynikających z zastosowania procesów technologicznych, których parametry fizyczne istotnie odbiegają od normalnych warunków środowiskowych
- mechanicznych.

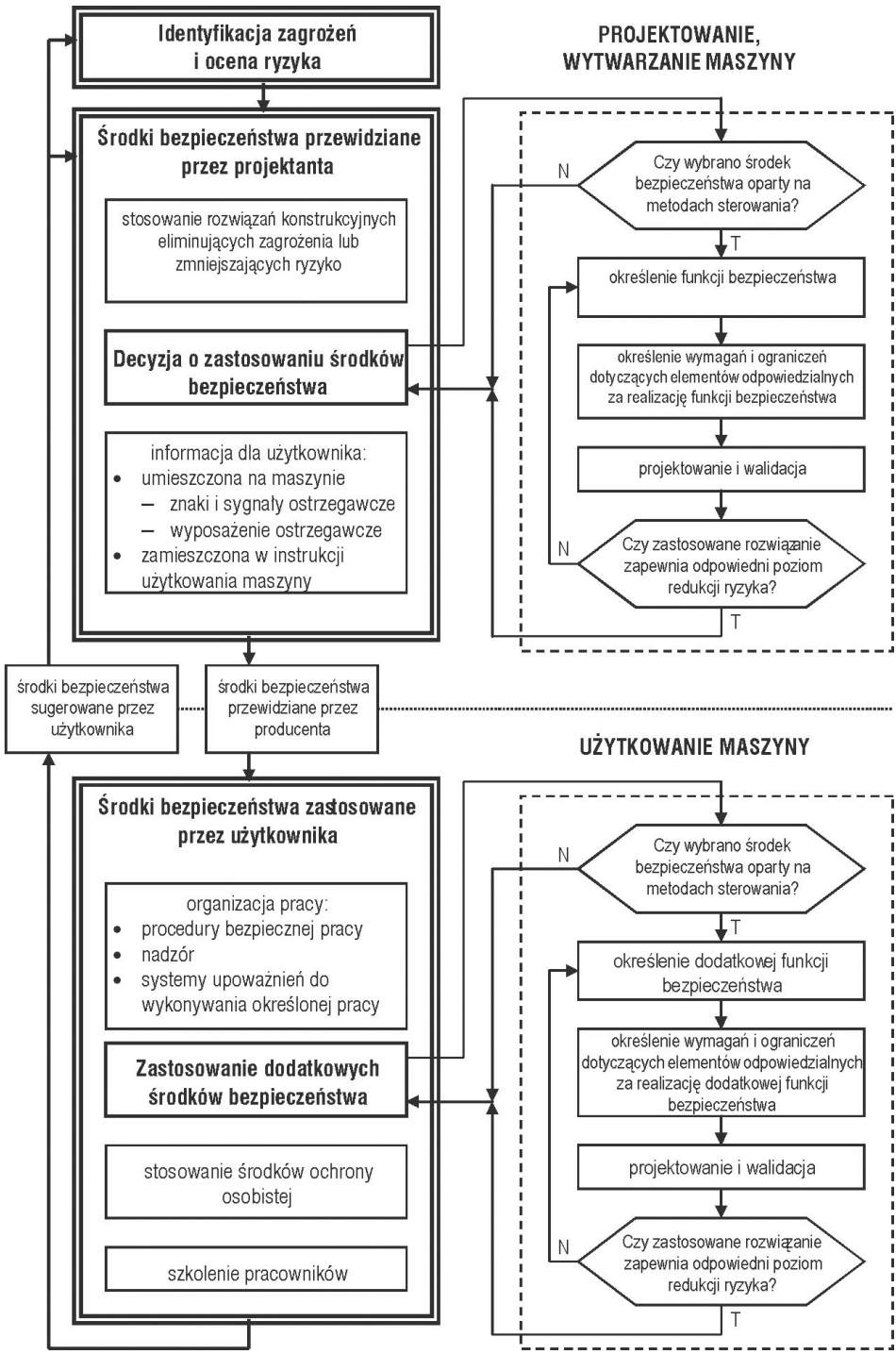
Zagrożenia wynikające z niewłaściwego zadziałania maszyny związanego z jej podstawowymi cechami i funkcjami, dotyczą takich sytuacji, jak: normalne uruchamianie i zatrzymywanie maszyny, jej poszczególnych napędów i funkcji roboczych, nieoczekiwane uruchomienie, zanik i powrót zasilania, zmiana parametrów technologicznych (np. prędkości, przyspieszenia, opóźnienia, kierunku ruchu, ciśnienia, temperatury, itp.), błędna sekwencja działań spowodowana przez operatora lub defekty układów logicznych, procesy związane z rozładowywaniem zmagazynowanej energii, itp. Zagrożenia te są integralne z układem sterowania maszyny, co wynika z faktu, że każda maszyna musi być zasilana energią oraz sterowana, co najmniej w zakresie jej uruchamiania i zatrzymywania. Ograniczanie ryzyka związanego z tymi zagrożeniami jest najbardziej skuteczne wówczas, gdy odpowiednie rozwiązania zostaną zastosowane bezpośrednio w układzie sterowania.

Normalne warunki środowiskowe w potocznym rozumieniu oznaczają warunki fizyczne akceptowane przez organizm człowieka i niestanowiące dla niego zagrożenia w dowolnie długim okresie ekspozycji na nie. Zastosowanie procesów technologicznych o parametrach fizycznych istotnie odbiegających od normalnych warunków środowiskowych powoduje powstanie zagrożeń związanych z możliwością nadmiernej ekspozycji pracowników na czynniki fizyczne o wartościach spoza dopuszczalnych zakresów. Dotyczy to procesów odbywających się w wysokiej lub bardzo niskiej temperaturze, w warunkach dużej wilgotności, pod wysokim ciśnieniem, w silnym polu magnetycznym lub elektrostatycznym, z użyciem substancji toksycznych, łatwo palnych i wybuchowych, w warunkach występowania promieniowania elektromagnetycznego: mikrofalowego, ultrafioletowego, laserowego, rentgenowskiego, jonizującego itp., a także hałasu i drgań. Ryzyko związane z tymi zagrożeniami, jeśli nie można ich wyeliminować przez zmianę technologii, jest ograniczane przez zastosowanie odpowiednio skutecznych

i wytrzymałych przegród, osłon, zbiorników, ekranów, urządzeń wyciągowych i podobnych rozwiązań technicznych. Środki te mogą zapewnić dostateczną redukcję ryzyka, pod warunkiem, że ze względu na charakter procesu technologicznego nie ma możliwości przekroczenia parametrów skuteczności i wytrzymałości zastosowanych środków bezpieczeństwa przez możliwe do wystąpienia poziomy zagrażających czynników fizycznych. W przeciwnym wypadku, w celu ograniczenia ryzyka, niezbędne jest monitorowanie poziomu zagrażających czynników fizycznych i automatyczne podejmowanie działań ograniczających ryzyko. Środki bezpieczeństwa oparte na metodach sterowania są wówczas bardzo użyteczne. Ich zastosowanie wiąże się z wykorzystaniem różnego rodzaju czujników pomiarowych wielkości fizycznych, z opracowaniem technicznych metod ograniczania wzrostu poziomu zagrażających czynników fizycznych i zastosowaniem w maszynie odpowiednich urządzeń wykonawczych. Powszechnie stosowanym rozwiązaniem tego rodzaju jest automatyczny, ciśnieniowy zawór nadmiarowy (zawór bezpieczeństwa) występujący w wielu instalacjach przemysłowych, a także w urządzeniach domowego użytku.

Zagrożenia mechaniczne występują praktycznie we wszystkich maszynach, ich występowanie jest bowiem związane z zastosowaniem napędów oraz części ruchomych i zasadniczo dotyczą ograniczonych przestrzennie stref ruchu tych elementów. Strefami występowania zagrożeń mechanicznych w maszynach są: przestrzenie przy napędach i elementach przeniesienia napędu (silniki, przekładnie pasowe, zębate, łańcuchowe, wały napędowe, układy korbowe, siłowniki pneumatyczne i hydrauliczne, itp.), strefy robocze obrabiarek (toczenia, frezowania, wiercenia, szlifowania, dłutowania, itp.), zamykania form we wtryskarkach, obróbki plastycznej materiałów (mieszanie, walcowanie, zgniatanie, tłoczenie) i inne strefy ruchu mechanizmów. Skuteczne ograniczenie ryzyka związanego z tymi zagrożeniami można zapewnić przez zastosowanie odpowiednich obudów i osłon, odgradzających od stref zagrożenia i zapobiegających dostępowi do nich. Jednak tam, gdzie jest wymagany okresowy lub nawet bardzo częsty dostęp do stref zagrożenia, związany z potrzebą umieszczania przetwarzanych przedmiotów i materiałów oraz wykonywania czynności produkcyjnych, konserwacyjnych i naprawczych, tego typu środki bezpieczeństwa uniemożliwiałyby osiągnięcie celów wytwórczych. Rozwiązaniem jest zastosowanie środków bezpieczeństwa związanych ze sterowaniem, w których wykorzystywane są urządzenia ochronne.

Stan bezpieczeństwa w przypadku zagrożeń mechanicznych jest osiągany po zatrzymaniu ruchów maszyny stwarzających zagrożenie. Urządzenia ochronne umożliwiają stwierdzenie naruszenia (wkroczenia, wniknięcia do) strefy zagrożenia przez człowieka lub część jego ciała, lub jego obecność w takiej strefie, a wytworzony przez nie sygnał może być wykorzystany do zatrzymania maszyny (jej niebezpiecznych ruchów) lub do blokowania możliwości jej uruchomienia.



Rys. 1.3. Schemat procesu redukcji ryzyka związanego z użytkowaniem maszyny z uwzględnieniem stosowania środków bezpieczeństwa opartych na metodach sterowania

Zastosowanie środków bezpieczeństwa opartych na metodach sterowania jest elementem procesu redukcji ryzyka związanego z użytkowaniem maszyny, który obowiązuje projektanta i użytkownika. Proces ten schematycznie przedstawiono na rys. 1.3 (Dźwiarek, 2008b). Na przedstawionym schemacie możliwość zastosowania środków bezpieczeństwa opartych na metodach sterowania występuje dwukrotnie: w fazie projektowania maszyny oraz w fazie jej użytkowania. Ta druga możliwość jest związana z tym, że na etapie projektowania nie zawsze można przewidzieć wszystkie okoliczności związane z użytkowaniem maszyny. Dotyczy ona także sytuacji modernizacji lub przebudowy maszyny. Jeżeli ocena ryzyka przeprowadzona u użytkownika po zainstalowaniu maszyny wykaże potrzebę zastosowania dodatkowych środków bezpieczeństwa, to również należy rozważyć zastosowanie środków związanych ze sterowaniem. W obu przypadkach obowiązuje procedura projektowania i walidacji, w wyniku której zostanie potwierdzony oczekiwany poziom redukcji ryzyka.

Metody sterowania mogą również pośrednio wspomagać ograniczanie ryzyka związanego z innymi zagrożeniami, np. ergonomicznymi, poprzez automatyzację czynności produkcyjnych, usprawnianie i upraszczanie obsługi, wspomaganie czynności operatorskich lub związanych ze statecznością maszyn mobilnych przez blokowanie ruchów, które mogą doprowadzić do wywrócenia. Zadaniem układów sterowania jest również przekazywanie operatorowi informacji mających wpływ na bezpieczeństwo, takich jak: informacje o stanie maszyny, o wykrytych uszkodzeniach i nieprawidłowościach działania, podpowiedzi co do kolejnych operacji technologicznych, sygnalizowanie konieczności wykonania okresowych przeglądów, konserwacji, wymiany narzędzi itp.

Środki bezpieczeństwa związane ze sterowaniem w znacznej części opierają się na wykorzystaniu czujników pomiarowych parametrów czynników fizycznych oraz urządzeń ochronnych przeznaczonych do wykrywania człowieka lub części jego ciała w określonych strefach wykrywania. Istotne jest, aby w warunkach środowiskowych towarzyszących użytkowaniu maszyny czujniki pomiarowe i urządzenia ochronne mogły poprawnie funkcjonować i nie ulegały defektom. W tych zastosowaniach ważne jest również, aby istniała możliwość doprowadzenia maszyny do stanu bezpieczeństwa (zatrzymania jej, zmniejszenia wartości parametru czynnika fizycznego) w czasie krótszym niż możliwość powstania szkody. Oba te aspekty mają decydujący wpływ na możliwość realizacji funkcji bezpieczeństwa, dlatego decyzja o wyborze środka bezpieczeństwa związanego z metodami sterowania powinna być uzupełniona odpowiednimi analizami projektowymi.

Ponieważ podstawowym celem funkcji bezpieczeństwa jest redukcja ryzyka, więc jej uszkodzenie oznacza, że ryzyko przestaje być redukowane. Dlatego też funkcje bezpieczeństwa definiuje się jako te funkcje maszyny, których wadliwa realizacja może bezpośrednio spowodować wzrost ryzyka.

Przykładami funkcji bezpieczeństwa są więc:
- związana z bezpieczeństwem funkcja zatrzymania inicjowana przez techniczne środki ochrony
- ręczne przywracanie funkcji – ręczne resetowanie
- start i start ponowny – start i restart
- funkcja lokalnego sterowania
- funkcja automatycznego zawieszenia – muting
- sterowanie podtrzymywaniem ruchu
- sterowanie zezwalające
- zapobieganie nieoczekiwanemu uruchomieniu
- funkcja izolowania i rozpraszania energii
- wybór trybu sterowania
- monitorowanie parametrów związanych z bezpieczeństwem
- funkcja awaryjnego zatrzymania
- wskazywanie i ostrzeganie.

1.3. Formułowanie założeń funkcjonalnych

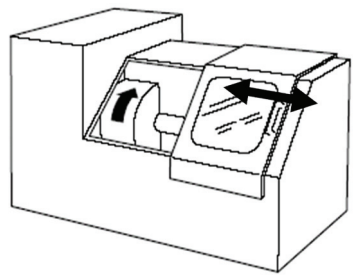
Funkcja bezpieczeństwa z założenia jest przewidziana do zapobiegania zdarzeniom niebezpiecznym związanym z występującymi przy maszynie zagrożeniami. Podstawą do sformułowania założeń funkcjonalnych jest identyfikacja zagrożeń. Zidentyfikowane zagrożenia, którym ze względów technologicznych nie można było zapobiec przez zastosowanie barier lub osłon, powinny być przeanalizowane z uwzględnieniem tych faz życia maszyny, w których one występują, a więc podczas rozruchu maszyny, jej normalnej obsługi, wyłączania, a także okresowych konserwacji oraz napraw. Przy formułowaniu wymagań funkcjonalnych należy określić sposób działania funkcji bezpieczeństwa w każdym z przewidywalnych zdarzeń. Należy uwzględnić co najmniej:
- działanie maszyny, w tym:
  - użytkowanie zgodne z przeznaczeniem (włączając w to przewidywalne niewłaściwe użycie)
  - rodzaje pracy maszyny (np. sterowanie ręczne, sterowanie automatyczne, sterowanie częścią maszyny)
  - czas cyklu pracy
  - czas zadziałania
- działanie awaryjne
- wzajemne oddziaływanie różnych procesów i działań (naprawy, regulacje itp.)

– działanie maszyny, któremu ma zapobiegać funkcja bezpieczeństwa
– warunki (np. rodzaj pracy), w których funkcja bezpieczeństwa powinna być aktywna i te, w których powinna być wyłączona
– kolejność priorytetów funkcji, które mogą zadziałać jednocześnie.

Przy formułowaniu założeń funkcjonalnych pomocne może być posługiwanie się normami określającymi podstawowe wymagania dotyczące działania funkcji bezpieczeństwa.

Przykład

Rozważmy problem dostępu do wirującego narzędzia w obrabiarce pokazanej na rys. 1.4. Identyfikacja zagrożeń wskazała, że występuje zagrożenie zranieniem podczas dostępu do strefy obróbki. Ze względów technologicznych nie jest możliwe zastosowanie rozwiązania wewnętrznie bezpiecznego (podczas obróbki narzędzie musi obracać się z dużą prędkością). Nie jest także możliwe zastosowanie osłony stałej – konieczny jest dostęp technologiczny w celu odbioru obrobionego elementu i dostarczenia kolejnej próbki materiału. Oznacza to konieczność zastosowania funkcji bezpieczeństwa polegającej na kontroli zamknięcia osłony. Identyfikacja zagrożenia wskazuje, że:



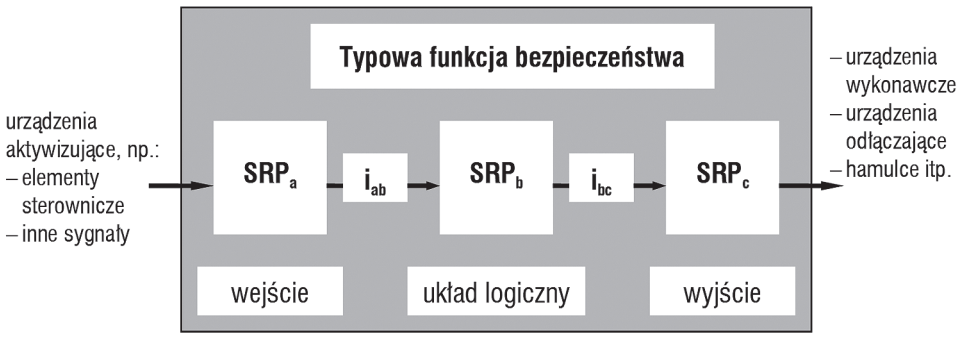
Rys. 1.4. Przykład funkcji bezpieczeństwa realizującej kontrolę dostępu do wirującego narzędzia (PN-EN 62061:2008)

– w razie otwarcia osłony system sterowania powinien zatrzymać ruch niebezpieczny w czasie krótszym niż wystarczający do dosięgnięcia do wirującego narzędzia (funkcja zatrzymywania inicjowana przez urządzenie ochronne; należy spełnić wymagania PN-EN ISO 13849-1:2008 p. 5.2.1, PN-EN ISO 12100:2011 p. 3.27.4 i 6.2.11.3, PN-EN 60204-1:2010 p. 9.2.2, 9.2.5.3, 9.2.5.5.)
– gdy osłona jest otwarta, nie powinno być możliwe włączenie ruchu niebezpiecznego (blokada uruchomienia; należy spełnić wymagania PN-EN ISO 12100:2011 p. 3.27.4 i 6.2.11.1, PN-EN 61496-1:2007/AC:2011 zał. A5)
– zamknięcie osłony nie powinno spowodować włączenia ruchu niebezpiecznego (blokada ponownego uruchomienia, należy spełnić wymagania PN-EN ISO 12100:2011 p. 6.2.1.11, PN-EN 61496-1:2007/AC:2011. zał. A6)
– w przypadku konserwacji i napraw powinno być możliwe włączenie ruchu niebezpiecznego przy otwartej osłonie, ale z ograniczoną prędkością (należy spełnić wymagania PN-EN ISO 13849-1:2010 p. 4.6.4, PN-EN ISO 12100:2011 p. 6.2.11.8 i 6.2.11.10, PN-EN 60204-1:2010, p. 9.2.3, 9.2.4).

Tak sformułowane założenia funkcjonalne powinny umożliwić projektantowi zaprojektowanie systemu, który będzie tę funkcję realizował. Jednocześnie działanie funkcji zapewni ograniczenie zagrożenia podczas przewidywanych rodzajów pracy obrabiarki.

1.4. Elementy systemów sterowania związane z bezpieczeństwem

Elementy układu sterowania biorące udział w realizacji co najmniej jednej funkcji bezpieczeństwa są zaliczane do elementów systemu sterowania związanych z bezpieczeństwem. Mogą być wykonane w różnych technikach realizacji i mogą funkcjonować z wykorzystaniem różnych rodzajów energii (układy mechaniczne, pneumatyczne, hydrauliczne oraz elektryczne, elektroniczne, programowalne elektroniczne). W strukturze systemu sterowania wyróżnia się: czujniki, układy logiczne i elementy wykonawcze (rys. 1.5).



Rys. 1.5. Ogólna struktura systemu sterowania realizującego funkcję bezpieczeństwa; SRP – element systemu sterowania związany z bezpieczeństwem (ang. *safety-related part of control system*), i – interfejs

Elementami pełniącymi funkcję czujników (źródeł sygnałów o bezpieczeństwie) w systemie sterowania są:

- urządzenia ochronne wykrywające (elektroczułe i czułe na nacisk)
- urządzenia blokujące (związane z osłonami)
- urządzenia sterowania oburęcznego (służące do inicjowania niebezpiecznych ruchów maszyny)
- urządzenia zatrzymywania awaryjnego
- czujniki parametrów zasilania
- czujniki parametrów fizycznych
- czujniki (łączniki) krańcowe

- czujniki prędkości zerowej
- elementy sterownicze służące do uruchamiania, zatrzymywania, wyboru trybu pracy, ręcznego znoszenia (resetowania) funkcji blokowania.

Układy logiczne mogą być zrealizowane z wykorzystaniem przekaźników, logicznych modułów półprzewodnikowych i modułów programowalnych typu PLC lub z wykorzystaniem pneumatycznych albo hydraulicznych bloków logicznych, bloków przełączających i zaworów zwrotnych. Układami wykonawczymi mogą być styczniki do włączania/wyłączania (lub sterowania) odbiorników mocy, elektrozawory, siłowniki.

Najczęściej system sterowania maszyny realizuje zarówno funkcje bezpieczeństwa, jak i funkcje nieistotne dla bezpieczeństwa. Ze względu na bezpieczeństwo zdecydowanie najkorzystniejsze jest rozwiązanie, w którym urządzenia realizujące funkcje ochronne są, w miarę możliwości w jak największym stopniu, wydzielone z całego systemu i połączone z urządzeniami roboczymi w sposób niezależny od układów realizujących funkcje sterujące. Zazwyczaj dzięki temu urządzenia odpowiedzialne za bezpieczeństwo są mniejsze i mniej złożone. Uzyskuje się także bardziej logiczną strukturę SRP. Wielkość, złożoność i struktura mają istotne znaczenie szczególnie w procesie walidacji urządzeń, a także wpływają na koszty i skuteczność uzyskania wymaganej kategorii bezpieczeństwa. Elementy systemu sterowania realizujące funkcje bezpieczeństwa są nazywane związanymi z bezpieczeństwem elementami systemu sterowania. Niniejsze opracowanie jest poświęcone wprowadzeniu w tematykę projektowania tych elementów systemów sterowania maszynami, które są odpowiedzialne za realizację funkcji bezpieczeństwa.

Rozdział 2

Badania wypadków przy maszynach spowodowanych niesprawnością ich systemu sterowania

2.1. Wprowadzenie

Rozwój technik komputerowych spowodował, że wśród wielu przyczyn wypadków przy pracy coraz większe znaczenie mają te spowodowane przez nieprzewidziane zadziałanie systemu sterowania maszyną (Kim i in., 2005). Niewłaściwe zadziałanie systemu sterowania powoduje, że maszyna zachowuje się w sposób niepożądany. Zachowanie to może polegać na przykład na zmianie parametrów ruchu roboczego czy też na niewłaściwym sygnalizowaniu stanu pracy maszyny. Efekty te prowadzą do niedotrzymania reżimów jakości produkcji lub wykonywania elementów wybrakowanych, co wiąże się z dodatkowymi kosztami produkcji. Badania prowadzone przez autora (Dźwiarek, 2000a, 2000b) wykazały, że znacznie groźniejsze jest wykonywanie przez maszynę nieprzewidzianych ruchów czy niezamierzona zmiana prędkości, nagłe uruchomienie lub niezatrzymanie ruchu w przewidzianym czasie, wyrzucanie ruchomych części lub obrabianych przedmiotów itp. Zjawiska takie występują, gdy nieprawidłowości w funkcjonowaniu systemu sterowania powodują utratę funkcji bezpieczeństwa odpowiedzialnej za zapobieganie im. Efektem takiego zachowania maszyny może być wypadek przy pracy, co wiąże się ze znacznie poważniejszymi skutkami prowadzącymi do utraty zdrowia, a nawet życia operatora. Przeciwdziałanie wypadkom może być skuteczne jedynie wówczas, gdy zjawiska, jakie do nich prowadzą, zostaną dokładnie zbadane. W tym celu należy przeprowadzić szczegółowe analizy zaistniałych wypadków.

Zazwyczaj statystyczne bazy danych o wypadkach zawierają informacje klasyfikowane według zawodów, miejsc pracy, wykonywanych czynności itp. Natomiast nie ma analiz bardziej szczegółowych – takich, które w razie wypadku związanego z funkcjonowaniem systemu sterowania maszyną, wskazywałyby na jego podstawowe przyczyny i które można by wykorzystać do sformułowania zasad zapobiegania

podobnym wypadkom w przyszłości. Dotyczy to zwłaszcza informacji wskazujących na rozwiązania techniczne, które mogłyby wypadkom zapobiec.

W dostępnej literaturze bardzo mało jest publikacji dotyczących analiz wypadków spowodowanych niesprawnością systemu sterowania maszynami. Backström i Harms-Ringdahl (1984) przedstawili wyniki badań prowadzonych w bardzo ograniczonej skali. Także Belisle i Laurin (1999), Edwards (2001) i Malm (2001) podali jedynie przykłady pojedynczych wypadków. Pewne informacje można znaleźć także w ogólnych opracowaniach dotyczących analiz wypadków przy pracy, (np.: Gould, 2000; Hale, Hale, 1971; Koornneef, Hale, 1995; MaTSU, 2000). Jednak autorzy tych prac informują jedynie, że wypadki takie zdarzają się i stanowią określony procent wszystkich wypadków przy pracy. Natomiast Henderson i in. (2000) omawiają, jako studium przypadku, kilka wypadków spowodowanych uszkodzeniem systemu sterowania lub niewłaściwą implementacją funkcji bezpieczeństwa. Przeprowadzone analizy wypadków wskazywały wprawdzie, że wystąpiły nieprawidłowości w działaniu systemu sterowania maszyny, ale nie wskazywały, na czym polegała wada konstrukcyjna. Nie były analizowane rozwiązania zastosowane przez konstruktorów. Wnioski sprowadzały się do sformułowania zaleceń dotyczących unikania podobnych sytuacji w przyszłości przez odpowiednią organizację pracy. Także analizy prowadzone przez Charpentiera (2005) przedstawiają jedynie ogólną informację statystyczną o wypadkach, które wydarzyły się we Francji. Jak dotychczas najbardziej ogólne były badania zaprezentowane przez Dźwiarka (2004a).

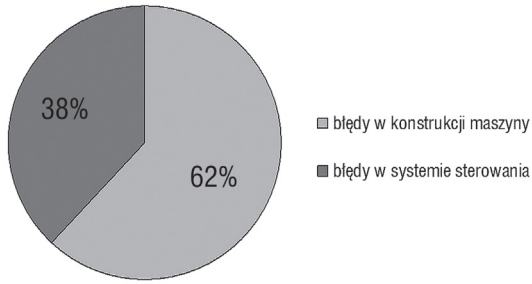
2.2. Wyniki prowadzonych badań wypadków

Wyniki analiz przedstawione przez Dźwiarka (2004a) dotyczyły danych o ok. 700 wypadkach, które odnotowano w latach 1996-2002, spowodowanych różnymi przyczynami. Dane pochodziły zarówno od korespondentów, jak i z rozesłanej ankiety. Ponieważ sieć korespondentów obejmuje głównie duże zakłady przemysłowe, więc dostarczone przez nich informacje dotyczyły przeważnie wypadków, które wydarzyły się w takich właśnie zakładach. Na ankietę odpowiedziały w większości zakłady duże i średnie.

Zebrane informacje o wypadkach i wydarzeniach bezurazowych pochodziły z następujących źródeł:

- dane o zdarzeniach potencjalnie wypadkowych zebrane w latach 1998-2002 w jednym z zakładów produkcyjnych
- dane zebrane przez grupę korespondentów z zakładów przemysłowych uczestniczących w realizacji projektu zamawianego
- opisy wybranych wypadków, które wydarzyły się w latach 2001-2002

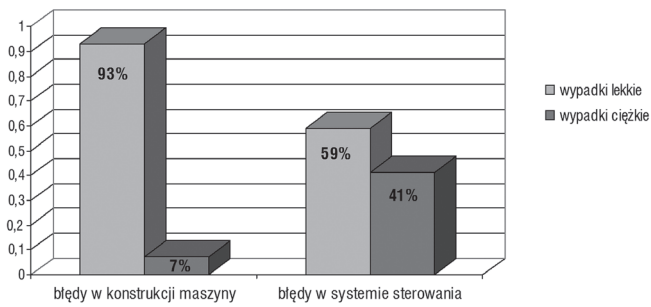
– publikacje PIP prezentujące dane statystyczne o wypadkach mających miejsce w latach 2000-2002.



Rys. 2.1. Wypadki spowodowane niewłaściwym działaniem systemu sterowania w odniesieniu do całej próbki wypadków przy maszynach

Zebrane opisy wypadków zostały pogrupowane według ich przyczyn wskazanych w ankietach i przekazane ekspertom z poszczególnych dziedzin do dalszej szczegółowej analizy. Poprawność wypełnienia ankiety była więc weryfikowana przez ekspertów. W efekcie zidentyfikowano 144 wypadki związane z obsługą maszyn. W tej grupie 54 wypadki były związane z niewłaściwym funkcjonowaniem systemu sterowania maszyną, co stanowi 38% wszystkich wypadków przy maszynach (rys. 2.1). Podczas analiz przyjęto podział ciężkości skutków na:

– lekkie (zwykle odwracalne) urazy: do tej grupy zaliczono wszelkiego typu skaleczenia, zranienia, drobne złamania, stłuczenia itp.
– ciężkie (zwykle nieodwracalne) urazy: do tej grupy zaliczono wszystkie amputacje i śmierć.



Rys. 2.2. Ciężkość skutków wypadków

Wyniki analizy wypadków przy maszynach pod względem ich ciężkości przedstawiono na rys. 2.2. W grupie wypadków spowodowanych niewłaściwym funkcjonowaniem systemu sterowania maszyny znacznie częściej występowały wypadki ciężkie (41%) niż wśród wypadków niezwiązanych z systemem sterowania (7%). Wskazuje to na wagę kwestii związanych z systemami sterowania maszynami.

Następnie wypadki spowodowane przez system sterowania przeanalizowane zostały pod kątem ich przyczyn. Wyniki pokazano na rys. 2.3. Najczęstszą przyczyną jest brak funkcji bezpieczeństwa (58%), takich jak kontrola położenia osłony lub nadzorowanie obecności w strefie niebezpiecznej. Kolejną grupę – 26% wypadków – stanowią te spowodowane uszkodzeniem elementu systemu sterowania związanego z bezpieczeństwem w sytuacji doboru niewłaściwej kategorii systemu sterowania lub niewłaściwej realizacji wymagań kategorii. Pozostałe przyczyny, a więc błędy w określaniu funkcji bezpieczeństwa (założenia do funkcji bezpieczeństwa nie przewidują wszystkich możliwych zdarzeń) stanowią 4%, błędy w oprogramowaniu systemu sterowania – 6% i brak wystarczającej odporności na oddziaływanie środowiska (oddziaływanie klimatyczne, zaburzenia w zasilaniu w energię, zarówno elektryczną jak i pneumatyczną) – 6%. Charakterystyczne jest, że w zdecydowanej większości analizowane wypadki były skutkiem jednoczesnego wystąpienia dwu zdarzeń:

– niewłaściwego zadziałania systemu sterowania

oraz

– nieprawidłowego zachowania operatora.

Nieprawidłowe zachowanie operatora polegało zwykle na:

– niewłaściwej reakcji na nagłe i nietypowe zdarzenia
– stosowaniu procedur pracy niezgodnych z zasadami bezpieczeństwa
– obchodzeniu systemów ochronnych.

Rys. 2.3. Częstość występowania różnych przyczyn wypadków spowodowanych przez nieprawidłowe działanie systemu sterowania

Działania te były zazwyczaj podejmowane spontanicznie, w reakcji na zaistniałą sytuację, ale zdarzały się też działania celowe. Zawsze jednak były one skutkiem nieprawidłowego zadziałania maszyny. Podstawową metodą przeciwdziałania nieprawidłowemu zachowaniu się operatora maszyny jest jego udział w szkoleniach oraz instruktażach poprawnej pracy. Jednak skuteczność takich działań jest ograniczona. Należy stwierdzić, że zastosowanie rozwiązań technicznych (tak jak to

przewidują przepisy i zasady dobrej praktyki inżynierskiej) jest znacznie skuteczniejszym środkiem zapobiegawczym niż poleganie na dobrej organizacji pracy i właściwych zachowaniach operatora maszyny.

2.3. Model wypadku spowodowanego zaburzeniem w realizacji funkcji bezpieczeństwa

2.3.1. Typowe przykłady modeli wypadków

Przedstawione wyniki badań umożliwiły zidentyfikowanie typowych sekwencji zdarzeń prowadzących do wypadku związanego z nieprawidłowym zadziałaniem systemu sterowania maszyną. Dzięki temu możliwe było opracowanie modelu takich wypadków.

Prace badawcze dotyczące formułowania modeli wypadków są prowadzone od wielu lat. Mają one na celu zidentyfikowanie najważniejszych zjawisk, które zachodzą podczas wypadku. Znane dotychczas modele różnią się zarówno poziomem szczegółowości, jak i zakresem zastosowań. Można stwierdzić, że im bardziej uniwersalny jest model, tym mniej szczegółowo analizuje zaistniałe zjawiska.

Najprostszym przykładem jest model zaproponowany przez Heinricha (1959), opracowany jeszcze w latach trzydziestych ubiegłego wieku. Model ten traktuje wypadek jako ciąg kolejno następujących po sobie zdarzeń. Jest więc modelem sekwencyjnym. Stanowił on podstawę do tworzenia wielu bardziej rozbudowanych modeli (Studenski, 1986). Przykładem modelu sekwencyjnego jest model STEP zaproponowany przez Hale i Hale (1971). Podstawową wadą modeli sekwencyjnych jest fakt, że analizują one jedynie zjawiska zachodzące bezpośrednio w trakcie wypadku. Umożliwiają więc wskazanie wszystkich najważniejszych czynników występujących w trakcie zdarzenia, lecz nie uwzględniają przyczyn, które zaistniały wcześniej i trwały jeszcze przed wypadkiem, a w trakcie wypadku umożliwiły wystąpienie wszystkich kolejnych zjawisk. Ponieważ niniejsza praca dotyczy przede wszystkim błędów popełnionych przez konstruktorów maszyn i projektantów stanowisk pracy, więc model sekwencyjny wypadku nie wydawał się najbardziej odpowiedni do analiz, które były prowadzone.

Podobna sytuacja ma miejsce w przypadku analizy metodą drzewa błędów FTA (Harms-Ringdahl, 1993) i drzewa zdarzeń ETA. Wprawdzie przy modelowaniu tymi metodami drzewo można rozwijać na tyle głęboko, na ile to jest konieczne, ale postępowanie takie prowadzi do nadmiernego skomplikowania analizy. Powoduje, że staje się ona bardzo pracochłonna, niewspółmiernie do uzyskanych efektów.

Dużą grupę modeli wypadków stanowią modele oparte na analizach zachowania człowieka w sytuacji stresowej. Przykładem jest model wpływu środowiska społecznego na bezpieczeństwo pracy opracowany przez Studenskiego lub model Smille (Studenski, 1986), model Glendona i Hale'a (Hale, Hale, 1971; Koornneef, Hale, 1995), i wiele innych. Modele te w zbyt małym, jak na potrzeby tego opracowania, zakresie uwzględniają czynnik techniczny, a więc także nie są najbardziej odpowiednie do stosowania w analizie wypadków spowodowanych niewłaściwą realizacją funkcji bezpieczeństwa.

W literaturze dostępne są jeszcze propozycje wielu innych modeli, np.:

- modele wykorzystujące analizę z wykorzystaniem logiki rozmytej
- model TOL
- modele wykorzystujące metodę transferu energii
- drzewo MORT
- model Surry'a i inne.

Wszystkie te modele skupiają się na zjawiskach zachodzących przy maszynie. Podczas ich tworzenia milcząco zakłada się, że główne przyczyny wypadku są generowane w otoczeniu maszyny. Nawet jeśli uwzględnia się fakt ewentualnej jej niesprawności, to i tak szczególnie dokładnie analizuje się działania podjęte przez jej użytkownika w celu zapobieżenia ewentualnym wypadkom w razie nieprawidłowego zadziałania maszyny. Natomiast prawie całkowicie pomija się analizę właściwości samej maszyny, a zwłaszcza nieprawidłowości w konstrukcji jej systemu sterowania. Tak więc modele tej postaci nie są przystosowane do przeprowadzania analiz dotyczących nieprawidłowości w realizacji funkcji bezpieczeństwa jako przyczyny wypadku.

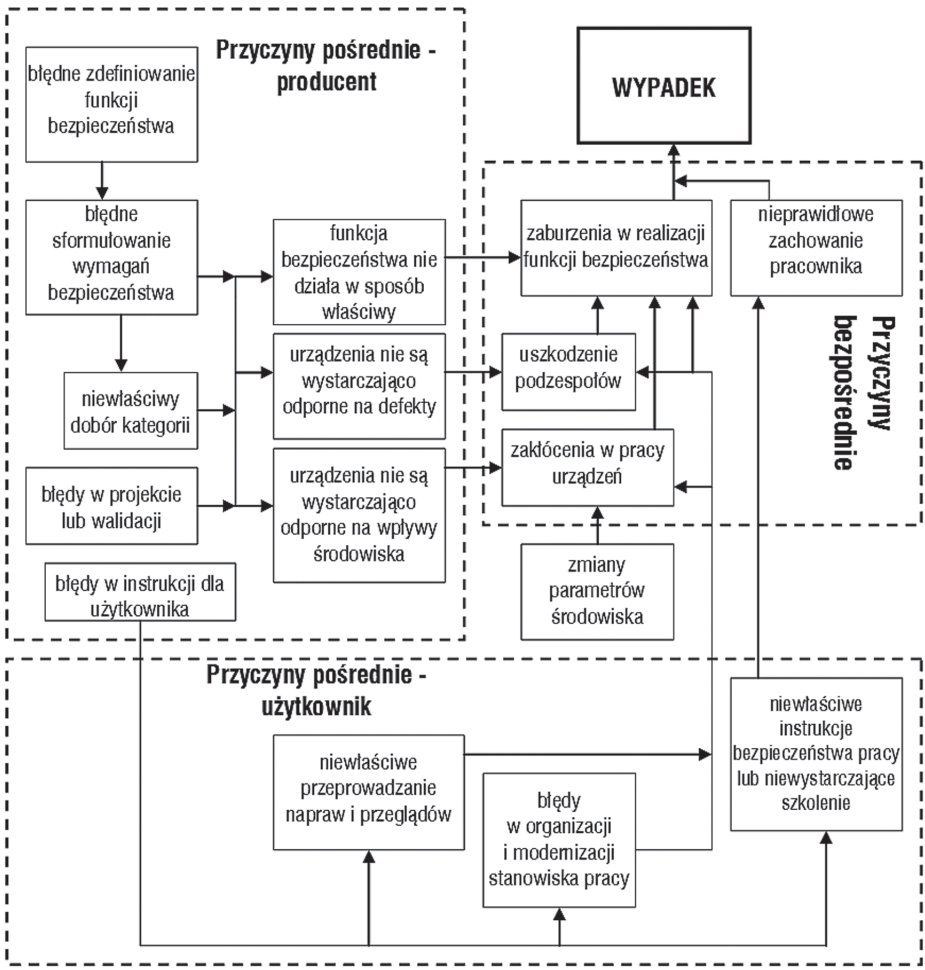
2.3.2. Opracowany model wypadku

Model wypadku spowodowanego zaburzeniami w realizacji funkcji bezpieczeństwa został zaproponowany przez Dźwiarka (2004a) na podstawie wyników analizy wypadków. Przy jego formułowaniu założono, że maszyna powinna być tak zaprojektowana, aby nie powodowała ryzyka nieakceptowanego, a więc w trakcie jej obsługi teoretycznie nie powinny zdarzać się wypadki spowodowane jej właściwościami. Skoro jednak zdarzenia takie mają miejsce, oznacza to, że popełniono jakieś błędy w trakcie projektowania lub użytkowania maszyny. Należy więc zidentyfikować najbardziej typowe, powodujące występowanie zdarzeń wypadkowych, odstępstwa od wymagań bezpieczeństwa. Przeprowadzone analizy wypadków pokazały, że zaburzenia w realizacji funkcji bezpieczeństwa mogą być spowodowane:

- uszkodzeniem elementów systemu sterowania
- zakłóceniami w działaniu maszyny wynikającymi z ekstremalnych oddziaływań środowiska (szczególne znaczenie mają tu zaburzenia napięć zasilających i zakłócenia elektromagnetyczne)

– zachowaniem się operatora niezgodnym z instrukcją obsługi oraz instrukcją bezpieczeństwa pracy, które nie zostało przewidziane przez projektanta funkcji bezpieczeństwa.

Zdarzenia te, zwłaszcza jeśli nastąpi koincydencja kilku z nich jednocześnie, mogą prowadzić do wypadku. Są to więc **przyczyny bezpośrednie wypadku**. Fakt, że zdarzenia takie mogły nastąpić wynika z błędów popełnionych wcześniej przez konstruktora lub użytkownika maszyny. Błędy te nie powodują natychmiastowego zaistnienia wypadku. Maszyna skonstruowana z błędami może przez wiele lat pracować poprawnie i dopiero szczególny zbieg okoliczności spowoduje ujawnienie się ukrytych wad konstrukcyjnych lub organizacyjnych. Są to **przyczyny pośrednie wypadku**.



Rys. 2.4. Model wypadku spowodowanego zaburzeniami w realizacji funkcji bezpieczeństwa

Model wypadku uwzględniający te zjawiska przedstawiono na rys. 2.4. W modelu pokazano, w jaki sposób przyczyny bezpośrednie są skutkiem poszczególnych przyczyn pośrednich. Dzięki temu, poruszając się kolejno od bloku „Wypadek", poprzez kolejne bloki przyczyn bezpośrednich aż do przyczyn pośrednich, można wskazać podstawowe źródła zdarzeń prowadzących do wypadku. Umożliwia to identyfikację wszystkich przyczyn oraz wskazanie najwłaściwszych środków zapobiegawczych.

2.3.3. Przykład zastosowania

Sposób zastosowania opracowanego modelu do prowadzenia analizy przyczyn wypadku zostanie pokazany na przykładzie wypadku, który wydarzył się w jednym z zakładów przemysłowych. W dniu wypadku, ok. godz. 4^{00}, operator zespołu ustawiania usłyszał odgłos drewnianej palety spadającej ze stosu na podajniku. Brak palety na swoim miejscu w ciągu sztaplowania powoduje zatrzymanie całej linii odbioru materiałów. Operator wyłączył podajnik palet, ale nie zatrzymał linii wyłącznikiem awaryjnym i przeszedł na miejsce upadku palety. Wszedł przez drzwi w ogrodzeniu siatki osłaniającej całą linię przed dostępem osób nieupoważnionych. Drzwi mają wyłącznik krańcowy i po ich otwarciu cała linia powinna być zatrzymana. Jak później stwierdzono, w dniu wypadku wyłącznik krańcowy był uszkodzony i nie zadziałał.

W tym czasie poszkodowany odwoził wózkiem widłowym gotowe wyroby na składowisko i ustawiał stosy palet na podajniku łańcuchowym. Ponieważ linia zatrzymała się, poszedł sprawdzić, co się dzieje i zobaczył, że operator przeszedł do ogrodzonego stanowiska podawania palet i usiłuje przenieść paletę na miejsce ułożenia na pomoście sztaplowania znajdującym się ok. 1,5 metra powyżej poziomu posadzki. Chcąc pomóc operatorowi, poszkodowany przeszedł przez barierkę ograniczającą krawędź pomostu. Nie zauważył jednak, że linia sztaplowania jest włączona, a fotokomórki kontrolujące proces działają. Przeciął strumień światła fotokomórek, co komputer odczytał jako sygnał, że paleta jest już na miejscu, i uruchomił układarkę z warstwą pustaków ceramicznych. Poszkodowany nie zdążył się uchylić i sztaplarka przygniotła mu lewą nogę. Operator, widząc to, przebiegł przez pomost, cofnął ręcznym sterowaniem chwytak układający wyroby i powiadomił pogotowie ratunkowe.

Inspektor pracy ustalił następujące przyczyny wypadku:

– wyłącznik krańcowy w drzwiach do ogrodzenia palet był uszkodzony, o czym operator nie wiedział
– operator nie zatrzymał wszystkich urządzeń za pomocą wyłącznika awaryjnego, pomimo że instrukcja stanowiskowa o tym mówi; tłumaczył to

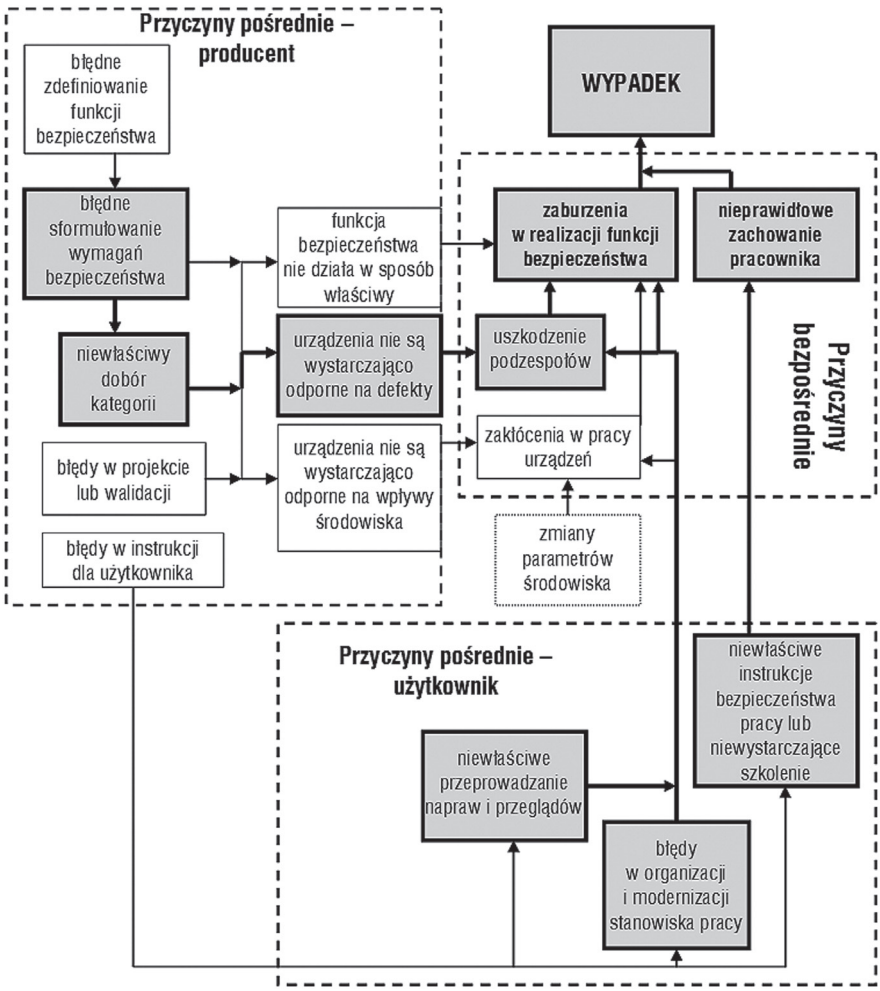
przekonaniem, że wyłącznik krańcowy w drzwiach działa w ten sam sposób, co awaryjny
- nierówno ułożony stos palet – przedostatnia paleta u góry stosu była wysunięta ok. 8 cm od pionu w prawo; układanie stosów palet i ich wyrównywanie jest obowiązkiem operatorów wózków widłowych, w tym poszkodowanego, a do wyrównywania ułożonych palet mają oni przygotowany specjalny pręt metalowy ułatwiający przesuwanie, jednak rozstaw chwytaka umożliwia przesunięcie tylko o 6 cm
- operator, zamiast odrzucić paletę, która spadła, postanowił ją przetransportować ręcznie, drogą, którą przesuwają się materiały
- na pomost sztaplowania pracownicy weszli przez barierkę, zamiast przez bramkę od strony pulpitu, gdzie jest również wyłącznik krańcowy, który w chwili zdarzenia był sprawny
- w czasie rozruchu próbnego okazało się, że fotokomórki zamontowane na linii podawania palet nie zadziałały.

Tak więc opisany wypadek był skutkiem nawarstwienia się wielu nieprawidłowości. W sprawozdaniu inspektora pracy przyczyny bezpośrednie i pośrednie są przemieszane, co utrudnia formułowanie wniosków ogólnych. Lepsze zobrazowanie zjawisk mających miejsce podczas tego wypadku da zastosowanie opracowanego modelu. Zgodnie z tym modelem przyczynami bezpośrednimi zdarzenia były:
- nieprawidłowe zachowanie się pracowników wynikające z:
  - nadmiernego zaufania do skuteczności urządzeń ochronnych
  - lekceważenia zasad bezpieczeństwa
- zaburzenie w realizacji funkcji bezpieczeństwa polegającej na kontroli dostępu do strefy niebezpiecznej przez wyłącznik krańcowy na drzwiach ogrodzenia – wynikające z uszkodzenia tego wyłącznika
- zaburzenia w realizacji funkcji bezpieczeństwa przez wyłącznik krańcowy zainstalowany w bramce w wyniku jego obejścia
- zaburzenia w realizacji funkcji kontrolnych przez fotokomórki zamontowane na linii palet.

Zdarzenia te wystąpiły na skutek przyczyn pośrednich, którymi były:
- niewystarczające przeszkolenie pracowników, którzy nie mieli dostatecznej wiedzy o potencjalnych zagrożeniach na stanowisku pracy, pomimo że opracowane były stosowne instrukcje stanowiskowe
- błędy projektanta stanowiska pracy polegające na niewystarczającej odporności na defekty elementów systemu sterowania:
  - pojedynczy wyłącznik krańcowy w drzwiach ogrodzenia z jednoczesnym brakiem procedury okresowego sprawdzania

- konstrukcja ogrodzenia umożliwiająca obejście bramki, a tym samym funkcji bezpieczeństwa realizowanej przez zainstalowany tam wyłącznik krańcowy
- niewłaściwy typ, według PN-EN 61496-1, fotokomórek zamontowanych na linii podawania palet, co uniemożliwiło odpowiednio wczesne wykrycie ich nieprawidłowego funkcjonowania

– niewystarczająca lub niewłaściwa konserwacja urządzeń odpowiedzialnych za bezpieczeństwo.



