Redakcja pracy zbiorowej
Wojciech CHOLEWA - Politechnika Śląska
Kazimierz T. KOSMOWSKI - Politechnika Gdańska
Stanisław RADKOWSKI - Politechnika Warszawska

Modele systemów oceny ryzyka i diagnostyki technicznej

Gliwice 2008

Recenzenci
prof. dr hab. inż. Jan Kiciński - Instytut Maszyn Przepływowych PAN, Gdańsk
prof. dr hab. Wojciech Moczulski - Politechnika Śląska, Gliwice

Redaktor zeszytów
Wojciech Cholewa

Redaktorzy techniczni
Paweł Chrzanowski, Marek Wyleżoł

Projekt okładki
Wojciech Cholewa, Marek Wyleżoł

BibTeX
```
@BOOK{, title = {Modele systemów oceny ryzyka i diagnostyki technicznej},
publisher = {Politechnika Śląska, Katedra Podstaw Konstrukcji Maszyn}, year
= {2008}, editor = {Cholewa, W. and Kosmowski, K. T. and Radkowski, S.}, volume
= {138}, series = {Zeszyty}, address = {Gliwice} }
```

ISBN 978-83-60759-09-7

Wydawca
Katedra Podstaw Konstrukcji Maszyn
Wydział Mechaniczny Technologiczny
Politechnika Śląska
ul. Konarskiego 18a, 44-100 Gliwice
tel. (032) 237-14-67, fax (032) 237-13-60
`https://kpkm.polsl.pl`

Druk i oprawa (z dostarczonych materiałów):
Drukarnia cyfrowa D&D sp. z o.o. ul. Moniuszki 6, 44-100 Gliwice

Spis treści

1 Wstęp **5**
Bibliografia . . . 7

2 Modele procesów diagnostyki technicznej **9**
2.1 Wstęp . . . 9
2.2 Podstawowe schematy procesu diagnozowania . . . 10
2.3 Modele obiektów . . . 12
2.4 Modele diagnostyczne . . . 14
2.5 Relacje stosowane w diagnostyce maszyn . . . 15
2.6 Rodzaje modeli diagnostycznych . . . 19
2.7 Doskonalenie modeli . . . 25
2.8 Identyfikacja modeli diagnostycznych . . . 29
2.9 Proces diagnozowania . . . 31
Bibliografia . . . 33

3 Analiza niezawodności i bezpieczeństwa maszyn i instalacji **37**
3.1 Wprowadzenie . . . 37
3.2 Niezawodność i nieuszkadzalność obiektów technicznych . . . 40
3.3 Bezpieczeństwo i ryzyko związane z eksploatacją obiektów technicznych . . . 43
3.4 Ocena i sterowanie ryzykiem . . . 44
3.5 Bezpieczenstwo funkcjonalne systemów sterowania i zabezpieczeń . . . 47
3.6 Zmniejszanie ryzyka i wyznaczanie wymaganego SIL dla funkcji bezpieczeństwa . . . 49
3.7 Weryfikacja probabilistyczna SIL dla funkcji bezpieczeństwa . . . 51
3.8 Wymagania dla podsystemów i zgrubna ocena jakościowa systemu E/E/PE . . . 55
Bibliografia . . . 57

4 Akceptowalność i niepewność w analizie i ocenie ryzyka **59**
4.1 Kryteria akceptowalności ryzyka . . . 59
4.2 Modelowanie niepewności . . . 63
Bibliografia . . . 69

5 Diagnostyka weryfikacyjna podsystemów i urządzeń **71**
5.1 Zakres diagnostyki weryfikacyjnej . . . 71
5.2 Diagnostyka w okresie projektowania . . . 74
5.3 Diagnostyka w okresie produkcji . . . 74
5.4 Diagnostyka w okresie eksploatacji . . . 75
5.5 Diagnostyka w okresie remontu . . . 76
5.6 Diagnostyka w okresie likwidacji . . . 76
5.7 Sformułowanie zadań diagnostyki weryfikacyjnej . . . 76
5.8 Wybrane metody diagnostyki weryfikacyjnej . . . 78
5.9 Parametry diagnostyczne . . . 79

5.10 Pomiary parametrów diagnostycznych . . . 80
5.11 Określanie stanu technicznego urządzeń i instalacji krytycznych . . . 81
Bibliografia . . . 84

6 Modelowanie bezpieczeństwa maszyn i instalacji krytycznych 85
6.1 Bezpieczeństwo maszyn i kategorie systemów sterowania . . . 85
6.2 Redukowanie ryzyka eksploatacji maszyn zorientowane na system sterowania . . . 88
6.3 Modelowanie bezpieczeństwa instalacji krytycznych . . . 93
6.4 Wpływ czynników ludzkich i organizacyjnych na bezpieczeństwo obiektu krytycznego 96
6.5 Problemy modelowania bezpieczeństwa rzeczywistych obiektów złożonych . . . 98
Bibliografia . . . 100

7 Eksperyment diagnostyczny jako źródło informacji aposteriorycznej 103
Bibliografia . . . 113

8 Wykorzystanie informacji diagnostycznej w analizie ryzyka technicznego 115
8.1 Wprowadzenie . . . 115
8.2 Metody eksploatacji zorientowane na bezpieczeństwo . . . 115
8.3 Wykorzystanie metody Bayesa . . . 119
8.4 Przykład wykorzystania metody prawdopodobieństwa subiektywnego w procesie podejmowania decyzji . . . 120
8.5 Przykład wykorzystania sieci bayesowskich . . . 125
Bibliografia . . . 128

9 Modele symulacyjne rozwoju procesów degradacyjnych i zmęczeniowych na przykładzie przekładni zębatej 129
9.1 Wprowadzenie . . . 129
9.2 Założenia ogólne o modelowaniu obiektu technicznego . . . 129
9.3 Modelowanie stanów dynamicznych przekładni zębatej . . . 131
9.4 Modelowanie oddziaływań międzyzębnych . . . 133
9.5 Symulacja procesów zmęczeniowych i degradacyjnych w eksploatacji przekładni zębatej 137
9.6 Podsumowanie . . . 152
Bibliografia . . . 152

10 Przykłady zastosowań 153
10.1 Przykładowe funkcje systemów sterowania i zabezpieczeń turbozespołu . . . 153
10.2 Konstruowanie przykładowych sieci stwierdzeń dla celów diagnostycznych . . . 159
Bibliografia . . . 165

11 Zarządzanie bezpieczeństwem w złożonych obiektach i instalacjach krytycznych 167
11.1 Metody wspomagające zarządzanie bezpieczeństwem . . . 167
11.2 Zarządzanie bezpieczeństwem w cyklu życia . . . 171
11.3 Wnioski końcowe . . . 174
Bibliografia . . . 177

Rozdział 1

Wstęp

Wojciech CHOLEWA, Kazimierz T. KOSMOWSKI, Stanisław RADKOWSKI

Kilka ostatnich dekad było związanych z intensywnym rozwojem metod badań diagnostycznych maszyn i urządzeń. Celem tych badań jest rozpoznawanie stanu obiektu na podstawie dostępnych wyników obserwacji działania tego obiektu i obserwacji oddziaływań występujących pomiędzy obiektem i jego otoczeniem. Szczególny rozwój zaobserwowano w zakresie diagnostyki wibroakustycznej. Rozwinięte zostały metody prognozowania zmian stanu technicznego. Odpowiednia jakość stawianych diagnoz stanowiła podstawę do postulowania zmian w strategiach zarządzania środkami technicznymi, wymagającymi przeprowadzania obsług profilaktycznych i remontów.

Stosowane początkowo metody planowania prac remontowych, charakteryzujące się stałymi, z góry ustalonymi i zalecanymi przez producentów okresami eksploatacji pomiędzy kolejnymi remontami, zaczęto zastępować metodami ustalania terminów remontów na podstawie aktualnego stanu obiektu. Postępowanie takie prowadziło ogólnie do wydłużenia okresów międzyremontowych i wynikającego stąd zmniejszenia kosztów prac remontowych. Wadą takiego postępowania była konieczność subiektywnego ustalania stopni ważności rozpoznawanych stanów oraz konieczność arbitralnego wskazywania stanów krytycznych.

Znaczącym postępem w sposobach zarządzania środkami technicznymi, stymulowanym między innymi potrzebami przemysłu chemicznego oraz energetyki jądrowej, było zaproponowanie działań bazujących na kryteriach związanych z minimalizowaniem ryzyka (na przykład strat ekonomicznych), definiowanego w uproszczeniu następująco

$$R = \sum\nolimits_i (P_i * K_i) \tag{1.1}$$

gdzie

- i identyfikator (indeks) uszkodzenia obiektu lub innego zdarzenia stanowiącego przyczynę zagrożenia zdrowia, życia, środowiska, bezpieczeństwa technicznego lub strat ekonomicznych,
- P_i prawdopodobieństwo wystąpienia i-tego uszkodzenia (zdarzenia),
- K_i koszty (straty) związane z oczekiwanymi skutkami wystąpienia i-tego uszkodzenia (zdarzenia).

Należy zwrócić uwagę, że straty K_i określane są w odniesieniu do skutków i-tego uszkodzenia, a nie do samego uszkodzenia. W celu określenia takich strat niezbędne jest budowanie scenariuszy rozwoju zdarzeń po wystąpieniu rozpatrywanych uszkodzeń.

Prawdopodobieństwa P_i występujące w zależności (1.1) przyjmowane są zwykle jako wartości stałe dla rozpatrywanego obiektu i zależą od jego budowy oraz istoty działania. Pozwalają one na wyznaczanie statycznego ryzyka R. Ponieważ wiadomo, że prawdopodobieństwo wystąpienia stanu

krytycznego jest zależne od aktualnego stanu technicznego obiektu, prawdopodobieństwo to może być rozpatrywane jako zależne od czasu $P_i(t)$, prowadząc do ryzyka dynamicznego

$$R(t) = \sum\nolimits_i (P_i(t) * K_i) \tag{1.2}$$

Zmiany mogą występować również w otoczeniu obiektu (inne obiekty i instalacje, substancje niebezpieczne, populacja wokół obiektu itp.), co stwarza potrzebę rozpatrywania zmiennych kosztów $K_i(t)$ podczas wyznaczania ryzyka dynamicznego

$$R(t) = \sum\nolimits_i (P_i(t) * K_i(t)) \tag{1.3}$$

Wyznaczanie ryzyka dynamicznego $R(t)$ wymaga identyfikacji aktualnego stanu technicznego, którą można przeprowadzić stosując metody diagnostyki technicznej, uwzględniając zmiany techniczne i organizacyjne w złożonym obiekcie antropotechnicznym w czasie, a także ewentualne zakłócenia i zmieniające się warunki otoczenia.

W niniejszej monografii podjęto próbę przedstawienia wybranych zagadnień dotyczących procesów diagnozowania oraz procesów oceniania ryzyka dla obiektów technicznych. Zamiarem autorów było zebranie wyników przeprowadzonych badań i zwrócenie uwagi na potrzebę i możliwości łącznego rozpatrywania tych procesów, w celu umożliwienia ich adaptacyjnego doskonalenia.

Procesy diagnostyki technicznej, pozwalają na ocenianie aktualnego stanu obiektu. Powinny one stanowić fragmenty działań zmierzających do określania ryzyka. Modele tych procesów opisano w rozdziale 2. W rozdziale tym pokazano również różne rodzaje modeli diagnostycznych stosowanych w procesach diagnozowania.

W rozdziale 3 omówiono główne pojęcia związane z analizą niezawodności i bezpieczeństwa maszyn i instalacji. Szczególną uwagę zwrócono na możliwości sterowania ryzykiem oraz zagadnienia związane z bezpieczeństwem funkcjonalnym systemów sterowania i zabezpieczeń. Wybrane zagadnienia dotyczące kryteriów akceptowalności ryzyka oraz modelowania niepewności w analizie ryzyka opisano w rozdziale 4. Zwrócono uwagę na typy rozróżnianych niepewności.

Podstawowym zadaniem diagnostyki technicznej jest ocenianie aktualnego stanu technicznego oraz prognozowanie jego zmian. Szczególnym zastosowaniem diagnostyki są badania weryfikacyjne, których celem jest sprawdzenie czy stan obiektu należy do określonej klasy stanów. Diagnostykę weryfikacyjną omówiono w rozdziale 5, rozpatrując jej rolę w kolejnych fazach istnienia środka technicznego, od projektowania przez wytwarzanie i eksploatację aż do remontów i utylizacji.

Wyodrębnionym zagadnieniem, omówionym w rozdziale 6, jest bezpieczeństwo maszyn i instalacji krytycznych oraz możliwości redukowania ryzyka eksploatacyjnego. Zwrócono również uwagę, iż w zadaniach szacowania ryzyka szczególnie ważnym jest opracowanie metod wykorzystania informacji aposteriorycznej, będącej wynikiem obserwacji lub eksperymentu diagnostycznego. Wybrane zagadnienia z tego obszaru przedstawiono w rozdziale 7 i rozdziale 8.

Dane niezbędne do szacowania ryzyka mogą być pozyskiwane również z eksperymentów symulacyjnych, realizowanych z zastosowaniem odpowiednio przygotowanych modeli. W rozdziale 9 pokazano przykład modelu przekładni zębatej, umożliwiającego symulowanie, wynikających z eksploatacji, procesów pojawiania się i rozwoju pittingu oraz osłabienia w stopie zęba.

W rozdziale 10 zamieszczono przykład dotyczący zaworu szybkozamykającego turbiny, ilustrujący sposób pozyskiwania wiedzy diagnostycznej i jej zapisywanie w szkieletowym systemie doradczym DIADYN [1.1], w którym wiedza reprezentowana jest w postaci sieci stwierdzeń.

Monografię kończy rozdział 11, zawierający przegląd wybranych metod wspomagających zarządzanie bezpieczeństwem w złożonych obiektach i instalacjach krytycznych. Podkreślono w nim, między innymi, znaczenie projektu RIMAP (*Risk Based Inspection and Maintenance Procedures for European Industries*), którego wynikiem są wytyczne dotyczące zarządzania środkami technicznymi, bazującego na ryzyku.

Monografia opisuje fragment wyników badań prowadzonych w ramach projektu PBZ-KBN-105/T10/2003 pt. *„Zintegrowany, dynamiczny system oceny ryzyka, diagnostyki oraz sterowania dla obiektów i procesów technicznych"* realizowanego przez liczną grupę zespołów badawczych, pod kierunkiem prof. dra hab. inż. Jana Kicińskiego.

Bibliografia

[1.1] Cholewa W., redaktor. *Szkieletowy system doradczy DIADYN*, wolumen 137 serii *Zeszyty*. Politechnika Śląska, Katedra Podstaw Konstrukcji Maszyn, Gliwice, 2008.

Rozdział 2

Modele procesów diagnostyki technicznej

Krzysztof PSIUK, Sebastian RZYDZIK

2.1. Wstęp

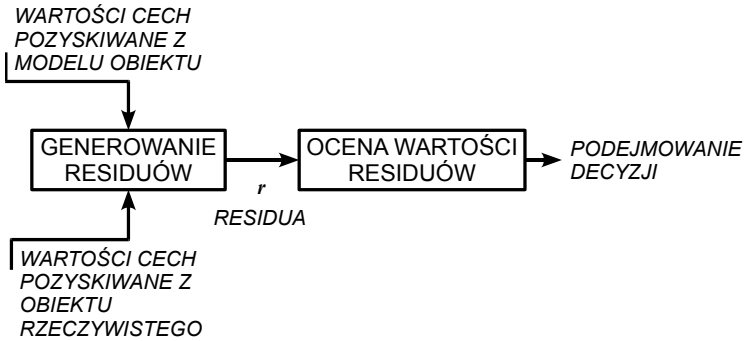
Proces diagnozowania obiektów technicznych (urządzeń technicznych i procesów przemysłowych) można zrealizować na dwa sposoby:

1. Metodami opartymi na analizie symptomów, tzw. **diagnostyka symptomowa**.
2. Metodami stosującymi modele obiektów poddawanych diagnostyce, tzw. **diagnostyka wsparta modelowo**.

W przypadku diagnostyki symptomowej przeprowadza się proces wnioskowania diagnostycznego polegający na poszukiwaniu nieznanych wartości stanów technicznych (w szczególności niezdatności) na podstawie znanych wartości parametrów diagnostycznych (symptomów):

$$S \Rightarrow Z \tag{2.1}$$

gdzie S jest symptomem stanu technicznego Z.



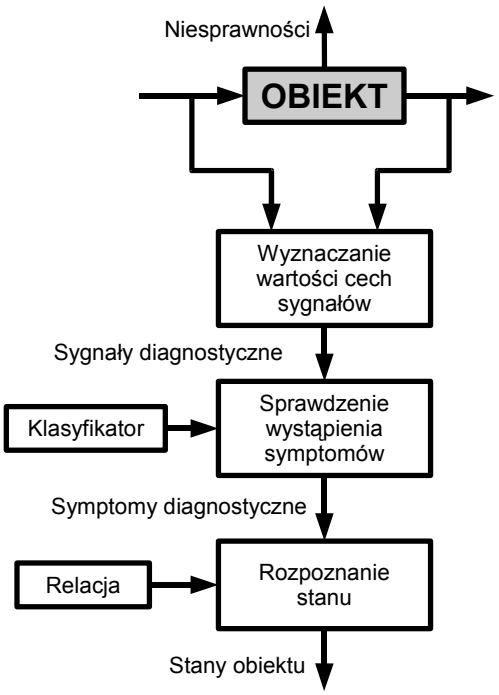
Rys. 2.1: Schemat procesu generowania residuum

W przypadku diagnostyki wspartej modelowo zakłada się, że dysponujemy modelem obiektu technicznego. Zwykle rozpatruje się model matematyczny obiektu. Model może reprezentować poprawną pracę obiektu lub reprezentować pracę tego obiektu w przypadku wystąpienia pewnej niesprawności. Diagnozowanie stanu technicznego polega na porównywaniu ze sobą wybranych wielkości (wartości

cech) pozyskiwanych z modelu obiektu i obiektu rzeczywistego (rys. 2.1). Na podstawie tego porównania wyznaczane są tzw. *residua* [2.27, 2.19], które mogą nas informować m.in. o pojawieniu się niesprawności w diagnozowanym obiekcie technicznym.

2.2. Podstawowe schematy procesu diagnozowania

Jak już powiedziano we wstępie, w przypadku diagnostyki symptomowej, stan danej maszyny określany jest na podstawie objawów tego stanu, które nazywane są symptomami stanu technicznego. Można tutaj przytoczyć porównanie z diagnostyką medyczną, w której stan pacjenta lekarz ocenia na podstawie zaobserwowanych objawów, którą może być np. podwyższona temperatura ciała pacjenta. W przypadku diagnostyki maszyn, obiektami badań są maszyny i urządzenia lub zachodzące w nich procesy, a objawami symptomy stanu technicznego. Na rys. 2.2 przedstawiono ogólny schemat procesu wnioskowania stosowany w diagnostyce symptomowej.



Rys. 2.2: Schemat procesu wnioskowania stosowany w diagnostyce symptomowej (opracowano na podstawie [2.48, 2.30])

Na przedstawionym schemacie pokazano, że na podstawie sygnałów wejścia i wyjścia z obserwowanego obiektu wyznaczane są wartości cech sygnałów diagnostycznych. Wyznaczone wartości cech sygnałów diagnostycznych są następnie klasyfikowane do określonej klasy stanów. W kolejnym kroku, na podstawie przeprowadzonej klasyfikacji określa się stan obiektu.

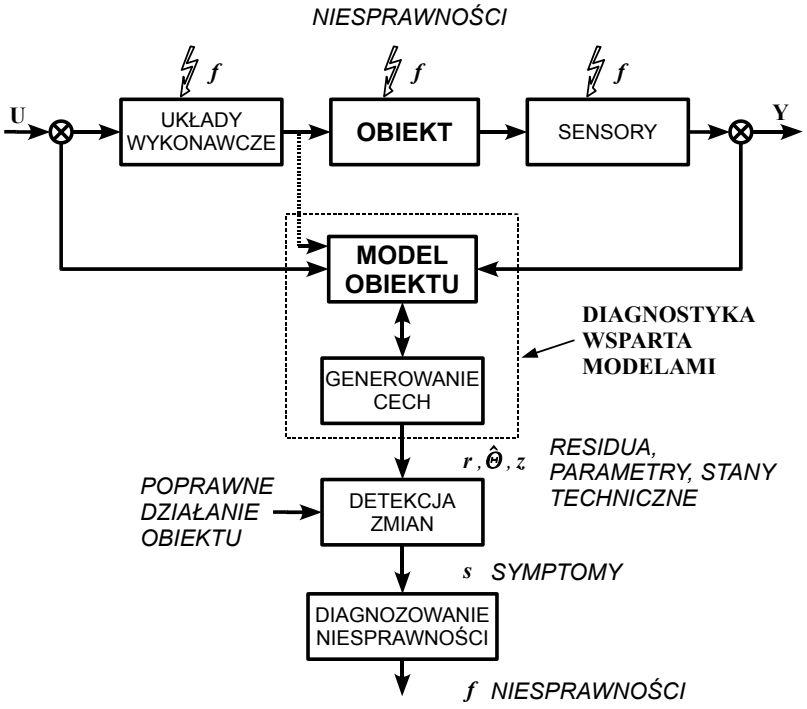
Należy tutaj zwrócić uwagę, że taki sposób określenia stanu dotyczy przypadku diagnostyki maszyn i urządzeń. W przypadku diagnostyki procesów przemysłowych proces diagnozowania składa się z trzech etapów [2.22, 2.30]:

- detekcji uszkodzenia,
- lokalizacji uszkodzenia,

- identyfikacji uszkodzenia.

Detekcja uszkodzeń definiowana jest jako wykrycie, zauważenie powstania uszkodzenia w obiekcie oraz chwili, w której to uszkodzenie nastąpiło. Lokalizacja pozwala na określenie rodzaju, miejsca i czasu wystąpienia uszkodzenia. Lokalizacja uszkodzenia może nastąpić dopiero po jego detekcji. Kolejnym krokiem jest identyfikacja uszkodzenia. Identyfikacja uszkodzenia określa rozmiar i charakter zmienności uszkodzenia w czasie.

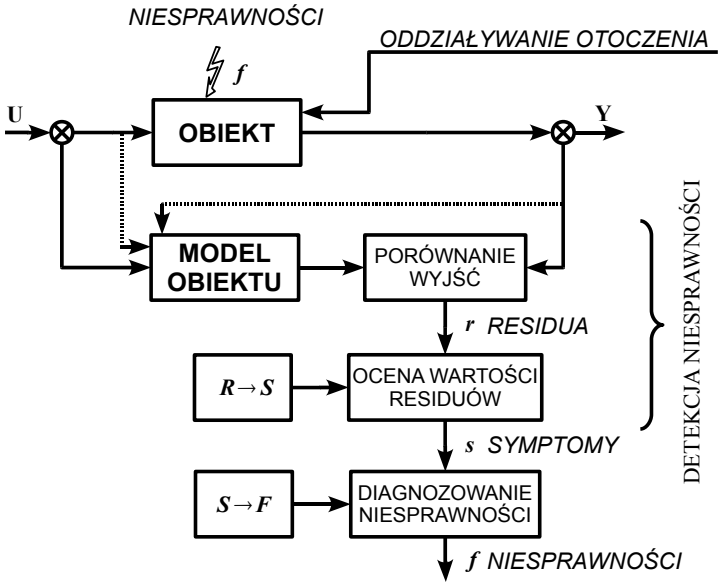
Ogólny schemat procesu diagnozowania stanu technicznego obiektu z użyciem jego modelu pokazano na rys. 2.3. Wartości mierzonych sygnałów wejściowych U, pozyskiwane z diagnozowanego obiektu, są podawane na wejścia modelu obiektu. Na podstawie porównania sygnałów wyjściowych obiektu Y z sygnałami wzorcowymi generowanymi przez model obiektu mogą być wyznaczane: residua r, parametry obiektu $\hat{\Theta}$ lub stany techniczne z [2.20, 2.21]. Na podstawie porównania wartości wymienionych zmiennych z wartościami zmiennych pochodzącymi z działającego obiektu wyznaczane są symptomy s, z użyciem których przeprowadzana jest diagnostyka stanu obiektu (rozpoznawanie niesprawności f). Należy pamiętać, że rozpoznawane stany techniczne badanego obiektu mogą zależeć również od stanów technicznych układów wykonawczych. Ponadto niesprawności w funkcjonowaniu aparatury pomiarowej (czujniki i tory pomiarowe) mogą powodować generowanie fałszywych danych pomiarowych, co w konsekwencji może doprowadzić do nieprawidłowego rozpoznania stanu technicznego diagnozowanego obiektu [2.19].



Rys. 2.3: Ogólny schemat procesu diagnozowania niesprawności obiektu z użyciem modelu obiektu (na podstawie [2.20])

Modele obiektów należy używać ze świadomością, że model nie zawsze musi zachowywać się podobnie jak obiekt działający w zadanych warunkach o określonym stanie technicznym. Przyjęte zazwyczaj uproszczenia, mające na celu uogólnienie modelu do pewnej klasy rozpatrywanych obiektów technicznych, powodują, że modele wykazują największą zgodność w stosunku do obiektów rzeczywistych tylko dla określonego zbioru branych pod uwagę stanów technicznych i jeszcze mniejszej liczby wyróżnionych warunków działania. W przypadku, gdy zachodzi potrzeba jak

najlepszego dopasowania modelu do wybranego egzemplarza obiektu technicznego przeprowadza się tzw. *strojenie modelu* za pomocą udostępnionych parametrów [2.43].



Rys. 2.4: Schemat procesu diagnozowania niesprawności obiektu z zastosowaniem modelu obiektu (na podstawie [2.20] i [2.27])

Na rys. 2.4 pokazano schemat szczególnego przypadku diagnozowania niesprawności z użyciem modelu obiektu. W wyniku porównania wartości wyjść generowanych przez obiekt rzeczywisty oraz model tego obiektu generowane są residua r. W kolejnym kroku wyznaczane są symptomy diagnostyczne s na podstawie zbiorów relacji odwzorowań wartości residuów r na wartości tych symptomów s. Etapy od porównania wyjść aż do wyznaczenia symptomów nazywa się *fazą detekcji niesprawności*. Ostatnim etapem jest przeprowadzenie wnioskowania diagnostycznego na podstawie relacji (p. 2.5):

$$S \Rightarrow F \tag{2.2}$$

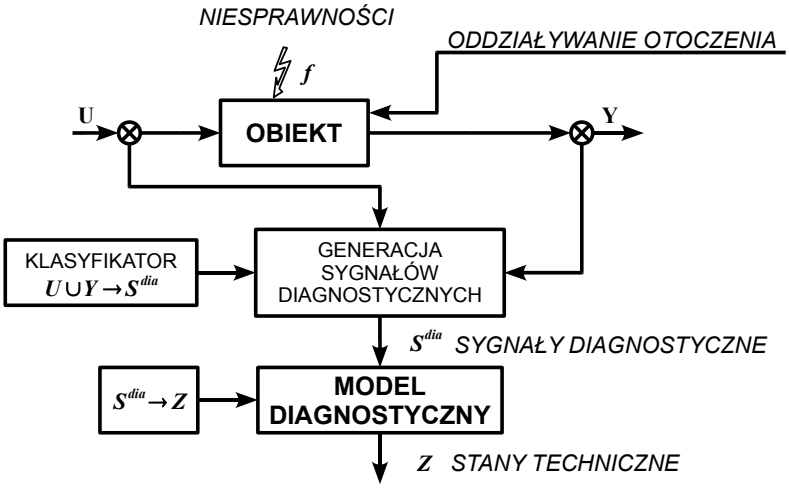
gdzie S jest symptomem danej niesprawności F.

W celu uproszczenia procesu diagnozowania zwykle pomija się wpływ stanu urządzeń wykonawczych i pomiarowych oraz innych obiektów technicznych na stan diagnozowanego obiektu i zastępuje się go tzw. *oddziaływaniem otoczenia*.

Inną grupą modeli są modele diagnostyczne. Na rys. 2.5 pokazano schemat procesu diagnozowania z użyciem takiej grupy modeli. Modele diagnostyczne wprowadza się w przypadku, gdy model obiektu jest zbyt złożony lub jego identyfikacja jest nieopłacalna ze względu na przyjęte kryteria. Model diagnostyczny przekształca cechy sygnałów diagnostycznych w klasy stanów technicznych (patrz diagnostyka symptomowa, por. rys. 2.2).

2.3. Modele obiektów

W diagnostyce technicznej przyjęto, że model obiektu jest to uproszczone odwzorowanie właściwości obiektu wybranych ze względu na możliwość oceny jego zdatności do wykonywania stawianych mu zadań [2.53]. Uproszczenie to polega na ograniczeniu zbioru właściwości obiektu uwzględnianych



Rys. 2.5: Schemat procesu diagnozowania niesprawności obiektu z zastosowaniem modelu diagnostycznego (na podstawie [2.20] i [2.27])

podczas identyfikacji jego modelu. Skutkiem czego może być brak zgodności szczegółowych wniosków z analizy relacji pomiędzy cechami sygnałów diagnostycznych i cechami stanu obiektu wyznaczonymi z modelu obiektu z wnioskami wyznaczonymi na podstawie obserwacji obiektu rzeczywistego [2.10].

Obiekty techniczne mogą być reprezentowane przez [2.49]:

1. *Model matematyczny* - przybliżony opis jakiejś klasy zjawisk wyrażony przy użyciu aparatu matematycznego;
2. *Model nominalny* - system założeń przyjmowanych w danej nauce w celu ułatwienia (lub umożliwienia) rozwiązania pewnego problemu badawczego;
3. *Model realny* - przedmiot lub układ przedmiotów (zdarzeń, sytuacji) spełniających założenia danej teorii, lub dostatecznie podobny do układu badanego, ale prostszy i łatwiej dostępny badaniom;
4. *Model teoretyczny* - konstrukcja hipotetyczna odwzorowująca dany rodzaj rzeczywistości w sposób uproszczony, sprowadzający jej cechy do związków najistotniejszych, budowana w celach heurystycznych;
5. *Model semantyczny* - logiczne odwzorowanie, czyli interpretacja danej teorii w postaci układu (dziedziny) przedmiotów opisywanego prawdziwie przez tę teorię.

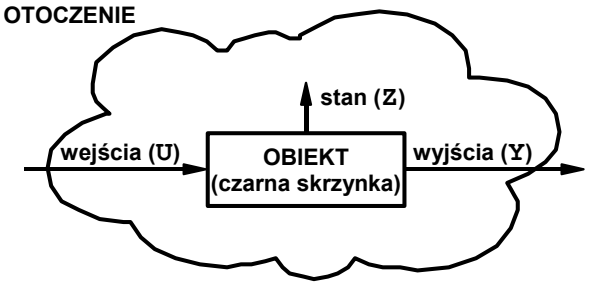
Wśród modeli obiektów technicznych należy rozróżnić ich dwie podstawowe grupy:

1. modele indywidualne,
2. modele grupowe.

Modele indywidualne opisują jeden wybrany obiekt. Natomiast modele grupowe opisują szereg obiektów podobnych ze względu na wybrane cechy. Modele indywidualne można tworzyć na podstawie modeli grupowych rozpatrywanych wówczas jako szczególne przypadki dla konkretnych egzemplarzy obiektów technicznych.

W najprostszym przypadku wprowadza się założenie, że każdy obiekt jest traktowany jak *czarna skrzynka* (rys. 2.6). Przyjęte uogólnienie pozwala wyodrębnić obiekt z jego otoczenia i nie zajmować się jego strukturą wewnętrzną. Konsekwencją takiego podejścia jest to, że [2.10]:

- oddziaływanie otoczenia na obiekt odbywa się wyłącznie za pośrednictwem wejść obiektu,
- oddziaływanie obiektu na otoczenie odbywa się wyłącznie za pośrednictwem wyjść obiektu,
- zbiór wejść i zbiór wyjść układu są zbiorami rozłącznymi.



Rys. 2.6: Koncepcja „czarnej skrzynki'

Dla znanych wartości wejść obiektu i znanych wartości cech stanu tego obiektu można wyznaczyć wartość jego wyjścia na podstawie:

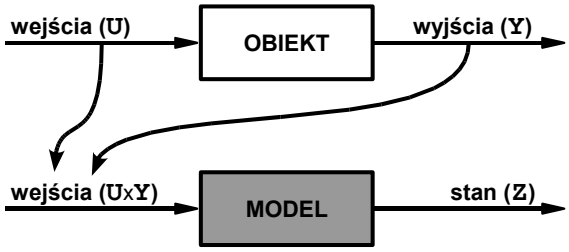
$$\mathtt{Y} = \mathtt{U} \times \mathtt{Z} \tag{2.3}$$

gdzie:

U - zbiór cech wejściowych,
Y - zbiór cech wyjściowych,
Z - przestrzeń cech stanów.

2.4. Modele diagnostyczne

Na potrzeby badań diagnostycznych tworzy się modele diagnostyczne [2.5, 2.4, 2.8, 2.24, 2.38, 2.52] (rys. 2.7). Model diagnostyczny przekształca dane o oddziaływaniu otoczenia na obiekt (poprzez



Rys. 2.7: Model diagnostyczny [2.10]

wejścia U) i obiektu na otoczenie (poprzez wyjścia Y) w stan obiektu Z [2.8]. Inaczej, jest to relacja pomiędzy cechami stanu obiektu a cechami sygnałów diagnostycznych [2.10, 2.11]:

$$\mathbf{M} \subset \mathtt{U} \times \mathtt{Y} \times \mathtt{Z} \tag{2.4}$$

gdzie:

M - model obiektu,
U - zbiór cech wejściowych,
Y - zbiór cech wyjściowych,
Z - przestrzeń cech stanów.

Modele diagnostyczne mogą być modelami ilościowymi, gdzie dane zapisane są w postaci liczb lub modelami jakościowymi, gdzie dane reprezentowane są w sposób przybliżony. W dużej liczbie przypadków modele diagnostyczne tworzą klasyfikatory. Klasyfikatory są używane w procesie klasyfikacji, czyli przyporządkowywania obiektów do wybranych klas na podstawie opisujących je cech.

Spośród wielu metod identyfikacji modelu diagnostycznego można wymienić:

- metodę regresyjną [2.5],
- metodę eksploatacyjnej analizy modalnej [2.45],
- metodę z zastosowaniem modelu odwrotnego [2.12],
- metody wykorzystujące opis obiektu w przestrzeni stanów [2.2],
- metody wykorzystujące sieci neuronalne [2.29],
- logikę rozmytą [2.28].

Niezależnie od przyjętej metodyki tworzenia modeli diagnostycznych, głównym problemem jest właściwa identyfikacja modelu. Zazwyczaj nie można obserwować wszystkich wejść obiektu lub z pewnych względów należy pominąć niektóre wejścia. Wiąże się to ze zredukowaniem rzędu modelu lub jego linearyzacją. W związku z tym model diagnostyczny może nie w pełni odwzorowywać zachowania obiektu. Dlatego też tworząc model diagnostyczny należy przewidzieć możliwość dostrajania go poprzez zmianę wybranych parametrów konfiguracyjnych.

2.5. Relacje stosowane w diagnostyce maszyn

Jednym z głównych celów diagnostyki technicznej jest ocena stanu technicznego maszyny. Ocena stanu maszyny może być realizowana w sposób „bezpośredni" lub „pośredni". Bezpośrednia ocena stanu może być realizowana przez [2.6, 2.10]:

- badanie elementów lub sposobu współdziałania współpracujących elementów,
- wykorzystanie arbitralnej oceny specjalistów.

Pierwsza z metod możliwa jest do zrealizowania jedynie poprzez demontaż maszyny. Wymaga przeprowadzenia odpowiednich badań, a czasem wymaga adaptacji samych elementów dla potrzeb przeprowadzenia badań. W drugim przypadku, gdy wykorzystywana będzie wiedza specjalistów, pojawia się problem związany z metodami formalizowania sposobów wyznaczanej opinii oraz ich właściwej oceny.

Stan maszyny może być również określony w sposób pośredni. Metody pośrednie określenia stanu polegają na tym, że na podstawie obserwacji sygnałów diagnostycznych wyznaczane są cechy stanu. Sygnałem diagnostycznym jest najczęściej przebieg dowolnej wielkości fizycznej, zależnej od stanu maszyny, który umożliwia przeniesienie informacji o jej stanie. Wartości wybranych cech sygnałów diagnostycznych maszyny, która znajduje się w określonym stanie, są symptomami tego stanu. Metody pośrednie mogą być stosowane do maszyn o wspólnej lub zbliżonej konstrukcji.

Zastosowanie pośrednich metod wyznaczania stanu maszyny wiąże się z przyjęciem pewnych założeń. Wyznaczenie bezpośrednich relacji pomiędzy symptomami stanu, a cechami sygnałów diagnostycznych nie jest zadaniem prostym. Wynika to między innymi ze złożoności budowy maszyn, oraz własności losowych procesów związanych z wytworzeniem i eksploatacją maszyn. W celu wyznaczenia takich relacji opracowuje się odpowiednie modele maszyn. Opracowane modele pozwalają na wnioskowanie o:

- rodzaju wielkości fizycznej, która powinna być obserwowana,
- rodzaju cech obserwowanych sygnałów, wrażliwych na zmiany stanu maszyny,

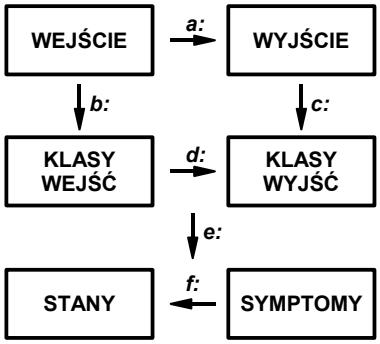
- zalecanej lokalizacji czujników pomiarowych,
- wymaganych warunkach działania maszyny podczas prowadzonych badań.

Stan maszyny zmienia się w sposób dynamiczny wraz z upływem czasu. Zmiany stanu mogą wpływać na zmiany cech sygnałów diagnostycznych. Zmienne w czasie wartości cech sygnałów diagnostycznych mogą stanowić podstawę do próby podejmowania decyzji o rozpoznaniu stanu maszyny. Podstawą do wykonania takich operacji jest założenie, że proces zmiany stanu oraz proces zmian sygnałów diagnostycznych odbywają się równolegle. Na tej podstawie poszukuje się zależności pomiędzy elementami obydwu procesów. Możliwość takiego opisu daje pojęcie relacji. Relacją R dwóch zbiorów A i B określa współzależność łączącą wybrane elementy należące do obydwu zbiorów [2.10]. W opisywanym przypadku wyróżniamy dwa zbiory na których definiujemy relacje. Są to:

- zbiór stanów badanego obiektu S_u,
- zbiór wartości cech sygnału diagnostycznego Z_u.

2.5.1. Klasy relacji diagnostycznych

Podczas prowadzonych badań diagnostycznych często wprowadza się różnego rodzaju relacje. Na rys. 2.8 pokazano klasy relacji diagnostycznych oraz związki pomiędzy nimi. Pokazane na rysunku



Rys. 2.8: Relacje stosowane w diagnostyce maszyn [2.12]

identyfikatory relacji reprezentują [2.12]:

a: model obiektu - relacja *wejście-wyjście*;

b: klasyfikator wejściowych cech modelu, który pozwala na przekształcanie cech ilościowych w cechy jakościowe;

c: klasyfikator wyjściowych cech modelu, który pozwala na przekształcanie cech ilościowych w cechy jakościowe (identyfikowany zazwyczaj z użyciem metod grupowania);

d: przybliżony model obiektu;

e: operacja odwracania modelu;

f: model odwrotny, który pozwala na wnioskowanie o klasie stanu technicznego obiektu na podstawie dostępnych symptomów.

2.5.2. Typy relacji diagnostycznych

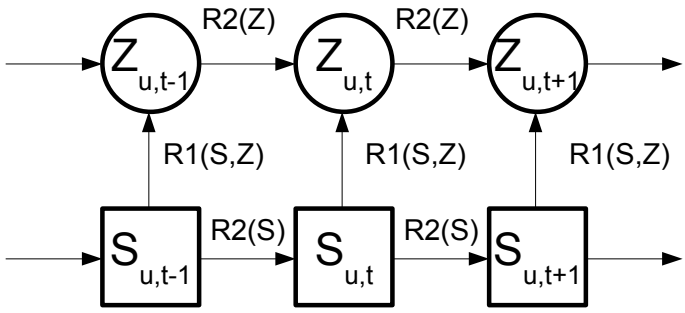
W badaniach diagnostycznych proces diagnozowany i sygnał diagnostyczny są najczęściej opisywane za pomocą uporządkowanych w czasie ciągów dyskretnych stanów/zdarzeń. Przykład takich uporządkowanych ciągów zdarzeń przedstawiono na rys. 2.9. Oś pozioma na tym rysunku jest osią czasu makro [2.10] i przyrasta od strony lewej do prawej. Bloki oznaczone na tym rysunku w postaci okręgów reprezentują chwilowe wartości cech sygnałów diagnostycznych. Bloki przedstawione w postaci

prostokątów odpowiadają zaś stanom badanego obiektu. Bloki połączone są liniami zakończonymi strzałkami, które odpowiadają relacjom, które mogą być identyfikowane w takiej sieci. Dla tak zdefiniowanej sieci można określić różne typy relacji. Pierwszą grupę relacji mogą stanowić relacje opisujące związki pomiędzy stanami badanego obiektu S_u i wartości cech sygnałów diagnostycznych Z_u zdefiniowane w następujący sposób [2.10]:

$$R1(S, Z) \subset S_U \times Z_U \tag{2.5}$$

Pierwszy typ relacji pokazano na rys. 2.9 za pomocą pionowych linii. Relacje tego typu są niezależne od czasu i zakłada się w nich równoczesność występowania obydwu zdarzeń jednocześnie. Można wtedy przyjąć, iż stan obiektu jest określany na podstawie wartości cech sygnału diagnostycznego.

Drugi z typów relacji diagnostycznych wiąże między sobą elementy jednej przestrzeni stanów. Do tej grupy relacji zaliczymy relacje wiążące kolejne w ciągu zdarzeń stany obiektu R1(S), a także zmieniające się w czasie wartości cech sygnałów diagnostycznych R2(Z). Jak widać na rys. 2.9 relacje tego typu są równoległe do osi czasu, a więc będą związane z jego upływem. Odpowiada to sytuacji, w której aktualny stan obiektu jest wynikiem jego stanów wcześniejszych.



Rys. 2.9: Sieć relacji dla procesu diagnozowanego i sygnału diagnostycznego [2.10]

Przedstawiony na rys. 2.9 schemat jest z praktycznego punktu widzenia mało przydatny, ze względu na liczbę możliwych cech stanu. Dlatego wymaga on modyfikacji.

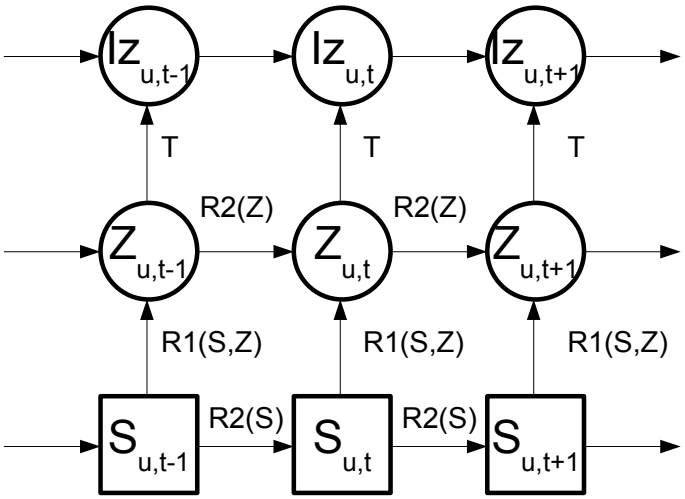
2.5.3. Modele relacji diagnostycznych

W praktycznych zastosowaniach wprowadza się ograniczenia związane z licznością zbioru rozpatrywanych cech sygnałów diagnostycznych. Wprowadzone ograniczenia wynikają między innymi z [2.10]:

- niemożliwości przeprowadzenia pomiarów niektórych oddziaływań pomiędzy obiektem badań i środowiskiem,
- ograniczenia liczby oddziaływań obiektu badań na otoczenie.

Przyjęte ograniczenia nie pozostają również bez wpływu na wyniki prowadzonych badań. Pociągają one za sobą ograniczenia zakresu wiedzy o naturze zjawisk zachodzących w obiekcie oraz wiedzy dotyczącej oddziaływań obiektu z otoczeniem.

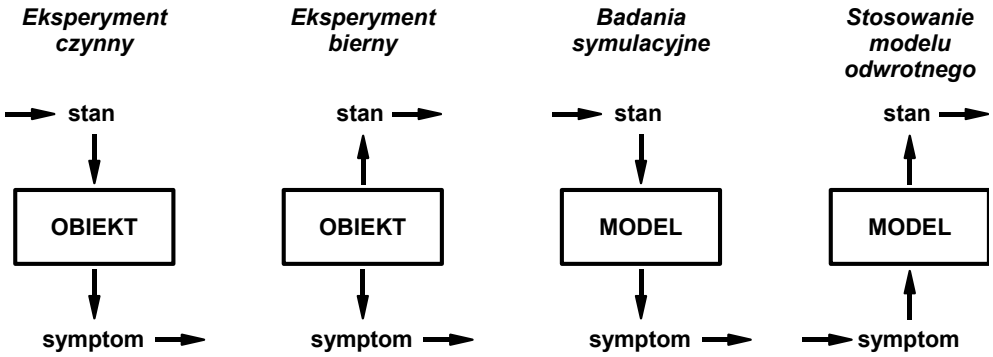
Podsumowując, przedstawiony na rys. 2.9 schemat nie uwzględnia odwzorowań stanów w przestrzeniach o ograniczonej liczbie wymiarów. Aby to uwzględnić schemat ten uzupełnia się o dodatkowe elementy nazywane *obrazami stanów maszyny* im$s_{u,t}$ oraz obrazami *wartości sygnału diagnostycznego* im$(z_{u,t})$ [2.10]. Uzupełniony schemat przedstawiono na rys. 2.10. W badaniach diagnostycznych wprowadza się ograniczenia jedynie na rozpatrywaną liczbę cech sygnałów diagnostycznych.



Rys. 2.10: Sieć relacji z uwzględnieniem obrazów cech [2.10]

2.5.4. Identyfikacja relacji diagnostycznych

Głównym celem prowadzenia badań diagnostycznych jest ocena stanu obserwowanego obiektu. Ocenę tą wykonuje się na podstawie opracowanych relacji diagnostycznych wiążących cechy sygnałów diagnostycznych z klasami stanów. Konieczna jest więc identyfikacja relacji diagnostycznych określających relacje przyczynowo-skutkowe, w których określone symptomy służą do rozpoznawania określonych stanów technicznych obiektu. Aby takie relacje określić prowadzi się badania eksperymentalne, w których dla dobrze znanego stanu obserwuje się sygnały diagnostyczne i poszukuje symptomów identyfikujących określony stan obiektu.



Rys. 2.11: Metody identyfikacji relacji w diagnostyce technicznej [2.12]

W diagnostyce technicznej wyróżnia się dwie podstawowe formy eksperymentów diagnostycznych na podstawie których identyfikuje się model diagnostyczny obiektu [2.12] (rys. 2.11):

- eksperyment czynny,
- eksperyment bierny.

Eksperyment czynny polega na celowym wprowadzeniu do badanego obiektu określonej niesprawności i obserwacji sygnałów diagnostycznych. Ponieważ w takim przypadku znany jest stan obiektu,

można poszukiwać symptomów, które posłużą do rozpoznania określonego stanu. W przypadku rzeczywistych obiektów trudno jest prowadzić tego typu badania. Jest to spowodowane faktem, że obiekt zazwyczaj pracuje i właściciel nie zezwoli na jego zatrzymanie jak również celowe wprowadzanie uszkodzeń. Dlatego też tego typu rozwiązania stosowane są głównie w przypadku niewielkich obiektów, o niewielkich kosztach wytworzenia, wytwarzanych w dużych seriach. Z tego powodu częściej od eksperymentu czynnego prowadzony jest eksperyment bierny.

Eksperyment bierny polega na obserwacji badanego obiektu bez ingerencji w jego stan. Na podstawie przeprowadzanych obserwacji prowadzone są badania zmierzające do identyfikacji relacji pomiędzy stanem obiektu a aktualnymi symptomami.

Interesującym sposobem prowadzenia eksperymentów jest wykorzystanie do tego celu modeli obiektów. Jeżeli znany jest dobry model obiektu, to wprowadzając modyfikacje do tego modelu możemy zmieniać jego stan. Wynikiem działania takiego modelu mogą być np. sygnały diagnostyczne, które będzie można również otrzymywać z rzeczywistych obiektów. Na podstawie otrzymanych sygnałów diagnostycznych możliwe będzie zidentyfikowanie relacji diagnostycznych. Wprowadzając do modelu obiektu określone zmiany, powodujące zmianę jego stanu, można w stosunkowy prosty sposób, przy niewielkich nakładach budować relacje diagnostyczne dla różnych stanów obiektu. W przypadku, gdy dysponujemy modelem obiektu możemy użyć go do:

- prowadzenia badań symulacyjnych (podczas których dla zadanych stanów generowane będą symptomy),
- odwracania modeli i stosowania modelu odwrotnego (identyfikacja relacji symptom-stan).

Użycie modelu w badaniach symulacyjnych pozwala zmniejszyć koszty oraz przeprowadzić badania, których nie można byłoby zrealizować na rzeczywistym obiekcie (np. testowanie niesprawności reaktorów jądrowych). W diagnostyce technicznej relacja stan-symptom nie jest użyteczna. Bardziej interesuje nas relacja odwrotna symptom-stan. Taka relacja jest realizowana z zastosowaniem tzw. modeli odwrotnych (p. 2.6.5).

2.6. Rodzaje modeli diagnostycznych

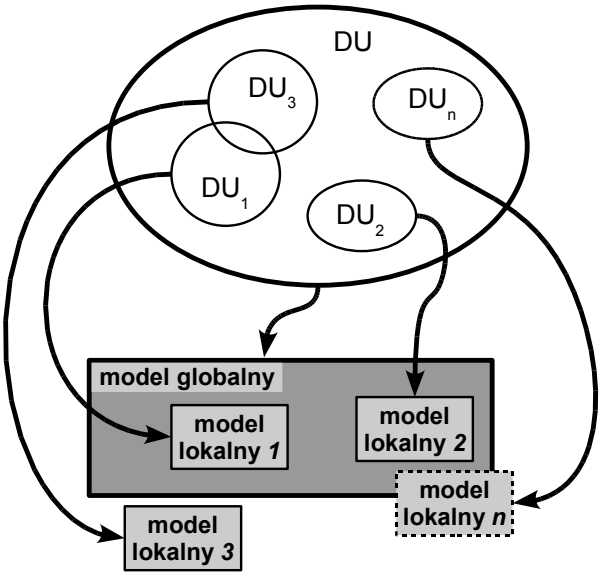
2.6.1. Modele lokalne i modele globalne

W badaniach diagnostycznych opartych na modelach, wyróżnia się klasę modeli globalnych i klasę modeli lokalnych (rys. 2.12). Model globalny opisuje dane uczące w pełnej przestrzeni ich wartości [2.25]. Podczas identyfikacji modeli globalnych pojawiają się dwa skrajne problemy związane z nadmiarem danych uczących oraz ich brakiem. Zwykle wprowadzane uproszczenia pogarszają jakość ich działania. Z drugiej strony wystarcza jeden model do rozpoznawania stanu całego obiektu. Natomiast model lokalny jest to model, który reprezentuje dane uczące tylko w wybranym obszarze przestrzeni wartości. Należy zaznaczyć, że model globalny nie jest sumą wypadkową modeli lokalnych. W pracach [2.12, 2.13, 2.17] pokazano, że zastosowanie modeli lokalnych jest rozwiązaniem bardziej korzystnym, niż zastosowanie modeli globalnych. Głównym argumentem są tutaj koszty identyfikacji modelu globalnego. Wśród innych zalet tworzenia modeli lokalnych, w odniesieniu do modeli globalnych, wymienia się:

- łatwiejszą identyfikację (związaną m.in. z mniejszą liczbą obserwowanych wejść i mniejszą liczbą wyznaczanych parametrów),
- zwykle wyższą dokładność.

Wadami modeli lokalnych jest to, że tego typu modele nie zawsze:

- reprezentują obiekt we wszystkich warunkach działania,
- uwzględniają wszystkie stany obiektu.



Rys. 2.12: Model globalny i model lokalny. DU - zbiór danych uczących, DU_n - podzbiór danych uczących

Modele lokalne mogą być identyfikowane osobno, przy czym należy uwzględnić na wejściu identyfikowanego modelu lokalnego wszystkie cechy sygnałów diagnostycznych całego obiektu, które mogą przyjmować formę dodatkowych wejść z danymi pochodzącymi od innych modeli lokalnych związanych z fragmentami obiektu. Wynika z tego pewna trudność polegająca na tym, że nie zawsze będzie możliwa dokładna identyfikacja modelu. W związku z tym, jak wspomniano wcześniej, należy przewidzieć możliwość strojenia modelu. W celu ułatwienia zadania identyfikacji stosuje się dekompozycję jednego modelu globalnego na zbiór modeli lokalnych związanych z fragmentami obiektu [2.39]. Podział rozpatrywanego obiektu na fragmenty nie musi być podziałem rozłącznym. Jest to możliwe w przypadku jeżeli przewidziano odpowiednie agregowanie lub uzgadnianie wyjść modeli lokalnych.

2.6.2. Wielomodele

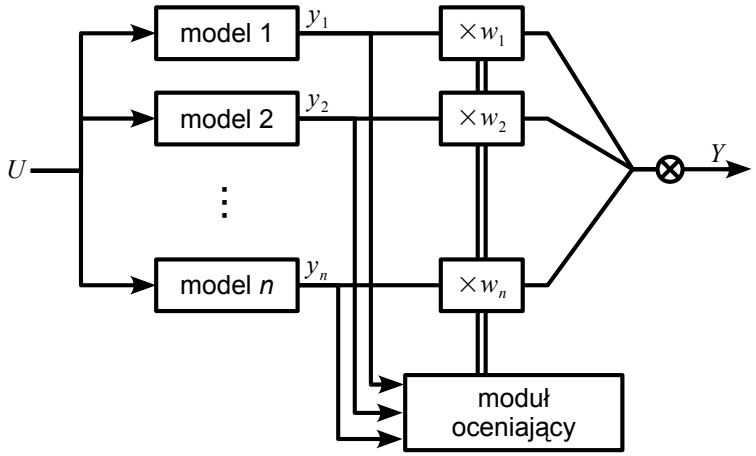
W pracy [2.48] wielomodele zdefiniowano jako modele o ustalonej strukturze, które są zbudowane co najmniej z dwóch modeli składowych. Najbardziej popularnymi strukturami łączenia modeli są:

1. struktura szeregowa, gdzie wyjście jednego modelu jest wejściem drugiego modelu, a poszczególne modele składowe tworzą kolejne stopnie identyfikujące ogólny model obiektu;
2. struktura równoległa, gdzie wejście i wyjście każdego modelu składowego jest powiązane z wejściem i wyjściem pozostałych modeli składowych;
3. struktura hierarchiczna, gdzie modele składowe są połączone na zasadzie nadrzędności i podrzędności;
4. struktura sieciowa, gdzie modele składowe są połączone w sposób nieuporządkowany, a w ogólnym przypadku każdy z każdym;
5. struktura mieszana, będąca połączeniem powyższych.

Modele składowe powinny być identyfikowane niezależnie od siebie, ale tak, żeby była ogólnie zachowana możliwie zupełna reprezentacja warunków działania całego obiektu oraz możliwie zupełna reprezentacja stanów całego obiektu. Liczba modeli składowych zależy od liczby i rodzaju posiadanych danych oraz od stopnia skomplikowania modelowanego obiektu.

2.6.3. Modele wielowarstwowe

Modele wielowarstwowe stosuje się, gdy występuje nadmierna liczba możliwych do wyznaczenia cech sygnałów diagnostycznych i/lub występuje duża liczba cech stanu na podstawie których rozpoznawana jest klasa stanu [2.8]. Modele te należą do klasy wielomodeli, przy czym modele składowe



Rys. 2.13: Model wielowarstwowy [2.48]

połączone są ze sobą równolegle (rys. 2.13). W związku z tym każdy model posiada taką samą porcję informacji na wejściu. Natomiast wyjściem modelu wielowarstwowego jest wyjście modelu (modeli) najlepiej reprezentującego stan techniczny diagnozowanego obiektu rozpatrywanego w chwili czasu. Wybór modelu następuje poprzez oszacowanie w module oceniającym ilości informacji o stanie technicznym obiektu dostarczanej przez poszczególne modele. Zaletą modeli wielowarstwowych jest to, że zastosowane modele mogą uzupełniać się nawzajem, polepszając tym samym skuteczność działania modelu. Natomiast wadą jest to, że każdy model dostaje tę samą porcję informacji oraz to, że nie ma szczegółowych wytycznych wspomagających dobór parametrów mechanizmu wybierającego model najlepiej reprezentujący stan obiektu (problem oceny informacji o stanie).

2.6.4. Modele wieloaspektowe

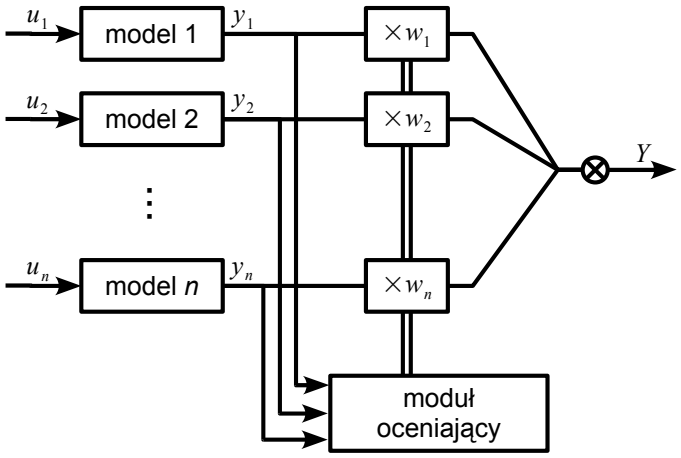
Modele wieloaspektowe również należą do klasy wielomodeli o strukturze równoległej. W odróżnieniu do modeli wielowarstwowych, każdy model składowy modelu wieloaspektowego posiada inną porcję informacji na wejściu (rys. 2.14). Każdy model składowy odpowiada jednemu aspektowi, w którym może być rozpatrywany modelowany obiekt. Liczba modeli (aspektów) zależy od liczby rodzajów źródeł informacji, na podstawie których modele składowe są identyfikowane.

2.6.5. Modele odwrotne

Modele odwrotne przekształcają, za pomocą relacji diagnostycznych, symptomy diagnostyczne w klasy stanów technicznych [2.8]. Modele odwrotne są identyfikowane na dwa sposoby:

1. przez odwracanie analitycznego modelu obiektu (zazwyczaj modelu matematycznego),
2. na podstawie danych uczących zebranych i opracowanych w trakcie eksperymentów diagnostycznych.

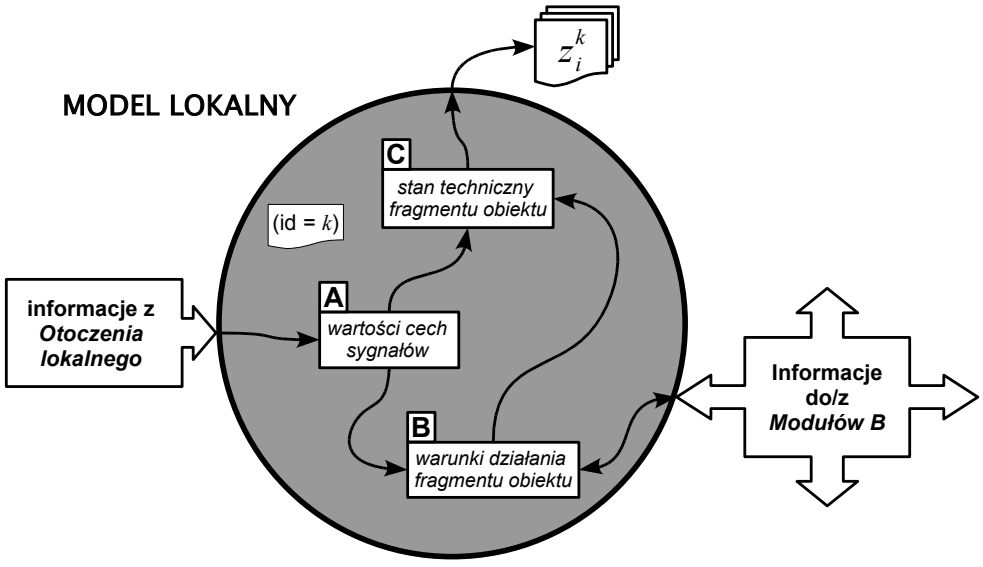
W przypadku, gdy nie jest możliwe analityczne wyznaczenie modelu odwrotnego, przeprowadza się identyfikację modelu odwrotnego z użyciem drugiego sposobu. W pierwszym etapie budowany jest numeryczny model symulacyjny, a następnie generowane są sygnały dla zadanych przypadków stanów technicznych. Otrzymane sygnały są weryfikowane z sygnałami pochodzącymi z rzeczywistego obiektu. W drugim etapie, na podstawie zebranych danych, wyznacza się model odwrotny [2.25].



Rys. 2.14: Model wieloaspektowy [2.48]

2.6.6. Modele wielomodułowe

Jak wspomniano wcześniej jednym ze sposobów tworzenia modeli jest rezygnacja z poszukiwania globalnego modelu diagnostycznego i zastąpienie go zbiorem modeli lokalnych, z których każdy pozwala na wyznaczenie (uwzględnienie) cech diagnostycznych dotyczących wyłącznie wybranego funkcjonalnego lub strukturalnego fragmentu obiektu [2.23].

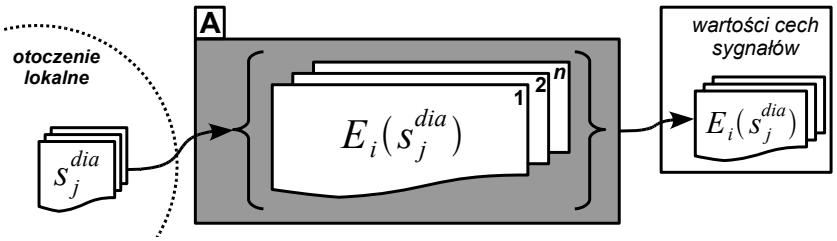


Rys. 2.15: Postać diagnostycznego modelu lokalnego [2.39]. A, B, C - moduły k-tego modelu lokalnego; z_i^k - i-ty stan k-tego fragmentu obiektu

Model lokalny może być modelem lokalnym strukturalnie (przestrzennie, terytorialnie), jak np. model łożyska tocznego, lub modelem lokalnym funkcjonalnie (lecz o możliwym znacznym rozproszeniu terytorialnym), jak np. model układu chłodzenia. W pracy [2.39] zaproponowano, że każdy model lokalny zbudowany jest z trzech współdziałających ze sobą modułów (rys. 2.15):

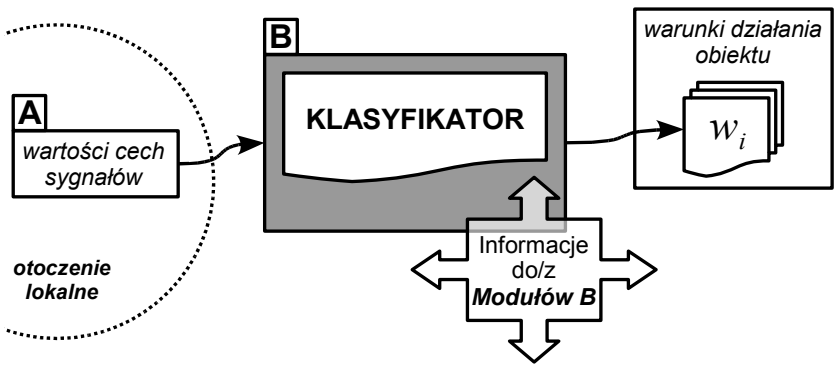
1. Modułu A, którego zadanie polega na obserwacji lokalnego nośnika informacji o stanie fragmentu obiektu (sygnału diagnostycznego);

2. Modułu B, którego zadanie polega na wnioskowaniu o warunkach działania fragmentu obiektu i całego obiektu oraz na uzgadnianiu wspólnej opinii o tych warunkach działania z innymi Modułami B;
3. Modułu C, którego zadanie polega na wnioskowaniu o stanie technicznym obiektu na podstawie wyników obserwacji lokalnych nośników informacji oraz wyników rozpoznawania i uzgadniania warunków działania całego obiektu.



Rys. 2.16: Postać Modułu A

Zadaniem Modułu A (rys. 2.16) jest wyznaczanie wartości cech sygnałów diagnostycznych s^{dia} pozyskanych z fragmentu obiektu o_i związanego z modelem lokalnym m_i^L. W związku z tym Moduł A będzie zawierał zbiór funkcji i procedur wyznaczających wartości cech sygnałów diagnostycznych [2.34, 2.30]. Moduł A ma dostęp wyłącznie do cech sygnałów pozyskanych z fragmentu obiektu związanego z tym modelem. Nie są dla niego dostępne (bezpośrednio) cechy sygnałów pochodzących z innych fragmentów obiektu.



Rys. 2.17: Postać Modułu B

Zadaniem Modułu B (rys. 2.17) jest rozpoznawanie warunków działania W fragmentu obiektu o_i związanego z modelem lokalnym m_i^L oraz uzgadnianie z innymi Modułami B warunków działania całego obiektu. Zakłada się, że Moduł B ma dostęp do wyników działania Modułu A. Każdy Moduł B ma przypisany pewien zbiór warunków działania fragmentu obiektu związanego z modelem lokalnym oraz zbiór warunków działania całego obiektu. Działanie Modułu B polega na wykonaniu trzech kroków:

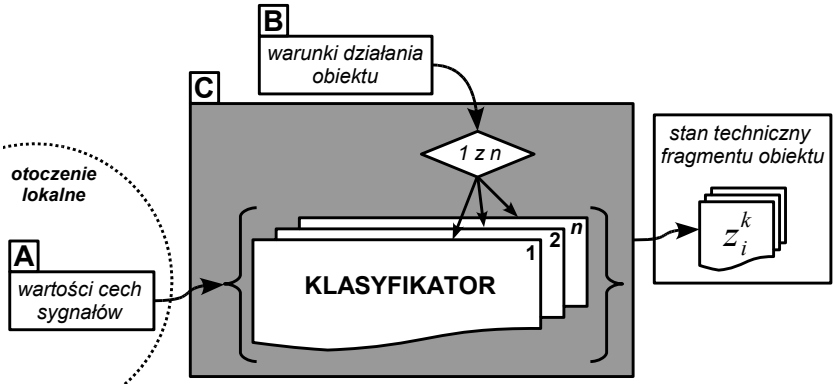
Krok 1 Rozpoznawanie warunków działania fragmentu obiektu.

Krok 2 Rozpoznawanie warunków działania całego obiektu.

Krok 3 Uzgadnianie z innymi Modułami B warunków działania całego obiektu.

W pierwszym kroku są rozpoznawane warunki działania dla fragmentu obiektu. Następnie stanowią one dane wejściowe do drugiego etapu - wyznaczania propozycji warunków działania całego obiektu.

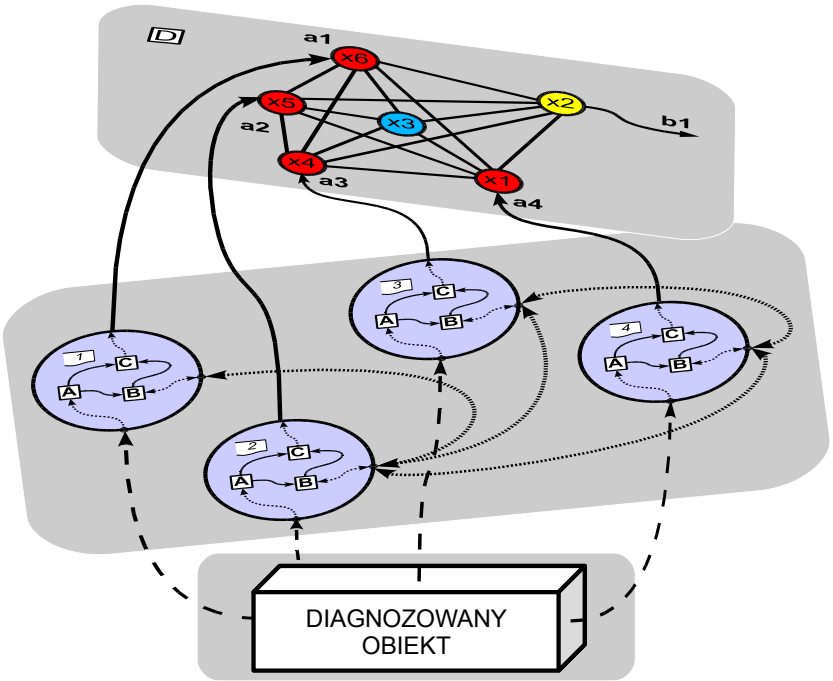
Ostatecznie, w procesie agregacji lub uzgadniania opinii Moduły B wypracowują wspólną opinię wskazując ostatecznie warunki działania fragmentów obiektu i całego obiektu.