Rys. 2.5. Model wypadku przy obsłudze podajnika palet

Graficzny obraz modelu tego wypadku przedstawiono na rys. 2.4, na którym zaciemnione pola pokazują sekwencję jego przyczyn. Z modelu wynika, że właściwymi sposobami zapobiegania takim wypadkom są:

– modyfikacja stanowiska pracy przez wprowadzenie redundancji w układzie wyłącznika krańcowego w drzwiach dostępu
– modyfikacja ogrodzenia, aby obejście bramki było niemożliwe
– wprowadzenie harmonogramu okresowych kontroli i konserwacji działania systemów ochronnych
– wprowadzenie systemu dodatkowych szkoleń bhp dla pracowników.

Środki te powinny być zastosowane w odniesieniu do wszystkich urządzeń w zakładzie.

2.4. Wnioski dotyczące wypadków związanych z niesprawnością systemu sterowania

Badania wypadków, które wydarzyły się podczas obsługi maszyn, wykazały, że istotny procent stanowią wśród nich te, które zostały spowodowane niewłaściwym funkcjonowaniem systemu sterowania maszyną. Na podkreślenie zasługuje zwłaszcza fakt, że ich skutki są zazwyczaj znacznie poważniejsze niż skutki wypadków spowodowanych innymi przyczynami. Dlatego szczególnie istotne są dokładne badania umożliwiające właściwe zaplanowanie działań zapobiegawczych. Badania takie powinny prowadzić nie tylko do wskazania i usunięcia przyczyny bezpośredniej, lecz także do zidentyfikowania głównej przyczyny pośredniej, gdyż jedynie jej usunięcie może zapobiec występowaniu podobnych wypadków w przyszłości. W zidentyfikowaniu tej przyczyny pomocne może być zastosowanie modelu zdarzeń wypadkowych związanych z nieprawidłowym funkcjonowaniem systemu sterownia. Model ten wspomaga pełne i właściwe wskazanie wszystkich przyczyn wypadku oraz źródeł zaistniałych nieprawidłowości. Może być z powodzeniem stosowany w dalszych analizach wypadków jako narzędzie pomocne w analizie i formułowaniu wniosków.

Przeprowadzone analizy wykazały, że istotnym czynnikiem w procesie powstawania wypadku jest niewłaściwe zachowanie się operatora maszyny. Oczywiście, najskuteczniejszym sposobem zapobiegania wypadkom byłoby wyeliminowanie nieprawidłowych działań pracowników. Sposobem na ich ograniczenie jest intensyfikacja szkoleń i nadzoru. Nie ulega jednak wątpliwości, że jest to sposób zawodny i nigdy nie uda się całkowicie wyeliminować błędu człowieka jako jednego z czynników w sekwencji zdarzeń prowadzących do wypadku. Dlatego też należy skupić się na środkach technicznych, które powinny neutralizować błędy pracownika. Przeprowadzone analizy wskazują, że podstawowe przyczyny wszystkich wypadków sprowadzają się do błędu popełnionego przez projektanta maszyny. Poprawnie zaprojektowany system sterowania powinien być odporny na błędy operatora. W tym sensie nieprawidłowe postępowanie operatora należy traktować jako

zjawisko normalne, a nie jako odstępstwo będące przyczyną wypadku. Niewłaściwe postępowanie operatora maszyny jest skutkiem zaburzeń w pracy systemu, a nie ich przyczyną (Dekker, 2003). Jedynie ten sposób traktowania błędów operatora w analizie wypadku umożliwi właściwe zidentyfikowanie jego faktycznych przyczyn i zaplanowanie działań zapobiegawczych.

Rozdział 3

Metody zwiększania odporności systemu sterowania na defekty

3.1. Zależność między bezpieczeństwem, niezawodnością a dostępnością maszyn

Przedstawione w rozdziale 2 wyniki analiz wypadków wskazują, jak istotne znaczenie ma zapewnienie realizacji funkcji bezpieczeństwa w każdych warunkach. Wymaga to od konstruktora przede wszystkim właściwego zrozumienia zależności pomiędzy bezpieczeństwem a niezawodnością. Podstawowe definicje tych pojęć można znaleźć w większości norm dotyczących bezpieczeństwa. Nie zawsze jednak są one właściwie interpretowane.

Pojęcie *bezpieczeństwo* jest zdefiniowane w PN-EN 61508-4:2010 jako:

– niewystępowanie ryzyka nieakceptowanego.

Należy zwrócić uwagę, że w definicji tej nie wymaga się, aby maszyna była sprawna, lecz by nie narażała operatora na ryzyko. Trzeba to interpretować w ten sposób, że poziom ryzyka nie powinien przekraczać poziomu akceptowalnego, także w warunkach uszkodzenia maszyny. Tak więc wymagania dotyczące bezpieczeństwa koncentrują się na wytworzeniu systemu, który nie powoduje wypadków. Wymagania dotyczące bezpieczeństwa powinny wskazywać, jakie środki zaleca się zastosować w przypadku zdarzeń nieprzewidzianych.

Natomiast wg PN-EN ISO 12100:2011 *niezawodność* (maszyny) to:

– zdolność maszyny, jej elementów lub wyposażenia do wykonywania wymaganej funkcji w określonych warunkach przez określony czas bez uszkodzenia.

Tak więc, z punktu widzenia bezpieczeństwa, nie jest ważne, że system nie służy swojemu celowi tak długo, jak długo wymagania dotyczące bezpieczeństwa nie są naruszone. Istnieje jednakże możliwość stosowania bardzo niezawodnego, ale niebezpiecznego systemu, np. systemu z formalnie sprawdzonym oprogramowaniem, w którym aspekty dotyczące bezpieczeństwa nie są prawidłowo uwzględnione.

Ważną cechą urządzenia jest także jego *dyspozycyjność* (Dźwiarek, Hryniewicz, 2011), czyli:

– zdolność maszyny do bycia w stanie gotowym do wypełniania żądanych funkcji w określonych warunkach w określonym czasie lub w określonym przedziale czasu, pod warunkiem, że dostarczone są wymagane środki zewnętrzne.

Dyspozycyjność może mieć wpływ na bezpieczeństwo, gdyż oznacza między innymi, że realizowane są funkcje związane z bezpieczeństwem. W przeciwnym razie mogło by to prowadzić, na przykład, do obchodzenia urządzeń ochronnych.

W systemach związanych z bezpieczeństwem istotne znaczenie ma właściwe określenie stanu bezpiecznego. Według PN-EN 61508-4:2010 *stan bezpieczny* jest to stan urządzenia, w którym zachowane jest bezpieczeństwo. Należy to rozumieć jako stan, w którym ryzyko jest na poziomie akceptowalnym. Z punktu widzenia bezpieczeństwa ważne jest, czy system wymaga aktywnego sterowania przy zmianie stanu ze stanu zagrożenia do bezpiecznego. Ma to niezwykłe znaczenie przy określaniu reakcji systemu na defekty. Przykładem systemu, który musi w sposób aktywny kontrolować przechodzenie ze stanu zagrożenia w stan bezpieczny, jest lecący samolot. Po wystąpieniu uszkodzenia w układzie elektronicznym systemu sterowania samolot musi być nadal sterowny, aby wylądować w sposób bezpieczny na najbliższym możliwym lądowisku. Podobny jest problem sterowania procesami przemysłowymi, na przykład w instalacjach chemicznych lub w elektrowniach atomowych. Sterowanie wyłączaniem reaktora lub zatrzymaniem procesu chemicznego wymaga aktywnej pracy systemu sterowania.

Inny jest przypadek jadącego pociągu. Hamulce pociągu mogą, a nawet powinny być tak zbudowane, aby w razie defektu automatycznie zablokować dalszy jego ruch. Przy obsłudze maszyn zazwyczaj mamy do czynienia z sytuacją, gdy wprowadzenie w stan bezpieczny nie wymaga aktywnego sterowania. Są oczywiście wyjątki od tej reguły, na przykład w zautomatyzowanych liniach montażowych, gdzie konieczna jest synchronizacja zatrzymania wszystkich stanowisk.

Brak możliwości sprowadzenia maszyny do stanu bezpiecznego, związany z utratą dyspozycyjności systemu, jest zazwyczaj skutkiem jego defektu lub uszkodzenia. *Uszkodzenie* jest to przerwanie zdolności urządzenia do wykonywania założonych funkcji. Uszkodzeniem może być np. przerwanie przewodów łączących poszczególne części urządzenia czy przepalenie się elementu elektronicznego. Uszkodzenie prowadzi zazwyczaj do defektu.

Defekt jest to stan urządzenia, który charakteryzuje się jego niezdolnością do wykonywania założonych funkcji. Tak więc urządzenie ma defekt na przykład wówczas, gdy zepsuty wyświetlacz wskazuje niewłaściwe cyfry lub gdy projektant nie przewidział właściwych urządzeń ochronnych. Defekt może być trwały albo chwilowy. Przykładem defektu trwałego jest uszkodzenie elementu urządzenia lub

zastosowanie przez projektanta niewłaściwych środków zapobiegania wypadkom. Przykładem defektu chwilowego może być niewłaściwe działanie urządzenia na skutek pomyłki operatora. Niejednokrotnie defekt chwilowy może zostać usunięty przez wykonanie czynności zgodnych z instrukcją obsługi, np. wyłączenie i powtórne włączenie systemu lub jego zresetowanie.

3.2. Defekty niebezpieczne

Tak więc ocena bezpieczeństwa maszyny dotyczy przede wszystkim możliwości wystąpienia zagrożeń, a jej niezawodności – jedynie w zakresie związanym z bezpieczeństwem. Oznacza to, że ze względu na bezpieczeństwo nie jest istotna częstość występowania defektów w ogóle, lecz przede wszystkim prawdopodobieństwo zmniejszenia skuteczności realizacji funkcji bezpieczeństwa. W normie PN-EN 61508-4:2010 zdefiniowano *uszkodzenie niebezpieczne* jako:

– uszkodzenie, które może potencjalnie wprowadzić system związany z bezpieczeństwem w stan występowania zagrożenia lub utraty funkcji.

To, czy stan potencjalny zostanie zrealizowany, zależy od architektury systemu. W systemach wielokanałowych jest mniejsze prawdopodobieństwo, że niebezpieczne uszkodzenie sprzętu doprowadzi do stanu występowania zagrożenia lub utraty funkcji.

Nieco inaczej pojęcie uszkodzenia niebezpiecznego jest zdefiniowane w normie PN-EN ISO 12100:2011:

– jest to każde uszkodzenie w maszynie lub jej zasilaniu, które zwiększa ryzyko.

W sensie tych definicji uszkodzenie, które zostanie wykryte, nie jest uszkodzeniem niebezpiecznym, jeśli konsekwencją jego wykrycia jest stan bezpieczny. Sprowadzenie do stanu bezpiecznego może być wykonywane automatycznie, na przykład przez zainicjowanie procedury zatrzymywania ruchu niebezpiecznego. Często spotykane są także układy, w których uzyskanie stanu bezpiecznego wymaga interwencji operatora. W takich układach efektem wykrycia uszkodzenia jest generowanie sygnałów ostrzegawczych, które jedynie informują operatora o występowaniu zagrożenia. Decyzja, czy należy stosować systemy automatycznie sprowadzające do stanu bezpiecznego, czy tylko ostrzegawcze, zależy od wyników analizy ryzyka. Zazwyczaj systemy automatyczne stosuje się w urządzeniach o wysokim poziomie ryzyka, a zwłaszcza wówczas, gdy częstość występowania narażenia jest znaczna. Systemy ostrzegawcze mogą być stosowane tam, gdzie operator rzadko ingeruje w strefę zagrożenia.

Zgodnie z podanymi tu definicjami, w przypadku maszyn, o tym, czy uszkodzenie jest niebezpieczne, decyduje przede wszystkim to, czy jego efektem jest

zagrożenie dla operatora lub utrata skuteczności realizacji procedury sprowadzającej do stanu bezpiecznego. Należy to rozumieć w ten sposób, że na skutek uszkodzenia poziom ryzyka przekroczył poziom akceptowalny. Tak więc, uszkodzenia jednego z kanałów układu redundancji nie należy traktować jako uszkodzenia niebezpiecznego. W poprawnie zbudowanym systemie redundancji uszkodzenie albo jest wykrywane i urządzenie jest sprowadzane do stanu bezpiecznego, albo funkcja bezpieczeństwa jest nadal realizowana przez drugi, wciąż sprawny kanał. W tym drugim przypadku skutkiem uszkodzenia jest obniżenie poziomu nienaruszalności bezpieczeństwa, ale bezpieczeństwo operatora jest nadal nadzorowane. Dopiero akumulacja niewykrytych uszkodzeń może spowodować utratę funkcji bezpieczeństwa, a więc stanowić będzie uszkodzenie niebezpieczne.

Istotne znaczenie ma także czas wykrycia uszkodzenia. Zazwyczaj, zanim uszkodzenie zostanie wykryte, mija pewien czas potrzebny na wykonanie diagnostyki systemu. Testy automatyczne przeważnie są wykonywane po uruchomieniu lub resecie systemu oraz periodycznie podczas jego pracy. Uszkodzenie może być także wykryte w trakcie okresowego sprawdzania lub konserwacji systemu. Tak więc w systemie może występować uszkodzenie, które spowoduje upośledzenie funkcji bezpieczeństwa i zostanie wykryte dopiero po jakimś czasie. Uszkodzenia takie stają się uszkodzeniami niebezpiecznymi, jeśli przywołanie funkcji bezpieczeństwa nastąpi przed ich wykryciem. Natomiast, jeśli uszkodzenie zostanie wykryte odpowiednio szybko, to nie powinno być rozpatrywane jako niebezpieczne. Ten typ uszkodzeń można zakwalifikować jako potencjalnie niebezpieczne.

Także nie wszystkie uszkodzenia systemu jednokanałowego są uszkodzeniami niebezpiecznymi. Niebezpieczne są tylko te, które powodują utratę funkcji bezpieczeństwa.

Defekty można podzielić na kilka różnych sposobów. Główny podział jest związany z przyczynami ich powstania. Zgodnie z tym podziałem wyróżnia się dwie podstawowe grupy defektów (Dźwiarek, 2000c; STSARCES, 2000):

- przypadkowe
- systematyczne.

3.3. Defekty przypadkowe

Zazwyczaj system sterowania zawiera dużą liczbę połączonych elektrycznie i mechanicznie elementów i podzespołów. Długotrwałe użytkowanie maszyny zwykle pociąga za sobą niszczenie jej podzespołów spowodowane pogorszeniem właściwości materiałowych i zużyciem mechanicznym. Pogorszenie właściwości lub parametrów podzespołów lub elementów systemu sterowania może

w przypadkowej chwili czasu prowadzić do defektu systemu. Mówi się wówczas o defekcie przypadkowym. W systemach sterowania zjawiska te powodują, że maszyna przestaje realizować założone funkcje. Jeśli są to funkcje bezpieczeństwa, skutkiem ich niezadziałania może być wzrost ryzyka.

3.4. Defekty systematyczne

Defekt systematyczny jest związany z błędem człowieka (wliczając w to zarówno niewłaściwe działanie, jak i brak działania) popełnionym na dowolnym etapie cyklu życia maszyny, który może prowadzić do powstania sytuacji niebezpiecznej w razie wystąpienia szczególnej kombinacji zjawisk zewnętrznych.

Można wyróżnić cztery podstawowe, omówione dalej, przyczyny powstawania defektów systematycznych.

Błędy ustalenia wymagań

Obejmują pomyłki lub przeoczenia popełnione podczas analizy zagrożeń, oceny ryzyka, ustalania wymagań bezpieczeństwa oraz formułowania założeń do projektu i opracowywania planu sprawdzania spełnienia wymagań bezpieczeństwa.

Błędy wyposażenia

Mogą wystąpić w dowolnej fazie projektowania, produkcji, instalowania lub użytkowania urządzenia. Obejmują zastosowanie niewłaściwych rozwiązań konstrukcyjnych, użycie nieodpowiednich elementów lub podzespołów, niespełnienie wymagań systemu jakości produkcji, użytkowanie niezgodne z dostarczoną instrukcją itp.

Błędy oprogramowania

Mogą być skutkiem niewłaściwego opracowania programu w fazie projektowania czy też użycia niewłaściwego wyposażenia, ale mogą zostać także wprowadzone podczas późniejszych modyfikacji programu.

Uszkodzenie od wspólnej przyczyny

Jednym z istotnych źródeł niesprawności są uszkodzenia od wspólnej przyczyny (ang. *common case failure* – CCF). Są to uszkodzenia, które powodują identyczne skutki w dwu lub więcej układach redundancji na skutek tych samych przyczyn, np. narażeń środowiskowych lub błędów projektanta. Tak więc uszkodzenia od wspólnej przyczyny są zawsze przejawem występowania defektów systematycznych.

Duże znaczenie tych uszkodzeń wynika z faktu, że nie można im zapobiegać w prosty sposób.

Defekty systematyczne mogą zatem występować zarówno w wyposażeniu, jak i w oprogramowaniu. Szczególnymi przypadkami takich defektów umiejscowionych w wyposażeniu są: brak odporności na warunki środowiskowe, zła ochrona przed porażeniem prądem elektrycznym, niewłaściwy stopień ochrony obudowy itp. Defekty te są skutkiem błędów ustalenia wymagań lub błędów projektanta. Powodują, że maszyna funkcjonuje nie tak, jak zamierzał projektant.

Ponieważ defekty systematyczne są związane ze sformułowaniem niewłaściwych założeń do projektu lub niewłaściwym projektowaniem i mają charakter wprowadzania nieprzewidzianych właściwości do systemu, więc nie można przewidzieć, jak często będą prowadzić do sytuacji niebezpiecznych. W odróżnieniu od defektów przypadkowych, metody symulacyjne nie zawsze umożliwiają wykrywanie defektów systematycznych. Zazwyczaj nie jest także możliwe określenie prawdopodobieństwa powstania sytuacji niebezpiecznej na skutek defektów systematycznych. Dlatego też takim defektom można zapobiegać głównie przez stosowanie odpowiednich systemów jakości w trakcie projektowania.

3.5. Trzypunktowa strategia zapobiegania defektom

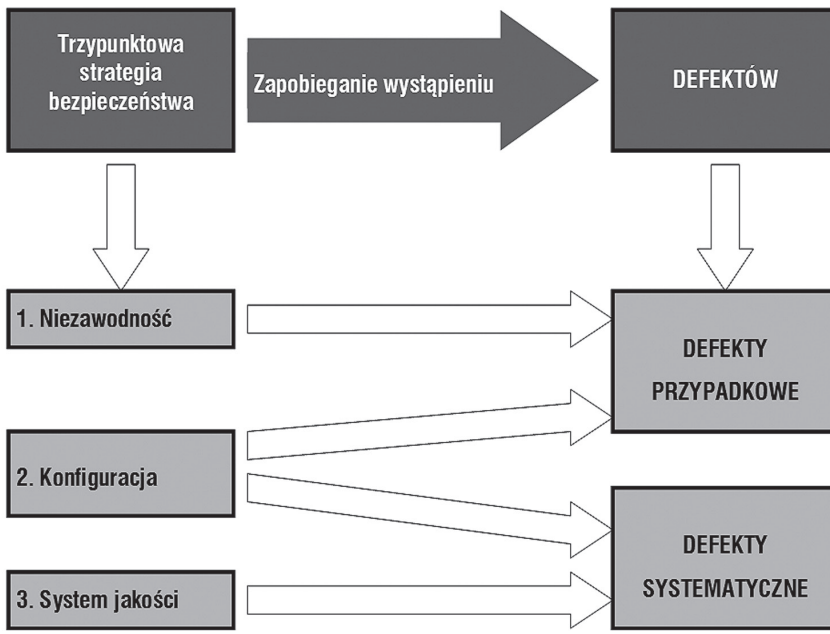
Zapobieganie występowaniu defektów w systemach sterowania może być realizowane na wiele różnych sposobów, zależnie od rodzaju przewidywanych defektów oraz od zamierzonego poziomu nienaruszalności bezpieczeństwa. Najskuteczniejsze jest postępowanie według trzypunktowej strategii zapobiegania defektom (Dźwiarek, 2000b). Ogólny schemat tej strategii pokazano na rys. 3.1. Opiera się ona na zastosowaniu trzech środków mających na celu uniknięcie wystąpienia defektów:

- uwzględnieniu wymagań niezawodności
- doborze odpowiedniej konfiguracji układu
- utrzymaniu zasad systemu jakości w całym cyklu życia sterownika.

Niezawodność systemu jest jednym z decydujących czynników określających prawdopodobieństwo wystąpienia defektów przypadkowych. Dlatego też uwzględnienie wymagań niezawodności przy doborze elementów oraz w fazie produkcji systemu może w dużym stopniu zapobiec występowaniu tego typu defektów w sprzęcie. Zasada ta dotyczy wszystkich elementów i podzespołów systemu sterowania. Dlatego istotne jest, aby projektant zawsze pamiętał o wymaganiach niezawodności.

Duże znaczenie ma także dobór właściwej konfiguracji systemu. Dotyczy to zarówno wewnętrznej konfiguracji sterownika, jak i sposobów połączenia go

z urządzeniami zewnętrznymi. Właściwa konfiguracja umożliwia zmniejszenie prawdopodobieństwa niewłaściwego działania systemu sterowania zarówno w przypadku wystąpienia większości defektów przypadkowych, jak i niektórych defektów systematycznych.



Rys. 3.1. Trzypunktowa strategia zapobiegania defektom

Ostatnim elementem trzypunktowej strategii zapobiegania defektom jest stosowanie zasad zapewnienia jakości w całym cyklu życia sterownika. Polegają one na ścisłym dokumentowaniu wszystkich czynności wykonywanych w poszczególnych etapach cyklu życia maszyny. Istotnymi elementami systemu jakości są także kompetencje personelu, dobór podwykonawców, współpraca dostawcy z użytkownikiem itp. Przestrzeganie zasad zapewnienia jakości umożliwia zmniejszenie prawdopodobieństwa wystąpienia defektów systematycznych.

Rozdział 4

Metody nadzorowania defektów

4.1. Ograniczanie prawdopodobieństwa występowania uszkodzeń

Jak wynika z rozdziału 3, odporność systemu sterowania na defekty można zwiększyć z jednej strony przez zmniejszenie prawdopodobieństwa wystąpienia uszkodzenia, z drugiej zaś przez spowodowanie, że ewentualny defekt nie będzie defektem niebezpiecznym.

Podstawowym środkiem zmniejszania prawdopodobieństwa wystąpienia uszkodzenia jest stosowanie niezawodnych elementów i podzespołów. Przy doborze elementów i podzespołów należy pamiętać, że powinny one być odporne na oddziaływanie następujących czynników:

- spodziewanego narażenia w czasie pracy (np. czasu pracy, oporów ruchu itp.)
- wpływu obrabianego materiału (np. detergentów, drewna, metalu itp.)
- wpływów środowiskowych (mechanicznych, klimatycznych, elektrycznych itp.).

Są to tzw. „podstawowe zasady bezpieczeństwa" zapewniające utrzymanie wskaźników niezawodnościowych podanych przez producentów tych elementów i podzespołów podczas ich stosowania w środowisku przemysłowym.

Dalsze ograniczenie prawdopodobieństwa wystąpienia uszkodzenia można uzyskać, stosując „wypróbowane" elementy i podzespoły. Do grupy „wypróbowanych" zalicza się elementy i podzespoły:

- szeroko stosowane w podobnych aplikacjach z dobrym rezultatem
- wykonane i przebadane w sposób potwierdzający ich niezawodność i przydatność w zastosowaniach związanych z bezpieczeństwem.

Skuteczną metodą zapobiegania defektom, a zwłaszcza defektom niebezpiecznym, jest stosowanie „wypróbowanych zasad projektowania". Są to np.:

– zapobieganie niektórym defektom, np. zwarciom przez izolowanie przewodów lub stosowanie właściwych odległości między ścieżkami
– ograniczenie prawdopodobieństwa występowania uszkodzeń, np. przez przewymiarowanie
– ukierunkowanie uszkodzeń, np. wymuszenie przepalenia się obwodu, jeśli konieczne jest szybkie odcięcie zasilania
– wystarczająco wczesne wykrywanie defektów
– ograniczanie skutków defektów, np. przez uziemianie obudów urządzeń elektrycznych.

W efekcie zastosowania „wypróbowanych elementów" oraz „wypróbowanych zasad" ogranicza się prawdopodobieństwo wystąpienia uszkodzeń, a także liczbę potencjalnych defektów przez ich wykluczenie. Ukierunkowuje się także niektóre potencjalne defekty, sprowadzając system do stanu bezpiecznego.

A zatem danymi, które charakteryzują ten sposób ograniczania prawdopodobieństwa wystąpienia defektu niebezpiecznego, niezbędnymi do prowadzenia analiz probabilistycznych, są:

– wskaźniki niezawodnościowe poszczególnych elementów systemu
– wykazy zastosowanych „wypróbowanych zasad bezpieczeństwa" i „wypróbowanych elementów"
– wykazy defektów wykluczonych.

Zazwyczaj niezawodność elementu charakteryzowana jest parametrem *MTTF* oznaczającym średni czas pomiędzy uszkodzeniami. Wskaźnik ten informuje, jaki jest najbardziej prawdopodobny odsetek podzespołów danego typu, które ulegną uszkodzeniu w określonym czasie.

W przypadku elementów mechanicznych, hydraulicznych, pneumatycznych i elektromechanicznych często jako parametr charakteryzujący pewność działania elementu producenci podają B_{10D}. Parametr ten określa liczbę zadziałań, przy której uszkodzeniu ulega 10% wyprodukowanych egzemplarzy elementu. Znając wartość parametru B_{10D}, można wyznaczyć wartość *MTTF* na podstawie przewidywanej częstości przywołań funkcji bezpieczeństwa oraz oczekiwanego czasu pracy maszyny.

Przy wyznaczaniu prawdopodobieństwa występowania defektów niebezpiecznych należy także uwzględnić parametr *SFF* (wskaźnik defektów bezpiecznych), wskazujący procent tych defektów elementu lub podzespołu, które nie są defektami niebezpiecznymi. Rozważmy na przykład tranzystor pracujący jako klucz w układzie elektronicznym. W zasadzie można przyjąć, że przy tego rodzaju pracy istotne są dwa rodzaje uszkodzenia – trwałe zamknięcie obwodu lub trwałe otwarcie obwodu. Jedno z tych uszkodzeń zawsze wprowadza system w stan bezpieczny, a więc można przyjąć, że w przypadku tranzystora pracującego jako klucz *SFF* wynosi 50%.

4.2. Nadzorowanie defektów

4.2.1. Wprowadzenie

Podstawowymi środkami nadzorowania uszkodzeń przypadkowych i zapobiegania ich skutkom są:

- monitorowanie sprawności systemu
- stosowanie architektury wielokanałowej (redundancja)
- wykorzystywanie systemów dynamicznych, w których informacje są przenoszone przez sygnały zmienne, a stan statyczny oznacza uszkodzenie.

Elektroniczne systemy sterowania mają możliwość wykrywania uszkodzeń wewnętrznych zanim ujawnią się one jako defekt systemu. Możliwe rozwiązania zawierają zarówno środki układowe, jak i programowe. W zależności od rodzaju zastosowanej metody wykrywane są uszkodzenia różnych części systemu.

Szczegółowy wykaz metod zapobiegania skutkom defektów i uszkodzeń jest podany w normie PN-EN 61508-7:2010 oraz w raporcie STSARCES (2000). Dalej zostaną omówione ogólne zasady stosowania metod najbardziej rozpowszechnionych i skutecznych.

4.2.2. Monitorowanie

Periodyczne kontrolowanie sprawności systemu jest jednym z najbardziej skutecznych układowych środków nadzorowania uszkodzeń. Polega ono na automatycznym sprawdzeniu, czy system działa poprawnie. Zazwyczaj stosuje się jedno z dwu rozwiązań:

- **testy wzorcowe**

W określonych odstępach czasu układ monitorujący generuje wzorcowe sygnały wejściowe. Sprawdzana jest reakcja systemu na te sygnały. Stan wyjść lub wyznaczone dane są porównywane z danymi wzorcowymi. Skuteczność testu zależy od reprezentatywności dobranych danych wzorcowych oraz od częstotliwości sprawdzeń. Należy pamiętać, że podczas sprawdzania system nie realizuje funkcji podstawowej, a więc czas sprawdzania powinien być wystarczająco mały w danym zastosowaniu, a proces sprawdzania nie może powodować zagrożeń dla operatora.

- **kontrolowanie sygnałów wyjściowych**

Układ kontrolujący na bieżąco analizuje sygnały wejściowe i wyjściowe w systemie. Dane z systemu są porównywane z informacjami wzorcowymi. Wynik porównania decyduje o potwierdzeniu poprawności funkcjonowania systemu. Ten rodzaj monitorowania działa podobnie jak układ redundancji, z tą różnicą, że jeden z kanałów nie bierze bezpośredniego udziału w realizacji funkcji bezpieczeństwa.

Monitorowanie może być realizowane zarówno sprzętowo, jak i programowo. W rozwiązaniach sprzętowych jest wykonywane przez dodatkowy obwód, który działa niezależnie od obwodu podstawowego. W realizacji programowej jest realizowane przez osobne procedury programu. Możliwe są także kombinacje obu tych rozwiązań. Najskuteczniejsze jest monitorowanie sprzętowe, które umożliwia wykrycie praktycznie wszystkich, istotnych dla funkcjonowania systemu, defektów. Monitorowanie tylko za pomocą dodatkowych procedur programowych jest mniej skuteczne.

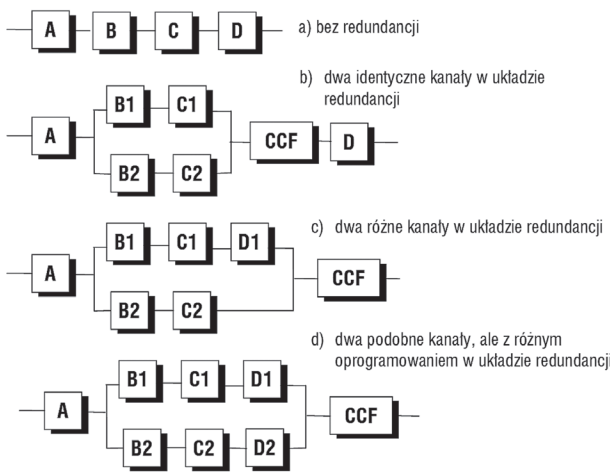
4.2.3. Redundancja

Równie skutecznym środkiem jak monitorowanie jest redundancja. Należy ona do najczęściej stosowanych układowych sposobów zapobiegania defektom niebezpiecznym.

Skuteczność układów redundancji

Redundancja może być stosowana w różnych wariantach technologicznych. Wpływ różnych rodzajów defektów na zapobieganie defektom systemu sterowania w kilku wariantach redundancji pokazano na rys. 4.1. Na rysunku tym zastosowano następujące oznaczenia:

A – błędy ustalenia wymagań
B – uszkodzenie przypadkowe sprzętu
C – defekt systematyczny sprzętu
D – defekt oprogramowania
CCF – uszkodzenie od wspólnej przyczyny.



Rys. 4.1. Schematyczne przedstawienie defektów w różnych rodzajach redundancji

W przypadku a), gdy nie zastosowano redundancji, wszystkie rodzaje uszkodzeń są uszkodzeniami niebezpiecznymi.

W przypadku b) uszkodzeniem niebezpiecznym jest jednoczesne wystąpienie uszkodzeń w obu gałęziach redundancji (np. B1 i B2 lub B1 i C2). A zatem zmniejszony został wpływ uszkodzeń sprzętu na nienaruszalność bezpieczeństwa. Natomiast w dalszym ciągu istotne znaczenie mają błędy oprogramowania. Czynnik CCF reprezentuje tę część defektu systematycznego sprzętu C, która powoduje powstawanie takich samych uszkodzeń w obu gałęziach redundancji (uszkodzenie od wspólnej przyczyny), nie jest to więc nowe źródło uszkodzeń, a jedynie część źródła dotychczasowego.

Przykład c) pokazuje sytuację, gdy jeden z kanałów redundancji nie zawiera elementów programowalnych, a jest wykonany w technologii mechanicznej lub elektrycznej. Rozwiązane takie ogranicza dodatkowo wpływ błędów oprogramowania. Znaczne różnice pomiędzy kanałami spowodują także, że pokazany na rysunku wpływ CCF będzie stosunkowo mały ze względu na małe prawdopodobieństwo wystąpienia uszkodzeń tego typu.

W przypadku d) pokazano sytuację dwu systemów programowalnych o różnym oprogramowaniu. Osiągnięte rezultaty są podobne jak w przypadku c), jednakże tym razem prawdopodobieństwo wystąpienia CCF jest większe.

Redundancja umożliwia zarówno wykrywanie uszkodzeń, jak i podtrzymywanie poprawnego funkcjonowania pomimo defektu. Wykrywanie uszkodzeń realizuje się poprzez identyfikację różnic w funkcjonowaniu poszczególnych kanałów redundancji. Zazwyczaj nie wszystkie uszkodzenia ujawniają się w ten sposób. Niektóre ujawnią się jedynie w szczególnych okolicznościach. W takim przypadku kanał bez uszkodzeń nadal realizuje funkcję bezpieczeństwa.

Architektura układów wielokanałowych

Przykłady pokazane na rys. 4.1 opisują redundancję dwukanałową. Jest to najprostszy przykład redundancji. W praktyce spotyka się często rozwiązania wielokanałowe, o liczbie kanałów większej niż 2. W ogólnym przypadku przyjęto opisywanie redundancji jako układu *MooN*, gdzie *N* oznacza liczbę wszystkich kanałów, a *M* minimalną liczbę kanałów sprawnych, niezbędnych do realizacji funkcji bezpieczeństwa. Tak więc architektura 1*oo*1 oznacza układ jednokanałowy. Architektura 1*oo*2 oznacza układ 2-kanałowy, w którym funkcja bezpieczeństwa jest realizowana, jeśli co najmniej jeden kanał jest sprawny. Układy pokazane na rys. 4.1 są przykładami architektury 1*oo*2. Architektura 2*oo*3 oznacza układ 3-kanałowy, w którym decyzja jest podejmowana przez głosowanie. W układzie takim funkcja bezpieczeństwa jest realizowana, gdy co najmniej dwa kanały są sprawne.

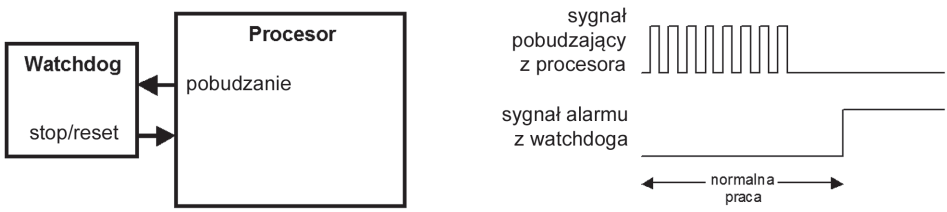
Układy z redundancją mogą być także wyposażone w systemy diagnostyczne. Mówi się wówczas o architekturze typu *MooND*.

4.2.4. Watchdog

Prawidłowa realizacja sekwencji programowych może być zakłócona zarówno przez defekty oprogramowania lub uszkodzenia sprzętu, jak i przez oddziaływania środowiskowe. Duża liczba różnych źródeł zaburzeń w realizacji programu powoduje, że prawdopodobieństwo ich wystąpienia jest znaczące. Konsekwencje takich zaburzeń są praktycznie nieprzewidywalne, co oznacza, że podczas walidacji systemu należy założyć że „wszystko jest możliwe". Dlatego też duże znaczenie ma stosowanie skutecznych środków kontroli sekwencji programowych. Może to być realizowane zarówno sprzętowo, jak i programowo. Najskuteczniejsze jest stosowanie kombinacji elementów sprzętowych („watchdog") wspieranych programowymi procedurami kontroli logicznej.

Monitorowanie sprzętowe

Watchdog jest sprzętowym urządzeniem, które monitoruje działanie urządzeń wewnętrznych systemu, a także oprogramowania aplikacyjnego i systemowego. Jeśli oczekiwane sygnały nie pojawiają się w określonym przedziale czasu, to watchdog powinien sprowadzić system do stanu bezpiecznego. W praktyce watchdog jest rodzajem timera pobudzanego periodycznie przez procesor. Jeżeli sygnał pobudzający nie dociera w określonym czasie, to generowany jest sygnał uruchomienia procedury sprowadzającej do stanu bezpiecznego.



Rys. 4.2. Watchdog – schemat blokowy i zasada działania

Obecnie dostępne są różne rozwiązania funkcjonalne systemu. Wiele mikroprocesorów ma wewnętrzne układy zaimplementowane specjalnie do realizacji funkcji watchdog. W takim przypadku watchdog jest programowany i sterowany przez wewnętrzny rejestr procesora. Oferowane są także specjalne układy scalone realizujące funkcję watchdog. Możliwe jest także zaprojektowanie własnego obwodu opartego na przerzutnikach monostabilnych.

Wybór właściwego rozwiązania zależy od właściwości konkretnego systemu. Zazwyczaj jednak zalecane jest stosowanie sprzętu niezależnego od procesora. W ten sposób zapobiega się sytuacji, gdy ta sama przyczyna powoduje zaburzenie sekwencji programowej i jednocześnie zatrzymuje funkcjonowanie systemu watchdog. Szczególną uwagę należy zwrócić na układy odmierzania czasu, tak aby procesor i watchdog nie korzystały z tego samego zegara, gdyż zatrzymanie zegara lub zmiana generowanej częstotliwości nie byłyby wówczas wykrywane. W systemach o dużych wymaganiach bezpieczeństwa może być także konieczne zapewnienie, aby procesor automatycznie sprawdzał, czy watchdog funkcjonuje poprawnie.

Aspekty programowe

Impulsy pobudzające watchdog sprzętowy są generowane przez program. Także wówczas, gdy sekwencje programowe są monitorowane bez użycia sprzętu, stosowne sygnały są generowane programowo. Najprostszym sposobem cyklicznego pobudzania systemu jest sprawdzanie wykonania programu po każdej sekwencji. Nie zaleca się, aby watchdog był pobudzany z wykorzystaniem przerwań lub specjalnych procedur programowych. Takie pobudzanie umożliwia jedynie sprawdzenie, czy pojedyncza procedura funkcjonuje. Skuteczniejszym sposobem sprawdzania sekwencji programowych jest wykorzystanie flag lub słów kluczowych, których ustawienie identyfikuje poszczególne części programu i wskazuje, że jest on wykonywany we właściwej sekwencji.

Działanie po wykryciu defektu

Sposób reakcji na wykrycie zaburzeń w sekwencji programowej może być bardzo różny w różnych systemach. Ważne jest jednak, aby reakcja ta była dobrana do konkretnych sytuacji. Większość maszyn można sprowadzić do stanu bezpiecznego po wykryciu defektu. Watchdog powinien mieć możliwość wymuszenia na procesorze i jego wyjściach stanu, w którym sygnały są nieaktywne. Inną możliwością jest odłączenie przez watchdog zasilania urządzeń wyjściowych, tak aby wprowadzić maszynę w stan bezpieczny. Wyprowadzenie maszyny z takiego stanu powinno być możliwe jedynie po wykonaniu specjalnych, zamierzonych czynności.

W zastosowaniach wymagających szczególnej dyspozycyjności sygnał generowany przez watchdog może być użyty do zatrzymania jednego procesora i kontynuowania pracy układu redundancji bez wpływu na normalne działanie całego systemu.

W systemach jednokanałowych przewidzianych do pracy w trybie ciągłym często jest wymagane, aby watchdog resetował procesor w taki sposób, że działanie systemu jest w miarę możliwości kontynuowane. W takiej sytuacji nie występuje

stan bezpieczny i należy uwzględnić zagrożenia związane z brakiem aktywności procesora.

W systemach, w których mierzone są wartości parametrów istotnych dla bezpieczeństwa, konieczne jest określenie, w jaki sposób parametry te będą kontrolowane po aktywizacji watchdoga.

4.2.5. Autotesty realizowane programowo

W systemach programowalnych jednostka centralna może ulegać uszkodzeniom na wiele różnych sposobów. Mogą to być na przykład uszkodzenia rejestrów wewnętrznych, niesprawności dekodera instrukcji, błędy w przesyłaniu danych i wiele innych. Systemy programowalne charakteryzują się możliwością autotestowania w trakcie funkcjonowania. Wynika to stąd, że podczas realizacji programu podstawowego niejednokrotnie procesor biernie czeka na sygnały zewnętrzne. Czas ten można wykorzystać do periodycznego sprawdzania stanu poszczególnych elementów systemu. W PN-EN 61508-7:2010 wyszczególnione są podstawowe metody testowania systemu wraz ze wskazaniem stosownej literatury.

Autotesty są wykonywane przez procedury programowe, które sprawdzają poprawność funkcjonowania procesora. Realizuje się to poprzez wykonanie określonych operacji i sprawdzenie, czy uzyskuje się właściwe rezultaty. W praktyce, zwłaszcza w przypadku niewielkich systemów, nie jest możliwe ciągłe przeprowadzanie testów całego systemu w trakcie jego pracy. Dlatego też pełne testy są przeprowadzane w charakterystycznych punktach programu, na przykład po uruchomieniu, resecie itp. Natomiast w trakcie pracy przeprowadza się testy ograniczone, których zakres zależy od możliwości procesora. W systemach wielokanałowych zazwyczaj jest realizowana wymiana danych między kanałami i sprawdzanie ich zgodności.

Do wykrywania uszkodzeń w jednostce centralnej najczęściej stosuje się następujące metody (według PN-EN 61508-7:2010):

- w pamięci stałej:
  - suma kontrolna
  - słowa lub bity parzystości
  - wielokrotny zapis
- w pamięci o swobodnym dostępie: zapis i odczyt zawartości określonych danych (np. testy „checkboard”, „walkpath”, „galapat” itp.)
- w układach I/O: zapisywanie i odczyt określonych danych
- w magistralach komunikacyjnych: wielokrotne przesyłanie danych, równoległe przesyłanie danych, bity parzystości, słowa kontrolne
- w zasilaczach: kontrola poziomu napięć.

4.2.6. Środki stosowane przez użytkownika systemu

Dodatkowymi środkami uzupełniającymi środki układowe, służącymi wykrywaniu uszkodzeń przypadkowych, są środki stosowane przez użytkownika systemu. Najważniejszymi z nich są:

– okresowe sprawdzenia i konserwacja (ang. *proof tests*)

Polegają na okresowej kontroli sprawności systemu mającej na celu wykrycie wszystkich ewentualnych uszkodzeń i ich usunięcie, tak aby doprowadzić system do stanu możliwie najbliższego stanowi początkowemu. Szczególne znaczenie ma okresowa wymiana podzespołów, które wprawdzie nie uległy uszkodzeniu, ale przepracowały gwarantowany przez producenta czas pracy bezawaryjnej. Okresowe sprawdzenia umożliwiają wyeliminowanie uszkodzeń niebezpiecznych, które nie zostały wykryte przez autotesty oraz nie ujawniły się w trakcie pracy systemu. Aby środek ten był w pełni efektywny, powinien zapewniać 100-procentową diagnostykę. W praktyce nie jest to możliwe. Konieczne jest jednak, aby sprawdzenia obejmowały wszystkie funkcje bezpieczeństwa, zgodnie z założeniami sformułowanymi przez projektanta. W przypadku systemów wielokanałowych sprawdzeniu powinien podlegać każdy kanał oddzielnie.

– periodyczne wyłączanie systemu (ang. *restoration*)

Większość testów automatycznych przeprowadza się po włączeniu systemu lub po jego resecie. Dlatego też wskazane jest, aby systemy związane z bezpieczeństwem były periodycznie wyłączane i ponownie włączane. Zazwyczaj jest to wykonywane raz na dobę lub raz na zmianę. Postępowanie takie zwiększa skuteczność autotestów. Częstość periodycznych wyłączeń powinna być określana przez dostawcę, który gwarantuje, że zakładany poziom bezpieczeństwa będzie utrzymywany jedynie pod warunkiem przestrzegania tej częstości.

Opisane tu zasady postępowania to przykłady możliwości poprawienia przez użytkownika skuteczności stosowanych systemów realizujących funkcje bezpieczeństwa. Najważniejsze jest jednak ścisłe przestrzeganie wszystkich zaleceń producenta w całym cyklu życia systemu. Wszelkie odstępstwa prowadzą bowiem do zmniejszenia pewności realizacji funkcji bezpieczeństwa zaprojektowanej przez producenta systemu, a w konsekwencji do podniesienia poziomu ryzyka.

4.2.7. Parametry określające skuteczność wykrywania uszkodzeń

Opisane wcześniej metody wykrywania uszkodzeń charakteryzują się różną skutecznością. Zależy ona od wielu czynników decydujących zarówno o tym, kiedy uszkodzenie zostanie wykryte, jak i o tym, czy w ogóle zostanie wykryte. Każda metoda wykrywania defektów może więc być opisana za pomocą jej najważniejszych parametrów. Zalicza się do nich:

– pokrycie diagnostyczne *DC* (ang. *diagnostic coverage*)
– częstotliwość sprawdzeń, f_d.

Parametry te odnoszą się zarówno do autotestów realizowanych automatycznie przez system, jak i do sprawdzeń wykonywanych przez użytkownika. W przypadku sprawdzeń okresowych, wykonywanych stosunkowo rzadko, wygodniej jest używać czasu pomiędzy sprawdzeniami jako charakteryzującego je parametru. Zazwyczaj stosuje się następujące oznaczenia:

– T_1 – czas pomiędzy okresowymi sprawdzeniami (w godzinach)
– *MTTR* – średni czas pomiędzy wyłączeniami (w godzinach).

Zarówno częstotliwość autotestów, f_d, jak i T_1 i *MTTR* są parametrami charakterystycznymi urządzenia i ich wartości powinny być podawane przez producenta. Podawane powinno być także pokrycie diagnostyczne, *DC*, dla poszczególnych testów. Parametr ten wskazuje, jaki procent wszystkich uszkodzeń stanowią uszkodzenia, które mogą być wykryte. Przy określaniu jego wartości powinno się uwzględniać jedynie uszkodzenia potencjalnie niebezpieczne. Tak więc pokrycie diagnostyczne wyznacza się według wzoru:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{\text{total}}} \tag{4.1}$$

gdzie:

λ_{DD} – prawdopodobieństwa wystąpienia uszkodzeń potencjalnie niebezpiecznych, które zostaną wykryte

λ_{total} – prawdopodobieństwa wystąpienia wszystkich uszkodzeń potencjalnie niebezpiecznych.

Szczegółowe zasady ustalania wartości *DC* podano w normie PN-EN 61508-6:2010, zał. C.

Oceniając skuteczność metod diagnostycznych, należy przyjąć założenie, że uszkodzenie potencjalnie niebezpieczne, które nie zostało wykryte podczas przeprowadzonego testu, jest uszkodzeniem niebezpiecznym. Wynika to stąd, że powtórne przeprowadzenie tego samego testu zazwyczaj daje taki sam rezultat, a więc uszkodzenie to nie zostanie wykryte także po wielokrotnym testowaniu. Wyjątkiem od tej reguły jest specjalny zbieg okoliczności zewnętrznych, w których uszkodzenie to może ujawnić się bez stwarzania zagrożenia. Są to jednak sytuacje wyjątkowe i w praktyce można je pominąć. Tak więc, uszkodzenie potencjalnie niebezpieczne należy zakwalifikować jako uszkodzenie niebezpieczne, jeśli po przeprowadzeniu wszystkich przewidzianych przez producenta testów i sprawdzeń nie zostanie ono wykryte.

Rozdział 5

Przegląd metod oceny probabilistycznej systemów przemysłowych

5.1. Wprowadzenie

W dostępnej literaturze problematyka oceny probabilistycznej systemów przemysłowych nie jest zbyt rozpowszechniona. Najważniejsze dostępne publikacje to opracowania Kalbfleischa i Prentice'a (1980) oraz Lawlessa (2003). W języku polskim literatura przedmiotu jest, niestety, bardzo uboga. Najbardziej zwartego przeglądu, ukierunkowanego na problematykę bezpieczeństwa funkcjonalnego takich metod, dokonali Hryniewicz i Lewin (2008) oraz Dźwiarek (2008a). Stwierdzają oni, że systemy techniczne realizujące funkcje bezpieczeństwa podlegają uszkodzeniom, których momentu wystąpienia nie da się przewidzieć. W związku z tym czas do wystąpienia takiego uszkodzenia jest zawsze zmienną losową, którą będziemy oznaczać dużą literą T. Jeżeli uszkodzenie wystąpi, to zgodnie z powszechnie przyjętą konwencją zaobserwowany czas do uszkodzenia, stanowiący realizację zmiennej losowej T, będziemy oznaczać małą literą t. Warto tu podkreślić, że losowość czasu do uszkodzenia, a także ogólny sposób jej opisu, nie zależą od mechanizmu wystąpienia takiego uszkodzenia. Mechanizm ten może mieć jednak wpływ na sposób opisu konkretnych rodzajów uszkodzeń.

Właściwym narzędziem służącym do opisu zjawisk losowych są rozkłady prawdopodobieństwa. W analizie niezawodności stosuje się tylko niektóre z nich, zwłaszcza te, których charakterystyki pozwalają na ich dopasowanie do opisu mechanizmów uszkodzeń. Podstawowe rozkłady stosowane w opisie niezawodnościowym elementów systemów technicznych mogą być wykorzystane w praktyce tylko wtedy, kiedy potrafimy je zidentyfikować na podstawie dostępnych danych statystycznych, tzn. określić ich postać funkcyjną i oszacować ich nieznane parametry.

5.2. Ogólny sposób opisu zjawisk losowych

Wspomniane wcześniej zmienne losowe służą do liczbowego opisu zdarzeń losowych. Rozróżnia się zmienne losowe dyskretne, mogące przyjmować przeliczalne (skończone lub nieskończone) zbiory możliwych wartości, zmienne ciągłe, przyjmujące wartości należące do zbioru liczb rzeczywistych, oraz mieszane zmienne dyskretno-ciągłe. Warto podkreślić, że w analizie systemów sterowania realizujących funkcje bezpieczeństwa występują zmienne losowe wszystkich tych rodzajów. Jednakże ze względu na konieczność praktycznego upraszczania wyników przeprowadzanych analiz w tej pracy ograniczono się do rozpatrywania wyłącznie przypadków ciągłych i dyskretnych.