Rys. 2.18: Postać Modułu C

Moduł C (rys. 2.18) jest klasyfikatorem stanu. Jego zadaniem jest klasyfikacja (rozpoznanie) stanu fragmentu obiektu o_i związanego z modelem lokalnym m_i^L. W celu przeprowadzenia procesu klasyfikacji stanu niezbędna jest znajomość wartości cech relewantnych oraz warunków działania w jakich znajduje się obiekt.

Wyniki rozpoznawania klas stanów, traktowane jak stopnie przekonania, stanowią wejście do sieci stwierdzeń (Moduł D) (rys. 2.19). Na podstawie obliczeń, uwzględniających m.in. wiedzę subiektywną zawartą w tablicach prawdopodobieństw warunkowych, wyznaczana jest wartość stopnia przekonania o klasie stanu technicznego całego obiektu [2.41, 2.31, 2.3].



Rys. 2.19: Synteza modelu wielomodułowego [2.39]

Sieć stwierdzeń składa się z trzech zbiorów stwierdzeń:

1. wejściowych,
2. pomocniczych,
3. wyjściowych.

Każdy element tych zbiorów przyjmuje wartości z przedziału $[0; 1]$ i są to wartości stopnia przekonania o wystąpieniu danego stanu technicznego. Każdy stan obiektu jest związany z wybranym stwierdzeniem wejściowym. Oprócz stwierdzeń wejściowych są jeszcze stwierdzenia pomocnicze (np. spełniające rolę stwierdzeń grupujących stwierdzenia związane ze stanami wybranego fragmentu obiektu) oraz stwierdzenia wyjściowe, które reprezentują stany całego obiektu.

2.6.7. Inne klasy modeli

Oprócz powyżej wymienionych klas modeli w literaturze poświęconej diagnostyce technicznej można spotkać inne klasy modeli, takie jak:

Model statystyczny: W modelu statystycznym dane reprezentowane są w postaci łącznych rozkładów gęstości prawdopodobieństw ich wartości [2.8].

Model przekonań: W modelu przekonań dane reprezentowane są w postaci rozkładów przekonań o ich wartościach, gdzie modele przekonań są odpowiednikami modeli statystycznych, w których miary prawdopodobieństwa zastąpiono miarami subiektywnych przekonań [2.8].

Model strukturalny: Model strukturalny odwzorowuje dynamiczną strukturę modelowanego układu, jak również wzajemne oddziaływanie występujące pomiędzy elementami rozpatrywanego układu [2.35, 2.5].

Model logiczny: Model logiczny jest budowany w oparciu o aparat logiki matematycznej. Obejmuje stwierdzenia, orzekające o własnościach i właściwościach modelowanego obiektu oraz wnioski, dotyczące stanu obiektu, które na ich podstawie można wyciągnąć, a dotyczące własności i zachowania się modelowanego układu [2.35, 2.37].

2.7. Doskonalenie modeli

2.7.1. Ocena modelu obiektu

Analiza i ocena wyników generowanych przez opracowany model obiektu jest nieodzownym składnikiem każdej symulacji. Ocena polega na porównaniu wyników uzyskanych z przeprowadzonej symulacji i obserwacji obiektu rzeczywistego. Informacjami o własnościach obiektu rzeczywistego mogą być zarówno dane zebrane w czasie obserwacji pracy obiektu, jak i wyniki dostarczone przez odpowiednio uproszczone modele analityczne obiektów. Wprowadzone przybliżenia w modelu obiektu mające na celu uproszczenie systemu rzeczywistego powodują występowanie odchyłek. Jeżeli w systemie rzeczywistym spełniona jest zależność:

$$Y_r = f_r\left(U_r, t_r\right) \tag{2.6}$$

gdzie

Y_r - wyjścia obiektu rzeczywistego;
U_r - wejścia obiektu rzeczywistego;
t_r - czas;
$f_r(.)$ - funkcja wiążąca wejścia i wyjścia obiektu, funkcja przejścia.

to w modelu obiektu spotykamy się z sytuacją następującą:

$$Y_m \pm \Delta Y = f_m\left(U_m, t_m\right) \tag{2.7}$$

gdzie

Y_m - wyjścia obiektu rzeczywistego;
U_m - wejścia obiektu rzeczywistego;
t_m - czas;
$f_m(.)$ - funkcja wiążąca wejścia i wyjścia obiektu, funkcja przejścia;
ΔY - odchyłka modelowania.

Odchyłka modelowania zależy od następujących czynników [2.32]:

- od niedokładności związanych z określeniem parametrów systemu rzeczywistego,
- od niedokładności uwarunkowanych odchyłkami pomiarów wykonywanych podczas badań,
- od niedokładności uwarunkowanych istnieniem czynników inaczej występujących w badaniach modelowych niż w badaniach systemów rzeczywistych, przez co zmieniają się parametry modelu. Niedokładności tego rodzaju występują zwłaszcza w stanach, w których istotną rolę odgrywają nieliniowe charakterystyki wiążące ze sobą poszczególne parametry. Konsekwencją istnienia tego typu niedokładności może być całkowita rozbieżność pomiędzy wynikami badań modelowych i rzeczywistością,
- od niedokładności wywołanych niepełnym uwzględnieniem w modelu czynników wpływających na podstawowe zjawiska, tj. od niedokładności wynikających z przybliżonego modelowania.

W celu dokonania oceny modelu obiektu niezbędne jest przyjęcie metryki określonej na przestrzeni wszystkich par *wejście-wyjście* [2.18]. Metryką określoną na zbiorze W nazywamy przekształcenie $d : W^2 \rightarrow \Re$ takie, że:

1. $d(w, w) = 0$ dla wszystkich $w \in W$;
2. $d(w_1, w_2) = d(w_2, w_1)$ dla wszystkich par $w_1, w_2 \in W$;
3. $d(w_1, w_3) = d(w_1, w_2) + d(w_2, w_3)$ dla wszystkich trójek $w_1, w_2, w_3 \in W$;

Dla każdych dwóch par *wejścia–wyjścia* metryka d przyporządkowuje liczbę rzeczywistą dodatnią, która jest odległością między tymi parami. W przypadku badania zgodności obiektu rzeczywistego z jego modelem mamy:

$$d\left(\left(x_r, y_r\right), \left(x_m, y_m\right)\right) \tag{2.8}$$

gdzie

x_r, y_r - odnosi się do obiektu rzeczywistego;
x_m, y_m - odnosi się do modelu.

W powyższym przypadku metryka d może być interpretowana jako wartość bezwzględna odchyłki między tymi parami.

Po przyjęciu odpowiedniej metryki należy ustalić próg decyzyjny, określający kiedy pary *wejścia–wyjścia* modelu i obiektu rzeczywistego są dostatecznie bliskie ze względu na cele, do których model został przeznaczony. Korzysta się tutaj z pojęcia tolerancji, czyli modelowa para *wejścia–wyjścia* (x_m, y_m) jest w granicach tolerancji pary systemu rzeczywistego (x_r, y_r) jeżeli:

$$d\left(\left(x_r, y_r\right), \left(x_m, y_m\right)\right) \leqslant L \tag{2.9}$$

gdzie L jest poziomem akceptacji.

Dużą liczbę metryk stanowią metryki oparte na normach określonych na przestrzeniach liniowych. Norma wyznacza odległość od zera (należącego do przestrzeni liniowej) do każdego elementu należącego do tej przestrzeni. Przykładami norm mogą być [2.18]:

- maksimum odchyłki

$$\|\rho\| = max\{\rho(t) : t \in D(\rho)\} \tag{2.10}$$

- całka z wartości bezwzględnej odchyłki

$$\|\rho\| = \int_D (\rho)|\rho(t)|dt \tag{2.11}$$

- całka z kwadratu odchyłki

$$\|\rho\| = \int_D (\rho)\rho^2(t)dt \tag{2.12}$$

Mając normę $\|.\|$, metrykę d_0 definiuje się jako:

$$d_0(\rho, \rho') = \|\rho - \rho'\| \tag{2.13}$$

Jest to odległość pomiędzy ρ i ρ', która jest odległością różnicy $\rho - \rho'$ od zera. Na przykład dla całki z kwadratu mamy:

$$d_0(\rho, \rho') = \int_{[0,\tau]} \left[\rho(t) - \rho'(t)\right]^2 dt \tag{2.14}$$

gdzie $[0, \tau]$ jest wspólną dziedziną wielkości ρ i ρ'.

Ponieważ $e = \rho - \rho'$ jest trajektorią odchyłki, więc $d_0(\rho, \rho')$ jest scałkowaną odchyłką kwadratową.

Jak już powiedziano, w wynikach obserwacji obiektu rzeczywistego i jego modelu zawsze występuje pewna niezgodność w przestrzeniach par *wejścia–wyjścia* tych systemów. Przyczyn tej niezgodności można poszukiwać w funkcjach wyjściowych i w funkcjach przejścia.

W przypadku funkcji wyjściowych dąży się do minimalizacji odległości pomiędzy wartościami generowanymi na wyjściach obiektu rzeczywistego i jego modelu. Dla założonej metryki związanej z przestrzenią klas stanów wyjściowych przyjmuje się, że ε_y jest granicą niezgodności wartości pojawiających się na wyjściach, tj. dla wszystkich $q \in Q$ mamy:

$$d_y\left(y_r\left(q\right), y_m\left(q\right)\right) \leqslant \varepsilon_y \tag{2.15}$$

W przypadku funkcji przejścia dąży się do minimalizacji odległości pomiędzy trajektoriami tych funkcji wyznaczonych dla obiektu rzeczywistego i jego modelu. Dla założonej metryki związanej z przestrzenią klas stanów przyjmuje się, że ε_h jest granicą niezgodności odpowiadających sobie kolejnych punktów trajektorii funkcji przejścia, tj. dla wszystkich $q \in Q$ mamy:

$$d_h\left(h_r\left(q\right), h_m\left(q\right)\right) \leqslant \varepsilon_h \tag{2.16}$$

Do oceny jakości modelu obiektu można również użyć metod statystycznych. Do najbardziej popularnych metod należą:

- *Test χ^2 (Chi-kwadrat)*. Test χ^2 służy do weryfikacji hipotezy, że zbiór danych empirycznych (w tym przypadku otrzymanych za pomocą modelu) ma taki sam rozkład jak obserwacje zarejestrowane w obiekcie rzeczywistym. Stosowany jest on przy testowaniu hipotez nieparametrycznych. Test jest prosty do wykonania, lecz wymaga dużej liczby obserwacji (rzędu dziesiątek).
- *Analiza wariancji*. Analiza wariancji pozwala sprawdzić, czy wartości średnie wielu populacji (reprezentowane przez wartości zmiennych pozyskanych z modelu i odpowiadające im wartości zmiennych zarejestrowanych w obiekcie rzeczywistym) różnią się istotnie. W ogólnym przypadku testy analizy wariancji służą do badania wpływu pewnych kontrolowanych parametrów na postać populacji wyjściowej i jej charakterystyki. W szczególności jednak, przyjmując takie same wartości wejściowe dla wszystkich zmiennych, zarówno modelowych, jak i rzeczywistych, można sprawdzić hipotezę statystyczną o równości średnich wartości tych zmiennych.

- *Analiza regresji*. Funkcją regresji I rodzaju zmiennej losowej Y względem zmiennej X jest funkcja przyporządkowująca poszczególnym wartościom zmiennej X wartości oczekiwane w odpowiednim warunkowym rozkładzie zmiennej Y. Przy porównywaniu przebiegów z modelu i obiektu rzeczywistego szczególnie istotną rolę odgrywa liniowa funkcja regresji:

$$f(x) = ax + b \tag{2.17}$$

gdzie a jest współczynnikiem regresji liniowej Y względem X wyrażającym przyrost wartości oczekiwanej zmiennej Y spowodowany jednostkowym przyrostem wartości zmiennej losowej X. Przedmiotem testów będzie sprawdzenie czy b nie różni się w sposób istotny od 0 oraz czy a nie różni się istotnie od 1. Wartości zmiennych a i b, dla znanych wartości ciągów $\{X_n\}$ i $\{Y_n\}$, wyznacza się ze wzorów:

$$a = \frac{\sum_{i=1}^{n} (X_i - \bar{X})(Y_i - \bar{Y})}{\sum_{i=1}^{n} (X_i - \bar{X})^2} \qquad b = \bar{Y} - a\bar{X} \tag{2.18}$$

gdzie $\bar{X}$ i $\bar{Y}$ są średnimi arytmetycznymi odpowiednio z ciągów $\{X_n\}$ i $\{Y_n\}$.

2.7.2. Doskonalenie modelu diagnostycznego

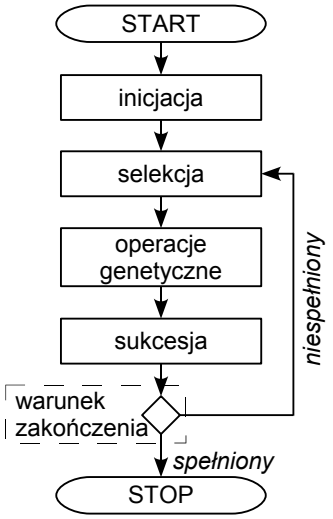
Celem doskonalenia modeli diagnostycznych, zarówno globalnych jak i lokalnych, jest poprawa jakości ich działania. Wynikiem działania modeli diagnostycznych jest wskazanie jednego lub zbioru stanów diagnozowanego obiektu. Zatem doskonalenie modeli powinno prowadzić do poprawy jakości stawianych diagnoz. Modele można doskonalić przez zmianę:

- struktury modelu (jego postaci),
- rodzaju parametrów modelu i ich wartości,
- liczby i rodzaju cech na wejściu modelu,
- zbioru przykładów uczących (zbiór powinien zawierać dane uczące związane z jak największą liczbą możliwych klas stanów technicznych i warunków działania obiektu).

Ostatnia z wymienionych metod doskonalenia modeli może pośrednio wpływać na strukturę modelu oraz wartości parametrów modelu. Identyfikowanie modeli globalnych jest dużo kosztowniejsze niż identyfikowanie modeli lokalnych. Również doskonalenie modeli globalnych jest trudne i nie zawsze uzasadnione. Powodem jest przeszukiwanie wielowymiarowych przestrzeni, co wiąże się z przeprowadzeniem dużej liczby obliczeń.

Jedną z ciekawszych metod doskonalenia modeli diagnosycznych jest doskonalenie ewolucyjne z zastosowaniem algorytmu przedstawionego na rys. 2.20. Zastosowanie algorytmu ewolucyjnego wymaga określenia [2.1]:

- sposobu kodowania fenotypu w genotypie (sposobu reprezentacji potencjalnych rozwiązań),
- sposobu tworzenia populacji początkowej,
- funkcji oceniającej (funkcji przystosowania),
- sposobu selekcji i sukcesji osobników,
- sposobu prowadzenia operacji genetycznych,
- warunku (warunków) zakończenia działania algorytmu,
- wartości różnych parametrów używanych w algorytmie (rozmiaru populacji, prawdopodobieństwa użycia operatorów genetycznych itp.).



Rys. 2.20: Schemat algorytmu ewolucyjnego

Bardzo ważnym elementem jest funkcja oceniająca, która ma decydujący wpływ na skuteczność działania algorytmu ewolucyjnego. Pomimo jej dużego znaczenia nie ma wytycznych na opracowanie jej postaci. Najczęściej funkcję oceniającą dobiera się indywidualnie na potrzeby rozpatrywanego zadania. Pozostałe elementy można dobrać zgodnie z wytycznymi zawartymi w literaturze (np. [2.1, 2.33]).

W pracach [2.46] i [2.39] pokazano optymalizację zbioru danych uczących z zastosowaniem algorytmu ewolucyjnego. Dla znanych wartości cech sygnałów diagnostycznych i dla znanych klas stanów przyjęto, że jako klasyfikator stanu zostanie użyta sieć neuronalna. Zastosowana sieć neuronalna była jednocześnie funkcją oceniającą osobniki w kolejnych iteracjach (pokoleniach) użytego algorytmu ewolucyjnego. Na potrzeby optymalizacji przyjęto, że:

- genotyp osobnika jest chromosomem zbudowanym z rzeczywistoliczbowego ciągu o długości odpowiadającej liczbie rozpatrywanych cech;
- fenotyp osobnika stanowi rozkład przykładów trenujących w przestrzeni cech relewantnych;
- populacje początkowe są generowane losowo;
- selekcja jest przeprowadzana metodą selekcji proporcjonalnej;
- sukcesja jest przeprowadzana według modelu elitarnego;
- krzyżowanie osobników jest przeprowadzane metodą krzyżowania jednopunktowego;
- wartości parametrów algorytmu są następujące:
  - liczba osobników jest stała i wynosi 30,
  - liczba rozpatrywanych cech jest równa max 7,
  - liczba pokoleń jest równa 50,
  - współczynnik krzyżowania wynosi 30 $[\%]$,
  - współczynnik mutacji wynosi 1 $[\%]$.

W wyniku optymalizacji otrzymano zbiory cech relewantnych, czyli cech, które niosą istotne informacje pozwalające na jak najlepsze rozpoznanie stanu technicznego diagnozowanego obiektu.

2.8. Identyfikacja modeli diagnostycznych

Przed przystąpieniem do budowy modelu należy dysponować zbiorami zmiennych procesowych (parametry pracy, sygnały sterujące, inne sygnały wejściowe, sygnały wyjściowe). Zbiory te powinny zostać

zarejestrowane podczas normalnej pracy obiektu lub podczas badań laboratoryjnych. Następnie wyznaczane są zbiory sygnałów diagnostycznych S^{dia} według jednej z metod [2.26]:

1. w wyniku oceny wartości zmiennej procesowej (np. kontrola granic alarmowych);
2. w wyniku wyliczenia i oceny wartości parametru zmiennej procesowej (np. szybkość zmian, średnia);
3. w wyniku kontroli związków jakościowych między zmiennymi procesowymi (np. relacje między wartościami zmiennych, zgodność kierunków zmian);
4. w wyniku wyliczenia i oceny residuum (rys. 2.1).

Zatem, w celu identyfikacji modelu diagnostycznego należy dysponować:

- zbiorem klas warunków działania,
- zbiorem danych uczących zawartym w zbiorze wartości cech sygnałów diagnostycznych,
- zbiorem danych testujących zawartym w zbiorze wartości cech sygnałów diagnostycznych.

Powyżej wymienione zbiory powinny być określone na drodze analizy badanego obiektu lub jego fragmentu, w przypadku identyfikowania modeli lokalnych.

Jeżeli dysponujemy gotowym zbiorem klas stanów Z wówczas nie trzeba przeprowadzać identyfikacji tego zbioru. W przeciwnym razie klasy stanów technicznych można wyznaczyć przeprowadzając na przykład analizę procesów resztkowych towarzyszących badanemu obiektowi. Zastosowanie wiedzy eksperckiej (np. zawartej w poradnikach, normach, zaleceniach itp.) lub wiedzy pozyskiwanej w sposób automatyczny ze zbiorów danych [2.35] pozwala na zdefiniowanie zbioru klas stanów Z. W przypadku metod pozyskiwania wiedzy do poszukiwania takiego zbioru można użyć na przykład metod grupowania [2.44, 2.42, 2.51, 2.47].

Kolejny krok identyfikacji modelu diagnostycznego polega na przeprowadzeniu operacji redukcji liczby cech sygnałów diagnostycznych. Podobnie jak w przypadku tworzenia zbioru klas stanów, tak i tutaj zbiór cech relewantnych można określić z użyciem wiedzy specjalistów lub z użyciem wiedzy pozyskiwanej automatycznie [2.9, 2.5]. W tym celu można użyć metody optymalizacji ewolucyjnej (rys. 2.20) lub poddać zbiór danych uczących analizie wrażliwości. Rozpoczynając analizę wrażliwości należy [2.39]:

- ustalić zbiór stanów technicznych Z i zbiór warunków działania W, które będą brane pod uwagę w analizie wrażliwości;
- określić interesujące, ze względów diagnostycznych, klasy stanu Z^k i klasy warunków działania W^k;
- przyporządkować rozpatrywane stany poszczególnym klasom stanu, a warunki działania danym klasom warunków działania;
- określić zbiór rozpatrywanych cech sygnałów diagnostycznych S_i^{dia} związany z modelem.

Następnie należy użyć jednego z pośród wielu algorytmów [2.40]:

- analiza wariancji;
- metody rangowe (np. nieparametryczny test Kruskala-Wallisa);
- metoda FAST (ang. Fourier Amplitude Sensitivity Test).

Budowę pojedynczego klasyfikatora stanu przeprowadza się na podstawie danych zawartych w:

- zbiorze klas warunków działania,
- zbiorze klas stanów,
- zbiorze cech relewantnych.

Do budowy klasyfikatora stanu można użyć jednej z wielu metod, np.:

- systemu ekspertowego [2.16],
- tablicy decyzyjnej [2.36],
- klasyfikacji i grupowania z użyciem miar odległości,
- sieci neuronalnej [2.29].

Budowa klasyfikatora może być przeprowadzana z nauczycielem lub bez nauczyciela. Najczęściej jest dostępny zbiór przykładów trenujących, w związku z tym budowa klasyfikatora jest przeprowadzana z nauczycielem. Sprawność otrzymanego klasyfikatora ocenia się na podstawie jego weryfikacji z użyciem danych testujących zawartych w zbiorze cech sygnałów diagnostycznych S^{dia}.

W przypadku użycia logiki rozmytej zakłada się, że na wejście identyfikowanego modelu podawane są dane o wartościach ostrych. Wartości tych danych w pierwszym etapie są rozmywane z użyciem zadanej funkcji rozmywania [2.50, 2.26, 2.7]. Rozmyte wartości danych stanowią wejście do systemu wnioskowania rozmytego. Następnie w wyniku działania układu wnioskującego otrzymujemy wektor stanów z przyporządkowanymi wartościami stopni przekonania o wystąpieniu danego stanu.

2.9. Proces diagnozowania

Na rys. 2.2 przedstawiono schemat prowadzenia procesu wnioskowania z wykorzystaniem diagnostyki symptomowej. Jak widać, proces tan składa się z kilku etapów. W kolejnych punktach opisane zostaną szczegóły dotyczące poszczególnych etapów.

2.9.1. Cechy sygnałów, symptomy

Według [2.14] proces wnioskowania diagnostycznego oparty jest o informacje pozyskane w wyniku prowadzenia obserwacji diagnozowanego obiektu. W wyniku prowadzonej obserwacji można uzyskać informacje dotyczące wielkości związanych z działaniem obserwowanego obiektu (np. temperatura pary w turbinie, czy natężenie przepływu pary) lub wielkości fizycznych związanych z procesami resztkowymi, powstającymi w czasie działania obserwowanego obiektu (np. poziom drgań obudowy podpory łożyska ślizgowego w turbozespole). Do opisu nośnika informacji pozyskiwanych z obiektu posługujemy się pojęciem sygnału, a dokładniej sygnału diagnostycznego. Skutecznym sposobem opisu sygnałów diagnostycznych są zbiory wartości cech takich sygnałów, które mogą być efektem przeprowadzonych analiz. Na przykład dla sygnałów rozpatrywanych jako proces stochastyczny, takimi cechami mogą być estymaty sygnału. W celu uporządkowania badań wprowadza się rozróżnienie pomiędzy klasami cech sygnałów oraz ich wartościami. Przykładem klasy cechy diagnostycznej może być *Temperatura czynnika roboczego*, a jego wartością liczba $40^{\circ}C$. Należy tutaj zwrócić uwagę, że wartości cech mogą należeć do różnych klas. Wartości cech sygnałów diagnostycznych, w ogólnym przypadku, mogą być wartościami punktowymi lub funkcyjnymi. Przykładem wartości punktowych może być *Maksymalna temperatura oleju silnika*, a wartości funkcyjnych *Gęstość rozkładu temperatury*. Zarówno sygnały diagnostyczne, jak również ich cechy rozpatrywane są w różnych dziedzinach np. dziedzinie czasu, częstotliwości czy dziedzinie modalnej. Sygnały będące wynikiem obserwacji badanego obiektu należy w dalszym kroku poddać analizie. Bazą do przeprowadzenia analizy jest przyjęcie odpowiedniego modelu sygnału. Można tutaj wyróżnić [2.14]:

- Uniwersalne modele sygnałów określane w postaci modeli niezależnych od badanego obiektu i obserwowanego sygnału (modele nieparametryczne).
- Modele bazujące na założeniu, że model może być pozyskany z analizowanych danych, bez potrzeby uwzględniania informacji o badanym obiekcie (np. modele autoregresyjne AR, z ruchomą średnią MA lub autoregresyjne z ruchomą średnią ARMA).
- Modele bazujące na założeniu, że model powinien uwzględniać specyficzne skutki wywołane działaniem badanego obiektu.

Szczegółowe metody analizy sygnałów można znaleźć w wielu publikacjach np. [2.6, 2.15, 2.14]. Wynikiem analizy sygnałów są wartości cech sygnałów, które w kolejnym kroku należy poddać działaniu klasyfikatora, którego wynikiem jest otrzymanie symptomów diagnostycznych. Ponieważ zdefiniowanie pojęcia symptom nie jest zadaniem prostym, przyjmuje się, że symptom jest objawem czegoś. W diagnostyce przyjęto, że symptom jest objawem wystąpienia jakiegoś stanu w obserwowanym obiekcie. Ponieważ te same symptomy mogą być objawami różnych stanów, w jakich może znaleźć się diagnozowany obiekt, przyjmuje się, że symptom jest rozumiany jako symptom klasy lub klas stanu. Dla określenia symptomów definiujących daną klasę stanów można przyjąć, że zgodne są chwilowe wartości sygnałów diagnostycznych i odpowiadającego tej klasie wzorca wartości cech sygnałów [2.30].

2.9.2. Detekcja uszkodzeń

Zagadnienia dotyczące detekcji i lokalizacji uszkodzeń są związane bardziej z diagnostyką procesów niż diagnostyką maszyn i urządzeń. Jednakże z uwagi na fakt, że należą one również do diagnostyki symptomowej zostały tutaj opisane. Detekcja uszkodzeń jest procesem, w którym sygnały diagnostyczne są generowane na podstawie zmiennych procesowych. W tym celu stosuje się algorytmy, których zadaniem jest wyodrębnienie z sygnałów diagnostycznych informacji o uszkodzeniach czyli symptomów. Metody detekcji uszkodzeń można podzielić na dwie grupy:

- metody wykorzystujące związki pomiędzy zmiennymi procesowymi,
- metody bazujące na kontroli parametrów zmiennych procesowych.

Pierwsza grupa metod wymaga pozyskania informacji o badanym obiekcie. Informacje takie są reprezentowane w postaci modeli ilościowych lub jakościowych, np. modele analityczne, neuronowe czy rozmyte. Dane te można również uzyskać badając związki pomiędzy zmiennymi procesowymi. Do tej grupy metod można zaliczyć metody w których wykorzystuje się modele obiektów budowane z wykorzystaniem na przykład [2.30]:

- równań fizycznych,
- transmitancji obiektu,
- równań stanu,
- na podstawie obserwatorów stanu,
- identyfikacji on-line,
- modeli neuronowych i rozmytych.

Kolejna grupa metod do wykrywania symptomów uszkodzeń wykorzystuje analizę wyłącznie jednej zmiennej procesowej. Analizując przebieg zmian takiej zmiennej sprawdza się, czy nie zostały przekroczone narzucone wartości graniczne, dopuszczalna szybkość zmian sygnału itp. Prowadzi się również analizę stochastyczną lub spektralną. Celem prowadzenia takich analiz jest uchwycenie zmian zachodzących w sygnale diagnostycznym, które to mogą być symptomami uszkodzeń. Metody stosowane w tej grupie wykorzystują między innymi [2.30]:

- redundancję sprzętową,
- sygnały sprzężeń zwrotnych,
- związki statystyczne pomiędzy zmiennymi procesowymi,
- relacje między zmiennymi procesowymi,
- analizę sygnałów i kontrolę ograniczeń,
- parametry statystyczne sygnałów,
- analizę spektralną.

2.9.3. Lokalizacja uszkodzeń

Na podstawie sygnałów diagnostycznych generowanych przez algorytmy detekcyjne prowadzony jest kolejny krok - lokalizacja uszkodzeń. Lokalizacja uszkodzeń, podobnie jak detekcja uszkodzeń, dotyczy głównie zadań diagnostycznych prowadzonych w diagnostyce procesów. Jej wynikiem jest wskazanie miejsca w obiekcie, gdzie wystąpiło uszkodzenie lub wskazanie stanu obiektu. Aby można było to wykonać konieczna jest znajomość relacji pomiędzy symptomami i stanami obiektu. Ponieważ wiedza na temat obiektów może być niepełna lub niepewna, nie zawsze udaje się jednoznacznie wskazać uszkodzenie. Problemy z tym związane wynikają również z ograniczonej rozróżnialności klas stanów i niepewnością sygnałów diagnostycznych. Istnieje duża różnorodność metod lokalizacji uszkodzeń. W pracy [2.30] wyróżniono między innymi metody:

- w których relacje wynikają ze struktury zastosowanych modeli matematycznych,
- wymagające określenia relacji w fazie uczenia,
- bazujące na wiedzy specjalistów,
- wykorzystujące funkcje logiczne,
- oparte na regułach,
- oparte o sieci neuronowe,
- rozpoznawania obrazów.

Bibliografia

[2.1] Arabas J. *Wykłady z algorytmów ewolucyjnych*. Wydawnictwa Naukowo-Techniczne, Warszawa 2001.

[2.2] Basseville M., Abdelghani M., Beneveniste A. *Subspace-based fault detection algorithms for vibration monitoring*, wolumen 36/1.

[2.3] Bednarski M. *Metody doskonalenia sieci bayesowskich stosowanych w diagnostycznych systemach doradczych*. Zeszyt 131. Katedra Podstaw Konstrukcji Maszyn Politechniki Śląskiej, Gliwice, 2006.

[2.4] Cempel Cz. *Podstawy wibroakustycznej diagnostyki maszyn*. WNT, Warszawa, 1982.

[2.5] Cempel Cz. *Diagnostyka wibroakustyczna maszyn*. PWN, Warszawa, 1989.

[2.6] Cempel Cz., Tomaszewski F., redaktorzy. *Diagnostyka maszyn. Zasady ogólne. Przykłady zastosowań*. Międzyresortowe Centrum Naukowe Eksploatacji Majątku Trwałego, Radom, 1992.

[2.7] Cholewa W. *Metoda diagnozowania maszyn z zastosowaniem zbiorów rozmytych*. Mechanika. Zeszyty Naukowe Politechniki Śląskiej. Zeszyt 79. Wydawnictwo Politechniki Śląskiej, Gliwice, 1983.

[2.8] Cholewa W. Diagnostyczne modele obiektów. Kiciński J., redaktor, *Modelowanie i diagnostyka oddziaływań mechanicznych, i magnetycznych w turbozespołach energetycznych*, strony 27–52, Gdańsk, 2005. Wydawnictwo IMP PAN.

[2.9] Cholewa W. Relewantne cechy sygnałów. Kiciński J., redaktor, *Modelowanie i diagnostyka oddziaływań mechanicznych, i magnetycznych w turbozespołach energetycznych*, strona 1261–1296, Gdańsk, 2005. Wydawnictwo IMP PAN. r. 26.

[2.10] Cholewa W., Kaźmierczak J. *Diagnostyka techniczna maszyn. Przetwarzanie cech sygnałów*. Skrypt uczelniany 1904. Wydawnictwo Politechniki Śląskiej, Gliwice 1995.

[2.11] Cholewa W., Kaźmierczak J. *Data Processing and Reasoning in Technical Diagnostics*. WNT, Warszawa 1995.

[2.12] Cholewa W., Kiciński J. *Odwrotne modele diagnostyczne*. Wydawnictwo Politechniki Śląskiej, Gliwice, 1997.

[2.13] Cholewa W., Kiciński J. *Diagnostyka techniczna. Metody odwracania nieliniowych modeli obiektów*. Mechanika. Zeszyty Naukowe Politechniki Śląskiej. Zeszyt 120. Wydawnictwo Politechniki Śląskiej, Gliwice 2001.

[2.14] Cholewa W., Korbicz J., Moczulski W., Timofiejczuk A. Metody analizy sygnałów. Korbicz J., Kościelny J. M., Kowalczuk Z., Cholewa W., redaktorzy, *Diagnostyka procesów. Modele, metody sztucznej inteligencji, zastosowania*, strony 115–146. WNT, Warszawa 2002.

[2.15] Cholewa W., Moczulski W. *Diagnostyka techniczna maszyn. Pomiary i analiza sygnałów*. Skrypt uczelniany 1758. Politechnika Śląska, 1993.

[2.16] Cholewa W., Pedrycz W. *Systemy doradcze*. Skrypt uczelniany 1447. Wydawnictwo Politechniki Śląskiej, Gliwice 1987.

[2.17] Cholewa W., White M.F. *Application of neural networks for inversing of vibration models*. Mechanika. Zeszyty Naukowe Politechniki Śląskiej. Zeszyt 116. Wydawnictwo Politechniki Śląskiej, Gliwice, 1994.

[2.18] Evans G. W., Wallace G. F., Sutherland G. L. *Symulacja na maszynach cyfrowych*. WNT, Warszawa 1973.

[2.19] Frisk E. *Model-based fault diagnosis applied to an SI-Engine*. Praca doktorska, Examensarbete utfört i Fordonssystem vid Tekniska Högskolan i Linköping, Linköping, 1996.

[2.20] Isermann R. Model-based fault detection and diagnosis. Status and applications. *IFAC Committee SAFEPROCESS*, 2004.

[2.21] Isermann R. Model-based fault detection and diagnosis. Status and applications. *Annual Reviews in Control, vol. 29*, strony 71–85, 2005.

[2.22] Isermann R., Ballé P. Terminology in the field of supervision, fault detection and diagnosis. *IFAC Committee SAFEPROCESS*, 1996.

[2.23] Kiciński J., redaktor. *Modelowanie i diagnostyka oddziaływań mechanicznych, i magnetycznych w turbozespołach energetycznych*, Gdańsk, 2005. Wydawnictwo IMP PAN.

[2.24] Kiciński J. Symptomy diagnostyczne turbozespołów energetycznych określone metodą komputerowej i analogowej symulacji ich defektów. *Mat. Ogólnopolskiego Seminarium Wibrodiagnostyka turbozespołów energetycznych*, strony 51–92, Gdańsk 1994.

[2.25] Klimek A. *Metody doskonalenia odwrotnych modeli diagnostycznych*. Mechanika. Zeszyty Naukowe Politechniki Śląskiej. Zeszyt 134. Wydawnictwo Politechniki Śląskiej, Gliwice 1999.

[2.26] Kościelny J. M. *Diagnostyka zautomatyzowanych procesów przemysłowych*. Akademicka Oficyna Wydawnicza EXIT, Warszawa 2001.

[2.27] Kościelny J. M. Modele w diagnostyce procesów. Korbicz J., Kościelny J. M., Kowalczuk Z., Cholewa W., redaktorzy, *Diagnostyka procesów. Modele, metody sztucznej inteligencji, zastosowania*, strony 29–56. WNT, Warszawa 2002.

[2.28] Kościelny J. M., Syfert M. Current diagnostics of power boiler system with use of fuzzy logic. *Proc. 4th IFAC Symp. Fault Detection, Supervision and Safety for Technical Process. SAFEPROCESS 2000*, 2:681–686, 2000.

[2.29] Korbicz J. Sztuczne sieci neuronowe i ich zastosowanie w diagnostyce procesów przemysłowych. *Pomiary Automatyka Kontrola*, 4:129–133, 1998.

[2.30] Korbicz J., Kościelny J. M., Kowalczuk Z., Cholewa W., redaktorzy. *Diagnostyka procesów. Modele, metody sztucznej inteligencji, zastosowania*. WNT, Warszawa 2002.

[2.31] Leray P., Francois O. BNT Structure Learning Package: Documentation and Experiments. Laboratoire PSI - INSA Rouen- FRE CNRS 2645, BP 08 - Av. de l'Université, 76801 St-Etienne du Rouvray Cedex, 15th November 2004.

[2.32] Martin F. F. *Wstęp do modelowania cyfrowego*. PWN, Warszawa 1970.

[2.33] Michalewicz Z. *Algorytmy genetyczne + struktury danych = programy ewolucyjne*. WNT, Warszawa, 1999.

[2.34] Moczulski W. Knowledge discovery in diagnostic databases. *Proc 2nd Symp. Methods of Artificial Intelligence in Mechanics and Mechanical Engineering, AI-Mech, Gliwice*, 2:149–154, 2001.

[2.35] Moczulski W. *Metody pozyskiwania wiedzy dla potrzeb diagnostyki maszyn*. Mechanika. Zeszyty naukowe Politechniki Śląskiej. Zeszyt 130. Wydawnictwo Politechniki Śląskiej, Gliwice 1997.

[2.36] Pollack S. L., Hicks H. T. Jr, Harrison W. J. *Tablice decyzyjne*. PWN, Warszawa 1975.

[2.37] Psiuk K. *Obiektowe modele procesu propagacji stanów w układach maszyn*. Zeszyt 119. Katedra Podstaw Konstrukcji Maszyn Politechniki Śląskiej, Gliwice 2001.

[2.38] Radkowski S. *Wibroakustyczna diagnostyka uszkodzeń niskoenergetycznych*. Biblioteka Problemów Eksploatacji. Warszawa-Radom, 2002.

[2.39] Rzydzik S. *Identyfikacja stanu w układach rozproszonych*. Zeszyt 135. Katedra Podstaw Konstrukcji Maszyn Politechniki Śląskiej, Gliwice, 2007.

[2.40] Sławik D. *Metody badania wrażliwości cech sygnałów diagnostycznych*. Zeszyt 126. Katedra Podstaw Konstrukcji Maszyn Politechniki Śląskiej, 2006.

[2.41] Schwall M. L., Gerdes J. C., Bäker B., Forchert T. A probabilistic vehicle diagnostic system using multiple models. 2003.

[2.42] Sobczak W., Malina W. *Metody selekcji i redukcji informacji*. WNT, Warszawa, 1985.

[2.43] Sreedharan P., Haves P. Comparison of chiller models for use in model-based fault detection. *International Conference for Enhanced Building Operations, Austin, July 17*, 2001.

[2.44] Tadeusiewicz R., Flasiński M. *Rozpoznawanie obrazów*. Współczesna nauka i technika. Informatyka. Wydawnictwo naukowe PWN, Warszawa, 1991.

[2.45] Uhl T. Zastosowanie analizy modalnej w diagnostyce. *Diagnostyka t. 10*, strony 24–32.

[2.46] Urbanek G. *Zastosowanie algorytmów ewolucyjnych w identyfikacji odwrotnych modeli diagnostycznych*. Zeszyt 132. Katedra Podstaw Konstrukcji Maszyn Politechniki Śląskiej, Gliwice, 2006.

[2.47] Urbanek G. Grupowanie, klasyfikacja, selekcja. `http://https://kpkm.polsl.pl/PROJEKTY/Klas/`, 2007.

[2.48] Wojtusik J. *Wielomodele diagnostyczne maszyn wirnikowych*. Zeszyt 128. Katedra Podstaw Konstrukcji Maszyn Politechniki Śląskiej, Gliwice, 2006.

[2.49] Wydawnictwo Naukowe PWN. *Encyklopedia Popularna*. PWN, Warszawa 1992.

[2.50] Zadeh L. A. Fuzzy sets. *Information and Control*, 8 (3):338–353, 1965.

[2.51] Zahn C. T. Graph-theoretical methods for detecting and describing gestalt clusters. *IEEE Transactions on Computers*, 1:68–86, 1971.

[2.52] Żółtowski B. *Podstawy diagnostyki maszyn*. Wydawnictwo Uczelniane ATR, Bydgoszcz, 1996.

[2.53] Żółtowski B., Ćwik Z. *Leksykon diagnostyki technicznej*. Wydawnictwo Uczelniane Akademii Techniczno-Rolniczej, Bydgoszcz, 1996.

Rozdział 3

Analiza niezawodności i bezpieczeństwa maszyn i instalacji

Kazimierz T. KOSMOWSKI, Jacek ZAWALICH

3.1. Wprowadzenie

Racjonalne *zarządzanie niezawodnością i bezpieczeństwem* złożonego obiektu (systemu) technicznego, na przykład maszyny krytycznej w postaci turbiny energetycznej, wymaga zastosowania odpowiednich metod modelowania probabilistycznego wraz ze staranną analizą danych wejściowych i oceną uzyskanych wyników. Parametrami modelu probabilistycznego systemu, na przykład jego nieuszkadzalności lub niegotowości [3.27], są m.in. intensywności uszkodzeń różnych kategorii elementów lub podsystemów, które pozyskuje się zwykle z różnych źródeł danych niezawodnościowych.

Do wyznaczania *funkcji intensywności uszkodzeń* elementów (podsystemów) wskazane jest korzystanie z danych statystycznych dotyczących przebiegu eksploatacji i uszkodzeń obiektów identycznych lub podobnych, eksploatowanych przez dłuższy czas w zbliżonych warunkach środowiskowych. Nie jest to jednak możliwe w przypadku nowoprojektowanych obiektów. Wówczas korzysta się z dostępnych baz danych niezawodnościowych o charakterze ogólnym, dokonując odpowiedniej korekty funkcji intensywności uszkodzeń dla przewidywanych warunków środowiskowych [3.34], [3.33].

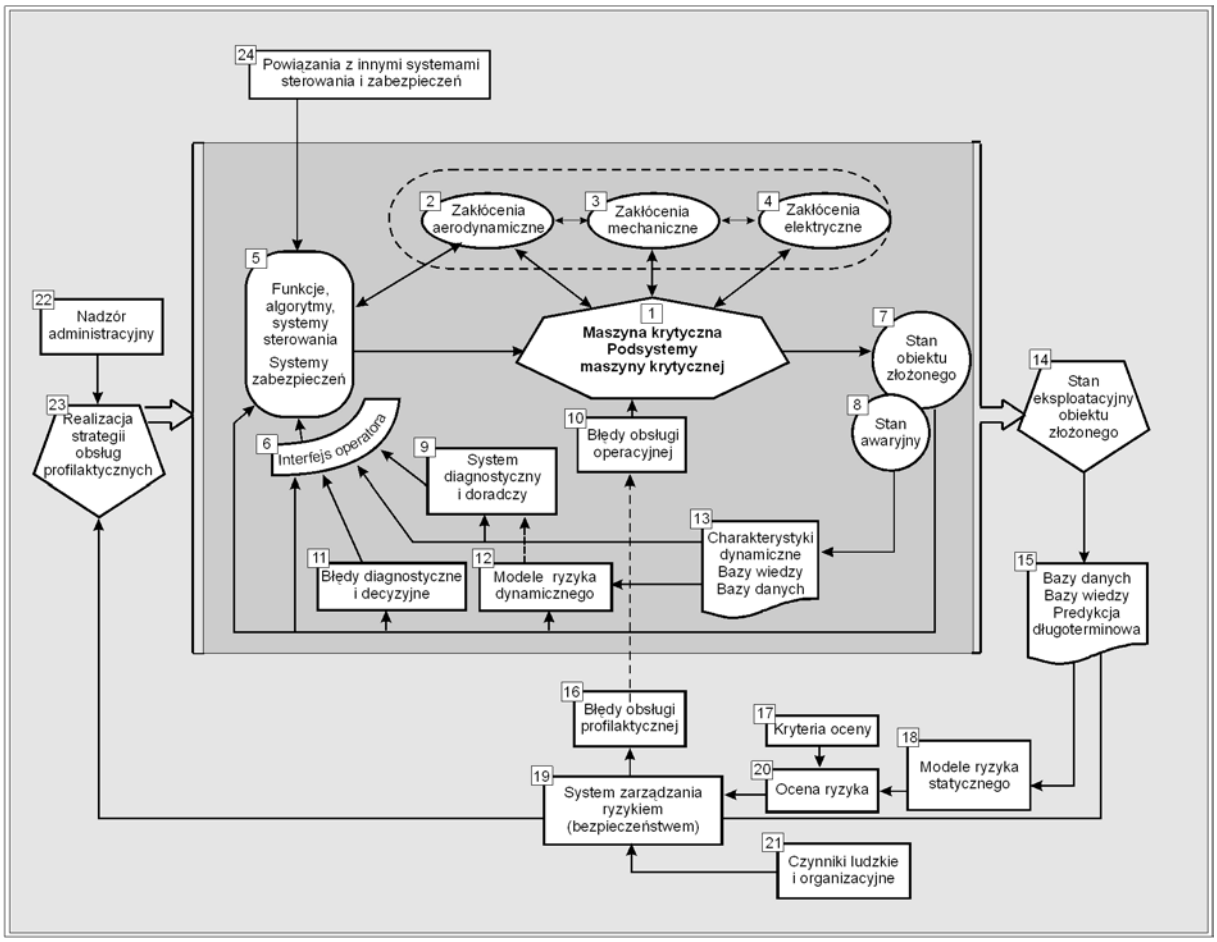
W przypadku niektórych obiektów lub podsystemów przyjmuje się często założenie o stałej w czasie funkcji intensywności uszkodzeń ($\lambda(t) = \lambda = const$), co znacznie ułatwia modelowanie probabilistyczne [3.23], [3.24], [3.26]. Założenie to jest uzasadnione w przypadkach niewystępowania procesów zużycia i starzenia materiałów. Również inne parametry modelu probabilistycznego podsystemu – jak na przykład: intensywność odnowy, pokrycie diagnostyczne, czy też czas pomiędzy przeprowadzaniem testów sprawności funkcjonalnej elementów wyposażenia – wyznacza się często, ze względu na brak danych z przebiegu eksploatacji, korzystając z różnych źródeł danych niezawodnościowych. Uwzględnia się niekiedy w oszacowaniach tych parametrów opinie ekspertów [3.19].

Zarządzanie bezpieczeństwem opiera się na analizie i ocenie ryzyka [3.17], [3.21], [3.31], [3.1]. Analiza ryzyka obejmuje wyznaczenie miary prawdopodobieństwa lub częstości rozważanych scenariuszy awaryjnych [3.9]. Każdy zdefiniowany scenariusz awaryjny obejmuje określone straty, które szacuje się na podstawie odpowiednich metod modelowania procesów (tzw. modelowanie deterministyczne procesów fizycznych i/lub chemicznych), przy czym korzysta się również często z opinii ekspertów. Jakość tych opinii, wpływa zwykle istotnie na założenia dotyczące modelu ryzyka i jego parametrów, a zatem jego wiarygodność i przydatność uzyskanych wyników w podejmowaniu decyzji.

Każdy współczesny obiekt techniczny wyposaża się w systemy sterowania i zabezpieczeń, które wpływają istotnie na niezawodność i bezpieczeństwo całego systemu [3.6], [3.17], [3.22], [3.1]. Zakres zarządzania niezawodnością i ryzykiem złożonej maszyny krytycznej na przykładzie turbiny dużej mocy zainstalowanej w elektrowni w procesie jej eksploatacji przedstawiono na Rys.3.1. Zarządzanie

bezpieczeństwem złożonego obiektu przeprowadza się w całym cyklu życia [3.10], [3.12], [3.13].

Maszyna krytyczna (1) na Rys.3.1 składa się z wielu podzespołów, układów i elementów, których zadaniem jest poprawne prowadzenie danego procesu technologicznego. Jest ona sterowana za pomocą dedykowanych algorytmów wyposażonych często w złożone systemy sterowania i zabezpieczeń (5). Na maszynę krytyczną działają w sposób ciągły zakłócenia aerodynamiczne (2), mechaniczne (3) oraz elektryczne (4). Stan (7) takiej maszyny krytycznej, zainstalowanej na przykład w elektrowni konwencjonalnej, oraz jej podsystemów działających podczas eksploatacji, jest określany na podstawie bieżących pomiarów istotnych wielkości fizycznych, aby w razie potrzeby podjąć działania niezbędne do utrzymania jej w dozwolonych warunkach pracy.



Rys. 3.1: Zarządzanie niezawodnością i bezpieczeństwem złożonej maszyny krytycznej na podstawie ocen ryzyka

Ciągła kontrola stanu elementów maszyny krytycznej poprzez pomiary istotnych wielkości fizycznych i parametrów diagnostycznych oraz śledzenie ich trendów pozwala na wykrycie stanu nienormalnego (8), prognozowanie stanów przyszłych i podjęcie w razie potrzeby przeciwdziałania eliminującego potencjalne zdarzenie awaryjne lub redukującego jego skutki. Baza wiedzy (13), zawierająca m.in. charakterystyki dynamiczne oraz inne istotne informacje, w połączeniu z informacją o aktualnym stanie maszyny krytycznej, pozwalają na uaktualnienie parametrów modelu ryzyka dynamicznego (12), jak również uruchomienie odpowiednich funkcji systemu diagnostycznego o charakterze doradczym (9). Ostateczną decyzję o rodzaju i wielkości sterowania podejmuje operator za pośrednictwem interfejsu operatora (6), który ma bezpośredni dostęp do syntetycznej informacji o właściwościach i dynamicznych charakterystykach maszyny oraz do aktualnego jej stanu, łącznie z ewentualnymi alarmami i bieżącymi ocenami diagnostycznymi oraz propozycjami decyzyjnymi.

Na algorytmy oraz funkcje sterowania wpływają powiązania sygnałowe (24) z innymi systemami sterowania i systemami zabezpieczeniowymi. Drugi zewnętrzny tor powiązań ilustruje wpływ systemu zarządzania ryzykiem (19), który wykorzystuje informacje o stanie eksploatacyjnym obiektu złożonego (14) i bazę wiedzy z elementami predykcji długoterminowej (15). Opracowane modele ryzyka długoterminowego (statycznego) (18) wraz z przyjętymi kryteriami (17) umożliwiają uaktualnioną analizę ryzyka i wypracowanie oceny ryzyka niezbędnej do dalszego wykorzystania w systemie zarządzania bezpieczeństwem.

Na system ten mają również wpływ czynniki ludzkie i organizacyjne, które są główną przyczyną od 70 do 90% wypadków i zdarzeń awaryjnych, zależnie od kategorii obiektu złożonego [3.19], i powinny być dlatego starannie uwzględnione w analizie i oszacowaniach ryzyka. System zarządzania bezpieczeństwem wypracowuje wytyczne odnośnie testów funkcjonalności układów krytycznych, ich okresów eksploatacji do remontów lub ewentualnej wymiany. Powstające błędy obsługi profilaktycznej (16) bezpośrednio oddziałują na błędy obsługi operacyjnej (10) związanej z danym podukładem maszyny krytycznej lub konkretnych jej elementów. Realizacja strategii obsług profilaktycznych (23) odbywa się pod nadzorem administracyjnym (22) i ma istotny wpływ na bezpieczeństwo całej maszyny krytycznej.

Decyzje natury technicznej, organizacyjnej i ekonomicznej w cyklu życia danego obiektu złożonego podejmuje się na podstawie uzyskanych oszacowań ryzyka oraz analizy kosztów i efektów rozważanych (zidentyfikowanych) opcji sterowania ryzykiem (OSR) [3.19]. OSR mogą obejmować przedsięwzięcia natury technicznej i/lub organizacyjnej, które rozważa się już na etapie projektowania obiektu złożonego, a następnie na etapie jego eksploatacji. W podejmowaniu racjonalnych decyzji podczas eksploatacji istotne znaczenie ma informacja o stanie technicznym elementów i podsystemów uzyskana na podstawie odpowiednio zaplanowanych i przeprowadzonych badań diagnostycznych [3.2], [3.4], [3.5], [3.8], [3.16], [3.15], [3.25], [3.35].

Problematyka niezawodności i bezpieczeństwa ma coraz większe znaczenie w eksploatacji systemów technicznych. Zagadnienia te ujmują niektóre dyrektywy europejskie i krajowe akty prawne w postaci ustaw i rozporządzeń w kontekście wymagań dotyczących szeroko rozumianej jakości (projekt, wyrób, usługa itd.), ochrony środowiska przyrodniczego i bezpieczeństwa (pracy systemu, działalności gospodarczej, informacji itd.) [3.7], [3.32]. W przedsiębiorstwach wprowadza się zintegrowane systemy zarządzania jakością, środowiskiem i bezpieczeństwem. W takim szerokim ujęciu należy również spojrzeć na system zarządzania procesem eksploatacji w przedsiębiorstwie, który powinien obejmować system oceny ryzyka i diagnostyki technicznej wraz z zagadnieniami niezawodności [3.2], [3.3], [3.14], [3.21], [3.12].

W normach technicznych dotyczących zagadnień niezawodności i bezpieczeństwa formułuje się m.in. kryteria probabilistyczne, jakie powinny spełniać proponowane rozwiązania. Do takich norm można zaliczyć normę bezpieczeństwa funkcjonalnego IEC 61508 [3.12] i jej krajowy odpowiednik PN-EN 61508 [3.30] oraz normę dotyczącą bezpieczeństwa funkcjonalnego maszyn EN 62061 [3.13]. Części 1, 2, 3 i 4 normy IEC 61508 są bazowymi publikacjami bezpieczeństwa (IEC *basic safety publications*). Jednym z obowiązków *Komitetów Technicznych IEC* jest to, aby kiedykolwiek jest to możliwe, stosować te części norm sektorowych (w tym norm dotyczących konkretnych produktów), które zawierają w swoich ramach systemy E/E/PE związane z bezpieczeństwem (szczegóły zawiera IEC *Guide* 104).

Wprowadzenie norm serii IEC 61508 do zbioru EN poprzedziły dyskusje na forum CENELEC. W listopadzie 1999 r. po zebraniu ekspertów został wydany dokument CLC/BTWG/99-2/004: Raport wewnętrzny do CENELEC 102 BT od CLC/BTWG 99-2 dotyczący dyrektyw UE, bezpieczeństwa funkcjonalnego i roli normalizacji CENELEC. Praca Grupy Roboczej i raport dotyczyły rozpatrzenia zagadnienia bezpieczeństwa funkcjonalnego w świetle *Dyrektyw Nowego Podejścia* LVD, ATEX, MDD, MD, EMC [3.21]. W raporcie tym znalazły się zalecenia dotyczące akceptacji wprowadzenia rodziny norm 61508 do zbioru EN, norm sektorowych i raportu technicznego na temat aspektów kompatybilności elektromagnetycznej w bezpieczeństwie funkcjonalnym. W efekcie w grudniu 2001r., cała seria IEC 61508 została wprowadzona do zbioru norm europejskich. Jak wiadomo, kraje członkowskie

CENELEC, w tym Polska, są zobowiązane do przyjmowania norm europejskich EN bez jakichkolwiek zmian.

Prace badawcze zorientowane na opracowanie i wdrożenie technologii innowacyjnych w przemyśle, dotyczących urządzeń, instalacji, systemów sterowania i zabezpieczeń, oprogramowania i wspomaganych komputerowo systemów zarządzania powinny uwzględniać wspominane wymagania o charakterze ogólnym (dyrektywy europejskie i krajowe akty prawne) oraz kryteria formułowane w normach zharmonizowanych z tymi dyrektywami i innych normach technicznych, szczególnie krajowych. Europejskie normy techniczne nie zawsze mają charakter obligatoryjny. Jednak, jeżeli dotyczą one zagadnień bezpieczeństwa, powinny być one respektowane, szczególnie, jeśli zawierają wskazania dobrej praktyki inżynierskiej [3.21].

Zasadne jest, jeśli wykonane prace badawcze dotyczące zagadnień bezpieczeństwa w nawiązaniu do praktyki zarządzania ryzykiem z uwzględnieniem zagadnień diagnostyki technicznej były przydatne w opracowaniu lub uaktualnianiu norm technicznych. Przykładem takiej pracy finansowanej z programu badawczego UE jest projekt RIMAP [3.14], którego drugi etap ma zakończyć się opracowaniem normy europejskiej. Wyniki uzyskane podczas realizacji projektu DIADYN, w tym niniejszego rozdziału, będzie można wykorzystać w opracowaniu części takiej normy w zakresie zintegrowanego zarządzania bezpieczeństwem dużych maszyn krytycznych w cyklu życia.

W większości sytuacji odpowiedni poziom bezpieczeństwa uzyskuje się za pomocą pewnej liczby systemów zabezpieczeń, które wykorzystują różne techniki (na przykład mechaniczną, hydrauliczną, pneumatyczną, elektryczną, elektroniczną, programowalną elektroniczną). Dlatego też każda strategia bezpieczeństwa oparta na zarządzaniu ryzykiem musi rozpatrzyć nie tylko elementy wchodzące w skład danego systemu (na przykład czujniki, urządzenia sterujące i urządzenia wykonawcze), lecz także inne systemy związane z bezpieczeństwem tworzące całościowy zestaw systemów wiążących się z bezpieczeństwem [3.21], [3.12].

Ze względu na dynamikę rozwoju technologii innowacyjnych wzrasta znaczenie współpracy środowiska naukowego i kadry inżynieryjnej w przedsiębiorstwach. Współpraca ta wymaga posługiwania się zrozumiałym wzajemnie językiem specjalistycznym, zawierającym zbiór podstawowych terminów i określeń. W rozdziale następnym zestawiono, w nawiązaniu do zawartości odpowiednich norm krajowych i międzynarodowych, ważniejsze terminy i określenia oraz przedstawiono niektóre problemy analizy niezawodności i bezpieczeństwa maszyn i instalacji krytycznych.

3.2. Niezawodność i nieuszkadzalność obiektów technicznych

Duże znaczenie w porządkowaniu terminów, określeń i definicji dotyczących niezawodności ma norma PN-93/N-50191 [3.27], w której dokonano próby przetłumaczenia na język polski terminologii w języku angielskim, przyjętej przez zespół ekspertów w normie międzynarodowej IEC 60050(191):1990.

Przyjęto, że *obiektem* (ang. *item, entity*) jest dowolna część składowa, element, przyrząd, podsystem, jednostka funkcjonalna, urządzenie lub system, które mogą być rozpatrywane indywidualnie. Obiekt może być *naprawialny* (ang. *repaired item*), jeśli możliwa jest w określonych warunkach jego naprawa po wystąpieniu uszkodzenia.

Funkcja wymagana (ang. *required function*) jest to zdefiniowana funkcja lub zespół funkcji, których wypełnienie przez dany obiekt jest niezbędne do wykonania określonego *zadania* lub *misji*. Oczywiście obiekt taki musi być odpowiednio zaprojektowany, spełniając założenia i wymagania podane w *specyfikacji technicznej*, a następnie wykonany i użytkowany (eksploatowany) z dotrzymywaniem przyjętych kryteriów jakościowych w danych warunkach zewnętrznych i środowiskowych.

Eksploatacja (ang. *operation*) jest zespołem wszystkich działań technicznych i organizacyjnych, mających na celu umożliwienie obiektowi wypełnianie wymaganych funkcji, włącznie z niezbędnym dostosowaniem do zmian warunków zewnętrznych.

Skuteczność (efektywność w *działaniu*) (ang. *effectiveness*) jest zdolnością obiektu do wykonania żądanej funkcji (lub usługi) zgodnie z podanymi charakterystykami ilościowymi. Natomiast *trwałość*

(ang. *durability*) dotyczy zdolności obiektu do wypełnienia wymaganych funkcji w danych warunkach użytkowania i obsługiwania, aż do osiągnięcia stanu granicznego.

Zdefiniowano w tej normie również *wskaźnik* lub *miarę* (ang. *measure*) w odniesieniu do probabilistycznego opisu niezawodności, który jest funkcją lub wielkością używaną do opisu zmiennej losowej lub procesu losowego. Wyróżniono następujące właściwości szeroko rozumianego obiektu:

Niezawodność (ang. *dependability*) definiuje się jako zespół właściwości, które opisują gotowość obiektu i wpływające na nią: nieuszkadzalność, obsługiwalność i zapewnienie środków obsługi (termin niezawodność powinien być używany do ogólnego nieliczbowego opisu obiektu).

Zdolność do działania (ang. *capability*) jest zdolnością obiektu do wykonania żądanego zadania lub usługi zgodnie z danymi charakterystykami ilościowymi, w danych warunkach zewnętrznych (w odniesieniu do usług telekomunikacyjnych właściwość ta nazywa się *przepustowością*).

Nieuszkadzalność (ang. *reliability*) definiuje się jako zdolność obiektu do wypełnienia wymaganych funkcji w danych warunkach i w określonym przedziale czasu. Natomiast *gotowość; dyspozycyjność* (ang. *availability*) jest zdolnością obiektu do utrzymywania się w stanie umożliwiającym wypełnianie wymaganych funkcji w danych warunkach i określonej chwili lub w rozważanym przedziale czasu, przy założeniu, że zapewniono odpowiednie warunki zewnętrzne (zdolność ta zależy łącznie od nieuszkadzalności, obsługiwalności i zapewnienia środków obsługi obiektu).

Obsługiwalność; podatność na obsługę (ang. *maintainability*) jest zdolnością obiektu do utrzymywania lub odtwarzania stanu zdatności w danych warunkach eksploatacji, w którym może on wypełniać wymagane funkcje, przy założeniu, że obsługa jest przeprowadzana w określonych warunkach z zachowaniem ustalonych procedur i środków.

Nieuszkadzalność (nie powinna być utożsamiana z *niezawodnością*) jest więc zdolnością obiektu (wyrobu, systemu) do wypełnienia wymaganych funkcji w danych warunkach (zadany poziom maksymalnych obciążeń i narażeń w określonych warunkach środowiskowych) w danym przedziale czasu. Miarę tej zdolności wyraża się liczbowo na przykład jako *prawdopodobieństwo poprawnego wypełniania wymaganej funkcji* $P(t)$ w rozważanym przedziale czasu [0, t]. Prawdopodobieństwo to jest funkcją czasu i przy założeniu, że obiekt jest nienaprawialny w tym umownym przedziale czasu, wyraża się za pomocą znanego wzoru

$$P(t) = \exp[-\int_0^t \lambda(\tau)d\tau] \tag{3.1}$$

gdzie: $\lambda(t)$ jest funkcja intensywności uszkodzeń, definiowaną jako częstość uszkodzeń obiektów w przedziale czasu Δt od chwili t, przy warunku, że obiekt był sprawny do chwili t

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P\{t < T \leqslant t + \Delta t | T > t\}}{\Delta t} \tag{3.2}$$

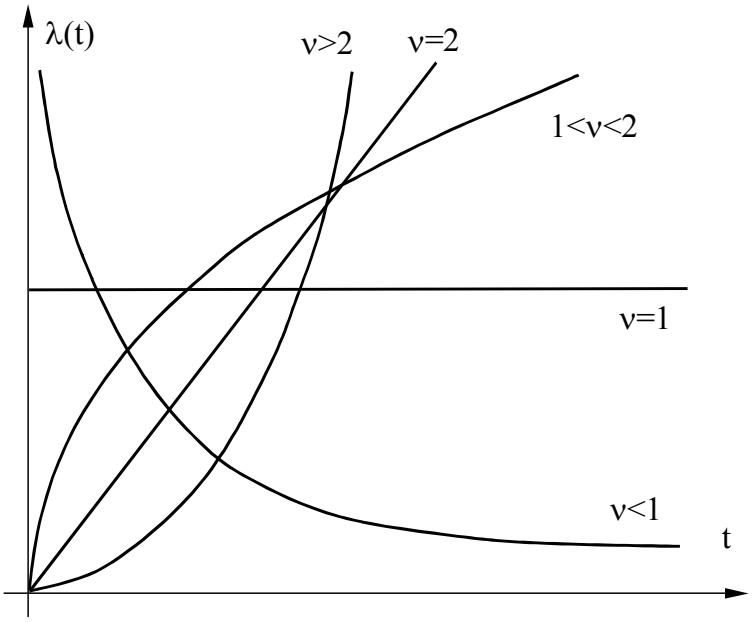
przy czym: T jest zmienną losową trwałości typu ciągłego, określającą czas przebywania obiektu prostego w stanie zdatności funkcjonalnej.

W badaniach niezawodności duże znaczenie ma rozkład Weibulla zmiennej losowej T. Funkcję intensywności uszkodzeń dla takiego rozkładu określa wzór

$$\lambda(t) \; = \; (\nu/b) \; (\mathrm{t} \; / \; \mathrm{b})^{\nu-1} \tag{3.3}$$

gdzie: b jest współczynnikiem skali, wyrażanym w jednostkach czasu, np. w *godz.*, a ν jest bezwymiarowym współczynnikiem kształtu. Na Rys.3.2 przedstawiono wykresy funkcji intensywności uszkodzeń dla różnych wartości współczynnika kształtu

Jak widać na Rys.3.2 dla współczynnika kształtu o wartości $\nu = 1$ uzyskano stałą w czasie funkcję intensywności uszkodzeń $\lambda(t) = \lambda = const$, identycznie jak w przypadku rozkładu wykładniczego. Rozkład wykładniczy jest, więc szczególnym przypadkiem rozkładu Weibulla. Rozkład wykładniczy ma duże znaczenie w analizie niezawodności, szczególnie w przypadku elementów elektronicznych i elektrycznych, w których nie występują procesy zużycia. Jeśli będą występować w nich od pewnego



Rys. 3.2: Wykresy funkcji intensywności uszkodzeń rozkładu Weibulla dla różnych wartości współczynnika kształtu ν

czasu procesy starzenia materiałów, wówczas może być celowe w analizie trwałości zastosowanie innych rozkładów probabilistycznych.

Jeżeli oszacowanie parametru intensywności uszkodzeń rozkładu wykładniczego przeprowadza się na podstawie badania losowej próbki obiektów, pracujących w określonych warunkach środowiskowych, o liczności *n* do chwili t_B, przed którą wystąpiło *m*-te uszkodzenie, wówczas otrzymuje się, korzystając z metody największej wiarogodności, następujące oszacowanie nieznanej wartości parametru λ_B^*

$$\lambda_B^* = \frac{m}{Z(t_B)} \tag{3.4}$$

przy czym wartość $Z(t_B)$ określa wzór

$$Z(t_B) = \sum_{i=1}^{m} t_{(i)} + (n-m)t_B \tag{3.5}$$

Wyznaczona w ten sposób wartość $Z(t_B)$ jest zaobserwowaną sumą czasów poprawnej pracy badanych obiektów w przedziale czasu $[0,\ t_B]$. W takim przypadku granice dwustronnego przedziału (*d*) – dolną (*dd*) i górną (*dg*) - $[\lambda_{dd}, \lambda_{dg}]$ na poziomie ufności β oblicza się z wzorów

$$\lambda_{dd} = \frac{\chi^2_{2m,(1-\beta)/2}}{2Z(t_B)} \tag{3.6}$$

$$\lambda_{dg} = \frac{\chi^2_{2(m+1),\ (1+\beta)/2}}{2Z(t_B)} \tag{3.7}$$

W liczniku wzorów (3.6) i (3.7) występują odpowiednio kwantyle $(1-\beta)/2$ i $(1+\beta)/2$ rozkładu chi kwadrat przy stopniach swobody $2m$ i $(2(m+1)$.

Należy podkreślić, że badania niezawodności zarysowane powyżej dotyczą określonych warunków zewnętrznych (obciążenie, udary) i czynników środowiskowych (np. temperatura, wibracje, wilgotność). W praktyce analiz niezawodności nie dysponuje się wynikami badań niezawodności dla różnych

warunków i trzeba dostosować posiadane wyniki (dotyczące danej kategorii elementów) do innych warunków zewnętrznych i środowiskowych. Korzysta się wówczas z zaawansowanych metod szacowania parametrów rozkładu probabilistycznego lub ich odpowiedniej korekty z uwzględnieniem odpowiednich czynników. Są one opisane szczegółowo w poradnikach specjalistycznych i normach [3.34], [3.33].

Opracowany model probabilistyczny obiektu należy uwiarygodniać w czasie, korzystając m.in. z danych o przebiegu eksploatacji i zaistniałych uszkodzeniach w zbiorze obserwowanych obiektów danej kategorii. W tym celu korzysta się zwykle z Beyesowskich metod uaktualniania modelu probabilistycznego lub metod agregowania informacji z różnych źródeł bazując na opiniach ekspertów [3.9].

3.3. Bezpieczeństwo i ryzyko związane z eksploatacją obiektów technicznych

Istnieje szereg definicji ryzyka i wiele różnych metod jego analizy. Są opracowywane nowe metody analizy ryzyka, w czym szczególne osiągnięcia mają nauki ekonomiczne i nauki techniczne.

Ze względu na zmieniające się otoczenie i postęp technologiczny wyróżnia się niekiedy *ryzyko statyczne* i *ryzyko dynamiczne*. Stwierdza się, że *ryzyko statyczne* występuje niezależnie od postępu technicznego i związane jest z takimi zjawiskami w otoczeniu jak: sztormy czy huragany. Natomiast *ryzyko dynamiczne* związane jest ze zmianami technicznymi, ekonomicznymi bądź organizacyjnymi. Jest więc ono związane z szeroko rozumianym postępem cywilizacyjnym świata i zachodzącymi dynamicznymi zmianami społecznymi. Poniżej rozważa się ryzyko statyczne (długoterminowe) i ryzyko dynamiczne w nieco węższym ujęciu, w ramach systemów technicznych o różnej złożoności, które mogą być wzajemnie uzależnione.

Ryzyko techniczne szacuje się w odniesieniu do rozważanego działania lub misji (np. nieudane uruchomienie turbozespołu), albo realizowanego procesu (np. proces eksploatacji bloku energetycznego) w określonym przedziale czasu, na przykład w ciągu roku. W sytuacji zmieniających się w czasie warunków wewnętrznych i/lub zewnętrznych, które mogą wpływać istotnie na stan obiektu, mówi się o występowaniu *ryzyka o charakterze dynamicznym*. Szacowanie miary ryzyka może dotyczyć, więc potencjalnych sytuacji, które mogą spowodować straty w rozważanym (długim) horyzoncie czasowym (*ryzyko długoterminowe* lub *statyczne*) lub po zaistnieniu określonej sytuacji, np. uszkodzeniu w redundancyjnym systemie zabezpieczeń, co spowoduje nagle duży wzrost niegotowości tego systemu i znaczny wzrost ryzyka wystąpienia strat (*ryzyko dynamiczne*). Ocena *ryzyka dynamicznego*, spowodowanego np. wzrostem drgań wału turbiny, umożliwia podjęcie odpowiednich decyzji i działań (zob. Rys.3.1), co przyczyni się do zredukowania ryzyka awarii do poziomu akceptowanego.

Ryzyko dotyczy, więc różnych aspektów analizowanej rzeczywistości i ma związek z dalszą lub bliższą przyszłością. Prowadzi się prace badawcze mające na celu poznanie natury ryzyka oraz wykorzystanie wyników analizy ryzyka w procesie zarządzania bezpieczeństwem [3.21]. Poniżej poświęca się uwagę głównie zagadnieniom ryzyka w projektowaniu i eksploatacji systemów technicznych.

Na problem analizy, oceny i zarządzania ryzykiem, w tym redukowania ryzyka technicznego można spojrzeć przez pryzmat zapobiegania potencjalnym stratom i awariom przemysłowym. Na retrospektywnej analizie zaistniałych wypadków, zdarzeń awaryjnych i katastrof oraz prognostycznej analizie i ocenie ryzyka opierają swoją działalność firmy ubezpieczeniowe. Na coraz bardziej konkurencyjnym rynku ubezpieczeniowym oszacowania różnego rodzaju ryzyk muszą być rzetelne. Stosuje się różne *strategie zarządzania ryzykiem*, w tym *retencję* (pokrycie ew. strat z własnych środków), *transfer ryzyka* do firm ubezpieczeniowych i *redukcję ryzyka* za pomocą odpowiednich rozwiązań technicznych i organizacyjnych [3.19].

Poniżej wprowadza się kilka podstawowych pojęć, terminów i definicji związanych z zagadnieniami zagrożeń, analizy i oceny ryzyka oraz zarządzania bezpieczeństwem, zestawionych na podstawie dostępnej literatury źródłowej [3.19], [3.31] i norm [3.12], [3.29], [3.28], [3.30].

Pojęcie *szkoda* ma charakter bardzo ogólny i może dotyczyć urazu fizycznego, uszczerbku na

zdrowiu, utraty mienia lub degradacji środowiska, co spowoduje mniejsze lub większe straty. *Zagrożenie* jest źródłem potencjalnej szkody lub okolicznościami potencjalnie szkodliwymi, powodującymi straty. *Zdarzenie niebezpieczne* jest zdarzeniem, które może spowodować szkodę.

Z kolei *ryzyko (techniczne)* jest pewną kombinacją częstości lub prawdopodobieństwa wystąpienia zdarzeń awaryjnych (niebezpiecznych) i ich konsekwencji w postaci określonych szkód (strat). W złożonym obiekcie technicznym może występować wiele takich zdarzeń, które grupuje się w kategorie jako scenariusze awaryjne.

Analiza ryzyka jest systematycznym stosowaniem dostępnych informacji do zidentyfikowania zagrożenia i do oszacowania ryzyka dla jednostek ludzkich, populacji, mienia i środowiska. *Oszacowanie ryzyka* polega na ilościowym wyznaczeniu miary ryzyka lub określeniu poziomu analizowanego ryzyka w sposób jakościowy.

Wyróżnia się *ryzyko indywidualne*, dotyczące jednostki ludzkiej znajdującej się w danym miejscu i w rozważanym czasie oraz *ryzyko społeczne*, dotyczące określonej populacji przebywającej na danym terytorium (np. w pobliżu instalacji niebezpiecznej) lub grupy ludzi w danym miejscu, np. w przemieszczającym się środku transportowym.

Ocena ryzyka (indywidualnego lub społecznego) obejmuje pełny proces analizowania ryzyka i wyznaczania dopuszczalności ryzyka w odniesieniu do przyjętych lub formalnie określonych (zdefiniowanych) kryteriów ryzyka.

Sterowanie ryzykiem jest procesem podejmowania decyzji mających na celu zarządzanie ryzykiem, w szczególności zmniejszenie ryzyka, przy wykorzystaniu wyników oceny ryzyka. W sterowaniu ryzykiem wyróżnić można dwa zasadnicze podejścia: (a) aktywne polegające na oddziaływaniu na przyczyny i czynniki ryzyka oraz (b) pasywne, koncentrujące się na zabezpieczaniu przed ewentualnymi stratami.

Natomiast *zarządzanie ryzykiem technicznym* polega na systematycznej realizacji polityki bezpieczeństwa w praktyce z realizacją procedur i działań mających na celu analizowanie, ocenę i sterowanie ryzykiem.

Nie ma systemu technicznego w pełni bezpiecznego i dlatego *bezpieczeństwo definiuje się jako warunki lub sytuacja niewystępowania ryzyka nieakceptowanego*. Żeby stwierdzić, czy ryzyko jest akceptowane, czy nie, należy je oszacować i ocenić względem wartości kryterialnych.

System techniczny z punktu widzenia przeprowadzanej analizy ryzyka jest uporządkowanym zbiorem obiektów o zróżnicowanym poziomie złożoności i występujących relacjach miedzy nimi. System taki obejmuje wyposażenie i infrastrukturę techniczną, materiały, źródła energii, narzędzia, personel, procedury, sieci, komputery i oprogramowanie, środki komunikacji itd. Elementy systemu realizują określone funkcje w danym otoczeniu i danych warunkach środowiskowych, aby realizować przewidziane zadania produkcyjne i funkcje bezpieczeństwa. Polegają one na osiąganiu założonych celów w razie wystąpienia stanów nienormalnych, a szczególnie stanów awaryjnych.

Jak wspomniano w złożonym obiekcie technologicznym może wystąpić wiele potencjalnych zdarzeń awaryjnych powodujących określone szkody i niekiedy znaczne straty materialne (ekonomiczne). Na przebieg tych zdarzeń i ich skutki wpływają nie tylko czynniki techniczne, ale również czynniki środowiskowe i czynniki organizacyjne. Czynniki te kształtuje się odpowiednio w procesie zarządzania ryzykiem.

3.4. Ocena i sterowanie ryzykiem

Miarę ryzyka długoterminowego dla danego systemu technicznego wyznacza się na podstawie zbioru trójek zawierających [3.19]: scenariusz (rozważany przypadek) zdarzenia awaryjnego, częstość lub prawdopodobieństwo tego zdarzenia oraz niekorzystny skutek (szkodę) po jego wystąpieniu, a mianowicie

$$\Re = \{< S_k, F_k, N_k >\} \tag{3.8}$$

gdzie: S_k oznacza potencjalne zdarzenie awaryjne zdefiniowane dla *k*-tego scenariusza, F_k jest częstością *k*-tego scenariusza (prawdopodobieństwo na jednostkę czasu, np. rok), N_k oznacza niekorzystny skutek w wyniku wystąpienia *k*-tego scenariusza – określoną szkodę (stratę), np. liczba obrażeń i/lub zejść śmiertelnych, zakres strat majątkowych (ekonomicznych).

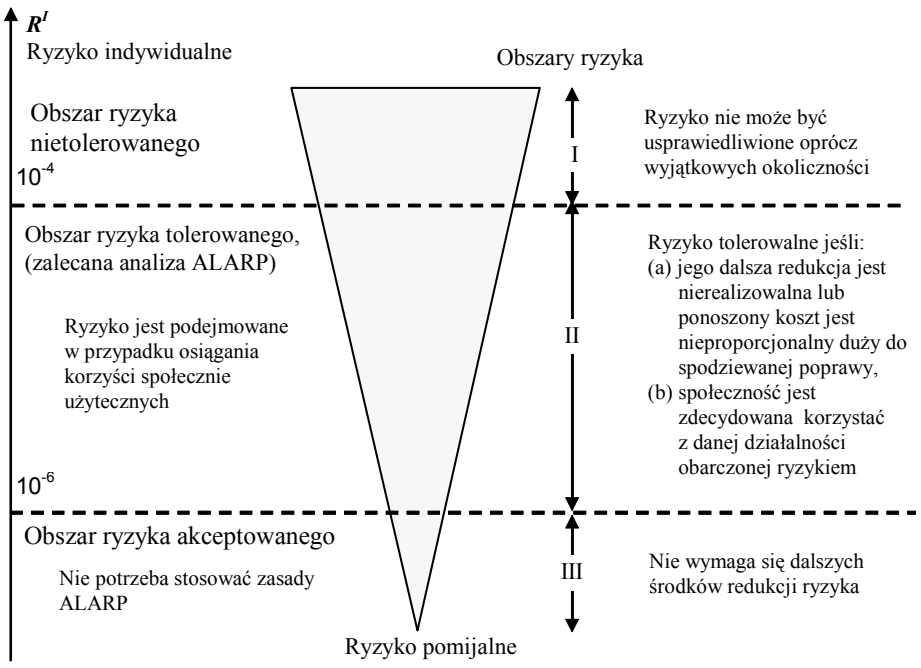
Ryzyko indywidualne związane z poszkodowaniem osoby znajdującej się w miejscu o współrzędnych *x,y* w wyniku poważnej awarii przemysłowej wyznacza się następująco

$$R^I_{(x,y)} = \sum_k F_k P_{k(x,y)} \tag{3.9}$$

gdzie: F_k jest częstością *k*-tego scenariusza awaryjnego szacowaną w przedziale czasowym, zwykle rok $[a]$, a $P_{k(x,y)}$ jest prawdopodobieństwem warunkowym poszkodowania osoby w wyniku wystąpieniu k-tego scenariusza awaryjnego w miejscu o współrzędnych (x, y) na terenie instalacji technicznej lub w jej otoczeniu.

Proponuje się w literaturze wartości kryterialne dozwolonego ryzyka indywidualnego, na poziomie $10^{-4}\ a^{-1}$ i poniżej [3.19], [3.21]. Za maksymalny poziom ryzyka indywidualnego przyjmuje się $10^{-5}a^{-1}$ dla istniejących obiektów przemysłowych, a wartości graniczne ryzyka akceptowanego przyjmuje się na poziomie $10^{-6}a^{-1}$ lub $10^{-7}a^{-1}$. Zaleca się rozważyć zmniejszenie tego ryzyka stosując zasadę ALARP (*as low as reasonably practicable*) [3.21], [3.12]. Jednym ze sposobów redukcji ryzyka indywidualnego w przemyśle jest zmniejszenie częstości F_k scenariuszy awaryjnych. Można to np. osiągnąć wprowadzając nowoczesne systemy zabezpieczeniowe zgodnie z koncepcją bezpieczeństwa funkcjonalnego [3.21], [3.12].

Zasadę analizy ALARP zilustrowano na Rys.3.3. Jeżeli poziom ryzyka w danej sytuacji należy do obszaru I (powyżej $10^{-4}a^{-1}$), ryzyko musi być zmniejszone, aby użytkowanie obiektu złożonego mogło być kontynuowane. W przypadku występowania ryzyka w obszarze II należy stosować zasadę ALARP. W obszarze ryzyka akceptowanego (III) nie ma potrzeby stosowania tej zasady.



Rys. 3.3: Poziomy ryzyka indywidualnego i stosowalność zasady ALARP

Jako miarę ryzyka społecznego (grupowego) R związanego z potencjalnymi zdarzeniami awaryjnymi może być oczekiwana strata, np. strata ekonomiczna lub przeciętna śmiertelność w ciągu roku

$$R = \sum_k F_k N_k \tag{3.10}$$

gdzie: F_k – częstość k-tego scenariusza awaryjnego [a^{-1}], N_k – prognozowana strata w wyniku k-tego scenariusza awaryjnego [*jedn. straty*].

Wyniki oszacowania ryzyka społecznego można przedstawić za pomocą *matrycy ryzyka*, w której wyróżniono kategorie (przedziały liczbowe) strat i kategorie częstości potencjalnych zdarzeń awaryjnych. Reprezentację graficzną wyników analizy ryzyka w postaci zbioru par $\{(F_k, N_k)\}$ reprezentowanych rombami, dla przykładowego obiektu i uwzględnionych w modelu ryzyka scenariuszy awaryjnych, przedstawiono na Rys.3.4. Wyróżniono w tej matrycy pięć kategorii (przedziałów) częstości $F^0 \div F^{-4}$ i pięć kategorii skutków awarii $N^A \div N^E$. Umożliwiają one klasyfikowanie wyników analizy ryzyka dla wyróżnionych scenariuszy awaryjnych do określonych klas ryzyka: I, II, III lub IV, zaznaczonych obszarów na tym rysunku. Kategorie częstości i skutków można definiować korzystając z informacji o charakterze ilościowym lub jakościowym [3.12]. W tym drugim przypadku stwierdzeniom (określeniom słownym) dotyczącym kolejnych kategorii (zob. Tablica 3.1) przypisuje się w procesie kalibracji modelu jakościowego przedziały liczbowe częstości zdarzeń awaryjnych i skutków tych zdarzeń.

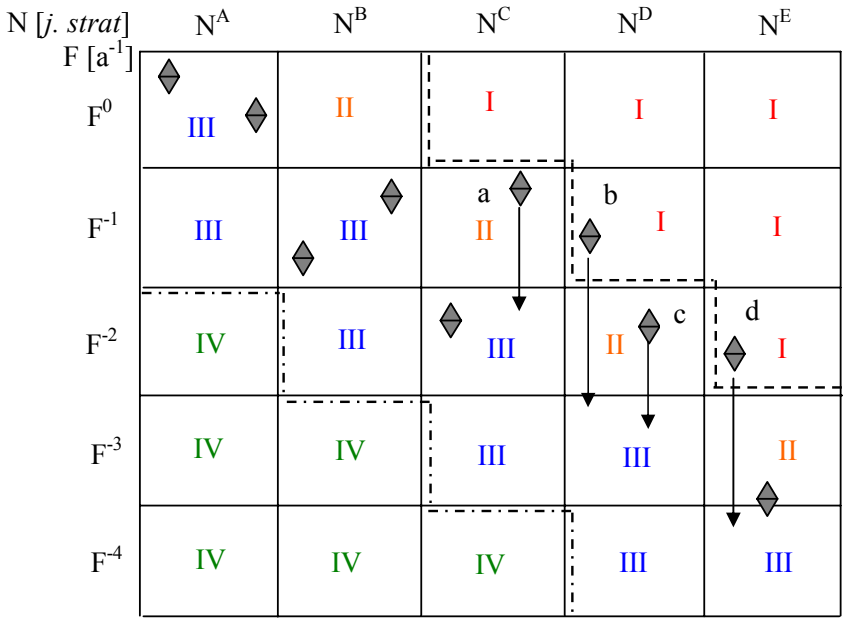
Na Rys.3.4 wyróżniono cztery klasy ryzyka dla potencjalnych zdarzeń awaryjnych zdefiniowanych dla danego złożonego obiektu podwyższonego ryzyka:

I – ryzyko niedozwolone, którego nie można tolerować ze względu na dużą częstość zdarzeń awaryjnych i ich poważne skutki,

II – ryzyko niepożądane, które należy redukować zgodnie z zasadą ALARP,

III – ryzyko tolerowane, jeśli koszt jego redukcji jest nieproporcjonalnie duży względem spodziewanych efektów (nieznaczne zmniejszenie ryzyka przy dużych kosztach), w przeciwnym razie ryzyko należy zmniejszać,

IV – ryzyko akceptowane.



Rys. 3.4: Ilustracja wyników analizy ryzyka przykładowego obiektu złożonego na tle obszarów wyróżnionych klas ryzyka

Jak widać, w obszarach ryzyka niedozwolonego (klasy I) i niepożądanego (klasy II) znajdują się cztery punkty, oznaczone kolejnymi literami a, b, c, d rosnąco według skutków. Jeśli przyjąć, w analizie ryzyka nie uwzględniono systemów zabezpieczeniowych, realizujących określone funkcje

związane z bezpieczeństwem, to po ich zastosowaniu nastąpi redukcja częstości danego scenariusza awaryjnego w kierunku wskazanym strzałkami (założono pesymistycznie, że wprowadzenie systemów dodatkowych zabezpieczeń nie powoduje zmniejszenia skutków awarii).

Tab. 3.1: Wyniki przykładowych kategorii zdarzeń awaryjnych i kategorii skutków przyjętych do kalibrowania matrycy ryzyka

Kategorie częstości zdarzenia	F^{-4}	F^{-3}	F^{-2}	F^{-1}	F^{0}
Określenie słowne kategorii częstości	Rzadkie	Mało prawdopodobne	Sporadyczne	Prawdopodobne	Częste
Przedziały wartości $[a^{-1}]$	$(10^{-5}, 10^{-4}]$	$(10^{-4}, 10^{-3}]$	$(10^{-3}, 10^{-2}]$	$(10^{-2}, 10^{-1}]$	$(10^{-1}, 1]$
Kategorie skutku zdarzenia	N^A	N^B	N^C	N^D	N^E
Określenie słowne kategorii skutku	Marginalne	Małe	Duże	Krytyczne	Katastrofalne
Orientacyjna liczba poszkodowanych	Pojedyncze obrażenia	Kilka obrażeń	Pojedyncze zejście	Kilka zejść	Wiele zejść

Przede wszystkim należy przeanalizować dogłębniej scenariusze b oraz d, ponieważ znajdują się one w obszarze ryzyka niedozwolonego. Celowa jest redukcja ich częstości, co najmniej 10 razy, a nawet 100 razy, czyli wprowadzając dodatkową funkcję bezpieczeństwa (system zabezpieczeniowy) z poziomem nienaruszalności bezpieczeństwa (ang. *safety integrity level*) SIL2 [3.12], [3.11]. Punkty a oraz c leżą w obszarze ryzyka niepożądanego. W tych przypadkach należy wprowadzić funkcję bezpieczeństwa charakteryzującą się co najmniej SIL1. Dla punktów znajdujących się w obszarze klasy ryzyka III należy przeprowadzić analizę ALARP.

Matrycę ryzyka przedstawioną na Rys.3.4 należy zweryfikować podczas analizy ryzyka złożonego obiektu technicznego innej kategorii. W definiowaniu obszarów klas ryzyka należy uwzględnić wyniki badań dotyczące wypadkowości i awaryjności w różnych sektorach gospodarki oraz akceptowalności ryzyka w nawiązaniu do aktualnych wartości społecznych.

3.5. Bezpieczenstwo funkcjonalne systemów sterowania i zabezpieczeń

Zainteresowanie zastosowaniem w gospodarce normy międzynarodowej IEC 61508 [3.12] i jej odpowiednika europejskiego EN 61508 oraz normy sektorowej IEC 61511 [3.11] w projektowaniu i eksploatacji systemów podwyższonego ryzyka wyraźnie wzrasta. Problematyka bezpieczeństwa funkcjonalnego jest coraz częściej podejmowana w badaniach naukowych. Firmy wytwarzające systemy sterowania i automatyki zabezpieczeniowej, firmy integrujące systemy dostępne na rynku oraz zakłady podwyższonego ryzyka o uznanej renomie na rynku starają się już teraz wdrażać normy bezpieczeństwa funkcjonalnego w praktyce [3.21]. Norma EN 61508 została przetłumaczona na język polski jako PN-EN 61508 [3.30]. Oryginalna wersja IEC 61508 ma charakter ogólny i dotyczy bezpieczeństwa funkcjonalnego w różnych sektorach gospodarki i obszarach zastosowania techniki.

Część 4 normy PN-EN 61508 została zatytułowana „Definicje i skrótowce". Według niej *ryzyko* jest kombinacją prawdopodobieństwa wystąpienia szkody i ciężkości tej szkody, czyli jak to już zdefiniowano powyżej. *Ryzyko tolerowane* to taki poziom ryzyka, które jest akceptowane w określonym kontekście, opartym na aktualnych wartościach społecznych. Zdefiniowano również *ryzyko resztkowe,*

jako ryzyko pozostające po zastosowaniu środków bezpieczeństwa. *Bezpieczeństwo* definiuje się jako okoliczność nie występowanie ryzyka nieakceptowanego.

Częścią bezpieczeństwa całkowitego jest *bezpieczeństwo funkcjonalne*, odnoszące się do wyposażenia sterowanego (*equipment under control - EUC*) i systemu sterowania EUC. Zależy ono od prawidłowego działania systemów E/E/PE (*elektrycznych / elektronicznych / programowalnych elektronicznych*) związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innych technikach i zewnętrznych środków zmniejszenia ryzyka.

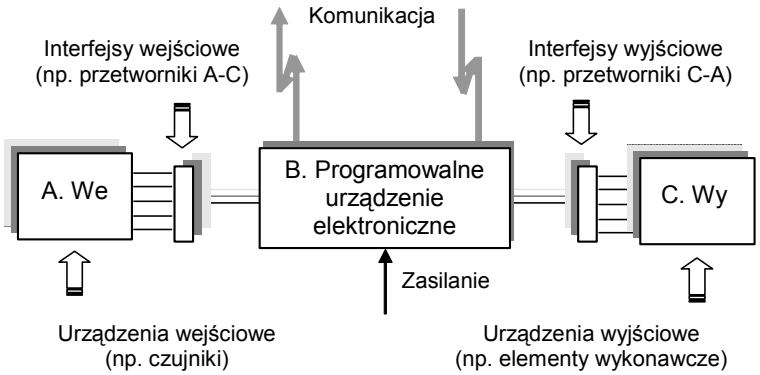
Strategię sterowania ryzykiem realizuje się poprzez projektowanie *funkcji bezpieczeństwa*, które są implementowane za pomocą systemów E/E/PE związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innej technice lub zewnętrzne urządzenia do zmniejszenie ryzyka. Przeznaczeniem kolejnej wyróżnionej podczas analizy ryzyka funkcji bezpieczeństwa jest osiągnięcie lub utrzymanie stanu bezpiecznego EUC w odniesieniu do konkretnego zdarzenia zagrażającego [3.17], [3.18]. Analizy ryzyka przeprowadza się uwzględniając system E/E/PE, którym jest zestaw elementów współdziałających zgodnie z projektem, a każdy element może być podsystemem. Zestaw ten może być systemem sterującym lub systemem sterowanym i obejmuje sprzęt, oprogramowanie i współdziałanie człowieka [3.20].

W normie IEC61508 definiuje się również *nienaruszalność bezpieczeństwa* jako prawdopodobieństwo, że system związany z bezpieczeństwem wykona właściwie wymagane funkcje bezpieczeństwa w określonych warunkach i w określonym przedziale czasu. Ważne praktyczne znaczenie ma *poziom nienaruszalności bezpieczeństwa* (ang. *safety integrity level - SIL*), poziom dyskretny (jeden z czterech możliwych $1 \div 4$) do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które mają być alokowane w systemach E/E/PE związanych z bezpieczeństwem.

Rozważa się dwa *rodzaje pracy*, czyli przewidziane sposoby pracy systemu związanego z bezpieczeństwem, odniesionej do częstości jego przywołań. Może nim być [3.12]:

1. *rodzaj pracy na rzadkie przywołanie*, gdy częstość przywołań zadziałania systemu związanego z bezpieczeństwem nie przekracza jednego na rok i nie przekracza dwukrotnej częstości testów okresowych;
2. *rodzaj pracy na częste przywołanie lub ciągły*, gdy częstość przywołań zadziałania systemu związanego z bezpieczeństwem jest większa od jednego na rok i większa niż dwukrotna częstość testów okresowych.

Przykładem systemu realizującego pierwszy rodzaj pracy jest system zabezpieczeń realizujący określoną funkcję bezpieczeństwa, który ma zadziałać tylko w określonej sytuacji nienormalnej, co powinno zdarzać się bardzo rzadko (np. rzadziej niż raz na rok). Przykładem systemu realizującego drugi rodzaj pracy jest system monitorowania przebiegu procesu, który powinien prawidłowo na bieżąco przedstawiać operatorowi stan procesu.



Rys. 3.5: Przykładowy system E/E/PE realizujący funkcję bezpieczeństwa

Na Rys.3.5 przedstawiono schemat przykładowego programowalnego systemu elektronicznego

(PES) realizującego funkcję bezpieczeństwa, współpracującego z urządzeniami wejściowymi, wyjściowymi i pomocniczymi (zasilanie energią elektryczną, komunikacja z innymi urządzeniami i panelem wizualizacji).

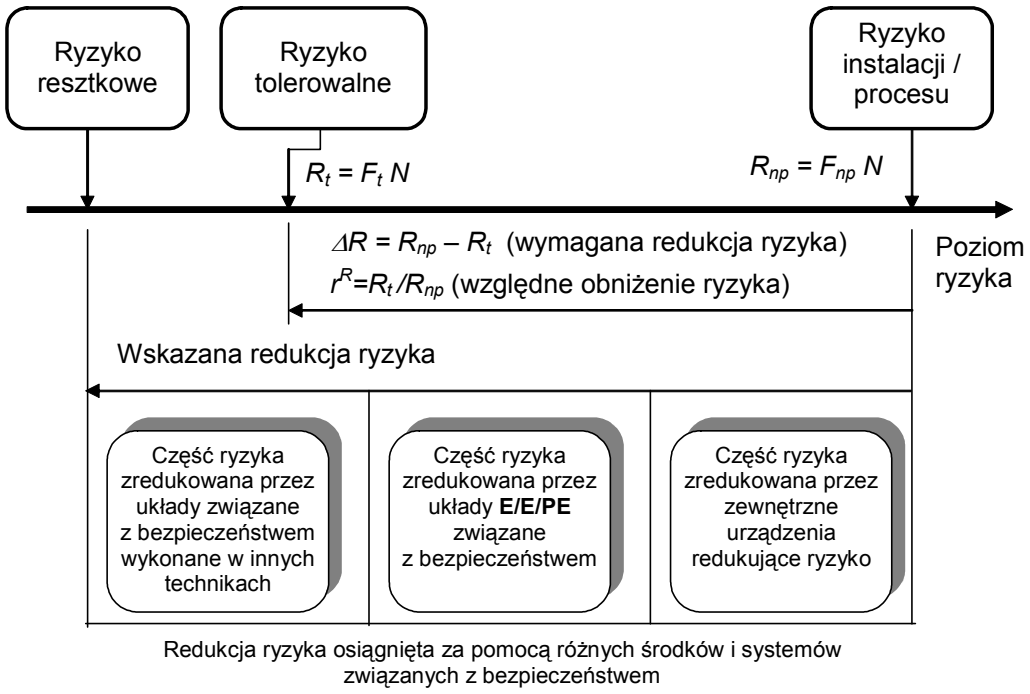
Należy podkreślić, że zarządzanie bezpieczeństwem w systemach technicznych zgodnie z normą EN 61508, polegające na ocenie możliwości zmniejszania ryzyka, obejmuje nie tylko systemy E/E/PE, ale również inne środki zmniejszania ryzyka.

3.6. Zmniejszanie ryzyka i wyznaczanie wymaganego SIL dla funkcji bezpieczeństwa

W nawiązaniu modelu ryzyka społecznego rozważa się poniżej prognozowane zmniejszenie ryzyka po wprowadzeniu zidentyfikowanej opcji sterowania ryzykiem (OSR), względem opcji bazowej (B). Jedną z takich opcji może być zastosowanie systemów E/E/PE [3.12] lub SIS (*safety instrumented system*) [3.11] pełniących funkcje związane z bezpieczeństwem. Redukcję ryzyka wyznacza się wówczas na podstawie wzoru [3.19]

$$\Delta R^{OSR} = \sum_k F_k^B N_k^B (1 - r_k^{F;OSR} r_k^{N;OSR}) \tag{3.11}$$

gdzie: F_k^B, N_k^B - częstość zdarzenia $[a^{-1}]$ i strata [*jedn. straty*] w wyniku k-tego scenariusza awaryjnego modelu ryzyka dla opcji B; $r_k^{F;OSR}$ - względne obniżenie częstości k-tego scenariusza awaryjnego po wprowadzeniu OSR ($r_k^{F;OSR} = F_k^{OSR}/F_k^B$); $r_k^{N;OSR}$ - względne obniżenie straty związanej z k-tym scenariuszem awaryjnym po wprowadzeniu OSR ($r_k^{N;OSR} = N_k^{OSR}/N_k^B$); ΔR^{OSR} ma wymiar [*jedn. straty/rok*].



Rys. 3.6: Sposoby zmniejszania ryzyka sugerowane w IEC 61508

Na Rys.3.6 przedstawiono sposoby redukowania ryzyka sugerowane w normie IEC 61508. Przy założeniu, że redukcję ryzyka do poziomu tolerowanego można uzyskać dzięki zastosowaniu systemu

E/E/PE otrzymuje się (dla tego samego poziomu skutków *N*) wzór na względne obniżenie poziomu ryzyka ma postać

$$r^R = R_t/R_{np} = F_t/F_{np} = r^F = PFD_{avg} \tag{3.12}$$

gdzie: R_{np} - ryzyko bez zastosowania rozważanych środków zabezpieczeniowych, F_{np} - częstość zdarzenia (dla skutków *N*) przed wprowadzeniem środka zabezpieczeniowego, R_t - ryzyko tolerowane, F_t - częstość potencjalnego zdarzenia awaryjnego po wprowadzeniu środka zabezpieczeniowego, wynikająca z poziomu ryzyka R_t przy skutkach $N = const$, r^F - względna redukcja częstości rozważanego zdarzeń (scenariusza) awaryjnego, PFD_{avg} - przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system E/E/PE.

Łatwo zauważyć, że redukcja ryzyka określana w IEC61508 metodą ilościową jest szczególnym przypadkiem opisanym za pomocą wzoru (3.11), jeśli przyjąć, że uwzględnia się tylko jeden scenariusz awaryjny ($k = 1$) i zakłada się, że $r^{N;OSR} = 1$, czyli zastosowanie danej opcji redukcji ryzyka (systemu E/E/PE) nie wpływa na poziom skutków zdarzenia awaryjnego (*N*), a jedynie na zmniejszenie jego częstości (*F*), przy czym dla efektywnej redukcji ryzyka zachodzi relacja $r^{F;OSR} << 1$.

Na podstawie wzoru (3.12) wyznacza się przeciętną wartość prawdopodobieństwa niezadziałania systemu zabezpieczeń na przywołanie PFD_{avg} (*probability of failure on demand – average*). Wartości kryterialne PFD_{avg} dla czterech poziomów nienaruszalności bezpieczeństwa SIL zestawiono w drugiej kolumnie Tabl.3.2 (rodzaj pracy rzadkiego przywołania do działania). W przypadku rodzaju pracy częstego przywoływania do działania systemu E/E/PE lub działania ciągłego rozważa się kryterium probabilistyczne zgodnie z trzecią kolumną tej tablicy, czyli prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę PFH(*frequency of dangerous failure per hour*).

Uzyskanie poziomu SIL3 dla rodzaju pracy rzadkiego przywołania do działania może okazać się niemożliwe bez zastosowania nadmiarowości strukturalnej w systemie E/E/PE. Spełnienie wymagań na SIL3, a zwłaszcza SIL4, wymaga zwykle zastosowania rozbudowanych struktur nadmiarowych i jest zwykle dużym wyzwaniem projektowym i technicznym z powodu konieczności eliminowania potencjalnych uszkodzeń zależnych w podsystemach nadmiarowych, a niekiedy nawet problemem organizacyjnym podczas użytkowania systemu (przeprowadzanie testów funkcjonalności podsystemów z uwzględnieniem danych statystycznych przebiegu użytkowania systemu i zaistniałych uszkodzeń).

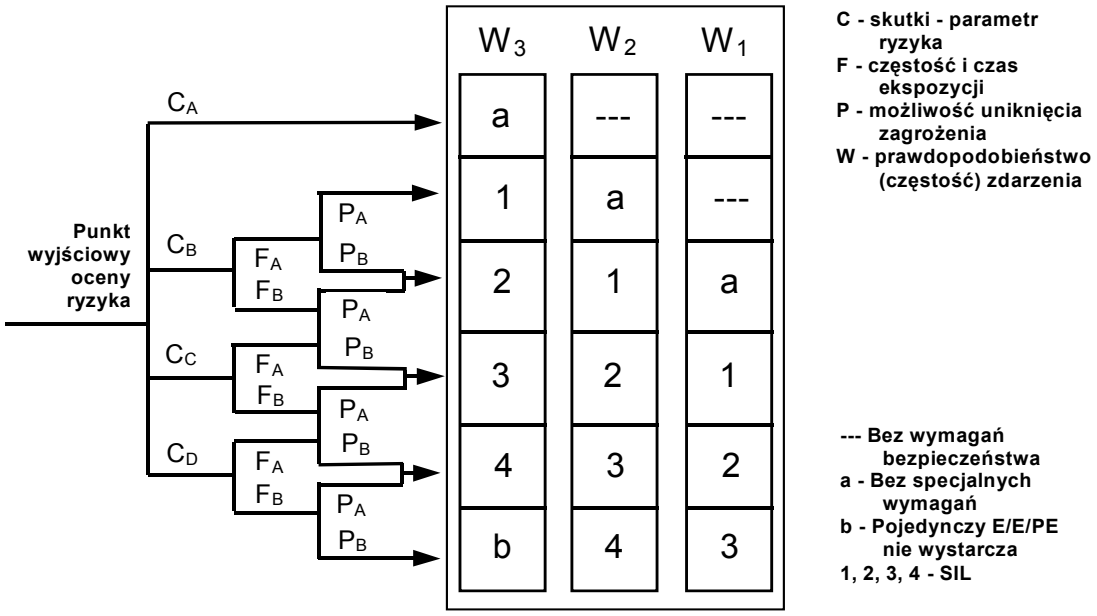
Tab. 3.2: Poziomy nienaruszalności bezpieczeństwa i kryteria probabilistyczne dla systemów związanych z bezpieczeństwem zaproponowane w normie IEC 61508

Poziom nienaruszalności bezpieczeństwa SIL	Przeciętne prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie PFD_{avg} (rodzaj pracy rzadkiego przywołania do działania)	Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę PFH (rodzaj pracy częstego przywoływania do działania lub działania ciągłego)
4	[10^{-5}, 10^{-4})	[10^{-9}, 10^{-8})
3	[10^{-4}, 10^{-3})	[10^{-8}, 10^{-7})
2	[10^{-3}, 10^{-2})	[10^{-7}, 10^{-6})
1	[10^{-2}, 10^{-1})	[10^{-6}, 10^{-5})

W przypadku trudności w przeprowadzeniu ilościowej analizy ryzyka proponuje się zgrubną, jakościową metodę wyznaczania SIL dla rozważanych funkcji bezpieczeństwa, korzystając z grafu ryzyka [3.12], [3.11]. Sugerowany w IEC 61508 do tego celu graf znajduje się na Rys.3.7. Poziom SIL przy takim podejściu zależy od czterech parametrów C, F, P i W, które opisano w prawej części tego rysunku.

Należy podkreślić, że taki graf wymaga kalibrowania zależnie od kategorii i charakterystyk technicznych i eksploatacyjnych analizowanego obiektu złożonego [3.12]. Przykładowe wartości tych parametrów dla uogólnionego obiektu złożonego zaproponowano w IEC 61508 [3.12], a dla typowego

obiektu złożonego w przemyśle procesowym w IEC 61511 [3.11]. W monografii [3.21] proponuje się wykorzystanie do kalibrowania grafu ryzyka podejścia bazującego na technice systemów z bazą wiedzy.



Rys. 3.7: Graf ryzyka do zgrubnego określania SIL sugerowany IEC 61508

3.7. Weryfikacja probabilistyczna SIL dla funkcji bezpieczeństwa

Weryfikacja wymaganego poziomu nienaruszalności bezpieczeństwa SIL systemu E/E/PE realizującego daną funkcję bezpieczeństwa wymaga modelowania probabilistycznego tego systemu z uwzględnieniem potencjalnych uszkodzeń i porównania uzyskanych wyników z przedziałami kryterialnymi podanymi w Tablicy 3.2. Poniżej przedstawione zostaną, po kilku definicjach przyjętych na podstawie PN-EN 61508, parametry uwzględniane w modelach probabilistycznych podsystemów.

Uszkodzenie (ang. *failure*) związane jest z zakończeniem zdolności jednostki funkcjonalnej do wypełniania wymaganej funkcji. Uszkodzenie może być przypadkowe (w sprzęcie) lub systematyczne (w sprzęcie i oprogramowaniu). *Uszkodzenie sprzętu przypadkowe* (ang. *random hardware failure*) jest uszkodzeniem pojawiającym się w przypadkowej chwili i wynika ono z różnych, możliwych mechanizmów degradacji sprzętu.

Uszkodzenie systematyczne (ang. *systematic failure*) jest uszkodzeniem wiążącym się w sposób deterministyczny z pewnymi przyczynami, które mogą zostać usunięte tylko przez modyfikację projektu lub procesu produkcyjnego, procedur eksploatacyjnych, dokumentacji lub innych czynników. Obsługiwanie korygujące bez wprowadzenia modyfikacji, normalnie nie usunie przyczyny uszkodzenia. Przykładami przyczyn uszkodzeń systematycznych mogą być błędy ludzkie popełnione podczas specyfikacji wymagań bezpieczeństwa, jak również podczas projektowania, wytwarzania, instalowania i eksploatacji sprzętu, a także podczas projektowania i implementacji oprogramowania.

Uszkodzenie niebezpieczne (ang. *dangerous failure*) jest uszkodzeniem, które ma możliwość wprowadzenia systemu wiążącego się z bezpieczeństwem w stan zagrażający lub w stan niemożliwości wypełniania funkcji. Czy możliwość ta zostanie zrealizowana czy nie, zależy od architektury systemu; w systemach o architekturze nadmiarowej, jest mniej prawdopodobne, aby uszkodzenie niebezpieczne sprzętu doprowadziło do stanu całkowicie niebezpiecznego lub stanu niemożliwości wypełniania funkcji.

Uszkodzenie bezpieczne (ang. *safe failure*) jest uszkodzeniem, które nie ma możliwości wprowadzenia systemu wiążącego się z bezpieczeństwem w stan niebezpieczny lub w stan niemożliwości wypełniania funkcji. Czy możliwość ta zostanie zrealizowana czy nie, zależy od architektury systemu; w systemach z nadmiarowością strukturalną, jest mniej prawdopodobne, aby uszkodzenie bezpieczne sprzętu doprowadziło do nieuzasadnionego wyłączenia systemu. Wyłączenie turbiny z powodu niepotrzebnego zadziałania systemu zabezpieczeniowego (ang. *spurious operation*), na przykład dużej turbiny energetycznej, jest poważnym zakłóceniem, potencjalnie z poważnymi skutkami dla systemu elektroenergetycznego [3.23], [3.26].

Jak wspomniano w systemach zabezpieczeń z nadmiarowością strukturalną poważny problem stanowią uszkodzenia zależne. *Uszkodzenie zależne* (ang. *dependent failure*) jest uszkodzeniem, którego prawdopodobieństwo nie może być wyrażone jako prosty iloczyn prawdopodobieństw bezwarunkowych poszczególnych zdarzeń. Dwa zdarzenia A i B są zależne, jeśli zachodzi następująca relacja na prawdopodobieństwach tych zdarzeń: $P(Z) = P(A \bigcap B) = P(A)P(B|A) > P(A)P(B)$. *Uszkodzenia* mogą być spowodowane *wspólną przyczyną* (ang. *common cause failure*). Uszkodzenia grupowe są wynikiem jednego lub kilku zdarzeń, powodujących jednoczesne uszkodzenie dwóch lub kilku (oddzielnych) kanałów w urządzeniu wielokanałowym, co może doprowadzić do uszkodzenia systemu.

Istotne znaczenie ma uwzględnienie błędów w modelowaniu systemów związanych z bezpieczeństwem. *Błąd* (ang. *error*) ogólnie jest rozbieżnością między obliczoną, zaobserwowaną lub zmierzoną wartością lub stanem i prawdziwą, ustaloną lub poprawną teoretycznie wartością lub stanem. Błąd może być w szczególności błędem ludzkim, wpływającym zwykle istotnie na bezpieczeństwo systemu. Ocenia się, że szeroko rozumiane błędy człowieka (od etapu projektowania obiektu, poprzez eksploatację do jego likwidacji) są przyczyną 70-90% wypadków i awarii, zależnie od kategorii obiektu złożonego.

Błąd ludzki, pomyłka (ang. *human error; mistake*) polega na niepoprawnym działaniu lub zaniechaniu działania przez człowieka, co może pociągnąć za sobą niezamierzone następstwa. Potrzeba uwzględnienia zdarzeń, polegających na popełnieniu błędów przez człowieka (np. operatora turbiny lub personelu obsługi technicznej) powinno być starannie rozpatrzone podczas modelowania logicznego i probabilistycznego systemu. Korzysta się w tym celu z odpowiedniej metody analizy niezawodności człowieka HRA (*human reliability analysis*) [3.19].

Test okresowy (ang. *proof test*) jest testem wykonywanym w celu wykrycia uszkodzeń w systemie wiążącym się z bezpieczeństwem (lub jego podsystemie), aby, jeśli to konieczne, system mógł być doprowadzony do stanu „jak nowy" lub do stanu bliskiego takiemu stanowi. Aby test okresowy był w pełni skuteczny konieczne jest wykrycie 100% uszkodzeń niebezpiecznych. Chociaż w praktyce osiągnięcie tych 100 % nie jest zawsze możliwe, zależnie od sposobu przeprowadzania testu (np. podczas pracy obiektu złożonego). Tylko w niektórych sytuacjach eksploatacyjnych możliwe jest przeprowadzenie pełnego testu funkcjonalnego systemu zabezpieczeń (np. odstawienie obiektu złożonego w celu wykonania remontu). Jako minimum, wszystkie wykonywane funkcje bezpieczeństwa, są sprawdzane według specyfikacji wymagań bezpieczeństwa systemów E/E/PE. Jeśli są używane oddzielne nadmiarowe kanały, test wykonuje się w każdym kanale oddzielnie.

Diagnostykę tylko niektórych części systemu E/E/PE można przeprowadzać automatycznie. Dlatego ważne znaczenie ma ocena pokrycia diagnostycznego. *Pokrycie diagnostyczne DC* (ang. *diagnostic coverage*) definiuje się jako względne zmniejszenie prawdopodobieństwa niebezpiecznych uszkodzeń sprzętu, wyrażane poprzez odpowiednie intensywności uszkodzeń w jednostkowym czasie, związane z działaniem automatycznych testów diagnostycznych [3.12]

$$DC = \frac{\lambda_{DD}}{\lambda_D} \tag{3.13}$$

gdzie: λ_{DD} oznacza prawdopodobieństwo na jednostkę czasu (intensywność) występowania wykrywalnych uszkodzeń niebezpiecznych (ang. *danger detected – DD*), λ_D oznacza sumaryczną intensywność wystąpienia wszystkich uszkodzeń niebezpiecznych (ang. *danger – D*). Pokrycie diagnostyczne może odnosić się do całego systemu wiążącego się z bezpieczeństwem lub do jego części. Na przykład

pokrycie diagnostyczne może odnosić się do czujników, układu logicznego i elementów końcowych.

Definiuje się również *pokrycie diagnostyczne uszkodzeń bezpiecznych* na podstawie intensywności uszkodzeń bezpiecznych wykrywalnych (ang. *safe detected - SD*) w odniesieniu do sumarycznej intensywności zidentyfikowanych uszkodzeń bezpiecznych (ang. *safe – S*)

$$DC_S = \frac{\lambda_{SD}}{\lambda_S} \tag{3.14}$$

Pokrycie diagnostyczne może odnosić się do dowolnego z podsystemów danego systemu E/E/PE związanego z bezpieczeństwem, w szczególności do podsystemów / kanałów: pomiarowego / inicjującego, układu przetwarzającego informację i elementu wykonawczego / końcowego. Zastosowane procedury diagnozowania mają istotny wpływ na bezpieczeństwo obiektu podwyższonego ryzyka wyposażonego w systemy sterowania i automatyki zabezpieczeniowej.

W modelowaniu probabilistycznym podsystemu wymagana jest znajomość jego całkowitej intensywności uszkodzeń λ, która obejmuje uszkodzenia niebezpieczne i bezpieczne

$$\lambda = \lambda_S + \lambda_D \tag{3.15}$$

gdzie: λ_S jest intensywnością uszkodzeń bezpiecznych na godzinę, h^{-1}, a λ_D intensywnością uszkodzeń niebezpiecznych.

Udział (współczynnik wagowy) *FS* uszkodzeń bezpiecznych tego podsystemu definiuje się jako

$$FS = \frac{\lambda_S}{\lambda} \tag{3.16}$$

Znając intensywność uszkodzeń λ podsystemu i udział uszkodzeń bezpiecznych FS można napisać na podstawie (3.15) i (3.16) wzory na intensywność uszkodzeń bezpiecznych

$$\lambda_S = FS \cdot \lambda \tag{3.17}$$

i intensywność uszkodzeń niebezpiecznych

$$\lambda_D = (1 - FS) \cdot \lambda \tag{3.18}$$

Uszkodzenia niebezpieczne podsystemu mogą być wykrywalne (ang. *dangerous detected - DD*) lub niewykrywalne (ang. *dangerous undetected - DU*) przez automatyczne testy diagnostyczne. Można więc napisać

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{3.19}$$

gdzie: λ_{DD} - intensywność uszkodzeń wykrywalnych przez automatyczne testy diagnostyczne, a λ_{DU} - intensywność uszkodzeń niewykrywalnych przez automatyczne testy diagnostyczne.

Uwzględniając (3.13) i (3.18) można napisać wzory na intensywność uszkodzeń niebezpiecznych wykrywalnych przez testy diagnostyczne

$$\lambda_{DD} = DC \cdot \lambda_D = DC(1 - FS) \cdot \lambda \tag{3.20}$$

i niebezpiecznych niewykrywalnych przez testy diagnostyczne

$$\lambda_{DU} = (1 - DC) \cdot \lambda_D = (1 - DC)(1 - FS) \cdot \lambda \tag{3.21}$$

Przy założeniu, że pokrycie diagnostyczne może odnosić się również do uszkodzeń bezpiecznych, wprowadzić można pojęcie uszkodzenia bezpiecznego wykrywalnego (*safe detected - SD*)

$$\lambda_{SD} = DC_S \cdot \lambda_S = DC_S \cdot FS \cdot \lambda \tag{3.22}$$

i uszkodzenia bezpiecznego niewykrywalnego (ang. *safe undetected - SU*).

$$\lambda_{SU} = (1 - DC_S) \cdot \lambda_S = (1 - DC_S) \cdot FS \cdot \lambda \tag{3.23}$$

Sumaryczna przeciętna wartość intensywności uszkodzeń podsystemu jest sumą przeciętnych wartości intensywności cząstkowych

$$\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU} \tag{3.24}$$

Znając wartości tych intensywności można wyznaczyć różne miary probabilistyczne dla podsystemu E/E/PE systemu zabezpieczeń:

(a) przeciętne prawdopodobieństwo PFD_{avg} niewypełnienia funkcji bezpieczeństwa na przywołanie (w przypadku rodzaju pracy na rzadkie przywołanie);

(b) prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę (częstość) *PFH* (w przypadku rodzaju pracy na częste przywołanie lub ciągłego);

(c) częstość uszkodzenia bezpiecznego prowadzącego do nieuzasadnionego zadziałania systemu zabezpieczeń *FSF*;

(d) niedyspozycyjność systemu spowodowana uszkodzeniami bezpiecznymi systemu zabezpieczeń *PSF*.

W przypadku rodzaju pracy systemu E/E/PE na rzadkie przywołanie wyznacza się średnie prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie PFD_{avg}. Prawdopodobieństwo to, wyznaczane dla poszczególnych podsystemów, zależy od dwóch parametrów:

- intensywności uszkodzeń niebezpiecznych niewykrywalnych λ_{DU} $[h^{-1}]$,
- interwału okresowych testów funkcjonalnych podsystemu T_I $[h]$.

Funkcja niegotowości podsystemu, którego stan uszkodzenia niebezpiecznego może być wykryty tylko podczas testu, ma postać:

$$PFD(t) = 1 - \exp[-\lambda_{DU} \cdot t] \tag{3.25}$$

Przyjmując, że $\lambda_{DU} \cdot t \leqslant 0.1$ i można przyjąć zamiast (3.25) wzór przybliżony: $PFD(t) \cong \lambda_{DU} \cdot t$. Uwzględniając interwał testów okresowych T_I można napisać wzór na średnie prawdopodobieństwo niewypełnienia przez podsystem funkcji bezpieczeństwa na przywołanie PFD_{avg} w postaci:

$$PFD_{avg} = \int_0^{T_I} PFD(t)\, dt \cong \frac{1}{T_I} \int_0^{T_I} \lambda_{DU} \cdot t\, dt = 0.5 \lambda_{DU} T_I \tag{3.26}$$

Interwały testu kontrolnego T_I przyjmuje się zwykle w analizach jako [3.12]: jeden tydzień (168 h), jeden miesiąc (730 h), trzy miesiące (2190 h), sześć miesięcy (4380 h), jeden rok (8760 h), dwa lata (17520 h), pięć lat (43800 h) lub dziesięć lat (87600 h). Interwały testu kontrolnego poszczególnych podsystemów w ramach systemu E/E/PE mogą być zróżnicowane zależnie od poziomu intensywności uszkodzeń podsystemów i zastosowanej nadmiarowości strukturalnej w systemie.

W wielu przypadkach uzasadnione jest wyznaczenie przeciętnego prawdopodobieństwa niezadziałania podsystemu na przywołanie PFD_avg ze wzoru w postaci rozszerzonej [3.18], [3.21]:

$$PFD_{avg} \cong PFD_{avg}^{FT} + PFD_{avg}^{AT} + PFD^{HE} \tag{3.27}$$

gdzie: PFD_{avg}^{FT} jest prawdopodobieństwem niewypełnienia funkcji z powodu uszkodzenia bezpiecznego wykrywanego okresowo podczas sprawdzającego testu funkcjonalnego (*functional test* - *FT*); PFD_{avg}^{AT} prawdopodobieństwem niewypełnienia funkcji związanej z naprawą po wykryciu uszkodzenia podsystemu przez test automatyczny (ang. *automatic test* - *AT*) wykonywany cyklicznie; PFD^{HE} prawdopodobieństwo zdarzenia, że podsystem nie wypełni funkcji na przywołanie niezależnie od przeprowadzonych testów wykrywających uszkodzenie sprzętu z powodu błędu człowieka (*human error* - *HE*).

Na podstawie modeli probabilistycznych podsystemów wyznacza się prawdopodobieństwo niezadziałania na przywołanie rozważanego systemu. W praktyce stosuje się najczęściej metodę schematów blokowych w zastosowaniu do modułów systemu E/E/PE (Rys. 3.5) uwzględniając:

A. Blok wejściowy (czujniki i przetworniki).

B. Blok przetwarzania informacji (sterowniki programowalne).

C. Blok wyjściowy (człony wykonawcze i elementy końcowe).

W blokach tych mogą występować nadmiarowości strukturalne, na przykład 1oo2, 2oo3 lub inne [3.12].

Przy założeniu małych wartości prawdopodobieństw niewypełnienia funkcji na żądanie przez te bloki, uzasadnione jest stosowanie przybliżonej zależności dla całego systemu E/E/PE:

$$PFD^{\mathrm{S}}_{\mathrm{avg}} \cong PFD^{\mathrm{A}}_{\mathrm{avg}} + PFD^{\mathrm{B}}_{\mathrm{avg}} + PFD^{\mathrm{C}}_{\mathrm{avg}} \tag{3.28}$$

gdzie: $PFD^{\mathrm{A}}_{\mathrm{avg}}$, $PFD^{\mathrm{B}}_{\mathrm{avg}}$, $PFD^{\mathrm{C}}_{\mathrm{avg}}$ są prawdopodobieństwami niewypełnienia funkcji na przywołanie odpowiednio przez moduły (bloki) A, B i C.

Jeśli dla przykładowego systemu E/E/PE związanego z bezpieczeństwem wyznaczono te prawdopodobieństwa jako równe: $PFD^{\mathrm{A}}_{\mathrm{avg}} = 2.2 \cdot 10^{-2}$ (SIL1), $PFD^{\mathrm{B}}_{\mathrm{avg}} = 1.5 \cdot 10^{-3}$ (SIL2), $PFD^{\mathrm{C}}_{\mathrm{avg}} = 1.4 \cdot 10^{-2}$ (SIL1) to prawdopodobieństwo niezadziałania na przywołanie systemu E/E/PE wynosi $PFD^{\mathrm{S}}_{\mathrm{avg}} \cong 3.75 \cdot 10^{-2}$, czyli spełnia on tylko wymagania kryterialne dla poziomu nienaruszalności bezpieczeństwa SIL1 (zob. Tabl. 3.2 – druga kolumna).

3.8. Wymagania dla podsystemów i zgrubna ocena jakościowa systemu E/E/PE

Weryfikowanie poziomu SIL zaprojektowanego systemu E/E/PE związanego z bezpieczeństwem jest niekiedy wyzwaniem z powodu braku wiarygodnych danych przyjmowanych jako parametry modelu probabilistycznego. W przypadku zupełnego braku danych numerycznych norma IEC 61508 dopuszcza ocenę SIL metodą jakościową według podanych reguł „zwijania" schematu blokowego analizowanego systemu związanego z bezpieczeństwem.

Wprowadzono jednak ograniczenia dotyczące poziomów nienaruszalności bezpieczeństwa SIL podsystemów E/E/PE zależnie od udziału uszkodzeń bezpiecznych S_{ff} w rozpatrywanym podsystemie, który wyznacza się ze wzoru

$$S_{ff} = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \tag{3.29}$$

gdzie: λ_S jest sumaryczną intensywnością uszkodzeń bezpiecznych, h^{-1}; λ_{DD} sumaryczną intensywnością uszkodzeń niebezpiecznych wykrywalnych, a λ_{DU} sumaryczną intensywnością uszkodzeń niebezpiecznych niewykrywalnych.

Wyróżnia się podsystemy typu A i typu B. Podsystem jest uważany za podsystem (element) kategorii A jeśli [3.12]:

(a) jego wszystkie rodzaje uszkodzeń są dobrze zdefiniowane,

(b) jego zachowanie w danych warunkach można w pełni określić, oraz

(c) są dostępne wystarczające dane empiryczne, na podstawie których można oszacować intensywności uszkodzeń wykrywalnych i niewykrywalnych niebezpiecznych.

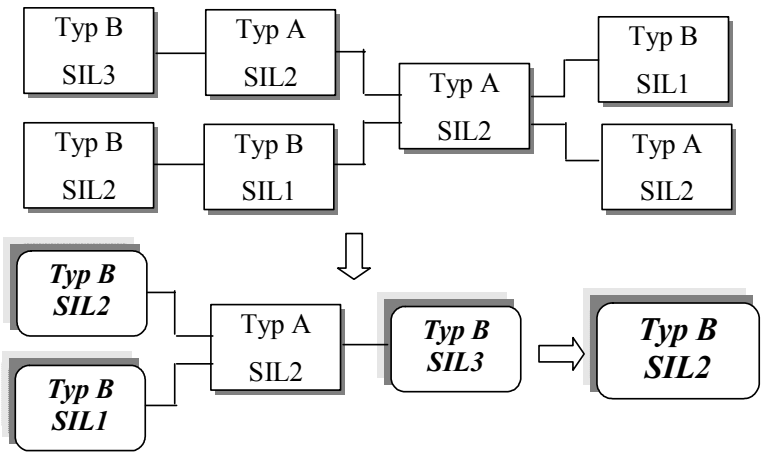
Jeśli dany podsystem nie spełnia tych wymagań, musi być on traktowany jako podsystem kategorii B, a jego intensywności uszkodzeń powinny być wówczas oceniane przez ekspertów. Ograniczenia architektoniczne dla podsystemów - najwyższy poziom SIL jaki można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy typu A i (typu B) podano na podstawie IEC 61508 w Tablicy

3.3. Jak widać, ograniczenia te zależą istotnie od udziału uszkodzeń bezpiecznych S_{ff}. Poziom SIL, jaki można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy typu B jest mniejszy niż w przypadku podsystemów typu A. Wynika to z mniejszego zaufania do podsystemów typu B, zawierających moduły programowalne, w których mogą wystąpić błędy systematyczne.

Weryfikowanie SIL systemu E/E/PE na podstawie znanych poziomów nienaruszalności podsystemów przeprowadza się metodą jakościową według podanych reguł „zwijania" [3.12] schematu blokowego. Przykładowy schemat takiego systemu przedstawiono na Rys.3.8. Wyróżniono na nim podsystemy typu A i typu B dla podsystemów pomiarowych i wykonawczych, natomiast podsystem logiczny (np. sterownik programowalny) umieszczony centralnie w schemacie wyjściowym jest typu A (SIL2). Przekształcając schemat wyjściowy w dwóch krokach, jak na Rys.3.8, uzyskuje się dla przykładowego systemu (rodzaj pracy na rzadkie przywołanie) wynikowy poziom nienaruszalności bezpieczeństwa dla systemu SIL2 i wynikowy „Typ B" systemu.

Tab. 3.3: Ograniczenia architektoniczne dla podsystemów - najwyższy poziom SIL jaki można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy typu A i (typu B)

Udział uszkodzeń bezpiecznych S_{ff}	Tolerowane uszkodzenia sprzętu N		
	0	1	2
$<$ 60 %	SIL1 (nie dozwolone)	SIL2 (SIL1)	SIL3 (SIL2)
60 % - $<$ 90 %	SIL2 (SIL1)	SIL3 (SIL2)	SIL4 (SIL3)
90 % - $<$ 99 %	SIL3 (SIL2)	SIL4 (SIL3)	SIL4 (SIL4)
$\geqslant$ 99 %	SIL3 (SIL3)	SIL4 (SIL4)	SIL4 (SIL4)
Tolerowane uszkodzenia sprzętu N oznacza, że $N+1$ uszkodzeń spowoduje utratę funkcji bezpieczeństwa			



Rys. 3.8: Wyznaczanie wynikowego SIL przykładowego systemu E/E/PE metodą jakościową w odniesieniu do defektów sprzętu

Metoda jakościowa weryfikacji SIL systemu E/E/PE jest przydatna szczególnie w początkowej fazie projektowania funkcji bezpieczeństwa do realizowania przez system E/E/PE, na przykład w przeprowadzaniu zgrubnej oceny proponowanych rozwiązań. Nie nadaje się ona na przykład do oceny wpływu interwałów testowania podsystemów na wynikowy SIL, co wymaga stosowania metody ilościowej.

Bibliografia

[3.1] American Institute of Chemical Engineers, New York. *Layer of Protection Analysis, Simplified Process Risk Assessment, Center for Chemical Process Safety*, 2001.

[3.2] Bahrami K., Price J. RBM, a risk-based maintenance case study. *Maintenance & Asset Management*, 16(1), 2001.

[3.3] Brandowski A. Bezpieczeństwo funkcjonalne aplikacją nauki o bezpieczeństwie. *Zarządzanie bezpieczeństwem funkcjonalnym*, Gdańsk / Jurata, 16–18.09.2004.

[3.4] Cempel C., Tomaszewski F. *Diagnostyka maszyn. Zasady ogólne. Przykłady zastosowań.* Wydawnictwo MCNEMT, Radom, 1992.

[3.5] Cholewa W., Kaźmierczak J. *Data processing and reasoning in technical diagnostics*. WNT, Warszawa, 1995.

[3.6] Dźwiarek M. Bezpieczeństwo funkcjonalne systemów sterowania maszynami w świetle wymagań dyrektyw ue. Gdańsk / Jurata, 16-18.09. 2004. Politechnika Gdańska, Polskie Towarzystwo Bezpieczeństwa i Niezawodności.

[3.7] Dyrektywa Unii Europejskiej. *98/37/WE z dnia 22 czerwca 1998 r. w sprawie zbliżenia prawa państw członkowskich, dotyczącego maszyn, zmienionej dyrektywą Unii Europejskiej 98/79/WE (Dyrektywa Maszynowa)*.

[3.8] Hernas A., Dobrzański J. *Trwałość i niszczenie elementów kotłów i turbin parowych*. Wydawnictwo Politechniki Śląskiej, Gliwice, Gliwice.

[3.9] International Atomic Energy Agency, Vienna. *IAEA-Safety Series No. 50-P-4: Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)*, 1992.

[3.10] International Atomic Energy Agency, Vienna. *IAEA-TECDOC-658: Safety related maintenance in the framework of the reliability centered maintenance concept*, 1992.

[3.11] International Electrotechnical Commission. *IEC 61511:2000: Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1–3*.

[3.12] International Electrotechnical Commission (IEC). *IEC 61508:1998. Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems. Parts 1–7*.

[3.13] International Electrotechnical Commission (IEC). *IEC/CEI 62061:2005 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*, 2005.

[3.14] Ivanovic A. et al. *Risk-Based Inspection and Maintenance Procedures for European Industry*. RIMAP CEN Workshop Document, MPA, 2005.

[3.15] Kościelny J.M. *Diagnostyka zautomatyzowanych procesów przemysłowych*. EXIT, Warszawa, 2001.

[3.16] Korbicz J., Kościelny J.M., Kowalczuk Z., Cholewa W. *Diagnostyka procesów. Modele sztucznej inteligencji. Zastosowania*. WNT, Warszawa, 2002.

[3.17] Kosmowki K. T. Koncepcja bezpieczeństwa funkcjonalnego w przemyśle. *Materiały konferencji Naukowo-Technicznej „Zarządzanie bezpieczeństwem funkcjonalnym"*, Jurata, 16-18.09.2004.

[3.18] Kosmowki K.T., Kozyra M., Śliwiński M. Metody modelowania probabilistycznego systemów związanych z bezpieczeństwem i ich implementacja komputerowa. *Materiały konferencji Naukowo-Technicznej „Zarządzanie bezpieczeństwem funkcjonalnym"*, Jurata, 16-18.09.2004.

[3.19] Kosmowski K.T. *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Monografie 33. Wydawnictwo Politechniki Gdańskiej, Gdańsk, 2003.

[3.20] Kosmowski K.T. Functional safety concept of hazardous systems and new challenges. *Journal of Loss Prevention in the Process Industries*, 19:298–305, 2006.

[3.21] Kosmowski K.T., redaktor. *Functional Safety Management In Critical Systems*. Politechnika Gdańska. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk, 2007.

[3.22] Kosmowski K.T., Śliwiński M. An integrated analysis of protection layers in hazardous systems. *Journal of Konbin*, 2, 2006.

[3.23] Laudyn D., Maksymiuk J. *Jakość i niezawodność w elektroenergetyce*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 1996.

[3.24] Maksymiuk J. *Niezawodność maszyn i urządzeń elektrycznych*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2003.

[3.25] Moubray J. *Reliability-Centered Maintenance*. Industrial Press Inc, New York, 1992.

[3.26] Paska J. *Niezawodność systemów elektroenergetycznych*. Oficyna Wydawnicza PW, Warszawa, 2005.

[3.27] *PN-93/N-50191. Słownik terminologiczny elektryki. Niezawodność, jakość usługi. [eqv IEC 60050(191):1990]*.

[3.28] *PN-EN 1050:1996. Maszyny. Bezpieczeństwo. Zasady oceny ryzyka*.

[3.29] *PN-IEC 300-3-9: 2000. Analiza ryzyka w systemach technicznych (IEC 300-3-9: 1995)*.

[3.30] Polski Komitet Normalizacyjny (PKN). *PN-EN 61508:2003. Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / elektronicznych programowalnych systemów związanych z bezpieczeństwem.*, 2003.

[3.31] Roland H.E., Moriarty B. *System Safety Engineering and Management*. A Wiley-Interscience Publication, New York, 1990.

[3.32] *Rozporządzenie Ministra Gospodarki, Pracy i Polityki społecznej z dnia 10 kwietnia 2003 r. w sprawie zasadniczych wymagań dla maszyn i elementów bezpieczeństwa. DzU nr 91. poz. 858.*

[3.33] Washington: U.S. Department of Defence. *MIL-HDBK-217F. Reliability Prediction of Electronic Equipment*, 1991.

[3.34] Wiley, New York. *IEEE Standard 500: IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*, 1984.

[3.35] Wiśniewski W. *Diagnostyka techniczna wytwórczych urządzeń energetycznych w elektrowniach*. PWN, Warszawa, 1991.

Rozdział 4

Akceptowalność i niepewność w analizie i ocenie ryzyka

Robert GUMIŃSKI, Stanisław RADKOWSKI

4.1. Kryteria akceptowalności ryzyka

Przystąpienie Polski do struktur Unii Europejskiej jest jednoznaczne z przyłączeniem do „Jednolitego rynku europejskiego", w którym największą barierą w swobodnym przepływie towarów jest odmienność regulacji technicznych w poszczególnych państwach.

Przezwyciężając te problemy Wspólnota Europejska wydała akty prawne pod nazwą Dyrektyw Starego Podejścia, szczegółowo opisujące różnorodne wymagania techniczne, specyfikowane dla poszczególnych grup wyrobów. Opracowywanie szczegółowych specyfikacji technicznych uwzględniających nowe rozwiązania konstrukcyjne i technologiczne, związana z tym przewlekłość procedur nowelizacji dyrektyw powodowały, że ten typ dyrektyw stał się swego rodzaju hamulcem postępu technicznego. Dodatkowo państwa wspólnoty nie miały obowiązku wycofywania własnych przepisów nawet gdy nie były one zgodne z dyrektywą. W ten sposób nie spełniały one swej funkcji harmonizacji, a dodatkowo stawały się barierą w wdrażaniu nowych rozwiązań.

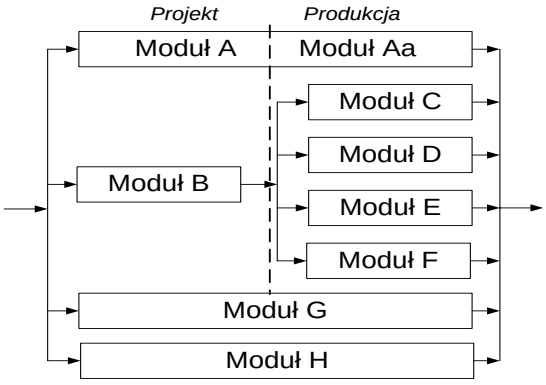
Od 1985 roku do harmonizacji regulacji technicznych we wspólnocie zaczęto stosować tzw. Nowe Podejście. Istotą Dyrektyw Nowego Podejścia jest harmonizacja wyłącznie podstawowych wymagań związanych z bezpieczeństwem, zdrowiem i ochroną środowiska. Szczegółowe wymagania są zawarte w normach zharmonizowanych, lecz ich stosowanie nie jest obowiązkowe i producent może wybrać inny sposób spełnienia wymagań. Produkt zgodny z wymaganiami dyrektyw jest oznaczany symbolem CE, a państwa członkowskie nie mogą zabronić ani utrudniać wprowadzenia na rynek tych wyrobów. Dyrektywa określa również procedury oceny zgodności wyrobu z jej wymaganiami.

Poważnym problemem mogło stać się stosowanie zróżnicowanych procedur oceny zgodności w poszczególnych krajach członkowskich, a co za tym idzie nie uznawanie deklaracji zgodności, poza krajem jej wydania. Stąd kolejnym etapem w harmonizacji regulacji technicznych stało się zadanie ujednolicenia procedur oceny zgodności. W tym celu rada EWG wydała decyzję 90/683/EWG „w sprawie modułów dla różnych faz procedur oceny zgodności przeznaczonych do stosowania w dyrektywach normalizacji technicznej", zastąpioną z kolei Decyzją Rady 93/465/EWG. Decyzja ta określa globalne podejście do oceny zgodności, polegające na zastosowaniu w dyrektywach procedur oceny na podstawie realizacji modułów.

Na rysunku 4.1 przedstawiono schemat modułowy procedur oceny zgodności, gdzie odpowiednie moduły oznaczają:

A – Wewnętrzna kontrola projektu.

Producent przechowuje dokumentację techniczną przygotowaną zgodnie z dyrektywą w ce-



Rys. 4.1: Uproszczony schemat modułowy procedur oceny zgodności

lu umożliwienia ewentualnej kontroli przez upoważniony organ państwowy, wystawia deklarację zgodności oraz umieszcza oznakowanie CE na wyrobie. Jednostka notyfikowana nie bierze udziału w tym module.

Aa – Zgodność wyrobu z wymaganiami.

Producent deklaruje zgodność wyrobu z wymaganiami zasadniczymi wystawiając deklarację zgodności oraz umieszcza oznakowanie CE. Jeśli producent nie stosuje norm zharmonizowanych, jednostka potwierdza na podstawie badań, zgodność z wymaganiami zasadniczymi.

B – Badanie typu.

Producent przedstawia jednostce notyfikowanej dokumentację techniczną oraz wyrób do badań. Jednostka notyfikowana sprawdza zgodność wyrobu z wymaganiami zasadniczymi i wystawia certyfikat zgodności typu.

C – Zgodność wyrobu z określonym typem (występuje w połączeniu z modułem B).