Podstawową charakterystyką opisującą zmienną losową jest jej rozkład prawdopodobieństwa jednoznacznie zdefiniowany za pomocą funkcji zwanej dystrybuantą i definiowanej jako:

$$F(x) = P(X \le x) \tag{5.1}$$

Znajomość postaci funkcji $F(x)$ w sposób jednoznaczny determinuje wszystkie informacje, jakie posiadamy o interesującej nas zmiennej losowej X. W przypadku zmiennych losowych dyskretnych każdą dystrybuantę można przedstawić w następującej postaci:

$$F(x) = P(X \le x) = \sum_{x_i \le x} P(X = x_i), \ i = 0,1,..... \tag{5.2}$$

Funkcja $P(X = x_i)$, która jest nazywana funkcją prawdopodobieństwa, mówi o prawdopodobieństwie zaobserwowania konkretnej realizacji rozpatrywanej zmiennej losowej. W interesujących nas zagadnieniach bezpieczeństwa i niezawodności rozkłady dyskretnych zmiennych losowych, zwane także dyskretnymi rozkładami prawdopodobieństwa, będą wykorzystywane do opisu takich wielkości losowych, jak liczba uszkodzeń w zadanym przedziale czasu, liczba ukrytych błędów w zainstalowanym oprogramowaniu itp. W przypadku zmiennych losowych ciągłych dystrybuantę można przedstawić w następujący sposób:

$$F(x) = P(X \le x) = \int_{-\infty}^{x} f(x)dx \tag{5.3}$$

gdzie funkcja $f(x)$ jest nazywana **funkcją gęstości prawdopodobieństwa** lub, w skrócie, funkcją gęstości. Interpretacja funkcji gęstości jest oczywista, gdy znane jest pojęcie histogramu. Jest to bowiem granica, do której dąży histogram wraz ze wzrostem liczby reprezentowanych przezeń danych. Rozkłady ciągłych zmiennych losowych, zwane także ciągłymi rozkładami prawdopodobieństwa, są

wykorzystywane do opisu wszelkich zdarzeń losowych mających wymiar czasu, a więc np. do opisu czasu do wystąpienia uszkodzenia.

Zmienne losowe są również opisywane pewnymi charakterystykami liczbowymi, zwanymi momentami: zwykłymi i centralnymi. W przypadku zmiennych losowych dyskretnych momenty zwykłe są definiowane zależnością:

$$m_k = \sum_i x_i^k \, p(X = x_i), \, k = 1, 2, ... \tag{5.4}$$

Z kolei, w przypadku zmiennych losowych ciągłych, momenty zwykłe wyznacza się z zależności:

$$m_k = \int_{-\infty}^{\infty} x^k \, f(x)dx, \, k = 1, 2, ... \tag{5.5}$$

W obu przypadkach wymagana jest zbieżność odpowiednich sum i całek, co nie zawsze ma miejsce. Momenty centralne są w przypadku rozkładów dyskretnych wyznaczane z zależności:

$$\mu_k = \sum_i (x_i - m_1)^k P(X = x_i), \, k = 1, 2, ... \tag{5.6}$$

a w przypadku rozkładów ciągłych z zależności:

$$\mu_k = \int_{-\infty}^{\infty} (x - m_1)^k \, f(x)dx, \, k = 1, 2, .. \tag{5.7}$$

Szczególnie ważnymi momentami są: moment zwykły pierwszego rzędu, m_1, zwany **wartością oczekiwaną** i oznaczany często jako $E(X)$, oraz moment centralny drugiego rzędu, μ_2, zwany **wariancją** i oznaczany często jako $V(X)$. Wartość oczekiwana jest także nazywana wartością średnią i jest jedną z miar położenia rozkładu. Wariancja, a także związana z nią zależnością $\sigma = \sqrt{V(x)}$ charakterystyka zwana **odchyleniem standardowym**, są miarami rozrzutu wartości zmiennej losowej wokół jej wartości oczekiwanej.

W praktyce korzysta się również z kilku innych liczbowych charakterystyk zmiennych losowych. Należy do nich **współczynnik asymetrii** definiowany jako:

$$\lambda = \frac{\mu_3}{(\sqrt{\mu_2})^3} \tag{5.8}$$

W przypadku symetrycznych rozkładów prawdopodobieństwa współczynnik asymetrii ma wartość równą zeru. Jeśli występuje tzw. asymetria prawostronna, odznaczająca się częstszym występowaniem dużych wartości rozpatrywanej zmiennej losowej, współczynnik asymetrii przyjmuje wartości dodatnie. Z kolei, jeśli jest to tzw. asymetria lewostronna, odznaczająca się częstszym występowaniem

małych wartości rozpatrywanej zmiennej losowej, współczynnik asymetrii przyjmuje wartości ujemne.

Inną ważną charakterystyką zmiennej losowej jest jej wartość modalna, oznaczana zazwyczaj jako $Mo(X)$. W przypadku zmiennych losowych dyskretnych jest to wartość, która występuje z największym prawdopodobieństwem, a więc najczęściej. Wartość modalna dla zmiennych losowych dyskretnych odpowiada tej wartości zmiennej losowej, dla której funkcja gęstości prawdopodobieństwa osiąga maksimum.

Kolejną ważną charakterystyką zmiennej losowej jest jej **kwantyl rzędu β,** oznaczany zazwyczaj jako x_β, definiowany zależnościami:

$$P(x \le x_\beta) \ge \beta \qquad \text{oraz} \qquad P(x \ge x_\beta) \ge 1-\beta \tag{5.9}$$

gdzie $0 < \beta < 1$.

Dla rozkładów ciągłych definicja (5.9) sprowadza się do jednego równania:

$$F(x_\beta) = \beta \tag{5.10}$$

Szczególnym przypadkiem kwantyla jest **mediana** zmiennej losowej, oznaczana zazwyczaj jako $Me(X)$, będąca kwantylem rzędu $\beta = 0{,}5$.

Przypomniane tu podstawowe charakterystyki liczbowe zmiennych losowych wykorzystuje się do oceny niezawodności i efektywności systemów zapewnienia bezpieczeństwa, jeśli dostępne dane statystyczne są niepełne. Na zakończenie tego podrozdziału wprowadźmy charakterystykę ciągłego rozkładu prawdopodobieństwa zmiennej losowej T (oznaczającej zazwyczaj losowy czas), która jest szczególnie często wykorzystywana w badaniu i ocenie niezawodności urządzeń technicznych. Charakterystyką tą jest funkcja ryzyka $h(t)$, w starszej literaturze nazywana także funkcją intensywności uszkodzeń, definiowana jako:

$$h(t) = \lim_{\Delta t \to 0} \frac{P(t \le T \le t + \Delta t \mid T > t)}{\Delta t} = \frac{f(t)}{1 - f(t)} = \frac{f(t)}{R(t)} = -\frac{d}{dt} \ln R(t) \tag{5.11}$$

Okazuje się, że istnieje istotny związek pomiędzy rodzajem mechanizmu powstawania uszkodzeń a charakterem przebiegu funkcji $h(t)$.

Analizując zależność (5.11), można zauważyć, że funkcja $h(t)$ jest związana ze **średnim prawdopodobieństwem wystąpienia uszkodzenia w jednostce czasu**, a więc charakterystyką zalecaną w normach międzynarodowych do oceny jakości systemów realizujących funkcję bezpieczeństwa. Z analizy wzoru (5.11) wynika bowiem, że funkcja ryzyka $h(t)$ jest ilorazem warunkowego prawdopodobieństwa wystąpienia uszkodzenia w pewnym (krótkim) przedziale czasu oraz długości tego przedziału. Warto zauważyć, że w ogólnym przypadku jest to wartość zależna od

czasu. Wartość stałą funkcja $h(t)$ przyjmuje tylko w jednym przypadku: rozkładu wykładniczego – opisanego w następnym podrozdziale. Można jednak wyznaczyć jej wartość średnią w przedziale czasu, np. $[a,b]$, z zależności:

$$h_{[a,b]} = \frac{\int_a^b h(t)dt}{b-a} \tag{5.12}$$

Niekiedy można spotkać się z interpretacją, że średnim prawdopodobieństwem wystąpienia uszkodzenia w jednostce czasu jest *odwrotność oczekiwanego czasu do uszkodzenia*.

5.3. Podstawowe rozkłady prawdopodobieństwa stosowane w analizie niezawodności i bezpieczeństwa

5.3.1. Wprowadzenie

Do matematycznego opisu niezawodności (a szczególnie nieuszkadzalności) obiektów technicznych, a w tym elementów systemów sterowania, można stosować wiele znanych rozkładów prawdopodobieństwa. W praktyce ograniczamy się jednak tylko do niektórych z nich. Stosowane są dwa podstawowe kryteria wyboru:

- istnienie możliwie prostych metod statystycznych, umożliwiających wnioskowanie o niezawodności opisywanych przez dany rozkład obiektów na podstawie dostępnych danych statystycznych
- możliwość zinterpretowania pewnych charakterystyk rozkładu w terminach opisu mechanizmów uszkodzeń, które można modelować za pomocą takiego rozkładu.

Dalej zostaną zaprezentowane rozkłady prawdopodobieństwa, które są najczęściej wykorzystywane w praktyce niezawodnościowej. Zastosowano jednolity schemat prezentacji obejmujący opis rozkładu oraz jego podstawowych charakterystyk, a następnie wskazanie obszarów, w których dany rozkład może być stosowany.

5.3.2. Rozkład wykładniczy

Jest to podstawowy rozkład prawdopodobieństwa wykorzystywany w badaniach niezawodności do opisu losowych czasów do wystąpienia uszkodzenia lub czasów pomiędzy kolejnymi uszkodzeniami. Dokładniej biorąc, te czasy odnoszą się do najważniejszego składnika niezawodności, jakim jest *nieuszkadzalność* (inne losowe czasy mogą odnosić się do *obsługiwalności*, która jest też składową niezawodności).

Rozkład wykładniczy jest zdefiniowany za pomocą dystrybuanty:

$$F(t)=\begin{cases}0 & t<0\\ 1-\mathrm{e}^{-\lambda t} & t\geq 0\end{cases} \tag{5.13}$$

gdzie parametr $\lambda > 0$ można interpretować jako „intensywność" występowania pewnych zdarzeń losowych mierzoną liczbą zdarzeń w jednostce czasu. W zastosowaniach niezawodnościowych zdarzeniami tymi są zazwyczaj uszkodzenia opisywanych obiektów, a parametr λ jest wtedy nazywany *intensywnością uszkodzeń*. Należy jednak podkreślić, że nawet w zastosowaniach niezawodnościowych nie jest to jedyna możliwa jego interpretacja.

Funkcja gęstości rozkładu wykładniczego jest opisana zależnością:

$$f(t)=\begin{cases}0 & t<0\\ \lambda\mathrm{e}^{-\lambda t} & t\geq 0\end{cases} \tag{5.14}$$

a funkcja ryzyka, $h(t)$, zdefiniowana zależnością (5.11), przyjmuje stałą, niezależną od czasu, wartość równą λ, najczęściej zwaną – jak już wspomniano – intensywnością uszkodzeń.

Zmienna losowa o rozkładzie wykładniczym ma wartość oczekiwaną równą $E(t)=1/\lambda$ oraz wariancję $V(t)=1/\lambda^2$. Rozkład wykładniczy jest jedynym rozkładem ciągłej zmiennej losowej, dla którego wartość oczekiwana jest równa jego odchyleniu standardowemu (pierwiastkowi kwadratowemu z wariancji). Warto ponadto zwrócić uwagę, że w przypadku rozkładu wykładniczego wspomniane w poprzednim podrozdziale charakterystyki związane z wielkością nazywaną *średnim prawdopodobieństwem uszkodzenia w jednostce czasu* przyjmują tę samą wartość równą λ. Należy także podkreślić, że jest to jedyny rozkład prawdopodobieństwa, dla którego taka właściwość występuje. Rozkład wykładniczy ma pewne cechy wyróżniające go spośród innych rozkładów prawdopodobieństwa. Należy o nich pamiętać, gdyż często jest on stosowany w sytuacjach, w których nie powinien być wykorzystywany. Podstawową właściwością rozkładu wykładniczego jest „brak pamięci" wyrażający się zależnością:

$$P(T \geq t+s/T \geq t) = P(T \geq s) \tag{5.15}$$

Oznacza to, że każdy obiekt opisany rozkładem wykładniczym, po stwierdzeniu jego stanu zdatności, należy traktować jako obiekt „nowy". Innymi słowy, czas dotychczasowej eksploatacji takiego obiektu *nie* wpływa na prawdopodobieństwo wystąpienia uszkodzenia w trakcie jego dalszej eksploatacji. Mówi się wówczas o braku występowania *efektu starzenia*, czego przejawem jest stałość w czasie funkcji ryzyka (intensywności uszkodzeń). Rozpatrując rozkład wykładniczy pod kątem

jego związku z możliwymi mechanizmami uszkodzeń, można łatwo zauważyć, że powinien on występować wtedy, kiedy uszkodzenia są wynikiem pojawiających się w sposób czysto przypadkowy obciążeń (używa się też określenia „szoków"), które swoją wielkością przekraczają wytrzymałość (stałą!) obiektu na takie obciążenia. W praktyce przyjmuje się, że właściwość ta może występować w tzw. normalnych okresach eksploatacji, gdy przeminie już okres wczesnych uszkodzeń „wieku dziecięcego", a nie wystąpią jeszcze efekty starzeniowe. W normie PN-EN ISO 13849-1:2008 przyjmuje się, że w pewnych sytuacjach za taki okres można uznać 20 lat eksploatacji systemów sterowania. Należy jednak podkreślić, że zauważa się tam również nieadekwatność tego założenia w odniesieniu do mechanicznych elementów takich systemów. Zgodnie z właściwą metodyką postępowania przyjmowane wstępnie (zwykle we wczesnej fazie projektowania) założenie o stałej intensywności uszkodzeń powinno być zweryfikowane, jak tylko pojawią się odpowiednie dane z badań empirycznych (testów niezawodnościowych).

5.3.3. Rozkład Weibulla

Rozkład Weibulla jest drugim najczęściej spotykanym w badaniach niezawodności rozkładem prawdopodobieństwa. Jest definiowany za pomocą następującej dystrybuanty:

$$F(t)=\begin{cases} 0 & t<0 \\ 1-\mathrm{e}^{-\lambda t^{\delta}}=1-\mathrm{e}^{-(\frac{t}{\Theta})^{\delta}} & t\geq 0 \end{cases} \tag{5.16}$$

Parametr $\delta > 0$ jest nazywany parametrem kształtu, a parametr $\Theta > 0$ *parametrem skali* rozkładu Weibulla. Parametr λ, jeżeli jest używany, nie ma swojej specyficznej nazwy (należy tu podkreślić, że w ogólnym przypadku nie ma on interpretacji „intensywności"). Funkcja gęstości rozkładu Weibulla dana jest zależnością:

$$f(t)=\begin{cases} 0 & t<0 \\ \delta\lambda t^{\delta-1}\mathrm{e}^{\lambda t^{\delta}}=\dfrac{\delta}{\Theta}(\dfrac{t}{\Theta})^{\delta-1}\mathrm{e}^{-(\frac{t}{\Theta})^{\delta}} & t\geq 0 \end{cases} \tag{5.17}$$

Przyglądając się zależnościom (5.16) i (5.17), łatwo zauważyć, że rozkład Weibulla jest uogólnieniem rozkładu wykładniczego, który jest jego szczególnym przypadkiem, gdy parametr kształtu, δ, jest równy 1.

Zmienna losowa o rozkładzie Weibulla ma wartość oczekiwaną równą:

$$E(T)=\Theta\Gamma(\frac{1}{\delta}+1) \tag{5.18}$$

gdzie funkcja gamma $\Gamma(T)$ dana jest zależnością:

$$\Gamma(x) = \int_0^\infty t^{x-1} \mathrm{e}^{-t} dt, \; x > 0 \tag{5.19}$$

Wariancja zmiennej losowej o rozkładzie Weibulla wynosi:

$$V(T) = \Theta^2[\Gamma(\frac{2}{\delta}+1) - \Gamma^2(\frac{1}{\delta}+1)] \tag{5.20}$$

Funkcja ryzyka $h(t)$ rozkładu Weibulla dana jest następującą zależnością:

$$h(t) = \begin{cases} 0 & t < 0 \\ \delta\lambda t^{\delta-1} = \dfrac{\delta}{\Theta}(\dfrac{t}{\Theta})^{\delta-1} & t \geq 0 \end{cases} \tag{5.21}$$

Gdy parametr kształtu δ przyjmuje wartości mniejsze od 1, funkcja ryzyka $h(t)$ dana wzorem (5.21) maleje monotonicznie od ∞ (dla t dążącego do 0) do 0 (dla t dążącego do ∞). Z kolei, gdy parametr kształtu δ przyjmuje wartości większe od 1, funkcja ryzyka $h(t)$ rozkładu Weibulla rośnie monotonicznie od 0 (dla $t = 0$) do ∞ (dla t dążącego do ∞). Oczywiście, gdy $\delta = 1$, mamy do czynienia z rozkładem wykładniczym i funkcja ryzyka przyjmuje wartość stałą, równą $\lambda = 1/\Theta$. Warto ponadto zwrócić uwagę, że w przypadku rozkładu Weibulla wartość funkcji ryzyka uśredniona w przedziale $[0, t]$ jest równa dokładnie $h(t)/\delta$. Oznacza to, że funkcja ryzyka rozkładu Weibulla, uśredniona w przedziale $(0, \infty)$, może przyjmować trzy wartości: 0 (gdy $\delta < 1$), λ (gdy $\delta = 1$) oraz ∞ (gdy $\delta > 1$).

Rozkład Weibulla zawdzięcza swoją popularność temu, że można go wykorzystać do modelowania różnych mechanizmów powstawania uszkodzeń. Przypadek malejącej w czasie funkcji ryzyka odpowiada sytuacji, gdy występują wczesne uszkodzenia „wieku dziecięcego". Z kolei, przypadek rosnącej w czasie funkcji ryzyka odpowiada sytuacji, gdy występują efekty starzeniowe, powodujące z upływem czasu pogarszanie się właściwości niezawodnościowych. Można również pokazać, że mieszanina dwu rozkładów Weibulla (jednego o malejącej, a drugiego o rosnącej funkcji ryzyka) może być wykorzystywana do modelowania przypadków, w których najpierw dominują uszkodzenia o mechanizmie typowym dla uszkodzeń wczesnych, a następnie dominują uszkodzenia o mechanizmie typowym dla uszkodzeń starzeniowych.

5.3.4. Rozkład logarytmo-normalny

Podstawowym rozkładem prawdopodobieństwa, który jest stosowany do opisu ciągłych zmiennych losowych, jest rozkład normalny. Nie ma on jednak szerokiego

zastosowania w praktyce niezawodnościowej. Są ku temu dwa ważne powody: teoretyczny i praktyczny. Przede wszystkim, rozkład normalny jest określony na całej osi liczb rzeczywistych, a więc może nie być odpowiedni do modelowania czasu, który jest wielkością nieujemną. Niektórzy autorzy zauważają, że jeśli wartość oczekiwana w rozkładzie normalnym, μ, jest wyraźnie większa od trzech jego odchyleń standardowych, σ, to rozkład normalny z bardzo dobrym przybliżeniem może opisywać wielkości nieujemne. W takich sytuacjach przeszkodą w stosowaniu rozkładu normalnego są trudności w wyznaczaniu ważnych charakterystyk niezawodnościowych. Trudności takich nie sprawia omówiony wcześniej rozkład Weibulla, który może stanowić dobre przybliżenie rozkładu normalnego.

W przeciwieństwie do rozkładu normalnego, w praktyce niezawodności stosowany jest ściśle z nim powiązany rozkład *logarytmo-normalny*, zwany też rozkładem logarytmiczno-normalnym lub, w skrócie, rozkładem lognormalnym. Mówimy, że zmienna losowa T ma rozkład logarytmo-normalny, gdy jej *logarytm* ma *rozkład normalny*. Zazwyczaj przyjmuje się, że jest to logarytm o podstawie naturalnej e, ale można także stosować przekształcenia logarytmiczne o innej podstawie, na przykład dziesiętnej.

Rozkład logarytmo-normalny może być formalnie zdefiniowany za pomocą następującej dystrybuanty:

$$F(t)=\begin{cases}0 & t<0\\ \Phi\left(\dfrac{\ln t-\mu}{\sigma}\right) & t\geq 0\end{cases} \tag{5.22}$$

gdzie funkcja $\Phi(t)$ jest zdefiniowana jako:

$$\Phi(t)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t}\mathrm{e}^{-\frac{u^2}{2}}du \tag{5.23}$$

Funkcja gęstości zmiennej losowej o rozkładzie logarytmo-normalnym dana jest zależnością:

$$f(t)=\begin{cases}0 & t<0\\ \dfrac{1}{\sigma t\sqrt{2\pi}}\mathrm{e}^{-\frac{1}{2}\left(\frac{\ln t-\mu}{\sigma}\right)^2} & t\geq 0\end{cases} \tag{5.24}$$

Występujące we wzorach (5.22) i (5.24) μ i σ mają oczywistą interpretację: μ jest wartością oczekiwaną logarytmu czasu T, a σ jest odchyleniem standardowym logarytmu czasu T. Jeżeli jednak rozpatruje się oryginalną skalę czasu, to odpowiednie charakterystyki wyrażają się bardziej skomplikowanymi zależnościami.

Wartość oczekiwana zmiennej losowej o rozkładzie logarytmo-normalnym dana jest zależnością:

$$E(T) = \mathrm{e}^{\mu+\sigma^2/2} \tag{5.25}$$

jej wariancja zaś zależnością:

$$V(T) = (\mathrm{e}^{\sigma^2} - 1)\mathrm{e}^{2\mu+\sigma^2} \tag{5.26}$$

Funkcja ryzyka $h(t)$ w przypadku rozkładu logarytmo-normalnego nie ma, niestety, prostej postaci. W celu jej wyznaczenia należy skorzystać z definicji danej wzorem (5.11) oraz ze wzorów (5.22) i (5.24). Ma ona jednak bardzo przydatną w praktyce modelownia niezawodnościowego właściwość – jest funkcją o jednym maksimum w punkcie t^* stanowiącym rozwiązanie równania:

$$h(t^*) = \frac{1}{\sigma^2 t^*}(\sigma^2 + \ln t^* - \mu) \tag{5.27}$$

Można pokazać, że wartość t^* spełnia następujący warunek:

$$\exp(\mu - \sigma^2) \le t^* \le \exp(\mu - \sigma^2 + 1) \tag{5.28}$$

Ta właściwość rozkładu logarytmo-normalnego sprawia, że bardzo dobrze nadaje się on do modelowania *losowych czasów naprawy* uszkodzonych obiektów. Z praktyki wiadomo bowiem, że intensywność napraw na początku rośnie, a później maleje, co odpowiada sytuacjom napraw wymagających bardzo długiego czasu. Można również znaleźć przypadki, w których w podobny sposób zachowuje się funkcja intensywności uszkodzeń, odzwierciedlająca mechanizm ich powstawania.

5.3.5. Rozkład gamma

Omówiony uprzednio rozkład Weibulla odznacza się monotonicznie malejącymi (rosnącymi) funkcjami ryzyka. Jednakże, jeśli funkcja ryzyka maleje, to maleje ona do zera, a jeśli rośnie to do nieskończoności. W pewnych przypadkach właściwość ta może być niekorzystna. Nie ma jej natomiast *rozkład gamma* definiowany za pomocą dystrybuanty:

$$F(t) = \begin{cases} 0 & t < 0 \\ I(k, \lambda t) & t \ge 0 \end{cases} \tag{5.29}$$

gdzie funkcja $I(k, \lambda t)$, nazywana niekompletną *funkcją gamma*, jest zdefiniowana jako:

$$I(k,\lambda t)=\frac{1}{\Gamma(k)}\int_0^{\lambda t}u^{k-1}\mathrm{e}^{-u}du \tag{5.30}$$

przy czym funkcja $\Gamma(k)$ dana jest wzorem (5.19). Funkcję gęstości zmiennej losowej o rozkładzie gamma opisuje zależność:

$$f(t)=\begin{cases}0 & t<0\\ \dfrac{\lambda(\lambda t)^{k-1}}{\Gamma(k)}\mathrm{e}^{-t} & t\geq 0\end{cases} \tag{5.31}$$

Wartość oczekiwana zmiennej losowej o rozkładzie gamma dana jest zależnością:

$$E(T)=\lambda^{-1}k \tag{5.32}$$

a jej wariancja:

$$V(T)=\lambda^{-2}k \tag{5.33}$$

Jak łatwo zauważyć, gdy $k = 1$, rozkład gamma sprowadza się do znanego już *rozkładu wykładniczego*. Jest to konsekwencja ważnej właściwości rozkładu gamma, dzięki której ma on wiele zastosowań: suma k niezależnych zmiennych losowych o jednakowym rozkładzie wykładniczym opisanym parametrem λ ma rozkład gamma o parametrach k oraz λ. W takim przypadku parametr k jest liczbą całkowitą, a rozkład gamma nazywany jest *rozkładem Erlanga*. Funkcja ryzyka $h(t)$ w przypadku rozkładu gamma musi być wyznaczana z definicji podanej wzorem (5.11) oraz, odpowiednio, ze wzorów (5.29) i (5.31). Można pokazać, że jeśli $k > 1$ (tak jak to jest np. w przypadku rozkładu Erlanga), to funkcja ryzyka monotonicznie rośnie od zera do wartości λ. Z kolei, gdy $k < 1$ (wówczas zamiast k używa się zazwyczaj symboli α lub p), funkcja ryzyka maleje od ∞ do λ. Gdy $k = 1$ występuje oczywiście przypadek rozkładu wykładniczego i $h(t) = \lambda$.

Przedstawione tu metody oceny intensywności uszkodzeń przypadkowych, zdefiniowanej wzorem (5.11), należą do najbardziej rozpowszechnionych w praktyce. Stanowiły one także podstawę teoretyczną do formułowania zasad bezpieczeństwa funkcjonalnego związanych z bezpieczeństwem systemów sterowania.

Rozdział 6

Modelowanie systemów sterowania maszynami metodą Markova

6.1. Wprowadzenie

Z rozważań zamieszczonych w rozdziale 4 wynika, że poszczególne środki zapobiegania defektom różnią się skutecznością. Powstaje więc problem oceny tej skuteczności. Ponieważ celem jest zapobieganie defektom niebezpiecznym, więc ocena związanego z bezpieczeństwem systemu sterowania powinna się odnosić do prawdopodobieństwa wystąpienia defektu niebezpiecznego. Ocenę taką można przeprowadzać różnymi metodami. Osoba oceniająca system powinna wybrać metodę najwłaściwszą w konkretnym przypadku. Można jednak stwierdzić, że obecnie najbardziej rozpowszechnione i najskuteczniejsze są:

- metoda drzewa defektów FTA (PN-EN 61025:2007)
- analiza rodzajów uszkodzeń i ich skutków FMEA (PN-EN 60812:2009)
- metoda grafów Markova (PN-EN 61165:2006)
- metoda HAZOP (PN-IEC 61882:2005).

Często stosuje się także kombinacje tych metod. Dobór metody analizy zależy od stopnia złożoności systemu oraz posiadanych danych statystycznych dotyczących zastosowanych podzespołów.

Wśród systemów sterowania realizujących funkcje bezpieczeństwa wyodrębnia się dwie grupy, różniące się rodzajem informacji, jakie można uzyskać o występujących w nich defektach. Są to systemy typu A i systemy typu B.

Sposób postępowania podczas oceny systemu sterowania maszynami związanego z bezpieczeństwem zależy od typu systemu.

Systemy typu A. Element systemu sterowania związany z bezpieczeństwem może być traktowany jako typu A, jeśli są spełnione wszystkie wymienione warunki:

- możliwe uszkodzenia wszystkich elementów składowych są dobrze zdefiniowane

– zachowanie się podsystemu w warunkach defektu może być całkowicie określone
– dostępne są wystarczająco pewne dane z doświadczeń eksploatacyjnych dotyczące uszkodzeń, służące do wykazania, że deklarowane intensywności uszkodzeń dla wykrytych i niewykrytych uszkodzeń niebezpiecznych są spełnione.

Systemami typu A są więc systemy, o których mamy pełną wiedzę i możemy przewidzieć wszystkie możliwe ich defekty oraz określić, jak system zachowa się po wystąpieniu tych defektów. Warunki te są zazwyczaj spełnione w przypadku niezbyt złożonych systemów elektromechanicznych, a także prostych systemów elektronicznych.

Z definicji wynika, że analiza urządzeń typu A powinna się opierać na identyfikacji poszczególnych możliwych uszkodzeń oraz określaniu prawdopodobieństwa ich wystąpienia i zachowania systemu. Do tego celu najbardziej odpowiednia jest analiza metodą FTA lub FMEA.

Systemy typu B. Element systemu sterowania związany z bezpieczeństwem powinien być traktowany jako typu B, jeśli nie jest spełniony którykolwiek z warunków kwalifikacji do typu A. Oznacza to, że system jest typu B, jeśli:

– nie można jednoznacznie zdefiniować defektu co najmniej jednego jego elementu lub
– nie można jednoznacznie określić, jak system zachowa się w razie jakiegoś jego defektu, lub
– nie dysponujemy wystarczająco pewnymi danymi dotyczącymi intensywności uszkodzeń elementów systemu.

Systemami typu B są więc te, co do których nie można jednoznacznie stwierdzić, że dysponujemy pełną wiedzą o ich możliwych uszkodzeniach. Sytuacja taka występuje na przykład w przypadku systemów programowalnych, w których zastosowane są złożone podzespoły elektroniczne o strukturze na tyle skomplikowanej, że liczba potencjalnych defektów uniemożliwia poddanie ich szczegółowej analizie.

Z powodu niewystarczających danych dotyczących mikroprocesorów i układów scalonych wielkiej skali integracji systemy zawierające elementy tego rodzaju należy zaliczyć do typu B.

W przypadku urządzeń typu B nie jest możliwe zidentyfikowanie poszczególnych defektów. Analiza powinna się zatem opierać na określeniu zachowania systemu w warunkach uszkodzenia. Najbardziej odpowiednie są więc metody FMEA lub grafów Markova.

Metody drzewa defektów oraz analizy rodzajów uszkodzeń i ich skutków są szczegółowo opisane w literaturze i powszechnie stosowane od wielu lat. Natomiast zasady stosowania metody grafów Markova do analizy systemów programowalnych są mało znane i niezbyt rozpowszechnione. Dlatego też skupimy się przede

wszystkim na przedstawieniu tej metody. Jest to bardzo skuteczne narzędzie do analizy probabilistycznej systemów, które mogą przyjmować wiele różnych stanów. W ogólności, metodę tę stosuje się powszechnie do analizy wszelkiego rodzaju procesów.

Analiza systemów związanych z bezpieczeństwem powinna dotyczyć kwestii związanych z zachowanie systemu w warunkach defektu. Zasady stosowania grafów Markova do analizy systemów sterowania maszynami przedstawiono w opracowaniu STSARCES (2000) oraz w pracy Dźwiarka (2000c). Ponieważ analizy dotyczą zachowania się systemu sterowania w warunkach defektu, więc graf nie obejmuje stanów funkcjonalnych systemu, lecz stany dotyczące jego sprawności. Przykładami takich stanów są:

- brak uszkodzenia
- wykryte uszkodzenie podzespołu A, B itd.
- uszkodzenie od wspólnej przyczyny
- uszkodzenie niebezpieczne.

Analizę należy przeprowadzać w odniesieniu do przewidywanego czasu użytkowania systemu, T_M, rozumianego jako czas jego przydatności do realizacji funkcji związanych z bezpieczeństwem. Czas ten powinien być deklarowany przez producenta. Oczekiwanym rezultatem tej analizy jest określenie prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego w czasie 1 h (w systemach o trybie pracy ciągłej) lub na przywołanie (w systemach o trybie pracy „na przywołanie").

6.2. Ogólna charakterystyka modeli Markova

Pełny model Markova składa się z dwu elementów: zbioru możliwych stanów $\boldsymbol{\Psi}$ oraz macierzy przejść $\mathbf{P} = [p_{ij}]$. Zbiór stanów $\boldsymbol{\Psi}$ powinien być pełny, to znaczy powinien zawierać wszystkie możliwe stany. Definicje poszczególnych stanów powinny być rozłączne. Oznacza to, że stany powinny być definiowane tak, że w określonym czasie system pozostaje zawsze tylko w jednym stanie. Elementy macierzy **P** określają prawdopodobieństwa przejścia z jednego stanu do drugiego tak, że p_{ij} określa prawdopodobieństwo przejścia ze stanu *i*-tego do stanu *j*-ego. Ponieważ system zawsze znajduje w jednym ze stanów $\boldsymbol{\Psi}$, więc zgodnie z podstawową zasadą prawdopodobieństwa można napisać, że dla każdego *i*:

$$\sum_{j=1}^{n} p_{i,j} = 1 \tag{6.1}$$

gdzie *n* oznacza liczbę wszystkich stanów.

Zwykle model systemu jest przedstawiany w postaci graficznej. Przedstawienie takie, poprzez wizualizację, czyni model bardziej przejrzystym i ułatwia jego analizę.

Model graficzny jest zbudowany z okręgów reprezentujących poszczególne stany oraz linii opisujących możliwe przejścia pomiędzy nimi. Stany powinny być jednoznacznie opisane oraz oznaczone symbolami. Przejścia scharakteryzowane są prawdopodobieństwem ich zaistnienia. Podstawą modelu Markova jest założenie, że wszystkie przejścia zależą jedynie od stanu aktualnego oraz przypisanego im prawdopodobieństwa, a nie zależą od historii układu. W tym sensie mówi się , że są to modele „bez pamięci".

6.3. Czynnik czasu w modelu

Prawdopodobieństwa przejść p_{ij} zawsze są określane w odniesieniu do określonego przedziału czasu Δt. Powinien to być ten sam przedział dla wszystkich przejść w modelu. Właściwy dobór Δt ma istotne znaczenie dla skuteczności zastosowanego modelu. Czas ten powinien być wystarczająco mały, aby zidentyfikować wszystkie możliwe zjawiska w systemie, ale też nie powinien być zbyt mały, aby niepotrzebnie nie komplikować modelu. Zazwyczaj jako Δt przyjmuje się czas pomiędzy kolejnymi przywołaniami funkcji bezpieczeństwa lub pomiędzy kolejnymi autotestami, w zależności od tego, który jest mniejszy.

Niech $\boldsymbol{S}$ oznacza wektor stanu modelu:

$$S = [s_1, s_2, ..., s_n] \tag{6.2}$$

gdzie: s_i – prawdopodobieństwo osiągnięcia i-tego stanu.

Elementy wektora $\boldsymbol{S}$ zmieniają się wraz z upływem czasu. Jeśli ich aktualna wartość wynosi $\boldsymbol{S_k}$, to po upływie jednostki czasu Δt przyjmą wartość $\boldsymbol{S_{k+1}}$:

$$S_{k+1} = S_k \cdot \mathrm{P} \tag{6.3}$$

Rozpoczynając analizę systemu, zakładamy, że znajduje się on w jednym z możliwych stanów. W omawianym przypadku jest to zazwyczaj stan braku uszkodzeń. W tej sytuacji wektor stanu S_0 przyjmuje postać:

$$S_0 = [1, 0, ..., 0] \tag{6.4}$$

Na tej podstawie można określić wartości elementów wektora stanu po upływie czasu $k\Delta t$:

$$S_k = S_0 \cdot \mathrm{P}^k \tag{6.5}$$

System będzie oceniany na podstawie prawdopodobieństwa wystąpienia niebezpiecznego defektu w ciągu godziny lub pomiędzy przywołaniami. Tak więc k przyjmie odpowiednio wartości 1 h/Δt lub $1/(\Delta t \cdot f_p)$, gdzie f_p oznacza średnią częstotliwość przywołań.

6.4. Redukowanie liczby stanów modelu

Typowe układy elektroniczne składają się zazwyczaj z wielu elementów i podzespołów o różnym stopniu złożoności. Uwzględnienie w modelu wszystkich możliwych uszkodzeń wszystkich elementów prowadziłoby do znacznego jego rozbudowania. Model taki byłby całkowicie nieczytelny, a ponadto jego analiza wymagałaby użycia dużych mocy obliczeniowych i znacznego czasu. Na przykład, pełny model układu zbudowanego z 10 elementów zawierałby 2^{10} stanów, przy założeniu, że każdy element może ulec uszkodzeniu tylko w jeden sposób. Dlatego też w praktyce powinno się stosować modele uproszczone.

Podstawową zasadą modelu uproszczonego jest podzielenie całego systemu na kilka niezależnych podzespołów. Podzespoły powinny być określane na podstawie realizowanych funkcji, a także na podstawie działania systemów diagnostycznych. Najbardziej naturalnym podziałem jest na przykład wydzielenie poszczególnych gałęzi redundancji lub układów funkcjonalnych i monitorujących. Można także dokonać podziału na podzespoły według skutków uszkodzeń, tak aby elementy, których uszkodzenie powoduje taki sam skutek, należały do jednego podzespołu. Korzystnym podziałem jest również wydzielenie w systemie podzespołów o identycznej budowie.

W każdym wydzielonym podzespole należy wyznaczyć prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego. Jeśli podzespół można zaliczyć do typu A, to prawdopodobieństwo niebezpiecznego uszkodzenia określa się metodami FMEA (analiza rodzajów i skutków uszkodzeń, PN-EN 60812:2009) lub FTA (analiza drzewa niezdatności, PN-EN 60025:2007). Jeśli rozpatruje się podzespoły typu B, konieczne jest oszacowanie prawdopodobieństwa wystąpienia uszkodzenia na podstawie analizy zastosowanych środków wykrywania uszkodzeń.

6.5. Określanie prawdopodobieństwa uszkodzeń

Do określenia poszczególnych elementów macierzy przejść, **P**, konieczna jest znajomość prawdopodobieństwa uszkodzeń poszczególnych elementów lub podzespołów systemu. W praktyce, poza nielicznymi wyjątkami, możliwe jest jedynie oszacowanie wartości odpowiednich wskaźników niezawodnościowych.

Zazwyczaj producenci urządzeń i elementów elektronicznych prowadzą własne badania statystyczne mające na celu określenie wskaźników niezawodnościowych wytwarzanych produktów. Niejednokrotnie informacje takie są zamieszczane w danych technicznych urządzeń. Dostępne są także odpowiednie bazy danych. W razie braku szczegółowych danych dotyczących konkretnego elementu lub podzespołu można wykorzystać dane ogólne, określone dla elementów danego typu. W normie PN EN 61508-2:2010 zaleca się, aby zastosowane dane były wyznaczone na poziomie ufności co najmniej 70%. Uzyskane w ten sposób wskaźniki mogą stanowić podstawę do wyznaczenia prawdopodobieństwa uszkodzenia zastosowanych elementów.

Znane obecnie bazy danych zawierają przede wszystkim informacje o pojedynczych elementach elektronicznych i elektrotechnicznych, takich jak rezystory, kondensatory, elementy półprzewodnikowe czy przekaźniki. Można także zdobyć dane dotyczące układów scalonych. Najprostszym sposobem oszacowania prawdopodobieństwa uszkodzenia elementów lub podzespołów jest wykorzystanie deklarowanego przez producenta średniego czasu pracy bezawaryjnej (*MTTF*). W zasadzie w systemach związanych z bezpieczeństwem nie powinno się stosować elementów lub podzespołów, dla których producent nie podaje wskaźnika *MTTF*. W praktyce można jednak spotkać podzespoły specjalistyczne lub stosowane dopiero od niedawna, dla których nie ma wystarczających danych statystycznych. Można wówczas wykorzystać dane szacunkowe, typowe dla tego rodzaju podzespołów. W STSARCES (2000) przedstawiono dane wynikające z wieloletniego doświadczenia jednostek badających systemy bezpieczeństwa. Dane te podano w tabl. 6.1.

Rozkład prawdopodobieństwa uszkodzenia elementu o określonej wartości *MTTF* zmienia się w czasie, wzrastając wraz z upływem czasu eksploatacji. Efekt ten wprowadza dodatkowy czynnik znacznie komplikujący model. Równanie (6.5) sformułowano przy założeniu, że elementy macierzy **P** są niezmienne w czasie.

Tablica 6.1. Szacunkowe wartości *MTTF* typowych podzespołów elektronicznych (STSARCES, 2000)

Mikroprocesory	$MTTF_M$	15 lat
Układy watchdog (WD)	$MTTF_{WD}$	100 lat
Czujniki (S)	$MTTF_S$	15 lat
Siłowniki (silniki) (D)	$MTTF_D$	30 lat
Przekaźniki (R)	$MTTF_R$	50 lat
Układy scalone	$MTTF_U$	15 lat
Ścieżki sygnałów wyjściowych	$MTTF_P$	30 lat

Ponieważ jednak dostępne dane oraz prowadzone obliczenia są szacunkowe, można dla uproszczenia przyjąć równomierny rozkład prawdopodobieństwa uszkodzenia elementu w czasie od 0 do *MTTF*. Założenie takie w sposób ukryty zostało także przyjęte w PN-EN 61508-1:2010. Metody zalecane w tych dokumentach nie uwzględniają efektów starzenia się elementów i umożliwiają określenie wskaźników niezawodnościowych systemu jednorodnie dla jego całego przewidywanego czasu pracy T_M. Można więc przyjąć, że prawdopodobieństwo uszkodzenia elementu w przedziale czasu Δt wyniesie:

$$\lambda = \frac{\Delta t}{MTTF} \tag{6.6}$$

W ocenie systemu uwzględniane są tylko uszkodzenia niebezpieczne. Stanowią one jedynie część wszystkich możliwych uszkodzeń. Budując model systemu, należy rozważać wszystkie uszkodzenia niebezpieczne poszczególnych elementów i podzespołów. Będą to więc uszkodzenia powodujące utratę funkcji realizowanej przez dany podzespół lub element. Uszkodzenia takie są zazwyczaj są potencjalnie niebezpieczne dla całego systemu. Dlatego też wszystkie powinny być uwzględniane przy budowie modelu. Dopiero po analizie modelu można określić, które z niebezpiecznych uszkodzeń danego podzespołu są niebezpiecznymi uszkodzeniami systemu.

6.6. Przykłady modeli najczęściej spotykanych układów

6.6.1. Model układu jednokanałowego

We wszystkich systemach można wyróżnić typowe, najczęściej powtarzające się konfiguracje elementów i podzespołów. Model całego systemu zawiera więc

wiele typowych fragmentów połączonych w całość odpowiadającą konkretnemu systemowi. Dalej zaprezentowano modele najbardziej typowych konfiguracji układowych.

Najprostszym przypadkiem układu sterowania jest pokazany na rys. 6.1 system jednokanałowy. Układ taki składa się z czujników, układu logicznego i elementów wykonawczych. Niebezpieczne uszkodzenie dowolnego elementu jest jednocześnie uszkodzeniem niebezpiecznym całego systemu. Ponieważ uszkodzenia takie są wzajemnie niezależne, to prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego w systemie jest równe sumie prawdopodobieństw uszkodzeń poszczególnych elementów:

$$\lambda_D = \lambda_{DS} + \lambda_{DL} + \lambda_{DD} \tag{6.7}$$

gdzie:

λ_D – prawdopodobieństwo niebezpiecznego uszkodzenia systemu

λ_{DS} – prawdopodobieństwo niebezpiecznego uszkodzenia czujników

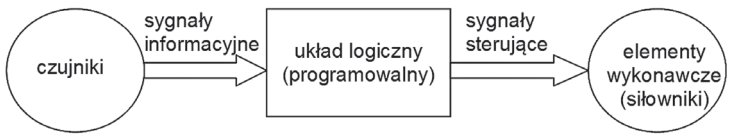
λ_{DL} – prawdopodobieństwo niebezpiecznego uszkodzenia układu logicznego

λ_{DD} – prawdopodobieństwo niebezpiecznego uszkodzenia elementów wykonawczych.

Układ taki może przyjmować tylko dwa stany:

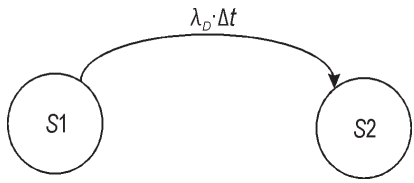
*S*1 – układ sprawny

*S*2 – układ uszkodzony.



Rys. 6.1. Układ o strukturze jednokanałowej

Każde uszkodzenie pojedynczego elementu jest niebezpieczne. Jednak w skali całego systemu niektóre rodzaje uszkodzeń elementu nie są kwalifikowane jako niebezpieczne. Przykładem jest uszkodzenie silnika powodujące zatrzymanie niebezpiecznego ruchu. Uszkodzenie takie powoduje, że silnik przestaje pełnić swoje funkcje, należy je więc zakwalifikować do uszkodzeń niebezpiecznych. Ale w skali całego systemu uszkodzenie to zazwyczaj prowadzi do stanu bezpiecznego, a więc nie jest uszkodzeniem niebezpiecznym. Dlatego też w przypadku pojedynczych elementów analizowanych w skali systemu należy dodatkowo uwzględnić współczynnik *k*, wskazujący, jaki procent uszkodzeń stanowią niebezpieczne uszkodzenia systemu.



Rys. 6.2. Model układu jednokanałowego

Jeśli znane są wartości *MTTF* poszczególnych elementów i podzespołów układu, można wyznaczyć prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego w jednostce czasu:

$$\lambda_D = \frac{k_S}{MTTF_S} + \frac{k_L}{MTTF_L} + \frac{k_D}{MTTF_D} \tag{6.8}$$

Model układu jednokanałowego pokazano na rys. 6.2. W tym modelu możliwe jest tylko jedno przejście: ze stanu *S*1 do stanu *S*2. Zakładamy, że nie nastąpi samoistna naprawa uszkodzenia niebezpiecznego, nie ma więc możliwości powrotu ze stanu *S*2 do *S*1. Macierz przejścia w tym modelu przyjmuje postać:

$$\mathbf{P} = \begin{bmatrix} 1-\lambda_D\Delta t & \lambda_D\Delta t \\ 0 & 1 \end{bmatrix} \tag{6.9}$$

Dla układów o typie pracy ciągłej prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego jest określane w odniesieniu do 1 godziny:

$$\mathrm{PFH}_D = 1\ \mathrm{h} \cdot \lambda_D. \tag{6.10}$$

6.6.2. Modelowanie periodycznych wyłączeń

Periodyczne wyłączenia (ang. *repetition*) lub resety urządzenia są powszechnie stosowanym środkiem zwiększania osiągniętego poziomu nienaruszalności bezpieczeństwa *SIL* (ang. *safety integrity level*). Mają one na celu okresowe sprawdzenie skuteczności realizacji funkcji bezpieczeństwa, które zazwyczaj odbywa się po powtórnym włączeniu systemu. Mogą to być sprawdzenia automatyczne, ale często są realizowane w ramach procedury obsługi systemu. Na rys. 6.3 pokazano model systemu jednokanałowego, pracującego w trybie „na przywołanie". Uwzględnia on periodyczne sprawdzenia funkcji bezpieczeństwa realizowane w ramach procedury obsługi. Model ten składa się z czterech stanów:

*S*1 – układ sprawny

*S*2 – uszkodzenie potencjalnie niebezpieczne

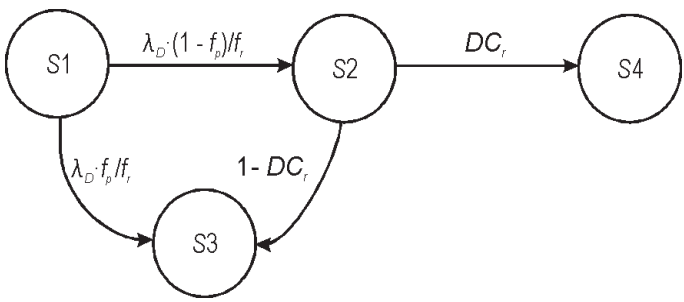
*S*3 – uszkodzenie niebezpieczne

*S*4 – stan bezpieczny po wykryciu uszkodzenia podczas włączania systemu.

Uszkodzenia, które w poprzednim modelu należało rozpatrywać jako niebezpieczne, w tym kwalifikują się do grupy uszkodzeń potencjalnie niebezpiecznych, gdyż mogą być wykryte przed przywołaniem funkcji bezpieczeństwa. Istotnym parametrem systemu jest częstotliwość dokonywania periodycznych wyłączeń, f_r. Zmiany w stanie sytemu są rozpatrywane w odniesieniu do przedziału czasu Δt określonego przez tę częstotliwość:

$$\Delta t = 1/f_r \tag{6.11}$$

Ze stanu *S*1 układ na skutek wystąpienia uszkodzenia przejdzie do stanu *S*2 lub *S*3, zależnie od tego, czy przed periodycznym wyłączeniem nastąpi przywołanie funkcji bezpieczeństwa, czy też nie. Tak więc prawdopodobieństwo przejścia do stanu *S*3 wyniesie $\lambda_D f_p/f_r$, co odpowiada sytuacji przywołania funkcji bezpieczeństwa po wystąpieniu uszkodzenia systemu. W pozostałych przypadkach mamy do czynienia z uszkodzeniem potencjalnie niebezpiecznym (stan *S*2).



Rys. 6.3. Model układu jednokanałowego periodycznie wyłączanego

Ze stanu *S*2 system przejdzie do stanu *S*4, jeśli uszkodzenie zostanie wykryte w trakcie testów po periodycznym wyłączeniu, lub do stanu *S*3, jeśli nie zostanie wykryte. O skuteczności sprawdzenia po włączeniu informuje pokrycie diagnostyczne DC_r. Określa ono, jak wiele z uszkodzeń potencjalnie niebezpiecznych zostanie wykrytych podczas sprawdzenia. Macierz przejść modelu pokazanego na rys. 6.3 przyjmuje postać:

$$\mathbf{P} = \begin{bmatrix} 1-\dfrac{\lambda_D}{f_r} & \dfrac{\lambda_D(1-f_p)}{f_r} & \dfrac{\lambda_D \cdot f_p}{f_r} & 0 \\ 0 & 0 & 1-DC_r & DC_r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{6.12}$$

Bezpieczeństwo tego modelu ocenia się dla przewidywanego czasu użytkowania, T_M, a więc po k cyklach:

$$k = T_M \cdot f_r \tag{6.13}$$

Wówczas wektor stanu jest równy:

$$\mathbf{S}_k = [1, 0, 0, 0, 0] \cdot \mathbf{P}^k = [s_1^k, s_2^k, s_3^k, s_4^k] \tag{6.14}$$

gdzie s_i^k – oznacza i-ty element wektora $\mathbf{S}_k$.

Ponieważ stanem niebezpiecznym jest S_3, więc prawdopodobieństwo wystąpienia defektu niebezpiecznego w tym przypadku wynosi:

$$\mathrm{PFH}_D = s_3^k \tag{6.15}$$

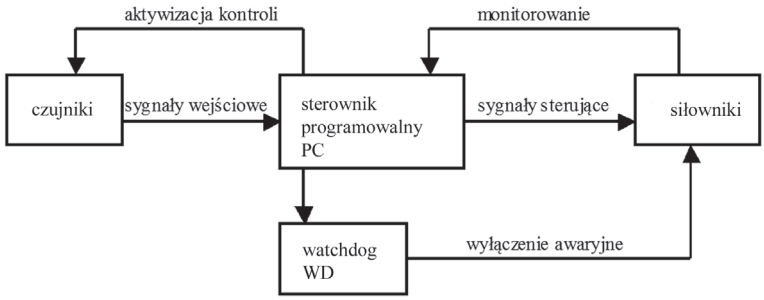
W podobny sposób można modelować konserwacje i naprawy („proof testy").

Model systemów o pracy ciągłej różni się tym, że podstawową jednostką czasu jest 1 h, a nie czas pomiędzy kolejnymi wyłączeniami.

6.6.3. Model systemu programowalnego z monitorowaniem

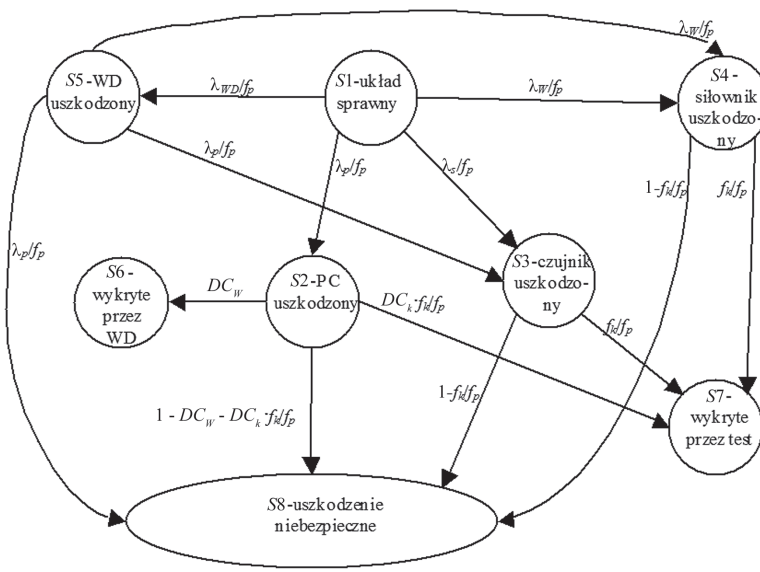
Często spotykanym rozwiązaniem jest system programowalny z monitorowaniem. Schemat blokowy takiego systemu pokazano na rys. 6.4. W takim układzie sterownik programowalny generuje periodycznie sygnały aktywizujące kontrolę sprawności systemu. Oznaczmy przez f_k częstotliwość tej kontroli. Zazwyczaj kontrola wykrywa wszystkie uszkodzenia czujników i elementów sterujących siłownikami oraz znaczny procent możliwych uszkodzeń samego sterownika. Pokrycie diagnostyczne tego sprawdzenia oznaczmy przez DC_k. Podobnie przez DC_w oznaczmy pokrycie diagnostyczne układu WD. Zauważmy, że uszkodzenie WD nie jest uszkodzeniem niebezpiecznym, ale powoduje, że większa część możliwych uszkodzeń systemu programowalnego to uszkodzenia niebezpieczne. Uszkodzenia czujników lub elementów sterujących siłownikami staną się uszkodzeniami niebezpiecznymi, jeśli nie zostaną wykryte przed przywołaniem funkcji bezpieczeństwa. Prawdopodobieństwa tych potencjalnie niebezpiecznych uszkodzeń układu programowalnego, czujników, WD i elementów wykonawczych oznaczmy odpowiednio przez λ_p, λ_s, λ_{WD} i λ_W.

Przedział czasu Δt, dla którego przeprowadzana będzie analiza, zależy od trybu pracy systemu, a także od wzajemnych zależności pomiędzy częstością przywołań, f_p, i częstością kontroli, f_k.



Rys. 6.4. Schemat blokowy układu programowalnego z monitorowaniem

Model układu z periodycznym monitorowaniem o trybie pracy z dużą częstością przywołań, f_p, pokazano na rys. 6.5. Model ten może przyjmować jeden z ośmiu stanów. Nie uwzględniono w nim wystąpienia uszkodzenia dwu elementów systemu pomiędzy kolejnymi przywołaniami, gdyż prawdopodobieństwo takiego stanu jest o kilka rzędów wielkości mniejsze niż dla stanów pozostałych, a stan uszkodzenia kilku elementów jednocześnie zawiera się w stanie opisującym uszkodzenie co najmniej jednego z nich. Założenie takie znacznie upraszcza analizę, a popełniany w związku z tym błąd jest pomijalny w stosunku do błędów pochodzących z innych źródeł.



Rys. 6.5. Model układu programowalnego z monitorowaniem

Stanami stabilnymi są *S*1, *S*5, *S*6 i *S*8. Wszystkie pozostałe trwają tylko do następnego przywołania funkcji bezpieczeństwa. Gdy przed przywołaniem funkcji nastąpi wykrycie uszkodzenia przez periodyczne monitorowanie lub WD, system

przechodzi w stan bezpieczny *S*6 lub *S*7. Jeśli takie wykrycie nie nastąpi, system znajdzie się w stanie uszkodzenia niebezpiecznego *S*8.

Nieco inaczej jest w razie uszkodzenia WD (stan *S*5). Samo uszkodzenie WD nie powoduje utraty funkcji bezpieczeństwa, więc system może trwale pozostawać w tym stanie. Zmiana stanu nastąpi dopiero po wystąpieniu uszkodzenia któregoś z pozostałych elementów systemu. Zakłada się przy tym, że jednoczesne uszkodzenie WD i sterownika jest uszkodzeniem niebezpiecznym. Pozostałe uszkodzenia należy traktować jako potencjalnie niebezpieczne.

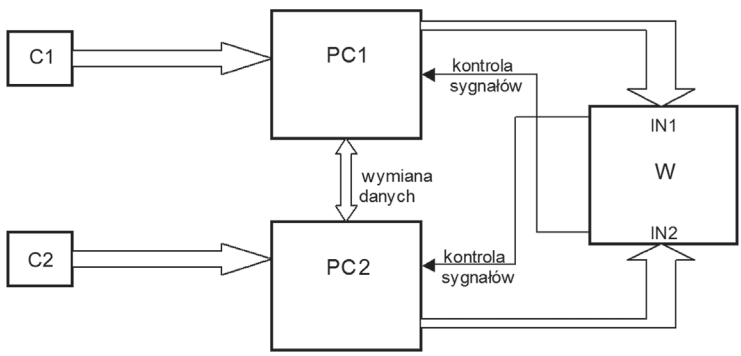
Tak więc:

$$\mathrm{PFH}_D = s_8^k \tag{6.16}$$

gdzie $k = 1\ \mathrm{h} \cdot f_p$.

6.6.4. Model systemu dwukanałowego

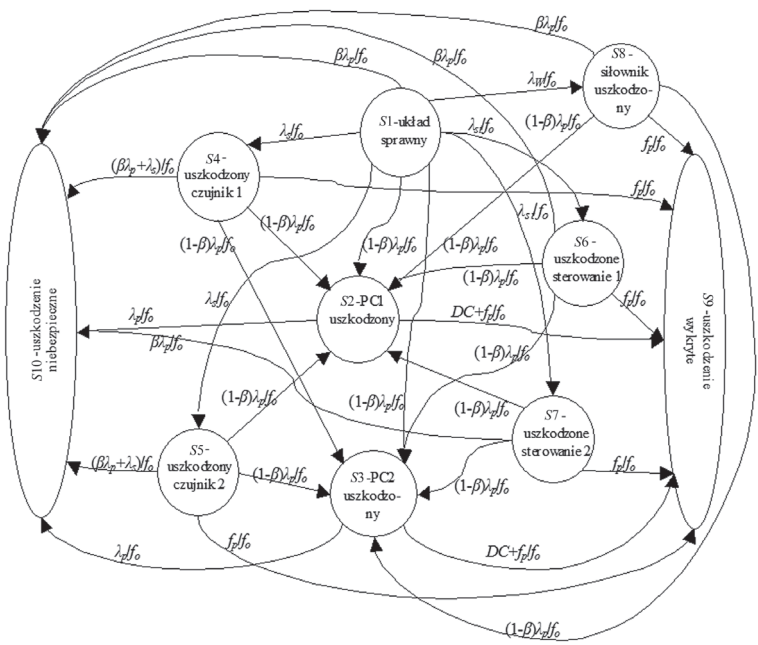
Dwukanałowy system w układzie redundancji pokazano na rys. 6.6. Jest to system typu 1*oo*2. W układzie tym dwa identyczne kanały, składające się z czujników C, sterowników programowalnych PC i układu wykonawczego W, realizują tę samą funkcję bezpieczeństwa. Załóżmy, że system pracuje w trybie pracy „na rzadkie przywołanie", w którym przywołanie funkcji bezpieczeństwa następuje z częstotliwością f_p. Każdorazowo po przywołaniu sterowniki programowalne wymieniają dane oraz sprawdzają wzajemnie stany sygnałów sterujących elementami wykonawczymi. W razie rozbieżności między danymi lub sygnałami sterującymi system jest sprowadzany do stanu bezpiecznego. Każdy ze sterowników dokonuje także automatycznego testu programowego (test on-line). Test ten jest wykonywany z częstotliwością f_o i pokryciem diagnostycznym *DC*. Załóżmy, że częstość przywołań funkcji bezpieczeństwa jest znacznie mniejsza niż częstość testów on-line. Wówczas system powinien być analizowany w odniesieniu do czasu równego $1/f_o$.



Rys. 6.6. System dwukanałowy

W modelowaniu takiego systemu należy dodatkowo uwzględnić efekt uszkodzeń pochodzących od wspólnej przyczyny, które mają znaczący wpływ na funkcjonowanie systemów o identycznych kanałach redundancji. Uszkodzenia takie charakteryzuje współczynnik β określający, jaka część uszkodzeń niebezpiecznych uaktywni się jednocześnie w obu kanałach jako uszkodzenie od wspólnej przyczyny. Wartość współczynnika β jest zazwyczaj mniejsza od 10% i zależy od konfiguracji konkretnego systemu. Dokładne jej wyznaczenie jest niezwykle trudne. Zadowalające oszacowanie można uzyskać, stosując metodę szczegółowo opisaną w załączniku D do normy PN-EN 61508-6:2010 lub załączniku F do PN-EN ISO 13849-1:2008.

Ponieważ w opisywanym przykładzie wzajemne porównanie działania obu kanałów następuje dopiero po przywołaniu funkcji bezpieczeństwa, co zdarza się bardzo rzadko w stosunku do częstości testów, więc tym razem istotne stają się także prawdopodobieństwa uszkodzenia obu kanałów. Dotyczy to zwłaszcza uszkodzenia obu czujników, które powoduje, że system nie jest w stanie wykryć utraty funkcji bezpieczeństwa. Podobnie jest w sytuacji niewykrytych uszkodzeń obu sterowników PC1 i PC2 kolejno. Przypadki takie należy zakwalifikować jako uszkodzenia niebezpieczne. Dotyczy to także uszkodzeń od wspólnej przyczyny. Natomiast uszkodzenie jednego sterownika, które nie zostało wykryte przez test on-line, jest wykrywane przez drugi sterownik po przywołaniu funkcji, nie jest więc uszkodzeniem niebezpiecznym.



Rys. 6.7. Model systemu dwukanałowego

Osobnego traktowania nie wymaga także sytuacja kolejnego uszkodzenia, np. czujnika, a następnie jednego ze sterowań elementami wykonawczymi. Wynika to stąd, że układ reaguje na tę sytuację tak samo, jak na uszkodzenie tylko czujnika lub tylko sterowania, to znaczy uszkodzenie jest wykrywane przez PC1 lub PC2 po przywołaniu funkcji bezpieczeństwa.

Model systemu dwukanałowego przedstawiono na rys. 6.7. Dla tego modelu prawdopodobieństwo wystąpienia defektu niebezpiecznego wynosi:

$$\mathrm{PFH}_D = s_{10}^k \tag{6.17}$$

gdzie $k = T_M \cdot f_o$.

6.7. Główne problemy modelowania

Przedstawione modele najbardziej typowych rozwiązań układowych systemów sterowania realizujących funkcje bezpieczeństwa oczywiście nie wyczerpują wszystkich zagadnień. Są to jedynie przykłady dobrane tak, aby były możliwie najbardziej reprezentatywne. W praktycznych rozwiązaniach przykłady te można wykorzystać jako fragmenty większych modeli. Rozwiązania praktyczne zawierają zazwyczaj znacznie więcej zastosowanych środków zapobiegania skutkom uszkodzeń. Na przykład w układach wielokanałowych w każdym z kanałów stosowane są nie tylko testy on-line, ale także układy WD, monitorowanie, okresowe wyłączanie, „proof testy" itp. Tak więc każdy konkretny przykład wymaga opracowania odrębnego, szczegółowego modelu.

Poprawność wyznaczenia PFH_D zależy przede wszystkim od poprawności sformułowania modelu systemu. Decydujące znaczenie mają zwłaszcza:

- poprawność zidentyfikowania uszkodzeń niebezpiecznych
- właściwe określenie wskaźników niezawodnościowych
- zdefiniowanie zbioru stanów w modelu
- dobór kroku czasowego modelu.

Sposób rozwiązania tych problemów decyduje o przydatności sformułowanego modelu, zarówno pod względem dokładności, jak i możliwości wykorzystania. W praktyce może się okazać, że model zbyt rozbudowany i zbyt szczegółowy przestaje być czytelny i przejrzysty, a ponadto wymaga zaangażowania znacznych mocy obliczeniowych i w efekcie może być całkowicie nieprzydatny. Jednocześnie model nazbyt uproszczony może prowadzić do przeoczenia istotnych zjawisk występujących w systemie, co może spowodować popełnienie znaczących błędów. Dlatego też należy zawsze uwzględniać możliwość ograniczenia liczby stanów, tak jak to zrobiono w zaprezentowanych przykładach. Aby jednak model był powtarzalny

i porównywalny z modelami opracowywanymi przez inne zespoły, np. weryfikujące projekt, konieczne jest bardzo precyzyjne opisanie wszystkich stanów i zastosowanych założeń, które są podstawą redukcji ich liczby.

Podczas opracowywania modeli szczególną uwagę należy zwrócić na kwestię właściwego doboru kroku czasowego Δt. Jeśli wybrany zostanie krok zbyt mały, to w układzie rzeczywistym może się okazać, że k przyjmie wartości rzędu tysięcy. Oznacza to, że wykonanie stosownej liczby mnożeń macierzy **P** wymagałoby zaangażowania bardzo dużych mocy obliczeniowych w długim czasie. Rozwiązaniem tego problemu może być zwiększenie jednostki czasu w modelu i przyjęcie jako odniesienia na przykład jednej zmiany lub jednej doby. Łatwo wykazać, że w rzeczywistych przypadkach zmiana przedziału czasu z Δt na $k \cdot \Delta t$ ma pomijalny wpływ na wyznaczany poziom nienaruszalności bezpieczeństwa *SIL*, pod warunkiem, że nie powoduje ona pominięcia zjawisk ważnych dla funkcjonowania systemu, takich jak na przykład akumulacja uszkodzeń. Jednak dobranie wartości zbyt dużych może prowadzić do takich przeoczeń. Tak więc, doboru tego powinno się dokonywać bardzo uważnie, a jego uzasadnienie trzeba jednoznacznie opisać w raporcie z analizy.

Zarówno liczba stanów, jak i dobór kroku czasowego decydują o liczbie obliczeń koniecznych do określenia *SIL*. Obecny rozwój systemów komputerowych sprawia, że wykonanie kilku tysięcy mnożeń macierzy 10×10 nie stanowi problemu. Może się jednak okazać, że zarówno wielkość macierzy, jak i konieczna liczba mnożeń będą znacznie większe. Wówczas można stosować metody umożliwiające ograniczenie liczby mnożeń. Bardzo skuteczna jest na przykład metoda polegająca na binarnej reprezentacji liczby k (Dźwiarek, 1996):

$$k = \sum_{i=0}^{l} b_i \cdot 2^{\mathrm{i}} \tag{6.18}$$

gdzie: l = część całkowita $[\log_2 l]$, $\quad b_i \in \{0,1\}$.

Wówczas:

$$\mathbf{P}^k = \prod_{i=0}^{l} \mathbf{P}^{b_i \cdot 2^i} \tag{6.19}$$

Ponieważ do wyznaczenia $\mathbf{P}^{2^l}$ wystarcza wykonanie l mnożeń, więc całkowita liczba mnożeń będzie nie większa niż $2 \cdot l$. Na przykład, jeśli $k = 1024 = 2^{10}$, to konieczne jest wykonanie jedynie 10 mnożeń, a gdy $k = 2047 = 2^{11} - 1$, liczba koniecznych mnożeń wyniesie 20.

Innym problemem praktycznym jest właściwe określenie parametrów systemu, takich jak przewidywana częstość uszkodzeń, średni czas pracy bezawaryjnej,

pokrycie diagnostyczne, określenie zbioru uszkodzeń niebezpiecznych, współczynnika uszkodzeń od wspólnej przyczyny itp. Pomocne może być posłużenie się metodami podanymi w normach PN-EN 61508-2 i PN-EN 61508-6. Wszystkie zastosowane metody wyznaczania tych wartości, a także źródła danych statystycznych, powinny być opisane i zidentyfikowane w raportach z oceny, tak aby zawsze można było je odtworzyć. Także przeprowadzone analizy struktury podzespołów, takie jak FTA czy FMEA, powinny być opisane i udokumentowane zgodnie z właściwymi procedurami.

Jednak nawet precyzyjne procedury modelowania związane z bezpieczeństwem systemów sterowania nie zapewnią, że analizy przeprowadzane przez różne osoby dadzą zawsze dokładnie taki sam wynik. Brak wystarczająco dokładnych danych statystycznych dotyczących nieuszkadzalności elementów i podzespołów powoduje, że wszystkie obliczenia są szacunkowe i umożliwiają jedynie orientacyjne określenie odporności systemu na defekty. Zazwyczaj oszacowanie takie jest wystarczające.

Rozdział 7

Jakościowa metoda oceny bezpieczeństwa systemów sterowania maszynami

7.1. Wprowadzenie

Opisane w poprzednich rozdziałach metody zwiększania odporności systemu na defekty charakteryzują się różną skutecznością. Metodę oraz sposób jej realizacji powinno się wybierać z uwzględnieniem ryzyka, które redukuje funkcja bezpieczeństwa. Wynika stąd, że określenie wymagań związanych z bezpieczeństwem funkcjonalnym powinno wywodzić się z oceny ryzyka dotyczącej zagrożenia (sytuacji zagrożenia) i być przeprowadzone w odniesieniu do planowanej implementacji funkcji bezpieczeństwa. W celu określenia wymagań dotyczących bezpieczeństwa funkcjonalnego opracowano dwie różne metodyki postępowania, które zostały przedstawione w normach PN-EN ISO 13849-1:2008 i PN-EN 62061:2008.

W obszarze układów elektrycznych i elektronicznych wybór metodyki określania wymagań dotyczących bezpieczeństwa funkcjonalnego należy do projektanta i może być na przykład uwarunkowany jego doświadczeniem związanym z daną metodyką lub z możliwością wykorzystania dokumentacji wcześniej wykonanych projektów. Także w tym obszarze, pomimo różnego podejścia do określania wymagań, realizacje funkcji bezpieczeństwa uzyskane z zastosowaniem obu dostępnych metodyk dają podobne wyniki w sensie zapewnienia bezpieczeństwa funkcjonalnego.

Projektując urządzenia, które realizują funkcje bezpieczeństwa, zawsze należy uwzględniać dwa aspekty:

– założenia funkcjonalne powinny być tak sformułowane, aby zapobieganie zagrożeniom, do których funkcja bezpieczeństwa jest przewidziana, było

skuteczne w sytuacji wystąpienia wszystkich przewidywalnych zdarzeń związanych z obsługą maszyny
– założenia bezpieczeństwa powinny uwzględniać wszystkie przewidywalne defekty, aby jak najskuteczniej wykluczyć możliwość utraty funkcji bezpieczeństwa na skutek defektu.

Jeśli założenia funkcjonalne zostaną prawidłowo sformułowane, to funkcja bezpieczeństwa powinna ograniczyć zagrożenia, do których jest przypisana. Ograniczenie to będzie skuteczne pod warunkiem, że funkcja bezpieczeństwa zadziała. Możliwe jest jednak, że na przykład na skutek wystąpienia defektu funkcja bezpieczeństwa nie działa. Mówi się wówczas, że nastąpiła utrata funkcji bezpieczeństwa. Zdarzenie takie powoduje, że ryzyko przestaje być ograniczone do akceptowalnego poziomu i może nastąpić wypadek. Dlatego też, projektując funkcje bezpieczeństwa, należy uwzględnić nie tylko założenia funkcjonalne, lecz także zachowanie funkcji w warunkach defektu.

Wybór normy, według której będzie projektowany system sterowania, zależy od techniki realizacji projektowanego układu sterowania oraz jego złożoności. Nie ma zdecydowanych wymagań w tym zakresie, jednak przedstawiane są następujące zalecenia:

– normę PN-EN ISO 13849-1 powinno się stosować w odniesieniu do systemów hydraulicznych, pneumatycznych, elektromechanicznych, elektronicznych
– w przypadku prostych systemów elektronicznych programowalnych, budowanych z podstawowych elementów elektronicznych, normę PN-EN ISO 13849-1 można stosować, gdy:
  - ryzyko związane z eliminowanym zagrożeniem jest niewielkie
  - funkcja bezpieczeństwa jest realizowana w pełni sprzętowo oraz zachowanie systemu w warunkach defektu jest jednoznacznie określone
  - udział systemu programowalnego w realizacji funkcji bezpieczeństwa jest niewielki (np. monitorowanie)
  - funkcja bezpieczeństwa jest realizowana przez dwa różne systemy programowalne (przez różne systemy programowalne rozumie się układy o różnych systemach operacyjnych i różnym oprogramowaniu)
  - zastosowane elementy systemu sterowania związane z bezpieczeństwem (z uwzględnieniem oprogramowania) zostały zaprojektowane zgodnie z zaleceniami stosownych norm
– normę PN-EN 62061 zaleca się stosować w odniesieniu do integracji systemów sterowania maszyny z podzespołów wykonanych zgodnie z PN-EN 13849-1 lub PN EN 61508, np. sterowników PLC.

7.2. Kategorie odporności systemów sterowania maszynami na defekty

Elementy systemów sterowania maszynami związane z bezpieczeństwem są sklasyfikowane według PN-EN ISO 13849-1:2008 na pięć kategorii. Podział ten został utrzymany tak jak w poprzedniej (już wycofanej z wykazu norm) normie PN-EN 954-1. Kryteria podziału nie zależą od zastosowanych technologii, lecz jedynie od odporności urządzeń na defekty i ich zachowania w stanie defektu określonego przez strukturę urządzenia i jego niezawodność.

Podstawową kategorią jest kategoria B. Wystąpienie defektu w urządzeniach tej kategorii może spowodować utratę funkcji bezpieczeństwa. Urządzenia kategorii 1 mają podwyższoną odporność na defekty głównie dzięki selekcji zastosowanych elementów. W kategoriach 2, 3 i 4 wzrost odporności uzyskuje się przez rozbudowanie struktury urządzeń. W kategorii 2 jest to realizowane przez okresowy autotest działania funkcji bezpieczeństwa. W kategorii 3 i 4 odporność wynika z ciągłego zapewnienia, że pojedynczy defekt nie spowoduje utraty funkcji bezpieczeństwa. W urządzeniach kategorii 3 defekty powinny być wykryte, gdy jest to praktycznie uzasadnione, a w urządzeniach kategorii 4, gdy jest to możliwe. W tym ostatnim przypadku powinna być także określona odporność na akumulację defektów.

W normie PN-EN ISO 13849-1:2008 w porównaniu z PN-EN 954-1 dodatkowo przypisano architektury systemu sterowania. Zastosowanie tych architektur upraszcza proces walidacji systemu.

Kategoria B

Do tej kategorii zalicza się urządzenia odporne na oddziaływanie następujących czynników:

- spodziewane narażenia w czasie pracy (np. czas pracy, opory ruchu itp.)
- wpływ obrabianego materiału (np. detergentów, drewna, metalu itp.)
- wpływy środowiskowe (mechaniczne, klimatyczne, elektryczne itp.).

Są to więc urządzenia zaprojektowane i wykonane z uwzględnieniem podstawowych zasad bezpieczeństwa i zapobiegania niekorzystnym oddziaływaniom (np. przez stosowanie systemów zapewnienia jakości, zapobieganie ewentualnym problemom związanym z kompatybilnością elektromagnetyczną itp.). Muszą one spełniać wymagania stosownych norm i przepisów. Urządzenia te zapewniają realizację funkcji bezpieczeństwa w środowisku przemysłowym.

Wymagania kategorii B są obligatoryjnie stosowane do wszystkich pozostałych kategorii.

Kategoria 1

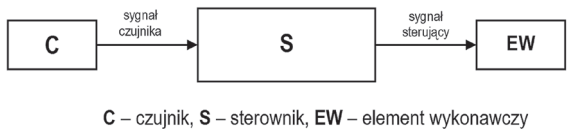
Ta kategoria wzmacnia wymagania dotyczące odporności na oddziaływanie środowiska i niezawodności urządzeń. Realizuje się to poprzez właściwy dobór elementów i podzespołów, które powinny być zgodne z wymaganiami norm (np. IEC dla elementów elektronicznych). Powinny być stosowane jedynie „wypróbowane" (ang. *well-tried*) elementy i podzespoły. Pod pojęciem „wypróbowane" rozumie się elementy, które są:

- szeroko stosowane w podobnych aplikacjach z dobrym rezultatem
- wykonane i przebadane w sposób potwierdzający ich niezawodność i przydatność w zastosowaniach związanych z bezpieczeństwem.

Istotne jest także stosowanie zasad projektowania bardziej precyzyjnych niż w kategorii B. Zasadami takimi są np.:

- zapobieganie niektórym defektom, np. zapobieganie zwarciom przez izolowanie przewodów lub stosowanie właściwych odległości między ścieżkami
- ograniczenie prawdopodobieństwa występowania defektów, np. przez przewymiarowanie
- ukierunkowanie defektów, np. wymuszenie przepalenia się obwodu, jeśli konieczne jest szybkie odcięcie zasilania
- wystarczająco wczesne wykrywanie defektów
- ograniczanie skutków defektów, np. przez uziemianie obudów urządzeń elektrycznych.

Zasady takie są nazywane „wypróbowanymi zasadami bezpieczeństwa" (ang. *well-tried safety principles*).



Rys. 7.1. Architektura przypisana do kategorii B i kategorii 1 (PN-EN ISO 13849-1:2008)

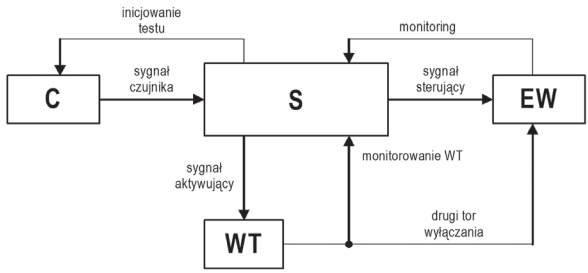
Uznaje się, że systemy elektroniczne nie spełniają wymagań kategorii 1, gdyż nie ma w nich możliwości wykluczenia defektów.

Wymagania kategorii B i kategorii 1 spełniają układy o architekturze szeregowej, pokazanej na rys. 7.1.

Kategoria 2

W tej kategorii jest wymagana periodyczna kontrola związanych z bezpieczeństwem części systemów sterowania z częstotliwością zależną od konkretnego

zastosowania. Kontynuowanie działania maszyny jest możliwe tylko wtedy, kiedy wynik sprawdzenia jest pozytywny, to znaczy funkcja bezpieczeństwa jest aktywna. W razie wykrycia defektu generowany jest sygnał zatrzymania maszyny w pozycji bezpiecznej (najczęściej przez jej wyłączenie).



C – czujnik, **S** – sterownik, **EW** – element wykonawczy, **WT**– wyposażenie testujące

Rys. 7.2. Architektura przypisana do kategorii 2 (PN-EN ISO 13849-1:2008)

Wymaganie to oznacza, że detekcja defektów odbywa się tylko w kolejnych krokach sterowania. Tak więc, wystąpienie defektu pomiędzy kolejnymi sprawdzeniami może spowodować utratę funkcji bezpieczeństwa.

Wymagania kategorii 2 realizuje się przez właściwą architekturę systemu, a nie analizę jego niezawodności. Zgodność z tą kategorią można uzyskać, stosując technikę jednokanałową i jednocześnie zapewniając automatyczne testowanie części krytycznych dla bezpieczeństwa.

Architekturę przypisaną do kategorii 2 pokazano na rys. 7.2. Zawiera ona urządzenie periodycznie testujące system w celu wykrycia ewentualnych defektów.

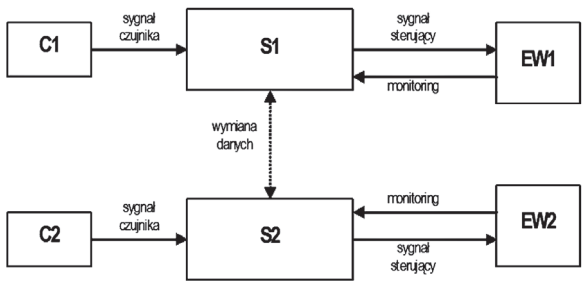
Kategorie 3 i 4

Kategorie te są definiowane w podobny sposób. Różnice pomiędzy nimi polegają przede wszystkim na ostrości wymagań, zwłaszcza w zakresie odporności na kumulację defektów. Kategoria 3 może być niewystarczająca do zapewnienia bezpieczeństwa w razie wystąpienia kombinacji różnych defektów. Natomiast urządzenia kategorii 4 powinny, przynajmniej teoretycznie, być odporne na każdą ich kumulację.

Dla obu tych kategorii odporność na pojedyncze uszkodzenie jest jednoznacznie określona: żaden pojedynczy defekt dowolnej części systemu sterowania nie może spowodować utraty funkcji bezpieczeństwa. Inaczej jest z wymaganiami dotyczącymi wykrywania defektów. Dla obu kategorii należy zapobiegać występowaniu niewykrytych defektów (również niepowodujących natychmiastowych skutków), które w powiązaniu z innymi defektami mogą prowadzić do powstania sytuacji niebezpiecznych. Rozwiązaniem tego problemu może być na przykład

natychmiastowa detekcja wszystkich defektów, tak żeby nie była możliwa ich kumulacja. Taki typ detekcji zazwyczaj jest realizowany przez stosowanie procedur samokontroli umożliwiających potwierdzenie, że różne funkcje urządzenia są realizowane bez defektów. Dla kategorii 3 wymaga się wykrywania defektów, „jeśli jest to praktycznie uzasadnione" (ang. *whenever reasonably practicable*). Sformułowanie takie daje szerokie możliwości interpretacji, co pozwala na zredukowanie ostrości wymagań dotyczących wykrywania defektów. Urządzenia kategorii 3 zachowują się więc w sposób bezpieczny w razie wystąpienia pojedynczego uszkodzenia, ale zapewniają niższy poziom bezpieczeństwa w związku z niewykrywaniem wszystkich defektów. W sytuacji kumulacji defektów może wystąpić utrata funkcji bezpieczeństwa.

Od urządzeń kategorii 4 wymaga się zredukowania tych niedoskonałości. W definicji tej kategorii słowa „jeśli jest to praktycznie uzasadnione" są zastąpione słowami „jeśli jest to możliwe". Tak więc wykrywanie defektów jest ograniczone tylko aktualnym stanem wiedzy.



Rys. 7.3. Architektura przypisana do kategorii 3 i 4 (PN-EN ISO 13849-1:2008)

Architekturę przypisaną do kategorii 3 i 4 przedstawiono na rys. 7.3. Dla kategorii 3 jest to redundancja, a w przypadku kategorii 4 redundancja z monitorowaniem.

Realizując wymagania kategorii 3 i 4, trzeba uwzględnić zarówno analizę niezawodnościową, jak i dobór właściwej architektury systemu. Przykłady stosowanych metod przedstawiono w rozdziale 4.

7.3. Poziomy zapewnienia bezpieczeństwa

Systemy programowalne, a zwłaszcza proste PLC, stały się obecnie na tyle tanie, że coraz częściej wypierają tradycyjne, elektromechaniczne systemy sterowania. Są one obecnie spotykane nawet w najprostszych maszynach. Dlatego też problem ich oceny pod względem zapewnianego poziomu bezpieczeństwa stał się

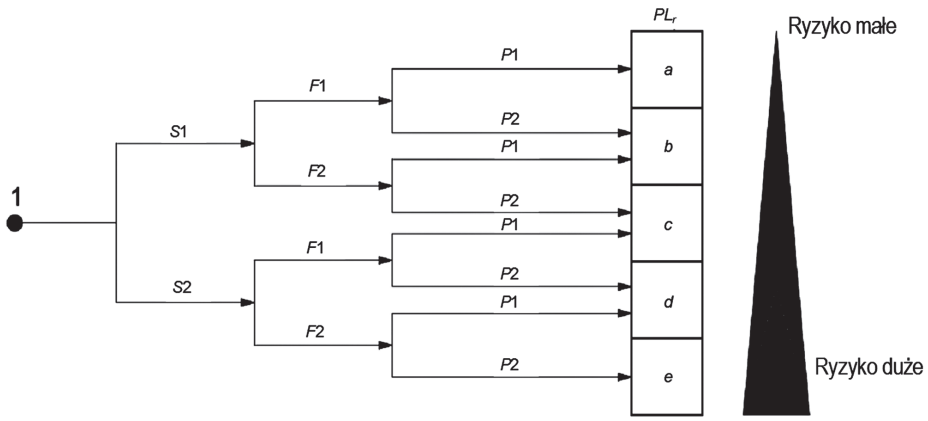
niezwykle istotny. Spowodowało to konieczność uwzględnienia systemu wskaźników umożliwiających ocenę systemów programowalnych. W normie PN-EN ISO 13849-1:2008 wskaźnikiem takim jest poziom zapewnienia bezpieczeństwa *PL*. Rozróżnia się pięć poziomów zapewnienia bezpieczeństwa: od „a" do „e" (tabl. 7.1) Poziomy te są quasi probabilistycznymi wskaźnikami prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego na godzinę w przewidywanym czasie użytkowania maszyny (zazwyczaj 20 lat).

Tablica 7.1. Poziomy zapewnienia bezpieczeństwa, *PL* (PN-EN ISO 13849-1:2008)

Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę	***PL***
$10^{-5} \leq p < 10^{-4}$	*a*
$3 \times 10^{-6} \leq p < 10^{-5}$	*b*
$10^{-6} \leq p < 3 \times 10^{-6}$	*c*
$10^{-7} \leq p < 10^{-6}$	*d*
$10^{-8} \leq p < 10^{-7}$	*e*

7.4. Określanie wymaganego poziomu zapewnienia bezpieczeństwa na podstawie analizy ryzyka

Założenia bezpieczeństwa, określające wymagany poziom zapewnienia bezpieczeństwa PL_r (ang. *required perfomance level*), są formułowane na podstawie



Rys. 7.4. Zależność pomiędzy poziomem ryzyka a wymaganym PL_r; *S*1 – mała ciężkość szkody, *S*2 – duża ciężkość szkody, *F*1 – mała częstość lub czas ekspozycji, *F*2 – duża częstość lub czas ekspozycji, *P*1 – możliwe uniknięcie szkody, *P*2 – niemożliwe uniknięcie szkody (PN-EN ISO 13849-1:2008)

analizy ryzyka związanego z zagrożeniem, któremu funkcja bezpieczeństwa zapobiega. W analizie należy uwzględnić wszystkie parametry ryzyka, to znaczy:

- S – ciężkość szkody
- F – częstość lub czas ekspozycji na zagrożenie
- P – możliwość uniknięcia lub ograniczenia ciężkości szkody.

Kombinacja tych parametrów decyduje o wymaganym poziomie zapewnienia bezpieczeństwa, PL_r, projektowanej funkcji bezpieczeństwa, w sposób wynikający z grafu ryzyka przedstawionego na rys. 7.4.

7.5. Szacowanie uzyskanego poziomu zapewnienia bezpieczeństwa

Po zaprojektowaniu systemu sterowania realizującego funkcję bezpieczeństwa należy wyznaczyć osiągnięty PL_a (ang. *achived performance level*). Zgodnie z tabl. 7.1 powinno się tego dokonać przez wyznaczenie prawdopodobieństwa wystąpienia defektu, PFH_D. Zazwyczaj wymaga to przeprowadzenia złożonych analiz probabilistycznych, opisanych w rozdziałach 5 i 6. Norma PN-EN ISO 13849-1:2008 umożliwia także zastosowanie metod uproszczonych (Dźwiarek, 2000b). W tym celu podstawowym parametrom opisującym cechy probabilistyczne systemu przypisano wskaźniki jakościowe: „duży", „średni", „mały". Zasady przypisywania tych wskaźników do poszczególnych parametrów pokazano w tabl. 7.2 i 7.3.

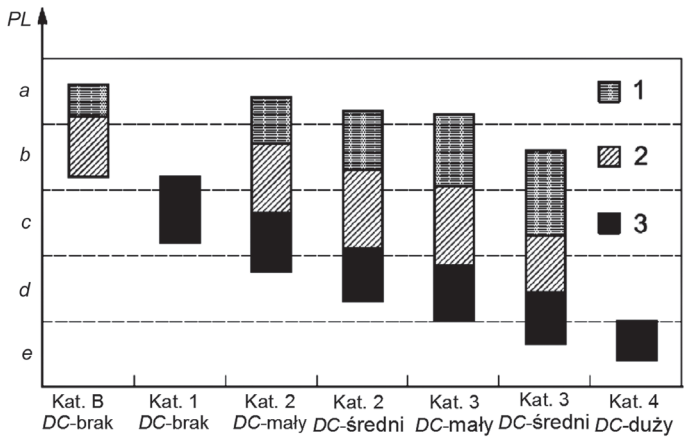
Tablica 7.2. Średni czas do wystąpienia defektu niebezpiecznego ($MTTF_d$), (PN-EN ISO 13849-1:2008)

Wielkość parametru	Przedział wartości
mały	3 lata $\leq MTTF_d <$ 10 lat
średni	10 lat $\leq MTTF_d <$ 30 lat
duży	30 lat $\leq MTTF_d <$ 100 lat

Tablica 7.3. Pokrycie diagnostyczne (DC), (PN-EN ISO 13849-1:2008)

Wielkość parametru	Przedział wartości
brak	$DC < 60\%$
małe	$60\% \leq DC < 90\%$
średnie	$90\% \leq DC < 99\%$
duże	$99\% \leq DC$

Gdy projektant systemu sterowania zastosuje architekturę przypisaną do wybranej kategorii i oszacuje wielkości $MTTF_d$ i DC, osiągnięty PL_a można wyznaczyć według grafu pokazanego na rys. 7.5.



PL - poziom zapewnienia bezpieczeństwa
1 - *MTTF* mały
2 - *MTTF* średni
3 - *MTTF* duży

Rys. 7.5. Wyznaczanie osiągniętego PL_a (PN-EN ISO 13849-1:2008)

Oceniając system, należy także uwzględnić działania mające na celu:
- zapobieganie defektom systematycznym (system zapewnienia jakości projektowania i wytwarzania maszyny)
- zapobieganie defektom oprogramowania
- zapobieganie defektom od wspólnej przyczyny.

Są to aspekty jakościowe projektowania. Ich oceny dokonuje się za pomocą list kontrolnych i audytów.

7.6. Walidacja

Walidacja jest działaniem mającym na celu potwierdzenie (przez analizy i badania), że system spełnia założone wymagania i w ten sposób zapewni oczekiwaną skuteczność tego rodzaju środków bezpieczeństwa. Dodatkowo systematycznie prowadzony proces walidacji jest czynnikiem wymuszającym tworzenie i gromadzenie pełnej dokumentacji projektowej wymaganej przez organy nadzoru rynku. Podstawowe zasady prowadzenia walidacji przedstawili Dźwiarek i Strawiński (2008). Wymaganiom dotyczącym zasad prowadzenia walidacji elementów systemu sterowania związanych z bezpieczeństwem (ESSZB) poświęcono normę ISO/FDIS 13849-2:2011.

Walidacja powinna obejmować:
- przewidziane funkcje bezpieczeństwa
- osiągniętą kategorię i poziom zapewnienia bezpieczeństwa.

Wymaga się, aby walidację prowadziły osoby niezależne, niezwiązane z procesem projektowania systemu. Ponadto powinna być przeprowadzona zgodnie z planem walidacji, z zastosowaniem analizy oraz – jeśli to konieczne – wykonaniem badań.

Analizy powinno się zacząć tak wcześnie, jak to jest tylko możliwe i równolegle z procesem projektowania, aby wykryte problemy można było rozwiązywać we wczesnej fazie, gdy stosunkowo łatwo jest je skorygować. Może się również okazać konieczne przesunięcie niektórych elementów analizy na dalsze etapy procesu, kiedy projekt jest już zaawansowany.

Proces walidacji powinien obejmować przeanalizowanie zachowania systemu przy wszystkich defektach, które należy rozważyć. Podstawą do analizy powinny być odpowiednie, wynikające z doświadczenia, wykazy defektów. W wykazach defektów szczególnych należy również uwzględnić możliwość wystąpienia uszkodzeń spowodowanych wspólną przyczyną.

Wymagane informacje dotyczące prowadzonej walidacji różnią się w zależności od zastosowanej techniki, wymaganej (lub wymaganych) kategorii, przesłanek projektowania systemu oraz udziału elementów systemu sterowania związanych z bezpieczeństwem w obniżeniu ryzyka. Do walidacji należy wykorzystać dokumenty zawierające wystarczające informacje, które umożliwią wykazanie, że kategoria (lub kategorie) oraz funkcja (lub funkcje) bezpieczeństwa realizowane przez system zostały osiągnięte.

Walidacja przeprowadzona przez analizę i badanie powinna być zaprotokołowana. Protokół powinien odzwierciedlać proces walidacji każdego z wymagań dotyczącego bezpieczeństwa. Można powoływać się na protokóły poprzednich walidacji, pod warunkiem, że są one prawidłowo zidentyfikowane.

Gdy walidacja poprzez analizę jest niewystarczająca, aby potwierdzić osiągnięcie określonych funkcji bezpieczeństwa, odpowiedniej kategorii lub *PL*, należy przeprowadzić badanie dopełniające. Badanie zawsze jest dopełnieniem analizy i często się zdarza, że jest konieczne. Badania walidacyjne powinny być zaplanowane i wykonane w sposób logiczny. W szczególności należy sporządzić:
- plan badań (jako część planu walidacji) – należy go sporządzić przed rozpoczęciem badań i zawrzeć w nim ich wykaz, oczekiwane wyniki oraz kolejność wykonywania
- sprawozdania z badań – powinny one zawierać nazwisko osoby wykonującej badania, warunki środowiskowe panujące w ich trakcie, procedury badań oraz zastosowany sprzęt badawczy i pomocniczy, wyniki oraz inne niezbędne informacje.

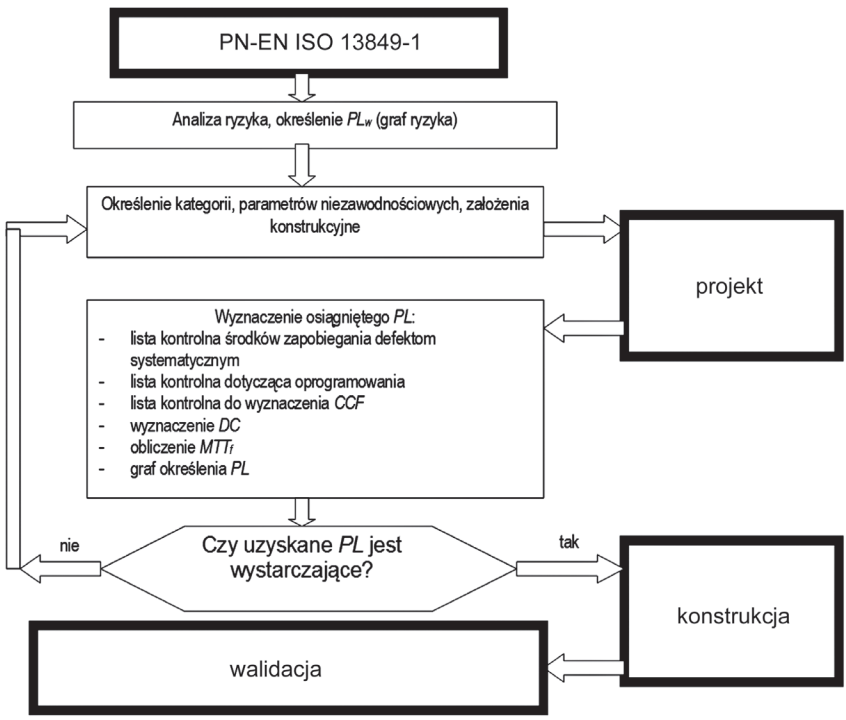
Wyniki badań należy porównać z planem badań, aby upewnić się, że zostały osiągnięte zakładane cele funkcjonalne i eksploatacyjne.

7.7. Ogólna strategia projektowania systemów sterowania maszynami związanych z bezpieczeństwem wg PN-EN ISO 13849-1:2008

Całość działań obejmujących projektowanie i ocenę jakościową systemu sterowania związanego z bezpieczeństwem przedstawiono w pracy (Dźwiarek, 2008b). Są to:

- sformułowanie wymagań funkcjonalnych na podstawie identyfikacji zagrożeń
- sformułowanie wymagań pewności realizacji funkcji bezpieczeństwa na podstawie oceny ryzyka
- dobór metody realizacji wymagań przypisanych do wymaganego poziomu zapewnienia bezpieczeństwa, a więc dobór kategorii i architektury systemu oraz określenie wymagań dotyczących parametrów niezawodnościowych
- szczegółowy projekt
- ocena systemu
- walidacja.

Algorytm postępowania podczas formułowania i weryfikacji wymagań bezpieczeństwa wg PN-EN ISO 13849-1:2008 pokazano na rys. 7.6.



Rys. 7.6. Algorytm postępowania podczas formułowania i weryfikacji wymagań wg PN-EN ISO 13849-1:2008

Rozdział 8

Ilościowa metoda oceny bezpieczeństwa systemów sterowania maszynami

8.1. Wprowadzenie

Przedstawiona w rozdziale 7 koncepcja jakościowej oceny odporności systemu sterowania na defekty wymaga wiedzy o rodzajach i skutkach defektów, które mogą w nim wystąpić. Może więc być stosowana głównie do systemów typu A. W przypadku systemów typu B, gdy wiedza o możliwych defektach jest ograniczona, zwłaszcza w odniesieniu do złożonych systemów programowalnych, ocena jakościowa jest niewystarczająca, lub jej przeprowadzenie nie jest możliwe. Dlatego też w połowie lat dziewięćdziesiątych ubiegłego wieku została sformułowana koncepcja tzw. „bezpieczeństwa funkcjonalnego".

8.2. Koncepcja bezpieczeństwa funkcjonalnego

Bezpieczeństwo funkcjonalne można scharakteryzować następująco (Dźwiarek, 1996; Missala, 1997):

- koncepcja ma zastosowanie do systemów i funkcji wiążących się z bezpieczeństwem
- bezpieczeństwo funkcjonalne uzyskuje się przez eliminację ewentualnych defektów systematycznych za pomocą działań prewencyjnych
- drogą do uzyskania bezpieczeństwa funkcjonalnego jest przestrzeganie odpowiednich procedur przez odpowiednio wyszkolony personel
- poprzez audyty i ocenę realizowanych działań uzyskuje się pewność, że wymagany poziom bezpieczeństwa funkcjonalnego został osiągnięty
- miernikiem osiągniętego poziomu bezpieczeństwa funkcjonalnego są wskaźniki probabilistyczne.

Wymagania bezpieczeństwa funkcjonalnego są sformułowane w serii norm PN-EN 61508, opracowanych w celu:

- umożliwienia wykorzystania w pełni potencjału technologii elektronicznych, zwłaszcza programowalnych, zarówno w zakresie poprawy bezpieczeństwa, jak i wzrostu konkurencyjności
- umożliwienia rozwoju technologicznego w całym obszarze bezpieczeństwa
- dostarczenia podejścia systemowego, uwzględniającego postęp techniczny, elastycznego względem przyszłych zastosowań
- dostarczenia metody, która na podstawie oceny ryzyka umożliwi określenie wymaganej pewności działania układów związanych w bezpieczeństwem
- dostarczenia podstawowej normy, która może być bezpośrednio zastosowana przez przemysł, ale może okazać się także pomocna przy formułowaniu norm sektorowych (dotyczących np. maszyn, zakładów przetwórstwa chemicznego, medycyny czy kolejnictwa)
- dostarczenia użytkownikom oraz ustawodawcom środków umożliwiających zachowanie pewności w użytkowaniu technologii wspomaganych komputerowo
- dostarczenia wymagań, wynikających z oczywistych podstawowych zasad, umożliwiających:
  - poprawę efektywności w łańcuchu dostaw dla dostawców podukładów i elementów w różnych sektorach
  - ułatwienie porozumienia w formułowaniu wymagań
  - rozwój technik i środków, które mogą być stosowane we wszystkich sektorach, zwiększając tym samym dostępne zasoby
  - rozwój usług oceny zgodności, jeśli to konieczne.

Realizacja metodyki bezpieczeństwa funkcjonalnego polega na:

- stosowaniu oceny ryzyka w celu określenia wymagań nienaruszalności bezpieczeństwa w układach związanych z bezpieczeństwem
- wykorzystaniu modelu cyklu całkowitego życia bezpieczeństwa jako technicznych ram dla czynności niezbędnych do zapewnienia, że układy związane z bezpieczeństwem osiągają bezpieczeństwo funkcjonalne
- uwzględnianiu wszystkich działań cyklu życia bezpieczeństwa od koncepcji początkowej, poprzez analizę zagrożeń i ocenę ryzyka, sformułowanie wymagań bezpieczeństwa, specyfikację, zaprojektowanie i wdrożenie, obsługę i konserwację oraz modyfikację do końcowej likwidacji i/lub wyrzucenia
- uwzględnianiu aspektów systemowych (wraz ze wszystkimi podukładami realizującymi funkcje bezpieczeństwa, włączając w to sprzęt komputerowy i oprogramowanie) i mechanizmów defektów (przypadkowych i systematycznych)

– określeniu wymagań dotyczących zapobiegania uszkodzeniom (unikania defektów), jak również wymagań dotyczących kontrolowania uszkodzeń (co zapewnia bezpieczeństwo, nawet w razie wystąpienia defektów)
– określeniu technik i środków koniecznych do osiągnięcia wymaganej nienaruszalności bezpieczeństwa.