Producent zapewnia zgodność wyrobu z typem posiadającym certyfikat zgodności typu wydany przez jednostkę notyfikowaną na zasadach modułu B, wystawia deklarację zgodności i umieszcza oznakowanie CE. Udział jednostki notyfikowanej ograniczony do zakresu wynikającego z modułu B.

D – Zapewnienie jakości produkcji (występuje w połączeniu z modułem B).

Producent stosuje system zarządzania jakością wg normy ISO 9000, wystawia deklarację zgodności wyrobu z certyfikowanym typem, umieszcza oznakowanie CE na wyrobie. Jednostka notyfikowana zatwierdza i prowadzi nadzór nad systemem jakości oraz działa w zakresie określonym przez moduł B.

E – Zapewnienie jakości wyrobu (występuje w połączeniu z modułem B).

Producent stosuje system zarządzania jakością wg normy ISO 9000 w odniesieniu do produkcji i prób, wystawia deklarację zgodności z certyfikowanym typem, umieszcza oznakowanie CE na wyrobie. Jednostka notyfikowana zatwierdza i prowadzi nadzór nad systemem jakości oraz działa w zakresie określonym przez moduł B.

F – Weryfikacja wyrobu.

Producent deklaruje zgodność z certyfikowanym typem lub wymaganiami zasadniczymi wystawiając deklarację zgodności i umieszcza oznakowanie CE na wyrobie. Jednostka notyfikowana weryfikuje zgodność, wystawia certyfikat zgodności oraz działa w zakresie określonym przez moduł B.

G – Weryfikacja produkcji jednostkowej.

Producent przedstawia dokumentację techniczną i wyrób do badań przez jednostkę notyfikowaną, wystawia deklarację zgodności z wymaganiami zasadniczymi, umieszcza oznakowanie

CE na wyrobie. Jednostka notyfikowana weryfikuje zgodność z wymaganiami zasadniczymi i wydaje certyfikat dla konkretnego wyrobu.

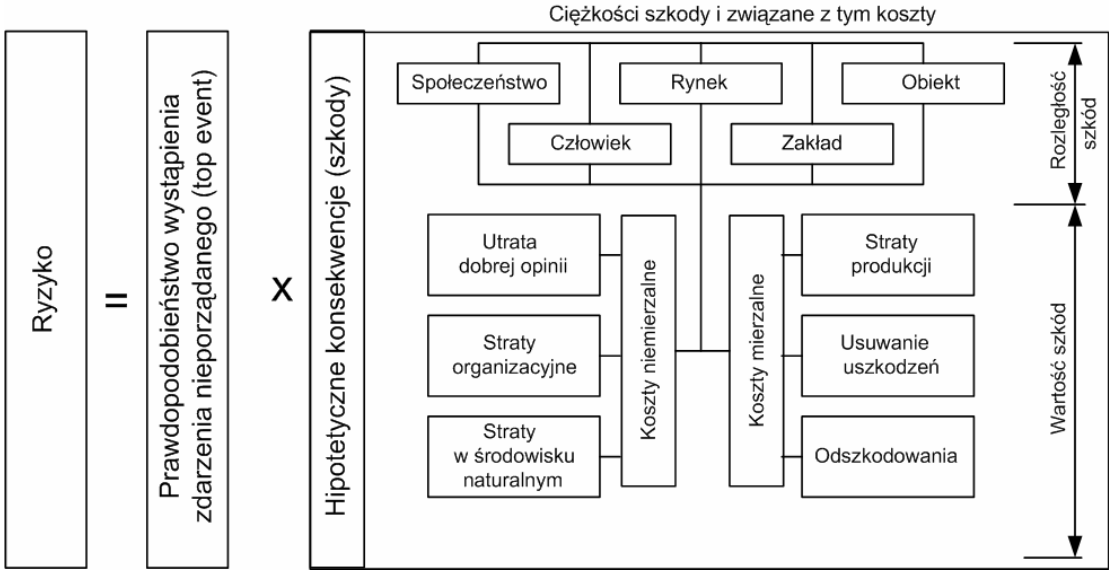
H – Pełne zapewnienie jakości.

Producent stosuje system zarządzania jakością w fazie projektowania i produkcji, deklaruje zgodność projektu z wymaganiami zasadniczymi oraz zgodność wyrobów z projektem, wystawia deklarację zgodności i umieszcza oznakowanie CE na wyrobach. Jednostka notyfikowana wydaje certyfikat zgodności projektu i nadzoruje system jakości.

Procedura oceny zgodności jest uproszczona w przypadku:

1. stosowania norm zharmonizowanych (moduł Aa)
2. stosowania systemu zarządzana jakością ISO 9000 (moduł D i E)

Za każdym razem gdy jest mowa, że producent wystawia deklarację zgodności, a jednostka notyfikowana potwierdza zgodność z wymaganiami zasadniczymi i nie są stosowane normy zharmonizowane czy system zarządzania jakością producent lub/i jednostka notyfikowana powinni przeprowadzić badania pozwalające na ocenę spełnienia zasadniczych wymagań. Wiąże się to z koniecznością wykonania analizy ryzyka. Im dokładniejsza ocena ryzyka tym łatwiej i ściślej można spełnić wymagania. Na rozrzut oceny ryzyka wpływa wiele czynników między innymi zmiana warunków pracy maszyny.
W praktyce inżynierskiej ryzyko rozumiane jest jako kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i konsekwencji tak materialnych jak i niematerialnych tego zdarzenia. W szczególności mogą być analizowane konsekwencje w postaci możliwych ofiar śmiertelnych i liczby rannych, kosztów rekonstrukcji, strat wynikających z ograniczonej aktywności gospodarczej, strat środowiskowych i innych (Rys.4.2).



Rys. 4.2: Elementy ryzyka [4.11]

Z tego punktu widzenia można powiedzieć, że celem inżynierii bezpieczeństwa jest osiągnięcie w maksymalnym stopniu akceptowalnego poziomu ryzyka. W tym miejscu należy podkreślić, że chociaż inżynier nie bierze udziału bezpośrednio w kształtowaniu decyzji odnośnie akceptowalnego poziomu ryzyka to stale musi odpowiadać na pytanie czy proponowany przez niego poziom bezpieczeństwa jest dostateczny, czy może lub powinien być zaakceptowany. Zanim bardziej szczegółowo rozpatrzymy możliwości oszacowania poziomu akceptowalnego ryzyka, proponuje się by zwrócić uwagę na rolę etycznej strony tego zagadnienia. W pracy [4.4] punktem wyjścia w rozważaniach nad etyką podejmowania decyzji odnośnie akceptowalności ryzyka jest etyka deontologiczna (etyka obowiązku), w której przyjęte rozstrzygnięcia oceniane są ze względu na stopień spełnienia imperatywów (nakazów).

W tym ujęciu bezwarunkowy nakaz etyki deontologicznej wyprowadzony wprost z etyki kantowskiej w pracy [4.14] przedstawiono jako imperatyw który mówi: „Postępuj wedle takiej tylko zasady, co do której mógłbyś jednocześnie chcieć, aby stała się prawem powszechnym". Znajduje to odzwierciedlenie w ważnych aktach prawnych np. w Powszechnej Deklaracji Praw Człowieka zawarte są między innymi następujące zapisy:

Artykuł 1

Wszyscy ludzie rodzą się wolni i równi w swej godności i w swych prawach. Są oni obdarzeni rozumem i sumieniem i powinni postępować wobec innych w duchu braterstwa.

Artykuł 2

Każdy człowiek jest uprawniony do korzystania z wszystkich praw i wolności wyłożonych w niniejszej Deklaracji, bez względu na różnice rasy, koloru skóry, płci, języka, religii, poglądów politycznych lub innych przekonań, narodowości, pochodzenia społecznego, majątku, urodzenia lub jakiekolwiek inne różnice.

Nie wolno ponadto czynić żadnej różnicy w zależności od sytuacji politycznej, prawnej lub międzynarodowej kraju lub obszaru, do którego dana osoba przynależy, bez względu na to, czy jest on niepodległy, powierniczy, autonomiczny lub poddany innym ograniczeniom suwerenności.

Artykuł 3

Każdy człowiek ma prawo do życia, wolności i bezpieczeństwa swojej osoby.

Podobne treści zostały również zawarte w Karcie Praw Podstawowych Unii Europejskiej w następujących artykułach:

Artykuł 1

Godność ludzka

Godność ludzka jest nienaruszalna. Musi być szanowana i chroniona.

Artykuł 2

Prawo do życia

1. Każdy ma prawo do życia.
2. Nikt nie może być skazany na karę śmierci ani poddany jej wykonaniu.

Artykuł 3

Prawo do integralności osoby

1. Każdy ma prawo do poszanowania swej integralności fizycznej i psychicznej.

Pewną ilustracją powyżej przedstawionych zasad są zamieszczone na rysunku 4.3 linie poziomu ryzyka. Ilustrację przytoczono za pracą [4.12]. Wybór współrzędnych logarytmicznych pozwolił przedstawić szereg zjawisk o różnym poziomie akceptowalności oraz wyróżnić tę grupę zjawisk, która w zadowalającym stopniu opisana jest odcinkiem prostej. Zwraca uwagę fakt akceptowalności wyższego poziomu ryzyka związanego z katastrofami naturalnymi niż ryzyka wynikającego z działalności człowieka. W tym drugim przypadku widać wpływ dodatkowych czynników na poziom akceptowalności. Porównując położenie krzywych dla transportu chloru i plutonu, zauważamy mniejszą akceptowalność dla tego ostatniego. Wynika to z braku doświadczeń oraz większej niepewności odnośnie możliwych zagrożeń i bardziej dramatycznych przebiegów katastrof. Poza tym transport materiałów radioaktywnych budzi więcej kontrowersji niż przewóz innych niebezpiecznych materiałów.

Uwzględniając przedstawione wyniki dotyczące naturalnych katastrof, w pracy [4.13] podjęto próbę określenia reguł, które mogłyby być wykorzystane do definiowania akceptowalnego poziomu ryzyka. Historyczna analiza zachowań ludzi wobec ryzyka związanego z wprowadzeniem nowych technologii wykazała, że istnieje dodatnie skorelowanie pomiędzy użytecznością rozwiązania technicznego a poziomem akceptowalnego ryzyka. Uzyskane rezultaty pozwoliły na sformułowanie następujących reguł:

- poziom akceptowalnego ryzyka rośnie zgodnie z użytecznością podniesioną do trzeciej potęgi;
- ryzyko, które podejmowane jest dobrowolnie, może być o 10^3 większe od ryzyka narzuconego wbrew naszej woli;
- przyjęte wbrew naszej woli ryzyko może być zaakceptowane mimo braku widocznej użyteczności, jeśli jest mniejsze od ryzyka-związanego z naturalnymi katastrofami;
- ryzyko powinno być przyjmowane według zasady ALARP (ang. *As Low* As *Reasonably Practicable)*;
- w ocenie bezpieczeństwa nie istnieje ograniczenie w czasie (horyzont czasowy);
- przyszłe generacje nie mogą ponosić ciężarów obecnie przyjmowanych rozwiązań;
- otrzymana ocena ryzyka powinna być poddana analizie niepewności.

Spośród metod ustalania wartości kryterialnych ryzyka zwraca uwagę wspomniana wcześniej procedura ALARP, której podstawą są wyniki analizy ryzyka.

Na rysunku 4.4 ilustrującym tą metodę, granicami obszaru stosowalności procedury są: poziom maksymalnego ryzyka tolerowanego oraz poziom ryzyka akceptowalnego.

Jak podaje Brandowski [4.1], w kolejnictwie Wielkiej Brytanii przyjmuje się następujące wartości kryterialne:

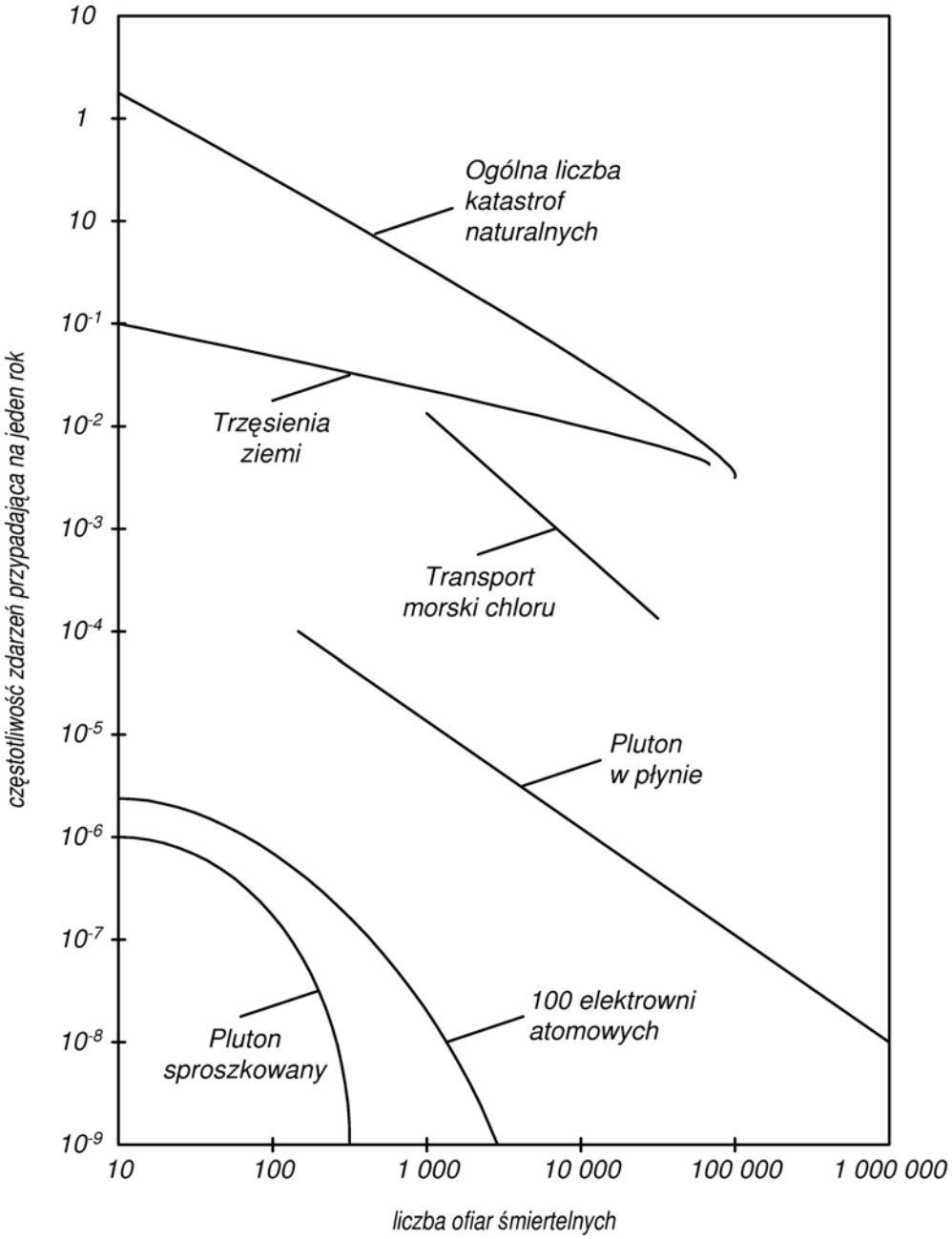
- górna granica obszaru ALARP definiowana jest przez indywidualne ryzyko pracowników kolei – 10^{-3} oraz indywidualne ryzyko pasażerów i osób trzecich – 10^{-4} zgonów/rok;
- odpowiednio dolną granicę określa indywidualne ryzyko pracowników, pasażerów i osób trzecich, które nie może być większe niż 10^{-6} zgonów/rok.

Zauważmy, że omawiając miary ryzyka, skupiono się na oszacowaniu ryzyka neutralnego, którego miary tworzone są na podstawie krzywej Farmera i wartości oczekiwanej, bezpośrednio wyprowadzanych z funkcji gęstości prawdopodobieństwa. W przypadku oceny akceptacji ryzyka czy awersji ryzyka, wprowadza się dodatkowe współczynniki wagi wartości oczekiwanej, współczynniki awersji lub uwzględnia rozrzut opinii, analizując odchylenie standardowe. Szerzej zagadnienia wyboru miar ryzyka przedstawiono w pracy [4.8].

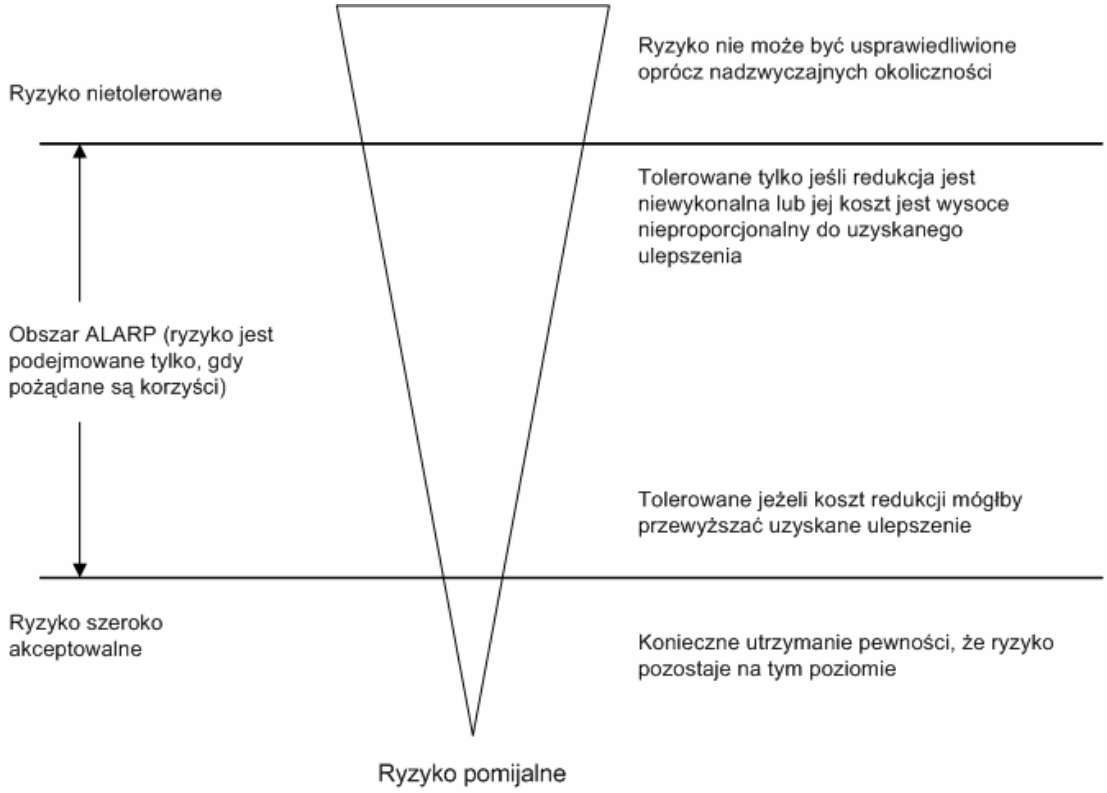
4.2. Modelowanie niepewności

W środowisku naukowo-technicznym coraz szersze zainteresowanie towarzyszy próbom wykorzystania metod diagnostyki wibroakustycznej w analizach procesów degradacji i niezawodności krytycznych elementów układów technicznych. Najczęściej podstawę przyjmowanego sposobu postępowania stanowi metodologia bayesowska, w której w odróżnieniu do klasycznej teorii estymacji zakładającej zdeterminowany charakter parametrów, przyjmuje się pewną, różnie rozumianą losowość. Oznacza to konieczność przyjęcia założenia o istnieniu apriorycznej nieokreśloności, opisanej apriorycznymi rozkładami prawdopodobieństwa. Takie rozumowanie jest pochodną założenia przyjętego między innymi przez Bernouliego i Laplace'a, że prawdopodobieństwo jest miarą stopnia niepewności [4.10]. Rozwinięciem tego sposobu rozumienia prawdopodobieństwa były prace Bayes'a, w których estymowano prawdopodobieństwo warunkowe na podstawie prawdopodobieństw niewarunkowych. Mimo ogromnego rozwoju tych metod podstawowym problemem pozostaje brak uzasadnionych reguł wyboru rozkładów apriorycznych.

W klasycznym bayesowskim ujęciu, zgodnie z zasadą Laplace'a, w przypadku braku informacji apriorycznej przyjmuje się rozkład równomierny jako rozkład aprioryczny. W połowie XX wieku Jeffreys opracował teorię ustalania rozkładów apriorycznych na podstawie danych eksperymentalnych. Ogromną zaletą tego sposobu postępowania jest stworzenie możliwości ustalenia rozkładu apriorycznego nawet na podstawie niewielkiego zbioru zdarzeń. Dodatkowo możliwa jest w ten sposób kwalifikacja miary subiektywnego, ludzkiego doświadczenia, czy wręcz indywidualny stosunek do



Rys. 4.3: Ryzyko związane z wystąpieniem katastrof naturalnych oraz uszkodzeń systemów i środków technicznych wykreowanych przez człowieka [4.12]



Rys. 4.4: Metoda ALARP [4.1]

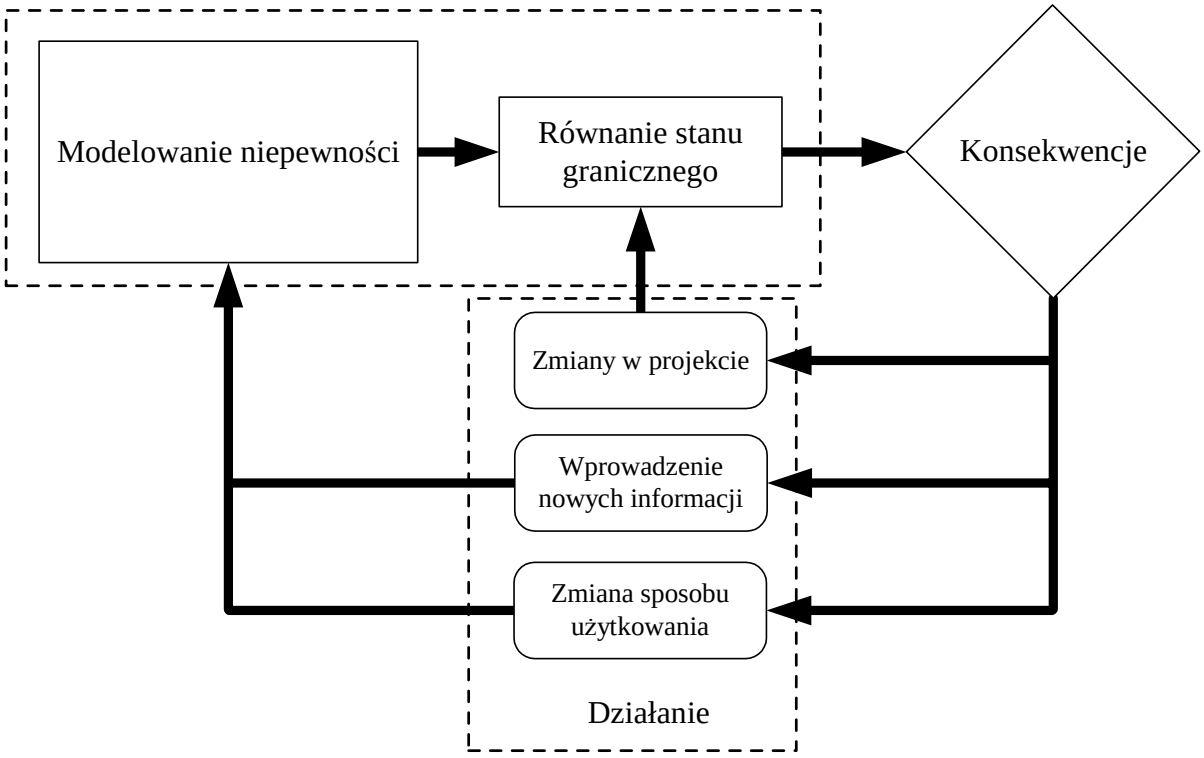
uzyskanych rezultatów badań i eksperymentów. Ostatnio coraz częściej podejmowane są próby wykorzystania tego podejścia w aplikacji rezultatów diagnostyki. Przykładem wykorzystania tego podejścia jest propozycja oceny prawdopodobieństwa uszkodzenia systemu przedstawionego na rysunku 4.5.

Z tego względu w zagadnieniach zarządzania ryzykiem szczególne miejsce zajmują zagadnienia analizy niepewności, bowiem trudno wyobrazić sobie odpowiedzialne wykorzystywanie przez decydenta przedstawionych mu rezultatów oszacowania ryzyka jeśli potencjalne szkody i ich prawdopodobieństwo są nieznane lub wysoce niepewne. Stąd, zmniejszenie niepewności analiz i ocen ryzyka pozostaje jednym z podstawowych zagadnień od wielu lat. W pracy [4.2], w której podjęto między innymi zagadnienie modelowania z uwzględnieniem niepewności podkreślono, że zagadnienia zmniejszenia niepewności stanowią istotę analizy ryzyka technicznego.

W ogólności można powiedzieć, że zjawisko randomizacji, niepełna informacja statystyczna w zadaniu estymacji parametrów modelu, przyjęcie uproszczonych modeli zjawisk i procesów, uproszczenie procedur określania zmiennych procesu zużycia i degradacji, wpływ warunków środowiska, modelowania błędów operatora a w szczególności procedur określania relacji i wzajemnych sprzężeń w systemie człowiek-środowisko-technika, są wskazywane jako istotne źródła niepewności.

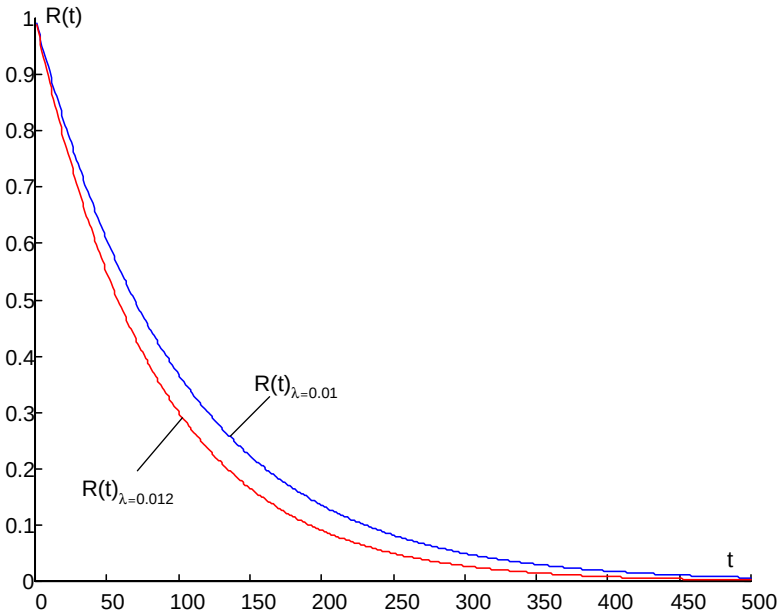
Problematyka źródeł niepewności jest szeroko analizowana w literaturze. Na przykład [4.9] zwracając uwagę, że algorytm oszacowania ryzyka można traktować jako szczególny sposób integrowania informacji z różnych źródeł, podkreśla konieczność analizy niepewności modelowania systemów, szczególnie ich kompletności, adekwatności i stopnia pewności parametrów modelu oraz podobnej analizy stosowanych metod symulacyjnych. Inną systematykę wprowadza Hryniewicz [4.6], który dzieli informacje na klasy (pewne i precyzyjne, niepewne i precyzyjne, pewne i nieprecyzyjne, oraz niepewne i nieprecyzyjne) i wskazuje, że najciekawsze zadanie z punktu widzenia wykorzystania wyników obserwacji diagnostycznej mamy wówczas, gdy decyzja jest podejmowana po analizie wyników eksperymentu wyjaśniającego mechanizm wpływu czynników losowych.

Ogólnie można stwierdzić, że w analizie ryzyka i badaniu niepewności systemów technicznych rozróżnia się następujące typy niepewności [4.5]: właściwą losową zmienność lub niepewność, niepewność

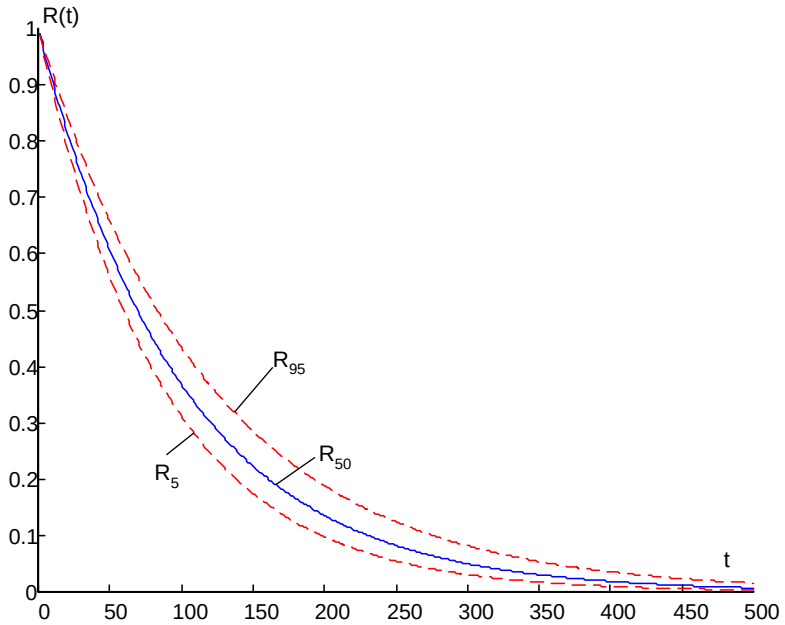


Rys. 4.5: Bayesowska ocena prawdopodobieństwa uszkodzeń systemu [4.5]

epistemologiczną i niepewność aleatoryczną. Analizując właściwą zmienność losową wprowadza się dwie kategorie niepewności: niepewność na którą działalność człowieka nie ma wpływu, do której należą zjawiska i katastrofy naturalne. Drugą grupę stanowi niepewność, którą można zmniejszyć dzięki działalności człowieka. Na przykład zmniejszenie prawdopodobieństwa wystąpienia zdarzenia niepożądanego w systemie technicznym może być efektem wprowadzenia nowoczesnych metod produkcji i kontroli jakości. W tym miejscu warto przybliżyć istotę różnicy pomiędzy niepewnością epistemologiczną i aleatoryczną, bowiem próby ich zmniejszenia wymagają w każdym przypadku zupełnie innych zabiegów. Na wstępie porównajmy rezultaty estymacji funkcji niezawodności w przypadku występowania jakościowo różnych przyczyn niepewności wykorzystując wyniki przedstawione na rysunkach 4.6 i 4.7. Na rysunku 4.6 zaznaczone krzywe obrazują funkcje niezawodności rozkładu wykładniczego otrzymane na podstawie dwóch różnych wartości funkcji intensywności uszkodzeń.
Taki wynik otrzymamy w przypadku braku dostatecznej wiedzy o mechaniźmie i intensywności procesu uszkodzeń. Ogólnie niepewność epistemologiczną dzieli się na dwie kategorie. Do pierwszej zalicza się niepewność, która może być zmniejszona w efekcie prac badawczych lub ogólnie poznawczej aktywności człowieka. Przykładem tego będzie próba zmniejszenia niepewności przez rozwinięcie zbyt uproszczonego modelu zjawiska lub procesu. Drugą kategorię tworzy niepewność odnośnie możliwej prognozy zachowania się systemu w przyszłości. W tym przypadku możliwość zmniejszenia niepewności istnieje, ale ze względu na stochastyczny charakter wpływu czynników zewnętrznych, szczególnie środowiskowych jest znacznie mniejsza, w porównaniu do efektów możliwych do uzyskania, w przypadku niepewności poprzedniej kategorii. Niezależnie od kategorii rozważanej niepewności epistemologicznej, wskazuje się na [4.3] cały szereg zagadnień, które muszą być podjęte dla otrzymania użytecznego opisu niepewności. W pierwszej kolejności należy do nich zaliczyć: konwersję dostępnej informacji w matematyczne formuły dostosowane do wymogów opisu epistemologicznej niepewności, agregację niepewności towarzyszącej różnym źródłom i utworzenie jednolitej reprezentacji niepewności, określenie wpływu niepewności wejść i niepewności modelu na strukturę niepewności analizowanych rezultatów, dobór sposobu prezentacji z właściwą interpretacją niepewności rezultatów oraz przeprowadzenie analizy wrażliwości.



Rys. 4.6: Funkcja niezawodności jako przykład niepewności epistemologicznej odnośnie funkcji intensywności uszkodzeń



Rys. 4.7: Funkcja niezawodności jako przykład niepewności aleatorycznej obrazujący przypadkowość realizacji w wyznaczonych granicach

Dla porównania, na rysunku 4.7 zilustrowano istotę niepewności aleatorycznej związanej ze statystyczną ewaluacją rezultatów testów i obserwacji. Może ona być związana i wynikać z:

1. przyjętych procedur estymowania statystycznych parametrów rozkładu prawdopodobieństwa na podstawie ograniczonej liczby wyników obserwacji lub testów;
2. pomijania wpływu systematycznych zmian obserwowanych zmiennych;
3. pomijania możliwego skorelowania zmiennych.

Przykładem statystycznej niepewności jest częstotliwościowa ocena prawdopodobieństwa uszkodzenia elementu systemu na podstawie ograniczonej liczby obserwacji.

Najczęściej w tego typu eksperymentach zakłada się, że znane są klasy rozkładów prawdopodobieństwa, natomiast na podstawie obserwacji diagnostycznych należy określić parametry tych rozkładów. W ogólnym przypadku gdy brak przesłanek do przyjęcia hipotezy o rozkładzie prawdopodobieństwa można odwołać się do wyboru rozkładu prawdopodobieństwa na podstawie zasady Jaynes'a [4.7] o maksymalizacji entropii rozkładu.

W ogólności możemy powiedzieć, że jesteśmy w stanie określić wartości oczekiwane dla funkcji zmiennej losowej X, która przyjmuje wartości $x_1, x_2, x_3, \ldots, x_n$:

$$m_{1_r} = \sum_{k=1}^{n} p_k g_r(x_k) \;\; - \;\; \text{dla}\, r = 1 \ldots l \tag{4.1}$$

Uwzględniając zależność:

$$\sum_{k=1}^{n} p_k = 1 \tag{4.2}$$

otrzymujemy $l+1$ zależności pomiędzy poszczególnymi prawdopodobieństwami $p_1 \ldots p_n$. Jaynes [4.7] zauważył, że w przypadku, gdy $n > l+1$ mamy nieskończenie wiele możliwych rozkładów prawdopodobieństwa, które będą spełniać zależności (4.1) i (4.2), a podstawą wyboru jednego z nich może być maksymalna entropia rozkładu, obrazująca stan naszej niepewności. Jeżeli zostałby wybrany rozkład o mniejszej entropii oznaczałoby to, że dysponowaliśmy dodatkową informacją, którą wykorzystaliśmy w mniej lub bardziej świadomy sposób.

Zasadę maksimum entropii Jaynes'a można zapisać w następujący sposób – maksymalizujemy wyrażenie

$$H = -\sum_{k=1}^{n} p_k \ln p_k \tag{4.3}$$

uwzględniając ograniczenia

$$\sum_{k=1}^{n} p_k q_r(x_k) = m_{1_r}; \quad \sum_{k=1}^{n} p_k = 1 \tag{4.4}$$

oraz

$$p_k \geqslant 0 \quad \text{dla} \qquad \begin{matrix} r = 1 \ldots l \\ k = 1 \ldots n \end{matrix} \tag{4.5}$$

Zauważmy, że w powyższym ujęciu zakłada się, że nie posiadamy dodatkowej informacji o możliwych zmianach wartości parametrów rozkładu prawdopodobieństwa. W wielu przypadkach obserwacje diagnostyczne pozwalają założyć śledzenie ewolucji wartości parametrów. Zagadnienia wykorzystywania rezultatów procedur diagnostycznych będą tematem kolejnych rozdziałów.

Bibliografia

[4.1] Brandowski A. *Nauka o bezpieczeństwie*. Politechnika Warszawska, 1993.

[4.2] Dybała J., Mączak J., Radkowski S. *Wykorzystanie sygnału wibroakustycznego w analizie ryzyka technicznego*. ITE, Warszawa – Radom, 2006.

[4.3] Editorial Guest. *Alternative representations of epistemic uncertainty, Reliability Engineering and System Safety*, wolumen 85. 2004.

[4.4] Ersdal E., Aven T. Risk informed decision-making and its ethical basis. *Reliability Engineering & System Safety*, (93):197–203, 2008.

[4.5] Faber M.H. *Risk and Safety in Civil Engineering*. Swiss Federal Institute of Technology, 2001.

[4.6] Hryniewicz O. *Podejmowanie decyzji w warunkach losowej niepewności I przy nieprecyzyjnym modelu decyzyjnym. Badania operacyjne i systemowe wobec wyzwań XXI wieku*. 2002.

[4.7] Jaynes E.T. *Information Theory and Statistical Mechanics, Physical Reviews*, wolumen 106. 1957.

[4.8] Jonkman B., Gelder van P., Vrijliny H. *An overview of quantitative risk measures and their application for calculation of flood risk*. ESREL, 2002.

[4.9] Kosmowski K.T. *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrownii jądrowych*. Politechnika Gdańska, Gdańsk, 2003.

[4.10] Nozer D., Singpurwalla N.D. *Reliability and Risk A Bayesian Perspective*. John Wiley & Sons Ltd, Chichester England, 2006.

[4.11] Radkowski S. *Podstawy bezpiecznej techniki*. OWPW, 2003.

[4.12] Roland M.E., Moriarty B. *System Safety Engineering Management*. John Willey & Sons, New York, 1990.

[4.13] Schneiber J., redaktor. *Risiko und Sicherhbeit technischer Systeme*. Birkhäuser Verlag, Bazylea, 1991.

[4.14] Tatarkiewicz W. *Historia filozofii*, wolumen 2, str. 177. PWN, Warszawa, 1970.

Rozdział 5

Diagnostyka weryfikacyjna podsystemów i urządzeń

Kazimierz T. KOSMOWSKI, Jacek ZAWALICH

5.1. Zakres diagnostyki weryfikacyjnej

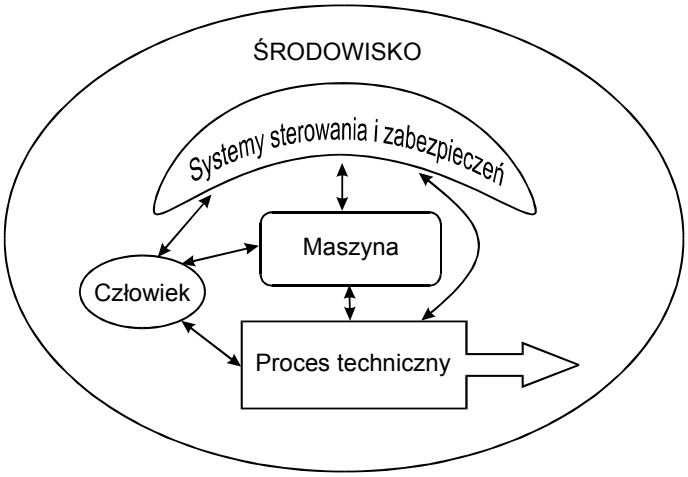
Diagnostyka techniczna rozwija się dynamicznie od przeszło 30 lat. Początkowo dotyczyła maszyn i urządzeń mechanicznych. Obecnie jej zainteresowanie rozszerzyło się na urządzenia, układy oraz systemy elektryczne i elektroniczne, jak również instalacje technologiczne, układy sterowania oraz systemy związane z bezpieczeństwem. Z pomocą metod diagnostycznych można określać i oceniać aktualny stan maszyny lub złożonego procesu, oraz przewidywać jego przebieg w określonym okresie predykcji.

Diagnostyka maszyn w dużym stopniu bazuje na wykonywaniu pomiarów bezpośrednich oraz na badaniach pośrednich, które głównie wykorzystują procesy resztkowe towarzyszące funkcjonowaniu danej maszyny. Procesy te mają charakter elektryczny, mechaniczny, lub cieplny. Z pośród tej kategorii najczęściej stosuje się metody wibroakustyczne, ultradźwiękowe oraz termowizyjne [5.5].

Diagnostykę techniczną można podzielić na diagnostykę uszkodzeniową, która zajmuje się identyfikacją i lokalizacją uszkodzeń i defektów maszyny lub jego podzespołów oraz na diagnostykę weryfikacyjną, której zadaniem jest kontrola i ciągła weryfikacja istotnych parametrów z przyjętym modelem, traktowanym jako wzorcowy. Dzięki diagnostyce weryfikacyjnej można określić czy dany obiekt jest zdatny do wykonywania postawionych zadań, czyli czy wartości wybranych istotnych parametrów zawierają się w dopuszczalnych granicach. Odstępstwa od wzorcowego modelu są wówczas informacją o nieprawidłowej pracy maszyny lub przebiegu danego procesu. Na podstawie ciągłej rejestracji dostępnych parametrów obiektu rzeczywistego jest również możliwość prognozowania zmian jego stanu w danym horyzoncie czasowym.

Złożony układ urządzeń i elementów (określony jako maszyna), realizowany proces techniczny, układy zabezpieczeń oraz człowiek pracujący w ich obecności, to podstawowe i nierozerwalne elementy każdego systemu technicznego (Rys.5.1). Chcąc go analizować prawidłowo, trzeba rozpatrywać wszystkie jego elementy w sposób kompleksowy. Nawet, jeśli rozpatruje się fragment złożonego systemu, należy uwzględniać wszystkie zewnętrzne uwarunkowania, które w sposób znaczący wpływają na pracę i właściwości urządzeń składowych oraz na jakość końcowego produktu.

Systemy, urządzenia, podukłady i inne elementy składowe mają swój określony i skończony czas życia, na który permanentnie wpływają czynniki wewnętrzne i zewnętrzne nierozerwalnie zależne od aktualnego stanu środowiska. Każdy projekt nowych urządzeń oraz systemów sterujących, kontrolujących, czy też zabezpieczających musi uwzględniać ich wpływ, aby zapewnić prawidłowe funkcjonowanie tych urządzeń i spełnianie powierzonych im zadań. Istnienie systemu technicznego, którego zadaniem jest wytwarzanie konkretnych dóbr materialnych wiąże się z ingerencją w środowisko po-



Rys. 5.1: Struktura systemu technicznego

przez czerpanie z zasobów ziemskich, z zakłócaniem naturalnych ekosystemów, degradacją i zmianami w najbliższym otoczeniu człowieka. System techniczny jest przede wszystkim czynnikiem, który stanowi źródło potencjalnych i rzeczywistych zagrożeń. Nie ma możliwości całkowitego wyeliminowania wpływu danego obiektu technicznego na najbliższe otoczenie w tym również uszkodzeń, i awarii. Można jedynie zmniejszać ich częstość i rozmiary w sposób kontrolowany, w zależności od potrzeb i tolerancji, które wymaga człowiek i środowisko. Dlatego też potencjalne zagrożenia należy przewidywać już w fazie projektu danego systemu lub urządzenia, aby odpowiednio wcześniej przedsięwziąć odpowiednie środki mające na celu zabezpieczenie przed ewentualnymi niepożądanymi skutkami, szczególnie tymi, które są o znacznych rozmiarach i mają charakter katastrofalny [5.1], [5.6].

Diagnostykę techniczną należy brać po uwagę w każdym etapie życia systemu technicznego, dowolnej maszyny lub instalacji technicznej. Głównym jej celem jest wypracowanie oceny dotyczącej ich gotowości do wypełnienia postawionych zadań lub przypisanych funkcji. W szczególności bierze się tu pod uwagę:

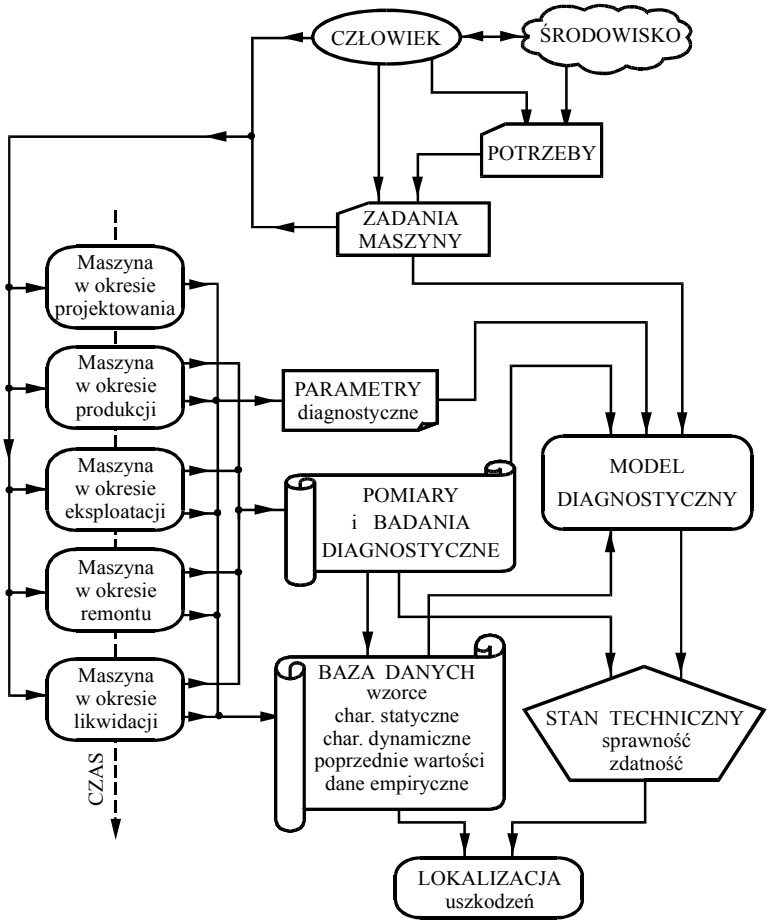
- zapewnienie wysokiej dyspozycyjności danej maszyny (czyli wysokiej niezawodności i trwałości),
- zabezpieczenie jej i urządzeń towarzyszących przed awariami i poważnymi katastrofami,
- prognozowanie czasu sprawności, okresów prowadzenia przeglądów i testów sprawdzających.

Badania diagnostyczne obejmują zarówno pomiary, kontrolę, jak i formułowanie oceny diagnostycznej zawierającej określenie sprawności i jakości badanego urządzenia. Informacje diagnostyczne pozyskuje się na każdym etapie życia systemu technicznego (Rys.5.2). Mogą to być komputerowe badania symulacyjne, oszacowania ekspertów lub dane z systemów o podobnym przeznaczeniu i podobnej strukturze. Jednak dopiero w okresie powstawania i eksploatacji systemu, będącego przedmiotem rozważań, można uzyskać dokładne dane poparte pomiarami z elementów rzeczywistych. W okresie projektowania wprawdzie nie ma możliwości wykonywania pomiarów, ale należy przewidzieć taką strukturę przyszłego urządzenia, która pozwoli na sprawne ich wykonywanie i to zgodnie z potrzebami diagnostycznymi oraz z możliwością szybkiego i wiarygodnego kontrolowania funkcji wymaganych przez to urządzenie. Okres produkcji i likwidacji to okres kompleksowych testów i konieczność weryfikacji wyprodukowanych lub wyeksploatowanych elementów urządzenia.

Proces diagnozowania wymaga utworzenia modelu diagnostycznego obejmującego istotne elementy systemu, niezbędne przy określaniu oceny końcowej. W modelowaniu można posłużyć się metodą dekompozycji wyróżniając część technologiczną, sterowniczą, kontrolno-pomiarową oraz część odpowiedzialną za bezpieczeństwo procesu, obsługi technicznej i środowiska. Prowadzenie badań diagnostycznych łączy się z wymaganiem utworzenia modelu diagnostycznego, wybrania istotnych parametrów diagnostycznych oraz skompletowania sprzętu pomiarowego o podwyższonej dokładności w celu uzyskać wiarygodnych oceny stanu danej maszyny w kontekście założonych zadań i funkcji.

Jeżeli diagnozowany jest system bezpieczeństwa, to diagnostyka weryfikacyjna przyjmuje funkcje bezpieczeństwa jako wzorcowe i na ich bazie wnioskuje o zdatności tego systemu oraz o jego okresach niezbędnych przeglądów i testów, aby zapobiegać ewentualnej awarii krytycznego układu lub systemu chronionego

Ocena diagnostyczna powstaje na podstawie aktualnego stanu systemu technicznego (lub na podstawie wyników symulacyjnych – w przypadku okresu projektowania) przyjętego modelu oraz bazy danych o szczegółowych właściwościach poszczególnych elementów. Każdy etap życia systemu ma inne wymagania i możliwości pozyskiwania informacji. W rezultacie wybór metody diagnostycznej wiąże się z wieloma czynnikami, m.in. warunkami zewnętrznymi urządzeń ich stanem technicznym, rodzajem wykonywanych funkcji, możliwością wykonywania pomiarów, nakładami ekonomicznymi i innymi.



Rys. 5.2: Ogólny schemat prowadzenia diagnostyki maszyn krytycznych na różnych etapach życia [5.6]

Stawianie diagnozy odnośnie sprawności i niezawodności oraz bezpieczeństwa poszczególnych elementów jest podstawą do wydania kompleksowej oceny całego systemu technicznego oraz procesu przez niego wykonywanego. W ocenie diagnostycznej istotne są elementy związane z przewidywaniem okresu dyspozycyjności i gotowości pojedynczych elementów i całych układów, które wpływają, często w sposób drastyczny, na okres dyspozycyjności całego systemu oraz koszty eksploatacji i obsługi remontowo-naprawczej. Poszczególne funkcje urządzeń, w tym również funkcje związane z bezpieczeństwem muszą być szczegółowo określone wraz z powiązaniami sprzętowymi, aby oceny diagnostyczne, wytyczne eksploatacyjne, jak również zalecenia dla projektantów były wiarygodne i miały pożądany efekt końcowy.

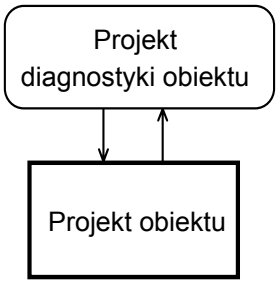
Ważnym okresem życia maszyny lub systemu technicznego jest okres likwidacji. W tym miejscu

diagnostyka ma dość szczególną rolę, gdyż likwidowane urządzenia i całe instalacje techniczne mogą posiadać elementy, które (po odpowiedniej renowacji i przeprowadzonych testach) mogą posłużyć jako elementy zastępcze w innych podobnych instalacjach technicznych. Ogólny schemat dotyczący etapów składowych kompleksowej diagnostyki przedstawiono na Rys.5.2.

5.2. Diagnostyka w okresie projektowania

Na etapie projektowania nowych urządzeń i instalacji krytycznych należy zdefiniować potrzeby sprzętowe strukturalne oraz organizacyjne, które w przyszłości będą niezbędne podczas normalnej eksploatacji, dając szybką i wiarygodną ocenę diagnostyczną. Są to zwykle dodatkowe układy i rozwiązania techniczne z łatwym dostępem do newralgicznych elementów mechanicznych pozwalających na pomiary istotnych parametrów diagnostycznych.

Nowy obiekt powstaje na podstawie określonych założeń, które powinny zawierać wymagania dotyczące prowadzenia przewidywanych badań diagnostycznych w okresie eksploatacji (Rys.5.3). Już na tym etapie należy przewidywać sposoby prowadzenia badań dających szybką i wiarygodną diagnozę. Do tego celu należy projektować dodatkowe elementy umożliwiające przeprowadzanie takich badań, punkty pomiarowe, systemy i układy autotestujące itp. W tym okresie schemat diagnostyki wygląda dość skromnie, ale właśnie wówczas można najtaniej zaprojektować przyszłą diagnostykę, aby w okresie eksploatacji nie ponosić zbyt dużych nakładów ekonomicznych.



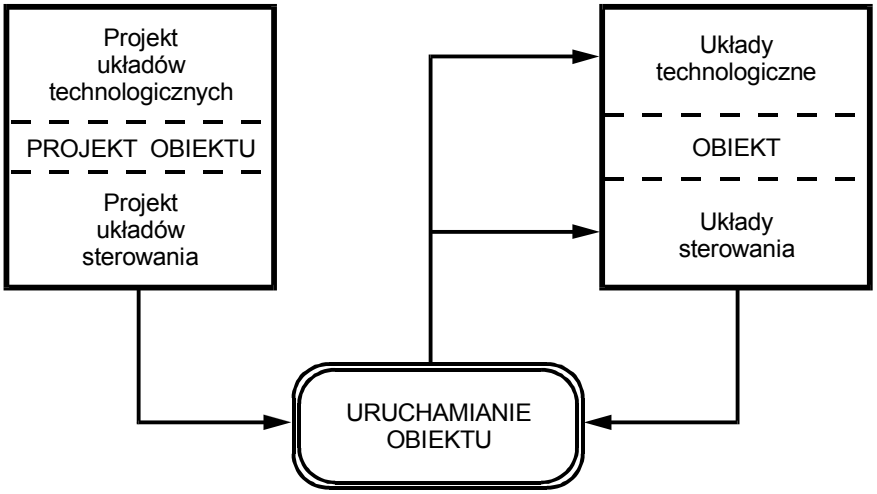
Rys. 5.3: Diagnostyka w okresie projektowania [5.6]

Projektowanie diagnostyki technicznej jest odpowiedzialnym procesem, i jednocześnie dość złożonym, gdyż na tym etapie nie można otrzymać rzeczywistych ocen pracy przyszłego obiektu, a jednocześnie przewidywania projektanta można zweryfikować dopiero po całkowitym zbudowaniu i rzeczywistym uruchomieniu wszystkich jego podzespołów. Pozostają więc jedynie symulacje komputerowe, które bazują na uproszczonych modelach rzeczywistości i bardzo często nie odzwierciedlają w pełni przyszłych problemów eksploatacyjnych.

5.3. Diagnostyka w okresie produkcji

Etap produkcji łączy się z uruchamianiem poszczególnych podzespołów i układów całych bloków sterowania. Prace związane z diagnostyką polegają na tym etapie na wprowadzaniu niewielkich poprawek w strukturze już wykonanej, na implementacji programów sterujących, na dopasowaniu parametrów układów i aparatów do zaprojektowanych wartości (3.22). W urządzeniach można już wtedy wyodrębnić układy odpowiedzialne bezpośrednio za prowadzoną produkcję oraz układu sterownicze i zabezpieczające a często układy zarządzające bezpieczeństwem.

Okres produkcji to czas na dokładne badania całego urządzenia krytycznego, gdyż w tym czasie najłatwiej wyeliminować wszystkie usterki i niedomagania poszczególnych podzespołów, z racji tego, iż nie prowadzona jest eksploatacja produkowanej maszyny krytycznej. Dopuszczenie do eksploatacji powinno być poprzedzone szeregiem testów sprawdzających według przyjętych procedur określonych w czasie projektowania. Odpowiednio zaprojektowane układy diagnostyczne powinny pozwalać na

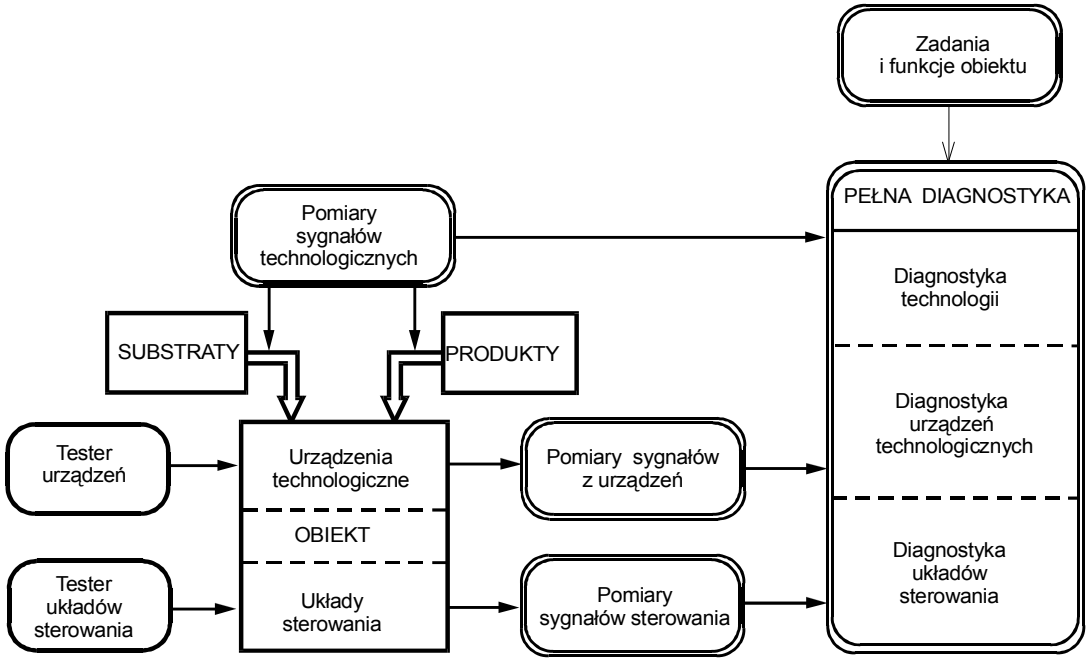


Rys. 5.4: Diagnostyka w czasie produkcji [5.6]

dokładne sprawdzenie wszystkich elementów i podukładów, gdyż okres eksploatacji będzie odwoływał się do wykonanych badań celem porównania i określenia procesów starzenia.

5.4. Diagnostyka w okresie eksploatacji

Eksploatacja jest najtrudniejszym okresem życia maszyny krytycznej, od której wymaga się wypełnienia wszystkich projektowanych funkcji i zadań poszczególnych aparatów i podukładów (Rys.5.5).



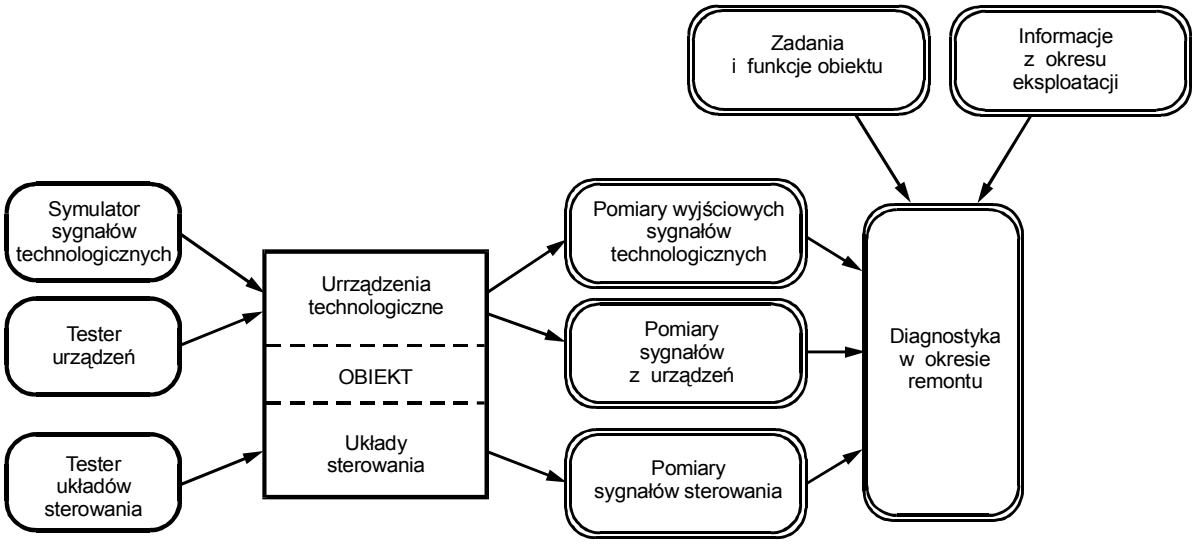
Rys. 5.5: Diagnostyka w okresie eksploatacji [5.6]

Wszystkie układy eksploatacyjne pracują wówczas w znamionowych warunkach. Ich kontrola i okresowa lub ciągła diagnostyka pozwala na wyeliminowanie wielu usterek i uszkodzeń, które mogą w zwiększonej ilości występować w krótkim okresie po uruchomianiu nowej maszyny krytycznej. Każdy obiekt o charakterze krytycznym jest przeznaczony do wykonania konkretnej produkcji, w przypadku turbozespołu jest to określona energia elektryczna lub cieplna. W takim przypadku diagnostykę w

czasie eksploatacji należy rozpatrywać w odniesieniu do części procesowej instalacji krytycznej oraz w odniesieniu do procesu realizowanego przez tę instalację.

5.5. Diagnostyka w okresie remontu

Okres remontu (Rys.5.6) to okres, w którym instalacja krytyczna nie realizuje procesu technologicznego w sposób prawidłowy, więc z założenia występują uszkodzenia, które należy zlokalizować i wyeliminować. Ten okres pod względem diagnostyki jest podobny do okresu produkcji, gdyż również w tym okresie należy wykonać szczegółowe badania wszystkich elementów i podzespołów remontowanej instalacji oraz dodatkowo podjąć decyzje odnośnie wymiany zużytych elementów lub podzespołów. W tym okresie badania diagnostyczne powinny odnosić się do wyników badań uzyskanych podczas eksploatacji.



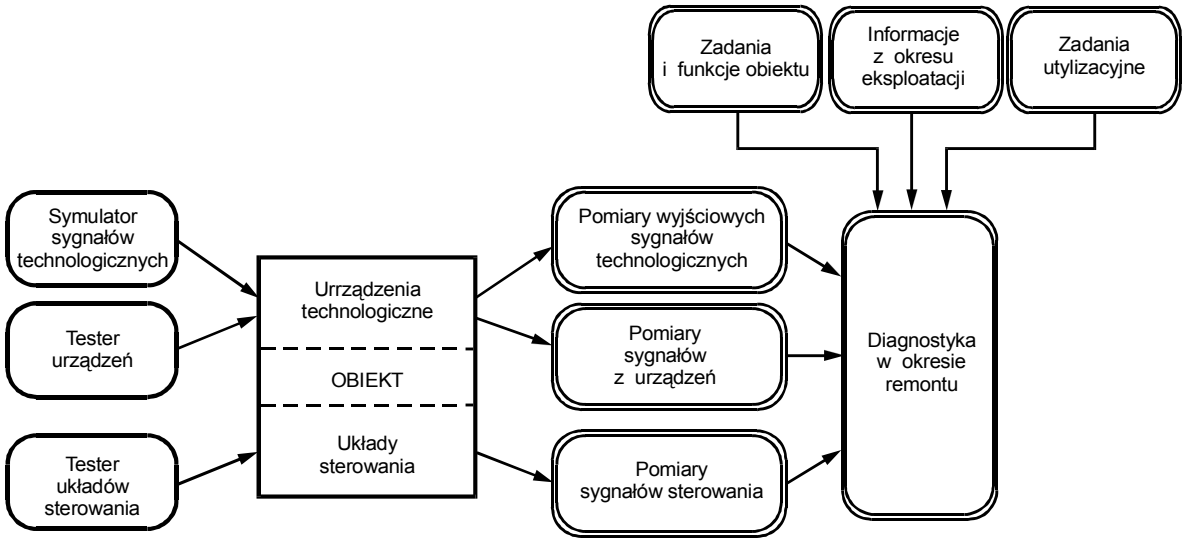
Rys. 5.6: Diagnostyka w okresie remontu [5.6]

5.6. Diagnostyka w okresie likwidacji

Dana instalacja krytyczna może być poddawana remontom do czasu, gdy dalsze remonty nie rokują otrzymania zadawalającej zdatności i gotowości do podjęcia zadań produkcyjnych (Rys.5.7). Renowacja uszkodzonych elementów może nie przynieść oczekiwanych rezultatów, co w rezultacie prowadzi do decyzji o wymianie określonych podzespołów lub dość znacznych jej części. Jeżeli kompleksowe badania całej instalacji krytycznej dadzą wynik negatywny, wówczas rozpoczyna się okres likwidacji maszyny krytycznej. Czynności likwidacyjne muszą obejmować działania mające na celu właściwe zagospodarowanie elementów nadal zdatnych do dalszego wykorzystania (na przykład jako części zapasowe) oraz likwidację z odpowiednią utylizacją elementów zużytych. Pomocne tu są informacje o wstępnych założeniach projektowych oraz wyniki badań diagnostycznych prowadzonych w poprzednich okresach życia maszyny likwidowanej.

5.7. Sformułowanie zadań diagnostyki weryfikacyjnej

Na maszyny i urządzenia procesowe działają różnorodne czynniki wewnętrzne i zewnętrzne Określenie ich stanu technicznego jest niezbędne do prawidłowej eksploatacji całego systemu realizującego daną technologię. Diagnostyka techniczna ma za zadanie przede wszystkim wykrywać uszkodzenia



Rys. 5.7: Diagnostyka w okresie likwidacji [5.6]

i zdarzenia powodujące poważne konsekwencje techniczne i ludzkie na podstawie bieżących badań, wykonywanych testów, oraz znajomości szczegółowych właściwości podzespołów i elementów. Obecnie diagnostyka rozszerza się również na dalsze zakresy, mianowicie na genezowanie i prognozowanie czyli na określanie stanów wcześniejszych i przyszłych danej maszyny [5.5].

Zadania i cele diagnostyki technicznej w tym również weryfikacyjnej określane są na bazie znajomości właściwości danej instalacji technicznej. W każdym procesie diagnostycznym występują czynności o charakterze pomiarowym, kontrolnym, oraz decyzyjnym. Wyniki pomiarów, są sprawdzane z wzorcowym lub zalecanym zakresem zmian danego parametru badanej maszyny i na bazie analizy danych ekspertowych wystawiana jest ocena oraz decyzja o dalszym sposobie wykorzystania badanego elementu lub całego podzespołu.

Do głównych zadań diagnostyki weryfikacyjnej w okresie produkcji, eksploatacji, remontu i likwidacji maszyn i urządzeń o charakterze krytycznym można zaliczyć:

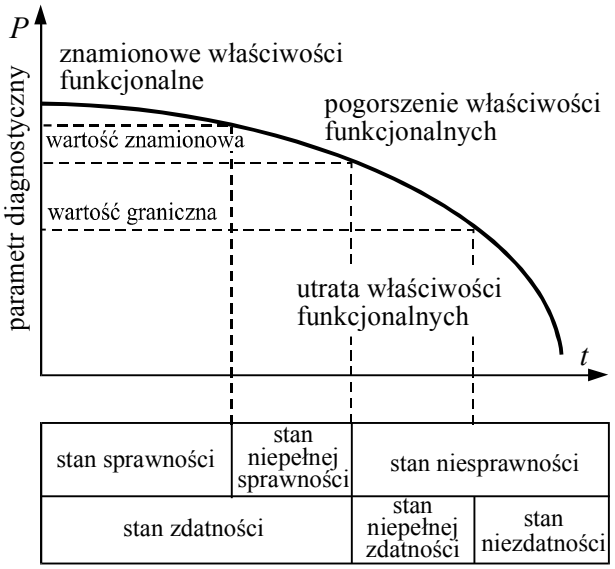
- sformułowanie modelu diagnostycznego uwzględniającego istotne właściwości obiektu,
- właściwe określenie parametrów diagnostycznych w modelu diagnostycznym,
- wykonywanie pomiarów wybranych parametrów diagnostycznych oraz porównywanie ich z przyjętymi wzorcami,
- określanie bieżącego stanu technicznego,
- określenie bieżącej zdatności podukładów diagnozowanych do wykonywania założonych zadań i funkcji,
- postawienie oceny diagnostycznej na postawie porównania z dopuszczalnymi przedziałami zmian badanych wielkości fizycznych,
- testowanie urządzeń i elementów wraz ze strojeniem parametrów technologicznych,
- testowanie podukładów celem wydania decyzji o dalszej ich eksploatacji,
- przewidywanie okresu sprawności diagnozowanych podukładów maszyn krytycznych z możliwością estymacji częstości ich uszkodzeń,
- określanie dryftów parametrów diagnostycznych i przewidywanie zmian stanu technicznego wybranych elementów,
- wizualizacja otrzymanych wyników w postaci wykresów lub odpowiednich diagramów z możliwością drukowania raportów diagnostycznych,

- wyznaczanie sposobów kontynuowania dalszej pracy po wystąpieniu drobnych awarii,
- wskazywanie procedur ruchowych zabezpieczających przed rozszerzeniem się obszaru zidentyfikowanej awarii,
- analizowanie przyczyn wystąpienia niesprawności w celu uzupełnienia bazy danych diagnostycznych,
- formułowanie sposobów zapobiegania przed uszkodzeniami,
- określanie wskazówek dotyczących projektowania maszyn i urządzeń o podobnej strukturze,
- rozszerzanie bazy danych diagnostycznych w celu uszczegółowienia systemów doradczych dla operatorów procesowych.

Okres projektowania maszyn, instalacji procesowych i innych obiektów technicznych jest również przedmiotem zainteresowania diagnostyki weryfikacyjne, przy czym nie może ona wówczas bazować na pomiarach rzeczywistych. Pozostają więc jedynie komputerowe badania symulacyjne, wnioski i zalecenia doradcze dla projektantów oraz formułowanie wymagań dla przyszłych systemów diagnostycznych dedykowanych dla obsługi serwisowej.