8.3. Poziomy nienaruszalności bezpieczeństwa

W normie PN-EN 61508 zdefiniowano cztery poziomy pewności działania funkcji bezpieczeństwa związanego z bezpieczeństwem. Są one nazywane poziomami nienaruszalności bezpieczeństwa. Poziom nienaruszalności bezpieczeństwa 1 (*SIL* 1) jest najniższy, a poziom nienaruszalności bezpieczeństwa 4 (*SIL* 4) najwyższy. Norma szczegółowo podaje wymagania niezbędne do osiągnięcia każdego z poziomów nienaruszalności bezpieczeństwa. Wymagania te są bardziej ostre na wyższych poziomach nienaruszalności bezpieczeństwa, tak aby uzyskać wymagane mniejsze prawdopodobieństwo uszkodzenia niebezpiecznego.

Poziom nienaruszalności bezpieczeństwa określa się jako prawdopodobieństwo wystąpienia defektu niebezpiecznego. Wyróżnia się dwa różne rodzaje pracy systemów realizujących funkcje bezpieczeństwa:

– **na częste lub ciągłe przywołanie:** gdy system związany z bezpieczeństwem jest przywoływany częściej niż raz na rok i częściej niż wynosi dwukrotność testów okresowych
– **na rzadkie przywołanie:** gdy system związany z bezpieczeństwem jest przywoływany nie częściej niż raz na rok i nie częściej niż wynosi dwukrotność testów okresowych.

Jeśli praca jest rodzaju na częste lub ciągłe przywołanie, prawdopodobieństwo to wyznacza się na godzinę. W drugim przypadku prawdopodobieństwo określa się na przywołanie. Wartości odpowiednich wskaźników podano w tabl. 8.1 i 8.2.

Tablica 8.1. Poziomy nienaruszalności bezpieczeństwa: miary docelowe uszkodzeń funkcji bezpieczeństwa działających w rodzaju pracy na rzadkie przywołanie (PN-EN 61508-1:2010)

Prawdopodobieństwo uszkodzenia niebezpiecznego na przywołanie	Poziom nienaruszalności bezpieczeństwa
od $\geq 10^{-2}$ do $< 10^{-1}$	*SIL* 1
od $\geq 10^{-3}$ do $< 10^{-2}$	*SIL* 2
od $\geq 10^{-4}$ do $< 10^{-3}$	*SIL* 3
od $\geq 10^{-5}$ do $< 10^{-4}$	*SIL* 4

Tablica 8.2. Poziomy nienaruszalności bezpieczeństwa: miary docelowe uszkodzeń funkcji bezpieczeństwa działających w rodzaju pracy na częste przywołanie lub ciągłym (PN-EN 61508-1:2010)

Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę	Poziom nienaruszalności bezpieczeństwa
od $\geq 10^{-6}$ do $< 10^{-5}$	*SIL* 1
od $\geq 10^{-7}$ do $< 10^{-6}$	*SIL* 2
od $\geq 10^{-8}$ do $< 10^{-7}$	*SIL* 3
od $\geq 10^{-9}$ do $< 10^{-8}$	*SIL* 4

W układach związanych z bezpieczeństwem zwykle stosuje się więcej niż jedną funkcję bezpieczeństwa. Jeśli wymagania nienaruszalności bezpieczeństwa różnią się dla tych funkcji, to do całego układu związanego z bezpieczeństwem należy stosować wymagania dla najwyższego występującego poziomu nienaruszalności bezpieczeństwa, chyba że można wykazać dostateczną niezależność poszczególnych funkcji.

8.4. Cykl życia systemu

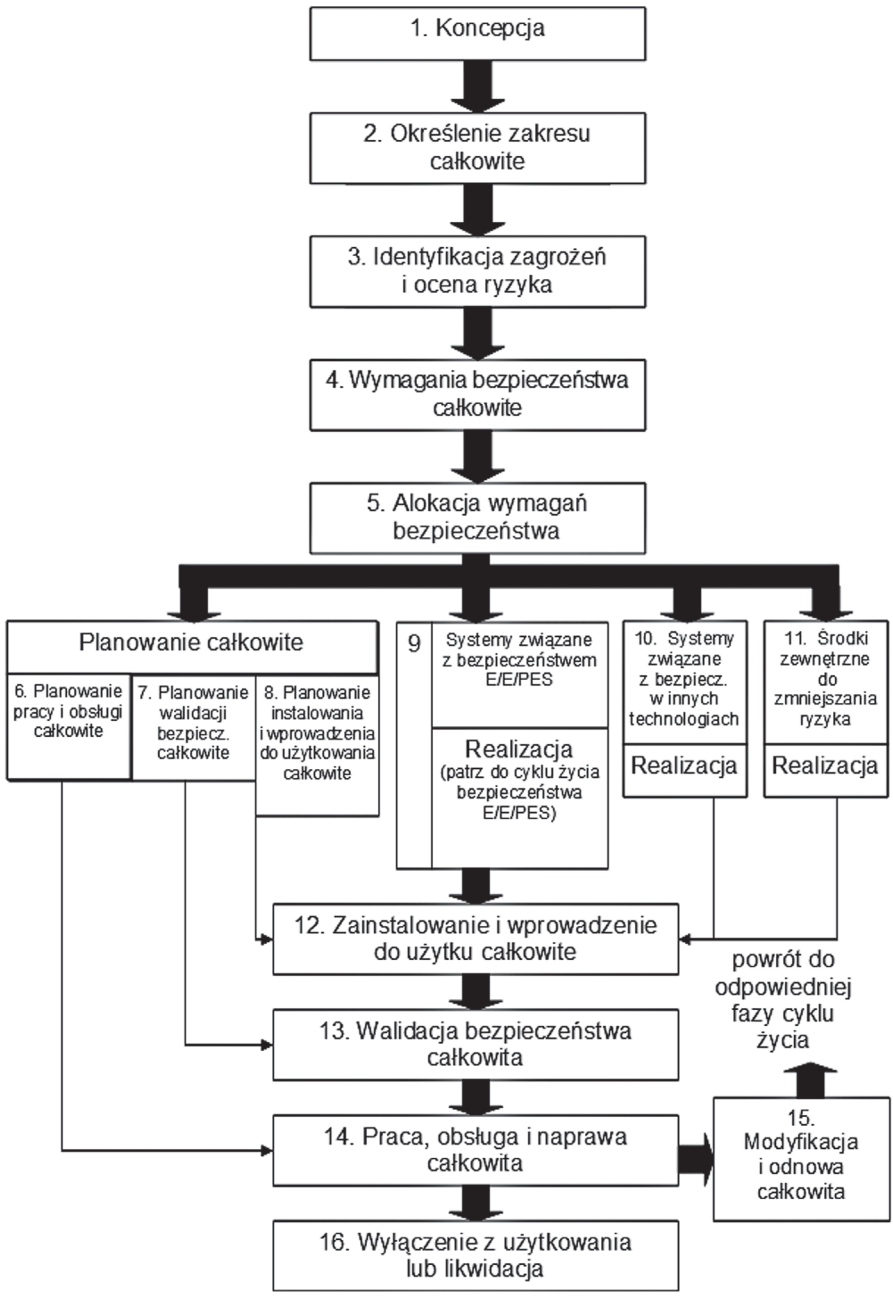
Ogólny cykl życia bezpieczeństwa systemów związanych z bezpieczeństwem jest szczegółowo scharakteryzowany w normie PN-EN 61508-1, rozdz. 7 „Wymagania dotyczące cyklu całkowitego życia bezpieczeństwa" (rys. 8.1).

Cykl ten został opracowany w celu usystematyzowania czynności koniecznych do osiągnięcia wymaganego poziomu nienaruszalności bezpieczeństwa systemów E/E/PE związanych z bezpieczeństwem (Dźwiarek, 2004c).

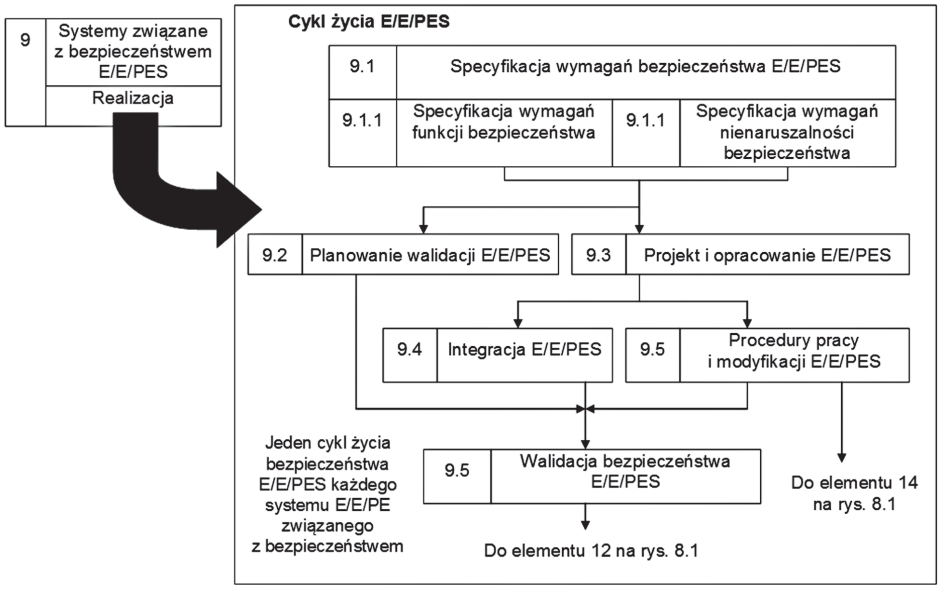
W cyklu całkowitym życia bezpieczeństwa przyjęto następujące środki zmniejszenia ryzyka:

- systemy E/E/PE związane z bezpieczeństwem
- systemy związane z bezpieczeństwem wykonane w innych technikach
- zewnętrzne środki zmniejszania ryzyka.

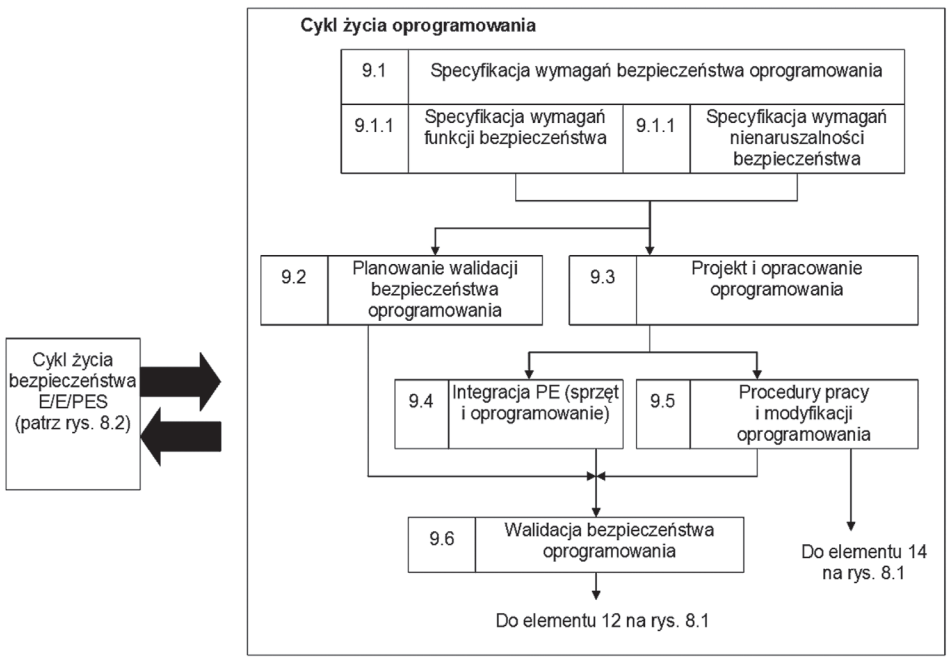
Część cyklu całkowitego życia bezpieczeństwa dotycząca systemów E/E/PE związanych z bezpieczeństwem, szczegółowiej przedstawiona na rys. 8.2, została nazwana cyklem życia bezpieczeństwa E/E/PES i tworzy podstawy techniczne do formułowania wymagań zawartych w PN-EN 61508-2. Cykl życia bezpieczeństwa oprogramowania pokazano na rys. 8.3. Tworzy on podstawy techniczne do formułowania wymagań zawartych w PN-EN 61508-3. Relację cyklu całkowitego życia bezpieczeństwa do cykli życia bezpieczeństwa E/E/PES i oprogramowania przedstawiono na rys. 8.4.



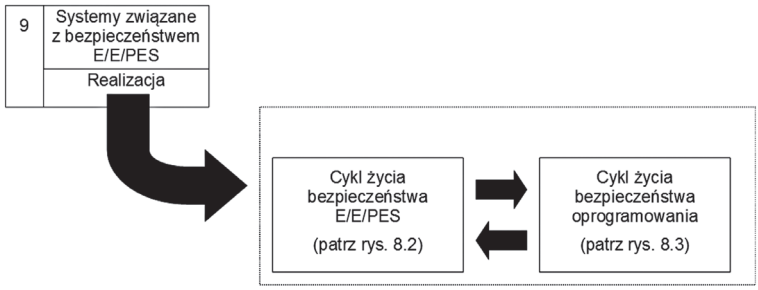
Rys. 8.1. Cykl całkowity życia bezpieczeństwa związanego z bezpieczeństwem systemu sterowania (PN-EN 61508-1:2010)



Rys. 8.2. Cykl życia bezpieczeństwa sprzętu w fazie realizacji (PN-EN 61508-1:2010)



Rys. 8.3. Cykl życia bezpieczeństwa oprogramowania w fazie realizacji (PN-EN 61508-1:2010)



Rys. 8.4. Relacje między cyklem całkowitym życia bezpieczeństwa a cyklami E/E/PES i oprogramowania (PN-EN 61508-1:2010)

Do poszczególnych faz cyklu życia bezpieczeństwa przypisane są odpowiednie wymagania dotyczące zapewnienia bezpieczeństwa. Wymagania te pogrupowane są w następujący sposób:

1. Koncepcja
2. Określenie zakresu całkowitego
3. Analiza zagrożeń i ryzyka
4. Wymagania bezpieczeństwa całkowite
5. Alokacja wymagań bezpieczeństwa
6. Planowanie całkowite pracy i obsługi
7. Planowanie całkowite walidacji bezpieczeństwa
8. Planowanie całkowite instalowania i wprowadzenia do eksploatacji
9. Realizacja: E/E/PES
10. Realizacja: inne techniki
11. Realizacja: środki zewnętrzne do zmniejszania ryzyka
12. Zainstalowanie całkowite i wprowadzenie do eksploatacji
13. Walidacja całkowita bezpieczeństwa
14. Całkowita praca, obsługa i naprawa
15. Całkowita modyfikacja i odnowa
16. Wyłączenie z eksploatacji lub likwidacja

Cykle życia bezpieczeństwa: całkowitego, E/E/PES i oprogramowania (rys. 8.1 do rys. 8.3) są uproszczonym przedstawieniem rzeczywistości i tym samym nie mogą pokazywać wszystkich iteracji odnoszących się do poszczególnych faz lub zachodzących między fazami. Jednakże iteracja jest podstawową i najistotniejszą częścią rozwoju przez cykle życia bezpieczeństwa: całkowity, E/E/PES i oprogramowania. W celu uproszczenia reprezentacji graficznej na rysunkach nie uwzględniono czynności dotyczących zarządzania bezpieczeństwem

funkcjonalnym, weryfikacji i oceny bezpieczeństwa funkcjonalnego. W szczególnych przypadkach celowe może się okazać uwzględnienie ich w poszczególnych fazach cyklu życia. W ogólności należy jednak pamiętać, że są one znaczącym elementem uzyskiwania bezpieczeństwa funkcjonalnego urządzeń w każdej fazie ich cyklu życia.

W rozdziałach 7.2 do 7.17 normy PN-EN 61508-1 określono cele i wymagania poszczególnych faz cyklu życia systemu jako całości. Cele i wymagania odnoszące się do cykli życia bezpieczeństwa E/E/PES i oprogramowania są zawarte odpowiednio w PN-EN 61508-2 i PN-EN 61508-3.

Wszystkie działania podejmowane w poszczególnych fazach cyklu życia powinny być dokumentowane wraz z ich efektami. W tabl. 1 w normie PN-EN 61508-1 zostały określone:

- cele, jakie mają zostać osiągnięte w poszczególnych fazach
- zakresy zastosowań faz
- powołania podrozdziałów zawierających wymagania
- dane wejściowe wymagane do fazy
- dane wyjściowe wymagane do spełnienia wymagań.

Podstawowym celem wymagań dotyczących cyklu całkowitego życia bezpieczeństwa jest uporządkowanie tych jego faz, które odgrywają istotną rolę w uzyskiwaniu wymaganego bezpieczeństwa funkcjonalnego systemów E/E/PE związanych z bezpieczeństwem.

Należy więc stwierdzić, że podstawą deklarowania zgodności z normami PN-EN 61508 jest stosowanie cyklu życia pokazanego na rys. 8.1 – 8.4. Możliwe jest oczywiście stosowanie innego cyklu życia. Jednak wówczas powinien on być precyzyjnie określony w planach bezpieczeństwa funkcjonalnego. Należy przy tym zapewnić, że spełnione będą wszystkie cele i wymagania dotyczące cyklu życia podane w PN-EN 61508.

Jednocześnie z fazami cyklu całkowitego życia bezpieczeństwa powinny być formułowane wymagania dotyczące zarządzania bezpieczeństwem funkcjonalnym.

Podstawą deklarowania zgodności z normą jest zapewnienie, że:

- każda faza cyklu całkowitego życia bezpieczeństwa zostanie uwzględniona, chyba że jasno uzasadnione zostaną szczególne odstępstwa
- każda faza cyklu całkowitego życia bezpieczeństwa zostanie podzielona na czynności elementarne, o zakresie, wejściach i wyjściach wyszczególnionych w ramach każdej fazy
- zakres i wejścia każdej fazy cyklu całkowitego życia bezpieczeństwa powinny być takie, jak wyszczególniono w tabl. 1 w PN-EN 61508-1
- jeśli nie uzasadniono inaczej w planie bezpieczeństwa funkcjonalnego lub nie wyszczególniono inaczej w normach sektorowych, to wyjścia z każdej

fazy cyklu całkowitego życia bezpieczeństwa zostaną udokumentowane tak, jak to wyszczególniono w tabl. 1 w PN-EN 61508-1
- wyjścia z każdej fazy cyklu całkowitego życia bezpieczeństwa powinny być zgodne z celami i spełniać wymagania każdej fazy
- wymagania dotyczące weryfikacji, które powinny być spełnione w każdej fazie cyklu całkowitego życia bezpieczeństwa, są takie jak wyszczególniono w p. 7.18 normy.

Podstawową zasadą jest, że do każdej fazy cyklu całkowitego życia bezpieczeństwa należy opracować plan określający:
- harmonogram postępowania
- osoby odpowiedzialne za wykonanie poszczególnych czynności w danej fazie
- procedury postępowania
- kryteria oceny, czy wszystkie niezbędne działania zostały przeprowadzone prawidłowo
- procedury postępowania w razie wykrycia niezgodności lub odstępstw.

8.5. Dokumentowanie cyklu życia

Istotnym elementem bezpieczeństwa funkcjonalnego jest zapewnienie udokumentowania, w ciągu całkowitego cyklu życia bezpieczeństwa, kluczowych informacji dotyczących bezpieczeństwa funkcjonalnego systemów E/E/PE związanych z bezpieczeństwem (Dźwiarek, 2003, 2006), zarówno w aspekcie zawartości merytorycznej dokumentacji, jak i jej struktury. Powinna ona uwzględniać dotychczasowe doświadczenia przedsiębiorstwa, ale także procedury i praktykę postępowania wypracowaną w konkretnych sektorach.

Dokumentacja niezbędna do uporządkowania informacji, aby spełnić wymagania bezpieczeństwa funkcjonalnego, powinna zawierać wystarczające informacje konieczne do:
- wypełnienia każdej fazy cykli życia bezpieczeństwa całkowitego, E/E/PES i oprogramowania
- zarządzania bezpieczeństwem funkcjonalnym
- oceny bezpieczeństwa funkcjonalnego.

Minimalna zawartość wystarczającej informacji zależy od różnych czynników, zwłaszcza od złożoności i rozmiaru systemów E/E/PE związanych z bezpieczeństwem i wymagań dotyczących konkretnego zastosowania. Zakres niezbędnej dokumentacji może być określony w normach dotyczących konkretnego sektora zastosowań. Zawartość każdego dokumentu może się zmieniać od kilku wierszy do wielu stronic, a całkowity zbiór informacji może

być podzielony i przedstawiany w wielu fizycznych dokumentach lub w jednym dokumencie. Struktura dokumentacji fizycznej zależy także od rozmiaru i złożoności systemów E/E/PE związanych z bezpieczeństwem i odpowiada procedurom przedsiębiorstwa oraz przyjętej praktyce w konkretnym sektorze zastosowań.

Przykładową strukturę dokumentacji całkowitego cyklu życia bezpieczeństwa pokazano w tabl. 8.3. Podobnie wygląda struktura dokumentacji dotyczącej cyklu życia sprzętu oraz cyklu życia oprogramowania. Bardziej szczegółowe informacje dotyczące zakresu dokumentacji cyklu życia podano w zał. A do PN-EN 61508-1. Należy jednak pamiętać, że zgodnie z podstawową zasadą wszelkie działania w każdej fazie cyklu życia bezpieczeństwa powinny być szczegółowo udokumentowane.

Tablica 8.3. Przykładowa struktura dokumentacji z informacjami związanymi z całkowitym cyklem życia bezpieczeństwa (PN-EN 61508-1:2010)

Faza cyklu całkowitego życia bezpieczeństwa	**Informacja**
Koncepcja	opis (koncepcja całkowita)
Określenie całkowite zakresu	opis (określenie całkowite zakresu)
Analiza zagrożeń i ryzyka	opis (analiza zagrożeń i ryzyka)
Wymagania całkowite bezpieczeństwa	specyfikacja (wymagania całkowite bezpieczeństwa, obejmujące funkcje całkowite bezpieczeństwa i całkowitą nienaruszaność bezpieczeństwa)
Przypisanie wymagań bezpieczeństwa	opis (przypisanie wymagań bezpieczeństwa)
Planowanie całkowite pracy i obsługi	plan (całkowita praca i obsługa)
Planowanie całkowitej walidacji bezpieczeństwa	plan (walidacja całkowita bezpieczeństwa)
Planowanie całkowite instalowania i wprowadzenia do eksploatacji	plan (zainstalowanie całkowite) plan (wprowadzenie do eksploatacji całkowite)
Realizacja	realizacja systemów E/E/PE związanych z bezpieczeństwem (patrz PN-EN 61508-2 i PN-EN 61508-3)
Zainstalowanie całkowite i wprowadzenie do eksploatacji	sprawozdanie (zainstalowanie całkowite); sprawozdanie (wprowadzenie do eksploatacji całkowite)

Tablica 8.3. cd.

Faza cyklu całkowitego życia bezpieczeństwa	Informacja
Całkowita walidacja bezpieczeństwa	sprawozdanie (całkowita walidacja bezpieczeństwa)
Całkowita praca i obsługa	dziennik (całkowita praca i obsługa)
Całkowita modyfikacja i odnowa	żądanie (modyfikacja całkowita); sprawozdanie (analiza oddziaływań przy modyfikacji całkowitej i odnowie); dziennik (modyfikacja całkowita i odnowa)
Wyłączenie z eksploatacji lub likwidacja	sprawozdanie (analiza oddziaływań przy wyłączeniu z ruchu całkowitym lub likwidacji); plan (wyłączenie z ruchu całkowite lub likwidacja); dziennik (wyłączenie z ruchu całkowite lub likwidacja)
Dotyczy wszystkich faz	plan (bezpieczeństwo); plan (weryfikacja); sprawozdanie (weryfikacja); plan (ocena bezpieczeństwa funkcjonalnego); sprawozdanie (ocena bezpieczeństwa funkcjonalnego)

8.6. Sektorowe dokumenty normatywne

Koncepcja bezpieczeństwa funkcjonalnego zawarta w normie PN-EN 61508 jest przykładem dobrej praktyki inżynierskiej w projektowaniu i eksploatacji systemów elektrycznych, elektronicznych i programowalnych elektronicznych związanych z bezpieczeństwem. Systemy takie są obecnie coraz szerzej stosowane w przemyśle i gospodarce. Bezpieczeństwo funkcjonalne jest postrzegane jako istotna część nowoczesnych systemów zarządzania jakością, bezpieczeństwem (pracy) czy zarządzania środowiskowego. Stosowane rozwiązania systemów zabezpieczeniowych w przemyśle są i będą coraz częściej oceniane pod kątem wymagań bezpieczeństwa funkcjonalnego przez organy nadzoru technicznego i firmy ubezpieczeniowe. Wymagania zawarte w normie PN-EN 61508 są również uwzględniane w zamówieniach wyposażenia systemów związanych z bezpieczeństwem. Producenci wyposażenia podają coraz częściej, jaki poziom nienaruszalności bezpieczeństwa (*SIL*) zapewniają produkowane u nich urządzenia. W efekcie projektanci i użytkownicy systemów produkcyjnych coraz powszechniej w swojej praktyce spotykają się z problematyką bezpieczeństwa funkcjonalnego (Dźwiarek, 2004b; Dźwiarek i Kosmowski, 2007).

8.6.1. PN-EN 61508 jako podstawa dla innych norm

Norma PN-EN 61508 określa ogólne zasady postępowania we wszystkich działaniach cyklu życia tych urządzeń E/E/EP związanych z bezpieczeństwem, które stosowane są do realizacji funkcji bezpieczeństwa. To ujednolicone podejście zostało przyjęte ze względu na konieczność wypracowania spójnej i racjonalnej metodologii postępowania z urządzeniami E/E/EP związanymi z bezpieczeństwem, bez względu na branżę, w której są stosowane. Głównym celem normy jest określenie punktu odniesienia przy formułowaniu norm i przewodników dla różnych branż oraz wspomaganie projektowania specjalistycznych urządzeń i podzespołów. Dlatego cztery pierwsze części normy są zaliczane do podstawowych publikacji w dziedzinie bezpieczeństwa.

Twórcy norm sektorowych uwzględniają bezpieczeństwo funkcjonalne w swoich normach, jeśli z analizy zagrożeń przeprowadzonej przez Komitet Techniczny wynika, że jest to niezbędne, aby odpowiednio zapobiegać znaczącym zagrożeniom lub zdarzeniom niebezpiecznym.

Zasada ta została określona w przewodnikach IEC (International Electrotechnical Commission):

- IEC Guide 104, *The preparation of safety publications and the use of basic safety publications and group safety publications*
- ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*.

Stały postęp prac normalizacyjnych powoduje, że powstaje coraz więcej norm dotyczących szczególnych sektorów lub urządzeń i zawierających odniesienie do metodyki bezpieczeństwa funkcjonalnego. Obecnie najbardziej zaawansowane w tym zakresie są prace dotyczące normalizacji w obszarze sektora energii nuklearnej, procesów produkcyjnych, transportu, maszyn. Powstają także normy dotyczące wyrobów, zawierające wymagania bezpieczeństwa funkcjonalnego (silniki o regulowanej prędkości, przemysłowe czujniki gazu itp.). A zatem metodyka ta ma wpływ na rozwój układów i produktów E/E/EP związanych z bezpieczeństwem we wszystkich branżach. Normy sektorowe określają szczególne wymagania dotyczące różnych zastosowań układów E/E/EP związanych z bezpieczeństwem (zwykle właściwe dla danego sektora) oraz szczegółowe wymagania konstrukcyjne (zwykle nie zależą od sektora). Tak więc, normy sektorowe określają zasady budowania systemów właściwych dla danego sektora z wykorzystaniem powszechnie dostępnych urządzeń konstruowanych zgodnie z wymaganiami PN-EN 61508.

8.6.2. Sektor maszynowy

Norma PN-EN 62061:2008 adaptuje metodykę określania wymagań związanych z bezpieczeństwem funkcjonalnym przedstawioną w serii norm PN-EN 61508 do specyfiki systemów sterowania maszynami. Formułuje ona podstawowe zalecenia dotyczące projektowania i wykonywania urządzeń zasilanych energią elektryczną.

Tablica 8.4. Poziomy nienaruszalności bezpieczeństwa (*SIL*) a poziomy zapewnienia bezpieczeństwa (*PL*), (PN-EN ISO 13849-1:2008)

PL	***SIL***
a	–
b	*SIL* 1
c	
d	*SIL* 2
e	*SIL* 3

Systemy sterowania realizujące funkcje bezpieczeństwa są klasyfikowane pod względem zapewnianych poziomów nienaruszalności bezpieczeństwa. Poziom nienaruszalności bezpieczeństwa (*SIL*) jest określany przedziałem prawdopodobieństwa wystąpienia w ciągu godziny zdarzenia utraty zdolności do realizacji funkcji bezpieczeństwa. Wartości prawdopodobieństwa dla poszczególnych *SIL* są takie, jak w normie PN-EN 61508 (patrz tabl. 8.2), a ich powiązanie z poziomami zapewniania bezpieczeństwa, *PL*, podano w tabl. 8.4. Ze względu na specyfikę sterowania maszynami, w normie PN-EN 62061 nie uwzględnia się *SIL* 4 i rozważa się jedynie systemy działające ciągle lub na częste przywołanie (Dźwiarek, 2000a, 2000b, 2007, 2008b).

Wymagania dotyczące systemów sterowania maszynami uwzględniają w zasadzie wszystkie etapy ich cyklu życia. Zostały pogrupowane według aspektów, których dotyczą, w następujący sposób:

- zarządzanie bezpieczeństwem funkcjonalnym w cyklu życia systemu
- formułowanie założeń dotyczących funkcji bezpieczeństwa
- projektowanie i wykonywanie systemu
- informacje dla użytkownika
- walidacja systemu
- modyfikacje systemu.

Ocena ryzyka w celu wyznaczenia wymagań bezpieczeństwa jest w przypadku stosowania metodyki z normy PN-EN 62061:2008 bardziej szczegółowa niż w normie PN-EN ISO 13849-1. Ciężkość szkody jest klasyfikowana zgodnie z tabl. 8.5.

Częstość narażenia i czas trwania ekspozycji na zagrożenie są klasyfikowane według skali punktowej zgodnie z tabl. 8.6.

Tablica 8.5. Klasyfikacja ciężkości szkody (*Se*), (PN-EN 62061:2008)

Konsekwencje	**Ciężkość szkody (*Se*)**
Nieodwracalne: śmierć, utrata oka lub ręki	4
Nieodwracalne: złamania kończyn(-y), utrata palca(-ów)	3
Odwracalne: wymagana interwencja personelu medycznego	2
Odwracalne: wymagana pierwsza pomoc	1

Tablica 8.6. Klasyfikacja częstości narażenia i czasu trwania ekspozycji (*Fr*), (PN-EN 62061:2008)

Częstość narażenia i czas ekspozycji (*Fr*)		
Czas *t* pomiędzy sytuacjami wystąpienia narażenia	**Czas ekspozycji < 10 min**	**Czas ekspozycji > 10 min**
$t \leq 1$ h	5 pkt	5 pkt
1 h $< t \leq$ 1 dzień	4 pkt	5 pkt
1 dzień $< t \leq$ 2 tygodnie	3 pkt	4 pkt
2 tygodnie $< t \leq$ 1 rok	2 pkt	3 pkt
1 rok $< t$	1 pkt	2 pkt

Prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego (Pr) określa się według następującej 5-stopniowej skali punktowej:

5 pkt – bardzo wysokie (zdarzenie niebezpieczne występuje regularnie z dużą częstością)
4 pkt – dogodne (zdarzenie niebezpieczne występuje regularnie z małą częstością)
3 pkt – możliwe (wystąpienie zdarzenia niebezpiecznego jest możliwe)
2 pkt – rzadkie (zdarzenie niebezpieczne występuje rzadko)
1 pkt – pomijalne (wystąpienie zdarzenia niebezpiecznego można pominąć).

Natomiast prawdopodobieństwo (możliwość) uniknięcia lub ograniczenia szkody (Av) szacuje się według następującej 3-stopniowej skali punktowej:

5 pkt – brak możliwości uniknięcia lub ograniczenia szkody
3 pkt – czasem (rzadko) istnieje możliwość uniknięcia lub ograniczenia szkody
1 pkt – prawdopodobne jest uniknięcie lub ograniczenie szkody.

Klasę prawdopodobieństwa wystąpienia szkody *Cl* wyznacza się na podstawie sumy punktów *Fr*, Pr i Av. Następnie, na podstawie wskaźnika ciężkości szkody oraz klasy prawdopodobieństwa *Cl*, wyznacza się wymagane *SIL* według tabl. 8.7

Tablica 8.7. Określenie *SIL* wymaganego dla funkcji bezpieczeństwa (PN-EN 62061:2008)

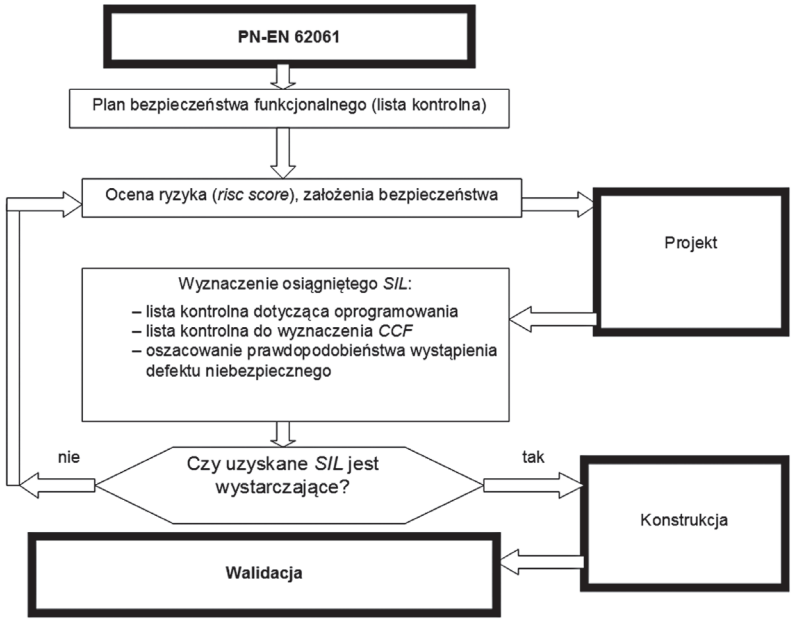
Ciężkość szkody (*Se*)	**Klasa prawdopodobieństwa wystąpienia szkody (*Cl*) [pkt]**				
	3-4	**5-7**	**8-10**	**11-13**	**14-15**
4	*SIL* 2	*SIL* 2	*SIL* 2	*SIL* 3	*SIL* 3
3		(OM)	*SIL* 1	*SIL* 2	*SIL* 3
2			(OM)	*SIL* 1	*SIL* 2
1				(OM)	*SIL* 1

W tabl. 8.7 obszarem szarym (OM) oznaczono zakres dopuszczalny pod warunkiem zastosowania innych środków bezpieczeństwa. Wynik oceny ryzyka powinien być odpowiednio udokumentowany.

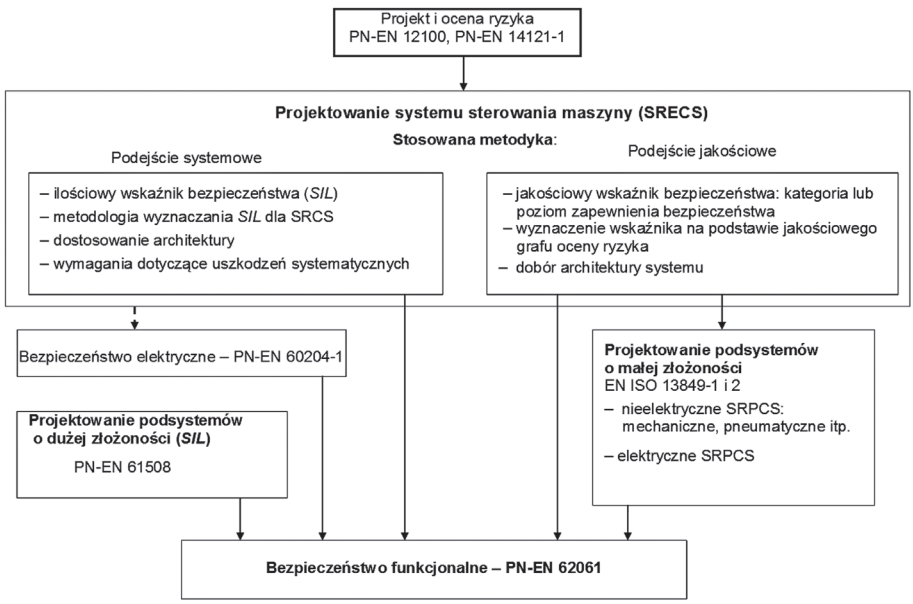
Po określeniu wymaganego *SIL* należy dobrać architekturę sprzętową systemu sterowania. Podstawową zasadą zalecaną w projektowaniu systemu sterowania jest jego dekompozycja na podsystemy wprowadzana już na etapie formułowania założeń. Dotyczy to zarówno definiowania funkcji bezpieczeństwa, które należy dzielić na funkcje elementarne, jak i zespołów realizujących te funkcje. W zespołach tych powinno się wydzielać podzespoły. Proces dekompozycji powinien być prowadzony stopniowo, aż do poziomu gotowych podzespołów, nabywanych na rynku. Podzespoły takie powinny mieć deklaracje producenta dotyczące zapewnianego przez nie poziomu nienaruszalności bezpieczeństwa określonego zgodnie z wymaganiami PN-EN 61508. Na podstawie tych deklaracji oraz zastosowanych rozwiązań konstrukcyjnych określa się *SIL* zestawionego w ten sposób systemu sterowania.

Norma PN-EN 62061:2008 traktuje projektowanie systemu sterowania określonej maszyny jako proces zestawiania go z gotowych podzespołów w większą całość. Może być stosowana zarówno przez projektantów nowych maszyn, jak i przez projektantów doposażających konkretne stanowiska pracy w dodatkowe środki bezpieczeństwa oparte na metodach sterowania.

Zasady doboru architektury systemu sterowania podano w rozdziale 6.6.2.1 normy PN-EN 62061:2008. Po określeniu architektury systemu i jego zaprojektowaniu należy dokonać weryfikacji osiągniętego *SIL*, na podstawie znajomości *SIL* podzespołów. W razie uzyskania negatywnego wyniku oceny *SIL* konieczna jest modyfikacja projektu. Natomiast wynik pozytywny umożliwia przystąpienie do wykonania systemu, a następnie do jego walidacji.



Rys. 8.5. Algorytm postępowania zgodnie z normą PN-EN 62061:2008



Rys. 8.6. Zasady stosowania norm w procesie formułowania wymagań dotyczących bezpieczeństwa funkcjonalnego (PN-EN 62061:2008)

Algorytm postępowania podczas określania wymagań bezpieczeństwa według normy PN-EN 62061:2008 pokazano na rys. 8.5

Stosowanie normy PN EN 62061:2008 w znacznym stopniu upraszcza procedurę deklarowania zgodności z postanowieniami dyrektywy maszynowej 2006/42/WE.

Wzajemne powiązania między normami określającymi wymagania związane z bezpieczeństwem funkcjonalnym przedstawiono na rys. 8.6.

8.6.3. Sektor procesów produkcyjnych

Układy zawierające oprzyrządowanie związane z bezpieczeństwem są stosowane od wielu lat do realizacji funkcji związanych z bezpieczeństwem w procesach produkcyjnych. Aby oprzyrządowanie to można było skutecznie w tym celu stosować, oczywiście musi ono spełniać pewne minimalne wymagania dotyczące bezpieczeństwa.

Norma PN-EN 61511 dotyczy stosowania systemów zawierających oprzyrządowanie związane z bezpieczeństwem w procesach przemysłowych. Określa zasady prowadzenia analizy zagrożeń oraz oceny ryzyka w celu umożliwienia prawidłowego formułowania wymagań dotyczących tego oprzyrządowania. Inne układy związane z bezpieczeństwem są rozważane tylko w takim zakresie, w jakim należy je uwzględnić, określając wymagania dotyczące działania układów zawierających oprzyrządowanie związane z bezpieczeństwem. Układ zawierający oprzyrządowanie związane z bezpieczeństwem obejmuje wszystkie elementy i podukłady konieczne do realizacji funkcji bezpieczeństwa, począwszy od czujników aż do urządzeń wykonawczych.

Omawiana norma uwzględnia oba podstawowe aspekty bezpieczeństwa: cykl życia oraz poziomy nienaruszalności bezpieczeństwa. Dotyczy układów zawierających oprzyrządowanie związane z bezpieczeństwem, oparte na technologii układów elektrycznych/elektronicznych/elektronicznych programowalnych (E/E/EP). Zasady tej normy mogą być także stosowane do układów logicznych zbudowanych w innych technologiach. Norma ta dotyczy także czujników i elementów końcowych układów zawierających oprzyrządowanie związane z bezpieczeństwem bez względu na zastosowaną technologię.

W normie PN-EN 61511 określono sposób postępowania w poszczególnych etapach cyklu życia bezpieczeństwa niezbędny do spełnienia wymagań bezpieczeństwa.

W większości przypadków najlepszą drogą do osiągnięcia bezpieczeństwa jest zaprojektowanie procesu bezpiecznego wewnętrznie, tam gdzie to konieczne w połączeniu z układami ochronnymi wykonanymi w różnych technologiach (chemicznymi, mechanicznymi, hydraulicznymi, pneumatycznymi, elektrycznymi, elektronicznymi, elektronicznymi programowalnymi), które redukują ryzyko do poziomu ryzyka szczątkowego. Norma określa sposób realizacji tego celu poprzez:

- wymaganie przeprowadzenia oceny zagrożeń i ryzyka w celu określenia ogólnych wymagań bezpieczeństwa
- wymaganie przeprowadzenia alokacji wymagań bezpieczeństwa dotyczących układów zawierających oprzyrządowanie związane z bezpieczeństwem
- zastosowanie wszystkich metod uzyskiwania bezpieczeństwa funkcjonalnego
- wymaganie stosowania działań organizacyjnych, takich jak zarządzanie bezpieczeństwem, które mogą mieć zastosowanie we wszystkich etapach osiągania bezpieczeństwa funkcjonalnego.

Celem wprowadzenia normy PN-EN 61511 jest osiągnięcie wysokiego stopnia zgodności (np. przez podanie zasad, terminologii czy informacji) w obszarze procesów przemysłowych. Przewiduje się, że przyniesie to korzyści zarówno w zakresie bezpieczeństwa procesów, jak i ekonomiczne.

Norma ta składa się z trzech części:

- część 1 – formułuje wymagania dotyczące specyfikacji, projektowania, instalowania, działania i konserwacji układów zawierających oprzyrządowanie związane z bezpieczeństwem, niezbędne do zapewnienia bezpiecznego przebiegu procesu. Jest ona sektorowym wdrożeniem normy PN-EN 61508
- część 2 – jest przewodnikiem do stosowania części 1
- część 3 – opisuje zasady określania poziomów nienaruszalności bezpieczeństwa przez analizę zagrożeń i ryzyka.

8.6.4. Napędy z regulowaną prędkością

W układach sterowania coraz częściej są stosowane elektryczne układy napędowe z nastawną prędkością (PDS). Jeśli są to układy związane z bezpieczeństwem, należy stosować zasady bezpieczeństwa funkcjonalnego. Zasady takie w odniesieniu do układów napędowych o regulowanej prędkości formułuje dokument PN-EN 61800-5-2.

Układy sterowania zawierające PDS są powszechnie spotykane, na przykład jako element środków bezpieczeństwa użytych w celu zmniejszenia ryzyka. Typowym przykładem jest ryglowana osłona ograniczająca dostęp do strefy zagrożenia. Dostęp powinien być możliwy tylko wówczas, gdy części ruchome osiągają prędkości uznane za bezpieczne. W normie określono metodykę identyfikacji udziału PDS w realizacji funkcji bezpieczeństwa oraz zasady projektowania i walidacji wymaganego działania. Podano także środki potrzebne do koordynacji działania PDS związanego z bezpieczeństwem z wymaganiami dotyczącymi redukcji ryzyka, z uwzględnieniem prawdopodobieństwa i skutków jego przypadkowego i systematycznego defektu.

PN-EN 61800-5-2 jest normą przedmiotową, w której określono wymagania i podano zalecenia dotyczące projektowania, integracji i walidacji elektrycznych

układów napędowych z nastawną prędkością przeznaczonych do zastosowań związanych z bezpieczeństwem (PDS), poprzez analizę ich bezpieczeństwa funkcjonalnego.

Normę tę stosuje się wówczas, gdy bezpieczeństwo funkcjonalne PDS ma istotne znaczenia i gdy PDS pracuje w ostrym reżimie lub w trybie ciągłym. Określono w niej zasady analizy aspektów bezpieczeństwa PDS w zakresie określonym przez PN-EN 61508 i wprowadzono wymagania dla PDS jako podzespołów systemów związanych z bezpieczeństwem. Jej celem jest ułatwienie wykonywania elementów elektrycznych/elektronicznych/elektronicznych programowalnych w PDS w aspekcie realizacji funkcji bezpieczeństwa.

Producenci i dostawcy PDS, wykorzystując wymagania normy, wskazują użytkownikom (tzn. projektantom układów sterowania, maszyn, instalacji itp.) wymagane wartości *SIL* (PN-EN 61508) lub poziom zapewnienia bezpieczeństwa *PL* (PN-EN ISO 13849-1). Ułatwia to włączenie PDS w układ sterowania związany z bezpieczeństwem z wykorzystaniem zasad podanych w normie PN-EN 61508 lub szczególnych normach sektorowych, np. PN-EN 61511, IEC 61513:2001 i PN-EN 62061 oraz w ISO 13849-1.

8.6.5. Inne normy sektorowe i przedmiotowe

W poprzednich rozdziałach omówiono najważniejsze sektorowe wymagania bezpieczeństwa funkcjonalnego zawarte w normach PN-EN 61511, PN-EN 62061:2005 oraz normie przedmiotowej IEC 61800-5-2. Normy te są przykładami wdrażania zasad bezpieczeństwa funkcjonalnego w różnych sektorach przemysłu oraz w formułowaniu wymagań dotyczących wyrobów. Prace normalizacyjne dotyczące stosowania metodyki bezpieczeństwa funkcjonalnego są stale rozwijane i obejmują coraz większy obszar zastosowań. A oto przykłady:

- IEC 61513:2011 Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems (Elektrownie jądrowe – Oprzyrządowanie i sterowanie układów ważnych dla bezpieczeństwa – Ogólne wymagania dla układów)
- PN-EN 60601-1-1:2002 (U) Medyczne urządzenia elektryczne. Część 1-1: Ogólne wymagania bezpieczeństwa. Norma uzupełniająca. Wymagania bezpieczeństwa medycznych systemów elektrycznych
- PN-EN 60601-1-4:2006 Medyczne urządzenia elektryczne. Część 1-4: Ogólne wymagania bezpieczeństwa. Norma uzupełniająca. Medyczne systemy elektryczne programowane
- PN-EN 61326-3-1:2010. Wyposażenie elektryczne do pomiarów, sterowania i użytku w laboratoriach – Wymagania dotyczące kompatybilności elektromagnetycznej (EMC) – Część 3-1: Wymagania odporności dotyczące

systemów związanych z bezpieczeństwem i wyposażenia przeznaczonego do wypełniania funkcji związanych z bezpieczeństwem (bezpieczeństwo funkcjonalne) – Ogólne zastosowania przemysłowe
- ISO/IEC/TR 14762 (2001-01) Information technology – Home Control Systems – Guidelines for functional safety
- PN-ISO/IEC 14762:2010 Technika informatyczna – Wymagania bezpieczeństwa funkcjonalnego dla domowych i budynkowych systemów elektronicznych (HBES)
- PN-EN 50402:2007 Urządzenia elektryczne przeznaczone do wykrywania i pomiaru wybuchowych lub toksycznych gazów i par oraz tlenu. Wymagania bezpieczeństwa funkcjonalnego stacjonarnych systemów wykrywania gazów
- PN-EN 50126:2002 Zastosowania kolejowe. Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa
- PN-EN 50128:2011 Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Programy dla kolejowych systemów sterowania i zabezpieczenia
- PN-EN 50129:2007 Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.

Rozdział 9

Narzędzia metodyczne wspierające ocenę ryzyka na etapie projektowania maszyn

9.1. Wprowadzenie

Ocena ryzyka jest ciągiem logicznych kroków mających na celu określenie, w usystematyzowany sposób, ryzyka związanego z obsługą maszyn. Podstawowe zasady prowadzenia i dokumentowania oceny ryzyka zostały przedstawione w pracach (Dźwiarek, 2008a, 2008c). Zasady te opracowano zgodnie z normą PN-EN ISO 12100:2011. W ocenie ryzyka szczególną uwagę należy zwrócić na systematyczność prowadzonych działań oraz ich udokumentowanie. Zastosowanie do tego celu narzędzi komputerowych może w znacznym stopniu uprościć całą procedurę oraz ułatwić wygenerowanie jednorodnej dokumentacji. Przykładem odpowiedniego oprogramowania jest opracowany przez Centrum Zaawansowanych Technologii „Technology Partners" program ekspercki PRO-M. Program ten został opracowany przede wszystkim z myślą o producentach maszyn, ale może być także stosowany podczas ich modernizacji i przebudowy.

9.2. Metodyka prowadzenia oceny ryzyka

Ogólną strategię stosowania środków ochronnych do maszyn podano w normie PN-EN ISO 12100:2011. Środki ochronne powinny być stosowane zarówno przez projektanta maszyny, jak i przez jej użytkownika. Jednak środki stosowane przez projektanta są zazwyczaj znacznie skuteczniejsze, dlatego też należy im przypisać szczególne znaczenie. Projektant maszyny, dobierając środki ochronne, powinien stosować następującą ich hierarchię:

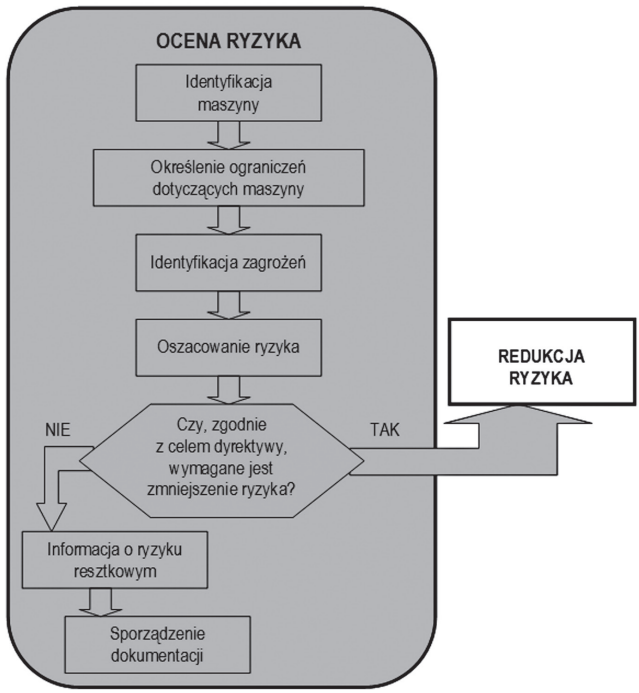
1) konstrukcja bezpieczna sama w sobie
2) stosowanie technicznych i uzupełniających środków ochronnych
3) informowanie o ryzyku resztkowym.

Hierarchia ta ma także odzwierciedlenie w dyrektywie 2006/42/WE, określającej podstawowe obowiązki producenta maszyny. Dyrektywa ta w art. 5 p. 1 stanowi między innymi:

1. *Producent maszyny lub jego upoważniony przedstawiciel musi zapewnić przeprowadzenie oceny ryzyka w celu określenia wymagań w zakresie ochrony zdrowia i bezpieczeństwa, które mają zastosowanie do maszyny; zatem maszyna musi być zaprojektowana i wykonana z uwzględnieniem wyników oceny ryzyka.*
2. *Za pomocą iteracyjnego procesu oceny ryzyka i zmniejszania ryzyka, o którym mowa powyżej, producent lub jego upoważniony przedstawiciel:*
   a) *określa ograniczenia dotyczące maszyny, w tym zamierzonego używania i możliwego do przewidzenia w uzasadniony sposób niewłaściwego jej użycia,*
   b) *określa zagrożenia, jakie może stwarzać maszyna i związane z tym niebezpieczne sytuacje,*
   c) *szacuje ryzyko, biorąc pod uwagę stopień możliwych obrażeń lub uszczerbku na zdrowiu i prawdopodobieństwo ich wystąpienia,*
   d) *ocenia ryzyko, mając na celu ustalenie, czy wymagane jest zmniejszenie ryzyka, zgodnie z celem niniejszej dyrektywy,*
   e) *eliminuje zagrożenia lub zmniejsza ryzyko związane z takimi zagrożeniami poprzez zastosowanie środków ochronnych, zgodnie z hierarchią ważności ustanowioną w sekcji 1.1.2.b).*
3. *Przy wybieraniu najwłaściwszych metod producent lub jego upoważniony przedstawiciel musi stosować następujące zasady, według podanej kolejności:*
   a) *wyeliminowanie lub zminimalizowanie ryzyka, tak dalece jak jest to możliwe (projektowanie i wykonywanie maszyn bezpiecznych z samego założenia);*
   b) *zastosowanie koniecznych środków ochronnych w związku z ryzykiem, którego nie można wyeliminować;*
   c) *informowanie użytkowników o ryzyku resztkowym, spowodowanym jakimikolwiek brakami w przyjętych środkach ochronnych, wskazanie, czy konieczne jest szczególne przeszkolenie oraz określenie potrzeby stosowania środków ochrony osobistej.*

Wymagania te stanowią podstawę metodyki oceny ryzyka zastosowanej w programie PRO-M. Kolejne kroki składające się na proces oceny ryzyka pokazano na rys. 9.1. Obejmują one:

- identyfikację maszyny
- określenie ograniczeń dotyczących maszyny
- identyfikację zagrożeń
- oszacowanie ryzyka
- ocenę czy – zgodnie z celami dyrektywy – konieczna jest dalsza redukcja ryzyka.



Rys. 9.1. Ogólna metodyka oceny ryzyka zastosowana w programie PRO-M

Decyzja dotycząca konieczności dalszej redukcji ryzyka zależy od poziomu ryzyka oraz technicznych możliwości jego dalszej redukcji przez zmiany w konstrukcji maszyny. Podstawą jest ogólna zasada sformułowana w załączniku 1 do dyrektywy, mówiąca, że:

Zasadnicze wymagania w zakresie ochrony zdrowia i bezpieczeństwa ustanowione w niniejszym załączniku są obowiązkowe. Jednakże, biorąc pod uwagę stan wiedzy technicznej, osiągnięcie wyznaczonych przez nie celów może nie być możliwe. W takim przypadku, maszyna musi być zaprojektowana i wykonana, na ile to możliwe, z zamiarem zbliżenia się do tych celów.

Oznacza to, że projektant maszyny powinien, w miarę możliwości, dążyć do zredukowania ryzyka związanego z poszczególnymi zagrożeniami do poziomu akceptowalnego, wykorzystując do tego celu wszelkie środki i rozwiązania konstrukcyjne dostępne przy aktualnym stanie wiedzy. Jeśli jednak zastosowanie wszelkich dostępnych środków nie umożliwia zredukowania ryzyka do poziomu akceptowalnego, to obowiązkiem projektanta jest udokumentowanie, że zastosował wszelkie możliwe środki, oraz poinformowanie użytkownika o pozostałym ryzyku resztkowym.

9.3. Charakterystyka programu PRO-M

Podstawowe informacje o programie PRO-M przedstawione są w pracach (Dźwiarek, 2008a, 2008c). Program ten jest przeznaczony do wspomagania projektantów maszyn w prowadzeniu i dokumentowaniu oceny ryzyka. Jego cechami charakterystycznymi są:

- struktura modułowa
- moduł główny stanowi narzędzie zarządzania procesem oceny ryzyka
- moduły szczegółowe dotyczą zagrożeń najczęściej występujących przy maszynach:
  - mechanicznych
  - elektrycznych
  - związanych z niesprawnością systemu sterowania
  - związanych z hałasem
  - związanych z wybuchem
  - biomechanicznych
  - pyłowych.

Moduły określają sposób postępowania podczas oceny ryzyka wynikającego z tych zagrożeń oraz tworzą dokumentację tej oceny. Końcowym efektem stosowania systemu jest wygenerowanie dokumentacji niezbędnej do przeprowadzenia oceny zgodności wg dyrektywy 2006/42/WE.

9.4. Zarządzanie procesem oceny ryzyka w programie PRO-M

W programie PRO-M proces oceny ryzyka jest zarządzany z poziomu modułu głównego. Dlatego też jego działanie rozpoczyna się na poziomie tego modułu. Moduł główny gromadzi dane ogólne o projekcie oraz nadzoruje tworzenie dokumentacji i przepływ informacji pomiędzy modułami szczegółowymi.

Pracę z programem administrator rozpoczyna od utworzenia bazy jego potencjalnych użytkowników. Baza ta zawiera wykaz osób, które będą uczestniczyć w prowadzeniu oceny ryzyka. Każdej osobie są przypisywane uprawnienia według następujących zasad:

- **administrator:** zarządza systemem, tworzy listę jego użytkowników, nadaje uprawnienia, konfiguruje system, zarządza projektami (kontroluje stan realizacji, archiwizuje zakończone), wskazuje projektantów. Funkcję tę powinna sprawować osoba odpowiedzialna za przygotowanie deklaracji zgodności, np. kierownik zespołu projektantów
- **projektant:** ma uprawnienia dostępu do modułu (zagrożenia) wskazanego przez głównego projektanta, przeprowadza ocenę ryzyka w ramach danego modułu, tworzy dokumentację z przeprowadzonej oceny oraz przekazuje wyniki końcowe do modułu głównego. Nabywa uprawnień głównego projektanta w projekcie, który sam utworzył
- **główny projektant** tworzy i edytuje projekt, zarządza oceną ryzyka z poziomu modułu głównego, przeprowadza wstępną identyfikację zagrożeń, nadaje uprawnienia pozostałym osobom uczestniczącym w projekcie, tworzy ostateczną dokumentację z oceny ryzyka
- **walidator:** ma uprawnienia dostępu do modułu wskazanego przez administratora (standardowo posiada uprawnienia do zagrożeń związanych z niesprawnością systemu sterowania), przeprowadza walidację projektu i sprawdza dokumentację sporządzoną przez projektanta
- **edytor baz danych:** ma uprawnienia do modyfikacji i uzupełniania baz danych.

Administrator systemu wprowadza dane identyfikacyjne wszystkich użytkowników systemu. Przypisuje im login oraz hasło.

Program umożliwia pracę nad wieloma projektami jednocześnie. Wszystkie projekty, które aktualnie realizuje dany użytkownik, są dostępne z poziomu okna głównego programu. Zaznaczenie projektu umożliwia edycję jego danych w zakresie posiadanych przez użytkownika uprawnień. W dolnej części okna są pokazane projekty, w których nie uczestniczy dany użytkownik. Dane tych projektów można przeglądać, ale nie można ich modyfikować.

9.5. Tworzenie i edycja projektu

9.5.1. Wprowadzenie

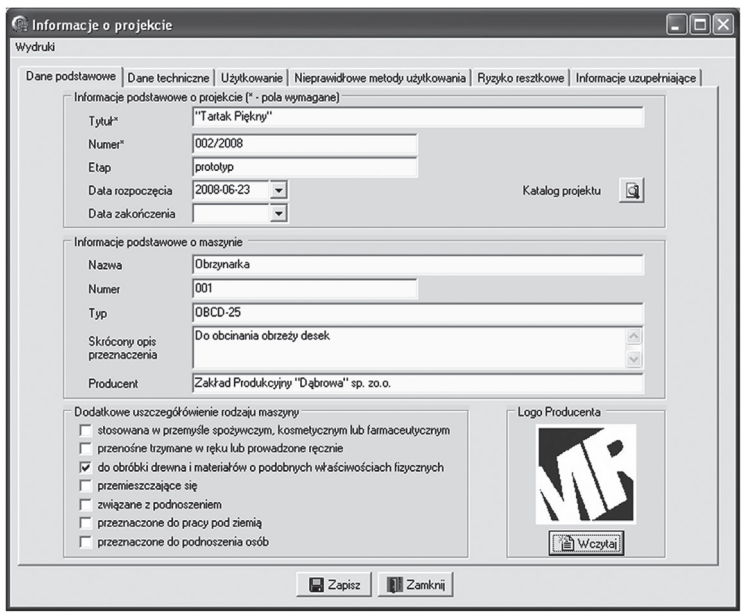
Nowy projekt tworzy osoba mająca uprawnienia projektanta. Osoba ta, tworząc nowy projekt, nabywa uprawnień głównego projektanta w zakresie

danych danego projektu. Utworzenie projektu aktywizuje formularz „Informacje o projekcie". W formularzu tym wprowadza się dane dotyczące projektu. We wstępnych etapach realizacji dane te wynikają z założeń do projektu. W miarę postępów w projektowaniu są uzupełniane o informacje wytworzone w modułach szczegółowych.

Informacje o projekcie obejmują:

– identyfikację projektu
– informacje podstawowe:
  - tytuł (identyfikator, po którym projekt jest rozpoznawany)
  - numer (unikalny nr identyfikacyjny projektu, który będzie przywoływany na każdym dokumencie wygenerowanym w ramach projektu)
  - etap – aktualny etap projektowania (np. założenia wstępne, projekt wstępny, projekt końcowy, prototyp)
  - daty: rozpoczęcia i zakończenia
– informacje podstawowe o maszynie (identyfikacja egzemplarza maszyny, dla którego przeprowadza się ocenę ryzyka)
– dodatkowe uszczegółowienie rodzaju maszyny (gdy maszyna kwalifikuje się do jednej z grup maszyn, dla których w dyrektywie sformułowano dodatkowe wymagania zasadnicze).

Dane te są uzupełnione o logo producenta, które jest umieszczane na większości dokumentów tworzonych w programie. Przykład danych podstawowych pokazano na rys. 9.2.



Rys. 9.2. Przykład danych podstawowych o projekcie

Następnie wprowadzane są podstawowe dane techniczne wynikające z kontraktu. W miarę postępów w projektowaniu dane te są uzupełniane przez głównego projektanta (np. o maksymalną moc pobieraną przez maszynę, układ sieci zasilającej maszyny itp.).

Dane są uzupełniane o opisy przewidywanego użytkowania maszyny, z uwzględnieniem wszystkich faz jej życia (obsługa stała, konserwacje, czyszczenie, wymiany zużytych podzespołów, naprawy itp.). Te informacje są przeznaczone do wykorzystania podczas opracowywania instrukcji obsługi maszyny. Należy także wskazać zabronione sposoby użytkowania. Wszystkie informacje są na bieżąco modyfikowane, wraz z postępem prac projektowych oraz zgdnie z wynikami oceny ryzyka prowadzonej w poszczególnych modułach.

9.5.2. Identyfikacja zagrożeń

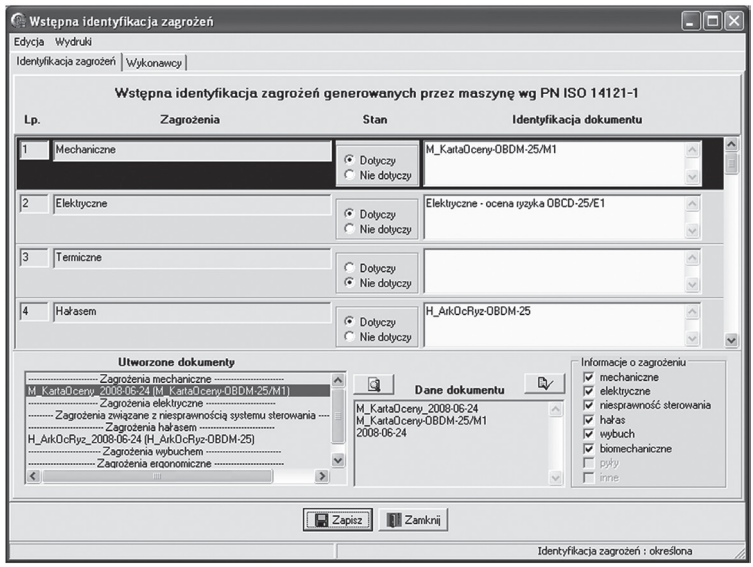
Pierwszym krokiem głównego projektanta jest wstępna identyfikacja zagrożeń występujących przy obsłudze maszyny. Według dyrektywy 2006/42/WE „zagrożenie" oznacza potencjalne źródło obrażeń lub uszczerbku na zdrowiu. Podstawowe zagrożenia spotykane w maszynach są wymienione w załączniku A do normy PN-EN ISO 12100:2011. Główny projektant, dokonując identyfikacji zagrożeń, określa, jaki będzie zakres oceny ryzyka. Obowiązkiem producenta jest, między innymi, opracowanie dokumentacji zawierającej: *opis środków zapobiegawczych wdrożonych w celu wyeliminowania rozpoznanych zagrożeń lub zmniejszenia ryzyka oraz, w stosownych przypadkach, wskazanie ryzyka resztkowego związanego z maszyną* (dyrektywa 2006/42/WE, zał. VII, rozdz. A p. 1.a).ii.)). Dokumentacja ta jest tworzona w zakładce „Identyfikacja zagrożeń".

Wstępnej identyfikacji zagrożeń główny projektant dokonuje na podstawie założeń projektowych. Jeśli zagrożenie zostało uwzględnione w jednym z modułów programu PRO-M, to w sposób automatyczny jest aktywowany stosowny moduł programu. W miarę postępów w procesie projektowania można dokonywać zmian w identyfikacji zagrożeń, zgodnie ze wskazaniami modułów szczegółowych. Modyfikacje takie mogą wynikać z pojawienia się wcześniej nieprzewidzianych zagrożeń, w związku z zastosowanymi rozwiązaniami konstrukcyjnymi. Wstępna identyfikacja zagrożeń jest uzupełniana na poziomie poszczególnych modułów, poprzez jej uszczegółowienie, odpowiednio do specyfiki danego modułu.

W miarę postępów procesu oceny ryzyka do poszczególnych zagrożeń są przypisywane dokumenty, które opisują środki zastosowane w celu wyeliminowania danego zagrożenia. Jeśli jest to zagrożenie zaimplementowane w jednym z modułów programu, będzie to numer dokumentu podsumowującego dla danego modułu. Jeśli jest to zagrożenie nieuwzględnione w modułach szczegółowych, będzie to identyfikacja dokumentu zewnętrznego, spoza programu. Po ostatecznym

zakończeniu oceny ryzyka wszystkie pola „Identyfikacja dokumentu" przypisane do zidentyfikowanych wcześniej zagrożeń powinny być wypełnione.

Przykład wykazu zidentyfikowanych zagrożeń pokazano na rys. 9.3.



Rys. 9.3. Przykład wykazu zidentyfikowanych zagrożeń

9.5.3. Informacja o ryzyku resztkowym

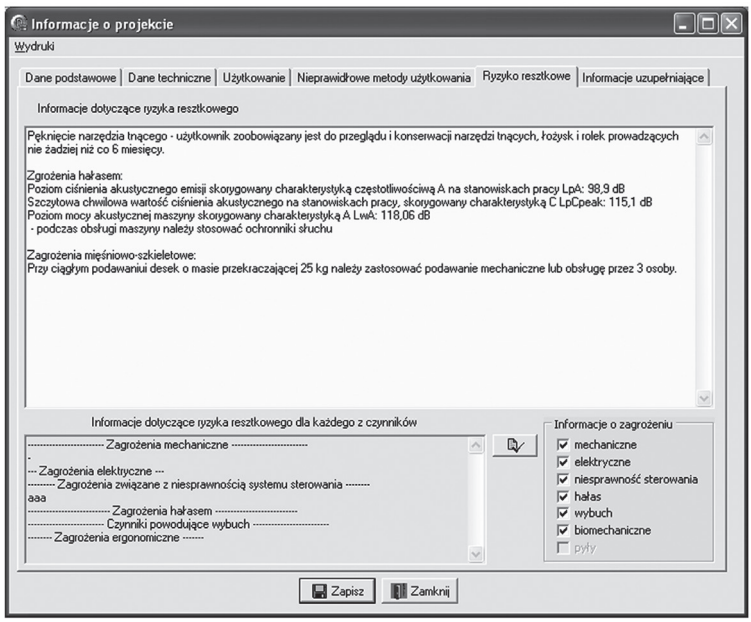
Ryzyko resztkowe jest to ryzyko, które nie mogło być wyeliminowane przez zaprojektowanie maszyny bezpiecznej z założenia lub zastosowanie urządzeń ochronnych. Przykładem ryzyka resztkowego jest hałas emitowany przez maszynę wynikający z procesu technologicznego, którego nie można było wyeliminować metodami konstrukcyjnymi. Ryzykiem resztkowym jest także ryzyko wynikające z możliwości uszkodzenia elementów systemu sterowania. Użytkownik maszyny powinien być poinformowany o ryzyku resztkowym oraz sposobach zapobiegania mu przez:

- stosowanie dodatkowych technicznych środków bezpieczeństwa
- odpowiednią organizację pracy (np. praca w zespołach dwuosobowych, ograniczenie czasu pracy itp.)
- stosowanie środków ochrony indywidualnej lub narzędzi pomocniczych (np. ochronników słuchu, mechanicznego podawania materiału itp.)
- okresowe kontrole i sprawdzenia elementów i podzespołów maszyny
- przeszkolenie pracowników w zakresie bezpiecznej obsługi.

W miarę możliwości również operator maszyny powinien być informowany o ryzyku resztkowym za pomocą sygnałów ostrzegawczych, akustycznych i optycznych oraz oznakowania na maszynie.

Informacje o ryzyku resztkowym są generowane w poszczególnych modułach programu, a następnie, w miarę postępów w projektowaniu, zbierane z poszczególnych modułów. Informacje te są przeznaczone do wykorzystania podczas opracowywania instrukcji obsługi maszyny.

Przykład informacji o ryzyku resztkowym pokazano na rys. 9.4.



Rys. 9.4. Przykład informacji o ryzyku resztkowym

9.5.4. Listy kontrolne wymagań zasadniczych

Dokumentacja zgromadzona przez producenta maszyny w celu wystawienia deklaracji zgodności powinna zawierać między innymi wykaz zasadniczych wymagań w zakresie ochrony zdrowia i bezpieczeństwa, które mają zastosowanie do maszyny, oraz zastosowane normy i inne specyfikacje techniczne, wskazujące zasadnicze wymagania w zakresie ochrony zdrowia i bezpieczeństwa objęte tymi normami. Dokumenty te tworzy główny projektant przez wypełnienie formularza „Listy kontrolne wymagań zasadniczych". Na formularzu tym główny projektant podsumowuje wyniki oceny ryzyka, wskazując dokumenty potwierdzające spełnienie zasadniczych wymagań dyrektywy. Mogą to być dokumenty wygenerowane w modułach szczegółowych lub opracowane poza programem (schematy, rysunki

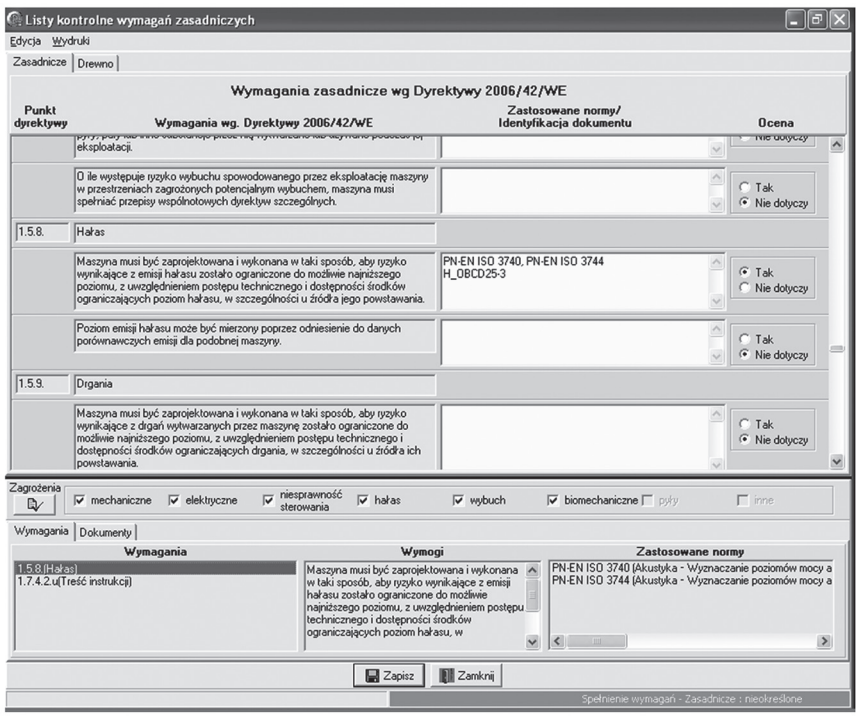
złożeniowe, protokoły badań i pomiarów itp.). W przypadku maszyn, których dotyczą dodatkowe wymagania zasadnicze, należy wypełnić także odpowiednią dodatkową listę kontrolną.

Dodatkowe wymagania dotyczące niektórych kategorii maszyn są zawarte w kolejnych rozdziałach załącznika I dyrektywy 2006/42/WE. Dotyczą one następujących maszyn:

- stosowanych w przemyśle spożywczym, kosmetycznym i farmaceutycznym
- przenośnych trzymanych w ręku lub prowadzonych ręcznie
- do obróbki drewna lub materiałów o podobnych właściwościach fizycznych
- przemieszczających się
- związanych z podnoszeniem
- przeznaczonych do pracy pod ziemią
- przeznaczonych do podnoszenia osób.

Wskazanie w formularzu „Dane podstawowe", że dana maszyna kwalifikuje się do jednej z wymienionych kategorii, spowoduje uaktywnienie odpowiedniej listy kontrolnej dodatkowych wymagań zasadniczych. Listę tę należy wypełnić tak jak listę podstawową.

Przykład listy kontrolnej wymagań zasadniczych pokazano na rys. 9.5.



Rys. 9.5. Przykład listy kontrolnej wymagań zasadniczych

9.5.5. Zakończenie oceny ryzyka

Proces oceny ryzyka jest zakończony, gdy wypełnione są wszystkie pola listy kontrolnej wymagań zasadniczych oraz wszystkie wskazane listy kontrolne dodatkowych wymagań zasadniczych. Ostatecznym podsumowaniem wszystkich działań jest wydrukowanie dokumentów wytworzonych w procesie analizy ryzyka. Dokumenty te stanowić będą część dokumentacji niezbędnej do wystawienia deklaracji zgodności. Najważniejsze z nich to:

- Identyfikacja zagrożeń generowanych przez maszynę wg PN-EN ISO 12100:2011
- Wymagania zasadnicze wg dyrektywy 2006/42/WE
- Opis ograniczeń dotyczących maszyny.

Dokumenty te są wymienione w załączniku VII do dyrektywy 2006/42/WE jako część obowiązkowej dokumentacji konstrukcyjnej. Pozostałe przywołane w nich dokumenty stanowią załączniki do dokumentacji. Po wydrukowaniu i podpisaniu przez osoby upoważnione (głównego wykonawcę i osobę zatwierdzającą) dokumenty te należy zarchiwizować. Zalecane jest także zarchiwizowanie wersji elektronicznej oceny ryzyka. Dokumenty wraz z kopią wersji elektronicznej należy przechowywać przez 10 lat w celu udostępnienia organom nadzoru rynku na ich żądanie.

Rozdział 10

Zastosowanie technologii AR (ang. *augmented reality*) do sygnalizowania zagrożeń przy obsłudze maszyn

10.1. Wprowadzenie

Wyniki przeprowadzonych analiz wypadków przedstawione w rozdziale 2 zawierają opisy wypadków, których przyczynami były między innymi nieskuteczne sygnały ostrzegawcze lub ich brak. Także na stronach internetowych www.pip.gov.pl podano przykłady wypadków, którym można było zapobiec przez odpowiednio wczesne ostrzeżenie o zagrożeniu. Wnioski takie sformułowali również Haas i Casali (1995), którzy stwierdzili, że *wciąż odnotowywane są wypadki spowodowane tym, że sygnały ostrzegawcze nie zostały usłyszane lub dostrzeżone*. A zatem informowanie operatora maszyny o występujących sytuacjach zagrożenia jest jednym z istotnych środków zapobiegania nieprzewidzianym wypadkom.

Informacja ostrzegawcza powinna być przekazywana operatorowi możliwie szybko i skutecznie. Norma PN-EN ISO 12100:2011 zaleca stosowanie sygnałów ostrzegawczych jako uzupełniającego środka redukcji ryzyka, zwłaszcza w sytuacjach, w których nie ma możliwości zastosowania innych, bardziej skutecznych środków. Systemy te odgrywają szczególnie istotną rolę podczas regulacji, konserwacji lub napraw maszyny, gdyż w trakcie tych prac systemy bezpieczeństwa są zazwyczaj odłączane w celu uzyskania bezpośredniego dostępu do stref niebezpiecznych. Podobnie jest, gdy operator uruchamiający maszynę nie ma możliwości obserwacji wszystkich stref niebezpiecznych. Występuje wówczas konieczność zasygnalizowania zamiaru uruchomienia maszyny w taki sposób, że wszystkie osoby znajdujące się w pobliżu zostaną poinformowane o niebezpieczeństwie wystarczająco wcześnie.

Tak więc sygnały ostrzegawcze stosuje się do sygnalizowania nagłych zdarzeń, takich jak nagłe uruchomienie maszyny lub wzrost prędkości ruchu narzędzia. Sygnały takie mogą być użyte do ostrzegania operatora zanim niebezpieczna sytuacja

spowoduje zaktywizowanie automatycznych urządzeń ochronnych. A ponadto (Dźwiarek, Łuczak, 2008):

- powinny być emitowane zanim nastąpi niebezpieczne zdarzenie
- powinny być jednoznaczne
- muszą wyraźnie odróżniać się od innych sygnałów występujących na stanowisku pracy.

Obecnie najczęściej stosowanymi środkami ostrzegawczymi są sygnały wizualne i dźwiękowe. Ich podstawową wadą jest to, że docierają do wielu osób, a nie tylko do osoby zagrożonej. Mogą więc powodować odwrócenie uwagi wielu osób oraz dezorganizację ich pracy. Ponadto sygnały wizualne są dostrzegane jedynie wtedy, kiedy znajdują się w polu widzenia osoby narażonej, więc często operator skupiony przede wszystkim na wykonywanej czynności ich nie zauważa.

Urządzenia rzeczywistości rozszerzonej, AR, spełniają wszystkie wymagania dotyczące sygnałów ostrzegawczych, a jednocześnie nie mają wad urządzeń stosowanych obecnie. Można przewidzieć, że wraz z rozwojem techniki zakres zastosowań systemów AR będzie coraz szerszy i obejmie także zagadnienia dotyczące bezpieczeństwa pracy. Założenie takie jest zgodne z konkluzją sformułowaną w opracowaniu Wogalter i Mayhorn (2005), dotyczącym analizy korzyści ze stosowania nowoczesnych technologii do systemów ostrzegawczych. Autorzy w podsumowaniu stwierdzają, że: *w przyszłości systemy ostrzegawcze będą zapewne mieć właściwości inne i lepsze niż tradycyjne ostrzeżenia statyczne*. W wyniku analiz przeprowadzanych przez tych autorów wskazano niektóre perspektywiczne korzyści technologiczne i określono kierunki przyszłego rozwoju systemów ostrzegawczych. Jakkolwiek do zapewnienia, że bardziej zaawansowane, oparte na technologii AR systemy ostrzegawcze będą skuteczne, brakuje jeszcze wielu prac doświadczalnych. Badania przedstawione przez Dźwiarka i Łuczak (2008) wpisują się w ten nurt rozwoju nowoczesnych systemów ostrzegawczych.

10.2. Analiza stanowisk pracy pod kątem przydatności sygnałów ostrzegawczych AR

Ogólne zasady stosowania sygnałów ostrzegawczych określone są w normie PN-EN 61310-1:2009. Stanowi ona, że sygnały alarmowe i ostrzegawcze interfejsu człowiek–maszyna powinny dostarczać informacji dotyczących bezpieczeństwa, aby operatorzy i osoby narażone mogły bezpiecznie użytkować i nadzorować maszyny. Zwłaszcza do sygnalizacji zagrożenia lub konieczności podjęcia odpowiednich działań przez operatora powinny być używane sygnały aktywne. Ponieważ sygnały te odgrywają znaczącą rolę w redukcji ryzyka, na które narażeni są ludzie, więc stosowane są bardzo powszechnie.

W celu dokładniejszego rozpoznania ewentualnej przydatności zastosowania sygnałów ostrzegawczych AR przeanalizowano następujące stanowiska pracy operatorów maszyn:

- zautomatyzowana linia produkcyjna
- stanowisko obsługi linii automatycznego tłoczenia w trybie SETUP
- stanowisko operatora wózka transportowego
- stanowisko nakładania kleju na szyby samochodowe
- stanowisko obsługi stacji zakładania dachu
- stanowisko obsługi automatu montującego
- stanowisko obsługi prasy automatycznej do wytwarzania drobnych detali.

Dalej omówiono wybrane przykłady.

Ostrzeganie o uruchomieniu maszyny na przykładzie zautomatyzowanej linii produkcyjnej

Do najbardziej rozpowszechnionych systemów ostrzegawczych należą systemy ostrzegające o uruchomieniu maszyny. Obowiązek ich stosowania wynika z przepisów dotyczących projektowania maszyn oraz ich użytkowania. Dyrektywa maszynowa 2006/42/WE zawiera następujące wymagania:

> *§16.3. Z głównego stanowiska sterowania operator powinien mieć możliwość upewnienia się, że w strefach niebezpiecznych nie przebywają osoby narażone. § 17.1. Jeżeli nie jest możliwe spełnienie wymagań, o których mowa w § 16 ust. 3, system sterowania powinien być zaprojektowany i wykonany w taki sposób, aby uruchomienie maszyny było każdorazowo poprzedzane akustycznym lub optycznym sygnałem ostrzegawczym.*

Przepisy te zobowiązują do wyposażenia dużej grupy maszyn w akustyczny lub optyczny sygnał ostrzegający o uruchomieniu. Przykładem może być zautomatyzowana linia produkcyjna, która zawiera szereg gniazd produkcyjnych (rys. 10.1). W każdym gnieździe jest wykonywana automatyczna obróbka wytwarzanych produktów. Cykl obróbki trwa około 10 min. Po jego zakończeniu operator powinien wejść w obszar gniazda i usunąć pozostałe po obróbce odpady. Następnie opuszcza gniazdo i uruchamia kolejny cykl automatycznej obróbki. Zazwyczaj linię obsługuje dwu operatorów. Każde gniazdo jest wyposażone w urządzenie, które sygnalizuje stany niebezpieczne i ostrzega operatora przed wejściem w obszar gniazda po podaniu sygnału do uruchomienia cyklu obróbki. Sygnał ten jest widoczny jedynie na zewnątrz urządzenia. Natomiast osoba wykonująca pracę wewnątrz gniazda nie ma możliwości zauważenia go, co było powodem wypadku, który wydarzył się przy obsłudze tej linii. Wypadkowi można było zapobiec, gdyby osoba pracująca w gnieździe została odpowiednio wcześnie ostrzeżona o niebezpieczeństwie, np. za pomocą sygnału AR.

Rys. 10.1. Przykład urządzeń ostrzegających o uruchomieniu zautomatyzowanej linii produkcyjnej

Stanowisko obsługi linii automatycznego tłoczenia w trybie SETUP

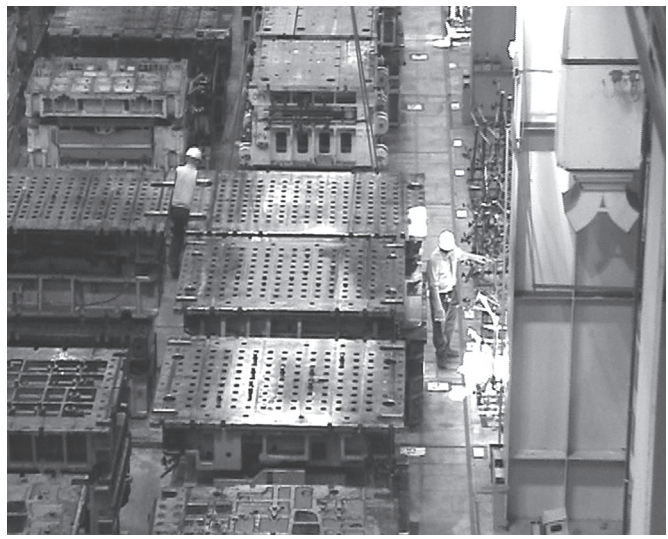
Urządzenia do podnoszenia i przemieszczania ładunku, np. suwnice, stanowią wyposażenie prawie każdej hali produkcyjnej. Przy organizacji pracy z wykorzystaniem suwnic należy uwzględnić postanowienia dyrektywy 2009/104/WE, która stanowi:

Zał. II p. 3.1.3. Pracownicy nie powinni przebywać pod wiszącymi ładunkami, o ile nie jest to konieczne dla sprawnego wykonywania pracy. Jeżeli jednak zachodzi taka konieczność, pracodawca powinien zapewnić bezpieczeństwo pracownikom i właściwe zabezpieczenie wiszących ładunków.

Nie przenosi się ładunków nad niezabezpieczonymi miejscami pracy, w których zwyczajowo przebywają pracownicy.

Przykładem stanowiska pracy wyposażonego w suwnice jest stanowisko do obsługi linii automatycznego tłoczenia w trybie SETUP (rys. 10.2). Na stanowisku tym pracownicy wymieniają matryce w linii pras automatycznych. Matryce są zestawiane w stosy obok linii. Pracę wykonuje dwu robotników. Robotnik *1* przygotowuje wybraną matrycę do podniesienia przez suwnicę (usuwa mocowania, instaluje zaczepy do podwieszenia na suwnicy). W tym czasie pracownik *2* przenosi wcześniej przygotowaną matrycę. Podczas wykonywania tej pracy zdarzył się wypadek:

Robotnik 1. przygotowywał kolejną matrycę, stojąc za ich stosem. Uwagę miał skupioną na wykonywanych czynnościach, czyli instalowaniu uchwytów do matrycy, i nie zauważył zbliżającej się suwnicy. Robotnik 2, obsługujący suwnicę, nie widział robotnika 1, gdyż był on zasłonięty stosem matryc. Pękła lina w suwnicy i przewożony ładunek spadł na stos matryc, który obsunął się na pracującego za nim robotnika 1. Wypadek był ciężki, robotnik stracił nogę.



Rys. 10.2. Stanowisko obsługi linii automatycznego tłoczenia w trybie SETUP

Jednym ze sposobów umożliwiających zapobiegnięcie takiemu wypadkowi jest ostrzeżenie robotnika zagrożonego o zbliżaniu się suwnicy. Zastosowany na tym stanowisku tradycyjny sygnał ostrzegawczy nie spełnił swojej roli, gdyż jest przeznaczony dla osób postronnych i sygnalizuje zakaz zbliżania się do obszaru pracy suwnicy. Natomiast robotnicy wykonujący wymianę matryc muszą w tym obszarze przebywać. Skuteczny mógłby być sygnał AR, który dociera bezpośrednio do osoby zagrożonej.

Stanowisko operatora wózka transportowego

Praca operatora wózka transportowego polega na dowożeniu materiałów z magazynu do stanowisk pracy. Na drodze komunikacyjnej występują liczne miejsca możliwych kolizji, zarówno z pieszymi jak i z wyposażeniem roboczym. Zgodnie ze stosowanymi w zakładzie zasadami, na całym terenie zakładu wózki transportowe mają bezwzględne pierwszeństwo przejazdu. Wszyscy pracownicy są o tym poinformowani i mają obowiązek stosowania się do tej zasady.

Na rys. 10.3 pokazano skrzyżowanie drogi transportowej z przejściem dla pieszych. Na skrzyżowaniu tym doszło do wypadku w następujących okolicznościach:

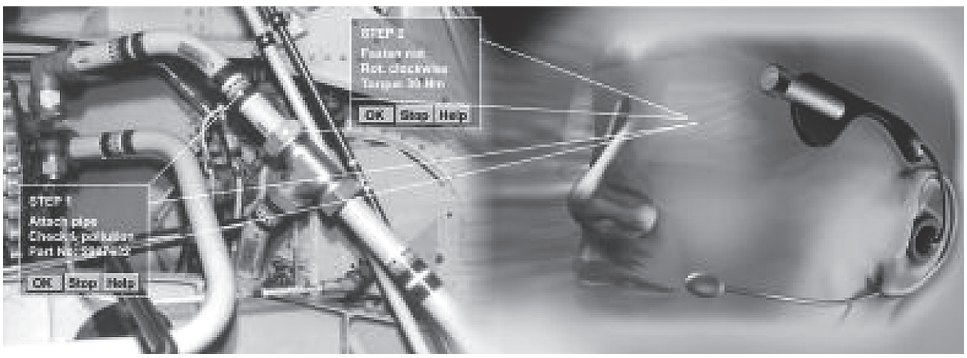
Pracownik dokonujący naprawy sprzętu udał się do magazynu po części zamienne. Idąc, skupił swoją uwagę na przeglądaniu dokumentacji, którą niósł, i nie zauważył nadjeżdżającego wózka transportowego. Skutkiem wypadku było złamanie nogi. Według danych zakładowych służb bhp, wypadki takie są dość częste. Zazwyczaj przyczyną jest niezauważenie nadjeżdżającego wózka z powodu odwrócenia uwagi.

Rys. 10.3. Skrzyżowanie drogi ruchu wózka transportowego z przejściem dla pieszych

Wyposażenie okularów ochronnych noszonych przez pracowników w system sygnałów ostrzegawczych AR, informujących o zagrożeniach związanych ze zbliżającym się wózkiem transportowym, mogłoby zapobiec przynajmniej części wypadków.

10.3. Zastosowanie AR w przemyśle

W literaturze naukowej od kilku lat pojawiają się informacje o próbach zastosowania systemów rzeczywistości rozszerzonej, AR, na stanowiskach pracy w przemyśle. Jak dotychczas były to informacje o próbach zastosowania systemów AR do zwiększenia skuteczności prac kontrolnych i konserwacyjnych oraz do szkoleń. Ogólną analizę takich zastosowań systemów AR przeprowadzili Kyung i in. (2002). Kwestie możliwości wykorzystania AR do prowadzenia szkoleń pracowników realizujących prace montażowe przedstawili Bound i in. (1999) oraz Michalak i in. (2009, 2010). Natomiast zastosowania systemów AR do wspomagania okresowych kontroli maszyn zaprezentowali Chung i in. (2002). Podobne wyniki przedstawili także Weidenhausen i in. (2003). Anastassova i in. (2005) zaprezentowali wstępne rezultaty projektu dotyczącego wykorzystania urządzeń AR do podnoszenia efektywności pracy przy naprawach samochodów. Natomiast Dangelmaier i in. (2005) zbadali możliwość stosowania systemów AR w projektowaniu systemów produkcyjnych. Oehme i Bruns (2003) zaprezentowali przykład zastosowania systemu AR do wspomagania prac związanych z konserwacją i naprawami maszyn. Podobne rozwiązania zastosowano w projekcie ARVIKA (2001), (rys. 10.4).



Rys. 10.4. Wykorzystanie technologii AR w pracach serwisowych/montażowych – na obraz rzeczywisty nakładane są wskazówki dla pracownika (www.arvika.de)

Badania porównawcze efektywności pracy prowadzonej w sposób tradycyjny z efektywnością uzyskiwaną ze wspomaganiem systemami AR, przeprowadzone przez Chunga i in. (2002), wykazały, że zastosowanie AR znacznie poprawia wskaźniki efektywności, takie jak liczba popełnionych błędów oraz czas reakcji na sygnały.

10.4. Wymagania dotyczące sygnałów ostrzegawczych AR

Dotychczas spotykane zastosowania systemów AR, opisane w rozdziale 10.3, charakteryzują się następującymi cechami:

- obrazy AR mają ścisły związek z prowadzoną pracą
- obrazy AR są wyświetlane w sposób ciągły i powinny być umiejscowione w pobliżu urządzeń, na których skupia się wzrok operatora
- uwaga operatora jest skoncentrowana na obrazach, których on oczekuje.

W przypadku sygnałów ostrzegawczych wymagania są zupełnie inne. A ich cechy charakterystyczne są następujące:

- zazwyczaj w niewielkim stopniu wiążą się z aktualnie wykonywanymi czynnościami
- pojawiają się sporadycznie, tylko w sytuacjach wyjątkowych i w oddaleniu od urządzenia, na którym skupia się wzrok operatora
- pojawiają się nieoczekiwanie, w sytuacji gdy uwaga operatora skoncentrowana jest na innych czynnościach.

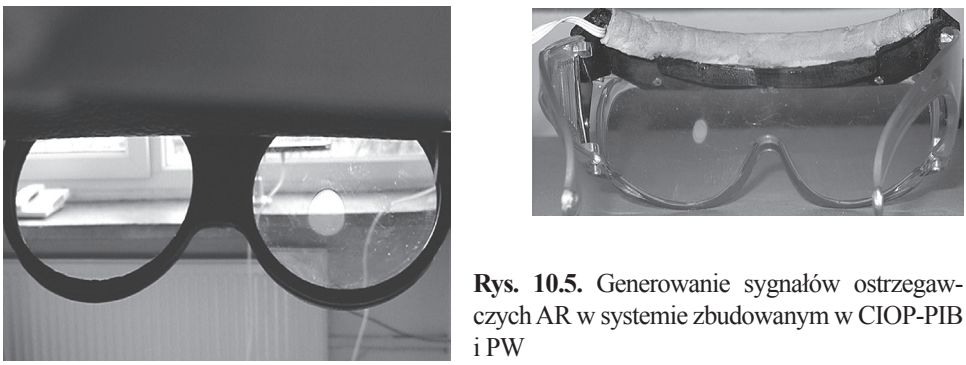
Specjalizowaną aparaturę, zaprojektowaną do takich zastosowań, zbudowano na Politechnice Warszawskiej, we współpracy z CIOP-PIB. Założenia do jej opracowania, które powstały na podstawie analizy dostępnych systemów, z uwzględnieniem

zasad sformułowanych przez Dźwiarka i in. (2003, 2004) i Dźwiarka i Łuczak (2008), są następujące:

1. Powinien to być system typu *see-through*. W takich systemach, przy braku sygnału obserwowane jest rzeczywiste stanowisko pracy. Natomiast w systemach, które funkcjonują na zasadzie uzupełniania obrazu z kamery o dodatkowe sygnały otoczenie jest obserwowane na monitorze. Jeśli się weźmie pod uwagę obecny stan wiedzy, to rozwiązanie takie nie jest wystarczająco dokładne i pewne, aby mogło być stosowane przemyśle. Wiąże się to przede wszystkim ze zbyt małą dokładnością odtwarzania obrazów rzeczywistych oraz uzupełniania ich obrazami wirtualnymi (Hagele i in., 2002).
2. Okulary, na których generowany jest sygnał AR, nie powinny w miarę możliwości powodować uciążliwości związanych z ich użytkowaniem.
3. Przy braku sygnałów AR okulary powinny w możliwie jak najmniejszym stopniu ograniczać pole widzenia, a także wprowadzać jak najmniej zakłóceń, zniekształceń lub odbarwień obrazu.

Opracowane okulary AR pokazano na rys. 10.5. Innym rozwiązaniem jest np. wykorzystanie zaawansowanych okularów LITEYE, pokazanych na rys. 10.6.

Wyniki badań skuteczności sygnałów ostrzegawczych generowanych metodą AR zostały przedstawione w pracy (Dźwiarek i in., 2007a).



Rys. 10.5. Generowanie sygnałów ostrzegawczych AR w systemie zbudowanym w CIOP-PIB i PW

Rys. 10.6. Sygnał alfanumeryczny STOP widoczny od zewnętrznej strony okularu LITEYE-500

10.5. Metody badania percepcji sygnałów ostrzegawczych

Z dostępnych danych literaturowych wynika, że typową metodą prowadzenia badań percepcji przemysłowych sygnałów ostrzegawczych jest zastosowanie określonych przez Shingledecker (1984) zasad *criterion task set* (CTS), zazwyczaj w wersji 2.1, *probability monitoring task*, jako typowej dla działalności operatorów systemów technicznych. Badania są zazwyczaj realizowane na stanowiskach laboratoryjnych. Przy ich budowie zwykle nie stawia się celu w postaci wiernego odwzorowania środowiska/otoczenia rzeczywistych konkretnych stanowisk pracy. Stanowiska badawcze są projektowane w taki sposób, aby możliwe było badanie wyizolowanych aspektów charakteryzujących zachowanie człowieka – postrzegania i reakcji na sygnały ostrzegawcze – na „stanowisku uogólnionym" reprezentującym całą klasę stanowisk pracy.

Bardzo częstym rozwiązaniem są tu proste stanowiska, a zadania stawiane badanym w niewielkim stopniu przypominają pracę w warunkach rzeczywistych. Głównym elementem zapewniającym interakcję z badanym człowiekiem jest zwykle system komputerowy z monitorami do prezentacji efektów wizualnych i głośnikami w przypadku badań percepcji sygnałów dźwiękowych.

W eksperymencie przeprowadzonym przez Burt i in. (1995) podczas zadania, polegającego na śledzeniu kulistego kształtu na ekranie monitora komputerowego, generowane były 30-sekundowe sygnały ostrzegające o możliwości wystąpienia awarii, a kulisty cel zmieniał kształt na kwadratowy. Gdy kwadratowy cel przestawał być kontrolowany przez joystick i zaczynał dryfować poza prostokątne granice, system śledzenia przestawał działać. Osoby badane miały za zadania naciśnięcie przycisku w celu przywrócenia śledzenia. Zapamiętywany był czas reakcji od chwili utraty śledzenia do chwili pojawienia się sygnału z przycisku.

Haas i Casali (1995) w pracy dotyczącej postrzegania sygnałów ostrzegawczych w warunkach silnych zakłóceń opisują eksperyment prowadzony w specjalnej komorze akustycznej, w której symulowano zarówno „naturalny" szum, jak i sygnały wymagające akcji badanego. Podstawowym zadaniem badanego, mającym na celu zaabsorbowanie jego uwagi, było obserwowanie wyświetlanych na trzech monitorach specjalnie spreparowanych „losowo" kolorowych obrazów. Badany powinien reagować naciśnięciem odpowiedniego klawisza w chwili, gdy na jednym z monitorów pojawiał się obraz odbiegający od „losowego". Właściwymi sygnałami, których percepcję badano, były sygnały akustyczne, generowane na tle akustycznego szumu. Czasy reakcji na pojawienie się właściwych sygnałów dźwiękowych były wskaźnikiem percepcji sygnału. Rejestrowano również subiektywne odczucia badanych – odpowiadali oni na pytanie, który

z dwóch sygnałów dźwiękowych (sygnały dźwiękowe generowano parami) był łatwiej zauważalny.

Również w pracy Bliss i in. (1995), dotyczącej badania reakcji (w tym efektu lekceważenia ostrzeżeń w odpowiedzi na znaczną liczbę alarmów fałszywych – ang. *cry-wolf effect*) na sygnały ostrzegawcze i informacyjne o różnym stopniu istotności (DANGER!!, WARNING!, NOTE), typowe dla paneli sterujących w kabinach samolotów, wykorzystano bardzo proste stanowisko badawcze w postaci programu symulacyjnego i dwóch komputerów. Jeden z komputerów służył do symulowania „zajęcia uwagi" powodowanego właściwą pracą (ang. *primary task*), drugi do generowania sygnałów ostrzegawczych graficznych (kolorowe plansze: czerwone, żółte i zielone) z odpowiednimi napisami oraz dźwiękowych. Oceniano właściwą (w stosunku do „stopnia zagrożenia") reakcję na sygnał ostrzegawczy. Zadanie realizowane jako *primary task* nie przypominało w najmniejszym stopniu pracy pilota. Sprowadzało się do identyfikacji ręki (i wskazania odpowiedniej strzałki na ekranie), w której wyświetlany na ekranie manekin trzymał planszę

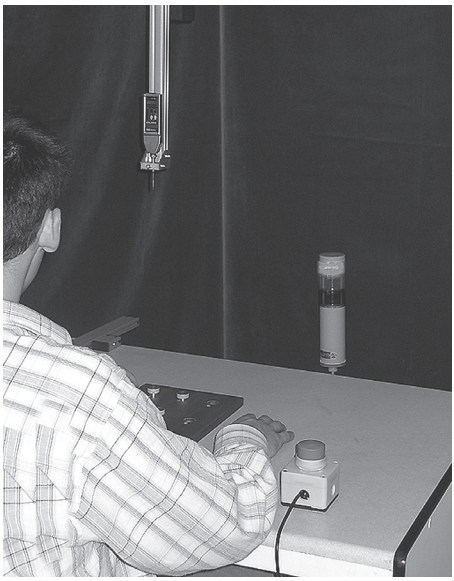
Podobny eksperyment przeprowadził Cohn (1996), który w teście „czas do zareagowania" stosował do stymulacji a) ikonę skaczącą ze strony na stronę, b) zakrzywioną strzałkę poruszającą się w widoczny sposób, c) falistą linię przesuwającą się z lewej do prawej. W trakcie stymulacji losowo generowany był sygnał ostrzegawczy, na który osoba badana miała zareagować naciśnięciem klawisza na klawiaturze komputera. Odnotowywana była poprawność i czas reakcji w każdej próbie.