5.8. Wybrane metody diagnostyki weryfikacyjnej

Diagnostyka ma zastosowanie w wielu dziedzinach techniki, takich jak przemysł maszynowy, chemiczny, spożywczy, elektroniczny itp. Prowadzone są badania diagnostyczne dla różnych obiektów technicznych i procesów przez nich wykonywanych. W celu wykonania oceny diagnostycznej należy w pierwszym rzędzie zbudować model diagnostyczny zawierający parametry, które istotnie warunkują wynik końcowy i pozwalają na dokładne określenie, czy dany system jest zdatny do wykonywania swoich funkcji, czyli czy wartości wybranych istotnych parametrów zawierają się w granicach dopuszczalnych (Rys.5.8).

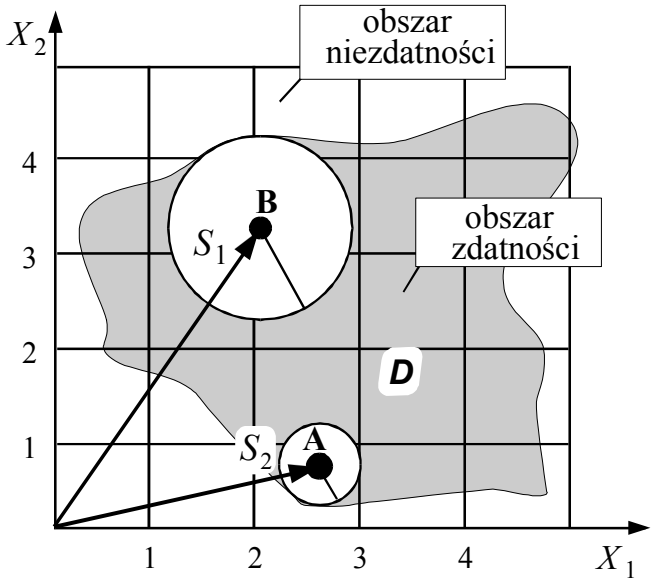


Rys. 5.8: Zmiana danego parametru diagnostycznego w funkcji czasu [5.7]

Wartość pojedynczego parametru diagnostycznego zmienia się w czasie i zwykle dąży do przekroczenia wartości granicznej, co nieuchronnie wiąże się z utratą właściwości funkcjonalnych danego urządzenia.

Model diagnostyczny zawiera zwykle kilka parametrów, które stanowią podstawę do uzyskania końcowej oceny diagnostycznej i do określenia stanu technicznego całego układu lub systemu oraz do predykcji ich funkcjonalności. Utworzone w ten sposób parametry diagnostyczne tworzą wektor w

wielowymiarowej przestrzeni R^n. W przypadku dwóch parametrów diagnostycznych można to zilustrować za pomocą obszarów na płaszczyźnie (Rys.5.9). Punkty A i B odzwierciedlają stan zdatności, lub gotowości układu badanego do wypełnienia swoich funkcji, a wartość promienia sąsiedztwa danego punktu całkowicie zawartego w obszarze *D* stanowi miarę tej zdatności. W konsekwencji można przewidywać jak długo dany system utrzyma swoją funkcjonalność i określić czas przejścia do stanu niezdatności.



Rys. 5.9: Interpretacja graficzna stanu technicznego urządzenia przy dwóch parametrach diagnostycznych X_1 i X_2; S_1, S_2 – wektory stanu technicznego

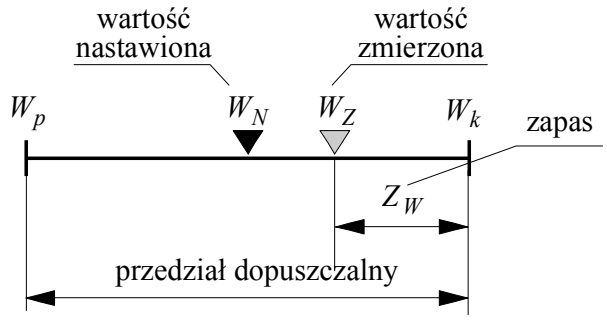
Model diagnostyczny danego podsystemu z odpowiednio dobranymi parametrami umożliwia oszacowanie czasu przejścia danego elementu do stanu niezdatności i tym samym pozwala na otrzymanie bieżącej częstości jego uszkodzeń. Istnieje też możliwość zmniejszenia tej częstości poprzez odpowiednio wcześniejszą renowację czy też wymianę elementu lub podzespołu, dla którego prowadzi się bieżącą kontrolę czasu jego normalnej eksploatacji. Odpowiednio prowadzona kontrola wybranych parametrów diagnostycznych pozwala na bieżące śledzenie stanu krytycznych elementów systemu lub przedziałów czasowych danego procesu.

5.9. Parametry diagnostyczne

Parametry diagnostyczne są kontrolowane pod względem ich zgodności z założonymi przedziałami dopuszczalnymi W_p, W_k. W celu podania dokładniejszej oceny parametru diagnostycznego stosuje się współczynnik zapasu parametru Z_W informujący o różnicy między wartościami danego parametru a jego wartościami dopuszczalnymi. W ten sposób powstała możliwość numerycznego śledzenia zmian badanego parametru nawet wówczas, gdy jego wartość zawiera się w zakresie dopuszczalnym (Rys.5.10).

Parametry diagnostyczne są kontrolowane pod względem ich zgodności z założonymi przedziałami dopuszczalnymi (W_p, W_k). Dla wartości W_Z pojedynczego parametru można podać ocenę w postaci funkcji dwuwartościowej $\{1, 0\}$ lub w postaci określenia lingwistycznego, tzn. „prawidłowo" lub „nieprawidłowo" zgodnie z poniższym wzorem.

$$W_Z \quad \textit{jest określona} \quad \begin{cases} \textit{prawidłowo} & dla \quad W_p \leqslant W_Z \leqslant W_k \\ \textit{nieprawidłowo} & dla \quad W_Z < W_p \quad \textit{lub} \quad W_Z > W_k \end{cases} \tag{5.1}$$



Rys. 5.10: Interpretacja graficzna zapasu parametru diagnostycznego [5.6]

W celu podania dokładniejszej oceny mierzonego parametru stosuje się współczynnik zapasu parametru Z_W określający różnicę między zmierzoną wartością parametru, a jego wartościami dopuszczalnymi [5.6].

Zapas parametru można wyrażać w procentach stosując zależność (3.29), otrzymując w ten sposób możliwość oszacowania czasu do prawdopodobnego przejścia danego podukładu w stan niesprawności i niegotowości do wykonywania postawionych zadań

$$Z_W = \begin{cases} \dfrac{\left|\dfrac{W_k - W_p}{2}\right| - |W_Z - W_N|}{\dfrac{|W_k - W_p|}{2}} 100\% & dla \quad W_p \leqslant W_Z \leqslant W_k \\ 0 & dla \quad W_Z < W_p \quad lub \quad W_Z > W_k \end{cases} \tag{5.2}$$

5.10. Pomiary parametrów diagnostycznych

Identyfikacja rzeczywistych przedziałów wartości wielkości fizycznych, w których występuje generacja sygnałów zewnętrznych, poprzez wykonanie odpowiednich pomiarów napotyka na trudności technologiczne. Zdawałoby się, że przy dzisiejszej zaawansowanej technice metrologicznej nie będzie tu żadnych problemów, a jednak wykonanie standardowego pomiaru prędkości obrotowej oraz wykonanie kontroli tej samej prędkości obrotowej ma zupełnie inny charakter. Sens tej różnicy polega na konieczności zastosowania przyrządów o zwiększonej dokładności oraz na innym interpretowaniu przeprowadzonego pomiaru, aby w sposób obiektywny wykonać rzeczywiste badanie. Tę różnicę najprościej przedstawić na przykładzie kontroli dopuszczalnego przedziału prędkości obrotowej ($n_s - \Delta N$, $n_s + \Delta N$), np. dla wału turbogeneratora, który powinien się obracać z prędkością synchroniczną [5.7].

Chcąc, dla celów kontroli, wykonać standardowy pomiar prędkości obrotowej, np. 3000 obr/min, stawia się pytanie: jaka jest wartość prędkości obrotowej? i otrzymuje się odpowiedź: prędkość obrotowa wynosi 3000 obr/min $\pm$5 obr/min, co w granicznych przypadkach może oznaczać, że prędkość obrotowa ma wartość 2995 obr/min albo 3005 obr/min. Natomiast wykonując kontrolę należy postawić pytanie: czy prędkości obrotowej wynosi 3000 obr/min $\pm$5 obr/min?

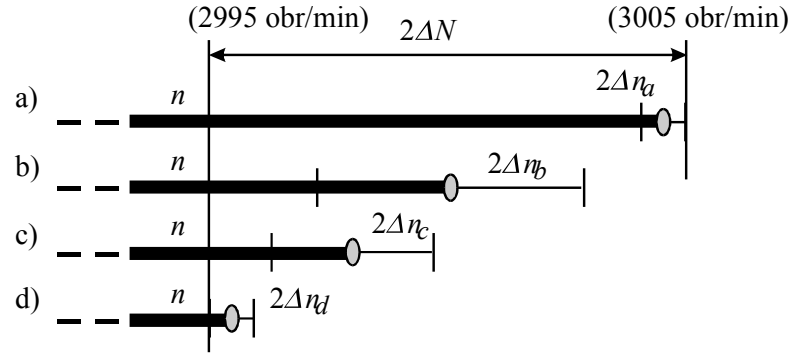
Odpowiedź na drugie pytanie jest trudniejszym zadaniem, gdyż przedział ($\pm$5 obr/min), który był mało istotny przy standardowym pomiarze, teraz stał się przedziałem $2\Delta N$ i jest przedmiotem głównych rozważań (Rys.5.10). Pojawiają się problemy z dokładnością przyrządów pomiarowych i sposobem wykonania samej czynności kontrolnej. Mimo, iż badana jest ta sama prędkość obrotowa i postawiono podobne pytanie, to odpowiedź na użytek kontroli będzie zupełnie inna, a mianowicie:

TAK – gdy jest spełniony zadany warunek,

NIE – gdy nie jest spełniony zadany warunek.

Dla przypadków b), c) (Rys.5.11) nie jest wymagana wysoka dokładność, ale jednak większa niż przy standardowym pomiarze, natomiast dla przypadków a) i d) dokładność musi być dużo większa.

W granicznym przypadku, gdy wartość prędkości obrotowej pokrywa się z dolną lub górną wartością dopuszczalnego przedziału, przyrząd do kontroli takiego przypadku musiałby mieć dokładność nieskończoną – co jest w praktyce nie do zrealizowania.



Rys. 5.11: Ilustracja kontroli prędkości obrotowej: $2\Delta N$ – przedział dopuszczalny wartości prędkości obrotowej, Δn_a, Δn_d – bezwzględne błędy pomiaru

Przy pomiarach kontrolnych w rzeczywistości mierzony jest przedział ΔN, mimo iż przyrząd pomiarowy wskazuje pełną wartość kontrolowanej wielkości fizycznej. W rezultacie dokładność, którą zapewnia przyrząd pomiarowy powinna być inna dla całej wartość n_s, a inna dla przedziału ΔN. Na przykład, przyjmując względny błąd pomiaru dla całkowitej wartości prędkości obrotowej $\delta n_s = (1/50) * 100\% = 2\%$, otrzymuje się względny błąd pomiaru dla badanego przedziału $\delta\Delta N = (1/1) * 100\% = 100\%$.
W celu zilustrowania wymaganych dokładności podczas kontroli, może być pomocny względny procentowy błąd kontroli prędkości obrotowej εf określony wzorem

$$\varepsilon f = \frac{\sigma}{\Delta N} \cdot 100\% \tag{5.3}$$

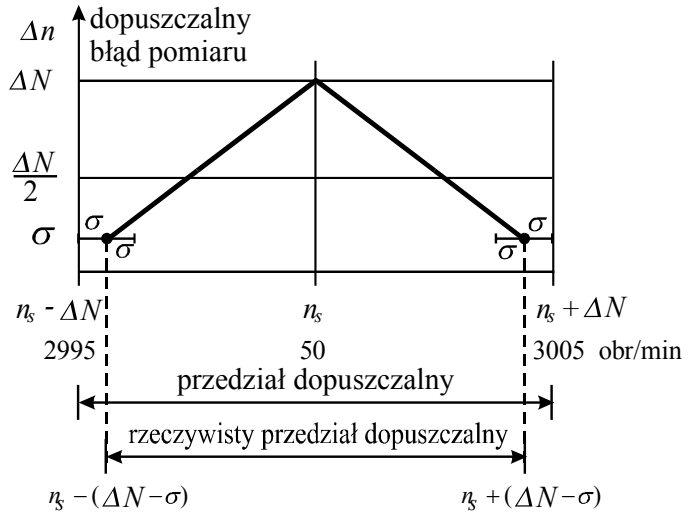
gdzie σ oznacza błąd bezwzględny pomiaru, a ΔN – dopuszczalną bezwzględna różnicę między nastawioną i rzeczywistą wartością wielkości kontrolowanej.

W praktyce wynik pomiaru kontrolnego musi zawierać się w przedziale dopuszczalnym pomniejszonym o wartość zależną od bezwzględnej wartości błędu pomiaru σ, którą oferuje zastosowany przyrząd, gdyż w przeciwnym przypadku nie można uznać badań kontrolnych za wiarygodne. W rezultacie rzeczywisty przedział dopuszczalny jest określony od wartości $n_s - (\Delta N - \sigma)$ do wartości $n_s + (\Delta N - \sigma)$ (Rys.5.12).

5.11. Określanie stanu technicznego urządzeń i instalacji krytycznych

Podstawowym zadaniem systemów diagnostycznych jest prawidłowe prowadzenie badań według wybranej metodyki z zachowaniem przyjętych reguł postępowania. Diagnostyka urządzeń krytycznych pracujących w sposób ciągły powinna zapewniać:

- wykonywanie ciągłej kontroli parametrów diagnostycznych uwzględniając przede wszystkim funkcje i zadania realizowane przez dane urządzenie; kontrolę tę prowadzi się w oparciu o układy pomiarowe, które przekazują niezbędne sygnały do centralnej bazy danych, w których następuje dalsze ich przetwarzanie i wypracowanie informacji dla personelu utrzymania ruchu;
- określanie chwilowych dryftów parametrów diagnostycznych oraz dalszą predykcję ich zmian w niezbędnym horyzoncie czasowym,
- identyfikacje i lokalizacje uszkodzeń elementów i podukładów urządzeń, które dopuszczają dalszą ich pracę w ograniczonym czasie i zakresie funkcjonalnym, umożliwiając obsłudze własne



Rys. 5.12: Ilustracja rzeczywistej wymaganej dokładności przy kontrolnym pomiarze prędkości obrotowej

podjęcie decyzji o ich naprawie lub wymianie w sposób niekolidujący z procesem technicznym całego system,

- określanie przyczyn zlokalizowanych uszkodzeń i formułowanie sposobów ich zapobiegania, szczególnie w punktach, które są odpowiedzialne za powstanie poważniejszych awarii,
- wizualizacje otrzymanych wyników pomiarów istotnych wielkości fizycznych, sygnałów będących symptomami ewentualnych uszkodzeń oraz generowanie zbiorczych wykresów w oparciu o bazę danych w sposób niezbędny do podejmowania przez operatora prawidłowych decyzji,
- rejestracje i archiwizację danych pomiarowych oraz wykonywanie raportów okresowych, które są niezbędne do oceny stanu technicznego diagnozowanego procesu technicznego.

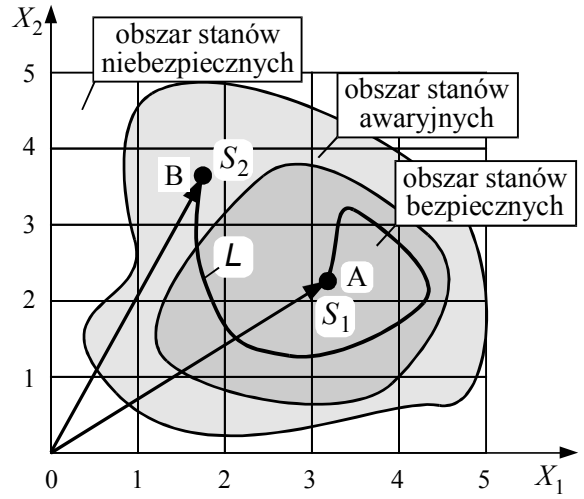
Na szczególną uwagę zasługuje metoda diagnostyki weryfikacyjnej urządzeń w systemie dynamicznym. Umożliwia ona oszacowanie zmiany parametru niezawodnościowego urządzenia danej kategorii. Przy wypracowaniu strategii testów diagnostycznych elementów/podsystemów systemu automatyki zabezpieczeniowej uwzględnia się:

- poziom nienaruszalności bezpieczeństwa danego systemu zabezpieczeniowego wyznaczony na podstawie oceny ryzyka;
- ocenę pokrycia diagnostycznego podsystemów;
- architekturę systemu zabezpieczeń.

W podsystemach systemu zabezpieczeń należy dążyć do rozwiązań z małym udziałem uszkodzeń niebezpiecznych, czyli z wysokim poziomem pokrycia diagnostycznego. Osiąga się to przez specjalne rozwiązania np. „inteligentnych" czujników i elementów wykonawczych z funkcjami diagnostycznymi. Należy też ograniczać stosowanie rozwiązań technicznych i strukturalnych systemów automatyki zabezpieczeniowej z dużym udziałem uszkodzeń bezpiecznych, gdyż prowadzą one do niepotrzebnych wyłączeń obiektu krytycznego, co powoduje nie tylko straty produkcyjne, ale może również zainicjować sytuacje niebezpieczne. Zagadnienia ta uwzględniają w różnym zakresie normy bezpieczeństwa funkcjonalnego [5.3], [5.2], [5.4].

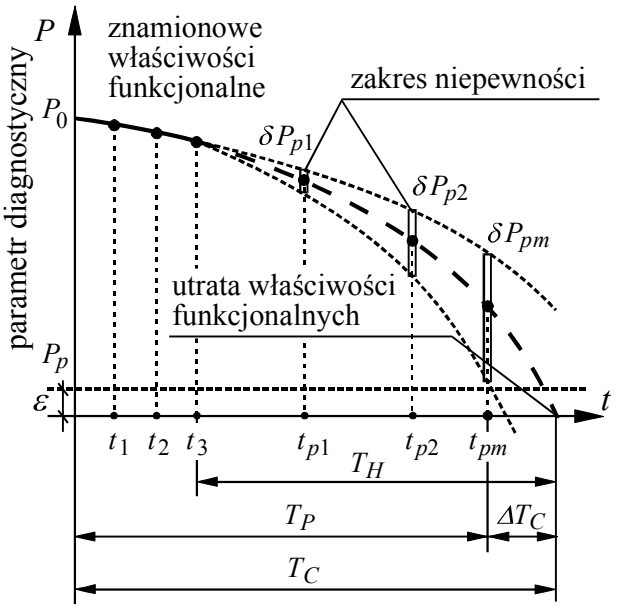
Bezpieczeństwo układów, urządzeń lub systemów łączy się z aktualnym ich stanem technicznym, który zmienia się w kolejnych chwilach czasu pod wpływem czynników technologicznych, sterowniczych i zakłóceń zewnętrznych. Wśród tych stanów można wyróżnić stany bezpieczne, awaryjne oraz stany niebezpieczne. Określenie stanu diagnozowanej maszyny następuje na podstawie danych odnośnie jej właściwości statycznych i dynamicznych oraz danych związanych z przyjętymi zadaniami.

Gdy trajektoria stanu przebiega w przestrzeni stanów bezpiecznych można wówczas powiedzieć, że dane urządzenia nie stwarza zagrożenia dla osób i swojego środowiska. W przeciwnym przypadku obiekt przejdzie w stan awarii, który może doprowadzić do powstania szkód z groźną katastrofą włącznie (Rys.5.13).



Rys. 5.13: Interpretacja graficzna stanu technicznego urządzenia w kontekście analizy bezpieczeństwa [5.8]

Na podstawie pomiarów danego zbioru parametrów diagnostycznych oraz predykcji ich parametrów w określonym horyzoncie czasowym można przewidzieć (oszacować) czas do chwili utraty (zdolności funkcjonalnej) zdatności badanego obiektu do wykonywania swych funkcji. Ilustrację przykładowego przebiegu zmian pojedynczego parametru diagnostycznego przedstawia Rys.5.14.



Rys. 5.14: Ilustracja określania okresu gotowości danego układu na podstawie monitoringu jego krytycznej właściwości [5.8]

W miarę wzrostu horyzontu predykcji, wzrasta również błąd szacowania okresu czasu pracy bezawaryjnej. Mając określony czas T_C do chwili utraty właściwości eksploatacyjnych pomniejszony o szacowaną niepewność predykcji ΔT_C otrzymujemy możliwy do przyjęcia czas T_P, który może sta-

nowić podstawę do dynamicznej estymacji intensywności uszkodzeń badanego elementu systemu.

Wymiana krytycznego podzespołu przed upływem czasu T_P może pomniejszyć o krotność wykonanych wymian i pozwoli na istotne zmniejszenie prawdopodobieństwa PFD_{avg}.

Efekty zmniejszenia PFD jest tylko wówczas znaczący, gdy pokrycie diagnostyczne DC jest stosunkowo duże i dotyczy elementów, które mogą spowodować znaczne straty osobowe w mieniu i środowisku zewnętrznym.

Bibliografia

[5.1] Brandowski A. Bezpieczeństwo funkcjonalne aplikacją nauki o bezpieczeństwie. *Zarządzanie bezpieczeństwem funkcjonalnym*, Gdańsk / Jurata, 16–18.09.2004.

[5.2] International Electrotechnical Commission. *IEC 61511:2000: Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1–3*.

[5.3] International Electrotechnical Commission (IEC). *IEC 61508:1998. Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems. Parts 1–7*.

[5.4] International Electrotechnical Commission (IEC). *IEC/CEI 62061:2005 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*, 2005.

[5.5] Korbicz J., Kościelny J.M., Kowalczuk Z., Cholewa W. *Diagnostyka procesów. Modele sztucznej inteligencji. Zastosowania*. WNT, Warszawa, 2002.

[5.6] Zawalich J. *Diagnostyka układów automatycznej synchronizacji prądnic*. Praca doktorska, Politechnika Gdańska, Wydział Elektrotechniki i Automatyki, Gdańsk, 2001.

[5.7] Zawalich J. Wybrane zagadnienia automatycznych synchronizatorów prądnic. *PAK*, 12:39–41, 2003.

[5.8] Zawalich J. A method of verification diagnostics for functional safety analysis. *Proceedings of IEEE International Conference on Technologies for Homeland Security and Safety*, TEHOSS, Gdańsk, Poland, September 28–30 2005.

Rozdział 6

Modelowanie bezpieczeństwa maszyn i instalacji krytycznych

Kazimierz T. KOSMOWSKI, Jacek ZAWALICH

6.1. Bezpieczeństwo maszyn i kategorie systemów sterowania

Podsystemy systemu sterowania maszyny służą nie tylko do realizacji funkcji (algorytmów) sterowania, ale również funkcji bezpieczeństwa. Nazywane są one wówczas podsystemami (lub elementami) systemów sterowania związanymi z bezpieczeństwem [6.17]. Elementy te mogą składać się ze sprzętu i oprogramowania. Mogą być one wydzielonymi lub integralnymi częściami systemu sterowania. W elementach takich mogą wystąpić defekty lub uszkodzenia. Zachowanie się elementów systemów sterowania związanych z bezpieczeństwem w przypadku występowania defektów, podzielono w normie PN-EN 954 na pięć kategorii: B, 1, 2, 3, 4.

W doborze kategorii i projektowaniu elementów systemu sterowania związanego z bezpieczeństwem projektant powinien podać co najmniej następujące informacje o każdym z tych elementów (podsystemów):

- właściwości funkcjonalne i dobrana kategoria;
- rola jaką spełnia jako środek zabezpieczeniowy (ochronny) w maszynie i jej granice;
- przewidywane i uwzględnione defekty wpływające na bezpieczeństwo;
- potencjalne inne defekty wpływające na bezpieczeństwo, które nie zostały uwzględnione (racjonalny – subiektywnie przyjęty zakres analizy), jednak z ogólną oceną zastosowanych środków, które umożliwiają wykluczenie niekorzystnych skutków tych defektów;
- czynniki wpływające na niezawodność, takie jak warunki środowiskowe;
- zastosowana technika.

Zamierzeniem jest stworzenie podstaw do oceny projektu konstrukcji i funkcjonalności w danym zastosowaniu systemu sterowania związanego z bezpieczeństwem i samej maszyny, na przykład przez stronę trzecią, bądź własne lub niezależne ośrodki badawcze.

Wymaga się, aby elementy systemu sterowania, które realizują funkcje bezpieczeństwa, były tak zaprojektowane i zbudowane, aby były uwzględnione w pełnym zakresie zasady zawartej w normie EN 1050 [6.14]:

- podczas zgodnego z przeznaczeniem oraz dającego się przewidzieć niewłaściwego użytkowania;
- podczas występowania defektów;
- w przypadku wystąpienia dających się przewidzieć błędów ludzkich podczas zgodnego z przeznaczeniem użytkowania maszyny jako całości.

Ogólna strategia projektowania polega na uwzględnieniu wyników analizy i oceny ryzyka. Na podstawie oceny ryzyka (zaleca się stosowanie EN 1050) związanego z eksploatacja maszyny, projektant powinien zadecydować o udziale każdego elementu systemu sterowania związanego z bezpieczeństwem w zmniejszaniu ryzyka.

Głównym celem projektowania jest zapewnienie, że elementy systemów sterowania związane z bezpieczeństwem wytworzą sygnały wyjściowe, które poprzez elementy wykonawcze umożliwią osiągnięcie celów zmniejszenia ryzyka zgodnie z EN 1050. Nie zawsze jest to możliwe i w takich przypadkach projektant powinien uwzględnić zastosowanie innych środków bezpieczeństwa [6.6].

Im bardziej zmniejszenie ryzyka jest zależne od elementów systemu sterowania związanego z bezpieczeństwem, tym wymagana jest większa odporność tych elementów na defekty. Odporność ta, zakładając, że wymagania realizacji danej funkcji są spełnione, powinna być wyrażona ilościowo wskaźnikami niezawodności z zastosowaniem struktury odpornej na defekty. Określoną odporność elementów związanych z bezpieczeństwem na defekty można osiągnąć określając poziomy niezawodności części składowych i/lub poprawiając strukturę elementów związanych z bezpieczeństwem. Możliwa jest zbliżona lub większa odporność na defekty jednokanałowych elementów związanych z bezpieczeństwem, o wysokiej niezawodności (wykonanych w pewnej technice), w porównaniu z rozwiązaniem w postaci struktury z tolerancją defektu o mniejszej niezawodności, wykonanej w innej technice. Jest to podstawowy problem projektowania strukturalnego systemu z uwzględnieniem wymagań niezawodności.

Zachowanie się elementów systemu sterowania związanych z bezpieczeństwem z punktu widzenia odporności na defekty zależy od różnych czynników:

- niezawodności realizacji funkcji bezpieczeństwa;
- struktury (lub architektury) systemu sterowania;
- jakości dokumentacji związanej z bezpieczeństwem (specyfikacji technicznej);
- kompletności wymagań i zakresu ich uwzględnienia;
- projektowania, wytwarzania i utrzymania (konserwacji);
- jakości i adekwatności oprogramowania;
- zakresu przeprowadzonych badań funkcjonalnych (weryfikacja i walidacja);
- właściwości eksploatacyjnych sterowanej maszyny lub jej części.

Czynniki te można ująć w trzech grupach według [6.17]:

- niezawodności sprzętu - poziom niezawodności elementów składowych umożliwiający unikanie defektów;
- struktury systemu - układ elementów systemu sterowania związanego z bezpieczeństwem umożliwiający unikanie, tolerowanie i wykrywanie defektów;
- ,jakościowych aspektów wpływających na potencjalne zachowanie się elementów systemu sterowania związanego z bezpieczeństwem, nie dających się określić ilościowo.

Proces doboru i projektowania środków bezpieczeństwa jest zwykle iteracyjny. Jest przy tym istotne ustalenie powiązań i oddziaływań pomiędzy elementami systemu sterowania związanymi z bezpieczeństwem, a elementami systemu sterowania niezwiązanymi z bezpieczeństwem i wszystkimi innymi częściami maszyny. Następnie powinien być określony udział elementów związanych z bezpieczeństwem w zmniejszeniu ryzyka stwarzanego przez maszynę, zgodnie z jego oceną według EN 1050. Istnieją różne sposoby zmniejszania ryzyka stwarzanego przez maszyny, co wpływa potencjalnie na alternatywność rozwiązań w projektowaniu elementów systemu sterowania związanych z bezpieczeństwem.

Decyzje i/lub założenia podejmowane w kolejnym kroku procedury analizy, mogą wpływać na decyzje i założenia podejmowane we wcześniejszych krokach. Wyróżnia się 5 podstawowych kroków tej analizy [6.17]:

Krok 1: Analiza zagrożeń i ocena ryzyka

- Identyfikacja zagrożeń stwarzanych przez maszynę w przypadku wszystkich rodzajów pracy i w każdej fazie jej życia według zaleceń zawartych w EN 292-1 i EN 1050.
- Ocena ryzyka związanego z zagrożeniami i podjęcie decyzji o zmniejszeniu ryzyka, właściwie dla danego zastosowania, zgodnie z tymi normami.

Krok 2: Zadecydowanie o sposobach zmniejszenia ryzyka środkami sterowania

- Zadecydowanie o rozwiązaniach konstrukcyjnych maszyny i zastosowaniu odpowiednich urządzeń zabezpieczeniowych w celu zmniejszenia ryzyka. Elementy systemu sterowania, które są integralną częścią tych rozwiązań konstrukcyjnych i sterowania urządzeniami zabezpieczeniowymi, powinny być rozpatrywane jako elementy związane z bezpieczeństwem.

Krok 3: Określenie wymagań dotyczących bezpieczeństwa, odnoszących się do elementów systemu sterowania związanych z bezpieczeństwem

- Określenie funkcji bezpieczeństwa, realizowanych poprzez system sterowania oraz sporządzenie ich wykazu i wymagań według kategorii. W EN 954 podano źródła informacji o typowych funkcjach bezpieczeństwa i ich właściwościach, które powinny być uwzględnione, jeśli wybrano określoną funkcję bezpieczeństwa.
- Określić, jak będą osiągane funkcje bezpieczeństwa oraz dobrać kategorię dla każdego elementu i kombinacji elementów systemu sterowania związanych z bezpieczeństwem.

Krok 4: Projektowanie

- Zaprojektowanie elementów systemu sterowania związanego z bezpieczeństwem zgodnie z wymaganiami określonymi w kroku 3 i ogólną strategią projektowania. Sporządzenie wykazu cech, stanowiących racjonalne uzasadnienie w odniesieniu do osiągniętej kategorii systemu.
- W każdej fazie weryfikowanie projektu, w celu upewnienia się, czy elementy związane z bezpieczeństwem spełniają wymagania określone w poprzedniej fazie i związane z ustalonymi funkcjami i kategoriami bezpieczeństwa.

Krok 5: Walidacja

- Przeprowadzenie walidacji założonych funkcji i kategorii bezpieczeństwa w celu sprawdzenia zgodności z wymaganiami określonymi w kroku 3. Powtórzenie projektowania, jeśli jest to zasadne.
- Jeśli w konstrukcji elementów systemów sterowania związanych z bezpieczeństwem, zastosowano programowalne systemy elektroniczne, to wymagane są dodatkowe, bardziej szczegółowe procedury postępowania (na przykład zawarte w normach bezpieczeństwa funkcjonalnego [6.6], [6.7]).

Zwykle nie można stwierdzić, że ma się pełne zaufanie do prawidłowego działania pojedynczego kanału programowalnego wyposażenia elektronicznego, szczególnie w sytuacjach, w których zagrożenie może powstać na skutek niewłaściwego działania systemu sterowania. Dlatego nie jest wskazane, aby polegać jedynie na poprawnym działaniu takiego jednokanałowego układu. Ponadto należy stwierdzić, że konieczna jest walidacja elementów systemu sterowania związanych z bezpieczeństwem w połączeniu z całym systemem sterowania, traktowanych jako części danej maszyny [6.17]. Projektant zestawia niezbędne funkcje bezpieczeństwa i zapewnienia środki umożliwiające spełnienie wymagań dotyczących bezpieczeństwa w odniesieniu do systemu sterowania w konkretnym zastosowaniu. W Tablicy 6.1 zestawiono wymagania dotyczące kategorii systemów sterowania.

Dobór i kombinacja elementów systemu sterowania związanego z bezpieczeństwem zależy od kategorii systemu. Kategorie zaleca się dobierać w odniesieniu do wszystkich elementów systemu sterowania związanych z bezpieczeństwem. Pojedynczą funkcję bezpieczeństwa może realizować jeden lub więcej elementów. Również kilka funkcji bezpieczeństwa może być realizowanych przez jeden element (lub więcej). W praktyce, w celu zapewnienia obniżenia ryzyka może być konieczne zastosowanie więcej niż jedna funkcji bezpieczeństwa.

Jeśli funkcja bezpieczeństwa jest realizowana za pomocą kilku elementów związanych z bezpieczeństwem, np. czujników, jednostek nadzorujących, elementów sterujących w obwodach mocy, elementy te mogą być jednej kategorii lub kombinacją innych kategorii. Jeśli do realizacji funkcji bezpieczeństwa stosowane są elementy związane z bezpieczeństwem tej samej lub różnych kategorii w kombinacji to w procesie pełnej walidacji (krok 5) powinna być przeprowadzona analiza takiej kombinacji.

Dobór kategorii w odniesieniu do określonego elementu systemu sterowania związanego z bezpieczeństwem zależy głównie od [6.17]:

- zmniejszenia ryzyka osiąganego w wyniku stosowania funkcji bezpieczeństwa, na którą wpływa element;
- prawdopodobieństwa wystąpienia defektu (lub defektów) w tym elemencie;
- ryzyka związanego z wystąpieniem defektu (lub defektów) w danym elemencie;
- możliwości uniknięcia defektu (lub defektów) w tym elemencie;
- zastosowanej techniki.

Norma PN-EN 954 proponuje stosowanie, do zgrubnego wyznaczania kategorii systemu sterowania, grafu koncepcyjnie zbliżonego do grafu ryzyka przedstawionego na Rys.3.7. W grafie do doboru kategorii systemu sterowania maszyn występują następujące parametry: *S - ciężkość urazów* (*S1*- lekkie, zwykle odwracalne urazy i *S2* – ciężkie, zwykle nieodwracalne urazy i urazy śmiertelne), *F - częstość narażenia i/lub czas jego trwania* (*F1*- rzadkie do dość częstych i/lub krótki czas narażenia i F2 - częste do ciągłych i/lub długi czas narażenia), *P - możliwość przeciwdziałania zagrożeniu* (P1 - możliwe w określonych warunkach, P2 - możliwe, ale utrudnione). Wskazanie tych parametrów może być w niektórych przypadkach analizy maszyny niejednoznaczne i dlatego należy przyjmować wówczas wyższą kategorię systemu sterowania maszyny.

6.2. Redukowanie ryzyka eksploatacji maszyn zorientowane na system sterowania

W wydanej ostatnio normie IEC 62061:2005 [6.7] podkreśla się znaczenie systemów sterowania pełniących funkcje związane z bezpieczeństwem maszyn, projektowanych z wykorzystaniem zaawansowanej technologii elektronicznej. Norma ta dotyczy głównie systemów sterowania SRECS (*Safety-Related Electrical Control Systems*), których zadaniem jest m.in. zmniejszenie ryzyka związanego z eksploatacją maszyn. Zawiera ona metodykę i wymagania związane z projektowaniem SRECS, w tym:

- umożliwia przypisanie poziomu nienaruszalności bezpieczeństwa SIL dla każdej funkcji zaimplementowanej w SRECS,
- określa zasady i kryteria projektowania SRECS zgodnie z zdefiniowanymi funkcjami sterowania związanymi z bezpieczeństwem,
- proponuje zasady integrowania podsystemów związanych z bezpieczeństwem zgodnie z ISO 13849 [6.2];
- zawiera procedurę walidacji SRECS.

Dokument ten nawiązuje w licznych miejscach do normy bezpieczeństwa funkcjonalnego IEC 61508 [6.6] co jest szczególnie uzasadnione w projektowaniu złożonych SRECS. Proces projektowania SRECS obejmuje również projektowanie funkcji diagnostycznych.

W IEC 62061 nie rozróżnia się podsystemów typu A i B i przyjmuje się tylko trzy poziomy nienaruszalności bezpieczeństwa SIL: od 1 do 3. Tablica 6.2 zawiera strukturalne ograniczenia dotyczące podsystemów - najwyższe poziomy SIL jakie można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy.

Tab. 6.1: Zestawienie wymagań dotyczących kategorii systemów sterowania [6.17]

Kategoria[1)]	Podsumowanie wymagań	Zachowanie się systemu[2)]	Zasady zachowania bezpieczeństwa
B	Elementy systemu sterowania związane z bezpieczeństwem i urządzenia ochronne oraz ich elementy składowe, powinny być zaprojektowane, zbudowane i zmontowane zgodnie z odpowiednimi normami, aby mogły wytrzymać przewidywane narażenia.	Wystąpienie defektu może spowodować utratę funkcji bezpieczeństwa.	Głównie poprzez dobór elementów składowych
1	Powinny być spełnione wymagania dotyczące kategorii B oraz stosowane wypróbowane elementy składowe i sprawdzone zasady bezpieczeństwa	Wystąpienie defektu może spowodować utratę funkcji, ale prawdopodobieństwo wystąpienia defektu jest mniejsze niż w przypadku kategorii B.	
2	Powinny być spełnione wymagania dotyczące kategorii B i zastosowane sprawdzone zasady bezpieczeństwa. Funkcja bezpieczeństwa powinna być sprawdzana we właściwych odstępach czasu przez system sterowania maszyny.	- Wystąpienie defektu może spowodować utratę funkcji bezpieczeństwa pomiędzy sprawdzeniami. - Utrata funkcji bezpieczeństwa jest wykrywana podczas sprawdzania.	Głównie przez dobór struktury
3	Powinny być spełnione wymagania dotyczące kategorii B i zastosowane sprawdzone zasady bezpieczeństwa. Elementy związane z bezpieczeństwem powinny być tak zaprojektowane, aby: - pojedynczy defekt w dowolnym elemencie nie powodował utraty funkcji bezpieczeństwa, oraz - jeśli jest to praktycznie uzasadnione, pojedynczy defekt powinien być wykryty.	- Po wystąpieniu pojedynczego defektu funkcja bezpieczeństwa jest dostępna. - Nie wszystkie defekty są wykrywane. - Nagromadzenie niewykrytych defektów może powodować utratę funkcji bezpieczeństwa.	Głównie przez dobór struktury
4	Powinny być spełnione wymagania dotyczące kategorii B i zastosowane sprawdzone zasady bezpieczeństwa. Elementy związane z bezpieczeństwem powinny być tak zaprojektowane, aby: - pojedynczy defekt w dowolnym elemencie nie powodował utraty funkcji bezpieczeństwa, - pojedynczy defekt był wykrywany natychmiast lub przed następnym przywołaniem funkcji bezpieczeństwa. Jeśli nie jest to możliwe, to nagromadzenie defektów nie powinno spowodować utraty funkcji bezpieczeństwa.	- Po wystąpieniu pojedynczego defektu funkcja bezpieczeństwa jest zawsze spełniona. - Wykryte w odpowiednim czasie defekty zapobiegają utracie funkcji bezpieczeństwa.	Głównie przez dobór struktury

[1)] Kategorie nie są przeznaczone do stosowania w jakimś określonym porządku lub hierarchii ze względu na wymagania dotyczące bezpieczeństwa.

[2)] Na podstawie wyników oceny ryzyka wnioskuje się, czy jest do zaakceptowania całkowita lub częściowa utrata funkcji bezpieczeństwa spowodowana wystąpieniem defektów.

Tab. 6.2: Ograniczenia architektoniczne na podsystemy - najwyższy poziom SIL jaki można przypisać funkcji bezpieczeństwa według reguł IEC 62061

Udział uszkodzeń bezpiecznych S_{ff}	Tolerowane uszkodzenia sprzętu N		
	0	1	2
$<$ 60 %	Nie dozwolone	SIL1	SIL2
60 % - $<$ 90 %	SIL1	SIL2	SIL3
90 % - $<$ 99 %	SIL2	SIL3	SIL3
$\geqslant$ 99 %	SIL3	SIL3	SIL3
Tolerowane uszkodzenia sprzętu N oznacza, że N+1 uszkodzeń spowoduje utratę funkcji sterowania związanej z bezpieczeństwem. Nie uwzględnia się w tej normie rozwiązań dla SIL4 według IEC 61508-1.			

Schemat przypisania SIL dla funkcji sterowania związanej z bezpieczeństwem (SRCF – *Safety Related Control Function*) według IEC 62061 przedstawiono na Rys.6.1.

Poziom nienaruszalności bezpieczeństwa SIL przypisuje się metodą jakościową na podstawie zdefiniowanej macierzy, w której wyróżniono cztery klasy krytyczności Se (*severity*) i pięć klas Cl prawdopodobieństw szkody, jakie mogą być spowodowane przez analizowaną maszynę. Cl wyznacza się na podstawie trzech parametrów: częstości lub czasu narażenia (ekspozycji) Fr, prawdopodobieństwa zdarzenia Pr i prawdopodobieństwa uniknięcia lub ograniczenia szkody Av. Podejście to jest zgrubne i wymaga dalszych badań z uwzględnieniem kategorii maszyn użytkowanych w różnych sektorach gospodarki. Bardziej ogólne podejście do wyznaczania SIL zawiera norma IEC 61508 [6.6], która może być stosowana do wszystkich obiektów technicznych podwyższonego ryzyka.

Istotne znaczenie w systemach sterowania mają uszkodzenia niebezpieczne, które mogą doprowadzić do niebezpiecznych stanów maszyny zagrażających obsłudze i otoczeniu. Wyznaczanie odpowiednich miar ryzyka związanego z takimi uszkodzeniami jest zwykle wyzwaniem z powodu braku danych niezawodnościowych i parametrów pokrycia diagnostycznego DC podsystemów. W tej sytuacji można posłużyć się odpowiednią metodą modelowania probabilistycznego, na przykład analizy rodzajów uszkodzeń, skutków i krytyczności FMECA [6.16] lub drzewa uszkodzeń i błędów FTA [6.14], korzystając z ogólnych baz danych niezawodnościowych takich jak standard amerykański [6.21] i poradnik [6.19].

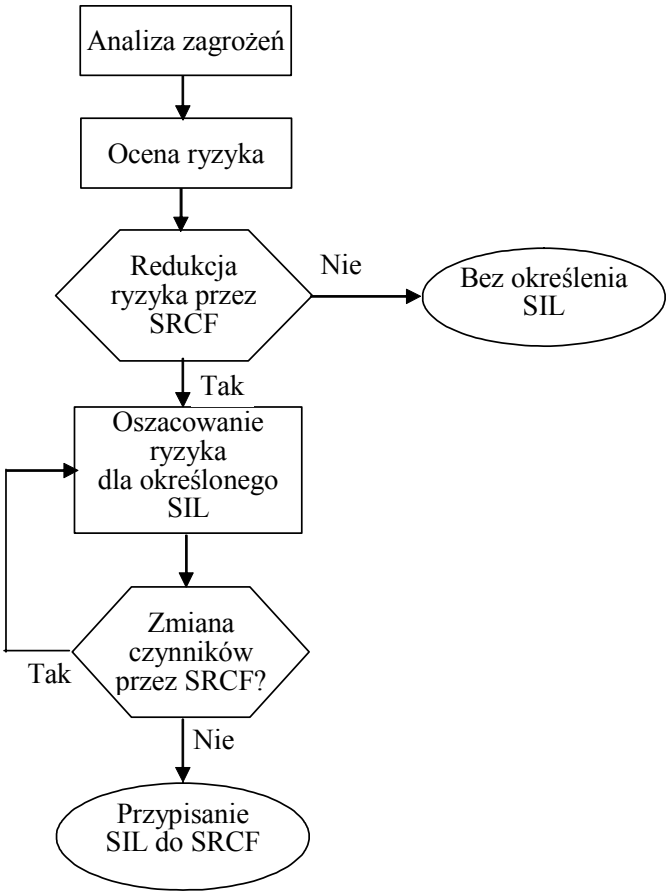
Można rozważać się różne architektury systemu sterowania maszyny zawierające podsystemy, w tym architekturę tolerującą pojedyncze uszkodzenie z funkcją diagnostyczną przedstawioną na Rys.6.2. Niebezpieczne uszkodzenie pojedynczego elementu nie spowoduje dla takiej architektury niebezpiecznego uszkodzenia systemu. Może jednak wystąpić uszkodzenie o wspólnej przyczynie, które spowoduje niebezpieczne uszkodzenie systemu.

Sumaryczną intensywność uszkodzeń elementów (podsystemów) szacuje się uwzględniając (3.15) na podstawie znajomości średniego czasu do uszkodzenia MTTF (*Mean Time To Failure*), przy założeniu rozkładu wykładniczego, ze wzoru

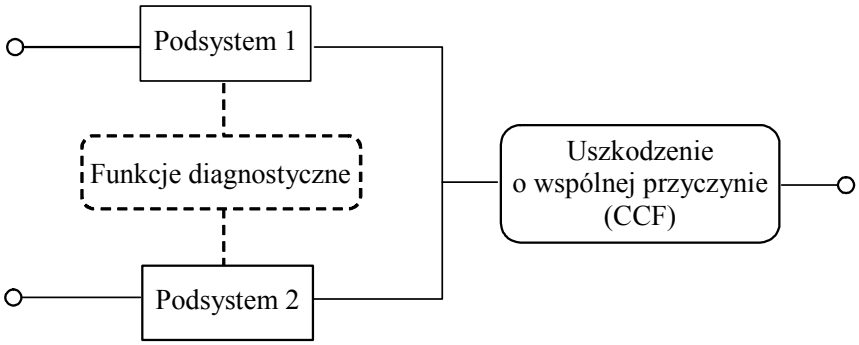
$$\lambda = \lambda_S + \lambda_D = MTTF_S^{-1} + MTTF_D^{-1} \tag{6.1}$$

gdzie: $MTTF_S$ jest średnim czasem do bezpiecznego uszkodzenia elementu, natomiast $MTTF_D$ jest średnim czasem do niebezpiecznego uszkodzenia elementu.

Prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego w systemie technicznym na jednostkę czasu można wyznaczyć na podstawie częstości $W_j(t)$ (oczekiwana liczba j-tej kombinacji uszkodzenia niebezpiecznego) kolejnych cięć minimalnych K_j



Rys. 6.1: Schemat przypisania SIL dla funkcji sterowania związanej z bezpieczeństwem SRCF na podstawie IEC 62061



Rys. 6.2: Przykładowa architektura tolerująca pojedyncze uszkodzenie z funkcją diagnostyczną

$$W_j(t) = \sum_{i \in K_j} w_i(t) \prod_{\substack{l \in K_j \\ l \neq i}} q_l(t) = \sum_{i \in K_j} w_i(t) \frac{Q_j(t)}{q_i(t)} \tag{6.2}$$

przy czym: $Q_j(t)$ jest prawdopodobieństwem wystąpienia j-tego cięcia minimalnego

$$Q_j(t) = \prod_{i \in K_j}^{n} q_i(t) \tag{6.3}$$

gdzie: $q_i(t)$ jest niegotowością *i*-tego elementu.

Częstość wystąpienia niezdatności *i*-tego elementu $w_i(t)$ o intensywności uszkodzeń λ_i określa wzór

$$w_i(t) = \lambda_i \cdot [1 - q_i(t)] \tag{6.4}$$

Z wzoru (6.4) wynika, że $w_i(t) \leqslant \lambda_i$, a dla elementów o małej zawodności ($q_i(t) \leqslant 0.01$), częstość jest w przybliżeniu równa $w_i(t) \approx \lambda_i$. Wzór wyprowadzono zakładając, że aby doszło do wystąpienia danego *j*-tego cięcia minimalnego w wyniku uszkodzenia *i*-tego elementu, jego wszystkie elementy, oprócz *i*-tego, muszą być już niesprawne w chwili *t*.

Częstość W_0 wystąpienia zdarzenia szczytowego drzewa niezdatności (spodziewana liczba wystąpienia zdarzenia na jednostkę czasu) będzie w przypadku *k* cięć minimalnych

$$W_0(t) = \sum_{j=1}^{k} W_j(t) \prod_{\substack{l=1 \\ l \neq j}}^{k} [1 - Q_l(t)] \cong \sum_{j=1}^{k} W_j(t)[1 - \sum_{\substack{l=1 \\ l \neq j}}^{k} Q_l(t)] \tag{6.5}$$

Wzór (6.5) wyprowadzono przy założeniu, że aby doszło do wystąpienia zdarzenia szczytowego drzewa niezdatności z powodu j-tego cięcia minimalnego, wszystkie pozostałe cięcia, oprócz j-tego, nie mogą wystąpić do danej chwili t, co reprezentują wyrażenia w nawiasach kwadratowych w tym wzorze.

Dla systemu o małej niegotowości (rząd cięć minimalnych od 2 i sporadyczna powtarzalność elementów w cięciach minimalnych) można przyjąć wzór uproszczony [6.8]

$$W_0(t) \approx \sum_{j=1}^{k} W_j(t) \tag{6.6}$$

Wzory (6.2)÷(6.6) mogą posłużyć do wyprowadzenia zależności na częstość zdarzeń niebezpiecznych PFH (zob. kryteria w Tablicy 3.2) dla ciągłego rodzaju pracy systemu E/E/PE, oznaczając intensywność uszkodzeń niebezpiecznych i-tego elementu λ_{Di}. Ze względu na zmianę tego wskaźnika w czasie wyznacza się jego wartość średnią z uwzględnieniem przedziałów czasowych pomiędzy testowaniem T_i kolejnych elementów tworzących strukturę.

Dla systemu na Rys.6.2 otrzymuje się, przy założeniu identycznych elementów o intensywności uszkodzeń niebezpiecznych elementów λ_D, bez uwzględnienia funkcji diagnostycznych i uszkodzeń zależnych, przeciętną częstość uszkodzeń niebezpiecznych w okresie pomiędzy testami T

$$PFH \cong \lambda_D^2 T \tag{6.7}$$

Uwzględniając uszkodzenia zależne dwóch elementów z parametrem β uzyskuje się zależność

$$PFH^Z \cong (1-\beta)^2 \lambda_D^2 T + \beta \lambda_D \tag{6.8}$$

Jeśli uwzględnić dodatkowo pokrycie diagnostyczne DC poszczególnych elementów i zróżnicowany czas pomiędzy ich testami diagnostycznymi uzyskuje się [6.7]

$$PFH_{DC}^{Z} \cong (1-\beta)^2[\lambda_D^2 \cdot DC \cdot T_2 + \lambda_D^2(1-DC) \cdot T_1] + \beta\lambda_D \tag{6.9}$$

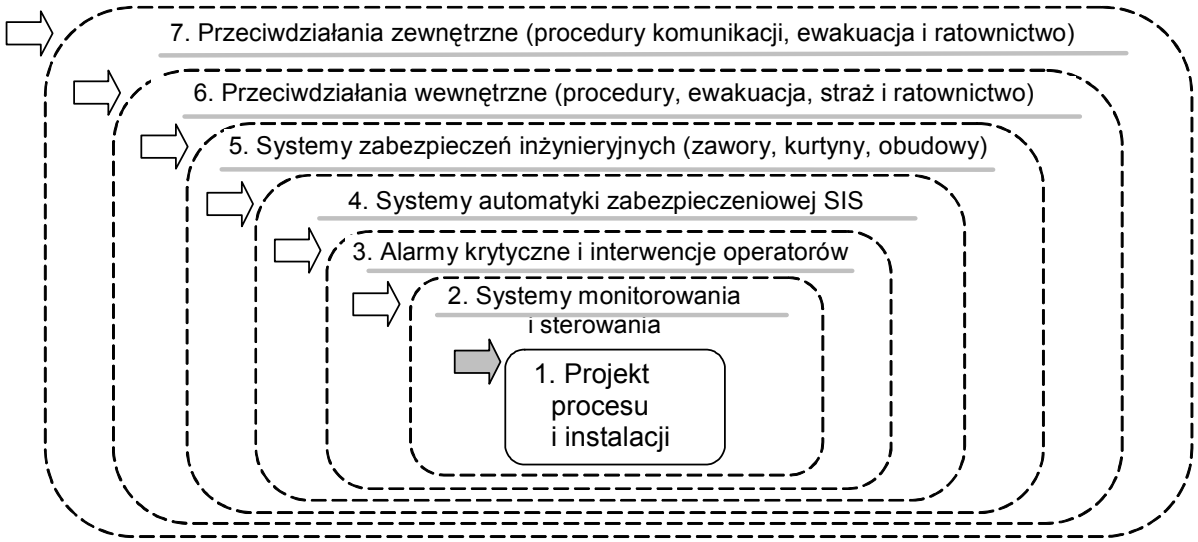
gdzie: T_1, T_2 – interwały testów diagnostycznych elementu (podsystemu) 1 i 2, β - współczynnik podatności elementów na uszkodzenie o wspólnej przyczynie (CCF); prawdopodobieństwo uszkodzenia niebezpiecznego w ciągu godziny będzie w tym przypadku $PDH_{DC}^{Z} \cong PFH_{DC}^{Z} \times 1h$.

Z wzorów (6.8) i (6.9) wynika, że architektura nadmiarowa pozwala na istotne zmniejszenie częstości uszkodzeń niebezpiecznych systemu, co najmniej o rząd wielkości, ponieważ w tych wzorach dominuje ostatni składnik (współczynnik β jest często przyjmowany na poziomie 0.1). Należy zaznaczyć, ze wzory dotyczące wyznaczania częstości zdarzeń niebezpiecznych podane w EN 62061 [6.7] są uproszczone i wymagają uaktualnienia. Jak wspomniano, integrowanie podsystemów związanych z bezpieczeństwem powinno być przeprowadzane zgodnie z zasadami podanymi w normie ISO 13849 [6.2]. Również ta norma wymaga weryfikacji i uaktualnienia podanych zależności.

6.3. Modelowanie bezpieczeństwa instalacji krytycznych

Współczesne złożone obiekty techniczne podwyższonego ryzyka, stwarzające zagrożenia dla człowieka i środowiska, projektuje się stosując warstwy zabezpieczeniowo-ochronne i zasadę „obrony w głąb". Obiekty te są coraz częściej w wysokim stopniu zautomatyzowane i skomputeryzowane. Istotny wpływ na ich bezpieczeństwo mają systemy sterowania i automatyki zabezpieczeniowej, które realizują różne funkcji bezpieczeństwa [6.1]. *Warstwy zabezpieczeń* obejmują nie tylko środki techniczne, ale i działania podejmowane przez człowieka. Jak wspomniano, na bezpieczeństwo obiektu złożonego mają istotny wpływ czynniki ludzkie i organizacyjne [6.8].

Podstawowym zadaniem systemu bezpieczeństwa jest redukcja częstości występowania stanów nienormalnych, a po wystąpieniu awarii ograniczenie rozmiaru szkody. Przykładowy warstwowy system zabezpieczeń złożonego obiektu podwyższonego ryzyka przedstawiono na Rys.6.3. Należy podkreślić znaczenie zastosowania właściwej technologii procesu i odporności instalacji na zakłócenia wewnętrzne, która jeśli to tylko możliwe powinna być projektowana zgodnie z zasadą *inherentnego bezpieczeństwa*. Dotyczy to warstwy 1 na Rys.6.3. Osobny problem stanowi eliminowanie lub redukowanie niekorzystnego wpływu zakłóceń zewnętrznych.



Rys. 6.3: Warstwy zabezpieczeń w złożonym obiekcie podwyższonego ryzyka

Do warstw zabezpieczeń systemu technologicznego podwyższonego ryzyka zalicza się (Rys.6.3): 2 - systemy monitorowania i sterowania, 3 - systemy alarmów krytycznych i interwencje operatorów, 4

- systemy automatyki zabezpieczeniowej SIS (*Safety Instrumented System*) [6.5], 5 - systemy zabezpieczeń inżynieryjnych i lokalizacji skutków awarii (zawory bezpieczeństwa instalacji ciśnieniowych, kurtyny, bariery i obudowy i inne urządzenia), 6 – przeciwdziałania wewnętrzne (plany awaryjne, procedury i środki techniczne, których celem jest minimalizowanie strat ludzkich i majątkowych), oraz 7 - przeciwdziałania zewnętrzne, których celem jest minimalizowanie strat na zewnątrz obiektu po wystąpieniu poważnej awarii.

Na skuteczność funkcjonowania całego systemu zabezpieczeń wpływa istotnie system zarządzania bezpieczeństwem w przedsiębiorstwie (technologiczne procedury awaryjne, procedury administracyjne, plany awaryjne) i współpraca z jednostkami zewnętrznymi (straż pożarna, ratownictwo, sztab zarządzania kryzysowego).

Należy podkreślić, że koncepcja bezpieczeństwa funkcjonalnego zawarta w normach IEC 61508 i IEC 61511 ma istotne znaczenie w zarządzaniu bezpieczeństwem obiektu, gdyż ma związek z warstwami 2, 3, 4, a nawet 5. Na funkcjonowanie kolejnych warstw zabezpieczeniowych mają istotny wpływ czynniki ludzkie oraz czynniki organizacyjne.

Rys.6.3 nie uwzględnia niektórych ważnych dla bezpieczeństwa obiektu systemów, takich jak system monitorowania pożarowego, systemy gaśnicze wraz z układami sterowania, systemy komunikacji i inne. Niektóre z nich powinny być również projektowane zgodnie z kryteriami bezpieczeństwa funkcjonalnego. Dotyczy to również systemów zainstalowanych w atmosferze zagrożonej wybuchem.

Warstwy zabezpieczeń oznaczone numerami od 2 do 5 na Rys.6.3 powinny być niezależne fizycznie i funkcjonalnie. Warstwę zabezpieczeń (urządzenie, system lub działanie) uważa się za niezależną (IPL - *Independent Protection Layer*) [6.1] jeśli:

- jest skuteczna w zapobieganiu lub ograniczaniu skutków stanów nienormalnych, kiedy funkcjonuje zgodnie z projektową specyfikacją techniczną,
- spełnia wymóg niezależności od rozważanych zdarzeń inicjujących i elementów składowych innych warstw zabezpieczeń, gdy są one przywoływane do działania (rozważa się szereg scenariuszy awaryjnych),
- jest audytowalna przez potwierdzenie założonej skuteczności działania warstwy na podstawie dokumentacji, przeglądów, testów, modelowania oraz osiągniętego poziomu nienaruszalności bezpieczeństwa SIL.

Wyróżnia się dwa podstawowe rodzaje niezależnych warstw zabezpieczeń IPL [6.1]:

- *bierne* IPL,
- *aktywne* IPL.

W systemie zabezpieczeń wymaga się funkcji aktywnej IPL, aby spowodować zmianę stanu systemu w odpowiedzi na stan procesu, reprezentowany zakresem zmian określonych wielkości fizycznych (np. temperatura, ciśnienie, poziom wibracji), albo na sygnał z innego miejsca (np. zmiana stanu przycisku lub wyłącznika). Aktywna warstwa typu IPL zawiera ogólnie:

- *sensor / czujnik* dowolnego rodzaju (przyrząd pomiarowy, urządzenie przestawne, narząd ludzki itd.),
- *element przetwarzania informacji i podejmowania decyzji* (przekaźnik, moduł logiczny, sterownik programowalny, człowiek itp.),
- *działanie* realizowane automatycznie i/lub przez człowieka.

W szczególności czynna IPL może być zaprojektowana jako system automatyki zabezpieczeniowej zrealizowany jako system E/E/PE [6.6] lub SIS [6.5].

Mimo stosowania kilku warstw zabezpieczeń w obiektach powyższego ryzyka występują w nich nadal awarie z poważnymi skutkami wewnątrz i niekiedy również na zewnątrz (w otoczeniu zakładu przemysłowego). W celu skutecznego przeciwdziałania potencjalnym awariom, podstawowe znaczenie ma zrozumienie ich przyczyn. Ze względu na złożoność problemu analizę ryzyka przeprowadza

się zwykle dla kilku najważniejszych scenariuszy awaryjnych, które reprezentują określone kategorie zdarzeń awaryjnych [6.4].

Metoda analizy warstw zabezpieczeń LOPA (*Layer of Protection Analysis*) [6.1] opiera się na zgrubnej ocenie ryzyka. Jest ona szczególnie przydatna we wstępnej analizie ryzyka dzięki wyróżnieniu ważniejszych scenariuszy awaryjnych na podstawie analizy HAZOP [6.14] i wstępnym zdefiniowaniu matrycy ryzyka (zakresy częstości i skutków potencjalnych zdarzeń awaryjnych). Szczególna zaleta tej metody tkwi w przejrzystej ocenie probabilistycznej funkcji bezpieczeństwa i warstw zabezpieczeń, które obejmują systemy sterowania i automatyki zabezpieczeniowej. Ilościowa oszacowanie probabilistyczne utraty funkcji bezpieczeństwa bazuje na prawdopodobieństwie niezadziałania na żądanie PFD. Dotyczy ono w szczególności systemów E/E/PE [6.6] i SIS [6.5].

Znając oszacowania wartości PFD funkcji bezpieczeństwa wyróżnionych w ramach i-tego scenariusza awaryjnego można napisać wzór na jego częstość

$$F_i = F_i^I \prod_{j=1}^{J} PFD_{ij} \tag{6.10}$$

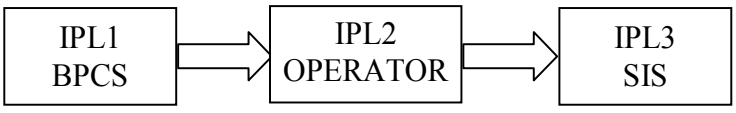
gdzie: F_i^I - częstość i-tego zdarzenia inicjującego (I), a^{-1}; PFD_{ij} - prawdopodobieństwo niewypełnienia j-tej funkcji na przywołanie dla i-tego zdarzenia inicjującego.

Dane niezawodnościowe i inne parametry modeli probabilistycznych występujące we wzorze (6.6) pochodzą w praktyce z różnych źródeł, którymi mogą być [6.1], [6.4]:

- dane pozyskane z podobnych instalacji danego sektora przemysłowego,
- dane pozyskane z baz danych ogólnych (dane generyczne) [6.21], [6.19],
- dane wyznaczone na podstawie danych statystycznych przebiegu eksploatacji konkretnej instalacji i zaistniałych uszkodzeń (niestety nie są one gromadzone systematycznie w przemyśle),
- dane dostawców wyposażenia (są one niestety zwykle zbyt optymistyczne),
- dane bazujące na opiniach ekspertów, w szczególności dane generyczne korygowane przez ekspertów z uwzględnieniem różnych czynników [6.10], [6.13], [6.21], [6.19].

Na Rys.6.4 przedstawiono trzy warstwy IPL [6.1], które mają zapobiec wstąpieniu zdarzenia awaryjnego:

- IPL1 – podstawowy system sterowania (*Basic Process Control System* - BPCS),
- IPL2 – człowiek-operator, który nadzoruje proces i interweniuje w razie wystąpienia sytuacji nienormalnej lub awaryjnej,
- IPL3 – system zabezpieczeń (*Safety Instrumented System* - SIS).



Rys. 6.4: Oddziaływanie przykładowych warstw zabezpieczeń

Stan awaryjny z poważnymi skutkami nastąpi, jeśli kolejne warstwy nie wypełnią funkcji związanych z bezpieczeństwem. Wobec tego częstość i-tego scenariusza awaryjnego w modelu ryzyka w przypadku tych warstw określa wzór

$$F_i = F_i^I \cdot PFD_{i;IPL1} \cdot PFD_{i;IPL2} \cdot PFD_{i;IPL3} \tag{6.11}$$

Przykładowe oszacowania wartości PFD dla różnych architektur systemów E/E/PE lub SIS, z uwzględnieniem pokrycia diagnostycznego podsystemów i możliwych uszkodzeń zależnych, można znaleźć w poradniku [6.1] i monografii [6.9]. W konkretnych rozwiązaniach architektury systemu

E/E/PE lub SIS należy zastosować odpowiednie metody modelowania probabilistycznego zarysowane odpowiednio w normach [6.6] i [6.5]. Problem polega na tym, że zdarzenia polegające na uszkodzeniach lub błędach człowieka w kolejnych warstwach zabezpieczeń mogą być zależne. Wymaga to stosowania odpowiednich metod modelowania probabilistycznego zdarzeń zależnych, czego nie zawiera poradnik [6.1] i norma [6.5]. Dlatego wzór (6.11) wymaga modyfikacji, a zamiast indeksów IPL (*Independent Protection Layer*) występują indeksy PL (*Protection Layer*)

$$F_i^Z = F_i^I \cdot PFD_{i;PL1} \cdot PFD_{i;PL2} \cdot PFD_{i;PL3} = k_Z F_i \tag{6.12}$$

Współczynnik k_Z ($k_Z >> 1$) we wzorze (6.12) może przyjmować wartość nawet na poziomie 10 i więcej zależnie od warstw zabezpieczeń i rodzajów zależności. Możliwość występowania zdarzeń zależnych jest uwarunkowana czynnikami technicznymi i środowiskowymi, a przede wszystkim czynnikami ludzkimi i organizacyjnymi [6.4], [6.7], [6.15], [6.14].

6.4. Wpływ czynników ludzkich i organizacyjnych na bezpieczeństwo obiektu krytycznego

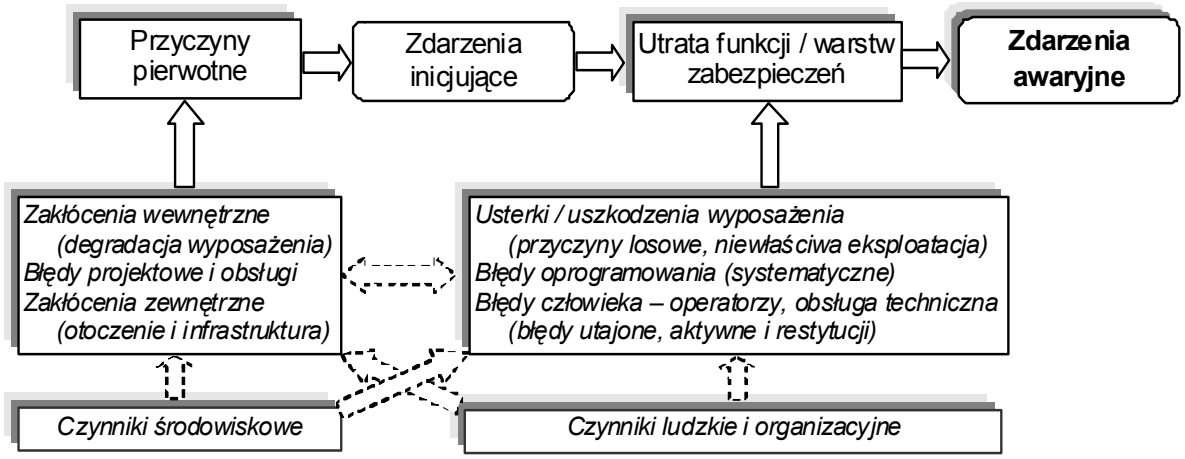
Warstwa IPL2 na Rys.6.4 stanowi szczególne wyzwanie w analizie i modelowaniu probabilistycznym, gdyż wymaga przeprowadzenia analizy niezawodności człowieka HRA (*human reliability analysis*) [6.4]. Podstawą HRA jest analiza zadań człowieka- operatora dla rozważanej funkcji związanej z bezpieczeństwem. Należy również uwzględnić interfejs człowiek-system MMI (*man machine interface*) obejmujący rozwiązania projektowe systemu SCADA (*supervisory control and data acquisition*). Skuteczność wypełnienia funkcji przez taką warstwę zależy istotnie od szeroko rozumianych czynników ludzkich i organizacyjnych.

Na podkreślenie zasługuje zgodny w literaturze pogląd, że niewłaściwie kształtowane czynniki ludzkie i organizacyjne są przyczyną aż 70%, a w niektórych sektorach aż 90% wypadków i zdarzeń awaryjnych w systemach technicznych [6.8]. Czynniki organizacyjne dotyczą wszystkich warstw przedstawionych na Rys.6.3. Niestety, analiza HRA jest traktowana często marginalnie w praktyce probabilistycznych oceny ryzyka.

Przyczyny sytuacji nienormalnych i uwarunkowania zdarzeń awaryjnych w złożonym obiekcie przemysłowym zestawiono poglądowo na Rys.6.5. Zdarzenia awaryjne mogą być zainicjowane zakłóceniami wewnętrznymi, spowodowanymi degradacją wyposażenia spowodowaną uszkodzeniami i błędami oraz zakłóceniami zewnętrznymi związanymi z niekorzystnym wpływem otoczenia i infrastruktury technicznej. Mogą się one rozwinąć w poważną awarię w przypadku utraty istotnych funkcji bezpieczeństwa, przewidzianych w projekcie systemu zabezpieczeniowego. Przyczynami utraty tych funkcji mogą być usterki i uszkodzenia wyposażenia (przyczyny losowe lub niewłaściwa eksploatacja urządzeń), a także błędy systematyczne oprogramowania w systemach sterowania i programowalnej automatyki zabezpieczeniowej. Szeroko rozumiane błędy człowieka obejmują zarówno błędy projektowe, operatorów w sterowni, jak i personelu obsługi technicznej [6.9].