W badaniach opisanych przez Chana i Chana (2006), mających na celu ocenę wpływu na czas reakcji i liczbę popełnianych błędów sygnałów ostrzegawczych akustycznych i wizualnych generowanych w sposób synchroniczny i asynchroniczny, wykorzystano bardzo proste stanowisko badawcze. Badani w trakcie eksperymentów zajmowali miejsce przed ekranem komputera, mając na uszach stereofoniczne słuchawki, przez które nadawano sygnały dźwiękowe. Sygnały wizualne były prezentowane w postaci czerwonych kółek o średnicy 20 mm wyświetlanych na ekranie komputera w odległości 80 mm z lewej lub prawej strony zielonego koła o tym samym promieniu, którego środek pokrywał się ze środkiem ekranu. Badanym polecano skupienie wzroku na kole zielonym i reagowanie na pojawiające się sygnały wizualne lub dźwiękowe (te, które zauważyli wcześniej) z lewej lub prawej strony przez naciśnięcie jednego z dwóch klawiszy. Mierzoną wielkością był czas reakcji. Rejestrowano również poprawność odpowiedzi.

10.6. Metoda badania percepcji sygnałów ostrzegawczych AR

10.6.1. Wprowadzenie

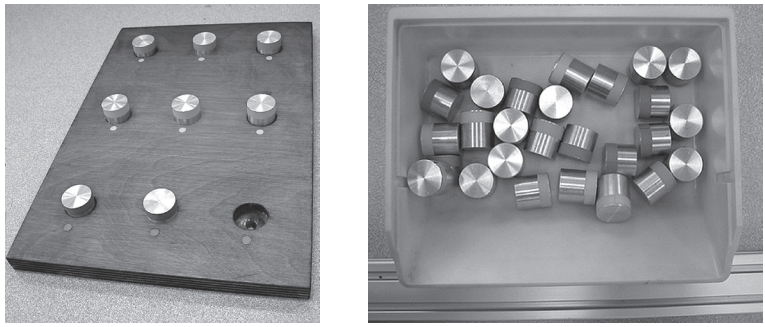
Metoda badania percepcji sygnałów ostrzegawczych AR, opracowana przez Dźwiarka i in. (2007), także opiera się na eksperymencie *criterion task set* (CTS), ale w wersji *dual task*. Zastosowane stanowisko badawcze, pokazane na rys. 10.7, zostało zaprojektowane jako model stanowiska pracy przy maszynie.



Rys. 10.7. Widok ogólny stanowiska eksperymentalnego

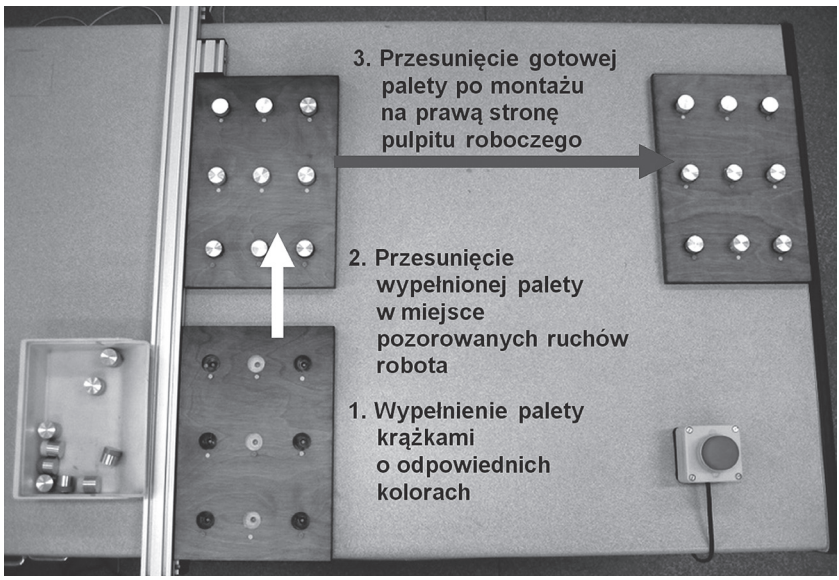
Całe stanowisko składa się z następujących elementów:
- pulpitu roboczego z listwą ograniczającą
- wysięgnika robota współpracującego
- elementów montażowych (rys. 10.8):
  - palet z otworami oznaczonymi różnymi kolorami
  - pojemnika z krążkami o różnych kolorach
- urządzeń sygnalizacyjnych (semafora, okularów z diodą lub okularów z wyświetlaczem)
- przycisku awaryjnego.

W zaplanowanym eksperymencie zadanie *probability monitoring task* zostało zastąpione zadaniem manualnym (*primary task*) polegającym na wkładaniu krążków oznaczonych odpowiednim kolorem w otwory na palecie o tym samym kolorze (rys. 10.8). Krążki są wybierane z pojemnika i wkładane w otwory palety pojedynczo, w tempie naturalnym dla każdej osoby badanej (zadanie nie jest wykonywane w tempie narzuconym).



Rys. 10.8. Elementy montażowe wykorzystane w eksperymencie

Po zapełnieniu wszystkich otworów osoba badana przesuwa wypełnioną paletę w miejsce ograniczone listwami na pulpicie, a następnie pobiera następną paletę i powtarza kolejny cykl wypełniania otworów krążkami o odpowiednich kolorach. W tym czasie robot bramowy pozoruje ruchy pomiaru wysokości elementów. Po zakończeniu wypełniania kolejnej palety badany odsuwa poprzednio wypełnioną w prawy koniec pulpitu, a na jej miejsce przy listwach przesuwa nową z wypełnionymi otworami. Tak wykonywane sekwencje powtarza się aż do końca sesji. Kolejne czynności składające się na cykl zadaniowy zaprezentowano na rys. 10.9. Zadaniem robota bramowego jest symulowanie naturalnego środowiska pracy.



Rys. 10.9. Kolejne fazy zadania roboczego

W trakcie wykonywania zadania eksperymentalnego prezentowane są sygnały ostrzegawcze w postaci klasycznego sygnału świetlnego na sygnalizatorze lub na okularach (czerwone światło diody, napis „stop", światło pulsujące). Zadaniem osoby badanej jest jak najszybsze naciśnięcie przycisku awaryjnego po pojawieniu się sygnału ostrzegawczego. Sygnały ostrzegawcze są prezentowane w losowych odstępach czasu w trakcie 20-minutowej sesji zadaniowej. Sygnał ostrzegawczy jest prezentowany maksymalnie przez 10 s i jest przerywany w momencie naciśnięcia przycisku grzybkowego. Jeśli osoba badana nie zareaguje naciśnięciem na przycisk grzybkowy, jest to odnotowywane jako błąd.

Oceny percepcji sygnałów ostrzegawczych AR (w rzeczywistości rozszerzonej) i klasycznych sygnałów ostrzegawczych dokonuje się za pomocą obiektywnych wskaźników i subiektywnej oceny.

10.6.2. Wskaźniki obiektywne

Badania systemów AR w zastosowaniach przemysłowych zazwyczaj polegają na porównaniu efektywności pracy na klasycznych stanowiskach z efektywnością na stanowiskach z zastosowaniem AR. Jako wskaźniki przydatności tych systemów stosuje się:

- czas reakcji
- liczbę popełnionych błędów.

Wskaźniki te przyjęli w badaniach Cohn (1996), a także Chung i in. (2002), Gros i in. (2005) oraz Oehme i in. (2003). Pierwszym obiektywnym wskaźnikiem skuteczności działania sygnałów typu AR i klasycznych sygnałów ostrzegawczych jest *refleks*. Refleks jest to czas, jaki upływa od momentu pojawienia się bodźca do wystąpienia reakcji na ten bodziec. Czas reakcji jest bardzo zmienny, wiąże się z szybkością pobudzenia nerwowego, z płcią, wiekiem, stanem fizjologicznym, z wprawą, zainteresowaniem itd. Obecnie badanie czasu reakcji odgrywa istotną rolę w doborze kandydatów do pewnych zawodów, przede wszystkim na stanowiska wymagające szybkich reakcji, dużego natężenia uwagi i do innych prac o charakterze operatorskim, co wykazał Sillamy (1989).

Znaczenie, jakie ma szybki refleks w wykonywaniu określonego typu prac i zawodów, wynika zapewne z faktu, że szybkość reakcji – będąc jedną z cech czasowej charakterystyki zachowań – jest zaliczana do cech temperamentu (Strelau, 1985). Wyniki badań Strelau (1996) oraz Zawadzkiego i Strelau (1992), nad regulacyjną rolą temperamentu w przebiegu zachowań w sytuacji stresowej, wykazały istnienie związku między stylem radzenia sobie ze stresem i żwawością – cechą temperamentu wyznaczającą czasowy charakter przebiegu reakcji.

W badaniach czasu reakcji warto uwzględnić, że – jak wynika z pracy Strelau (1985) – nie ma związku między motorycznymi i werbalnymi wskaźnikami

charakterystyki czasowej zachowania. Oznacza to, że średni czas reakcji motorycznej (np. naciśnięcie palcem przycisku) na określony bodziec (np. pojawienie się czerwonego światła) może być znacząco różny od czasu reakcji werbalnej (np. wypowiedzenie słowa „tak") na ten sam rodzaj bodźca.

Drugim obiektywnym wskaźnikiem skuteczności działania sygnałów typu AR i klasycznych sygnałów ostrzegawczych są błędy popełniane przez osoby badane. Analizowane są dwa rodzaje błędów, a mianowicie:

- brak reakcji na bodziec (nienaciśnięcie przycisku na sygnał alarmowy) lub wystąpienie reakcji bez bodźca (naciśnięcie przycisku, mimo że sygnał alarmowy się nie pojawił)
- błędy popełniane w trakcie rozwiązywania zadania komputerowego (pozostawienie obiektu na taśmie lub umieszczenie go w nieodpowiednim zasobniku).

10.6.3. Ocena subiektywna

Subiektywnej oceny skuteczności działania ostrzegawczych sygnałów typu AR i sygnałów klasycznych dokonuje się na podstawie ankiety, zawierającej cztery pytania kierowane do osób badanych. Pytania dotyczą oceny szybkości własnych reakcji na obydwa rodzaje bodźców, tj. sygnały ostrzegawcze, oraz preferencji jednego z nich. Jako podstawę do określania wskaźników subiektywnych przyjmuje się skalę trójstopniową, typu: „tak", „nie", „nieistotne", lub pięciostopniową skalę Likerta.

10.6.4. Opis eksperymentu

Eksperyment, podobnie jak w badaniach Chunga, Shewchuka i Willigesa (2002) oraz Oehmea i Brunsa (2003), polegał na porównaniu reakcji osób badanych w normalnych, obecnie spotykanych warunkach pracy z reakcjami w przypadku stosowania systemów AR. Szczególne znaczenie ma tutaj właściwy dobór sygnałów ostrzegawczych. W projektowaniu systemów ostrzegawczych do maszyn należy posługiwać się normami zharmonizowanymi z dyrektywą maszynową 2006/42/WE. Właściwa jest tu norma PN-EN 61310-1:2009. Zgodnie z tą normą sygnały AR należy zakwalifikować jako aktywne wizualne sygnały ostrzegawcze. Ponadto wszystkie sygnały dotyczące bezpieczeństwa powinny być tak zaprojektowane, aby ich znaczenie było dla przewidywanego użytkownika jasne, wyraźne i oczywiste, bez dwuznaczności. Należy przy tym uwzględnić zasady ergonomii. Informacje dotyczące bezpieczeństwa powinny być przedstawiane z wykorzystaniem środków dostosowanych do zdolności percepcyjnych operatorów i/lub osób narażonych na niebezpieczeństwo. Aktywne sygnały wizualne powinny być realizowane poprzez:

– załączanie/wyłączanie lub zmianę:
  - barwy
  - jaskrawości
  - kontrastu
  - nasycenia
– migotanie
– zmianę położenia.

Sygnał wizualny powinien:
– być umieszczony tak, by znajdował się w polu widzenia człowieka
– mieć odpowiednią jaskrawość i kontrastową barwę w porównaniu z jego tłem.

W celu ułatwienia postrzegania, sygnały wzrokowe należy stosować następująco:
– sygnały i źródła światła należy tak dobierać, aby ich działanie można było dostrzec ze wszystkich miejsc, z których powinny być widoczne
– sygnały aktywne dotyczące bezpieczeństwa powinny być tak umieszczone, aby były widoczne dla operatorów z pozycji ich pracy, i pod możliwie największym kątem.

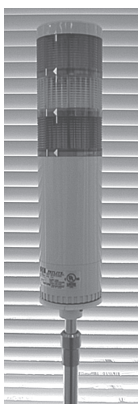
W kodach wizualnych informacje powinny być kodowane za pomocą metod dobranych spośród niżej wymienionych lub ich kombinacji:
– odcienia
– kontrastu
– symboli
– częstotliwości (trwanie/częstość powtarzania)
– położenia
– kształtu,

przy czym nie wymaga się użycia jedynie tych metod.

Barwy powinny być dobrane odpowiednio do informacji, którą mają przekazać; niebezpieczeństwo sygnalizuje barwa czerwona. Ponadto, jeśli kodowanie barwą jest stosowane w odniesieniu do bezpieczeństwa, to należy je uzupełnić dodatkowym sposobem kodowania. W przypadku sygnałów wizualnych są to:
– kształt (alfanumeryczny, graficzny)
– zmienność (migotanie).

Do sygnalizowania sytuacji niebezpiecznych zaleca się stosowanie znaków w kształcie koła.

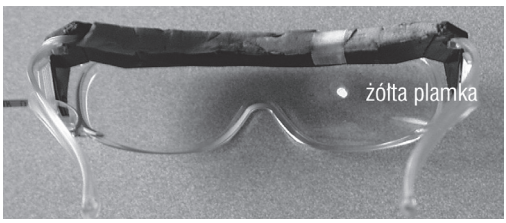
Zgodnie z tymi zasadami, a także wnioskami przedstawionymi przez Cohna (1996) oraz Grosa i in. (2005), w eksperymencie zastosowano następujące rodzaje sygnalizacji ostrzegawczej:
1) tradycyjny sygnał ostrzegawczy (rys. 10.10), tj. pojawienie się sygnału świetlnego w kolorze czerwonym (**ST**)



Rys. 10.10. Sygnalizator zastosowany jako tradycyjny sygnał ostrzegawczy

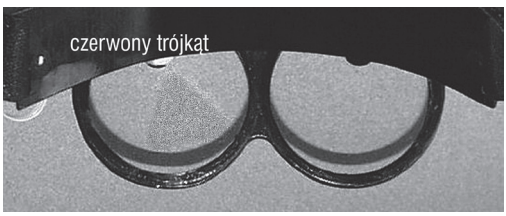
2) sygnał alarmowy typu AR w postaci czerwonej kropki wyświetlanej na okularze (**AR1**) – rys. 10.11
3) sygnał alarmowy typu AR w postaci czerwonej pulsującej kropki wyświetlanej na okularze (**AR2**) – częstotliwość pulsowania równa 4 Hz
4) sygnał alarmowy typu AR w postaci słowa STOP w kolorze czerwonym, wyświetlanego na okularze LITEYE-500 (**AR3**) – rys. 10.6
5) sygnał alarmowy typu AR w postaci żółtej kropki wyświetlanej na okularze (**AR4**) – rys. 10.12

Rys. 10.11. Widok czerwonej plamki, która była stosowana w wariantach AR1, AR2 i AR5



Rys. 10.12. Sygnał AR w postaci żółtej plamki

6) sygnał alarmowy typu AR w postaci czerwonej pulsującej kropki wyświetlanej na okularze (**AR5**) – częstotliwość pulsowania 8 Hz (większa częstotliwość migotania jest słabo rozpoznawalna)
7) sygnał alarmowy typu AR w postaci czerwonego trójkąta (**AR6**) – rys. 10.13.



Rys. 10.13. Sygnał AR w postaci czerwonego trójkąta

Eksperyment był prowadzony w dwu cyklach. Pierwszy cykl eksperymentalny w trzech następujących sesjach:

- sesja **E I** – wariant z klasycznym sygnałem ostrzegawczym + wariant z sygnałem typu AR1 (**ST + AR1**)
- sesja **E II** – wariant z klasycznym sygnałem ostrzegawczym + wariant z sygnałem typu AR2 (**ST + AR2**)

- sesja **E III** – wariant z klasycznym sygnałem ostrzegawczym + wariant z sygnałem AR2 (**ST + AR3**).

Drugi cykl eksperymentalny prowadzono w trzech następujących sesjach:

- sesja **E 4** – wariant z klasycznym sygnałem ostrzegawczym + wariant z sygnałem typu AR1 (**ST + AR4**)
- sesja **E 5** – wariant z klasycznym sygnałem ostrzegawczym + wariant z sygnałem typu AR2 (**ST + AR5**)
- sesja **E 6** – wariant z klasycznym sygnałem ostrzegawczym + wariant z sygnałem AR2 (**ST + AR6**).

Oznacza to, że w ramach jednej sesji eksperymentu osoba badana uczestniczyła w dwóch jego wariantach: wariant pierwszy – polegający na połączeniu zadania z klasycznym sygnałem ostrzegawczym oraz wariant drugi – polegający na połączeniu zadania z jednym z rodzajów sygnału typu AR.

Wszystkie sygnały były generowane na tym samym tle. Podczas eksperymentu warunki oświetleniowe zapewniano za pomocą oświetlenia sztucznego o współczynniku oddawania barw równym 82 (zmierzono metodą spektroradiometryczną; w normie PN-EN 12464-1:2011 zaleca się, aby w pomieszczeniach roboczych stosować oświetlenie o współczynniku oddawania barw powyżej 80), typowym dla oświetlenia stanowisk prac. Podczas eksperymentu w sposób ciągły mierzono natężenie oświetlenia w polu zadania. Natężenie to zmieniało się w zakresie 440 – 550 Lx. Norma PN-EN 12464-1:2011 zaleca, aby przy pracach we wnętrzu natężenie oświetlenia wynosiło powyżej 300 Lx. Natomiast przeprowadzone badania (Pawlak i Wolska, 2005a; 2005b; 2006), wykazały, że na rzeczywistych stanowiskach pracy natężenie oświetlenia zmienia się w zakresie 350 – 600 Lx.

Czas trwania każdego wariantu wynosił 20 min i w tym czasie sygnał ostrzegawczy pojawiał się około 10 razy z losową częstością. Dwa warianty, które odbywały się w ramach jednej sesji eksperymentu, dzieliła 30-minutowa przerwa.

Każda z badanych osób brała udział w trzech sesjach eksperymentu. W celu wyeliminowania efektu wprawy w wykonywaniu zadania komputerowego założono, że kolejność uczestniczenia w poszczególnych sesjach eksperymentu, jak również kolejność wariantu w każdej sesji, były określane losowo.

Wszystkie eksperymenty wykonywano o tej samej porze dnia, w godzinach $9^{00} – 12^{00}$.

10.6.5. Dobór grupy eksperymentalnej

Dobór wielkości grupy eksperymentalnej przez różnych badaczy jest bardzo zróżnicowany. Na przykład Papastavrou i Lehto (1995) do potwierdzenia modelu teorii detekcji sygnałów rozproszonych w zastosowaniu do projektowania sygnałów

ostrzegawczych przeprowadzili eksperyment z udziałem sześciu osób w wieku 19–31 lat. Także w eksperymencie przeprowadzonym przez Burt i in. (1995) badane były reakcje sześciu osób w wieku 20–30 lat. Natomiast Cohn (1996) przeprowadzał eksperyment z trzema osobami. W badaniach opisanych przez Chana i Chana (2006), mających na celu ocenę wpływu sygnałów ostrzegawczych akustycznych i wizualnych generowanych w sposób synchroniczny i asynchroniczny na czas reakcji i liczbę popełnianych błędów, uczestniczyły 34 osoby. Liu i Uang (2007) badali reakcję 30 osób w wieku 20–24 lat. Natomiast Campos i in. (2007) przeprowadzili eksperyment z udziałem dziewięciu studentów. Tak więc, badając percepcję sygnałów ostrzegawczych, zwłaszcza w celu określenia ogólnych tendencji jakościowych, a nie uzyskania precyzyjnych danych ilościowych, badacze stosują dużą dowolność w ustalaniu liczebności grupy eksperymentalnej. W związku z tym przyjęto kryterium wynikające z algorytmu wyboru testu istotności różnic (Brzeziński, 1997). Zgodnie z tym algorytmem grupa większa niż 30-osobowa jest traktowana jako duża i stosuje się do niej test *z*. Natomiast grupa mniejsza niż 30-osobowa jest traktowana jako mała i stosuje się do niej test *t*. Ponieważ w badaniach percepcji bardziej odpowiedni jest test *t*, więc przyjęto jako właściwą 30-osobową grupę badaną. Zdecydowano, że eksperyment będzie prowadzony w dwu cyklach. W pierwszym cyklu eksperymentalnym uczestniczyły 23 osoby, a w drugim 30 osób. W obu cyklach były to różne osoby. W efekcie w eksperymencie uczestniczyły 53 osoby, tak więc przeprowadzono badania 318 wariantów w 159 sesjach eksperymentalnych. Uczestnikami byli mężczyźni, studenci, w wieku 20–25 lat, nieużywający okularów ani soczewek korekcyjnych. Wybór tego rodzaju grupy wynikał z następujących założeń:

- grupa osób badanych powinna być jednorodna ze względu na płeć, a na stanowiskach operatorskich w warunkach przemysłowych pracują zazwyczaj mężczyźni
- osoby badane nie powinny mieć doświadczenia z pracą na stanowiskach z sygnalizacją ostrzegawczą
- osoby badane powinny mieć dobry wzrok.

Osoby badane otrzymały instrukcję, zgodnie z którą na badania miały się zgłaszać wypoczęte, wyspane, bez dolegliwości zdrowotnych oraz po śniadaniu.

Zgodnie z zasadami prowadzenia badań (Brzeziński, 1997) plan eksperymentu powinien spełniać – na zadowalającym poziomie – następujące metodologiczne kryteria jego „dobroci":

- **trafność teoretyczna:** metodykę prowadzenia badań opracowano zgodnie z zasadami *criterion task set* w wersji *dual task* (Shingledecker, 1984). Analiza literatury potwierdziła, że jest to najpowszechniej stosowany sposób prowadzenia eksperymentu dotyczącego badań sprawności operatorów systemów technicznych

– **trafność wewnętrzna:**
  - kontrolowano czynniki, które – poza rodzajem sygnału – mogły mieć wpływ na jakość percepcji, m.in. wiek, płeć, parametry wzroku, kondycję psychofizyczną osób przystępujących do badań, oświetlenie laboratorium
  - wyniki przeprowadzonych badań wskazują na efektywność manipulacji zmienną niezależną, jaką jest rodzaj sygnału
– **trafność zewnętrzna:** zapewniono reprezentatywność warunków badania – zadanie wykonywane przez osoby badane angażowało procesy poznawcze związane z pracą na tego typu stanowiskach
– **odpowiedniość modelu statystycznego:** analiza wariancji w badaniu eksperymentalnym typu „wielo-jednozmiennowym".

10.6.6. Wyniki badań

W badaniach jako wskaźniki obiektywne przyjęto czas reakcji na sygnał ostrzegawczy i liczbę popełnionych błędów. Natomiast jako wskaźniki subiektywne – wyniki ankiety zawierającej następujące pytania:

1. Który z zastosowanych rodzajów sygnałów szybciej Pan zauważał?
2. Który z zastosowanych rodzajów sygnałów był lepiej widoczny?
3. Który z zastosowanych rodzajów sygnałów bardziej przeszkadzał w wykonywaniu zadań?
4. Który z zastosowanych rodzajów sygnałów chętniej zastosowałby Pan w swojej pracy?

Uzyskane w trakcie eksperymentu wyniki pomiarów czasu reakcji poddane zostały analizie statystycznej przy założeniu rozkładu normalnego. Analizę prowadzono dla wyników zebranych w każdym cyklu eksperymentalnym niezależnie. Dla każdego zbioru wyników wyznaczone były podstawowe statystyki:

– wartość średnia – $T^{i}_{śr}$
– odchylenie średnie standardowe σ^{i}
– wartości: maksymalna T^{i}_{max} i minimalna T^{i}_{min},

gdzie i – numer kolejny osoby badanej.

Analizę czasów reakcji prowadzono przez porównanie wartości ich podstawowych statystyk ($T^{i}_{śr}$, σ^{i}, T^{i}_{max}, T^{i}_{min}) w następujących kombinacjach:

AR1^{i} z **ST1**^{i}
AR2^{i} z **ST2**^{i}
AR3^{i} z **ST3**^{i}
AR4^{i} z **ST**^{i}
AR5^{i} z **ST**^{i}
AR5^{i} z **ST**^{i} .

Porównanie wartości średnich czasów reakcji wskazywało, który z sygnałów był łatwiej rozpoznawany przez osobę badaną. Natomiast porównanie wartości odchyleń standardowych wskazywało, który z sygnałów prędzej do osoby badanej docierał.

Kolejnym zakładanym obiektywnym wskaźnikiem percepcji jest liczba popełnionych błędów. Rozważano dwa rodzaje błędów:

– pominięcie sygnału ostrzegawczego
– błędy w wykonywaniu zadania manualnego *primary task*.

Porównywano liczbę błędów popełnianych przez osobę badaną w dwu wariantach każdej sesji:

– z sygnałem ST
– z sygnałem AR.

Następnie przeanalizowano procentowy udział osób, u których wystąpiła istotna różnica w liczbie popełnionych błędów. Analizy te przeprowadzano dla trzech rodzajów sygnałów AR niezależnie w każdym cyklu eksperymentalnym.

Aby ocenić różnicę pomiędzy poszczególnymi rodzajami sygnałów w dwóch aspektach (klasyczny w porównaniu z rozszerzonym oraz porównanie trzech typów sygnałów), zastosowano dwuczynnikową analizę wariancji. Metoda ta polega na wyznaczeniu miary zróżnicowania odpowiedzialnej za uzyskany efekt (czyli różnic między średnimi w poszczególnych sytuacjach eksperymentalnych, V-efekt) oraz miar zróżnicowania będącego skutkiem rozrzutu uzyskanych wyników (V-błąd).

Aby ocenić, czy uzyskany efekt jest nieprzypadkowy, obliczano stosunek V-efekt do V-błąd, określając statystykę testu oznaczaną jako F. Jeśli jest ona odpowiednio duża, tj. zróżnicowanie między sytuacjami eksperymentalnymi jest znacznie większe niż płynące z losowego rozrzutu danych, stwierdza się, że efekt jest nieprzypadkowy, a zatem istotny statystycznie. Na podstawie F obliczano prawdopodobieństwo uzyskania takiego efektu przez przypadek, czyli poziom istotności „p". Jeśli $p < 0{,}05$, a zatem jest mniej niż 5% szans na to, że efekt był dziełem przypadku, to efekt ten uznawano za potwierdzony i istotny statystycznie. Interpretacja zależy od tego, o którym efekcie mowa:

1) jeśli istotny jest efekt pierwszego czynnika, uznaje się, że jest różnica między sygnałem klasycznym i rozszerzonym
2) jeśli istotny jest efekt drugiego czynnika, uznaje się, że jest różnica między różnymi wariantami sygnału rozszerzonego
3) jeśli istotna jest interakcja czynników, uznaje się, że różnice między sygnałem klasycznym i rozszerzonym są różne w zależności od wariantu sygnału.

Statystykę *t* wyznaczano na podobnej zasadzie, lecz w sytuacji kiedy do porównania były tylko dwie konkretne grupy wyników. Poziom istotności „p" oznacza

wówczas prawdopodobieństwo tego, że uzyskana różnica jest dziełem przypadku, i identycznie – różnica była interpretowana jako istotna, gdy $p < 0,05$.

Aby ocenić istotność różnicy pomiędzy średnimi uzyskanymi w różnych warunkach, wyniki poddano analizie statystycznej w modelu dwuczynnikowej analizy wariancji z powtarzanymi pomiarami. Pierwszy czynnik (AR) miał dwa poziomy i odpowiadał różnicom między sygnałem standardowym a sygnałem rzeczywistości rozszerzonej. Drugi czynnik (wariant) odpowiadał trzem wariantom prezentacji sygnału AR.

Wykazanie istotności wpływu pierwszego czynnika oznacza weryfikację tezy, że sygnał rozszerzony wywiera wpływ różny od klasycznego.

Istotność drugiego czynnika weryfikuje hipotezę o różnicach pomiędzy poszczególnymi wariantami sygnałów rozszerzonych.

Wykazanie istotnej interakcji oznacza, że różnice pomiędzy sygnałem klasycznym i rozszerzonym są nieidentyczne w poszczególnych wariantach sygnału. W każdym wariancie różnicę pomiędzy sygnałem klasycznym i rozszerzonym oceniono dodatkowo testem t-Studenta dla prób zależnych.

Wyniki ankiety dla trzech wariantów sygnału, wyrażone na skali szacunkowej, porównano testem porównywania proporcji.

Uzyskane wyniki wykazały, że percepcja wizualnych sygnałów ostrzegawczych generowanych metodą rzeczywistości rozszerzonej (AR) różni się istotnie od percepcji sygnałów ostrzegawczych generowanych metodą tradycyjną (ST), zarówno w zakresie wskaźników obiektywnych jak i subiektywnej oceny jakości percepcji. W pierwszym cyklu eksperymentalnym sygnał typu AR w postaci czerwonej plamki widocznej na okularach był istotnie lepszy w porównaniu z sygnałem tradycyjnym, ze względu na czas reakcji na sygnał oraz tempo pracy: reakcje osób badanych na sygnał AR były szybsze, jak również większa liczba wypełnionych palet towarzyszyła temu sygnałowi. Natomiast sygnał typu AR w postaci czerwonego napisu STOP widocznego na okularach okazał się istotnie gorszy od sygnału tradycyjnego pod względem czasu reakcji: w tym przypadku czas reagowania na napis STOP był dłuższy niż na sygnał tradycyjny. Natomiast w drugim cyklu eksperymentalnym sygnał AR w postaci żółtej plamki okazał się znacząco lepszy od sygnału tradycyjnego pod względem tempa pracy, ale gorszy ze względu na czas reakcji: osoby badane wolniej reagowały na żółtą plamkę ukazującą się na okularach niż na sygnał tradycyjny, choć liczba wypełnionych palet była w tym wypadku większa. Ponadto, w tym samym eksperymencie, sygnał AR w postaci czerwonej plamki widocznej na okularach i migającej z częstotliwością 8 Hz był istotnie lepszy w porównaniu z sygnałem tradycyjnym pod względem homogeniczności czasów reakcji: rozrzut wyników pomiaru czasu reakcji był mniejszy w wypadku sygnału AR.

Istotne różnice między percepcją sygnałów ostrzegawczych typu AR i sygnału tradycyjnego wystąpiły także w zakresie subiektywnej oceny jakości percepcji. Porównanie preferencji osób badanych dotyczących dwóch typów sygnałów, ST i AR, wskazuje na lepszą ocenę sygnału AR, gdy jest nim czerwona plamka lub czerwona migająca plamka, niezależnie od częstotliwości migania. Sygnał AR jest wówczas szybciej zauważany, lepiej widoczny i chętniej byłby stosowany w pracy. Natomiast czerwony napis STOP bardziej przeszkadza w wykonywaniu zadań niż sygnał tradycyjny. Bardziej przeszkadzający w pracy jest również sygnał AR w postaci żółtej plamki, choć jest on oceniany jako szybciej zauważany niż sygnał ST. Pod względem widoczności sygnał tradycyjny jest lepiej oceniany niż AR w postaci czerwonego trójkąta. Z kolei, czerwony trójkąt oceniono jako szybciej zauważany niż sygnał tradycyjny.

Można zatem stwierdzić, że w przypadku większości analizowanych wskaźników obiektywnych i subiektywnej oceny jakości percepcji sygnałów ostrzegawczych lepsze okazały się sygnały typu AR w porównaniu z sygnałem tradycyjnym. Jednym z możliwych wyjaśnień takiego wyniku może być fakt, że sygnał typu AR, wyświetlany na okularach, zawsze znajduje się w polu widzenia osoby, która w tych okularach pracuje, podczas gdy widoczność sygnału generowanego metodą tradycyjną na sygnalizatorze zmienia się w zależności od zmiany pozycji ciała lub miejsca na stanowisku, na którym aktualnie znajduje się pracownik.

Okazało się jednak, że sygnał tradycyjny „wygrywa" z sygnałem typu AR w postaci czerwonego napisu STOP. Czas reakcji na bodziec tradycyjny był bowiem istotnie krótszy. Wynik ten można wyjaśnić, odwołując się do teorii spostrzegania, która wyróżnia dwa poziomy tego procesu, a mianowicie: poziom sensomotoryczny i poziom semantyczno-operacyjny (Tomaszewski, 1976). Można przypuszczać, że percepcja sygnału tradycyjnego odbywa się na poziomie sensomotorycznym (spostrzeganie figuralne), umożliwiającym wyodrębnianie figur (np. punktów, linii, brył). Natomiast percepcja napisu STOP przebiega na poziomie semantyczno-operacyjnym (spostrzeganie przedmiotowe), więc nie ogranicza się do fizycznych cech przedmiotów jednostkowych (rzeczy, osób, zdarzeń), lecz umożliwia także spostrzeganie ich reprezentacji (modeli, wykresów, słów). Ponadto, można przypuszczać, że droga poprzez kolejne fazy procesu spostrzegania, zaczynając od wrażenia (rejestracji sensorycznej), poprzez organizację (ocenę emocjonalną), następnie rozpoznanie i ocenę znaczenia metaforycznego, może trwać dłużej w odniesieniu dno słowa STOP niż do czerwonego światła na sygnalizatorze, ze względu na fazę trzecią, czyli rozpoznanie (Kosslyn i Rosenberg, 2006). Na tym etapie procesu spostrzegania dochodzi bowiem do oceny semantycznej bodźca, umożliwiającej włączenie go do określonej kategorii. Działa wówczas efekt wielkości zbioru polegający na tym, że im więcej bodźców

należy wziąć pod uwagę w procesie porównywania, tym więcej czasu zajmuje ten proces (Maruszewski, 2001). W tej sytuacji napis STOP jest bodźcem bardziej złożonym niż czerwone światło.

W ocenie subiektywnej napis STOP uznano za bardziej przeszkadzający w pracy. Być może ocena ta wynika z faktu, że napis widoczny na okularach przesłania większą część pola widzenia niż znak w postaci plamki.

Wyniki przeprowadzonej analizy potwierdziły ponadto, że percepcja wizualnych sygnałów ostrzegawczych w zakresie trzech sygnałów AR (czerwona plamka, czerwony napis STOP, żółta plamka) i dwóch wskaźników jakości percepcji (czas reakcji, tempo pracy) jest istotnie różna. Okazało się bowiem, że w pierwszym cyklu eksperymentalnym najlepszy ze względu na czas reakcji okazał się sygnał w postaci czerwonej plamki widocznej na okularach, najgorszy zaś – czerwony napis STOP: osoby badane istotnie szybciej reagowały na czerwoną plamkę niż na napis STOP. Natomiast w drugim cyklu eksperymentalnym najgorszy ze względu na tempo pracy okazał się sygnał w postaci żółtej plamki widocznej na okularach: osoby badane wypełniały najmniejszą liczbę palet.

A zatem najwięcej zalet miał sygnał typu AR w postaci czerwonej plamki: reakcja na ten sygnał była najszybsza, a osoby badane miały przy nim najlepsze tempo pracy. Ponadto w ocenie subiektywnej czerwona plamka była najlepiej widoczna, najszybciej zauważana i byłaby najchętniej stosowana w rzeczywistych warunkach pracy. Natomiast, z porównania dwóch sygnałów różniących się barwą, a mianowicie czerwonej i żółtej plamki, wynika, że więcej zalet miała plamka w kolorze czerwonym. Wydaje się, że wynik ten ma uzasadnienie w systemie znaczeń społecznych, wykorzystywanym powszechnie w przypadku sygnałów ostrzegawczych, w którym barwa czerwona jest jednoznacznie kojarzona z zagrożeniem. Na istnienie tego rodzaju systemu wskazują m.in. wyniki badań nad percepcją słów i kolorów związanych z zagrożeniem – 76% osób badanych uznało kolor czerwony za najbardziej skojarzony z niebezpieczeństwem (Braun i Silver, 1995).

Istotnym uzupełnieniem przeprowadzonych analiz były komentarze dotyczące subiektywnego odczucia osób badanych w odniesieniu do obserwowanych sygnałów. W znakomitej większości tych komentarzy sygnały typu AR były oceniane jako bardziej przyjazne od sygnału tradycyjnego. Jednocześnie prawie wszyscy badani podkreślali znaczenie ergonomicznych właściwości okularów. Ich zdaniem lepsze przystosowanie ergonomiczne okularów AR znacznie poprawiłoby ich użyteczność.

10.7. Zalecenia dotyczące stosowania do maszyn sygnałów ostrzegawczych generowanych metodą AR

Wyniki prowadzonych badań wskazują, że wykorzystanie techniki AR do generowania sygnałów ostrzegawczych dla operatorów maszyn może być bardzo skuteczne, zwłaszcza tam, gdzie sygnały tradycyjne zawodzą. Tak więc, przy obecnym stanie wiedzy, systemy rzeczywistości rozszerzonej powinny być stosowane przede wszystkim jako uzupełnienie tradycyjnych systemów ostrzegawczych. Dotychczasowe doświadczenia z wykorzystania systemów AR są jeszcze zbyt ubogie, aby można było je stosować samodzielnie.

Sygnały rzeczywistości rozszerzonej zalicza się do grupy aktywnych sygnałów wizualnych. Wynika to stąd, że dostarczają one informacji o zmianie w stanie maszyny za pomocą jaskrawości, kontrastu, barwy, kształtu, rozmiaru lub położenia symbolu. Jeśli przekazywana informacja dotyczy zmiany ryzyka, to są to sygnały ostrzegawcze.

Podstawowe zasady stosowania sygnałów wizualnych mówią, że w celu ułatwienia postrzegania powinny być umieszczane tak, aby dostrzeżenie ich działania było możliwe ze wszystkich miejsc, z których powinny być widoczne. Aktywne sygnały dotyczące bezpieczeństwa powinny być umieszczone w miejscu widocznym dla operatorów z pozycji ich pracy, pod możliwie największym kątem. Podane wcześniej przykłady pokazują, że w tradycyjnych systemach ostrzegania wizualnego często jest to trudne do zrealizowania. Natura sygnałów AR gwarantuje spełnienie tych wymagań, gdyż one zawsze znajdują się w polu widzenia operatora. Ponadto istotną zaletą sygnałów AR jest to, że docierają jedynie do osoby zagrożonej, nie zakłócając pracy osób oddalonych.

Jak wiadomo, wszystkie sygnały dotyczące bezpieczeństwa powinny być tak zaprojektowane, aby ich znaczenie było dla przewidywanego użytkownika jasne, wyraźne i oczywiste bez dwuznaczności. Informacje dotyczące bezpieczeństwa powinny być przedstawiane z wykorzystaniem środków dostosowanych do zdolności percepcyjnych operatorów lub osób narażonych na niebezpieczeństwo. Dlatego też, aby sygnały te były skuteczne, należy je właściwie zaprojektować. Wyniki przeprowadzonych badań wskazują, że szczególne znaczenie ma rodzaj zastosowanego sygnału. Z oczywistych względów, podczas projektowania ostrzegawczych AR należy rozważać jedynie systemy *see-through*. W takich systemach, jeśli nie ma sygnału, obserwowane jest rzeczywiste stanowisko pracy. Natomiast w systemach, które funkcjonują na zasadzie uzupełniania obrazu z kamery o dodatkowe sygnały, otoczenie jest obserwowane na monitorze. Rozwiązanie takie nie jest wystarczająco dokładne i pewne, aby mogło być stosowane w przemyśle. Wiąże się to przede

wszystkim ze zbyt małą dokładnością odtwarzania obrazów rzeczywistych oraz uzupełniania ich obrazami wirtualnymi.

Do sygnalizowania zagrożeń powinno się stosować jak najprostsze symbole. Wyniki badań potwierdzają, że najskuteczniejsze są okrągłe plamy, których odbiór nie wymaga dalszej analizy semantyczno-operacyjnej. Wszelkie dodatkowe znaki znacząco wydłużają czas percepcji, co może ograniczyć ich skuteczność. Ponadto należy zwrócić uwagę na ryzyko „przeciążenia zmysłów" w wyniku nadmiaru sygnałów wizualnych, co może prowadzić do pomijania urządzeń sygnalizacji ostrzegawczej.

Istotny jest także właściwy dobór barwy znaku. Eksperyment przeprowadzony przez Dźwiarka i in. (2007) w zasadzie wykluczył stosowanie innych barw niż czerwona. Jest to także zgodne z wynikami uzyskanymi przez innych badawczy, a także z powszechnie przyjętymi zasadami i normami dotyczącymi sygnalizowania niebezpieczeństwa. Natomiast wskazane jest wspomaganie percepcji sygnału przez zastosowanie sygnałów migających. Badania wykazały, że najskuteczniejsze są sygnały migające z częstotliwością 4 – 8 Hz. Mniejsza częstotliwość migotania może powodować znaczne opóźnienia w reakcji na sygnał, gdyż przerwa pomiędzy kolejnymi rozbłyskami jest porównywalna z czasem reakcji operatora. Natomiast sygnał o większej częstotliwości migotania zaczyna być odbierany jako ciągły.

W projektowaniu urządzeń AR do zastosowań przemysłowych szczególną uwagę należy zwrócić na ich cechy ergonomiczne. Oceny subiektywne uzyskane podczas eksperymentu wyraźnie podkreślały znaczenie wygody użytkowania urządzenia. W miarę możliwości zaleca się, aby stosować urządzenia wykorzystujące aktualnie użytkowany sprzęt ochrony indywidualnej lub też konstruować wyposażenie podobne do aktualnie użytkowanego, uwzględniając przeprowadzenie oceny zgodności z właściwymi przepisami dotyczącymi wyposażenia roboczego.

Należy także pamiętać o przystosowaniu urządzeń do okresowych kontroli i konserwacji. Warunki środowiskowe w przemyśle mogą znacząco wpływać na pogorszenie stanu technicznego urządzeń. Powinny być więc przewidziane procedury sprawdzeń ich sprawności z wyraźnym wskazaniem użytkownikowi znaczenia tych sprawdzeń.

Podsumowując, urządzenia AR mogą być z powodzeniem stosowane do ostrzegania przed nadchodzącym zdarzeniem stwarzającym zagrożenie, takim jak rozruch maszyny lub nadmierna prędkość, jako urządzenia wspomagające tradycyjne systemy ostrzegawcze. Zwłaszcza wówczas, gdy ze specyfiki wykonywanej pracy wynika konieczność skierowania pola widzenia operatora w różnych kierunkach. Przykładami takich zastosowań mogą być:

- ostrzeganie o uruchomieniu maszyn w sytuacjach, gdy operator ma ograniczoną widoczność stref niebezpiecznych
- ostrzeganie o niebezpieczeństwie związanym z obsługą urządzeń transportu wewnętrznego, zwłaszcza suwnic
- sygnalizowanie zagrożeń w półzautomatyzowanych systemach wytwarzania.

Urządzenia ostrzegawcze powinny być tak zaprojektowane i umiejscowione, żeby bez trudności można było je sprawdzać. W informacjach dotyczących użytkowania powinien być zawarty opis sposobu regularnego sprawdzania urządzeń sygnalizacji ostrzegawczej.

Rozdział 11

Zastosowanie techniki VR do wspomagania doboru systemów ochronnych w projektowaniu maszyn

11.1. Wprowadzenie

Wykorzystanie technik komputerowych do projektowania maszyn w znacznym stopniu uprościło i przyśpieszyło prace konstruktorskie. Zazwyczaj symulacje komputerowe są wykonywane dla potrzeb analizy właściwości technicznych projektowanych urządzeń, ich możliwości technologicznych i parametrów roboczych (Niewieczerzał, 2006; Winkler, 2003). Natomiast projektant maszyny, tworząc nowe konstrukcje, powinien uwzględniać także kwestie bezpieczeństwa operatorów. Jedną z metod ograniczania ryzyka występującego przy obsłudze maszyn jest stosowanie urządzeń ochronnych. Obecnie etap uzbrajania maszyny w urządzenia ochronne jest najczęściej końcowym etapem jej konstruowania. Na tym etapie wszelkie zmiany konstrukcyjne mogą się okazać bardzo kosztowne. U podstaw podjęcia prac badawczych leżało założenie, że właściwego doboru urządzeń ochronnych można dokonać już na etapie projektu maszyny. Zwłaszcza zastosowanie w procesie projektowania techniki rzeczywistości wirtualnej może znacznie wspomagać dobór urządzeń ochronnych, ich sytuowanie w stosunku do stref zagrożenia i weryfikację zastosowanych rozwiązań. W dostępnej literaturze brakuje niestety publikacji o próbach modelowania stref zagrożenia w celu wspomagania projektowania systemów ochronnych do maszyn. Pierwsze próby wykorzystania systemów AR do redukcji ryzyka związanego z maszynami przedstawili Dźwiarek i Łuczak (2008). Doświadczenia zdobyte w związku z wykorzystaniem techniki VR do oceny ryzyka w procesie projektowania zautomatyzowanej linii produkcyjnej (Dźwiarek, 2010) stanowiły podstawę do podjęcia szerszych prac badawczych dotyczących modelowania stref zagrożenia przy projektowaniu maszyn.

11.2. Zastosowania VR w obszarze bezpieczeństwa

Prace dotyczące zastosowań technik rzeczywistości wirtualnej (badań wykorzystujących zaawansowane metody symulacji komputerowej) do analiz stanu bezpieczeństwa systemów przemysłowych są prowadzone w wielu ośrodkach na świecie. W USA najbardziej zaawansowane prace prowadzi np. Department of Health and Human Services, Center of Disease Control and Prevention NIOSH. Dotyczą one zastosowania wirtualnego modelowania do analiz ergonomicznych oraz oceny ryzyka na stanowiskach pracy w kopalniach. Zastosowanie tych technik do oceny ryzyka związanego z katastrofami naturalnymi zostało zaprezentowane przez Indirli (2007). Kim i Gong (2008) sformułowali zasady wykorzystania symulacji VR do oceny ryzyka wystąpienia kolizji w transporcie morskim. W Unii Europejskiej w ramach 6. Programu Ramowego został zrealizowany Projekt Zintegrowany VIRTHUALIS (VIrtual RealiTy and HUman Factors AppLications for Improving Safety). W ramach tego projektu opracowywane są metody wykorzystania modelowania wirtualnego do uwzględniania czynnika ludzkiego przy projektowaniu instalacji procesowych, zwłaszcza w przemyśle chemicznym i petrochemicznym (Winkler i in., 2005a, 2005b; Colombo i in., 2006). Zastosowanie techniki rzeczywistości wirtualnej do analiz bezpieczeństwa na placu budowy oraz wspomagania szkoleń przedstawili Haiyan i in. (2006). W pracy Dźwiarka i in. (2007b) zaprezentowano koncepcję zastosowania symulatorów VR do szkolenia kierowców wózków podnośnikowych w aspekcie bezpieczeństwa, a Grabowski i in. (2010) zaproponowali wykorzystanie symulacji wirtualnych do doboru systemów wizyjnych do maszyn. Winkler i in. (2009) opracowali zasady wykorzystania wizualizacji czynników ryzyka do zwiększania bezpieczeństwa w zakładach górnictwa podziemnego. Prowadzone są także prace dotyczące zastosowań systemów rzeczywistości rozszerzonej do zwiększenia bezpieczeństwa na stanowiskach pracy. Przykłady takich rozwiązań pokazano w rozdziale 10.

Ogólne zasady wykorzystania technik rzeczywistości wirtualnej w obszarze bezpieczeństwa pracy omówili Huelke i in. (2010) oraz Nickel i in. (2010). Przykłady zastosowań VR w dziedzinie bezpieczeństwa i ergonomii zaprezentowali Duffy i in. (2003), Mujber i in. (2004) oraz Nivolianitou i in. (2006). Prace w tym zakresie są prowadzone m.in. na potrzeby elektrowni nuklearnych, gdzie systemy VR dają możliwość szkolenia personelu w sytuacjach awaryjnych. Zastosowanie technik VR wydaje się szczególnie korzystne w sytuacjach, gdy szkolenia w warunkach rzeczywistych wiążą się z zagrożeniem zdrowia i życia człowieka. Z tego względu szkolenia w wirtualnym środowisku najczęściej są związane z takimi dziedzinami, jak medycyna (np. wirtualne operacje), (Gallagher i Cates, 2004) lub energetyka atomowa (np. ograniczenie narażenia pracownika na promieniowanie jonizujące), (Mól i in., 2008). Prowadzone są też badania z wykorzystaniem technik VR

obejmujące obsługę specjalistycznych maszyn, np. stosowanych w górnictwie (Ambrose i in., 2005). Techniki VR są stosowane do analizy ergonomicznych warunków pracy, np. przy obsłudze maszyn w kopalniach, oraz do identyfikacji potencjalnych zagrożeń, m.in. związanych z pracą w kopalni (Foster i Burton, 2003; Winkler i in., 2005a oraz Zhang i in. (2006). Przykład zastosowań VR do symulacji serwisowania i napraw maszyn przedstawili Winkler i in. (2008b). Prace te umożliwiły rozpoznanie potencjalnych zastosowań technik VR w różnych aspektach analizy i zwiększania bezpieczeństwa.

Istotnym krokiem do zastosowania technik komputerowych w analizie bezpieczeństwa na etapie projektowania maszyn było opracowanie systemu Computer Aided Safety Standards Application for Design (CASSA) przez Blaise i in. (2003). Narzędzie to wspomaga projektanta maszyny w prowadzeniu analizy możliwych scenariuszy zdarzeń z uwzględnieniem aspektów bezpieczeństwa. Do tego celu zastosowano specjalne, zorientowane na użytkownika interfejsy przystosowane do prowadzenia różnego rodzaju analiz. System uwzględnia także różne rodzaje użytkowników, takich jak projektanci maszyn czy eksperci grup normalizacyjnych. Narzędzie to wskazuje na skuteczność zastosowań modelowania 3D do oceny ryzyka na wczesnych etapach projektowania maszyn.

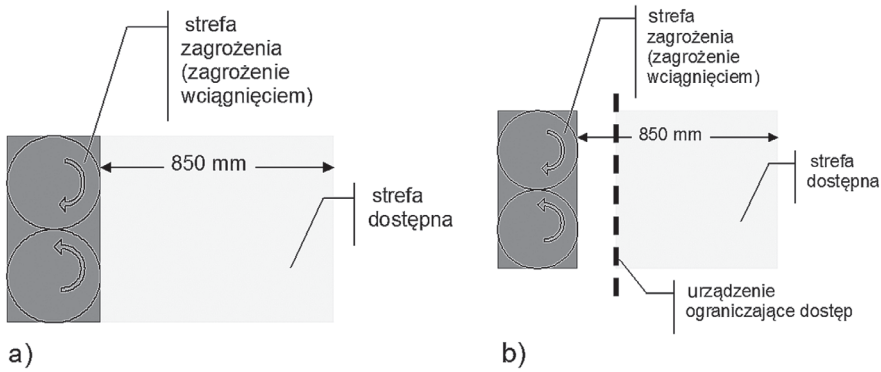
Doświadczenia praktyczne zdobyte podczas oceny ryzyka w fazie projektowania systemów wytwórczych, zaprezentowane przez Dźwiarka (2010), pokazały, że nawet niezbyt szczegółowe modele wirtualne zautomatyzowanych systemów wytwarzania mogą znacznie usprawnić niektóre etapy oceny ryzyka. Doświadczenia te potwierdziły się w trakcie opracowywania metody wirtualnego modelowania stref zagrożenia do wspomagania doboru urządzeń ochronnych do maszyn (Dźwiarek i in., 2010a, 2010b).

11.3. Zasady ograniczania dostępu do stref zagrożenia przy maszynach

Zasady wirtualnego modelowania stref zagrożenia (rozumianych jako strefy wewnątrz i/lub wokół maszyny, w których osoba może być narażona na zagrożenie) i stref dostępnych dla operatorów maszyn (rozumianych jako strefa wewnątrz i/lub wokół maszyny, w której może znaleźć się człowiek lub część jego ciała) wynikają z metod ograniczania ryzyka związanego z obsługą maszyn. Podstawowe zasady stosowania urządzeń ochronnych do maszyn, zaprezentowane przez Dźwiarka i in. (2010a, 2010b), prowadzą do następujących konkluzji (rys. 11.1):

- wypadek może się zdarzyć tylko wtedy, kiedy człowiek lub część jego ciała znajdzie się w strefie zagrożenia
- sytuacja taka jest możliwa, jeśli strefy dostępne docierają do stref zagrożenia

– projektant maszyny powinien zastosować wszelkie możliwe środki, aby zapewnić, że w maszynie nie będą występowały obszary wspólne dla stref zagrożenia i stref dostępnych.



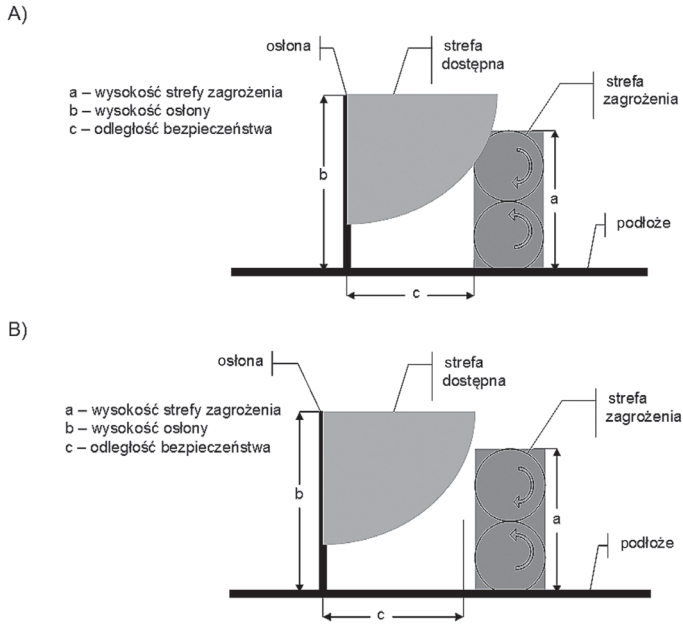
Rys. 11.1. Koncepcja ograniczania dostępu do stref zagrożenia przez stosowanie urządzeń ochronnych: a) brak urządzeń ochronnych – strefa dostępna dociera do strefy zagrożenia; b) zastosowano urządzenia ochronne – strefa zagrożenia jest odseparowana od strefy dostępnej

Do określania wielkości stref zagrożenia i stref dostępnych najwłaściwsze jest zastosowanie norm dotyczących bezpieczeństwa maszyn (PN-EN ISO 12100:2011, PN-EN ISO 13855:2010 i PN-EN ISO 13857:2010). Normy te określają, w jaki sposób należy rozdzielać strefy zagrożenia od stref dostępnych przez odpowiedni dobór kształtu i wzajemnego rozmieszczenia mechanicznych części składowych maszyny. Podstawowymi parametrami określającymi wielkość i wzajemne usytuowanie stref zagrożenia i stref dostępnych są odległości bezpieczeństwa, uniemożliwiające sięganie kończynami do stref niebezpiecznych.

Podstawowym środkiem ograniczania dostępu do stref zagrożenia są **osłony**. Są to wszelkiego typu bariery, przegrody, obudowy, ściany, siatki, drzwi itp. Osłony stanowią materialną barierę pomiędzy strefą zagrożenia a strefą dostępną, dzięki czemu uniemożliwiają dosięgnięcie do strefy zagrożenia. Skuteczność osłon zależy od ich usytuowania w stosunku do strefy zagrożenia. Istotne jest zwłaszcza zachowanie odległości, które uniemożliwią dosięgnięcie do strefy zagrożenia ponad otworami w osłonie, obok nich lub przez nie. W modelowaniu stref dostępnych przez osłony, obok nich lub ponad nimi uwzględnia się poziom redukowanego ryzyka oraz umiejscowienie osłon, a także ich wymiary geometryczne.

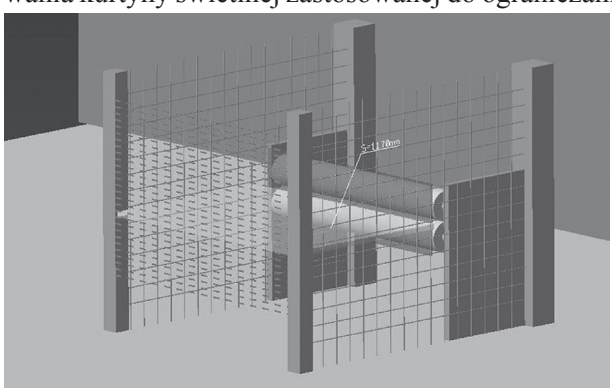
Przykład modelowania strefy zagrożenia i strefy dostępnej ponad osłoną pokazano na rys. 11.2.

Urządzenia ochronne są to techniczne środki bezpieczeństwa inne niż osłony. Do ograniczania dostępu do stref zagrożenia są stosowane urządzenia ochronne wykrywające człowieka lub części jego ciała i wytwarzające odpowiedni sygnał przesyłany do układu sterowania w celu ograniczenia ryzyka doznania urazu.



Rys. 11.2. Zasada modelowania strefy dostępnej i strefy zagrożenia w przypadku sięgania ponad osłoną: A) osłona usytuowania zbyt blisko strefy zagrożenia; B) osłona wystarczająco wysoka lub usytuowana wystarczająco daleko od strefy zagrożenia

Urządzenia te uniemożliwiają dosięgnięcie do strefy zagrożenia przez zatrzymanie ruchu niebezpiecznego, a więc wyeliminowanie zagrożenia, a tym samym wyeliminowanie strefy zagrożenia. W urządzeniach ochronnych wykrywających szczególną rolę odgrywa strefa wykrywania. Jest to strefa, w której wykrywana jest obecność człowieka. Strefa wykrywania jest więc obszarem, w którym kontrolowana jest strefa dostępna. Podstawowymi parametrami decydującymi o kształcie i umiejscowieniu strefy dostępnej z zastosowaniem urządzeń ochronnych są: czas zadziałania, rozdzielczość i wielkość strefy wykrywania. Na rys. 11.3 pokazano sposób modelowania kurtyny świetlnej zastosowanej do ograniczania dostępu do strefy zagrożenia przy prostopadłym kierunku zbliżania.



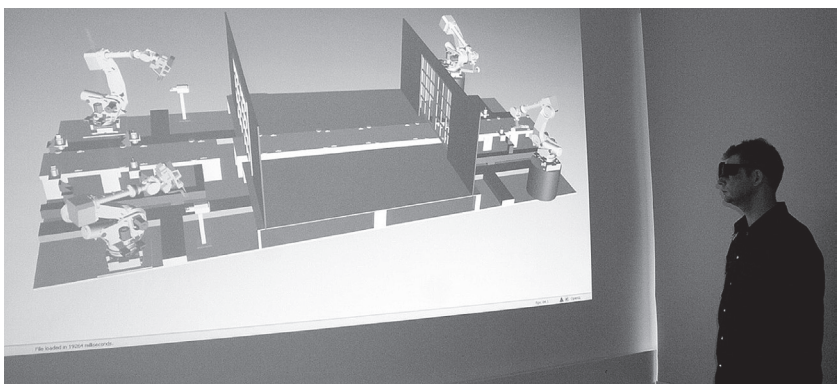
Rys. 11.3. Sposób modelowania kurtyny świetlnej zastosowanej do ograniczania dostępu do strefy zagrożenia przy prostopadłym kierunku zbliżania

11.4. Modelowanie stref zagrożenia w systemie VR

Pierwszym działaniem projektanta maszyny jest zidentyfikowanie stref zagrożenia i stref dostępnych. Oznacza to konieczność dysponowania przyjaznym interfejsem użytkownika. Dotyczy to dwu aspektów interaktywnej komunikacji z użytkownikiem w rzeczywistości wirtualnej:

- przyjaznego dla użytkownika prezentowania modelu
- wygodnego wprowadzania do modelu nowych obiektów z możliwością ich dowolnego sytuowania i tworzenia raportu zawierającego wszystkie uzyskane informacje.

Steed i Parker (2005) przedstawili wyniki eksperymentów mających na celu porównanie technik interakcji w wirtualnej rzeczywistości zanurzeniowej: techniki projekcyjnej (ang. *immersive projection technology* – IPT) i nagłownej (ang. *head mounted display* – HMD). W wyniku badań ustalono, że IPT jest najwłaściwsza w sytuacji dokonywania wyboru w VR, natomiast HMD powinna być stosowana, gdy w VR konieczne jest wykonywanie manipulacji z wykorzystaniem inforękawic. Tak więc zdecydowano, że do modelowania stref zagrożenia i stref dostępnych najwłaściwszy jest system projekcyjny (rys. 11.4), tym bardziej że umożliwia on prowadzenie badań przez grupę ekspertów.



Rys. 11.4. Prezentacja wirtualnego modelu systemu wytwórczego w stereowizyjnym systemie projekcyjnym

W celu usprawnienia procesu modelowania stref zagrożenia i stref dostępnych należy rozbudować interfejs graficzny użytkownika o dodatkowe funkcje, sterujące wprowadzaniem stref zagrożenia, stref dostępnych, osłon i urządzeń ochronnych do wirtualnego modelu analizowanych urządzeń. Można to osiągnąć za pomocą dodatkowych menu kontekstowych zawierających polecenia (Dźwiarek i in. 2010b):

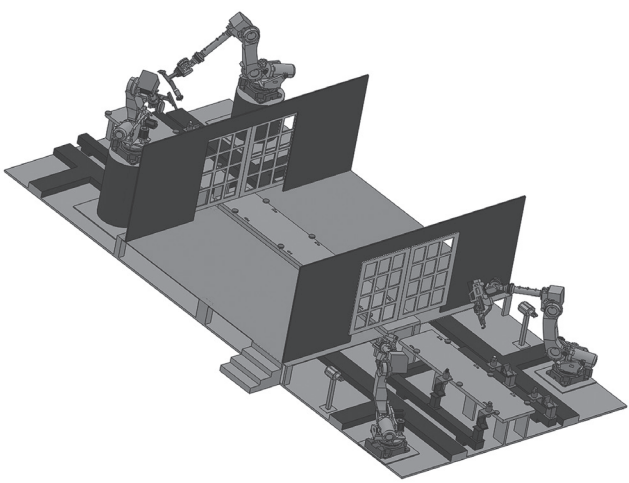
– „Wprowadź strefę zagrożenia”
– „Wprowadź osłonę lub urządzenie ochronne” → „Wprowadź osłonę”
– „Wprowadź urządzenie ochronne”.

Do wprowadzania modeli urządzeń ochronnych wykorzystuje się dodatkową bibliotekę obiektów, która zawiera modele funkcjonalne osłon i urządzeń ochronnych. Modele te są wyposażone w modele stref dostępnych, których parametry zadaje użytkownik. Dobór i sytuowanie urządzeń ochronnych i osłon jest tak prowadzony, aby nie występowały obszary przenikania się stref zagrożenia i stref dostępnych, co jest sygnalizowane przez system detekcji kolizji wbudowany w program Quest 3D. Wyniki przeprowadzonych prac są generowane w postaci raportu zawierającego wszystkie informacje o parametrach i usytuowaniu dobranych urządzeń ochronnych, tak aby można było je wykorzystać do projektowania maszyny w systemie CAD.

Przykład

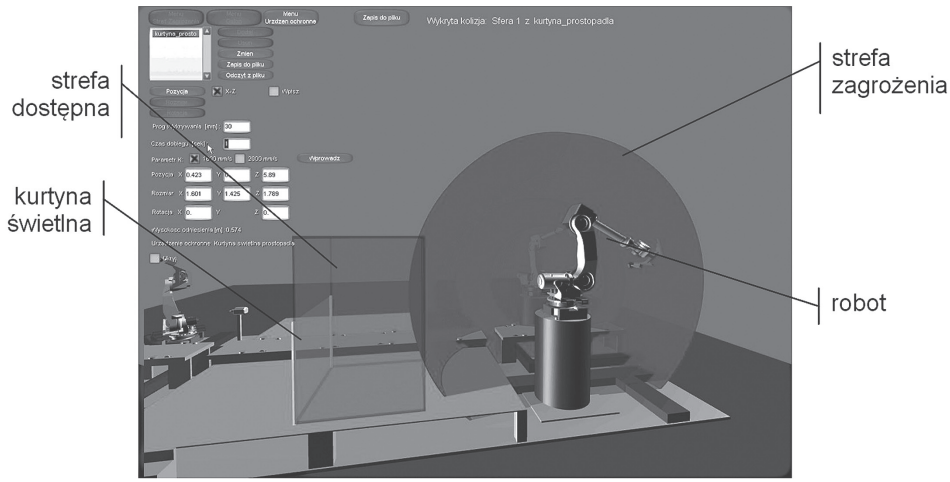
Metody modelowania VR stref zagrożenia i stref dostępnych w celu wspierania doboru systemów ochronnych do maszyn i systemów wytwórczych zostaną zademonstrowane na przykładzie modelu VR systemu wytwórczego. Dobierając system do modelowania, kierowano się kryterium różnorodności występujących stref zagrożenia, aby konieczne było zastosowanie jak największej liczby urządzeń ochronnych. W efekcie wykorzystano model systemu wytwórczego wykonany metodą inżynierii odwrotnej (Dźwiarek i in., 2010a; Dybała i in., 2011), pokazany na rys. 11.5, składający się z trzech stanowisk roboczych:

– robotów zgrzewających
– kontroli jakości
– robotów klejących.

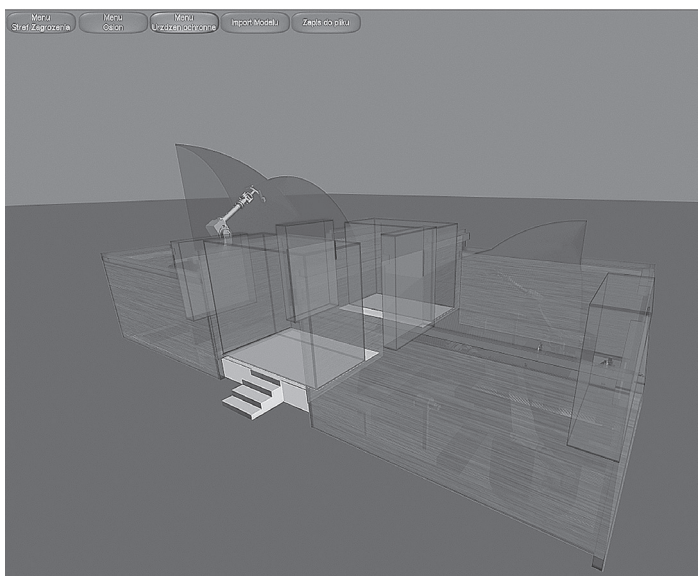


Rys. 11.5. Zrekonstruowany model CAD 3D systemu wytwórczego

Przykład modelowania strefy zagrożenia i doboru urządzenia ochronnego z zastosowaniem VR pokazano na rys. 11.6, a ostateczny efekt procesu doboru systemów ochronnych do systemu wytwórczego na rys. 11.7.



Rys. 11.6. Przykład doboru urządzenia ochronnego do zintegrowanego systemu wytwarzania z wykorzystaniem techniki VR



Rys. 11.7. Model VR systemu wytwórczego wyposażonego w systemy ochronne

Przeprowadzone badania potwierdziły, że wykorzystanie techniki VR w procesie doboru urządzeń ochronnych na etapie projektowania systemu wytwórczego umożliwia uwzględnienie zastosowania tych urządzeń podczas symulacji za pomocą nowoczesnych narzędzi komputerowych. Typowe podejście do symulacji procesów produkcyjnych w fazie wdrażania polega na analizie i optymalizacji takich parametrów, jak: czas cyklu, czas oczekiwania, czas procesu, określanych najczęściej na podstawie dokumentacji technologicznej produktu. Takie podejście nie uwzględnia wpływu konfiguracji systemu wytwórczego na analizowane parametry i w dużej mierze opiera się na doświadczeniu osoby opracowującej dane do modelu symulacyjnego. Dopiero wykorzystanie narzędzi wirtualnych opartych na modelach 3D daje możliwość dokładnej oceny czynności produkcyjnych i prowadzi do uzyskania wiarygodnych danych z etapu symulacji, przy czym nie jest obojętne użycie kompletnego modelu systemu wytwórczego, uwzględniającego również docelowe urządzenia ochronne.

Metody doboru urządzeń ochronnych mogą także być wykorzystane do przygotowania modeli służących do symulacji ergonomiczności i bezpieczeństwa. Modele zawierające urządzenia ograniczające dostęp do stref zagrożenia mogą w sposób obrazowy – zwłaszcza w środowisku rzeczywistości wirtualnej – pokazać skuteczność proponowanych środków ochrony. Ułatwi to w dużym stopniu proces projektowania systemów bezpieczeństwa.

Rozdział 12

Podsumowanie

Przedstawione w tej pracy aspekty projektowania systemów bezpieczeństwa do maszyn pokazują złożoność i szeroki zakres problemów, z jakimi musi się uporać projektant. Rozwój technik informatycznych umożliwił w znacznym zakresie wzrost funkcjonalności maszyn, ale zrodził także nowe, dotychczas nieznane problemy. Wypracowanie jednolitego, spójnego podejścia do projektowania systemów związanych z bezpieczeństwem, jakim jest metodyka bezpieczeństwa funkcjonalnego, dało możliwość przełamania wielu barier w rozwoju zastosowań nowoczesnych technologii. Wraz z opublikowaniem norm serii PN-EN 61508 zaproponowano jednoznaczny punkt odniesienia do formułowania wymagań dotyczących bezpieczeństwa złożonych systemów przemysłowych. Powstał swoisty język dyskusji, który umożliwia wzajemne zrozumienie różnych stron uczestniczących w tworzeniu urządzeń przemysłowych. Jednocześnie problematyka praktycznego stosowania metodyki bezpieczeństwa funkcjonalnego w bardzo różnych obszarach wskazuje na wiele zagadnień naukowych, których rozwiązanie wymaga szeroko zakrojonych badań. Dotyczy to głównie rozwiązania podstawowych problemów związanych z projektowaniem i programowaniem systemów:

- zasad oceny probabilistycznej
- doboru struktury odpowiedniej do kategorii lub poziomu nienaruszalności bezpieczeństwa
- organizacji cyklu trwałości bezpieczeństwa w zależności od złożoności systemu i poziomu ryzyka
- zarządzania jakością i bezpieczeństwem oprogramowania.

Wraz z rozwojem nowych technologii pojawiają się nowe zadania badawcze dotyczące skuteczności realizacji funkcji bezpieczeństwa. Obecnie najwięcej problemów napotyka prawidłowe rozwiązanie następujących zagadnień:

- koordynacji sterowania w systemach rozproszonych
- transmisji danych związanych z bezpieczeństwem w obrębie stanowiska pracy
- bezprzewodowego sterowania maszyną (np. zdalnego sterowania wyłączaniem awaryjnym) itp.

W najbliższej przyszłości należy się spodziewać problemów związanych ze stosowaniem do sterowania maszynami takich technologii, jak: sieci neuronowe, Internet, metody logiki rozmytej, systemy wizyjne, systemy samoprogramujące i samokonfigurujące się, sterowanie maszyn głosem itp. Technologie te formułują nowe zadania badawcze.

Zupełnie nową jakość stanowią próby wykorzystania technik VR i AR do wspomagania projektowania stanowisk pracy, a także do wykonywania pracy. W niedalekiej perspektywie spodziewany jest rozwój systemów teleoperacji, w których w środowisku wirtualnym odbywać się będzie sterowanie rzeczywistą maszyną. Można przewidywać, że zastosowanie technik VR i AR oraz nowoczesnych technik telekomunikacyjnych zrewolucjonizuje system organizacji pracy, tak jak już zrewolucjonizowało życie codzienne.

Bibliografia

Ambrose D.H., Bartels J.R., Kwitowski A.J., Helinski R.F., Gallagher S., McWilliams L.J., Battenhouse Jr. T.R. (2005) *Mining Roof Bolting Machine Safety: A Study of the Drill Boom Vertical Velocity.* Pittsburgh, NIOSH. Pub. No. 2005-128, Information Circular 9477, s. 1-56.

Anastassova M., Burkhardt J.M., Mégard C., Ehanno P. (2005) *Results from a user--centred critical incidents study for guiding future implementation of augmented reality in automotive maintenance.* International Journal of Industrial Ergonomics, 35(1), s. 67-77.

ARVIKA Konsortium (2001) *Augmented Reality for development, production and service* http://www.arvika.de.

Backström T., Harms-Ringdahl L. (1984) *A statistical study of control systems and accidents at work.* Journal of Occupational Accidents, 6(1-3), s. 197.

Belisle J., Laurin JA. (1999) *Analyse des causes d'un accident survenu une machine de coulee.* W: Proceedings of the 1st Conference on Safety of Industrial Automated Systems. Canada, Institut de recherché Robert-Sauvé en santé et en sécurité du Travail, s. 6-10.

Bliss J.P., Gilson R.D., Deaton J.E. (1995) *Human probability matching behaviour in response to alarms of varying reliability.* Ergonomics, vol. 38, no. 11, s. 2300-2312.

Blaise J-C., Lhoste P., Ciccotelli J. (2003) *Formalisation of normative knowledge for safe design.* Safety Science, vol. 41, no. 2-3, s. 241-261.

Bound A.C., Haniff D.J., Baber & Steiner S.J. (1999) *Virtual reality and augmented reality as a training tool for assembly tasks.* W: Proceedings of 1999 IEEE International Conference on Information Visualization. USA, Los Alamitos, s. 32-36.

Braun C.C., Silver N.C. (1995) *Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance*. Ergonomics, 38(11), s. 2207-2220.

Brzeziński J. (1997) *Metodologia badań psychologicznych.* Warszawa, PWN.

Burt J.L., Bartolome D.S., Burdette D.W., Comstock J.R. (1995) *A psychological evaluation of the perceived urgency of auditory warning signals.* Ergonomics, vol. 38, no. 11, s. 2327-2340.

Campos J.L., Yan J., Zhou L. *et al* (2007) *Visual and Auditory Information Specifying an Impending Collision of an Approaching Object.* Lecture Notes in Computer Science 4551, s. 720-729.

Chan A.H.S., Chan K.W.L. (2006) *Synchronous and asynchronous presentations of auditory and visual signals: Implications for control console design.* Applied Ergonomics, vol. 37, s. 131-140.

Charpentier Ph. (2005) *Safety of machinery: experience feedback on automation accidents from the EPICA database.* W: Proceedings of 4th Conference on Safety of Industrial Automated Systems (SIAS 2005).

Chung K.H., Shewchuk J.P., Williges R.C. (1999) *An application of augmented reality to thickness inspection.* Human Factors and Ergonomics in Manufacturing, 9(4), s. 331-342.

Chung K.H., Shewchuk J.P., Williges R.C. (2002) *An analysis Framework for Applying Virtual Enviroment Technology to Manufacturing Tasks.* Human Factors and Ergonomics in Manufacturing, vol. 12(4), s. 335-348.

Cohn T.E. (1996) *Engineered Visibility Warning Signals: Tests of Time to React, Detectability, Identifiability and Salience.* IDEA Program Transportation Research Board, National Research Council [praca niepublikowana].

Colombo S., Biardi G., De Michela M. (2006) *The systematic integration of Human & Organisational Factors into safety analyses: An integrated engineering approach.* W: Safety and Reliability for Managing Risk. Red. C. Guedes Soares, E. Zio. London, Taylor & Francis Group, s. 293-308.

Dangelmaier W., Fischer M., Gausemeier J. *et al.* (2005) *Virtual and augmented reality support for discrete manufacturing system simulation.* Computers in Industry, 56(4) s. 371-383.

Dekker S.W.A. (2003) *Accidents are normal and human error does not exist: a new look at the creation of occupational safety.* International Journal of Occupational Safety and Ergonomics, vol. 9, no. 2, s. 211-218.

Duffy V.G., Wu F.F, Parry P.W. Ng (2003) *Development of an Internet virtual layout system for improving workplace safety.* Computers in Industry, 50, s. 207-230.

Dybała B., Dźwiarek M., Będza T., Jankowski, J. (2011) *Wirtualny model systemu wytwórczego do analizy stref zagrożenia i wspomagania doboru systemów ochronnych.* Zeszyty Naukowe Politechniki Poznańskiej. Budowa maszyn i zarządzanie produkcją, nr 1(15), s. 47-54.

Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE (przekształcenie). DzUrz UE, 9.6.2006, L 157/24.

Dyrektywa Parlamentu Europejskiego i Rady 2009/104/WE z dnia 16 września 2009 r. dotycząca minimalnych wymagań w dziedzinie bezpieczeństwa i higieny użytkowania sprzętu roboczego przez pracowników podczas pracy (druga dyrektywa szczegółowa w rozumieniu art. 16 ust. 1 dyrektywy 89/391/EWG). DzUrz UE, 3.10.2009, L 260/5.

Dźwiarek M. (1996) *Opracowanie metodyki i stanowisk do badania programowalnych sterowników maszyn.* PBZ-1 „Bezpieczeństwo i ochrona zdrowia człowieka w środowisku pracy" zad. III.14.2. Raport CIOP. Warszawa, CIOP-PIB.

Dźwiarek M. (1999) *Zasady stosowania urządzeń ochronnych według wymagań polskich i europejskich.* Pomiary, Automatyka, Robotyka, 11/1999, s. 36-37.

Dźwiarek M. (2000a) *Advanced Technology in Safety Related Control Systems of Machinery.* In: Ergonomics and Safety for Global Business Quality and Productivity. Red. D. Podgórski & W. Karwowski. Warszawa, Central Institute for Labour Protection, s. 475-478.

Dźwiarek M. (2000b) *Application of Complex Electronics in Machinery Control Systems.* W: Proceedings of the 7th International Conference on Human Aspects of Advanced Manufacturing: Agility & Hybrid Automation. Red. T. Marek & W. Karwowski. Kraków, Institute of Management, Jagiellonian Univerisity, s. 341-344.

Dźwiarek M. (2000c) *Opracowanie zasad i metod określania poziomu nienaruszalności bezpieczeństwa dla programowalnych systemów sterowania maszyn. Opracowanie metod sprawdzania poziomu nienaruszalności bezpieczeństwa programowalnych systemów sterowania maszyn.* SPR-1 zad. 03.7.14. Raport CIOP-PIB. Warszawa, CIOP-PIB.

Dźwiarek M. (2003) *Procedures for functional safety assessment of programmable control systems of machinery.* W: Safety and Reliability International Conference, Gdynia, 27-30 maja 2003. Materiały konferencyjne, t. 2, s. 13-20.

Dźwiarek M. (2004a) *An analysis of Accident Caused by Improper Functioning of Machine Control Systems.* International Journal of Occupational Safety and Ergonomics, vol. 10, no. 2, s. 129-136.

Dźwiarek M. (2004b) *Koncepcja bezpieczeństwa funkcjonalnego, norma PN EN 61508.* W: Bezpieczeństwo Funkcjonalne Elektrycznych, Elektronicznych i Elektronicznych Programowalnych Systemów Sterowania Związanych z Bezpieczeństwem. Zasady Podstawowe, Metodologia. Red. M. Dźwiarek. Warszawa, CIOP-PIB.

Dźwiarek M. (2004c) *Bezpieczeństwo funkcjonalne w cyklu życia systemu.* W: Bezpieczeństwo Funkcjonalne Elektrycznych, Elektronicznych i Elektronicznych Programowalnych Systemów Sterowania Związanych z Bezpieczeństwem. Zasady Podstawowe, Metodologia. Red. M. Dźwiarek. Warszawa, CIOP-PIB.

Dźwiarek M. (2004d) *Aspekty prawne i sektorowe dokumenty normatywne.* W: Bezpieczeństwo Funkcjonalne Elektrycznych, Elektronicznych i Elektronicznych Programowalnych Systemów Sterowania Związanych z Bezpieczeństwem. Zasady Podstawowe, Metodologia. Red. M. Dźwiarek. Warszawa, CIOP-PIB.

Dźwiarek M. (2006) *Documenting functional safety as a part of conformity documentation according to Machinery Directive.* W: Production Engineering Knowledge – Vision – Framework Programmes. Red. E. Chlebus. Oficyna Wydawnicza Politechniki Wrocławskiej, s. 141-147.

Dźwiarek M. (2007) *Functional safety of machinery control systems – general consideration.* W: Functional Safety Management in Critical Systems. Red. K.T. Kosmowski. Fundacja Rozwoju Uniwersytetu Gdańskiego, s. 101-114.

Dźwiarek M. (2008a) *Komputerowe narzędzia wspomagające prowadzenie i dokumentowanie oceny ryzyka przy projektowaniu maszyn.* W: Bezpieczeństwo przemysłowe. T. 1. Red. W. Sobczykiewicz, M. Urbaniak, s. 49-54.

Dźwiarek M. (2008b) *Opracowanie szacunkowej metody określania prawdopodobieństwa utraty funkcji bezpieczeństwa przez systemy sterowania maszynami.* Program wieloletni „Poprawa bezpieczeństwa i warunków pracy" etap I, zadanie 3.S.06. Raport CIOP-PIB. Warszawa, CIOP-PIB.

Dźwiarek M. (2008c) *Supporting tools for risk assessment during the machine design process.* Journal of KONBIN, no. 3(6), s. 199-212.

Dźwiarek M. (2010) *Case study of conformity assessment of automated production line.* Journal of KONBIN, no. 1(13), s. 149-164.

Dźwiarek M., Dybała B., Jankowski J., Będza T. (2010a) *Metoda wirtualnego modelowania stref zagrożenia do wspomagania doboru systemów ochronnych na etapie projektowania maszyn i systemów wytwórczych.* Mechanik nr 7, s. 501-508.

Dźwiarek M., Dybała B., Jankowski J., Będza T., Strawiński T., Poznar T. (2010b) *Opracowanie metody wirtualnego modelowania stref zagrożenia do wspomagania doboru systemów ochronnych na etapie projektowania maszyn i systemów wytwórczych.* Raport CIOP-PIB. Warszawa, CIOP-PIB.

Dźwiarek M., Holejko K., Nowak, R. (2003) *Augmented Reality – a new kind of hazardous situation indicator.* W: Proceedings of International Conference Safety of Industrial Automated Systems. Nancy, 13-15 października 2003, s. 3-41 ÷ 3-45.

Dźwiarek M., Holejko K., Nowak R., Czarnecki T. (2004) *A system for signalling of emergency situation based on the augmented reality concept.* W: Human & Organisational Issues in the Digital Enterprise. Red. E.F. Fallon. The Department of Industrial Engineering, National University of Ireland, s. 479-488.

Dźwiarek M., Hryniewicz O. (2011) *Periodical inspection frequency of safety related control systems of machinery – practical recommendations for the determination.* W: Advances in Safety, Reliability and Risk Management. Red. Berenguer, Grall & Guedes Soares. London, Taylor & Francis Group, s. 495-502.

Dźwiarek M., Kosmowski K.T. (2007) *General concept of functional safety – standardisation and sector aspects*. W: Functional Safety Management in Critical Systems. Red. K.T. Kosmowski. Fundacja Rozwoju Uniwersytetu Gdańskiego, s. 81-100.

Dźwiarek M., Łuczak A. (2008) *Application Prospects of the Augmented Reality Technology for Improving Safety of Machine Operators.* In: Human – Computer Interaction. New Developments. Red. K. Asai. Vienna, In-Tech, s. 217-230.

Dźwiarek M., Łuczak A., Strawiński T. (2007a) *Badania percepcji wizualnych sygnałów ostrzegawczych generowanych metodą rzeczywistości wzbogaconej celem ich optymalizacji.* Raport końcowy. Raport CIOP-PIB. Warszawa, CIOP-PIB.

Dźwiarek M., Saulewicz, A. Kalwasiński, D. (2007b) *Investigation of Appropriateness of the VE for Training Purposes Using Fork-Lift VR Simulator.* W: Proceedings of HCI International 2007, 22-27 July 2007, Beijing, China, Springer, s. 815-819.

Dźwiarek M., Strawiński T. (2008) *Zapewnianie bezpieczeństwa użytkowania maszyn metodami sterowania.* Warszawa, CIOP-PIB 2008.

Edwards R. (2001) *Experience gained from accidents associated with complex electronic technology*. W: Proceedings of 2nd Conference on Safety of Industrial Automated Systems, November 13-15, 2001, Bonn, Germany, s. 39-44.

Foster P., Burton A. (2003) *Virtual reality in improving mining ergonomics.* Journal of South African Institute of Mining and Metallurgy, March 2004, s. 128-133.

Gallagher A.vG., Cates C. (2004) *Virtual reality training for the operating room and cardiac catheterisation laboratory.* The Lancet, vol. 364, issue 9444, October, s. 1538-1540.

Gould J. (2000) *Offshore accidents rates for April 1996 to March 1998.* Health and Safety Executive Report OTO 2000 012.

Grabowski A., Kosiński R., Dźwiarek M. (2010) V*ision safety system based on cellular neural networks.* Machine Vision and Applications, vol. 22, no. 3, s. 581-590.

Gros B.L., Greenhouse D.S., Cohn T.E. (2005) *Visual warning signals optimized for human perception: What the eye sees fastest.* Applied Bionics and Biomechanics, vol. 2(1), s. 45-52.

Haas E.C., Casali J.G. (1995) *Perceived urgency of response time to multi-tone and frequency-modular warning signals in broadband noise.* Ergonomics, vol. 38, no. 11, s. 2313-2326.

Hagele M., Helms E., Schaaf W. (2002) *Robot assistants at manual workplaces: effective co-operation and safety aspects.* W: Proceedings of the 33rd ISR (International Symposium of Robotics), 7-11 October [CD-ROM].

Haiyan Xie M., Tudoreanu E., Shi W. (2006) *Development of a Virtual Reality Safety-Training System for Construction Workers.* W: 6th International Conference on Construction Applications of Virtual Reality, 3-4 August 2006, Orlando, Florida, USA.

Hale AR., Hale M. (1971) *A Review of Industrial Accident Research.* London, Her Majesty's Safety Office.

Harms-Ringdahl L. (1993) *Safety Analysis. Principles and practice in occupational safety.* London, Elsevier.

Henderson J., Whittington C., Wright K. (2000) *Accident investigation – The drivers, methods and outcomes*. HSE Research Report 344/2001.

Heinrich H.W. (1959) *Industrial Accidents Prevention.* New York, Toronto, London, McGraw-Hill Book Company, Inc.

Hryniewicz O., Lewin W. (2008) *Przegląd metod oceny probabilistycznej systemów przemysłowych przy ograniczonych danych niezawodnościowych pod kątem odpowiedniości do oceny systemów sterowania maszynami wraz z określeniem metody prowadzenia analizy.* Raport Instytutu Badań Systemowych PAN. Warszawa, Instytut Badań Systemowych PAN.

Huelke M., Nickel P., Lungfiel A., Nischalke-Fehn Schaefer M. (2010) *Cave automatic virtual environments for research into occupational safety and health – Practical recommendations and solutions for the construction.* W: International Conference Safety of Industrial Automated Systems, Tampere, Finlandia, 14-15 June 2010.

Indirli M. (2007) *Overview on Risk Assessment Approaches for Natural Hazards*. Cost Action C26 – Urban Habitat Constructions Under Catastrophic Events, Praha, March 30-31, 2007.

Kalbfleisch J.D., Prentice R.L. (1980) *The Statistical Analysis of Failure Time Data.* New York, John Wiley.

Kim H., Gong I. (2008) *Building Geographic Database for Maritime Traffic Safety Assessment.* W: Proceedings of Tenth International Conference for Spatial Data Infrastructure GSDI-10, St. Augustine, Trinidad February 25-29, 2008.

Kim JW., Park J., Jung W. (2005) *A systematic approach to analysing errors of commission from diagnosis failure in accident progression.* Reliability Engineering & System Safety, 89(2) s. 137-150.

Koornneef F., A. Hale (1995) *Organisational Feedback from Accidents at Work.* W: Proceedings of 13th Int. NeTWork Workshop (TU Delft), 11-13 maj 1995, Bad Hamburg, Germany.

Kosmowski K.T. (2006) *Functional safety concept for hazardous systems and new challenges*. Journal of Loss Prevention in the Process Industries, vol. 19, s. 298-305.

Kosslyn S.M., Rosenberg R.S. (2006) *Psychologia. Mózg. Człowiek.* Kraków, Wydawnictwo Znak.

Kyung H.C, John P.S., Robert C.W. (2002) *An analysis Framework for Applying Virtual Environment Technology to Manufacturing Tasks*. Human Factors and Ergonomics in Manufacturing, vol. 12 (4), s. 335-348.

Lawless J.F. (2003) *Statistical Models and Methods for Lifetime data.* 2nd ed. New York, John Wiley.

Lebecki K., Rosmus P. (2007a) *Analityczna metoda oceny bezpieczeństwa funkcjonalnego procesów produkcyjnych w górnictwie węgla kamiennego.* Bezpieczeństwo Pracy i Ochrona Środowiska w Górnictwie, 9(157)/II.

Lebecki K., Rosmus P. (2007b) *Ilościowa ocena ryzyka dla zagrożeń naturalnych w górnictwie w oparciu o metodologię norm serii PN EN 61508.* Bezpieczeństwo Pracy i Ochrona Środowiska w Górnictwie, 8(156).

Liu C., Uang S. (2007) *Design Implications of Simultaneous Contrast Effects Under Different Viewing Conditions*. Lecture Notes of Computer Science, vol. 4554, s. 805-811.

Malm T. (2001) *Safety aspects in automation of paper roll handling.* W: Proceedings of 2nd Conference on Safety of Industrial Automated Systems, 13-15 November, Bonn, Germany, 51-8.

Markowski A. (2006) *Layer of Protection Analysis for the Process Industry.* Łodź, Polska Akademia Nauk, Oddział w Łodzi, Komisja Ochrony Środowiska.

MaTSU (2000). *Employers incident analysis 1991-1998.* Health and Safety Executive Report OTO 2000 002.

Maruszewski T. (2001) *Psychologia poznania. Sposoby rozumienia siebie i świata.* Warszawa, GWP.

Michalak D., Rosmus M., Jaszczyk Ł. (2009) *Możliwości zastosowania technologii Augmented Reality i RFID w szkoleniach pracowników transportu.* W: Materiały na konferencję: Bezpieczeństwo pracy urządzeń transportowych w górnictwie, V Międzynarodowa Konferencja, Ustroń, 4-6 listopada 2009.

Michalak D., Winkler T., Jaszczyk Ł. (2010) *Zastosowanie technologii Augmented Reality oraz RFID w szkoleniach operatorów maszyn.* Materiały na konferencję: XIV Międzynarodowa Szkoła Komputerowego Wspomagania Projektowania, Wytwarzania i Eksploatacji, Jurata, 10-14 maja 2010. Mechanik 2010, nr 7, s. 297-304.

Missala T. (1997) *Bezpieczeństwo funkcjonalne urządzeń automatyki i robotyki.* Pomiary, Automatyka, Robotyka, nr 3.

Missala T. (2010) *Bezpieczeństwo funkcjonalne zintegrowanego systemu wytwarzania.* Prace Naukowe Politechniki Warszawskiej. Elektronika, z. 175, t. 1, s. 275-284.

Mól A.C.A., Jorgea C.A.F., Coutob P.M., Augustoa S.C., Cunhac G.G., Landau L. (2008) *Virtual environments simulation for dose assessment in nuclear plants.* Progress in Nuclear Energy, vol. 51, issue 2, s. 382-387.

Mujber T.S., Szecsi T., Hashmi M.S.J. (2004) *Virtual reality applications in manufacturing process simulation.* Journal of Materials Processing Technology s. 155-156, 1834-1838.

Nickel P., Lungfiel A., Nischalke-Fehn G., Pappachan P., Huelke M., Schaefer M. (2010) *Evaluation of Virtual Reality for Usability Studies in Occupational Safety and Health.* International Conference Safety of Industrial Automated Systems, Tampere, Finlandia, 14-15 czerwiec 2010.

Niewieczerzał P. (2006) *Virtual design of robotized production cells.* W: Virtual Design and Automation. Red. Z. Weiss. Poznań, Publishing House of Poznań University of Technology.

Nivolianitou Z., Aneziris O.N., Nasios K. (2006) *Virtual Reality applications for improving safety in the process industry.* W: Safety and Reliability for Managing Risk. Red. Guedes Soares & Zio. London, Taylor & Francis Group.

Oehme O., Bruns I. (2003) *Ergonomic Requirements and Value Analysis of Augmented Reality Head Mounted Display for Production and Service.* W: Human Factors in Organizational Design and Management – VII. Santa Monica, CA, USA, IEA Press, s. 477-482.

Papastavrou J.D., Lehto M.R. (1995) *A distributed signal detection theory model: implication for the design of warnigs.* International Journal of Occupational Safety and Ergonomics, vol. 1, no. 3, s. 215-234.

Pawlak A., Wolska A. (2005a) *Badanie warunków pracy wzrokowej na stanowisku sortowacz opakowań szklanych oraz operator automatu szklarskiego.* Prace pozaplanowe CIOP-PIB. Warszawa, CIOP-PIB [praca niepublikowana].

Pawlak A., Wolska A. (2005b) *Ekspertyza warunków pracy na 6 wybranych stanowiskach pracy w ABB, Łódź.* Prace pozaplanowe CIOP-PIB. Warszawa, CIOP-PIB [praca niepublikowana].

Pawlak A., Wolska A. (2006) *Ocena warunków oświetleniowych na stanowisku kontroli jakości w POLAR S.A. we Wrocławiu.* Prace pozaplanowe CIOP-PIB. Warszawa, CIOP-PIB [praca niepublikowana].

Shingledecker C.A. (1984) *A task battery for applied human performance assessment research.* Technical Report AFAMRL-TR-84-071. Air Force Aerospace Medical Research Laboratory, Wright-Patterson Air Force Base, USA [praca niepublikowana].

Sillamy N. (1989) *Słownik psychologii.* Katowice, Wydawnictwo „Książnica".

Steed A., Parker C. (2005) *Evaluating Effectiveness of Interaction Techniques across Immersive Virtual Environmental Systems.* Presence, vol. 14, no. 5, s. 511-527.

Strelau J. (1985) *Temperament, osobowość, działanie*. Warszawa, PWN.

Strelau J. (1996) *Temperament a stres: temperament jako czynnik moderujący stresory, stan i skutki stresu oraz radzenie sobie ze stresem.* W: Człowiek w sytuacji stresu. Red. J. Heszen-Niejodek i Z. Ratajczak. Katowice, Wydawnictwo Uniwersytetu Śląskiego, s. 88-130.

Studenski R. (1986) *Teorie przyczynowości wypadkowej i ich empiryczna weryfikacja.* Seria: Prace Głównego Instytutu Górnictwa. Katowice, Główny Instytut Górnictwa.

STSARCES (2000) *Safety-Related Complex Electronic Systems.* Final report. Coordinator: INERIS, Partners: BIA, HSE, INRS, VTT, CETIM, INSHT – CNVM, SP, TÜV, SICK AG, JAY Electronique. European Commission – DG XII.

Tomaszewski T. (1976) *Procesy spostrzegania.* W: Psychologia. Red. T. Tomaszewski. Warszawa, PWN, s. 226-246.

Weidenhausen J., Knoepfle C., Stricker D. (2003) L*essons learned on the way to industrial augmented reality applications, a retrospective on ARVIKA.* Computers & Graphics, 27(6) s. 887-891.

Winkler T. (2003) *Element wirtualnego prototypowania maszyn górniczych.* W: Materiały na konferencję: KOMTECH „Nowoczesne, niezawodne i bezpieczne systemy mechaniczne w świetle wymagań Unii Europejskiej", Szczyrk, 17-19 listopada, s. 71-81.

Winkler T., Michalak D., Salem W., Määtä T., Colombo S. (2005a) *Technologia wirtualnej rzeczywistości w cyklu życia środków technicznych możliwość transferu metod w obszarze przemysłów wysokiego ryzyka.* W: Materiały na konferencję: KOMTECH 2005 „Systemy ograniczające zagrożenia w procesach eksploatacji maszyn i urządzeń", t. 1, Zakopane 15-17.11.2005, s. 207-222.

Winkler T., Michalak D., Bojara S., Jaszczyk Ł. (2005b) *Zastosowanie technik wirtualnych w rekonstrukcji przebiegu wypadków w górnictwie.* W: Materiały na konferencję: KOMTECH 2005 „Systemy ograniczające zagrożenia w procesach eksploatacji maszyn i urządzeń", t. 2, Zakopane 15-17.11.2005, s. 107-112.

Winkler T., Michalak D., Jaszczyk Ł., Tokarczyk J. (2006) *Virtual prototyping of the mining machines servicing and repair processes.* W: Materiały na konferencję: Mine Planning and Equipment Selection 2006, The Fifteenth International Symposium, t.1, Torino, Italy, 20 22 September 2006, s. 502-507.

Winkler T., Michalak D., Jaszczyk Ł. (2009) *The use of visualization of risk factors in creation of work safety.* W: Proceedings of MPES 2009, Eighteenth International Symposium on Mine Planning & Equipment Selection, Banff, Alberta, Canada, November 16-19, 2009. Int. J. Min. Reclam. Environ., Special Issue, s. 834-842.

Wogalter M.S., Mayhorn C.B. (2005) *Providing cognitive support with technology--based warning systems.* Ergonomics, vol. 48, no 5, s. 522-533.

Zawadzki B., Strelau J. (1992) *Cechy temperamentu w ujęciu Regulacyjnej Teorii Temperamentu i ich pomiar metodą kwestionariuszową.* Warszawa, Uniwersytet Warszawski.

Zhang Rui-xin, YUa Dong-fang, LIa Xin-wang, YA Xin-gang, Liu Yu (2006) *Surface Mine System Simulation and Safety Risk Management*. Journal of China University of Mining and Technology, vol. 16(4), s. 413-415.

PN-EN 12464-1:2011 Światło i oświetlenie – Oświetlenie miejsc pracy – Część 1: Miejsca pracy we wnętrzach.

PN-EN 60204-1:2010 Bezpieczeństwo maszyn – Wyposażenie elektryczne maszyn – Część 1: Wymagania ogólne.

PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów – Procedura analizy rodzajów i skutków uszkodzeń (FMEA).

PN-EN 61496-1:2007/AC:2011 Bezpieczeństwo maszyn – Elektroczułe wyposażenie ochronne – Część 1: Wymagania ogólne i badania.

PN-EN 61025:2007 Analiza drzewa niezdatności (FTA).

PN-EN 61165:2006. Zastosowanie procesów Markowa.

PN-EN 61310-1:2009. Bezpieczeństwo maszyn – Wskazywanie, oznaczanie i sterowanie – Część 1: Wymagania dotyczące sygnałów wizualnych, akustycznych i dotykowych.

PN-EN 61508-1:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 1: Wymagania ogólne.

PN-EN 61508-2:2010 Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem.

PN-EN 61508-3:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 3: Wymagania dotyczące oprogramowania.

PN-EN 61508-4:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 4: Definicje i skrótowce.

PN-EN 61508-5:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa.

PN-EN 61508-6:2010 Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3.

PN-EN 61508-7:2010 Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 7: Przegląd technik i miar. Polski Komitet Normalizacyjny.

PN-EN 61511-1:2007 Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego – Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania.

PN-EN 61511-2:2008 Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego – Część 2: Wytyczne do stosowania IEC 61511-1.

PN-EN 61511-3:2009 Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego – Część 3: Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa.

PN-EN 61800-5-2:2007 Elektryczne układy napędowe mocy o regulowanej prędkości – Część 5-2: Wymagania dotyczące bezpieczeństwa – Funkcjonalne.

PN-EN 62061:2008. Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.

PN-EN 62061/AC:2011 Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.

PN-EN ISO 12100:2011 Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka.

PN-EN ISO 13855:2010 Bezpieczeństwo maszyn – Umiejscowienie wyposażenia ochronnego ze względu na prędkości zbliżania części ciała człowieka.

PN-EN ISO 13857:2010 Bezpieczeństwo maszyn – Odległości bezpieczeństwa uniemożliwiające sięganie kończynami górnymi i dolnymi do stref niebezpiecznych.

PN-EN ISO 13849-1:2008/AC:2009 Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania.

PN-ISO/IEC 2382-14:2001 Technika informatyczna – Terminologia – Część 14: Niezawodność, obsługiwalność i dostępność.

PN-IEC 61882:2005 Badania zagrożeń i zdolności do działania (badania HAZOP) – Przewodnik zastosowań.

IEC 61513:2001 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.

ISO FDIS 13849-2:2011 Safety of machinery – Safety-related parts of control systems – Part 2: Validation.