Wyróżnia się błędy utajone, aktywne i restytucji. Mogą one mieć charakter pominięcia (*omission*) i popełnienia (*commission*). W sytuacjach nienormalnych szczególnie niekorzystna jest kombinacja błędów utajonych i aktywnych. Ważne znaczenie w HRA ma wyróżnienie rodzajów zachowań. Nawiązuje się w niektórych modelach niezawodności człowieka do klasyfikacji działań opartych na *wprawie*, *regułach* i *wiedzy* (SRK – *skill, rules, knowledge*). Analiza działań człowieka i identyfikacja potencjalnych błędów w ramach HRA wymagają oceny sytuacyjnej (kontekstowej) w ramach kolejnych scenariuszy awaryjnych.

Uszkodzenia można eliminować lub redukować ich częstość występowania poprzez wprowadzenie nowoczesnego systemu zarządzania jakością oraz skutecznego nadzoru technicznego i administracyjnego. W modelowaniu probabilistycznym warstw zabezpieczeń i sekwencji zdarzeń awaryjnych istotne jest uwzględnienie zdarzeń zależnych dotyczących uszkodzeń wyposażenia i błędów ludzkich.



Rys. 6.5: Przyczyny sytuacji nienormalnych i uwarunkowania przebiegu zdarzeń awaryjnych

Pominięcie tych zależności może doprowadzić do zbyt optymistycznych wyników modelowania probabilistycznego systemu, a tym samym oszacowań ryzyka [6.9].

Kształtowanie czynników ludzkich i organizacyjnych ma istotny wpływ na możliwość popełniania błędów w obiektach krytycznych. Błędy człowieka nadzorującego złożony obiekt techniczny klasyfikuje się m.in. ze względu na fazę ich występowania. Wyróżnia się trzy następujące kategorie działań i błędów człowieka [6.4]:

A. Działania i błędy popełnione przed wystąpieniem zdarzeń inicjujących (ZI) zakłócenie lub awarię, które mogą być przyczyną *niesprawności utajonych;*

B. Działania i błędy przyczyniające się do zainicjowania zdarzenia nienormalnego;

C. Działania i błędy popełnione po wystąpieniu ZI.

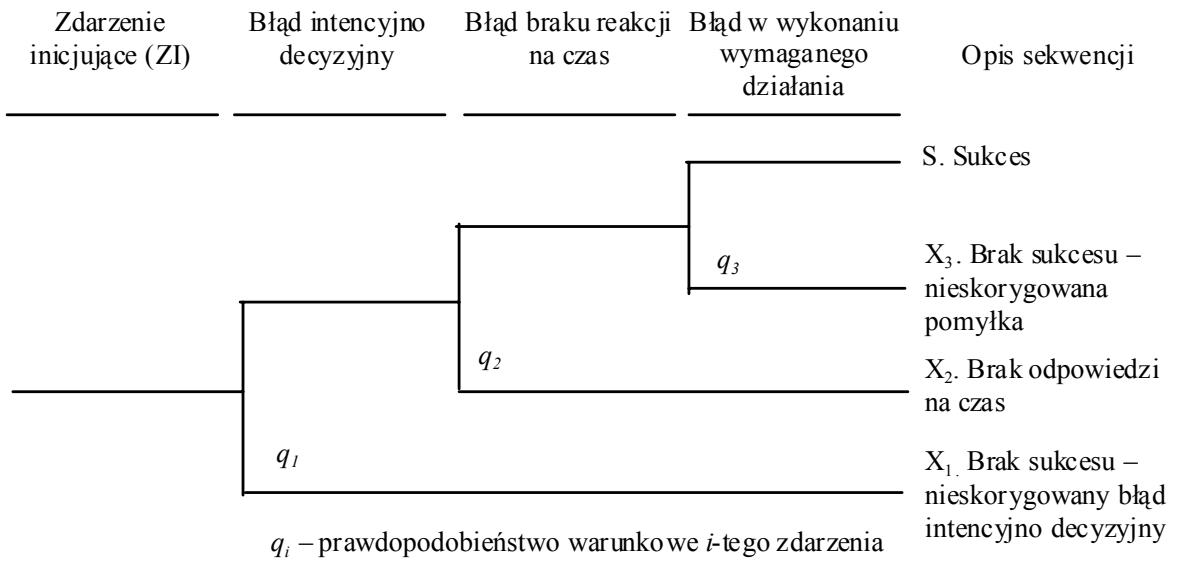
Działania i błędy kategorii C dzielą się na: (C1) proceduralne działania bezpieczeństwa, (C2) błędne działania (błędy aktywne) pogarszające przebieg sytuacji nienormalnej lub awarii oraz (C3) zaimprowizowane działania korygujące, zgodne z zasadami postępowania przewidzianymi na wypadek awarii, przywracające funkcjonowanie układów. Należy zaznaczyć, że w sytuacji popełnienia przez człowieka błędów utajonych (kategoria A), a następnie błędów aktywnych (B lub C2), mogą wystąpić bardzo niekorzystne sytuacje, podczas których realizacja działań proceduralnych (C1) lub korygujących (C3) będzie znacznie utrudniona, z małym prawdopodobieństwem sukcesu.

Na Rys.6.6 przedstawiono drzewo ilustrujące możliwe interakcje kategorii C. Wyróżniono na nim trzy kategorie zdarzeń – błędnych działań człowieka:

- X_1 – błąd intencyjny popełniany podczas diagnozy i podejmowania decyzji,
- X_2 – błąd braku reakcji na czas,
- X_3 – błąd (pomyłka) przeprowadzenia wymaganych, poprawnie zaplanowanych działań.

Powodami błędu X_1 może być niewłaściwa interpretacja procedur operacyjnych lub niepełna/ niepoprawna informacja dotycząca stanu obiektu (niedostateczne monitorowanie i komunikacja) lub braki wiedzy operatorów, co przyczyni się do błędnej diagnozy i niewłaściwej decyzji dotyczącej planu działania. Błąd X_2 występuje zwłaszcza w przypadku obiektów o większej dynamice. Błąd X_3 jest pomyłką (ang. *slip*) i dlatego jest łatwiejszy do korygowania. Jeśli załoga zorientuje się, że popełniła błąd, to możliwe jest podjęcie działań korygujących pod warunkiem, że proces o mniejszej dynamice jest odwracalny i występuje rezerwa czasowa na przeprowadzenie wymaganych działań.

Do wyznaczenia prawdopodobieństw *q1*, *q2* i *q3* występujących w drzewie zdarzeń na Rys.6.6 można stosować różne metody HRA [6.8], [6.9], [6.4]. Błędy intencyjne i decyzyjne człowieka-operatora są szczególnie trudne w ocenie [6.8]. Na prawdopodobieństwo popełnienia błędu przez



Rys. 6.6: Przykładowe drzewo zdarzeń z błędami kategorii C

człowieka-operatora wpływa szereg czynników o charakterze ogólnym, na przykład: (1) projekt interfejsu HMI (*Human-Machine Interface*), (2) stres, (3) kognitywne aspekty działania na poziomie wprawy, reguł i wiedzy SRK (*skill, rules & knowledge*), (4) doświadczenie, (5) kultura bezpieczeństwa, (6) poziom wyszkolenia, (7) motywacja, (8) obciążenie pracą, (9) nadzór, (10) komunikacja, (11) procedury. Czynniki wpływu można przedstawiać w ramach hierarchicznego diagramu wpływu [6.8].

W Tablicy 6.3 zestawiono orientacyjne wartości PFD (prawdopodobieństwa potencjalnych błędów człowieka-operatora na przywołanie i działanie) dla warstwy 3 na Rys.6.3. Do wyznaczania prawdopodobieństw błędów człowieka stosuje się często w praktyce przemysłowej metodę THERP [6.9].

Należy podkreślić znaczenie w redukowaniu potencjalnych błędów człowieka-operatora odpowiednio zaprojektowanych systemów doradczych, zaimplementowanych na przykład w ramach BPCS z przyjaznym HMI. Istotne znaczenie w eliminowaniu tych błędów mają również odpowiednio zaprojektowane systemy E/E/PE [6.6], [6.7] i SIS [6.5] pełniące funkcje związane z bezpieczeństwem.

6.5. Problemy modelowania bezpieczeństwa rzeczywistych obiektów złożonych

Na podstawie modeli probabilistycznych zarysowanych w niniejszym rozdziale możliwa jest ocena proponowanych rozwiązań projektowych systemów sterowania i zabezpieczeń redukujących ryzyko związane z eksploatacją maszyn i instalacji krytycznych. Zarządzanie bezpieczeństwem funkcjonalnym tych systemów polega na:

- analizie zagrożeń i identyfikacji funkcji bezpieczeństwa,
- wyznaczeniu wymaganego poziomu SIL dla tych funkcji na podstawie analizy i oceny ryzyka długoterminowego (statycznego),
- weryfikacji poziomu SIL na podstawie odpowiednich modeli probabilistycznych dla funkcji bezpieczeństwa do zaimplementowania w praktyce za pomocą proponowanych rozwiązań systemów E/E/PE lub SIS,
- weryfikacji poziomu SIL w procesie eksploatacji z uwzględnieniem interwałów testowania podsystemów w systemach E/E/PE lub SIS oraz uaktualnionych danych niezawodnościowych.

Tab. 6.3: Przykładowe działania człowieka i orientacyjne prawdopodobieństwa błędów w warstwie zabezpieczeń [6.9]

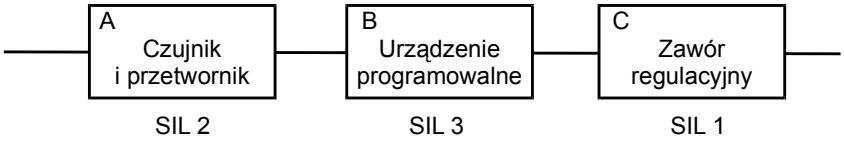
Działanie w warstwie IPL	Założenia i uwagi	PFD*
Działanie człowieka operatora w ciągu 1 minuty (dozwolony czas reakcji)	Interwencja w bardzo krótkim czasie w złożonym obiekcie przemysłowym	1
Działanie człowieka operatora w ciągu 10 minut	Dobrze określone działanie z przejrzystymi i niezawodnymi wskaźnikami wielkości charakteryzujących proces	10^{-1}
Działanie operatora według informacji z podstawowego systemu sterowania (BPCS) lub alarmów w ciągu 40 min.	Dobrze określone działanie z przejrzystymi i niezawodnymi wskaźnikami wielkości charakteryzujących proces, wymaganymi w danym działaniu (PFD sugerowane w IEC 61511 [6.5])	10^{-1}
Działanie człowieka operatora w ciągu 60 minut	Zdefiniowane działania z przejrzystą i niezawodną prezentacją wymaganej informacji	10^{-2}
*Prawdopodobieństwo błędu na przywołanie i działanie PFD (*probability of failure on demand*)		

Problem polega na tym, że systematyczne gromadzenie danych o przebiegu eksploatacji i zaistniałych uszkodzeniach jest jeszcze rzadkością w krajowym przemyśle. W związku z tym trzeba korzystać z różnych źródeł danych, w tym ogólnych danych niezawodnościowych oraz korzystać z opinii ekspertów. Dane niezawodnościowe o charakterze ogólnym dotyczące niektórych kategorii urządzeń, głównie elektrycznych i elektromechanicznych opublikowano w krajowych pracach [6.10], [6.11], [6.12], [6.18] i zagranicznych [6.20]. W standardzie amerykańskim [6.21] i poradniku [6.19] podano zasady korekcji danych generycznych dla odmiennych czynników środowiskowych w jakich zainstalowane będzie urządzenie. Przykładowe dane o charakterze ogólnym dotyczące elementów systemów E/E/PE i SIS znajdują się w normach międzynarodowych [6.3], [6.6], [6.5], [6.7], [6.2].

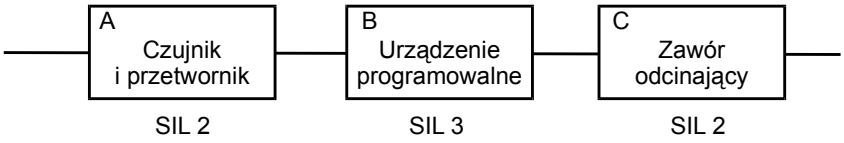
Dla przykładu rozważony będzie układ sterowania i układ zabezpieczeń turbiny przedstawiony na Rys.6.7, które realizują funkcję awaryjnego wyłączenia turbiny. Układy te pełnią funkcje związane z bezpieczeństwem. Pierwszy z nich jest przykładem układu o działaniu ciągłym, a drugi – układu działającego na przywołanie. W związku z tym mają zastosowanie, dla znanego poziomu SIL, kryteria probabilistyczne wyszczególnione w Tablicy 3.2, odpowiednio w drugiej i trzeciej kolumnie. Analiza możliwego scenariusza awaryjnego wykazała, że rozważana funkcja bezpieczeństwa powinna być realizowana na poziomie SIL4.

Wyniki zgrubnej analizy bezpieczeństwa funkcjonalnego rozważanych układów znajdują się odpowiednio na Rys.6.7 i Rys.6.8. Wynika z nich, że pierwszy z nich – układ sterowania turbiną (UST) umożliwia realizowanie poziomu nienaruszalności bezpieczeństwa SIL1, do czego przyczynił się głównie zawór regulacyjny (SIL1). Pozostałe elementy są znacznie bardziej niezawodne: A (SIL2) i B (SIL3). Natomiast układ zabezpieczenia turbiny (UZT) umożliwia realizowanie poziomu nienaruszalności bezpieczeństwa SIL2, ponieważ układ zaworu odcinającego jest bardziej niezawodny niż układ zaworu regulacyjnego.

Warstwy zabezpieczeń w systemie awaryjnego wyłączania turbiny w nawiązaniu do Rys.10.3 (BPCS-Operator-SIS) przedstawiono na Rys.6.8. Ze względu na dynamikę zdarzeń (wymagany bardzo krótki czas reakcji – zob. Tablica 6.3) przyjęto prawdopodobieństwo błędu człowieka równe 1, wobec tego cały system realizuje całą funkcję bezpieczeństwa na poziomie SIL3 (SIL1+SIL3). Wymaganie SIL4 nie jest więc spełnione i należy rozważyć modyfikację projektową, przede wszystkim

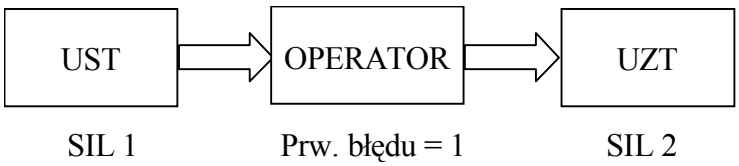


Rys. 6.7: System E/E/PE w układzie sterowania turbiną (UST) z funkcją bezpieczeństwa



Rys. 6.8: System E/E/PE w kładzie zabezpieczenia turbiny pełniący funkcję bezpieczeństwa

systemu UZT, który powinien spełniać wymagania SIL3. Wynika to z oceny, że podniesienie SIL układu zaworu regulacyjnego z SIL1 do SIL2 może okazać się bardzo trudne technicznie.



Rys. 6.9: Warstwy zabezpieczeń w systemie awaryjnego wyłączenia turbiny

Aby poprawić poziom nienaruszalności bezpieczeństwa w układzie zabezpieczenia turbiny (Rys.6.7) do SIL3, należy podnieść SIL w podukładzie A (czujnik i przetwornik) do SIL3 i w podukładzie zaworu odcinającego do SIL3. W podukładzie A proponuje się zastosować strukturę 2oo3, która pozwoli spełnić wymaganie SIL3. Aby uniknąć wyłączeń nieuzasadnionych turbiny o potencjalnie dużych stratach nie należy w tym przypadku stosować struktury 1oo2. W podukładzie C nie jest uzasadnione zastosowanie struktury redundancyjnej 1oo2 ze względów technicznych i bardzo wysokich kosztów. Dlatego należy przyjąć taką strategię obsługi i testowania zaworu odcinającego w czasie, aby było możliwe uzyskanie poziomu nienaruszalności bezpieczeństwa SIL3.

Bibliografia

[6.1] American Institute of Chemical Engineers, New York. *Layer of Protection Analysis, Simplified Process Risk Assessment, Center for Chemical Process Safety*, 2001.

[6.2] European Committee for Standardisation (CEN). *ISO/DIS 13849-1:2004 "Safety of Machinery – Safety – related parts of control systems – Part 1: General principles for design"*, 2004.

[6.3] Goble W.M., Cheddie H. Safety instrumented systems verification. *ISA (The Instrumentation, Systems and Automation Society)*, Research Triangle Park, NC 27709, 2005.

[6.4] International Atomic Energy Agency, Vienna. *IAEA-Safety Series No. 50-P-4: Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)*, 1992.

[6.5] International Electrotechnical Commission. *IEC 61511:2000: Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1–3*.

[6.6] International Electrotechnical Commission (IEC). *IEC 61508:1998. Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems. Parts 1–7*.

[6.7] International Electrotechnical Commission (IEC). *IEC/CEI 62061:2005 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*, 2005.

[6.8] Kosmowski K.T. *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Monografie 33. Wydawnictwo Politechniki Gdańskiej, Gdańsk, 2003.

[6.9] Kosmowski K.T., redaktor. *Functional Safety Management In Critical Systems*. Politechnika Gdańska. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk, 2007.

[6.10] Laudyn D., Maksymiuk J. *Jakość i niezawodność w elektroenergetyce*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 1996.

[6.11] Laudyn D., Pawlik M., Strzelczyk F. *Elektrownie*. WNT, 2000.

[6.12] Maksymiuk J. *Niezawodność maszyn i urządzeń elektrycznych*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2003.

[6.13] Moubray J. *Reliability-Centered Maintenance*. Industrial Press Inc, New York, 1992.

[6.14] *PN-EN 1050:1996. Maszyny. Bezpieczeństwo. Zasady oceny ryzyka*.

[6.15] *PN-IEC 300-3-9: 2000. Analiza ryzyka w systemach technicznych (IEC 300-3-9: 1995)*.

[6.16] *PN-IEC 812:1994: Techniki analizy niezawodności systemu - Procedura analizy postaci i skutków uszkodzeń (Procedure for Failure Mode and Effects Analysis - FMEA)*.

[6.17] Polski Komitet Normalizacyjny. *PN-EN 954-1:2001 Maszyny. Bezpieczeństwo. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania*, 2001.

[6.18] Sozański J. *Niezawodność i jakość pracy systemu elektroenergetycznego*. WNT, Warszawa, 1990.

[6.19] Washington: U.S. Department of Defence. *MIL-HDBK-217F. Reliability Prediction of Electronic Equipment*, 1991.

[6.20] Wenyuan Li. *Risk Assessment of Power Systems – Models, Methods and Applications*. IEEE Press, 2005.

[6.21] Wiley, New York. *IEEE Standard 500: IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*, 1984.

Rozdział 7

Eksperyment diagnostyczny jako źródło informacji aposteriorycznej

Robert GUMIŃSKI

Dla osiągnięcia większej efektywności aplikacji rezultatów diagnostyki wibroakustycznej w znacznie większym stopniu powinna być uwzględniana indywidualna charakterystyka wibroakustyczna określana podczas wstępnych pomiarów i analizy.

Takie podejście w pełni spełnia wymogi metodologii bayesowskiej [7.1] w tym:

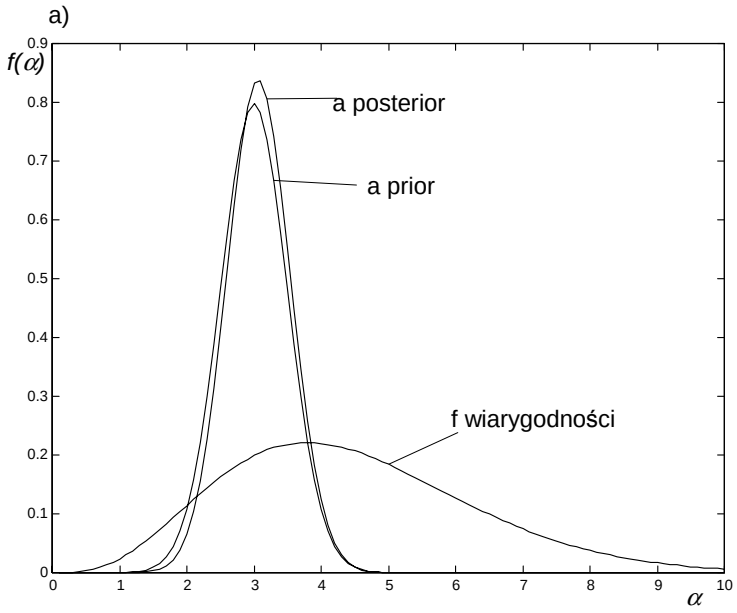
1. możliwości przyjęcia losowości parametru badanego modelu probabilistycznego;
2. możliwości otrzymania aposteriorycznego szacowania parametru na podstawie obserwacji i pomiarów sygnału wibroakustycznego oraz rozkładu apriorycznego, zgodnie z wymogami twierdzenia Bayesa;
3. wyboru optymalnego estymatora parametru w sensie bayesowskiej teorii decyzji.

Przyjmując, że efektem monitoringu wibroakustycznego jest detekcja, identyfikacja, lokalizacja zmian właściwości wibroakustycznych nadzorowanego obiektu, to aprioryczny rozkład prawdopodobieństwa parametrów można ustalić na podstawie wstępnie określonej charakterystyki wibroakustycznej.

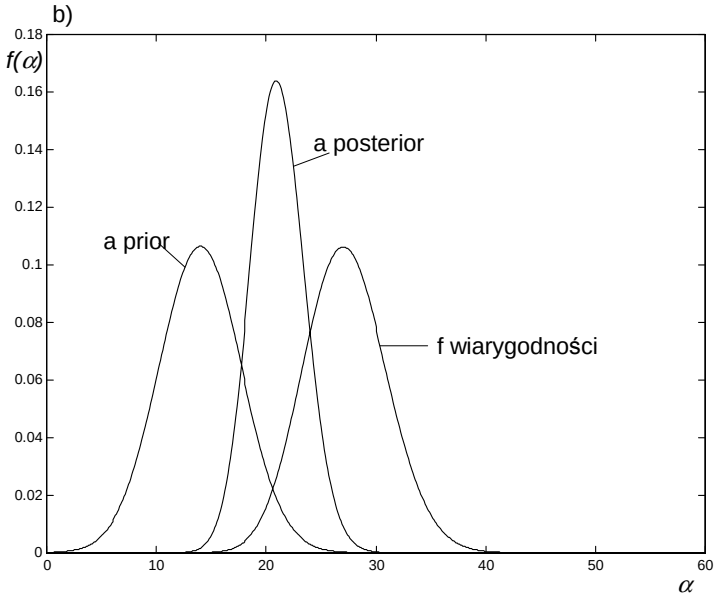
Przybliżając to zagadnienie, na Rys.7.1 do Rys.7.4 przedstawiono rezultaty wykorzystania metody uaktualnienia bayesowskiego w funkcji danych a priori oraz wyników eksperymentu będących źródłem dodatkowej informacji. Uzyskany wynik zależy od względnego położenia i rozrzutu funkcji określającej parametr a priori i funkcji wiarygodności. Należy podkreślić, że na powyższych rysunkach przedstawiono znormalizowaną funkcję wiarygodności. Przed omówieniem powyższych wyników przypomnijmy, że uaktualnienie bayesowskie umożliwia wprowadzenie do modelu dodatkowej informacji celem zmniejszenia niepewności prowadzonej analizy. Rozważono cztery przypadki:

a) informacja a priori o małym rozrzucie w stosunku do informacji a posteriori wprowadzonej do analizy w postaci funkcji wiarygodności utworzonej na podstawie realizacji (próby). Przeprowadzona analiza wykazuje nieznaczne zawężenie rozrzutu zaktualizowanego parametru, wynika to z niskiej informacyjności danych a posteriori. Z przeprowadzonej analizy wynika, że eksperyment diagnostyczny został źle zaplanowany. W związku z tym uzyskana informacja jest niepewna i przeprowadzony proces uaktualniania nie dał oczekiwanych rezultatów;

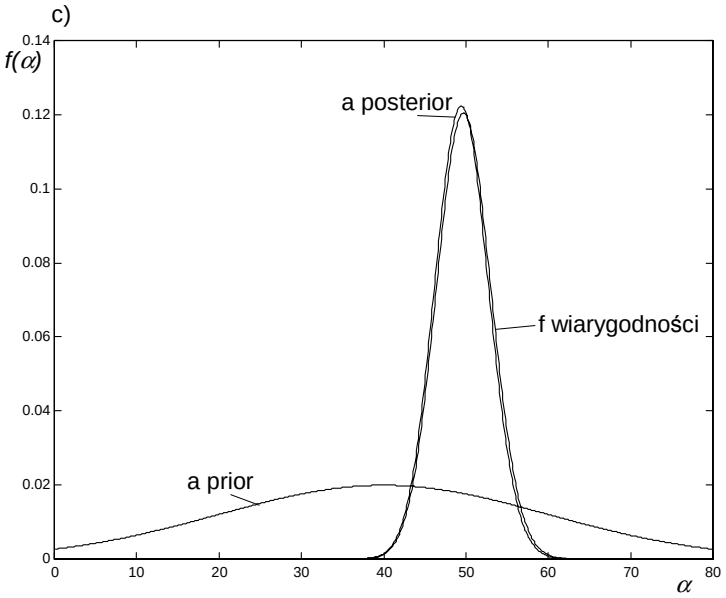
b) rozrzut danych a priori i a posteriori jest porównywalny natomiast występuje znaczne przesunięcie wartości średnich obu funkcji. Obrazuje to zmianę charakteru uszkadzania elementu, a co za tym idzie zmianę modelu statystycznego (niezawodnościowego) analizowanego obiektu. W efekcie otrzymujemy wynik o mniejszym rozrzucie, z wartością średnią przesuniętą w stosunku do wartości parametru estymowanej na podstawie wyników eksperymentu. Taki wynik



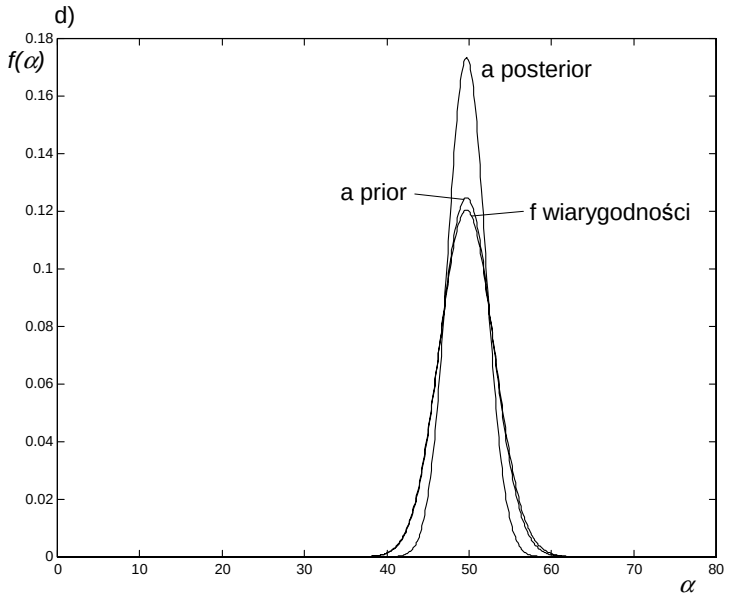
Rys. 7.1: Wyniki uaktualnienia bayesowskiego – porównanie



Rys. 7.2: Wyniki uaktualnienia bayesowskiego – porównanie



Rys. 7.3: Wyniki uaktualnienia bayesowskiego – porównanie



Rys. 7.4: Wyniki uaktualnienia bayesowskiego – porównanie

jest nie do zaakceptowania i podważa słuszność przeprowadzenia uaktualnienia bayesowkiego mino dobrze zaplanowanego eksperymentu. W takim przypadku lepszym rozwiązaniem wydaje się przeprowadzenie analizy na podstawie danych a posteriori;

c) w tym przypadku mamy do czynienia z niepewną informacją a priori. Aby zmniejszyć niepewność prowadzonej analizy zaplanowano eksperyment diagnostyczny, w wyniku którego otrzymano informację a posteriori o małym rozrzucie. Wynik przeprowadzonej analizy jest zadowalający ponieważ otrzymujemy znaczne zmniejszenie rozrzutu aktualizowanego parametru w stosunku do parametru a priori;

d) Ostatni rysunek przedstawia sytuację w której dane a priori i dane z eksperymentu pozwalają na uzyskanie parametru o podobnym rozrzucie. Otrzymany wynik uaktualniania ma mniejszy rozrzut niż w przypadku c). Sukces ten nie wynika z lepiej przeprowadzonego doświadczenia, mającego na celu uzyskanie dodatkowej informacji lecz z lepszej sytuacji jaką zastaliśmy przed rozpoczęciem analizy a mianowicie z małego rozrzutu parametru a priori. Zauważmy, że uzyskany wynik jest lepszy niż w przypadku c). Natomiast jeślibyśmy chcieli dokonać oceny wyników eksperymentu diagnostycznego, należałoby porównać rozrzuty parametru a priori i funkcji wiarygodności wyznaczonej na podstawie próby a posteriori (czyli używamy miary względnej np. stosunek rozrzutu obu funkcji). Okazuje się wówczas, że w przypadku c) uzyskano lepsze wyniki doświadczenia w stosunku do danych a priori niż w przypadku d).

Podsumowując, należy podkreślić, że w ocenie przydatności danych do procesu uaktualnienia bayesowskiego a tym samym poprawności planowania i prowadzenia eksperymentu należy porównać rozrzut parametru a priori i funkcji wiarygodności. Natomiast jeśli chcemy dokonać oceny rezultatów uaktualnienia bayesowskiego należy porównać rozkład parametru a priori i parametru zaktualizowanego. Można również zauważyć, że w przypadku gdy dane a posteriori mają znacznie mniejszy rozrzut od danych a priori, uaktualnienie bayesowskie powoduje nieznaczne zawężenie rozrzutu parametru w stosunku do funkcji wiarygodności. W tym przypadku klasyczna analiza statystyczna (z analizą niepewności na podstawie informacyjnej macierzy Fischera) na podstawie danych a posteriori dałaby przybliżone wyniki.

Z przeprowadzonej analizy wynika, że w procesie przygotowania danych do uaktualnienia bayesowskiego ważne jest odpowiednie zaplanowanie eksperymentu, bowiem gwarantuje to znaczne zmniejszenie niepewności. Dlatego niezbędne w trakcie planowania eksperymentu jest przeprowadzenie analizy pre-posteriori. Należy również pamiętać, iż nie wszystkie dane a posteriori pozwalają na przeprowadzenie uaktualnienia bayesowskiego prowadzącego do poprawnych decyzji eksploatacyjnych. Dane a posteriori muszą dotyczyć tego samego zjawiska lub sposobu uszkadzania.

W kolejnym przykładzie przeanalizowano proces uaktualnienia bayesowskiego parametru kształtu Weibulla przy założeniu różnych apriorycznych postaci rozkładu.

Na potrzeby tak zaplanowanego eksperymentu przygotowano dwa zbiory zmiennych losowych – czasów do wystąpienia uszkodzenia:

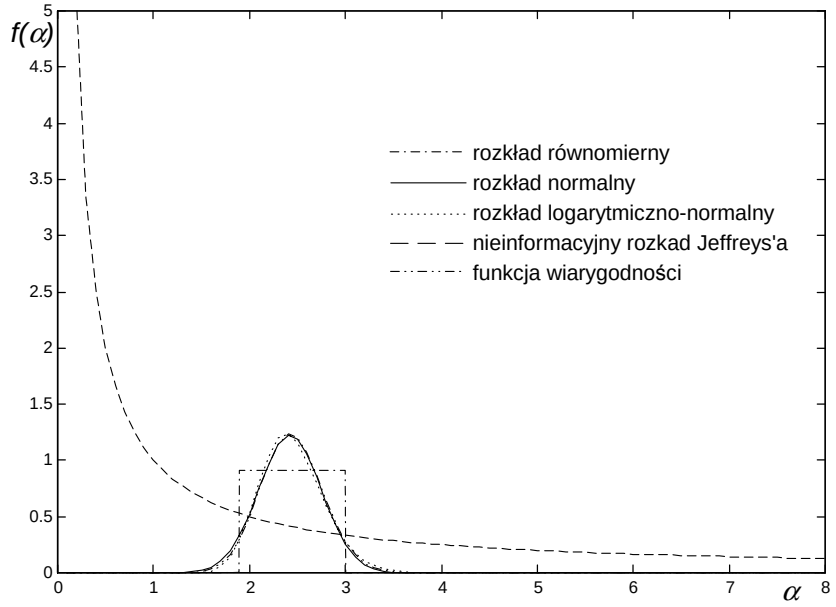
dane a priori:

4143.5	5659.6	8218.5	11839.9	14385.7	16071.4
4588.8	6956	9845.2	11989.9	15055.6	16886.7
4954.3	7091	9953.8	12435.2	15559.7	19446.3
5076.8	7427	9992.3	12495.1	15633.3	22134.9
5609.4	7875.4	11466.7	13205.7	15635	23417.7

dane a posteriori (P – elementy uszkodzone, S – elementy sprawne: w chwili zakończenia eksperymentu dwa elementy pozostały nieuszkodzone):

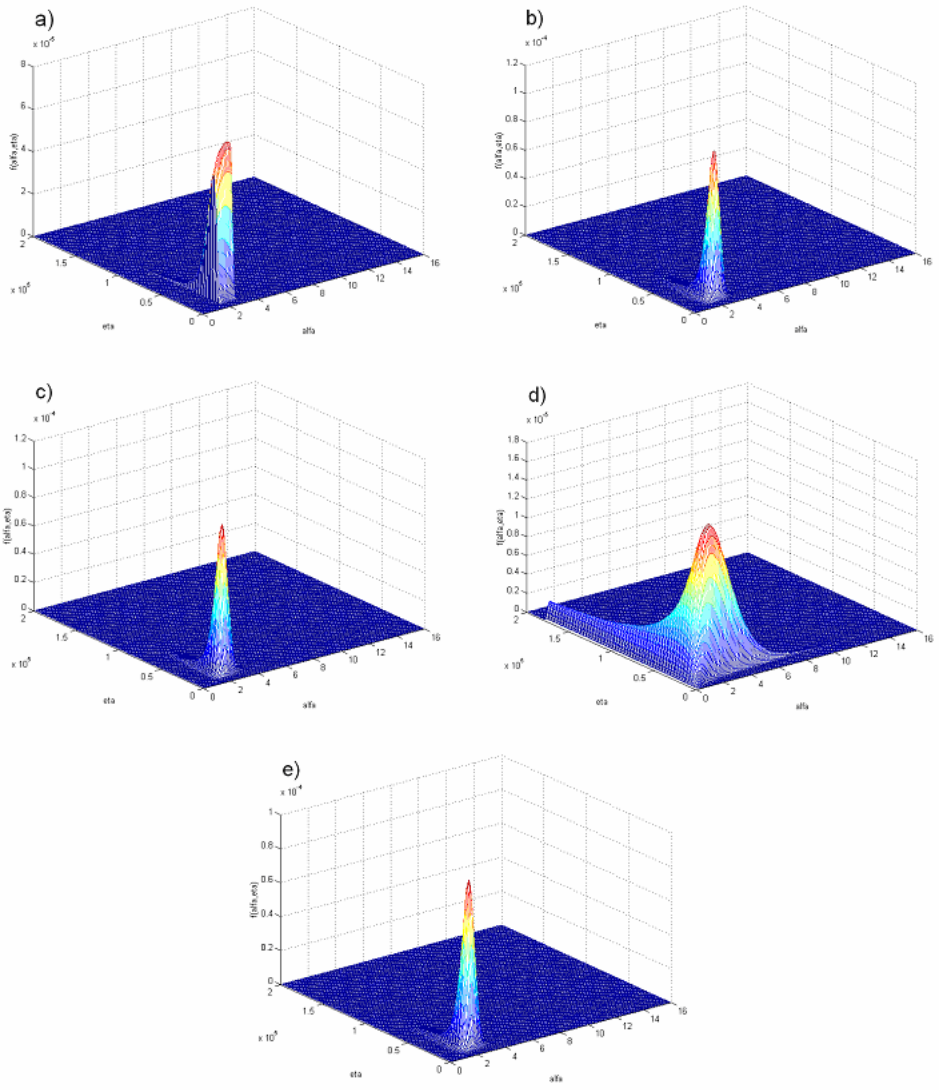
Czas	P/S
6494.7	P
11210.8	P
16226.2	P
16226.2	S
16226.2	S

Na podstawie powyższych danych założono rozkład Weibulla i estymowano parametry a priori czasu do wystąpienia uszkodzenia. Następnie korzystając z informacyjnej macierzy Fishera wyznaczono odchylenie standardowe parametru kształtu. W kolejnym kroku, dla tak wyznaczonych charakterystyk statystycznych parametru, wyznaczono aprioryczne funkcje gęstości prawdopodobieństwa parametru (Rys.7.5) przy założeniu rozkładów: równomiernego, normalnego i logarytmiczno-normalnego. Wyznaczono również rozkład Jefreysa, oraz aprioryczną funkcję wiarygodności. Parametr skali opisano rozkładem równomiernym o przedziale zmienności niewpływającym na kształt aposteriorycznej funkcji gęstości prawdopodobieństwa (nie jest to rozkład ucięty). Traktując jednowymiarowe rozkłady parametrów jako rozkłady graniczne, wyznaczono dwuwymiarowe rozkłady parametrów. Następnie wyznaczono dwuwymiarową funkcję wiarygodności i korzystając ze wzoru Bayesa, uaktualniono parametry rozkładu Weibulla (Rys.7.6). Na poniższych wykresach przedstawiono aprioryczne funkcje gęstości prawdopodobieństwa parametru kształtu oraz wyniki przeprowadzonej analizy.

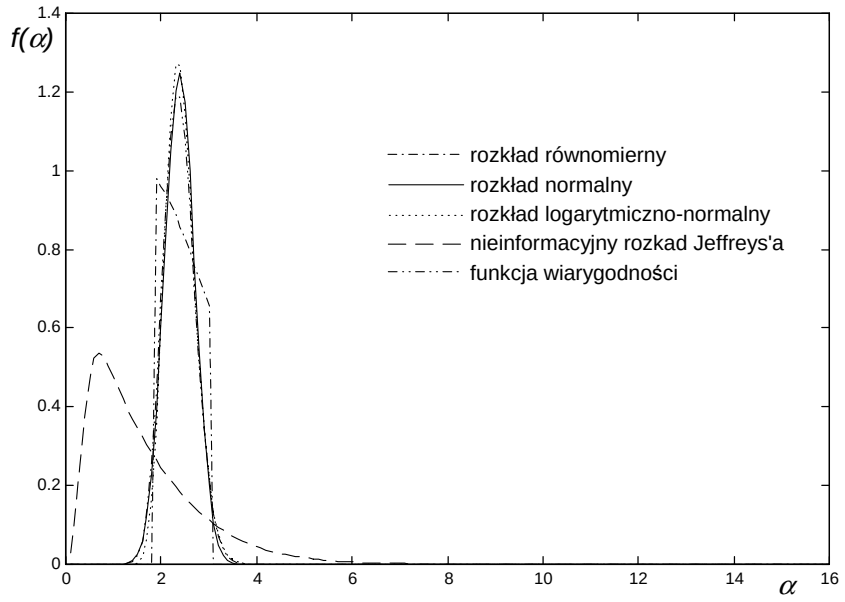


Rys. 7.5: Aprioryczna funkcja gęstości prawdopodobieństwa rozkładu parametru kształtu

Nieinformacyjny rozkład Jeffreys'a wykorzystujemy gdy nie mamy żadnej informacji o rozkładzie a priori. Rozkład ten jest odwrotnie proporcjonalny do wartości parametru i preferuje wartości parametru w pobliżu zera (dodatnie). W analizowanym przykładzie rozkład Jeffreys'a ma znacznie przesuniętą wartość modalną i w konsekwencji otrzymano zaktualizowaną funkcję rozkładu parametru w stosunku do wartości modalnej rozkładu parametru wyznaczonej na podstawie próby a posteriori. Analizując rezultaty aktualizacji parametru kształtu przy apriorycznym założeniu rozkładu Jeffreys'a dla parametru widzimy, że jest on bardziej skupiony i znacznie przesunięty w kierunku większych wartości: w kierunku wartości parametru wyznaczonej na podstawie próby. Zatem uwzględnienie w analizie dodatkowej informacji w postaci wyników pomiarów wprowadziło istotną zmianę. Porównując nowo otrzymany rozkład i wartości parametru estymowanej na podstawie próby możemy zauważyć, że wyżej wspomniane przesuniecie rozkładu w wyniku uaktualnienia bayesowskiego jest niewystarczające. Lepszym rozwiązaniem wydaje się wykonanie analizy na podstawie próby bez uwzględniania



Rys. 7.6: Dwuwymiarowy aposterioryczny rozkład parametrów rozkładu Weibulla dla założonego rozkładu a priori parametru kształtu: a) równomiernego, b) normalnego, c) logarytmiczno-normalnego, d)nieinformacyjnego Jeffreys'a, e) funkcji wiarygodności



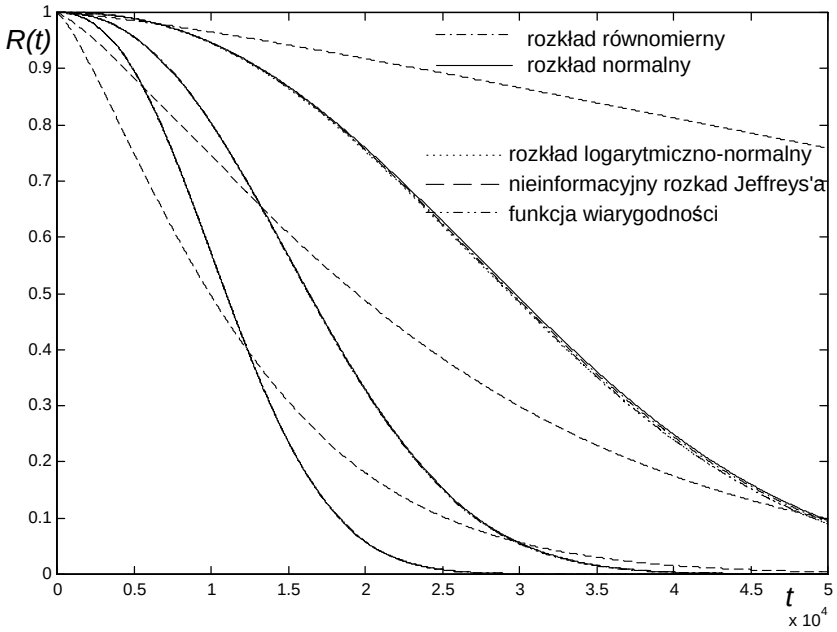
Rys. 7.7: Funkcje gęstości prawdopodobieństwa zaktualizowanego rozkładu a posteriori parametru kształtu dla różnych założonych rozkładów apriorycznych parametru kształtu

rozkładu a priori w postaci rozkładu Jeffreysa. Specyfika tego rozkładu powoduje nie tylko zmianę rozrzutu parametru ale również zmianę jego wartości (zjawisko to nie występuje gdy wartość parametru wyznaczona na podstawie próby jest zbliżona do zera).

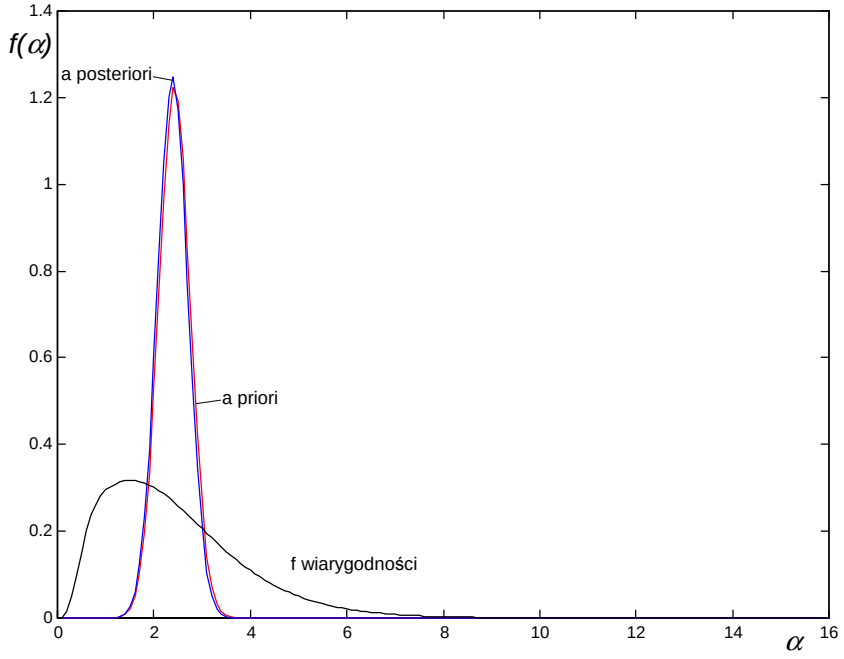
Mniejszy rozrzut parametru a posteriori uzyskujemy w przypadku założenia a priori rozkładu równomiernego, normalnego, logarytmiczno-normalnego. Wyniki uzyskane w przypadku użycia czterech pozostałych różnią się nieznacznie i prowadzą do takich samych wniosków w procesie podejmowania decyzji eksploatacyjnych (Rys.7.8). Spośród założonych postaci rozkładu a priori parametru wyróżnia się rozkład, którego podstawą jest funkcja wiarygodności. W tym przypadku nie jest wymagane wyznaczenie informacyjnej macierzy Fishera, natomiast otrzymujemy równie dobre wyniki jak dla rozkładów równomiernego, normalnego, logarytmiczno-normalnego.

Na rysunku 7.9 przedstawiono aprioryczną funkcję parametru kształtu o rozkładzie normalnym, funkcję wiarygodności i zaktualizowaną funkcję parametru kształtu a posteriori. Rysunek ten obrazuje „jakość" danych użytych w procesie uaktualnienia bayesowskiego. Rozrzut danych a posteriori (funkcja wiarygodności) jest dużo większy niż rozrzut danych a priori. W efekcie otrzymujemy nieznaczną zmianę funkcji gęstości prawdopodobieństwa zaktualizowanego parametru. Niska informacyjność danych a posteriori tłumaczy również nieznaczne przesunięci wartości modalnej zaktualizowanego parametru w przypadku założenia apriorycznie rozkładu Jeffreysa odnośnie parametru kształtu.

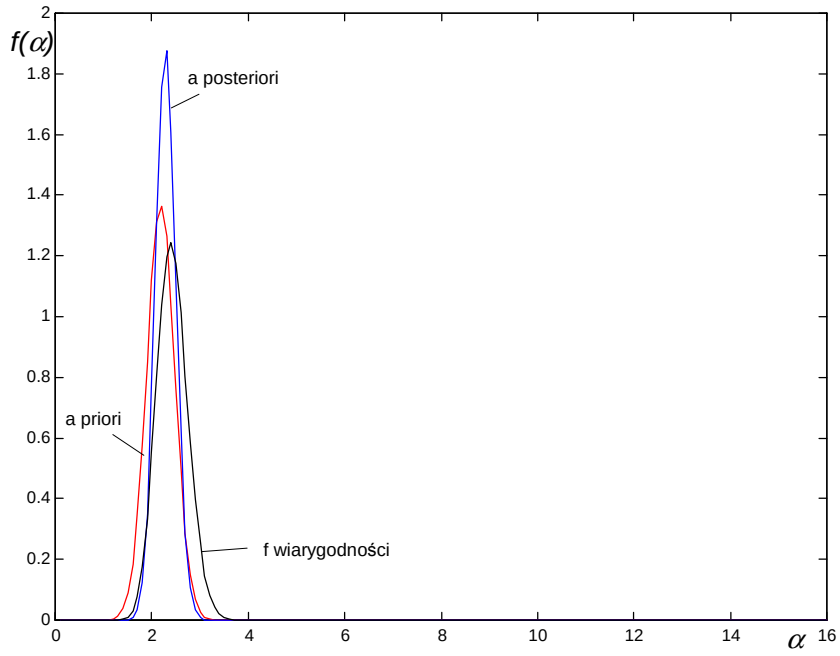
Poniżej przedstawiono wyniki uaktualnienia bayesowskiego dla różnych założonych apriorycznych postaci parametru kształtu i danych z eksperymentu o rozrzucie porównywalnym z apriorycznym rozrzutem parametru kształtu (Rys.7.10). Uzyskane wyniki potwierdzają, że założenie rozkładu Jeffreys'a odnośnie parametru kształtu daje największy rozrzut. Aprioryczna postać rozkładu ma tym większe znaczenie im wyniki przeprowadzonego eksperymentu są mniej informacyjne. Na podstawie powyższych przykładów widać, że w procesie uaktualnienia bayesowskiego kluczowym problemem jest zgromadzenie danych. W przypadku danych a posteriori o stosunkowo dużym rozrzucie najwygodniejsze wydaje się opisanie rozrzutu parametru a priori z wykorzystaniem funkcji wiarygodności, gdyż nie wymaga to postaci rozkładu i nie wprowadza przekłamań w postaci przesunięcia zaktualizowanego rozkładu.



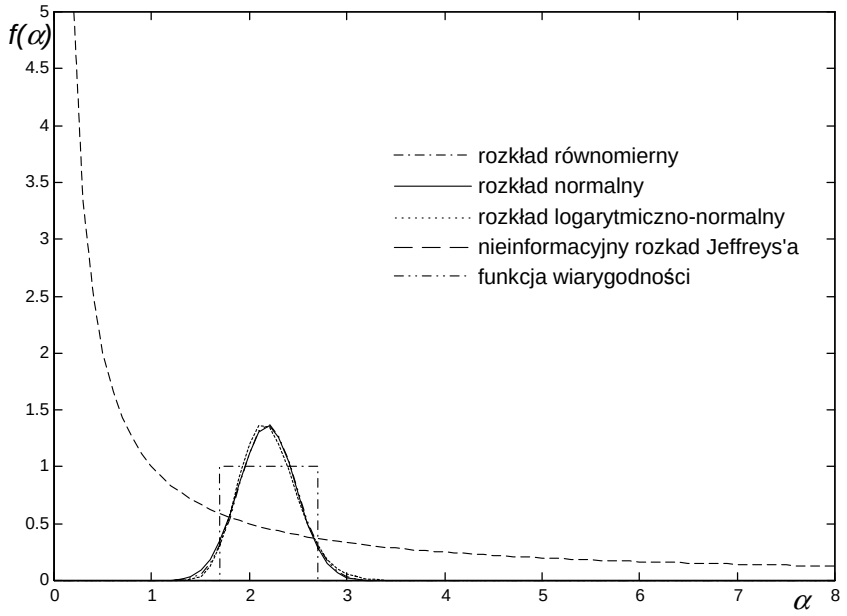
Rys. 7.8: Aposterioryczna funkcja niezawodności z zaznaczonym przedziałem ufności dla różnych apriorycznych funkcji gęstości prawdopodobieństwa parametru



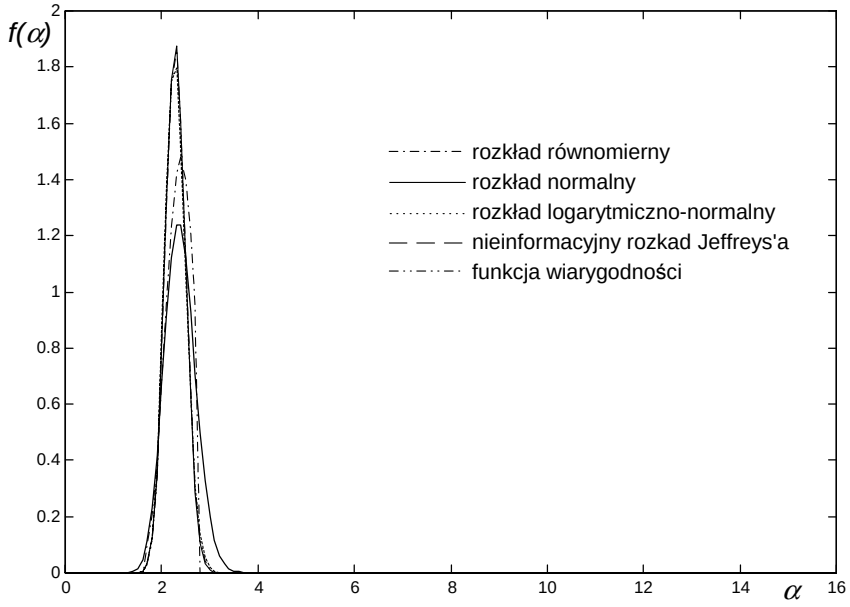
Rys. 7.9: Funkcja gęstości prawdopodobieństwa a priori, a posteriori parametru kształtu i funkcja wiarygodności



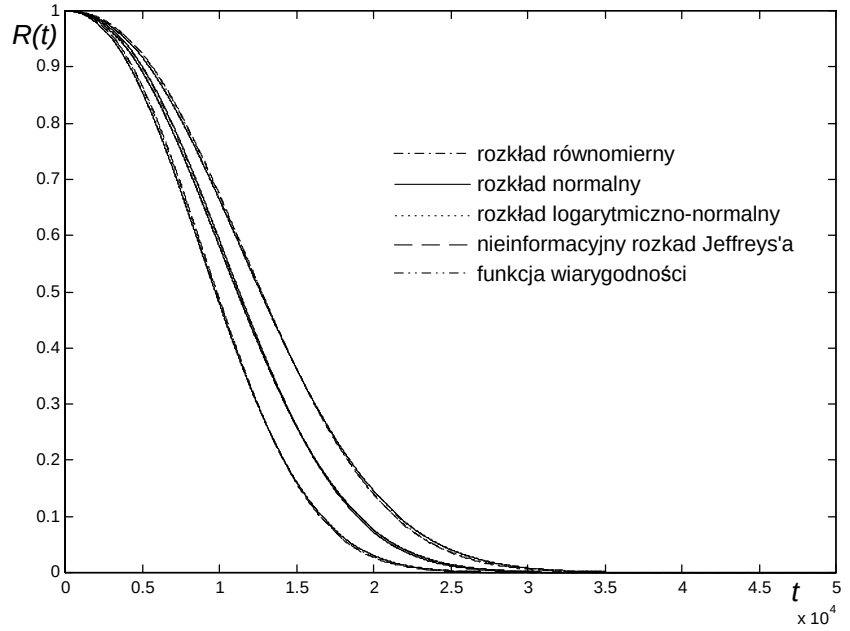
Rys. 7.10: Funkcja gęstości prawdopodobieństwa a priori, a posteriori parametru kształtu i funkcja wiarygodności



Rys. 7.11: Aprioryczna funkcja gęstości prawdopodobieństwa rozkładu parametru kształtu



Rys. 7.12: Funkcje gęstości prawdopodobieństwa zaktualizowanego rozkładu a posteriori parametru kształtu dla różnych założonych rozkładów apriorycznych parametru kształtu



Rys. 7.13: Aposterioryczna funkcja niezawodności z zaznaczonym przedziałem ufności dla różnych apriorycznych funkcji gęstości prawdopodobieństwa parametru

Bibliografia

[7.1] Grabski F., Jaźwiński J. *Metody Bayesowskie*. WKŁ, Warszawa, 2001.

Rozdział 8

Wykorzystanie informacji diagnostycznej w analizie ryzyka technicznego

Robert GUMIŃSKI, Stanisław RADKOWSKI

8.1. Wprowadzenie

Rozwój metod i środków diagnostyki technicznej spowodował, że coraz częściej wyniki postępowania diagnostycznego uwzględniane są w ocenie podatności eksploatacyjnej i stają się podstawą zapewnienia wyższej jakości oferowanych przez producenta wyrobów, zachowania odpowiedniej gotowości linii produkcyjnych a tym samym osiągnięcia lepszych wyników finansowych całego przedsiębiorstwa. Współczesne techniki i metody cyfrowej obróbki oraz analizy danych, umożliwiają zastosowanie procedur diagnostycznych zarówno do diagnozowania stanu prostych maszyn i urządzeń, jak również do nadzoru oraz diagnozowania realizacji procesów technologicznych i ewolucji stanów technicznych zachodzących w skomplikowanych systemach technicznych. Wymaga to z jednej strony uzupełnienia wiedzy o mechanizmach decydujących o przebiegu analizowanych zjawisk, z drugiej zaś, selekcji i opracowania metod oraz środków warunkujących wydobycie i rozpoznanie informacji diagnostycznej.

Jednym z istotnych etapów procesu diagnostycznego jest wnioskowanie diagnostyczne i związane z tym zagadnienie oceny przydatności informacji diagnostycznej w procesie podejmowania decyzji. Na przykład, przechodząc do eksploatacji według rzeczywistego stanu technicznego z wykorzystaniem rozbudowanych układów diagnostycznych, należy oprócz doboru i adaptacji metod diagnozowania, rozwiązać wiele dodatkowych zagadnień natury organizacyjnej i ekonomicznej. Zwróćmy uwagę, że rozstrzygającym kryterium odnośnie zastosowania układu diagnostycznego są efekty ekonomiczne.

8.2. Metody eksploatacji zorientowane na bezpieczeństwo

Współczesne propozycje rozwiązań techniczno-organizacyjnych [8.10] dodatkowo uwzględniają rozwój i aplikację technologii samoutrzymania przy zachowaniu wysokiej efektywności produkcji i możliwie niskich kosztach eksploatacji.

Stąd analiza ryzyka i zmniejszenie niepewności oszacowań niezawodności stały się krytycznymi metodami w procesie podejmowania decyzji strategicznych, których celem jest zapewnienie bezpieczeństwa technicznego i minimalizacja kosztów.

Zarówno w Europie jak i w Ameryce za najbardziej efektywne metody uznano RBI (Risk Based Inspection) – nadzór wsparty analizą ryzyka oraz RBM (Risk Based Maintenance) – eksploatacja zorientowana na bezpieczeństwo. W metodach RBI i RBM odwołujących się do identycznych pojęć i sposobów opisu systemu, podsystemów, podobnej klasyfikacji, funkcjonalnych uszkodzeń i rodzajów uszkodzeń jak w metodzie RCM (Reliability Center Maintenance - niezawodnościowo zorientowanej

eksploatacji) podejmowane są próby obliczenia ryzyka. Jest to istotnie różne podejście niż w metodzie RCM, w której celem jest określenie stopnia (klasy) krytyczności analizowanego obiektu lub elementu.

Taki sposób postępowania można przyjąć za satysfakcjonujący jedynie wówczas, gdy wartość strat jest mała i w analizie ryzyka wystarczy jedynie uwzględnić prawdopodobieństwo wystąpienia zdarzenia niepożądanego.

W każdym przypadku a szczególnie w przypadku aplikacji metod RBI i RBM, uwzględniając rozrzut ocen czasu do wystąpienia awarii, głównym celem metod predykcji wspartych analizą ryzyka jest zmniejszenie niepewności prognozy poziomu ryzyka. Jednym z istotnych sposobów rozwiązania tego problemu jest modelowanie oraz diagnozowanie przebiegu procesów degradacyjnych i zmęczeniowych, tym samym zmniejszenie wariancji ocen residualnego życia obiektu.

Realizacja tego celu wymaga oceny strukturalnej niezawodności systemu z uwzględnieniem detekcji i analizy procesów degradacji wszystkich składowych w uprzednim i aktualnym okresie użytkowania. Na tej podstawie możliwe jest zmniejszenie niepewności odnośnie oceny okresu czasu do wystąpienia awarii oraz prognozy wystąpienia i rozwoju innych typów uszkodzeń.
Takie ujęcie wymaga dostępu do odpowiedniej bazy danych o możliwych uszkodzeniach, składowych systemu oraz wiedzy zgromadzonej na podstawie doświadczeń zdobytych przez odpowiednio przygotowanych pracowników.

Ogólnie w omawianej metodzie wyróżnia się następujące etapy:

1. Dekomponowanie analizowanego systemu na podukłady i elementy, a następnie oszacowanie ich krytyczności w najbardziej niekorzystnych scenariuszach zdarzeń.
2. Określenie czasu i zakresu kolejnej inspekcji.
3. Oszacowanie poziomu ryzyka każdego podukładu i elementu.
4. Wyznaczenie priorytetów utrzymania elementów zgodnie z ustalonym rankingiem poziomu ryzyka technicznego.

Ogólnie, analiza ryzyka powinna uwzględniać każdy rodzaj uszkodzenia, którego wystąpienia można oczekiwać, odnośnie poszczególnych elementów i podzespołów oraz obejmować zarówno oszacowanie prawdopodobieństwa wystąpienia uszkodzenia jak również rozległości i wysokości strat (konsekwencji). Procedury estymacji prawdopodobieństwa wystąpienia zdarzenia niepożądanego powinny uwzględniać rzeczywisty stan rozwoju uszkodzenia, ważniejsze uszkodzenia, rezultaty inspekcji i możliwe przyszłe uszkodzenia.

Podobnie, oszacowania powinny uwzględniać zarówno aspekty bezpieczeństwa jak i zagadnienia strat ekonomicznych spowodowanych uszkodzeniami wtórnymi, w tym koszty napraw, straty spowodowane przerwą w produkcji i wypłatą rekompensat za utracone zdrowie lub życie.

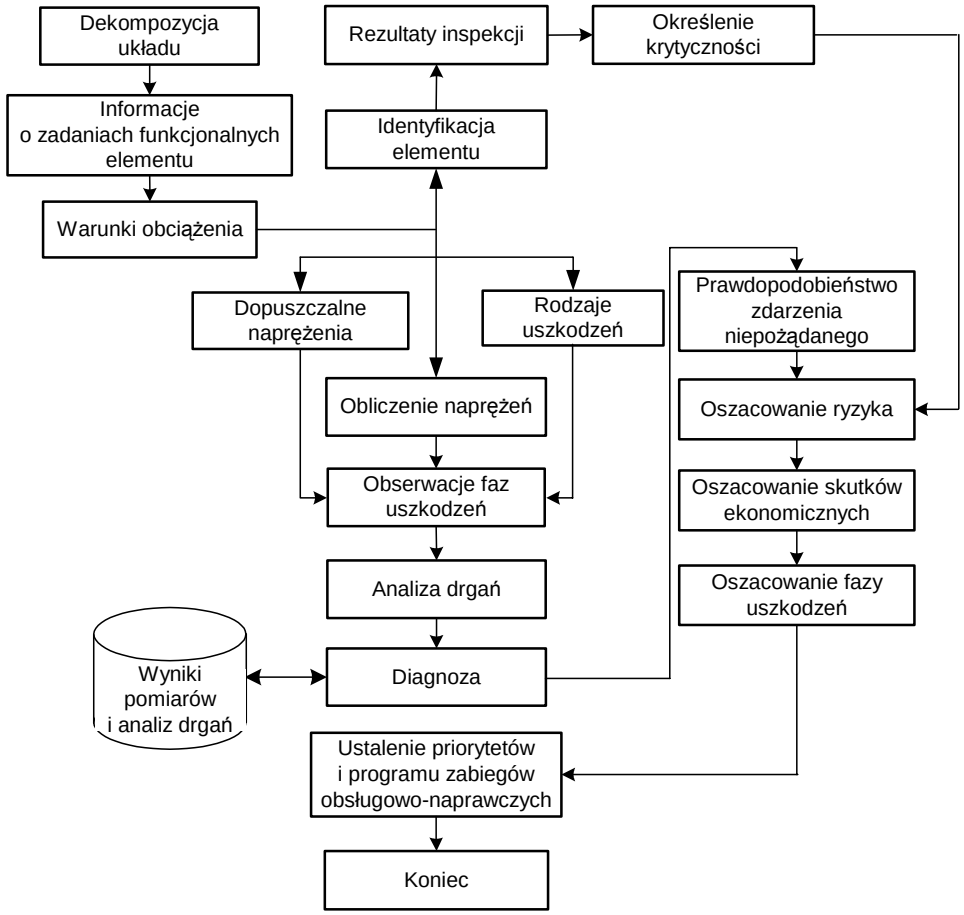
Otrzymane rezultaty szacowania ryzyka powinny być zestawione w postaci macierzy ryzyka, która w naturalny sposób pozwala określić kategorie scenariuszy i ustalić priorytety. Schemat przedstawiający możliwość zastosowania metody RBI wspartej diagnostyką wibroakustyczną zaprezentowano na rysunku 8.1.

Zauważmy że takie ujęcie wymaga opracowania miar umożliwiających prowadzenie analiz porównawczych. Najczęściej tworzone są odpowiednie miary użyteczności, uwzględniające koszty związane z każdą alternatywną decyzją, w tym z decyzją, która może spowodować awarię.

Jeśli uwzględnimy w naszym postępowaniu wszystkie etapy „życia maszyny", ocena użyteczności będzie stowarzyszona z występowaniem uszkodzeń oraz organizacją obsług, napraw i inspekcji diagnostycznych. Na przykład miara użyteczności może być wyrażona w postaci [8.7]:

$$E[C_R] = P_F C_F + P_E C_E + P_D C_D = E[C_F] + E[C_E] + E[C_D] \tag{8.1}$$

gdzie: $E[C_F]$, $E[C_E]$, $E[C_D]$ – wartości oczekiwane kosztów wystąpienia uszkodzenia, przeprowadzenia obsług i napraw oraz kosztów inspekcji diagnostycznej (monitoringu).



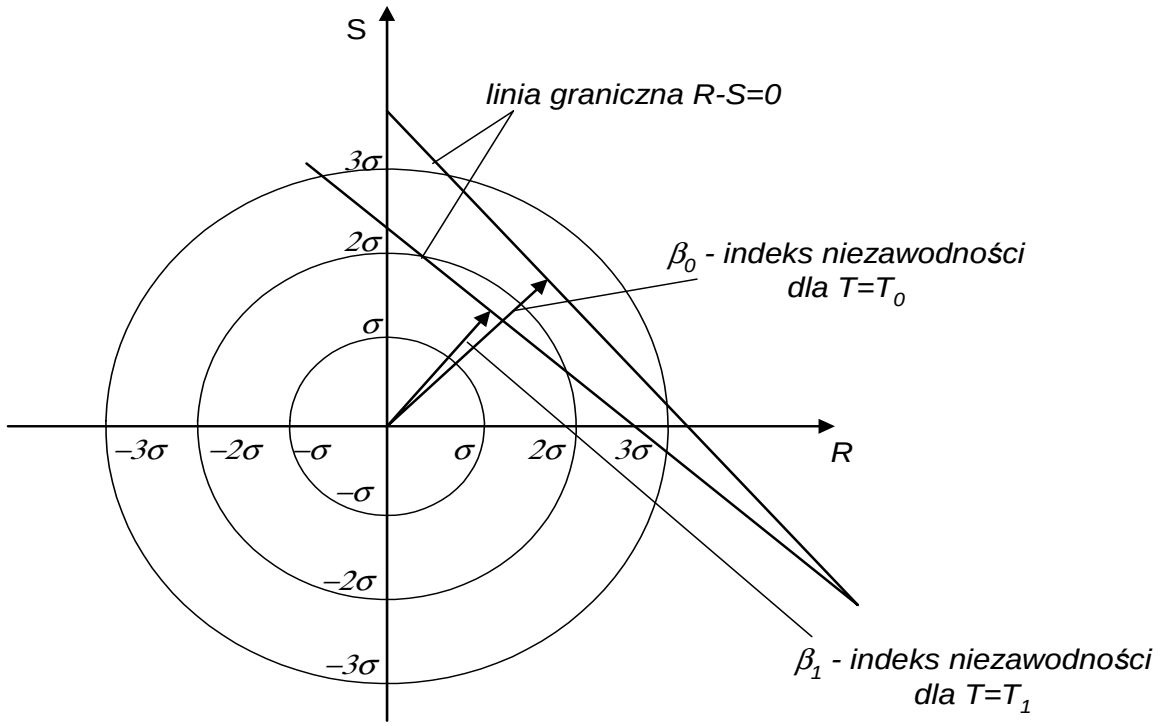
Rys. 8.1: Schemat procedury RBI wspartej diagnostyka wibroakustyczną [8.4]

Zauważmy, że przytoczona miara użyteczności może być włączona do funkcji użyteczności jako dodatkowy składnik. Zatem mając określoną funkcję użyteczności i prawdopodobieństwa poszczególnych stanów oraz koresponduj ące z nimi konsekwencje, możliwe jest określenie kosztów towarzyszących różnym alternatywnym akcjom. Odpowiednio w przypadku wykorzystania jedynie informacji apriorycznej odnośnie czasu T_0 i informacji o zużyciu eksploatacyjnym w czasie T_1 wartość oczekiwana funkcji przyjmuje postać:

$$E'[u] = \min \{P'(\theta_0/T_0) \cdot C_K + P'(\theta_1/T_0) \cdot (C_K + C_C) + \\ + P'(\theta_0/T_1) \cdot (C_K + C_E) + P'(\theta_1/T_1) \cdot (C_K + C_E + C_C)\} \tag{8.2}$$

gdzie:
P'(θ_0/T_0) – prawdopodobieństwo tego że obciążalność jest większa od obciążenia dla czasu $t = T_0$,
P'(θ_1/T_0) – prawdopodobieństwo tego że obciążenie jest większa od obciążalności dla czasu $t = T_0$,
P'(θ_0/T_1) – prawdopodobieństwo tego że obciążalność jest większa od obciążenia dla czasu $t = T_1$,
P'(θ_1/T_1) – prawdopodobieństwo tego że obciążenie jest większa od obciążalności dla czasu $t = T_1$,
C_K – koszty kontroli stanu,
C_C – konsekwencje hipotetycznych strat w przypadku wystąpienia awarii,
C_E – Koszty zabiegów eksploatacyjnych.

W przypadku możliwości uzyskania dodatkowej informacji np. w efekcie zastosowania procedur diagnostycznych (Rys. 8.2) przedstawiony model decyzyjny może być uaktualniony – możliwa jest analiza na podstawie modelu aposteriorycznego:



Rys. 8.2: Ilustracja wpływu zużycia eksploatacyjnego na wielkość indeksu niezawodności [8.9]

$$E"[u] = \min\Big\{P"(\theta_0/T_0, \hat{f}_u)\cdot C_K + P"(\theta_1/T_0, \hat{f}_u)\cdot (C_K + C_C) + \\ + P"(\theta_0/T_1, \hat{f}_u)\cdot (C_K + C_E) + P"(\theta_1/T_1, \hat{f}_u)\cdot (C_K + C_E + C_C)\Big\} \tag{8.3}$$

gdzie:
$P"(\theta_0/T_0, f_u)$ – prawdopodobieństwo a posteriori tego, że obciążalność jest większa od obciążenia dla czasu $t = T_0$,
$P"(\theta_1/T_0, f_u)$– prawdopodobieństwo a posteriori tego, że obciążenie jest większa od obciążalności dla czasu $t = T_0$,
$P"(\theta_0/T_1, f_u)$ – prawdopodobieństwo a posteriori tego, że obciążalność jest większa od obciążenia dla czasu $t = T_1$,
$P"(\theta_1/T_1, f_u)$ – prawdopodobieństwo a posteriori tego, że obciążenie jest większa od obciążalności dla czasu $t = T_1$.

Zauważmy, że bayesowskie uaktualnienie może dotyczyć różnych rodzajów informacji w tym, liczności obiektów w dobrym stanie technicznym, gotowości, charakterystyk materiałowych, imperfekcji geometrycznych i materiałowych, procesów degradacji i zmęczenia, zdolności przenoszenia obciążeń, statycznych i dynamicznych właściwości obiektu w różnych warunkach obciążeń i różnych warunkach środowiskowych. Uwzględniając w procedurach oceny stanu technicznego tego typu nową informację, mamy możliwość przekształcenia uproszczonych modeli w probabilistyczne modele aposterioryczne. Zadanie to zwykle jest sprowadzone do analizy obiektu obciążeń i wpływu środowiska, natomiast wybór zakresu, rodzaju i szczegółowości procedur diagnostycznych zwykle nie wchodzi w zakres analiz bayesowskich.

Tymczasem decyzja czy wystarczy jedynie uaktualnienie parametrów zmiennych losowych dotyczących obciążeń i obciążalności, czy należy też dodatkowo podjąć zagadnienie uaktualnienia prawdopodobieństwa zdarzeń (wystąpienia uszkodzenia) ma duży wpływ nie tylko na efektywność usuwania niepewności, ale również na wysokość ponoszonych kosztów.

Dla wyjaśnienia tych problemów prowadzi się często tzw. pre-posterioryczną analizę, której celem jest określenie potrzeby i zakresu eksperymentu diagnostycznego, z uwzględnieniem towarzyszących temu kosztów. Dodatkowo, jeśli jest możliwe przeprowadzenie kilku eksperymentów różnego typu, konieczne jest utworzenie kolejnej miary użyteczności, która będzie mogła być wykorzystana w procesie podejmowania decyzji.

Rozważmy sytuację gdy eksperyment diagnostyczny jest zaplanowany, a wyniki tego eksperymentu są ciągle nieznane, wówczas zależność opisująca miarę użyteczności przyjmuje postać:

$$E[u] = \sum_{i=1}^{n} P'(z_i) E"[u|z_i] = \sum_{i=1}^{n} P'(z_i) \min_{i=1,m} \{E"[u(T_j)|z_i]\} \tag{8.4}$$

gdzie:

$$P'(z_i) = P(z_i|\theta_0) \cdot P(\theta_0) + P(z_i|\theta_1) \cdot P(\theta_1) \tag{8.5}$$

przy czym:
i – liczba możliwych do przeprowadzenia eksperymentów,
j – liczba alternatywnych decyzji o różnych konsekwencjach.
Tak skonstruowana miara umożliwia wybór sekwencji lub rodzaju eksperymentu zgodnie z kryterium minimalizacji kosztów.

8.3. Wykorzystanie metody Bayesa

Dobrą ilustracją omawianego sposobu wykorzystania wzoru Bayesa w ocenie zmian parametrów rozkładu na podstawie informacji diagnostycznej jest praca Cruse'a [8.3], w której twierdzenie Bayesa wykorzystano do ustalenia wartości parametrów opisujących przyrost zmęczeniowego uszkodzenia z uwzględnieniem obserwacji rozwoju pęknięcia.

Istota tego podejścia polega na uaktualnieniu estymowanych parametrów probabilistycznego modelu dla osiągnięcia większej zgodności rezultatów modelowania i obserwacji.

Zgodnie z przedstawionymi wyżej założeniami przyjmuje się, że nieznane lub niepewne parametry rozkładu są zmiennymi losowymi. Niepewność estymacji parametrów może być kojarzona ze zmiennością zmiennych losowych za pomocą twierdzenia Bayesa.

Następnie zakładając, że będziemy estymować parametry apriorycznego rozkładu parametru a, funkcji gęstości prawdopodobieństwa $f(a)$ oraz, że D jest zbiorem obserwacji pozwalającym zmniejszyć niepewność aprioryczną pod warunkiem uwzględnienia wyników obserwacji, to estymację parametrów rozkładu aposteriorycznego będziemy mogli, uwzględniając własności całki Stieltjesa [8.8], prowadzić za pomocą formuły:

$$f(a|D) = \frac{f(D|a)f(a)}{f(D)} \tag{8.6}$$

gdzie:

$$f(D) = \int_{-\infty}^{\infty} f(D|a)f(a)da. \tag{8.7}$$

Dodatkowo można przyjąć, że mianownik opisany całką funkcji gęstości prawdopodobieństwa aposteriorycznego jest stały oraz, że $f(D/a)$ jest prawdopodobieństwem obserwacji, które może być wyrażone przez funkcję wiarygodności. Wówczas równanie (8.6) można zapisać w postaci:

$$f(a|D) = K_B \cdot L[D|a] \cdot f(a) \tag{8.8}$$

gdzie:
K_B – stała normująca,
$L[D/a]$ – funkcja wiarygodności.

Aby określić prawdopodobieństwo uszkodzenia w analizowanym przedziale czasu, informacja zawarta w obserwacjach powinna uwzględniać zarówno występowanie uszkodzenia, jak i jego brak. Dla ekspotencjalnej postaci funkcji opisującej rozkład, funkcję wiarygodności zapiszemy w postaci:

$$L\left[D|a\right] = \prod_{i=1}^{n} p(\theta_f|a) \times \prod_{j=1}^{m} \left[1 - P(\theta_f|a)\right] \tag{8.9}$$

gdzie:
n – oznacz zbiór wykrytych uszkodzeń,
m – oznacza zbiór zdarzeń określających brak uszkodzenia.
Zauważmy, że wzór Bayesa (8.6) można uprościć uwzględniając jedynie proporcjonalność rozkładu a posteriori i a priori:

$$f(a|D) = \frac{f(D|a)f(a)}{f(D)} \propto f(D|a)f(a) \tag{8.10}$$

Podobnie aprioryczna gęstość prawdopodobieństwa jest proporcjonalna do pierwiastka kwadratowego wyznacznika macierzy informacji Fishera [8.6]:

$$f(a) \propto (\det \mathrm{I}(a))^{1/2} \tag{8.11}$$

gdzie:
$\mathrm{I}(a) = -E\left[\frac{\partial^2 \ln f(D|a)}{\partial a^2}\right]$ – jest obliczona jako macierz uśrednionych drugich pochodnych z logarytmu funkcji wiarygodności określonej na podstawie wyników eksperymentu.
Stąd ostatecznie wzór (8.6) zapisujemy w postaci:

$$f(a|D) \propto L(D|a)(\det \mathrm{I}(a))^{1/2} \tag{8.12}$$

Przedstawiony w opracowaniu sposób wykorzystania metody analizy ryzyka wspartej diagnostyką wibroakustyczną w podejmowaniu decyzji eksploatacyjnych nawiązuje z jednej strony do definicji ryzyka i związanego z tym oszacowania prawdopodobieństwa wystąpienia zdarzenia niepożądanego oraz estymacji rozległości i wartości strat jakie temu zdarzeniu mogą towarzyszyć. Z drugiej zaś, do możliwości wykorzystania rezultatów eksperymentu diagnostycznego w zadaniu zmniejszania niepewności odnośnie estymacji parametrów aposteriorycznego rozkładu intensywności uszkodzeń. Wykorzystanie modeli bayesowskich umożliwia bezpośrednią aplikację wyników obserwacji diagnostycznej w bayesowskiej estymacji aposteriorycznego rozkładu oraz podjęcie problemu doboru aprioryczne-go rozkładu. Jak wykazano w przykładzie, takie zastosowanie informacji diagnostycznej umożliwia rozwiązanie zagadnienia wyznaczania warunkowego rozkładu prawdopodobieństwa parametrów intensywności uszkodzeń na podstawie rezultatów uzyskanych w eksperymencie diagnostycznym.

8.4. Przykład wykorzystania metody prawdopodobieństwa subiektywnego w procesie podejmowania decyzji

Zanim przedstawimy możliwość wykorzystania prawdopodobieństwa subiektywnego w procesie podejmowania decyzji omówimy przykład wykorzystania informacji diagnostycznej w zadaniu estymacji parametrów rozkładu prawdopodobieństwa z wykorzystaniem Modeli Proporcjonalnych. Przykład ten przytaczamy za [8.4], a uzyskane wyniki traktujemy jako rezultaty odniesione do omawianych tu zagadnień. Załóżmy, że przyjęta hipoteza o rozkładzie Weibulla została zweryfikowana, a naszym zadaniem jest wykorzystanie informacji o zmierzonych wartościach prędkości drgań do aktualizacji wartości parametrów kształtu i skali analizowanego rozkładu.

Zauważmy, że w tak sformułowanym zadaniu zmierzone wartości traktowane są jako wielkości zdeterminowane. W kolejnym przykładzie z wykorzystaniem sieci bayesowskich przyjmiemy, że otrzymane wyniki pomiarów są zmiennymi losowymi co będzie miało istotny wpływ na końcowe rezultaty.

Norma [8.1] do oceny drgań maszyny wykorzystuje jako kryterium intensywność punktową drgań szerokopasmowych lub zmiany intensywności punktowej. W przypadku pierwszego kryterium norma definiuje strefy klasyfikacyjne od A do D. Jako miarę intensywności drgań w szerokim zakresie częstotliwości przyjęto prędkość drgań. W załączniku B omawianej normy zamieszczono granice poszczególnych stref klasyfikacyjnych dla poszczególnych typów maszyn (Tab. 8.1).

Strefy klasyfikacyjne zostały zdefiniowane dla czterech klas określających wielkość maszyny i fundamentowanie. Kolejne strefy oznaczają:

Strefa A – w tej strefie mieszczą się zwykle drgania maszyn bezpośrednio po oddaniu do eksploatacji .

Strefa B – drgania określone w tej strefie są generowane na maszynach, które dopuszcza się do długotrwałego użytkowania bez ograniczeń eksploatacyjnych.

Tab. 8.1: Wartości graniczne stref klasyfikacyjnych intensywności drgań

<table>
<tr><th>Średniokwadratowa wartość prędkości drgań [mm/s]</th><th>Klasa I</th><th>Klasa II</th><th>Klasa III</th><th>Klasa IV</th></tr>
<tr><td>0,28</td><td rowspan="3">A</td><td rowspan="4">A</td><td rowspan="5">A</td><td rowspan="6">A</td></tr>
<tr><td>0,45</td></tr>
<tr><td>0,71</td></tr>
<tr><td>1,12</td><td rowspan="2">B</td></tr>
<tr><td>1,8</td><td rowspan="2">B</td></tr>
<tr><td>2,8</td><td rowspan="2">C</td><td rowspan="2">B</td></tr>
<tr><td>4,5</td><td rowspan="2">C</td><td rowspan="2">B</td></tr>
<tr><td>7,1</td><td rowspan="4">D</td><td rowspan="2">C</td></tr>
<tr><td>11,2</td><td rowspan="3">D</td><td rowspan="2">C</td></tr>
<tr><td>18</td><td rowspan="2">D</td></tr>
<tr><td>28</td><td rowspan="2">D</td></tr>
<tr><td>45</td></tr>
</table>

Strefa C – maszyny, których drgania mieszczą się w tej strefie, z reguły uważa się za nie nadające się do długotrwałej pracy ciągłej. Zwykle maszyna może być eksploatowana w tym stanie przez ograniczony czas, do chwili gdy możliwe jest podjęcie kroków zaradczych.

Strefa D – zwykle przyjmuje się, że intensywność drgań o wartościach mierzonych w tej strefie, wystarcza aby spowodować uszkodzenie maszyny.

Prędkość drgań przy ustalonej częstotliwości przekłada się na przyspieszenia drgań, a w rezultacie na dynamiczne obciążenie łożysk, na których są osadzone elementy wirujące maszyny. Natomiast trwałość łożysk wiąże się z wartością obciążenia dynamicznego. Wynika z tego, że intensywność uszkodzeń łożyska jest zależna od prędkości drgań, którą należy uznać za zmienną systemową.

Jak przedstawiono w pracy ([8.5]) zastosowanie modeli proporcjonalnych stwarza możliwość badania wpływu zmiennych systemowych (w tym przypadku drgań zmierzonych podczas diagnostyki kontrolnej) na niezawodność systemu.

Założenia modelu proporcjonalnego:

- Stosunek intensywności uszkodzeń dla dwóch różnych wartości zmiennej systemowej nie zależy od czasu;
- Intensywności uszkodzeń dla różnych wartości zmiennej systemowej są opisane tym samym rozkładem.

Na podstawie powyższych założeń możemy napisać:

$$\lambda\left(\mathrm{t},\mathrm{z},\beta\right)=\lambda_0\left(\mathrm{t}\right)\ \mathrm{r}\left(\mathrm{z},\beta\right) \tag{8.13}$$

gdzie:

t – czas,

z – zmienna systemowa,

β – nieznany parametr uwzględniający wpływ zmiennej systemowej,

$\lambda_0(t)$ – intensywność uszkodzeń dla wartości zmiennej systemowej przyjętej jako poziom odniesienia.

Przyjmując za modelem Coxa [8.2]:

$$r\left(z,\beta\right)=e^{z\beta} \tag{8.14}$$

otrzymujemy:

$$\lambda\left(\mathrm{t},\mathrm{z},\beta\right)=\lambda_0\left(\mathrm{t}\right)\ \mathrm{e}^{z\beta} \tag{8.15}$$

Model, który można zapisać za pomocą równania (8.13), nazywa się modelem proporcjonalnym, można go uogólnić na dowolną liczbę zmiennych systemowych:

$$\lambda\left(t,z_1,...z_n,\beta_1,...,\beta_n\right)=\lambda_0(t)\ \mathrm{r}\left(z_1,...z_n,\beta_1,...,\beta_n\right) \tag{8.16}$$

po podstawieniu modelu Coxa otrzymujemy:

$$\lambda\left(t,z_1,...z_n,\beta_1,...,\beta_n\right)=\lambda_0\left(\mathrm{t}\right)\ e^{z_1\beta_1+...+z_n\beta_n} \tag{8.17}$$

Wykładnicza postać funkcji *r(z,β)* gwarantuje, że funkcja intensywności przyjmuje wartości nieujemne bez względu na wartości współczynników.

Najczęściej wykorzystywanym rozkładem w analizie niezawodności jest rozkład wykładniczy dla którego intensywność uszkodzeń jest stała, zatem również stosunek intensywności dla dwóch grup danych o określonych uszkodzeniach będzie stały, co spełnia założenia modelu proporcjonalnego. Przyjmując założenie o rozkładzie wykładniczym wyklucza się możliwość uwzględnienia wpływu czasu. Z tego względu należy rozważyć możliwość użycia rozkładu Weibulla. Przeanalizujmy zatem, jakie warunki muszą spełniać parametry tego rozkładu żeby były spełnione założenia modelu proporcjonalnego. Intensywność uszkodzeń dla rozkładu Weibulla ma postać:

$$\lambda=\frac{\alpha}{\eta^{\alpha}}t^{\alpha-1} \tag{8.18}$$

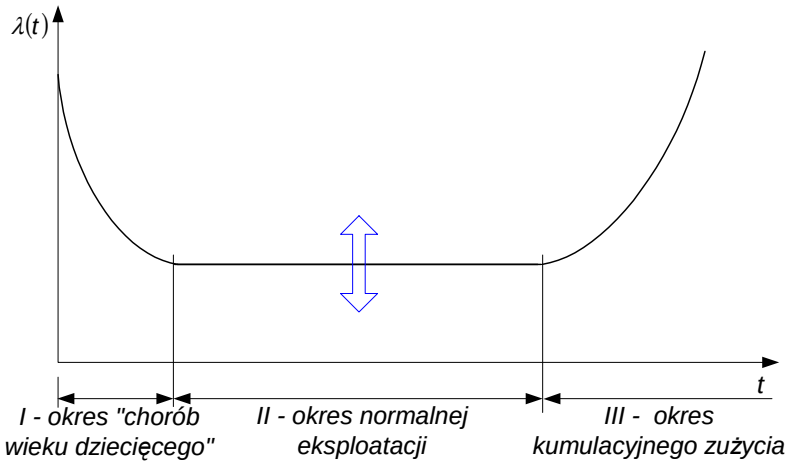
natomiast stosunek intensywności:

$$\frac{\lambda_1}{\lambda_2}=\frac{\frac{\alpha_1}{\eta_1^{\alpha_1}}t^{\alpha_1-1}}{\frac{\alpha_2}{\eta_2^{\alpha_2}}t^{\alpha_2-1}}=\frac{\alpha_1}{\alpha_2}\cdot\frac{\eta_2^{\alpha_2}}{\eta_1^{\alpha_1}}\cdot\frac{t^{\alpha_1-1}}{t^{\alpha_2-1}} \tag{8.19}$$

Z powyższej zależności wynika, że dla rozkładu Weibulla będą spełnione założenia modelu proporcjonalnego tylko wtedy gdy współczynnik kształtu pozostanie stały dla obu grup danych.

Skupmy się teraz na pomiarach wykonanych tuż po oddaniu maszyny do eksploatacji. Otrzymane wyniki dla poszczególnych maszyn, przy założeniu takich samych warunków pracy (obciążenie, prędkość obrotowa, itp.) w głównej mierze będą zależały od jakości wykonania oraz błędów montażowych. Jeśli drgania maszyny będą się zawierały w strefie A oznacza to, że prędkość drgań może się zawierać od 0,28 mm/s do 0,71 mm/s, co automatycznie przekłada się na prawdopodobieństwo wystąpienia uszkodzeń łożysk, a więc i na funkcję intensywności uszkodzeń.

Krzywa intensywności uszkodzeń w trakcie eksploatacji została przedstawiona na rysunku 8.3. Krzywa ta jest podzielona na trzy części:



Rys. 8.3: Funkcja intensywności uszkodzeń w czasie eksploatacji [8.9]

I. okres chorób wieku dziecięcego – przedział czasu, w którym ujawniają się wady procesu wytwarzania i montażu. Okres ten odpowiada dużej, ale malejącej intensywności uszkodzeń. Aby obniżyć liczbę awarii w tym czasie producenci starają się coraz dokładniej wykonywać współpracujące elementy i jeszcze przed oddaniem do eksploatacji maszyna jest uruchamiana na pewien czas w celu dopasowania poszczególnych elementów.

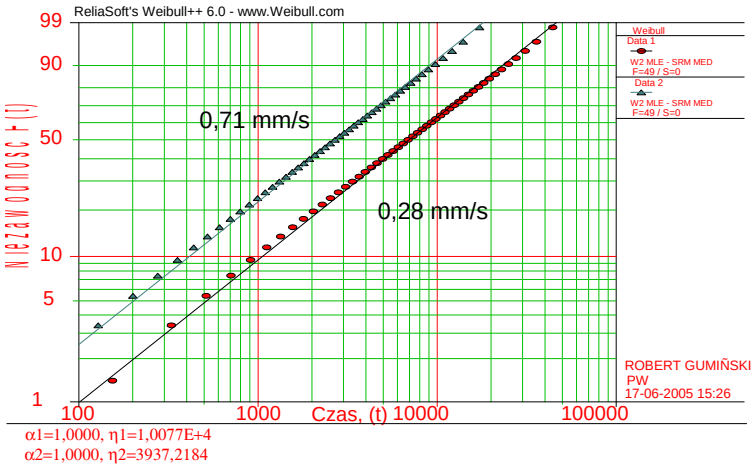
II. okres normalnej eksploatacji, w którym występowanie uszkodzeń wynika z losowego charakteru obciążenia i obciążalności, które umożliwiają modelowanie stałej – niezależnej od czasu eksploatacji – intensywności uszkodzeń. Gdy rozpatrujemy dane dotyczące uszkodzeń łożysk, jak było już wcześniej powiedziane obciążenia mogą się wahać w pewnych granicach co wynika z przynależności maszyny do pewnej strefy klasyfikacyjnej zgodnie z normą [8.1]. Tak więc położenie i kształt krzywej intensywności uszkodzeń będzie zależeć właśnie od tych sił, które jak wcześniej wykazano zależą od prędkości drgań mierzonych na obudowach łożysk.

III. okres kumulacyjnego zużycia, w którym występujące procesy degradacyjne objawiają się rosnącą intensywnością uszkodzeń.

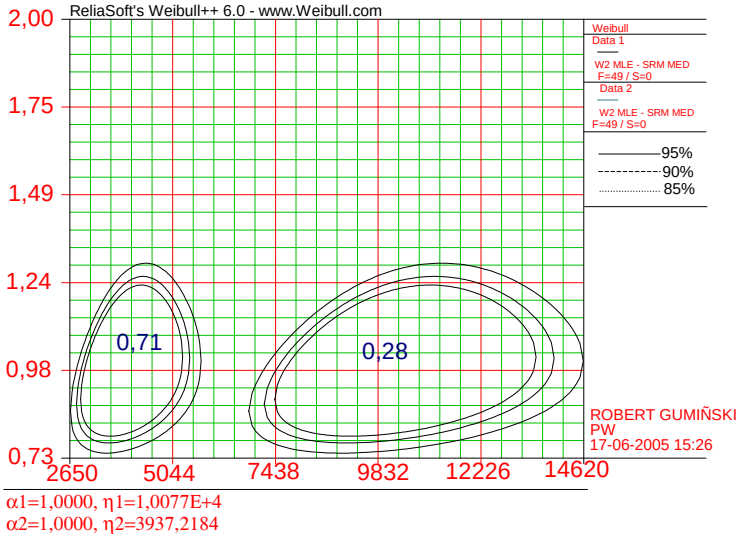
Empiryczne funkcje intensywności można opisać funkcjami teoretycznymi co ułatwia dalsze obliczenia.

Funkcja intensywności uszkodzeń w okresie normalnej eksploatacji spełnia założenia modeli proporcjonalnych ponieważ w tym czasie nie występują procesy degradacyjne, które mogłyby wywołać zmianę charakteru uszkadzania elementu. Dla rozpatrywanego przykładu w siatce probabilistycznej rozkładu Weibulla linie trendu dla danych o uszkodzeniach przy prędkościach drgań równych 0,28 mm/s i 0,71 mm/s będą równoległe (Rys.7.7), co jest spowodowane tym, że współczynniki kształtu rozkładu Weibulla w obu przypadkach są tej samej wartości (Rys.8.5). Na rysunku 8.6 przedstawiono graficzne sprawdzenie założeń Modeli Proporcjonalnych tzn. stosunek intensywności uszkodzeń nie zmienia się w czasie.

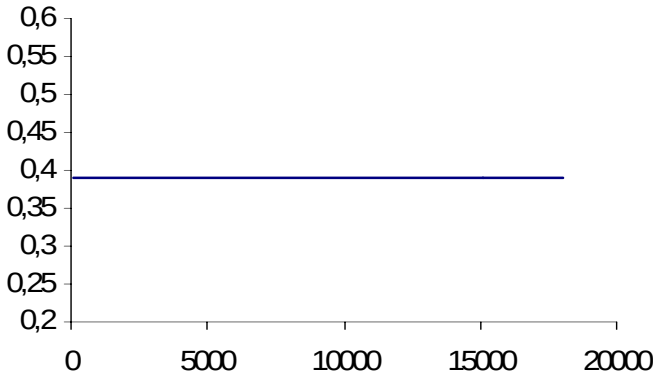
Jak podaje norma, wartości liczbowe przypisane granicom stref nie mają charakteru kryterium obowiązującego podczas prób odbiorczych. Zmierzone prędkości drgań mogą wykraczać poza strefę A. Powoduje to jeszcze większą rozbieżność wyznaczanych funkcji intensywności uszkodzeń. Wychodząc temu naprzeciw rozważmy przykład, w którym mierzone wartości są zmiennymi losowymi.



Rys. 8.4: Przedstawienie danych w siatce probabilistycznej rozkładu Weibulla dla różnych prędkości drgań



Rys. 8.5: Pola ufności parametrów rozkładu Weibulla dla różnych prędkości drgań



Rys. 8.6: Sprawdzenie warunku stosowalności modelu proporcjonalnego

8.5. Przykład wykorzystania sieci bayesowskich

Korzystamy z wartości granicznych stref klasyfikacyjnych intensywności drgań wg [8.1]. Rozważamy wartości graniczne strefy A dla I klasy urządzeń (V1 - 0.28mm/s – granica dolna, V2 - 0.71mm/s – granica górna). Załóżmy prawdopodobieństwa wystąpienia obu wartości: P(V1)=70%, P(V2)=30%.

Informacje te zostaną użyte w trakcie ustalania strategii eksploatacyjnej. Wystąpienie konkretnej wartości średniokwadratowej prędkości drgań przekłada się na prawdopodobieństwo wystąpienia uszkodzenia rozważanego obiektu lub systemu, więc ma wpływ na wybór konkretnej strategii eksploatacji, zapewnienie zapasów magazynowych, przygotowanie załogi itp.

Załóżmy, że przyjęcie nieodpowiedniej średniokwadratowej wartości prędkości drgań (ŚWPD) wiąże się z dodatkowymi kosztami eksploatacyjnymi.

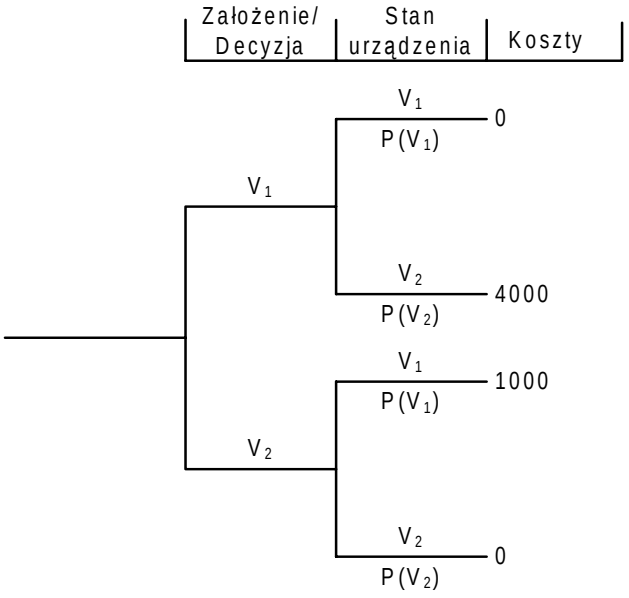
Jeżeli założono ŚWPD = V1 i w trakcie eksploatacji założenie potwierdzi się, koszty wynikające z podjęcia decyzji są zerowe, natomiast jeśli okaże się, że ŚWPD = V2, koszty wynoszą 4000 (możliwe wystąpienie awarii). Z drugiej strony jeśli podjęto decyzję na podstawie założenia ŚWPD = V2 i założenie potwierdzi się, koszty wynoszą zero, natomiast w przeciwnym razie (ŚWPD = V1), koszty wynoszą 1000 (są to koszty zbędnych napraw i obsługi). Aby w sytuacji niepewnych danych podjąć decyzję budujemy funkcję użyteczności, czyli wyznaczamy prawdopodobną wielkość strat dla obu decyzji i wyznaczamy minimum:

$$\mathrm{K} = \min\{\mathrm{P}(\mathrm{V}_1)\cdot 0 + \mathrm{P}(\mathrm{V}_2)\cdot 4000,\ \mathrm{P}(\mathrm{V}_1)\cdot 1000 + \mathrm{P}(\mathrm{V}_2)\cdot 0\ \} \tag{8.20}$$

stąd:

$$\mathrm{K} = \min\{0.7\cdot 0 + 0.3\cdot 4000,\ 0.7\cdot 1000 + 0.3\cdot 0\ \} = \min\{1200,\ 700\} =\ 700 \tag{8.21}$$

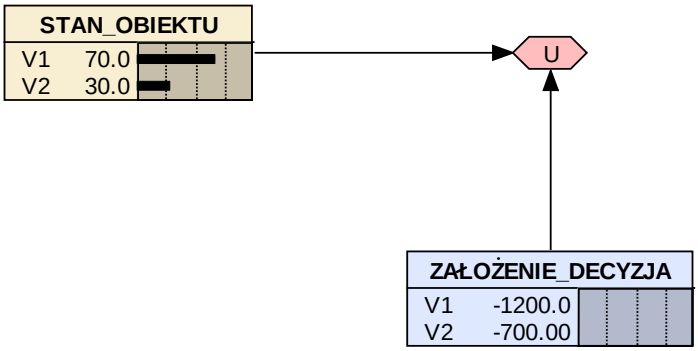
Poniżej przedstawiono rozważane zagadnienie w postaci drzewa zdarzeń (Rys.8.7).



Rys. 8.7: Drzewo zdarzeń

W procesie podejmowania decyzji eksploatacyjnych przydatne są sieci Bayesa. Poniżej przedstawiono sieć Bayesa wykorzystaną do rozwiązania omawianego zadania.

Chcąc zwiększyć pewność otrzymanych wyników można dokonać badań dla ustalenia rzeczywistej wartości ŚWPD w nadzorowanym obiekcie. Pomiary takie są obciążone niepewnością i kosztami. Przed podjęciem decyzji o wykonaniu pomiarów należy dokonać oceny ich ekonomicznej efektywności. Załóżmy, że rzeczywista wartość ŚWPD wynosi 0.28mm/s, natomiast uzyskane wyniki pomiarów



Rys. 8.8: Sieć Bayesa

można opisać rozkładem Weibulla (α=1.15; β=0.08, γ=0.28). W przypadku górnej granicy rzeczywista wartość ŚWPD wynosi 0.71mm/s i uzyskane wyniki pomiarów można opisać rozkładem Weibulla (α=12; β=0.58).

Na podstawie powyższych założeń wyznaczono prawdopodobieństwa warunkowe obrazujące niepewności użytej metody pomiarowej (Tab. 8.2).

Tab. 8.2: Prawdopodobieństwa warunkowe obrazujące niepewności metody pomiarowej

Stan faktyczny Wynik pomiarów	V1=0.28mm/s	V2=0.71mm/s
P1=0.28mm/s	0.8585	0.0226
P2=0.45mm/s	0.1285	0.5081
P3=0.71mm/s	0.0130	0.4693

Zatem dla tak określonych danych przyczynowych zależność opisująca prawdopodobieństwa warunkowe wystąpienia wartości ŚWPD pod warunkiem wystąpienia różnych wyników pomiaru P(Vj/Pi) przyjmuje postać:

$$\mathrm{P(V_j/P_i)} = \frac{\mathrm{P(P_i/V_j)P(V_j)}}{\mathrm{P(P_i)}} \tag{8.22}$$

Zauważmy, że wykorzystanie wzoru (8.22) jest związane z wyznaczeniem prawdopodobieństwa całkowitego *P(Pi)*:

$$P(P_1) = P(P_1/V_1)P(V_1) + P(P_1/V_2)P(V_2), P(P_1) = 0.8585 \cdot 0.7 + 0.0226 \cdot 0.3 = 0.6077 \tag{8.23}$$

$$P(P_2) = P(P_2/V_1)P(V_1) + P(P_2/V_2)P(V_2), P(P_2) = 0.1285 \cdot 0.7 + 0.5081 \cdot 0.3 = 0.2424 \tag{8.24}$$

$$P(P_3) = P(P_3/V_1)P(V_1) + P(P_3/V_2)P(V_2), P(P_3) = 0.0130 \cdot 0.7 + 0.4693 \cdot 0.3 = 0.1499 \tag{8.25}$$

Następnie obliczamy prawdopodobieństwo warunkowe przydatne diagnostycznie, czyli hipotetyczne prawdopodobieństwa wystąpienia konkretnych prędkości pod warunkiem wystąpienia poszczególnych wyników pomiarów:

$$P"(V_1/P_1) = \frac{P(P_1/V_1)P(V_1)}{P(P_1)}, P"(V_1/P_1) = \frac{0.8585 \cdot 0.7}{0.6077} = 0.9889 \tag{8.26}$$

$$P"(V_2/P_1) = \frac{P(P_1/V_2)P(V_2)}{P(P_1)}, P"(V_2/P_1) = \frac{0.0226 \cdot 0.3}{0.6077} = 0.0112 \tag{8.27}$$

$$P"(V_1/P_2) = \frac{P(P_2/V_1)P(V_1)}{P(P_2)}, P"(V_1/P_2) = \frac{0.1285 \cdot 0.7}{0.2424} = 0.3711 \tag{8.28}$$

$$P"(V_2/P_2) = \frac{P(P_2/V_2)P(V_2)}{P(P_2)}, P"(V_2/P_2) = \frac{0.5081 \cdot 0.3}{0.2424} = 0.6288 \tag{8.29}$$

$$P"(V_1/P_3) = \frac{P(P_3/V_1)P(V_1)}{P(P_3)}, P"(V_1/P_3) = \frac{0.130 \cdot 0.7}{0.1499} = 0.0607 \tag{8.30}$$

$$P"(V_2/P_3) = \frac{P(P_3/V_2)P(V_2)}{P(P_3)}, P"(V_2/P_3) = \frac{0.4693 \cdot 0.3}{0.1499} = 0.9392, \tag{8.31}$$

Otrzymane rezultaty wykorzystujemy do wyznaczenia funkcji użyteczności. Dla obu decyzji wyznaczamy prawdopodobną wielkość strat pod warunkiem wystąpienia konkretnych wyników pomiarów. Jako kryterium uwzględniamy wartość minimalną biorąc pod uwagę minimalne koszty:

$$K(V_i/P_1) = \min\{P(V_1/P_1) \cdot 0 + P(V_2/P_1) \cdot 4000, \;\; P(V_1/P_1) \cdot 1000 + P(V_2/P_1) \cdot 0\} = \\ = \min\{44.8, \;\; 988.9\} = 44.8 \tag{8.32}$$

$$K(V_i/P_2) = \min\{P(V_1/P_2) \cdot 0 + P(V_2/P_2) \cdot 4000, \;\; P(V_1/P_2) \cdot 1000 + P(V_2/P_2) \cdot 0\} = \\ = \min\{2515.2, \;\; 371.1\} = 371.1 \tag{8.33}$$

$$K(V_i/P_3) = \min\{P(V_1/P_3) \cdot 0 + P(V_2/P_3) \cdot 4000, \;\; P(V_1/P_3) \cdot 1000 + P(V_2/P_3) \cdot 0\} = \\ = \min\{3756, \;\; 60.7\} = 60.7 \tag{8.34}$$

Na tej podstawie obliczamy prawdopodobną wartość strat w przypadku wykonania serii pomiarów:

$$K = K(V_i/P_1) \cdot P(P_1) + K(V_i/P_2) \cdot P(P_2) + K(V_i/P_3) \cdot P(P_3) = 126.3 \tag{8.35}$$

Poniżej przedstawiono sieć Bayesa wykorzystaną do rozwiązania omawianego przykładu

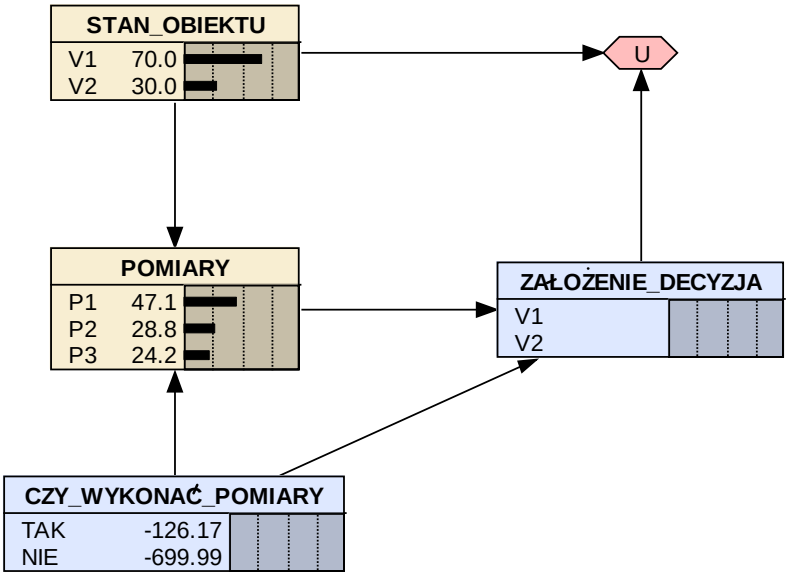
Z przeprowadzonej analizy wynika, że wykonanie pomiarów jest opłacalne gdy ich koszt jest niższy od różnicy pomiędzy prawdopodobną wielkością strat w przypadku gdy nie wykonano pomiarów oraz gdy pomiary wykonano: 700-126.17=573.83 .

Do tej pory omawiano analizę pre-posteriorii, poniżej zostanie opisana analiza a posteriorii. W przypadku wykonania pomiarów należy uzyskaną informację użyć w prowadzonej analizie. Załóżmy, że w trakcie pomiaru otrzymano wynik P_2, czyli w początkowej analizie wynik przez nas nieuwzględniany. Mając tę informację zaktualizujemy prawdopodobieństwa $P(V_i)$, a następnie na ich podstawie podejmiemy decyzję o wyborze strategii eksploatacji.

W tym celu korzystamy ze wzoru Bayesa określającego prawdopodobieństwo a posteriori:

$$\mathrm{P(V_1) = P(V_1/P_2) \Rightarrow P(V_1) = 0.3711} \tag{8.36}$$

$$\mathrm{P(V_2) = P(V_2/P_2) \Rightarrow P(V_2) = 0.6288} \tag{8.37}$$



Rys. 8.9: Sieć Bayesa

Dla zaktualizowanych prawdopodobieństw wyznaczamy funkcję użyteczności

$$\begin{aligned} \mathrm{K} = \min\{0.3711 \cdot 0 + 0.6288 \cdot 4000,\ 0.3711 \cdot 1000 + 0.6288 \cdot 0\ \} = \\ = \min\{2515.2,\ 371.1\} = \ 371.1 \end{aligned} \tag{8.38}$$

Uzyskany wynik prowadzi do podjęcia takiej samej decyzji jak na podstawie informacji a priori lecz prawdopodobna wartość strat jest inna i w tym przypadku wynosi 371.1, natomiast bez wykonania dodatkowych pomiarów wynosi 700.

Bibliografia

[8.1] *PN-ISO 10816-1: Drgania mechaniczne. Ocena drgań maszyny na podstawie pomiarów na częściach niewirujących*.

[8.2] Cox D.R. Regression models and life tables. *Journal of Royal Statistical Society, series B.*, 34:187–220, 1997.

[8.3] Cruse T.A. *Reliability – Based Mechanical Design*. Marcel Dekker Inc., New York, 1997.

[8.4] Dybała J., Mączak J., Radkowski S. *Wykorzystanie sygnału wibroakustycznego w analizie ryzyka technicznego*. ITE, Warszawa – Radom, 2006.

[8.5] Gumiński R., Radkowski S., Sobczykiewicz W. *Zastosowanie proporcjonalnych modeli uszkodzeń w analizie niezawodności na przykładzie układu antropotechnicznego*. Number zeszyt 23 serii Problemy Maszyn Roboczych. ITE Radom, 2005.

[8.6] Jeffreys H.J. *Theory of Probability*. Oxford: Clarendon Press, 1961.

[8.7] Nozer D., Singpurwalla N.D. *Reliability and Risk A Bayesian Perspective*. John Wiley & Sons Ltd, Chichester England, 2006.

[8.8] O'Hagan A., Forster J. *Kendall's Advanced Theory of Statistics: Bayesian Inference*, wolumen 2B. Hodder Arnold Publication, 2004.

[8.9] Radkowski S. *Podstawy bezpiecznej techniki*. OWPW, 2003.

[8.10] Yatomi M., inni i. Application of risk-based maintenance on materials handling systems. *IHI Enginnering Review*, 37(2):52–58, 2004.

Rozdział 9

Modele symulacyjne rozwoju procesów degradacyjnych i zmęczeniowych na przykładzie przekładni zębatej[1]

Ryszard FILONIK

9.1. Wprowadzenie

Modelowanie dynamiczne przekładni zębatych jest generalnie zadaniem złożonym. Dotyczy to głównie zagadnienia odwzorowywania oddziaływań międzyzębnych powszechnie uznanych za najbardziej skomplikowane. W każdym przypadku modelowanie można uważać za efektywne, jeśli jego wynikiem jest model obliczeniowy pozwalający wyznaczyć interesujące parametry dynamiczne. Historycznie, rozwój metod modelowania przedstawiony np. w [9.1], zapoczątkowany został próbami uproszczonych opisów oddziaływań międzyzębnych ograniczanych możliwościami rozwiązania budowanych równań matematycznych metodami analitycznymi z elementami komputerowego wspomagania obliczeń.

9.2. Założenia ogólne o modelowaniu obiektu technicznego

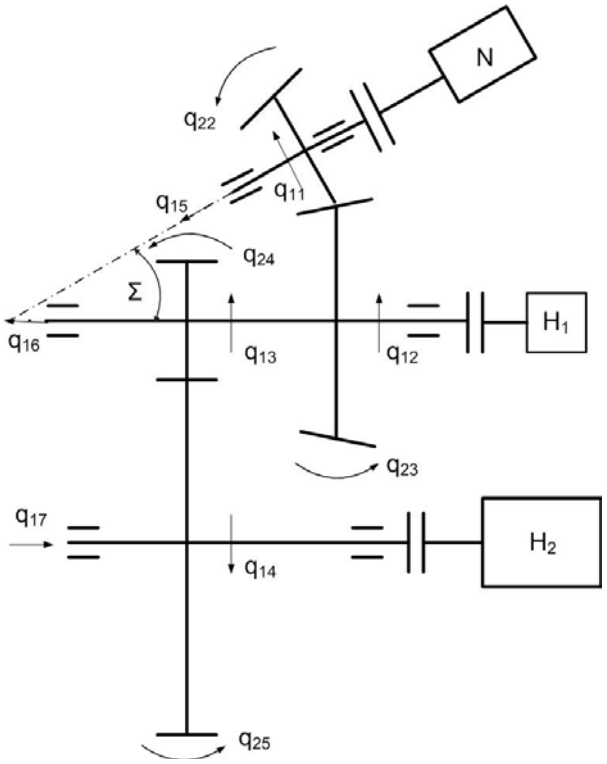
W ostatnich latach coraz wyraźniej kładzie się nacisk na traktowanie przekładni zębatych jako ogniwa całego łańcucha przeniesienia napędu, a nie wyizolowanego obiektu. Wymaga to oczywiście rozbudowy stosowanych modeli i praktycznie rzecz biorąc należy z góry przyjmować, że końcowym efektem modelowania musi być program komputerowy rozwiązujący równania ruchu badanego zespołu. Z tego punktu widzenia, skrupulatność odwzorowywania fizycznych własności obiektu rzeczywistego staje się pierwszoplanowym zadaniem, a uciekanie się do zbyt daleko idących uproszczeń modelu teoretycznego niecelowym. Oczywiście granica między skrupulatnością, a nadmierną drobiazgowością jest ustalana arbitralnie w ramach kryteriów technicznej realności i doświadczeń inżynierskich. Niektóre uproszczenia mogą być zresztą wprowadzone a posteriori po testowych obliczeniach.

Wydaje się, że sprostanie tak stawianemu zadaniu będzie najprostsze, jeśli w modelu teoretycznym będzie możliwie wiernie odwzorowana struktura obiektu rzeczywistego oraz związki konstytutywne określające węzły układu. Zasadniczo wymaga to brania pod uwagę całej gamy struktur definiowanych z dokładnością do parametrów. Od strony praktycznej warto tak dobierać opisy tych związków, by były łatwe do zaprogramowania w postaci jednokrokowych lub szybkobieżnych algorytmów, czy inaczej mówiąc informatycznie przyjaznych.

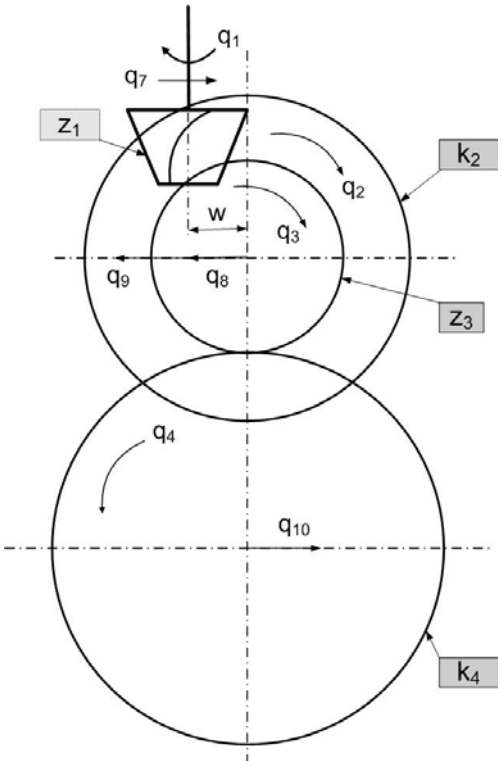
W ramach niniejszego opracowania rozważony będzie model przeniesienia napędu od silnika do

[1] Modele przedstawione w tym rozdziale są dostępne na stronie www.rfilonik.za.pl i mogą być używane jako demonstracyjne

dwóch odbiorników mocy poprzez dwustopniową przekładnię zębatą [9.4]. Proponowaną strukturę modelu przedstawiają rysunki 9.1 i 9.2. Jest to przekładnia kątowa o pierwszym stopniu hipoidalnym, co można sprowadzić do zwykłej przekładni stożkowej przyjmując parametr $w = 0$ (Rys.9.2).



Rys. 9.1: Schemat struktury układu napędowego - widok główny x – z



Rys. 9.2: Schemat struktury układu napędowego – widok z boku y – z

Jeżeli przyjąć kąt $\Sigma \to 0$ (Rys.9.1) i zerową zbieżność stożka zębnika z_1 (Rys.9.2) otrzymujemy walcową przekładnię zębatą o osiach równoległych. Przy niezerowym kącie Σ i zerowej zbieżności zębnika z_1 mamy przekładnię walcową o osiach wichrowatych. W zazębieniu stożkowym zakłada się krzywoliniowy (łukowy) kształt zębów; w przypadku szczególnym zęby skośne lub proste. Nie formułuje się na tym etapie szczegółów dotyczących geometrii wynikającej z technologii. Jest to uwzględniane na dalszym etapie modelowania. Zazębienie stopnia drugiego jest ogólnie skośne (w szczególnym przypadku proste). Przewidywanie modelu o tak szerokich założeniach podstawowych ma sens wtedy, gdy zakłada się podstawową cechę wspólną, a mianowicie zazębienie typu ewolwentowego. Jednocześnie wskazuje się na możliwość modelowania struktury w postaci sparametryzowanej. Zostanie to szerzej rozwinięte niżej. Należy podkreślić, że model obliczeniowy przekładni stożkowo-walcowej jest na etapie testowania, zaś model przekładni hipoidalnej na etapie programowania.

Koła zębate oznaczone symbolami z_1, k_2, z_3 i k_4 są osadzone na sprężystych wałkach podpartych w łożyskach o definiowanej sztywności, w szczególności odwzorowującej nierównomierne zużycia elementów tocznych. Wśród łożysk są przewidziane węzły zdolne do przenoszenia obciążeń wzdłużnych z napięciem wstępnym lub bez. Generalnie koła są osadzone na wałkach w dowolnych, realnych, warunkowanych wymiarami kół, odległościach od łożysk. Wałek zębnika stopnia pierwszego najczęściej jest łożyskowany wysięgnikowo. Można to uwzględnić przyjmując zerową sztywność dodatkowego łożyska na schemacie wg rysunku 9.1.

Przekładnia jest połączona sprzęgłami (podatnymi) z blokami: napędu „**N**", oraz odbioru mocy „H_1" i „H_2". Każdy z bloków może posiadać własną strukturę wewnętrzną i być obciążany momentami zmiennymi w czasie. Skierowanie całego strumienia mocy do bloku „H_1", przy dodatkowym założeniu zerowej masy zębnika z_3 redukuje przekładnię do jednostopniowej. W niniejszym opracowaniu założymy dla prostoty (co nie umniejsza istotnie ogólności), że omawiane bloki są walcami o stałych momentach bezwładności.

Ograniczenie się do przekładni dwustopniowej wynika z faktu, że, jak to będzie zasygnalizowane niżej, dodanie dodatkowego stopnia przełożenia (walcowego realnie rzecz biorąc), jest kwestią techniczną polegającą na dopisaniu dodatkowych, analogicznych do opisu stopnia drugiego, równań ruchu.

9.3. Modelowanie stanów dynamicznych przekładni zębatej

Model fizyczny, którego struktura została przedstawiona wyżej, jest mechanizmem złożonym z elementów odkształcalnych o ruchliwości 1. Oprócz ruchu podstawowego (obrotowego), mamy więc do czynienia z drganiami w układzie w istotny sposób wpływających na funkcjonowanie całości przeniesienia napędu. Wiele składowych tych drgań takich jak drgania gięte i skrętne wałków oraz sprzęgieł ma cechy drgań liniowych układu o wielu stopniach swobody i ich opis można uważać z elementarny. Drgania te są jednak sprzężone z drganiami kół zębatych wynikających z oddziaływań międzyzębnych specyficznych dla zazębienia ewolwentowego, do którego ogranicza się tu rozważania. Modelowanie tych oddziaływań jest najistotniejszym i najtrudniejszym zagadnieniem do rozwiązania.

Pomimo istnienia co najmniej kilku różnych, znanych z literatury podejść, autor opowiada się konsekwentnie za stosowaniem modelowania opartego na metodzie interferencji pozornej, zaproponowanej i skutecznie rozwijanej w ośrodku związanym z Pracownią Wibroakustyki IPBM Politechniki Warszawskiej. Założenia i wiele szczegółów tej metody było przedmiotem licznych opracowań m.in. [9.2]. Tutaj zostaną przedstawione tylko te aspekty metody, które wskazują na jej elastyczność i możliwości stosowania w modelach o cechach przedstawionych w punkcie poprzednim.

Opis dynamiki ruchu przekładni wymaga zdefiniowaniu układu współrzędnych uogólnionych, z których część przedstawiono na schematach z rysunku 9.1 i 9.2. Konkretnie będą to (uwzględniając również te nie przedstawione na schematach):

q_1 – kąt obrotu zębnika z_1 względem ruchu stacjonarnego $[rd]$

q_2 – kąt obrotu koła k_2 względem ruchu stacjonarnego $[rd]$

q_3 – kąt obrotu zębnika z_3 względem ruchu stacjonarnego $[rd]$

q_4 – kąt obrotu koła k_4 względem ruchu stacjonarnego $[rd]$

q_5 – kąt obrotu wirnika napędu względem ruchu stacjonarnego $[rd]$ (zwrot jak zębnik z_1)

q_6 – kąt obrotu wirnika części biernej względem ruchu stacjonarnego [rd] (zwrot jak koło k_4)

q_7 – przemieszczenie środka masy zębnika z_1 w płaszczyźnie y-z zwrot jak na Rys.9.2

q_8 – przemieszczenie środka masy koła k_2 w płaszczyźnie y-z zwrot jak na Rys.9.2

q_9 – przemieszczenie środka masy zębnika z_3 w płaszczyźnie y-z zwrot jak na Rys.9.2

q_{10} – przemieszczenie środka masy koła k_4 w płaszczyźnie y-z zwrot jak na Rys.9.2

q_{11} – przemieszczenie środka masy zębnika z_1 w płaszczyźnie x-z zwrot jak na Rys.9.1

q_{12} – przemieszczenie środka masy koła k_2 w płaszczyźnie x-z zwrot jak na Rys.9.1

q_{13} – przemieszczenie środka masy zębnika z_3 w płaszczyźnie x-z zwrot jak na Rys.9.1

q_{14} – przemieszczenie środka masy koła k_4 w płaszczyźnie x-z zwrot jak na Rys.9.1

q_{15} – przemieszczenie wzdłużne zębnika z_1 (z wałkiem) zwrot jak na Rys.9.1

q_{16} – przemieszczenie wzdłużne koła k_2 i zębnika z_3 z wałkiem zwrot jak na Rys.9.1

q_{17} – przemieszczenie wzdłużne koła k_4 z wałkiem zwrot jak na Rys.9.1

q_{18} – kąt obrotu zębnika z_1 w płaszczyźnie y-z w lewo względem współrzędnej q_7

q_{19} – kąt obrotu koła k_2 w płaszczyźnie y-z w lewo względem współrzędnej q_8

q_{20} – kąt obrotu zębnika z_3 w płaszczyźnie y-z w lewo względem współrzędnej q_9

q_{21} – kąt obrotu koła k_4 w płaszczyźnie y-z w lewo względem współrzędnej q_{10}

q_{22} – kąt obrotu zębnika z_1 w płaszczyźnie x-z w lewo względem współrzędnej q_{11}

q_{23} – kąt obrotu koła k_2 w płaszczyźnie x-z w lewo względem współrzędnej q_{12}

q_{24} – kąt obrotu zębnika z_3 w płaszczyźnie x-z w lewo względem współrzędnej q_{13}

q_{25} – kąt obrotu koła k_4 w płaszczyźnie x-z w lewo względem współrzędnej q_{14}

q_{26} – kąt obrotu wirnika bloku biernego stopnia I (zwrot jak koła k_2)

W wybranym układzie odniesienia ukryte jest założenie, ze rozłożone w sposób ciągły masy wałków dają się zredukować bez zbyt daleko idącego uproszczenia zredukować do środków osadzonych na nich kół zębatych. Same koła zębate są traktowane jako nieodkształcalne walce lub stożki zasadnicze, z rozmieszczonymi na ich powierzchniach bocznych elementów odkształcalnych (zębów) Przyjęte jest również założenie, że sprzęgła łączące bloki napędu i odbioru mocy z przekładnią eliminują wpływ tych bloków na zginania wałków. Jak już zaznaczono wcześniej pominięto ewentualną strukturę wewnętrzną tych bloków.

Zdefiniowanie kątów obrotów kół zębatych względem osi prostopadłych do wałków jest jak najbardziej uzasadnione mając na względzie fakt, że w realnych konstrukcjach szerokości kół są rzędu ich średnic (zębników). Szczegóły staną się ewidentne w świetle dalszych analiz.

Jak zaznaczono wyżej, struktura układu przypomina zwykły liniowy układ drgający o wielu stopniach swobody co pozwala zapisać symbolicznie równania ruchu (w postaci macierzowej) jako

$$M\,\ddot{Q} + C\,\dot{Q} + KQ + P_z(Q, \dot{Q}, \mathrm{t}) = P_e(t) \tag{9.1}$$

gdzie:

Q – wektor współrzędnych uogólnionych (odpowiednio pierwsza i druga pochodna względem czasu),

$P_e(t)$ – oddziaływania zewnętrzne (napęd, opór bierny),

M, C, K – kwadratowe macierze bezwładności, tłumienia i sztywności (dla prostoty zakłada się stałe),

$P_z(Q, \dot{Q}, \mathrm{t})$ – wektor reprezentujący oddziaływania międzyzębne.

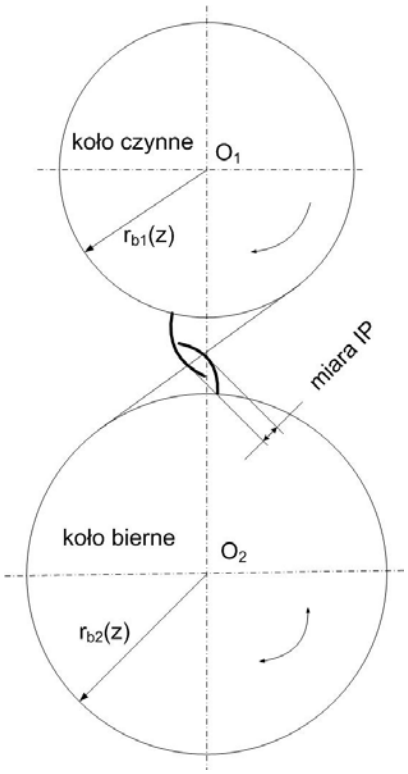
W istocie układ równań (9.1) jest układem różniczkowo – całkowym gdzie człony całkowe ukryte są właśnie w wektorze $P_z(Q, \dot{Q}, \mathrm{t})$.

Jeśli wg układu (9.1) mamy otrzymać efektywne rozwiązanie to należy rozumieć przez to całkowanie numeryczne np. metodą Rungego, Kutty i Gilla. Mając to na uwadze w budowaniu matematycznej postaci wektora $P_z(Q, \dot{Q}, \mathrm{t})$ warto kierować się przesłankami wynikającymi z pragmatyki informatycznej języków wysokiego poziomu (Pascal, C++).

Oddziaływanie międzyzębne z dokładnością do tarcia jest klasyczną siłą sprężystości. Uwzględniając fakt, że sprężystość pary współpracujących zębów jest dobrze zbadana i opisana, wyznaczenie oddziaływania jest zagadnieniem wyznaczenia odkształcenia. Pojawia się tu jednak istotna trudność polegająca na nieoznaczoności punktu przyłożenia takiej siły. Konkretniej mamy do czynienia z obciążeniem ciągłym rozłożonym wzdłuż linii, a właściwie wstęgi przyporu dla jednej pary zębów. Wypadkowa obciążeń na wszystkich parach aktualnie współpracujących, generująca moment względem osi obrotu koła może być odnaleziona jako całka wzdłuż linii efektywnego styku. Jest to właśnie sygnalizowany element całkowy w wektorze $P_z(Q, \dot{Q}, \mathrm{t})$. Do rozwiązania takiego zadanie nadaje się metoda interferencji pozornej.

9.4. Modelowanie oddziaływań międzyzębnych

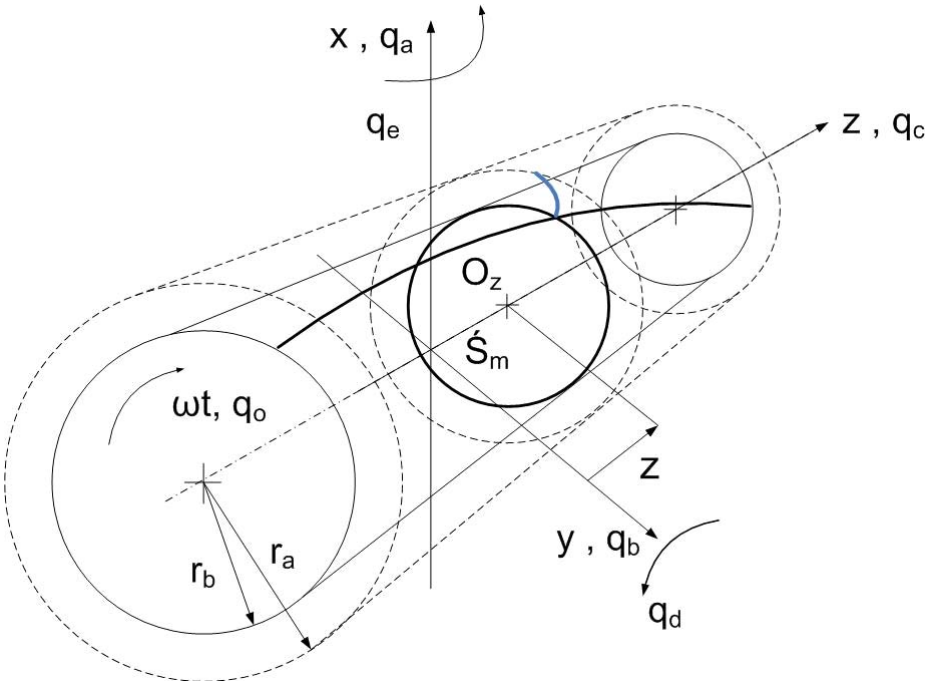
Metoda interferencji pozornej (IP) była wielokrotnie przedstawiana w cytowanych już opracowaniach. Tutaj dla porządku przypomnimy jej zasadniczą ideę polegającą na poszukiwaniu jako miary odkształcenia sprężystego współpracujących zębów jako wzajemnego przenikania się dwóch wyobrażalnych ewolwent (zarysów zębów), co przedstawia rysunek 9.3. Miarę IP definiujemy jako nieujemną, gdy koło czynne wyprzedza koło bierne. W przypadku przeciwnym $IP = 0$. Przedstawiona na rysunku 9.3 sytuacja ma miejsce w wybranym przekroju koła zębatego w postaci walca, lub ogólniej stożka ściętego.



Rys. 9.3: Miara interferencji pozornej

W zerowym przybliżeniu zakłada się, że obserwujemy idealne ewolwenty odtoczone z odpowiednich kół zasadniczych. Usytuowanie każdego z kół przekroju przedstawionego na rysunku 9.3 przedstawia rysunek 9.4. Oczywiście założenie braku zbieżności stożka sprowadza zagadnienie do koła walcowego. Zaznaczona na powierzchni bocznej krzywa linii zęba może być z kolei zastąpiona prostą, ogólnie nachyloną do tworzącej stożka (ząb skośny). Z każdego punktu linii zęba na stożku zasadniczym jest odtaczana, ograniczona powierzchnią boczną stożka wierzchołków, ewolwenta kulista (płaska dla koła walcowego).

Z samym kołem w jego środku masy wiążemy lokalny układ odniesienia $\acute{S}_m xyz$, który w położeniu jak na rysunku pokrywa się z globalnym, nieruchomym układzie odniesienia, w którym muszą być definiowane równania ruchu. Zaznaczone na rysunku obroty względem osi układu lokalnego jest powszechnie przyjęte za dopuszczalne dla opisu małych drgań.



Rys. 9.4: Położenie przekroju obliczeniowego na kole stożkowym

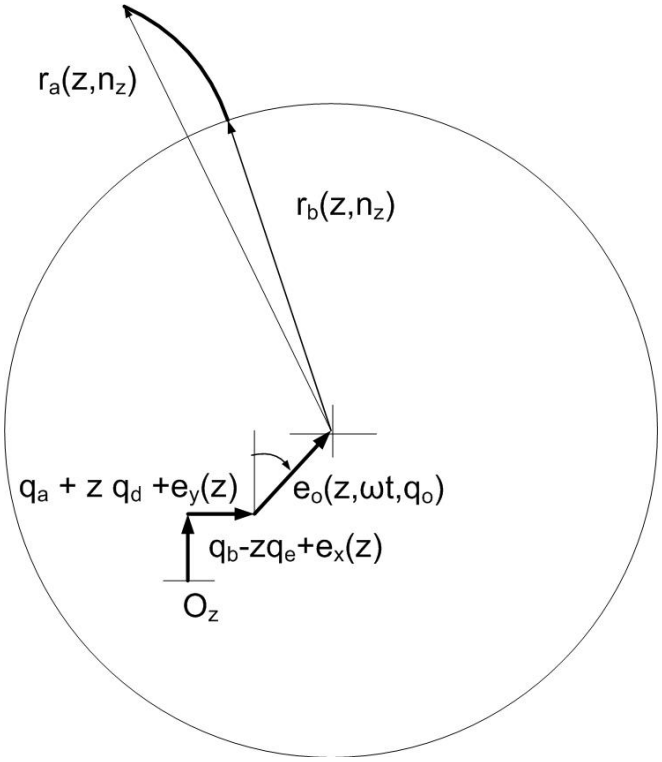
Na rysunku użyto również abstrakcyjnych symboli współrzędnych uogólnionych opisujących małe drgania. W równaniach ruchu (9.1) będą one identyfikowane ze zdefiniowanymi wcześniej współrzędnymi $q_i, i = 1..26$ koła zębatego jako całości. Mają one swój wpływ na położenie przekroju obliczeniowego i położonego na nim początku ewolwenty modelowej.

Bardziej szczegółowo przedstawia to rysunek 9.5, gdzie uszczegółowiono te zależności z podkreśleniem, że dotyczy to wybranego zarysu powiązanego z zębem o konkretnym numerze n_z.

Wyszczególnione na rysunku przemieszczenia e_x i e_y oznaczają przemieszczenia wynikające z wichrowatego montażu wałka w łożyskach, natomiast wirujący wektor e_o określa wichrowaty montaż danego koła na osi wałka. Uwzględnienie wprowadzonych dotychczas parametrów dla obydwu współpracujących kół dla wszystkich oddalonych od siebie o dz przekrojach pozwala wyznaczyć wartości $IP(z)$ wg definicji przedstawionej na rysunku 9.3 w kierunku wspólnej stycznej do odpowiednich kół zasadniczych. Z każdym ze współpracujących zębów wiązana jest sztywność definiowana na jednostkę długości linii styku, zależna od położenia na ewolwentach w punktach wyznaczonych styczną (linią przyporu). Odnotujmy, że pojęcie linii (odcinka) przyporu jest w takim ujęciu pojęciem wynikowym, a nie wyjściowym. Możliwe jest teraz zdefiniowane elementarnego nacisku (obciążenia ciągłego)

$$dp(z) = k_{zast}(\varphi_a, \varphi_b, z) IP(z) \tag{9.2}$$

gdzie:



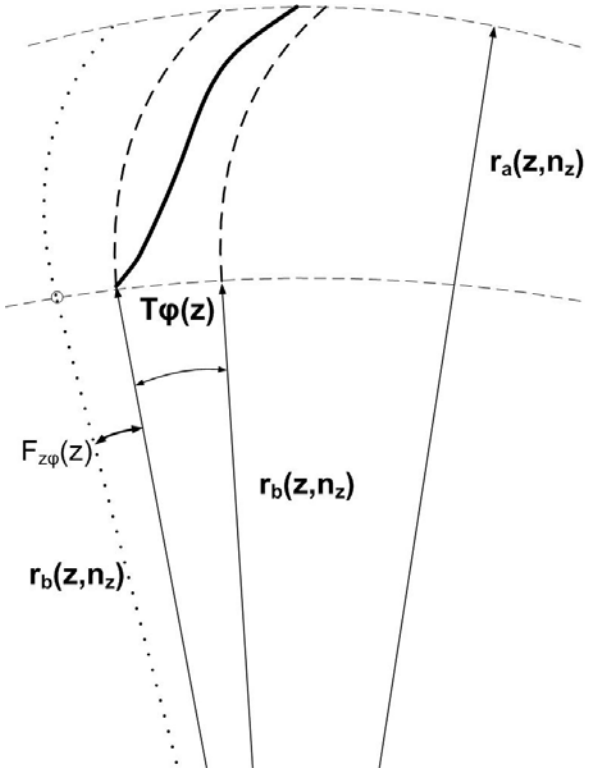
Rys. 9.5: Położenie ewolwenty modelowej z uwzględnieniem odkształceń sprężystych i błędów montażu

$k_{zast}(\varphi_a, \varphi_b, z)$ – wypadkowa sztywność pary zębów zależna od punktu ich styku będącego funkcją kątów obroty poszczególnych kół oraz położenia wzdłuż linii zęba.

Na tym poziomie, wykorzystując fakt, że, z powodów organizacji obliczeń, poszczególne zęby są numerowane możemy wygodnie odwzorować osłabienie zęba np. na skutek pojawienia się (mikro)szczeliny zmęczeniowej w stopie zęba, również zmiennej wzdłuż długości koła.

Przed scałkowaniem obciążenia wzdłuż linii styku i dla wszystkich będących w kontakcie par zębów należy uwzględnić odchyłki wynikające z nieidealnego profilu boków zębów. Szczegóły przedstawia rysunek 9.5. Zaznaczono tu linią kropkową położenie początku ewolwenty teoretycznej wymiarowane jak na rysunek 9.5. Rzeczywisty początek profilu zęba jest przemieszczony o kątową wartość błędu podziałki kinematycznej $F_{z\varphi}(z)$, natomiast pełny zarys znajduje się wewnątrz pola tolerancji przeliczonej na wartość kątową $T_{\varphi}(z)$. Na tym z kolei poziomie możemy dodatkowo odwzorować fakt (nie zaznaczony na rysunku), że na powierzchni zęba może pojawić się wgłębienie rzędu wyższego niż tolerancje i ugięcia sprężyste np. na skutek zmęczenia powierzchniowego (pittingu).

Zależność tolerancji od położenia wzdłuż linii styku jest uzasadnione głównie dla kół stożkowych. Na tym poziomie uwzględnia się również odchyłki oktoidalnego profilu zęba stożkowego wynikającego z technologii od zarysu ewolwenty kulistej przyjętej jako modelowa. Obliczenia testowe pokazują, że nie jest nadmiernym uproszczeniem odstąpienia od korygowania kąta zarysu w przypadku kół walcowych. W przypadku profili oktoidalnych w zazębieniach stożkowych problem pominięcia lokalnej korekty promienia zasadniczego nie jest rozstrzygnięty. Po uwzględnieniu tych poprawek możliwe będzie całkowania zależności (9.2). Praktycznie wystarczająco dokładne jest całkowanie metodą trapezów i to (jak wykazują obliczenia testowe) z dosyć dużym przedziałem (krokiem) rozmieszczenia węzłów (rzędu 1/15 do 1/30 szerokości koła). Ostatnim krokiem składowym w algorytmie wyznaczaniu wektora $P_z(Q, \dot{Q}, \mathrm{t})$ jest uwzględnienie składowej stycznej (tarcia) na powierzchniach styku inaczej odchylenie kierunku oddziaływania o kąt tarcia w stosunku do linii przyporu, zależnie od kierunku poślizgu. Model wartości współczynnika tarcia (dosyć złożony) przyjmuje się np. wg metodyki obliczania kół na zatarcie [9.3].



Rys. 9.6: Rzeczywisty zarys boku zęba

Ostateczna postać wektora $P_z(Q, \dot{Q}, \mathrm{t})$ wynika bezpośrednio

$$\delta L = \Sigma\Sigma dp_{zn}(Q) \cdot \delta r_{xn}(Q) = \Sigma p_{qi}(Q)\delta q_i \quad n = 1..4, i = 1..25 \tag{9.3}$$

z równości prac przygotowanych na przemieszczeniach przygotowanych δr zdefiniowanych w stałym układzie odniesienia i wyrażonych następnie w funkcji przemieszczeń wirtualnych δq_i. We wzorze (9.3) zawarto sygnalizowane wyżej całkowanie metodą trapezów.

Poszczególne przedstawione wyżej etapy modelowania są zapisywane bezpośrednio w hierarchicznej strukturze funkcji i procedur języków programowania wysokiego poziomu.

Zaproponowany wyżej model dynamiczny charakteryzuje się, jak widać, łatwością uwzględniania podstawowych imperfekcji geometrycznych i zgodnością z ogólnymi definicjami przewidzianych normami PN-ISO. Praktyczne stosowanie modelu wymaga uzupełnienia go blokiem wyjścia przetwarzającym teoretycznie, niezbędne i fizycznie oczywiste współrzędne uogólnione, na parametry inżyniersko zorientowane, przydatne w projektowaniu, diagnostyce i monitorowania stanów eksploatacyjnych. Należą do nich:

1. Reakcje w łożyskach wszystkich wałków przekładni; poprzeczne i wzdłużne
2. Chwilowe przełożenie między poszczególnymi stopniami
3. Całkowite siły międzyzębne w obydwu zazębieniach (parametry te mają charakter poglądowy i teoretyczny z uwagi na cechy sił międzyzębnych omówione wyżej)
4. Całkowite siły przypadające na jeden ząb (parametry poglądowe)
5. Siły przypadające na pojedynczy ząb z uwzględnieniem rozkładu wzdłuż linii styku rejestrowane w ustalonych, równoodległych przekrojach liczonych od brzegu koła.
6. Naprężenia powierzchniowe zębów współpracujących w funkcji położenia na zębie (ja siły wyżej)
7. Naprężenia gnące w stopach zębów wszystkich kół wzdłuż linii zębów

8. Naprężenia gnące i skręcające w niebezpiecznych przekrojach wałków
9. Inne parametry wyjściowe zgodnie z zainteresowaniem użytkownika programu obliczeniowego, np. dane do obliczeń naprężeń w uzębieniach metodami MES.

Wyprowadzanie takich parametrów przewidziano w programie obliczeniowym.

9.5. Symulacja procesów zmęczeniowych i degradacyjnych w eksploatacji przekładni zębatej

Scałkowanie układu równań (9.1) po zapisaniu go w postaci programu obliczeniowego daje rozwiązanie szczególne w praktycznej postaci parametrów wyjściowych wymienionych w punkcie poprzednim (oczywiście również w postaci współrzędnych stanu). Akcentując ten fakt zapisujemy

$$F(t) = g(\kappa, t) \tag{9.4}$$

gdzie:

F – wektor parametrów wyjściowych,

K – przestrzeń parametrów konstrukcyjnych i funkcjonalnych modelu definiujących układ (9.1).

Dla każdego wektora $\kappa \in \mathrm{K}$ funkcja **F** reprezentuje rozwiązanie szczególne. Niewykonalne jest znalezienie wszystkich funkcji (9.4) dla każdego $\kappa \in \mathrm{K}$, (co dawałoby pogląd na rozwiązanie ogólne), nawet ograniczając się do parametrów realnych technicznie. Możliwa jest jednak szersza analiza rozwiązania (9.4) dla dużej liczby wektorów κ, (rodzaj przeglądu do racjonalizacji konstrukcji). Dzięki odwzorowaniu w modelu zasadniczej struktury mechanicznej przekładni jest to zadanie formalnie łatwe, choć obszerne.

Najistotniejsze znaczenie wydaje się mieć zagadnienie analizy modelu o ustalonych nominalnych parametrach konstrukcyjnych pod kątem wpływu wszelkiego rodzaju, możliwych do odwzorowania w obliczeniach, odchyłek od wartości nominalnych. Będą to błędy wykonania i montażu oraz zużycia w procesie eksploatacji w szczególności zmęczeniowe. Ważną sprawą jest pozyskiwanie konkretnych danych opisujących omówione wyżej błędy; oprzemy więc rozważania na wyborach arbitralnych, ewentualnie wspomaganych metodami statystycznymi (poza modelem).

W ramach niniejszego opracowania zajmiemy się głównie problematyką procesów degradacyjnych w szczególności zagadnień pojawiania się i rozwoju uszkodzeń zmęczeniowych w uzębieniach, co jest jednym z możliwych rodzajów uszkodzenia. W ramach niniejszego opracowania pomija się problematykę uszkodzenia łożysk i wałków przekładni, aczkolwiek narzędzia do takich analiz są zakodowane w przedstawionym tu modelu dynamicznym.

Pękanie zęba w podstawie i pitting, dobrze widoczne w modelu symulacyjnym na sygnałach parametrów wyjściowych obliczanych, w warunkach normalnej eksploatacji obiektu technicznego jest znacznie trudniejsze do zaobserwowania i diagnozowania. Jeśli wykluczyć inspekcję bezpośrednią, wymagającą zatrzymania procesu eksploatacyjnego i demontażu urządzenia, to rozwiązania należy szukać w obserwacji (biernej) sygnałów przydatnych diagnostycznie, czyli względnie łatwych do obserwacji w trakcie normalnego użytkowania obiektu. Posiadanie modelu symulacyjnego, ułatwia interpretację pozyskiwanych wyników obserwacji, aczkolwiek nadal problem nie jest rozwiązany, tylko złagodzony.

Ważne zagadnienie, które może być w istotnym stopniu wyjaśnione, to analiza związków między symulowanymi sygnałami diagnostycznymi i niediagnostycznymi.

Przytoczone zostaną tu przyczynkowe przykłady oparte na symulacji procesów z powstającymi i rozwijającymi się uszkodzeniami w postaci pittingu i szczeliny zmęczeniowej w podstawie zęba. Dane o rodzaju, wielkości i postępach uszkodzeń są wybrane zupełnie arbitralnie celem ilustracji metody.

Za punkt wyjścia wybrano stan przekładni przenoszącej moc 300 kW o dużej dokładności wykonania (modelowych) wszystkich kół z wyjątkiem koła stopnia drugiego, gdzie założono losowo przyjęty błąd podziałek kinematycznych, uwzględniający błąd linii zęba. Wartości liczbowe podstawowych parametrów konstrukcyjno – eksploatacyjnych zestawiono w raporcie:

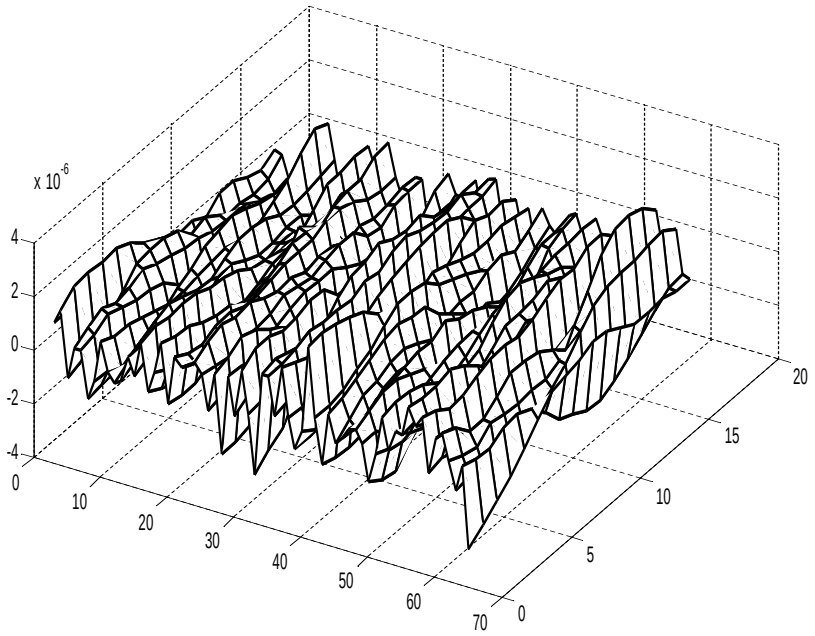
Stopień pierwszy

Liczba zębów zębnika z I	: 17
Liczba zębów koła z II	: 52
Moduł I	: 5.00
Korekcja zębnika	: 0.1820
Korekcja koła	: -0.1381
Kąt pochylenia (stopnie)	: 11.00
Kierunek pochylenia	: P
Szerokość czynna wieńców	: 70.00
Moment napędu $[Nm]$	: 1007.4
Moment bezwładności silnika $[kgm^2]$	: 4.365
Obroty zębnika $[Hz]$	: 50.0
Średnica wałka zębnika $[mm]$	: 75.00
Średnica wałka koła $[mm]$	: 85.00
Długość wałka zębnika $[mm]$	: 290.00
Długość wałka koła $[mm]$	: 290.00
Odległość od łożysk $[mm]$ (strona napędu)	: 75.00
Sztywność sprzęgła napędu $[kNm/rad]$	: 26.00
Sztywność poprzeczna łożyska IA $[kN/\mu m]$	: 0.213
Sztywność poprzeczna łożyska IB $[kN/\mu m]$	: 0.213
Sztywność wzdłużna łożyska I $[kN/\mu m]$	: 0.053
Sztywność poprzeczna łożyska IIA $[kN/\mu m]$	: 0.413
Sztywność poprzeczna łożyska IIB $[kN/\mu m]$	: 0.613
Sztywność wzdłużna łożyska II $[kN/\mu m]$	: 0.063

Stopień drugi

Liczba zębów zębnika z III	: 19
Liczba zębów koła z IV	: 63
Moduł II	: 6.00
Korekcja zębnika	: 0.0000
Korekcja koła	: 0.0000
Kąt pochylenia (stopnie)	: 6.50
Kierunek pochylenia	: L
Szerokość czynna wieńców	: 70.00
Moment bierny	: stały
Moment bezwładności odbioru mocy $[kgm^2]$	: 13.920
Średnica wałka zębnika $[mm]$	: 85.00
Średnica wałka koła $[mm]$	: 105.00
Długość wałka zębnika $[mm]$	: 290.00
Długość wałka koła $[mm]$	: 290.00
Odległość od łożysk $[mm]$ (strona napędu)	: 145.00
Sztywność sprzęgła biernego $[kNm/rad]$	: 60.8
Sztywność poprzeczna łożyska IIIA $[kN/\mu m]$	: 0.813
Sztywność poprzeczna łożyska IIIB $[kN/\mu m]$	: 0.913
Sztywność wzdłużna łożyska III $[kN/\mu m]$	: 0.073

Rozkład błędu podziałki kinematycznej koła k_4 otrzymany w drodze losowania przedstawia rysunek 9.7.



Rys. 9.7: Rozkład błędu podziałki kinematycznej dla koła **k4**

Wykonano obliczenia symulacyjne w przedziale czasu równym 1s, rejestrując wyniki co 1/32768s. Wybór parametrów rejestracji ma ułatwić czytelność widm (rozdzielczość 1Hz).
Rejestrowano:

- przełożenie chwilowe pomiędzy wszystkimi stopniami przekładni
- składowe poziome, pionowe i wzdłużne reakcji wszystkich łożysk w przekładni
- rozkład sił międzyzębnych wzdłuż linii zęba w 16 równo oddalonych przekrojach
- rozkład nacisków powierzchniowych j.w.
- rozkład naprężeń gnących j.w
- sumaryczne siły międzyzębne
- całkowite siły międzyzębne przypadające na poszczególne zęby

Dwa ostatnie typy parametrów wyjściowych mają oczywiście charakter poglądowy.

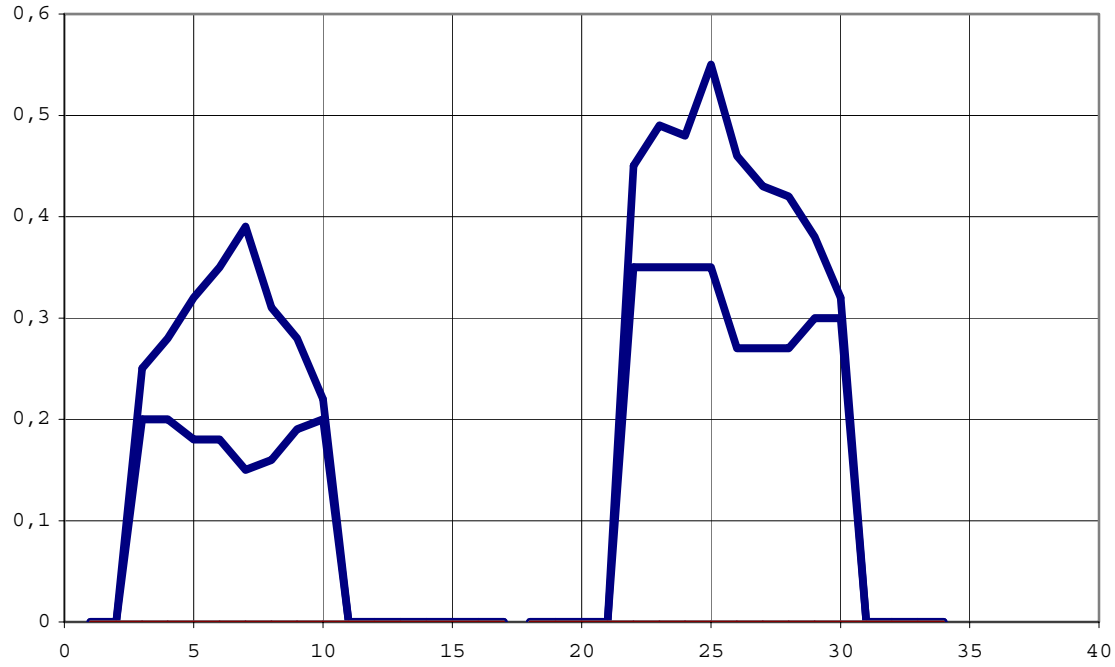
9.5.1. Symulacja procesu pojawiania się i rozwoju pittingu

Do przeanalizowania zagadnienia pojawiania się i rozwoju pittingu wykonano kolejno:

- serię obliczeń dla przekładni wolnej od wszelkich błędów (modelowej), dla uzyskania stanu odniesienia
- serię obliczeń dla przekładni z kołem k_4 obarczonym błędem podziałki (Rys.9.7)
- 3 serie obliczeń dla pojawiającego się i rozwijającego pittingu na zębniku z_3

Wąski zakres uwzględnionych w obliczeniach błędów nie wynika z ograniczeń modelu, lecz podyktowany jest poglądowością opracowania. Wnikliwsza bowiem analiza rezultatów symulacji jest zagadnieniem trudnym.

W kolejnych seriach obliczeń przyjęto pojawienie się pittingu na zębniku z_3 najpierw na dwóch, a później na trzech zębach z powiększającą się powierzchnią wykruszenia, tak jak to przedstawiają



Rys. 9.8: Schemat uszkodzenia powierzchni zębów nr 3 i nr 9 zębnika z_3

to rysunki 9.8 i 9.9. Wykruszenie (brak kontaktu) ma miejsce pomiędzy liniami tych samych kolorów wymiarowane względnie (do wysokości zęba).

W modelu symulacyjnym przyjęto 17 przekrojów obliczeniowych kontrolnych (podział szerokości koła na 16 równych przedziałów). Zgodnie z rysunkiem 8 na uszkodzonych zębach mamy po jednym obszarze wgłębienia, na rysunku 9.9 po dwa obszary wgłębień w różnych odległościach od podstawy zęba. W samych obliczeniach uwzględniano uszkodzenia pośrednie miedzy przedstawianymi na rysunkach.

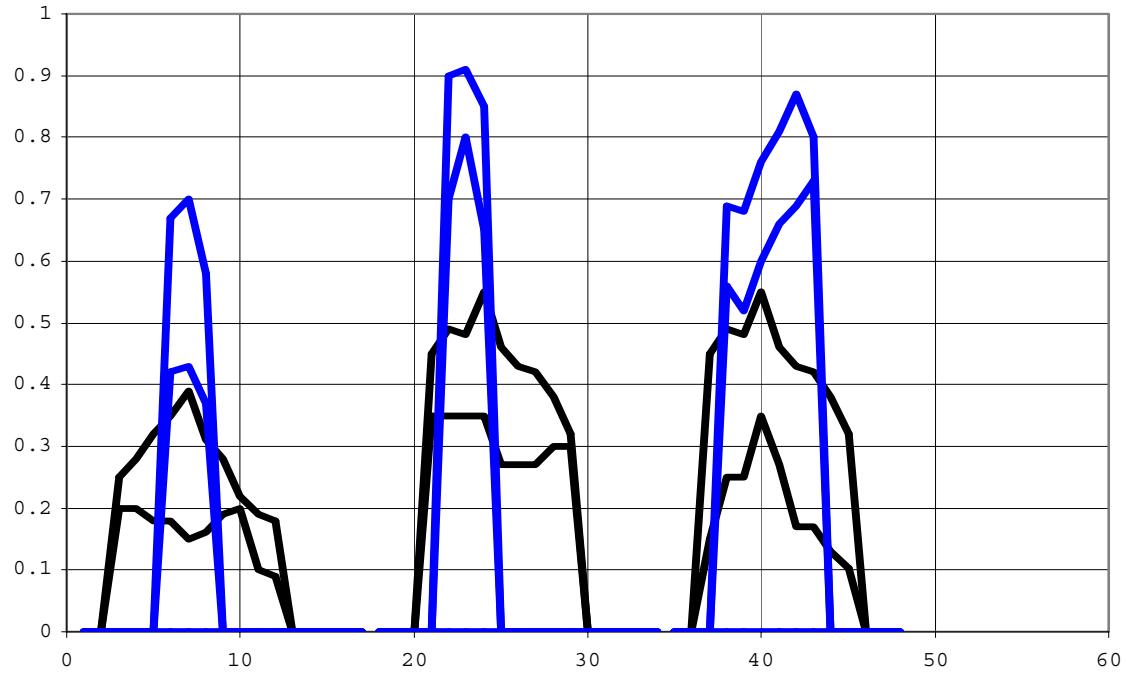
Jako parametr diagnostyczny wybrano zaburzenie przełożenia całkowitego oznaczanego dalej „urc". Powodem jest dobra wrażliwość tego parametru możliwego do obserwowania w trakcie normalnej eksploatacji obiektu technicznego przy użyciu np. laserowych urządzeń do pomiaru prędkości kątowych wałów wejściowego i wyjściowego. Inne parametry eksploatacyjne np. reakcje łożysk są mniej wrażliwe na stosunkowo niewielkie przecież zakłócenie warunków pracy, jakim jest częściowy zanik kontaktu na dwóch lub trzech spośród dziewiętnastu zębów zębnika wolnoobrotowego.

Na rysunku 9.10 zestawiono widma amplitudowe tego sygnału. Najwyżej położony wykres odpowiada sygnałowi z przekładni idealne, poniżej, przekładni z błędem podziałki wg rysunku 9.7 i kolejno z rozwijającym się pittingiem; wg rysunku 9.8, stan pośredni (bez schematu) i stan wg rysunku. 9.9.

Na zestawieniu widoczny jest powszechnie akceptowany fakt, że błędy wykonania i zużycia nie modyfikują głównych harmonicznych widma, których struktura zależy tylko od parametrów konstrukcyjnych, konstrukcyjnych rozważanym przypadku ustalonych.

Wpływ kolejno błędu wykonania i nakładających się na ten błąd zaburzeń powstających uszkodzeniem powierzchni obserwujemy w „czystych" w przypadku modelowym przedziałów między harmonicznymi częstotliwości zazębień.

Przy założonych parametrach podstawowych jak w raporcie wyżej, harmoniczne częstotliwości zazębień są wielokrotnościami wartości 850 i 311,5Hz. Z rysunku 9.10 wynika, że wpływ błędu podziałki ujawnia się w niskim zakresie, do pierwszej harmonicznej zazębienia pierwszego stopnia. Natomiast wpływ pittingu jest szerokopasmowy przekraczający nawet trzecią harmoniczną stopnia podstawowego. Aby uczynić obserwację łatwiejszą na rysunku 11 przedstawiono ewolucję składowej widma



Rys. 9.9: Schemat uszkodzenia powierzchni zębów nr 3, nr 9 i nr 13 zębnika z_3

związanej z pittingiem, przy czym wydłużono dla pewności przedział obserwacji. W symulowanym przykładzie znane (założone) są przyczyny zjawiska. Natomiast związek przyczynowo – skutkowy jest widoczny tylko jakościowo. Elementarnym pożytkiem wynikającym z przykładu jest wniosek o sposobie prowadzenia okresowych obserwacji i wnioskowaniu o pojawianiu się uszkodzeń powierzchniowych na podstawie analizy widma jak to zaproponowano.

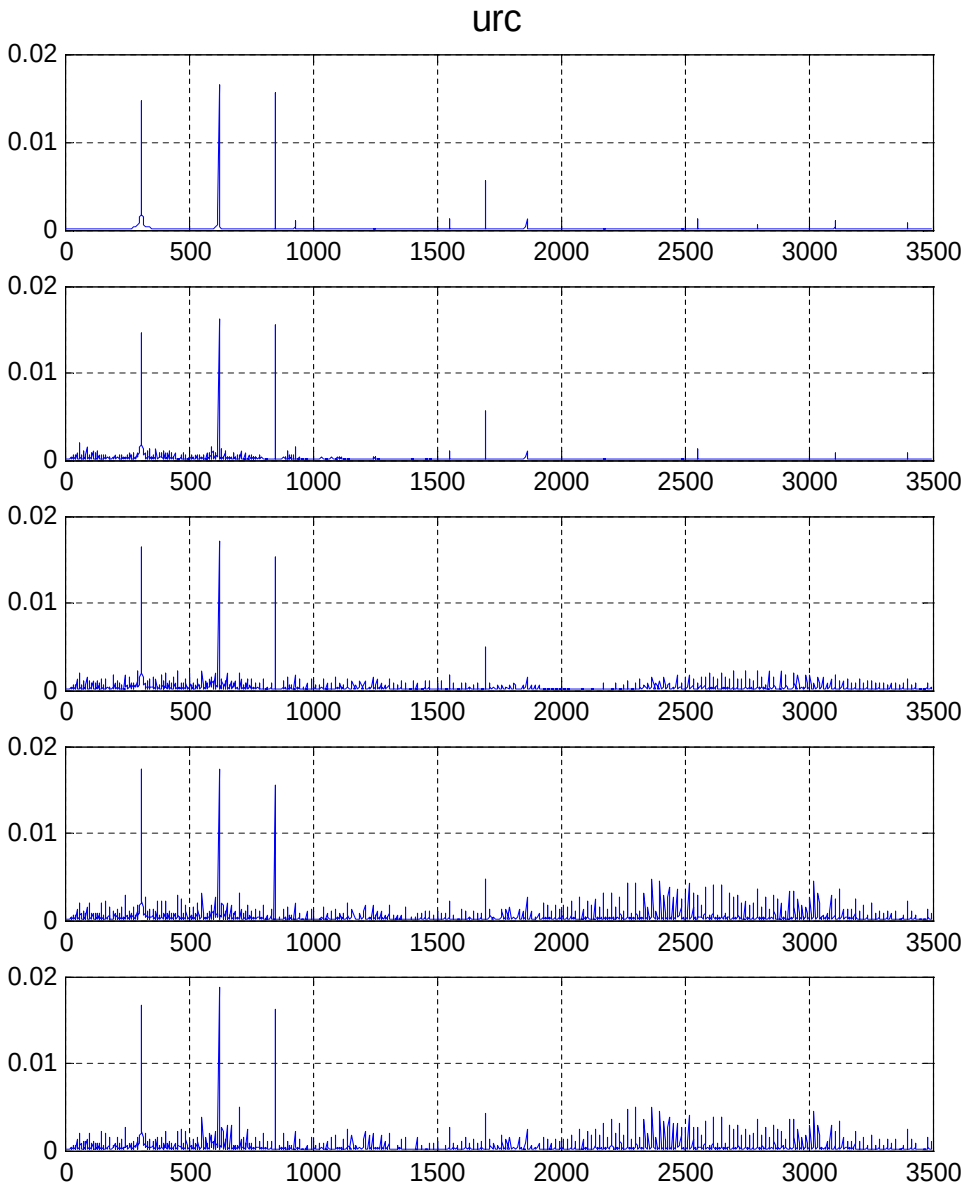
Wybór do obserwacji sygnału przełożenia całkowitego (dobre skutki daje w tym przypadku również obserwacja przełożenia między wałkiem pośrednim i wyjściowym), wynika z jego niezłej wrażliwości na badany typ uszkodzenia. Niektóre z innych sygnałów o charakterze diagnostycznym są praktycznie na nie niewrażliwe.

Poszukiwania innych sygnałów wrażliwych na pojawianie się i rozwój pittingu wśród reakcji łożysk wałków ujawniają inny użyteczny sygnał, budowany na składowych poziomej i pionowej reakcji R_{b3} łożyska najbliższego kołu k_4, a mianowicie ich chwilowego stosunku.

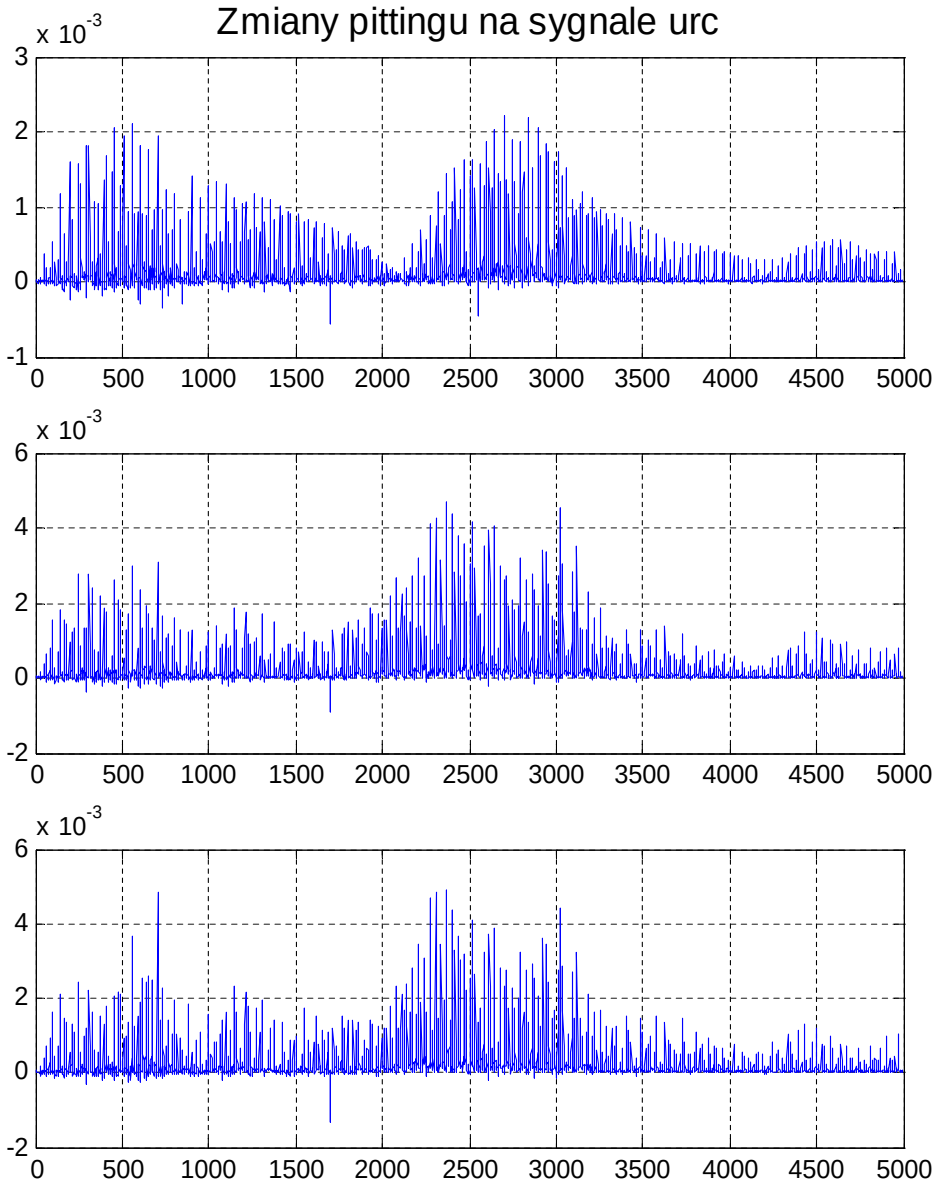
Na rysunku 9.12 pokazano zmiany w widmie odnoszone do stanu przed pojawieniem się uszkodzenia w tak otrzymanym sygnale.

Można poszukiwać dalszych (już słabszych) modyfikacji widm innych sygnałów, zakończymy to jednak na dwóch potwierdzeniach. Ten fakt wskazuje na celowość zainteresowania się sygnałami niediagnostycznymi dotyczącymi oddziaływań międzyzębnych. Wydaje się, że najciekawszy będzie stan sygnału w dziedzinie czasu. Wybrano przykładowo rozkład nacisków powierzchniowych. Przedstawia to rysunku 9.13 oraz rysunku 9.14. Przedstawiają one wartości nacisków w [MPa] dla 1, 4, 7, 10, 13 i 16 odcinka koła wzdłuż jego szerokości. Rysunek 9.13 pokazuje dwa, a rysunek 9.14 trzy uszkodzone zęby. Rysunek 9.15 pokazuje w innej skali sytuację w przedziale znacznie krótszym, natomiast rysunek 9.16 ten sam ząb w przypadku najbardziej zaawansowanego uszkodzenia (wtedy się pojawia), tym razem jednak nie rozkładu nacisków powierzchniowych, ale naprężeń gnących w stopie zębnika z_3.

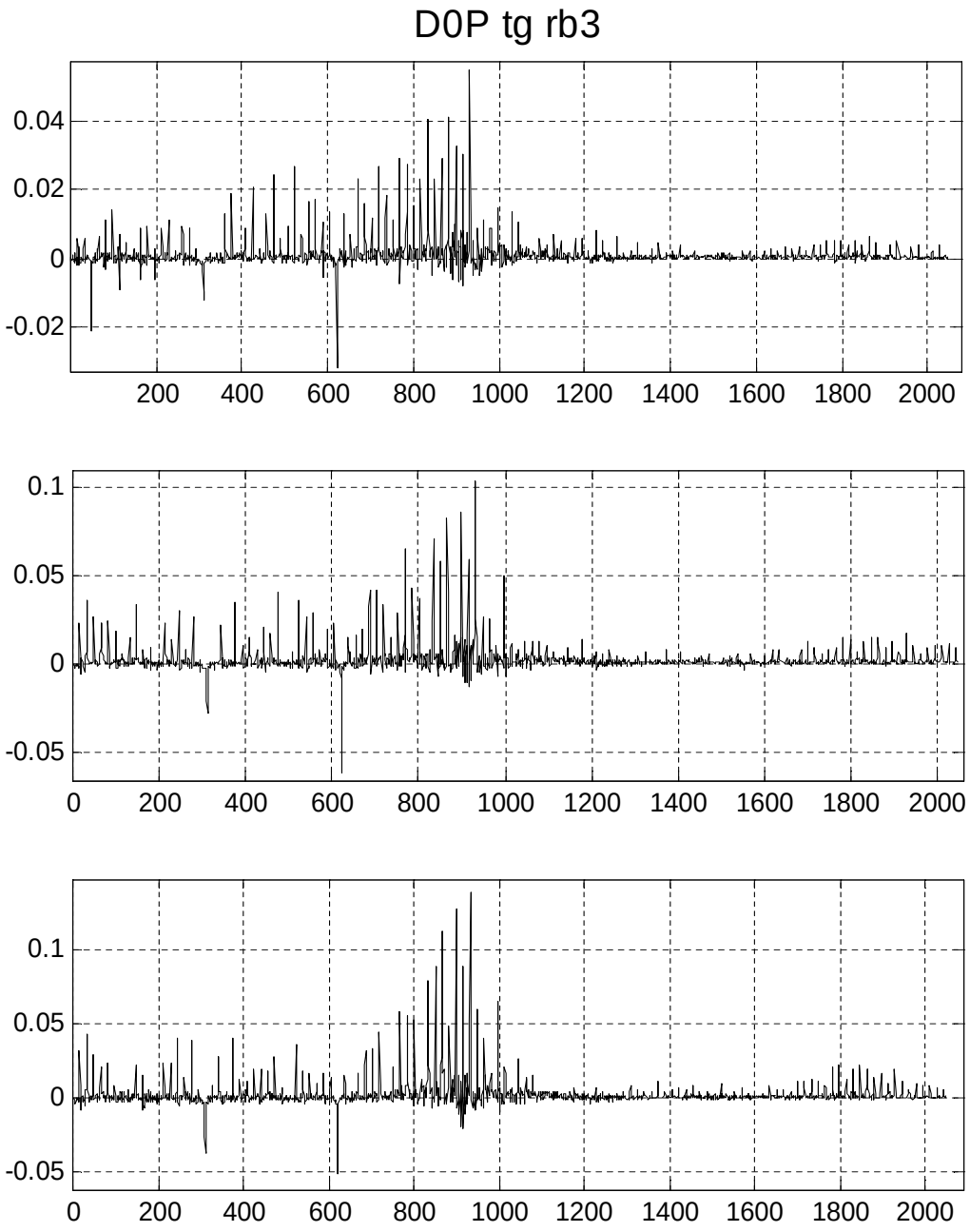
Wybieg ten zastosowano dla potwierdzenia spójności wyników, a zarazem pokazania przykładów odmienności przebiegów czasowych dwóch różnych parametrów.



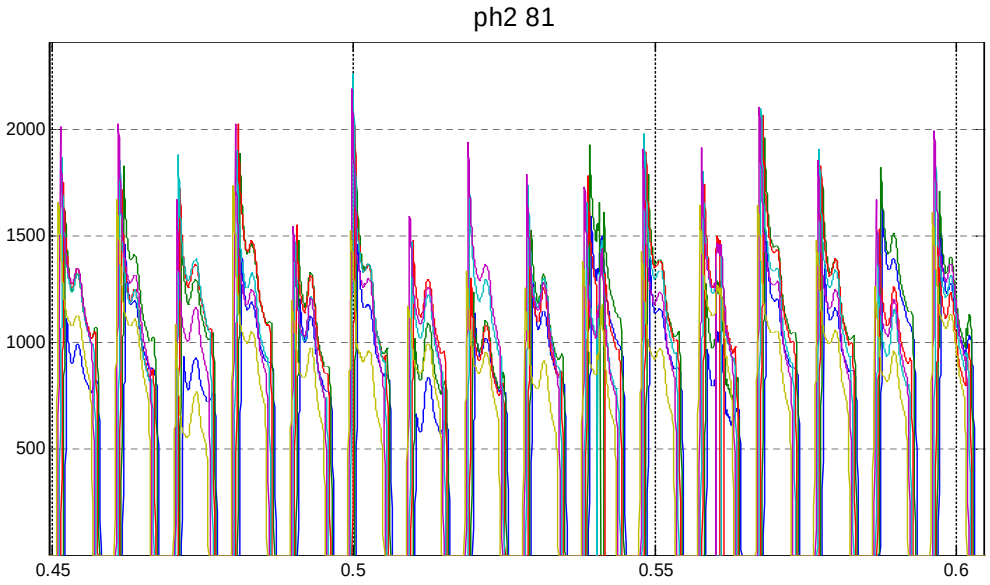
Rys. 9.10: Widma amplitudowe całkowitego przełożenia chwilowego przekładni



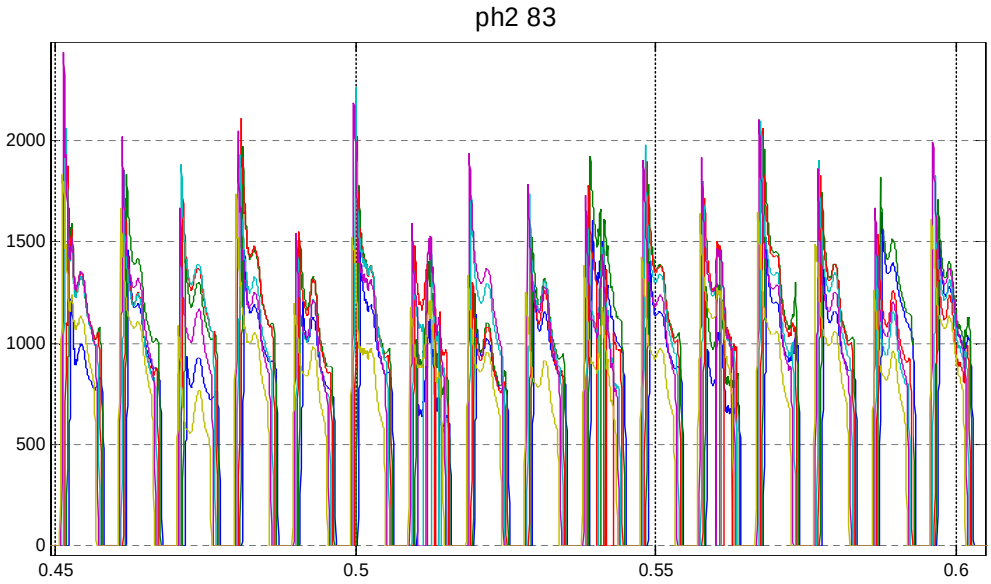
Rys. 9.11: Ewolucja zmian w widmie przełożenia całkowitego



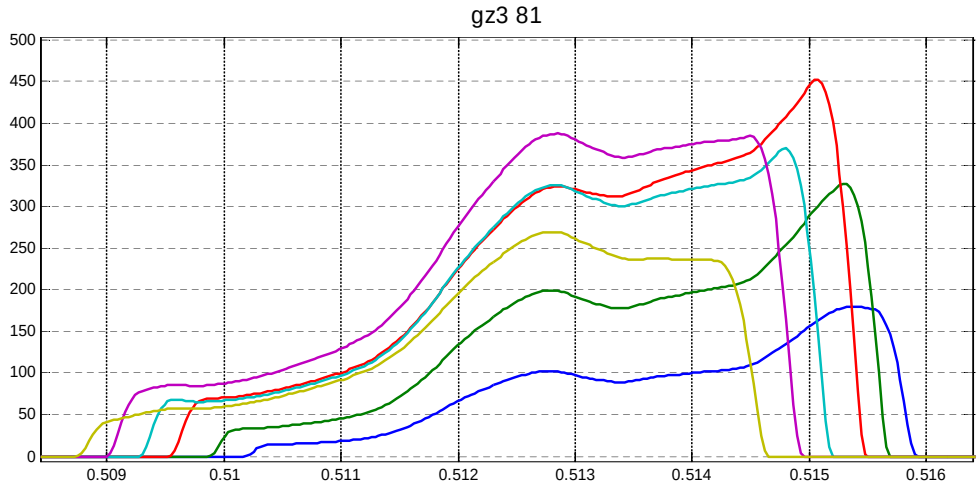
Rys. 9.12: Ewolucja widma kierunku reakcji łożyska R_{b3} przy rozwoju pittingu



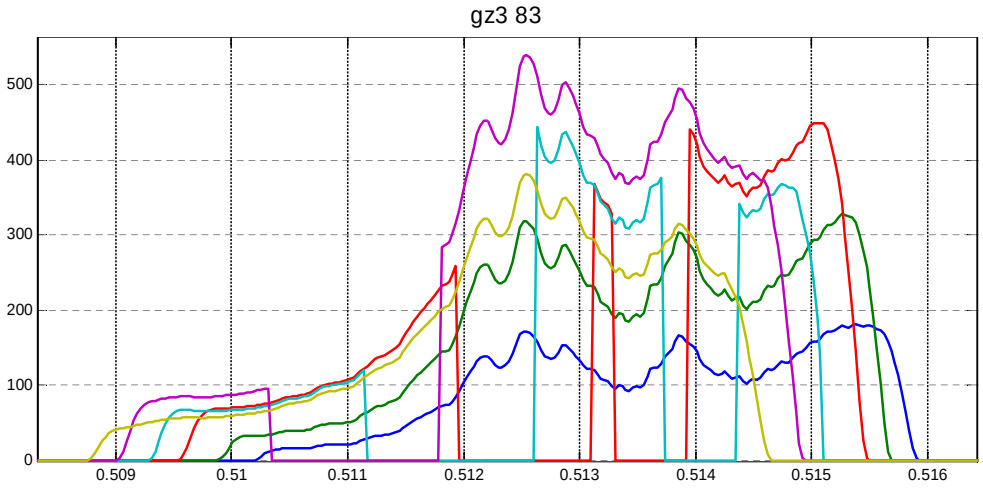
Rys. 9.13: Rozkład nacisków powierzchniowych [MPa] na stopniu drugim przełożenia z uszkodzeniem wg schematu jak na rysunku 9.8 w czasie



Rys. 9.14: Rozkład nacisków powierzchniowych [MPa] na stopniu drugim przełożenia z uszkodzeniem wg schematu jak na rysunku 9.9 w czsie



Rys. 9.15: Rozkład naprężeń gnących [MPa] w stopie z_3 z uszkodzeniem wg schematu jak na rysunku 9.8 w czasie



Rys. 9.16: Rozkład naprężeń gnących [MPa] w stopie z_3 z uszkodzeniem wg schematu jak na rysunku 9.9 w czasie

9.5.2. Symulacja procesu pojawiania się i rozwoju osłabienia w stopie zęba

Do przeanalizowania zagadnienia pojawiania się i rozwoju osłabienia w stopie zęba wykonano kolejno obliczenia analogiczne jak w punkcie poprzednim (bez błędów i z błędem podziałki), a nadto 3 serie obliczeń dla pojawiającego się i rozwijającego osłabienia stopy jednego z zębów również na zębniku z_3

Założono, że osłabienie którego przyczyną może być pojawienie się i rozwój szczeliny zmęczeniowej występuje tylko na jednym zębie w sposób nierównomiernie rozłożony wzdłuż szerokości koła. Przedstawia to schematycznie rysunek 9.17.

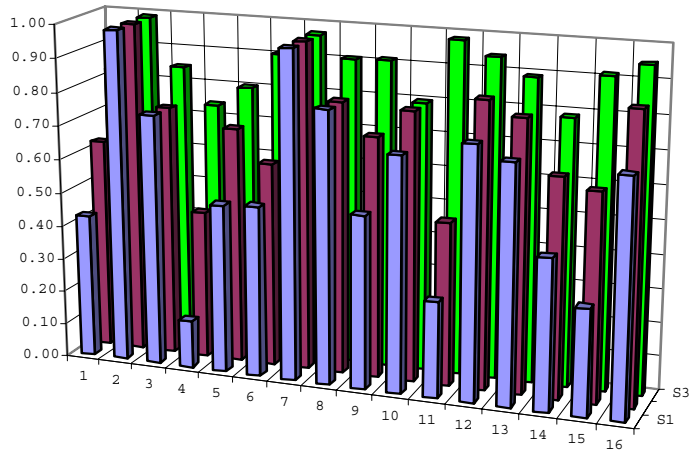
Numerycznie zapisuje się to seriami po 16 wartości (przypadki a, b i c)

a) 0.83, 0.99, 0.85, 0.74, 0.80, 0.91, 0.97, 0.91, 0.91, 0.80, 0.98, 0.94, 0.89, 0.79, 0.91, 0.95

b) 0.63, 0.99, 0.75, 0.44, 0.70, 0.61, 0.97, 0.81, 0.71, 0.80, 0.48, 0.84, 0.80, 0.65, 0.61, 0.85

c) 0.43, 0.99, 0.75, 0.14, 0.50, 0.51, 0.97, 0.81, 0.51, 0.70, 0.28, 0.74, 0.70, 0.45, 0.31, 0.70

Podkreślamy, że podobnie jak poprzednio wybór jest całkowicie arbitralny.



Rys. 9.17: Rozkład stopnia osłabienia stopy zęba nr 7 zębnika z_3

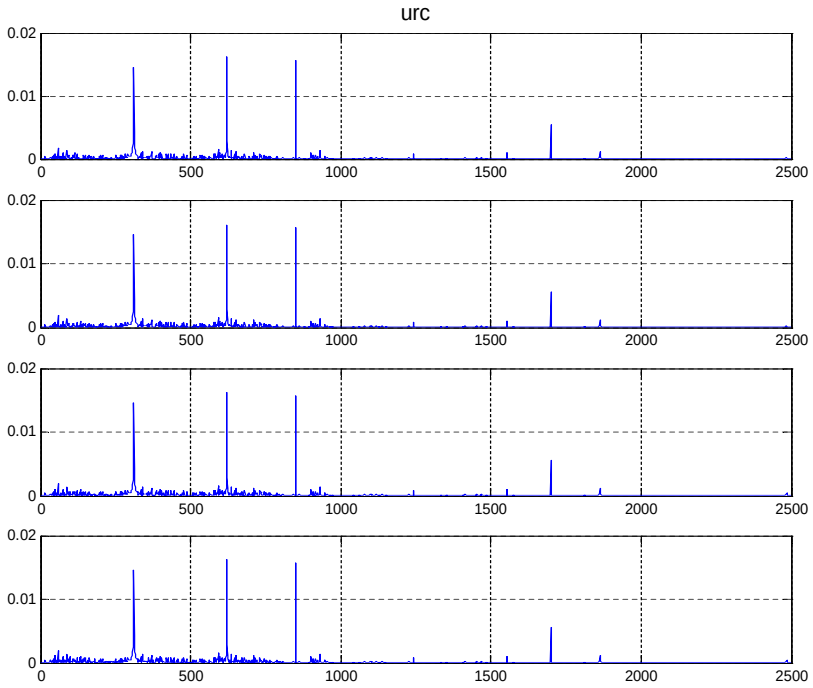
Jak widać ze schematu założono osłabienie na całej szerokości koła narastające nierównomiernie. Do analizy efektów tego zjawiska wybrano jak poprzednio sygnał w postaci przełożenia chwilowego, również dla porównania typów uszkodzenia między sobą. Przedstawia to zestaw widm na rysunku 9.18, gdzie kolejno mamy widmo mocy sygnału przy braku osłabienia, ale z uwzględnieniem błędu podziałki dokładnie tego samego (powtórzone), co w analizie poprzedniej wg rysunku 9.7.

W porównaniu do rozpatrzonego wcześniej zmęczenia powierzchniowego widzimy wyraźną zmianę. Wpływ osłabienia na sygnał wyjściowy jest trudniej zauważalny w tym ujęciu i sytuuje się w zakresie niskich częstotliwości. Zmiany jednak istnieją, co przedstawia rysunek 9.19, sporządzony w odniesieniu do sygnału przed pojawieniem się osłabienia, czyli ilustruje kolejno przypadki a), b) i c).

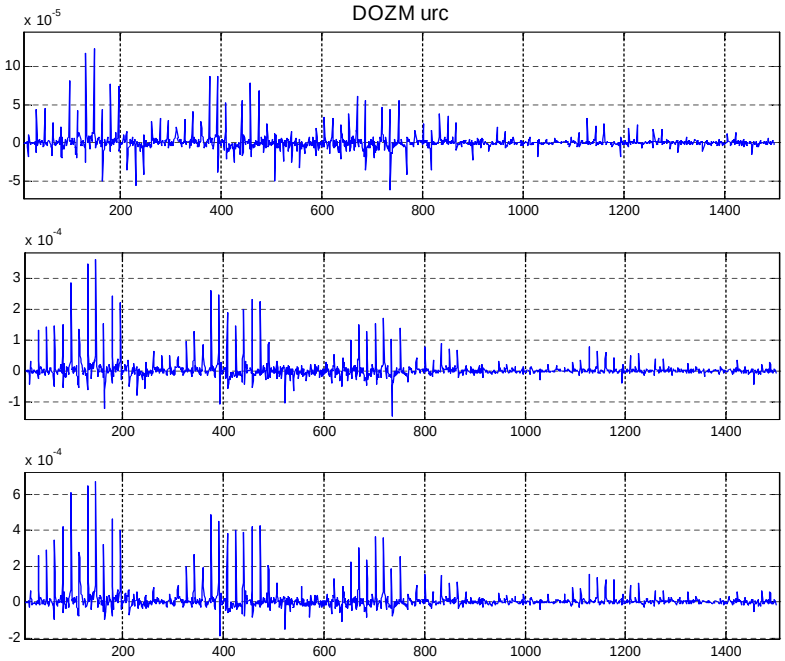
Efekt narastania modyfikacji widma jest niezaprzeczalny, choć w praktyce obserwacji sygnału mierzonego na obiekcie rzeczywistym może pojawić się kwestia czułości użytej aparatury pomiarowej. Jest to jednak problem odrębny, niebędący tutaj przedmiotem rozważań.

Dla analogii z rozważaniami na temat pittingu przedstawiamy teraz analizę sygnału w postaci zaburzenia kierunku reakcji w łożysku wałka wyjściowego bliższego koła k_4**.** Widma tego sygnału przedstawia rysunek 9.20, kolejno od przypadku bez osłabienia do przypadku c) włącznie.

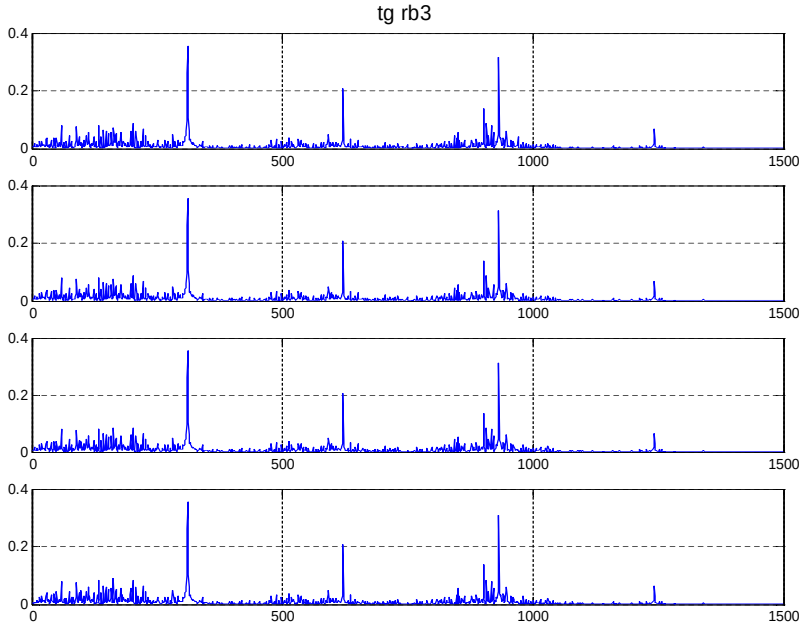
Powtarza się tu ta sama reguła modyfikacji widma w niskim zakresie częstotliwości, co staje się widoczne na wykresie przyrostów widma wyznaczone w odniesieniu do stanu przed pojawieniem się osłabienia przedstawione na rysunku 9.21.



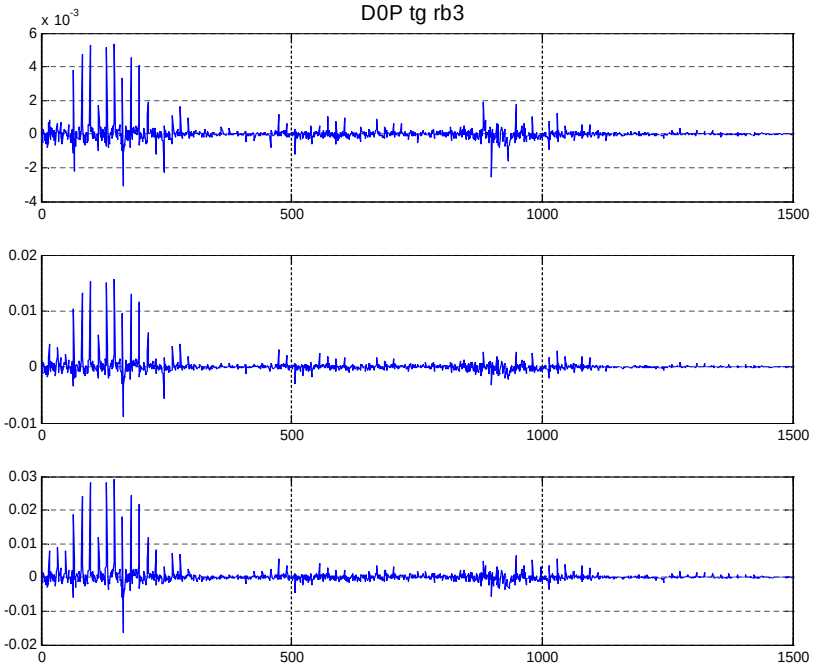
Rys. 9.18: Widma amplitudowe całkowitego przełożenia chwilowego przekładni przy pojawianiu się i narastaniu osłabienia zęba zębnika z_3



Rys. 9.19: Ewolucja widma amplitudowego całkowitego przełożenia chwilowego przekładni przy pojawieniu się i narastaniu osłabienia stopy zęba zębnika z_3



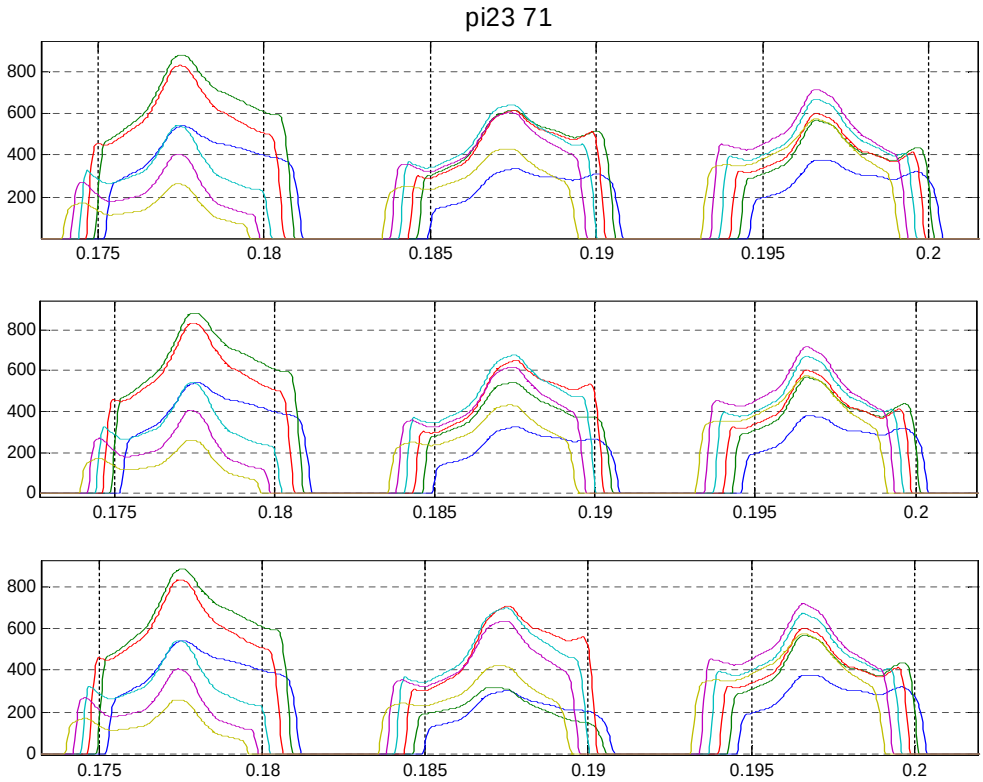
Rys. 9.20: Widma zaburzenia kierunku reakcji R_{b3} przy pojawianiu się i narastaniu osłabienia zęba



Rys. 9.21: Ewolucja widma zaburzenia kierunku R_{b3} po pojawieniu się i rozwoju osłabienia stopy zęba

Wskazuje to na celowość obserwacji takiego sygnałach przy monitorowaniu eksploatacji obiektu technicznego.

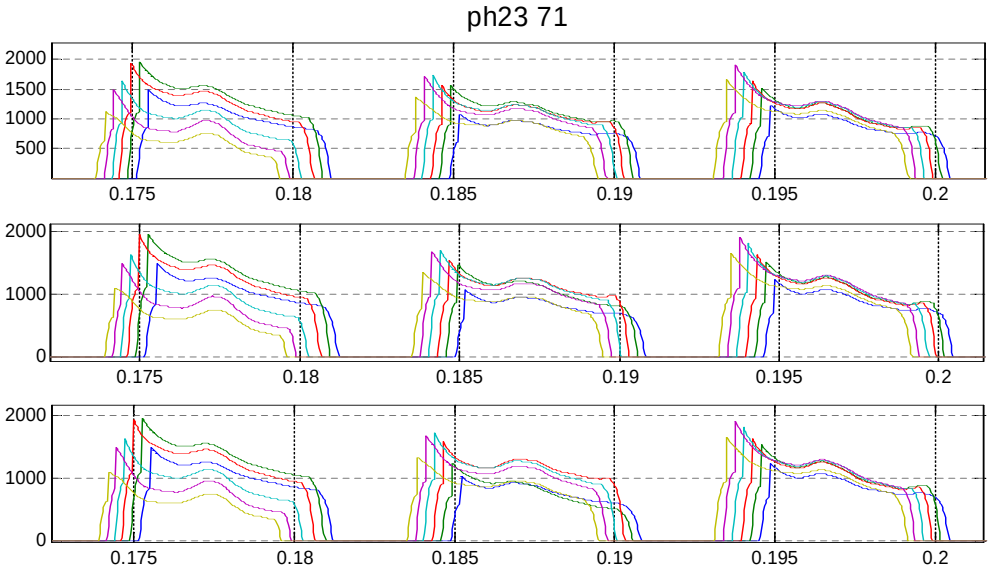
W modelu symulacyjnym możliwe są do obserwowania sygnały niediagnostyczne dotyczące oddziaływań międzyzębnych. W punkcie dotyczącym pittingu przedstawiono rozkłady nacisków powierzchniowych i naprężeń gnących w stopie zębnika. Te ostatnie w przypadku założonej szczeliny w stopie wymagają subtelniejszej metody obliczeniowej, np. MES. Zatem w tym przypadku przedstawione zostaną rozkłady średnich wartości obciążenia liniowego w wybranych przedziałach wzdłuż linii zęba (Rys.9.22), rozkład nacisków powierzchniowych (Rys.9.23) oraz rozkład naprężeń gnących w stopie zęba koła k_4 (Rys.9.24).



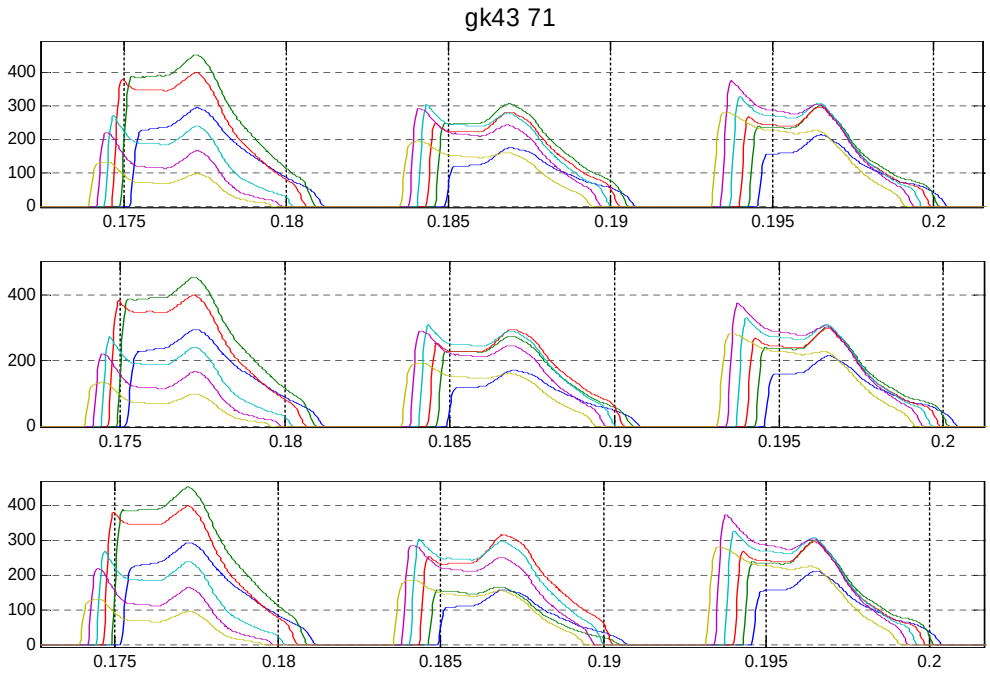
Rys. 9.22: Rozkład obciążenia międzyzębnego stopnia drugiego przekładni [N/mm] w czasie

Podobnie jak poprzednio, dla poprawienia czytelności wykresów, zamieszczono stan dla 1, 4, 7, 10, 13 i 16 odcinka koła wzdłuż jego szerokości. Charakterystyczny jest brak zaniku siły międzyzębnej, bo nie założono szczeliny na wskroś na żadnym odcinku zęba. Ząb osłabiony jest w kontakcie w chwili ok. 0,18s. Efekt dynamiczny jest wprawdzie widoczny, ale umiarkowany. Wynika to zarówno faktu, że zęby są skośne i co za tym idzie, we współpracy jest zawsze więcej niż jedna para zębów.

Jest to również wyjaśnienie relatywnie słabszego efektu wpływu osłabienia zęba na sygnały wyjściowe. Nadto, osłabienie zakładano tylko na jednym, a pitting na dwóch i trzech zębach. Wybór przykładów pozostaje jednak całkowicie arbitralny. Próba detekcji osłabienia tylko jednego zęba w całej przekładni ma na celu również pokazanie wrażliwości modelu symulacyjnego na ten fakt wstrzymując się z komentowaniem otrzymanych wyników.



Rys. 9.23: Rozkład naprężeń powierzchniowych [MPa] w zazębieniu drugiego stopnia przekładni w czasie



Rys. 9.24: Rozkład naprężeń gnących [MPa] w stopie zęba koła **k4** w czasie

9.6. Podsumowanie

Przedstawiony zarys problematyki budowy i wykorzystania symulacyjnego modelu przekładni zębatej, jako ogniwa łańcucha przeniesienia napędu pokazuje efektywność koncepcji. Zakres zastosowań efektywnie zaprogramowanych i przetestowanych modeli obliczeniowych jest znacznie szerszy niż tu przedstawiono. Poszerzanie grupy modelowanych obiektów mechanicznych, mechanicznych uwzględnieniem wewnętrznych struktur bloków napędu i odbioru mocy jest całkowicie realny. Istnieje np. model napędu jednocylindrowej sprężarki powietrza napędzanej silnikiem elektrycznym za pośrednictwem dwustopniowej walcowej przekładni zębatej.

Przedstawione w p. II zasady modelowania być może sugerują tendencję do budowy modeli o maksymalnie rozbudowanej strukturze sterowanej parametrami, choć praktyczniejsze jest chyba przygotowanie oddzielnych modeli dla węższych struktur.

Jednym z akcentów mało widocznych być może w przedstawionym opracowaniu jest pewna zmiana pragmatyki modelowania integralnie związana z powszechnością zastosowań informatycznych, co skutkuje opisami związków fizycznych w postaci hierarchicznej struktury funkcji i procedur właściwych językowi programowania.

Bibliografia

[9.1] Adams E., Keppler H., Schulte U. On the simulation of vibrations of industrial gear drives. *Complex Interactions of Physics, Mathematics, Numerics and Experiments. Archive of Applied Mechanics*, (65):142–160, 1995.

[9.2] Dąbrowski Z., Radkowski S., Wilk A. *Dynamika przekładni zębatych*. Warszawa-Katowice-Radom, 2000.

[9.3] Dziama A., Michniewicz M., Niedźwiedzki A. *Przekładnie zębate*. PWN, Warszawa, 1989.

[9.4] Filonik R. Modelowanie dynamiczne reduktorów dwustopniowych. www.rfilonik.za.pl.

Rozdział 10

Przykłady zastosowań

Kazimierz T. KOSMOWSKI, Jacek ZAWALICH

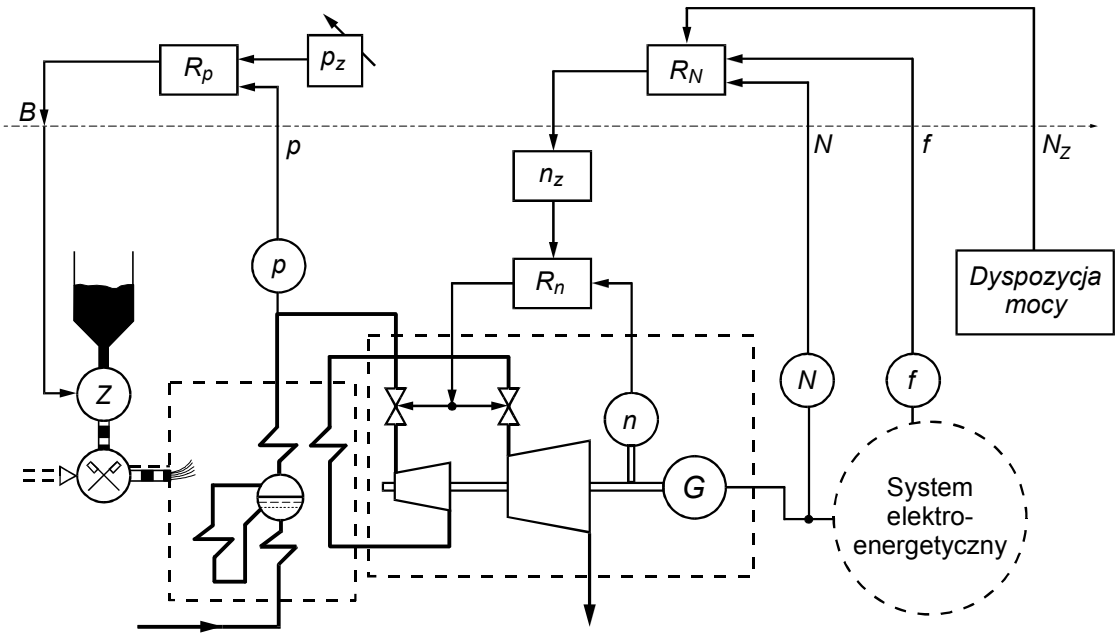
10.1. Przykładowe funkcje systemów sterowania i zabezpieczeń turbozespołu

Konwencjonalny turbozespół w dużym uproszczeniu składa się z kotła do wytwarzania pary pod ciśnieniem, turbiny zamieniającej energię cieplną na energię mechaniczną oraz generatora synchronicznego, który przetwarza energię mechaniczną na energię elektryczną czyli jest to tzw. blok: kocioł-turbna-generator. Przykładowy uproszczony schemat blokowy turbozespołu przedstawiono na Rys.10.1. Dla systemów automatyki blok ten jest obiektem regulacji, w którym przede wszystkim są regulowane takie wielkości, jak: obciążenie bloku, prędkość obrotowa wału, częstotliwość napięcia generatora, temperatura olej w łożyskach, itd. Wielkości te można podzielić na grupę wielkości cieplnych oraz grupę wielkości elektrycznych. Systemy automatyki w elektrowniach obejmują pomiary wielkości fizycznych, ich kontrolę z alarmami przekroczenia niebezpiecznych zakresów oraz sygnalizację aktualnych stanów urządzeń wykonawczych i współpracujących.

Główna rola systemów automatyki skupia się na sterowaniu procesami ciągłymi i na regulacji potrzebnych wielkości procesowych. Niezbędne jest również sterowanie procesami nieciągłymi, jak np. załączenie lub wyłączenie napędów elektrycznych i hydraulicznych, czy zamknięcie lub otwarcie klap i zaworów. Cały blok energetyczny musi być wyposażony w system blokad i zabezpieczeń technologicznych, które są konieczne w sytuacjach nagłych zakłóceń i przy wystąpieniu stanów awaryjnych. Nieodzowne są również systemy informatyczne wspomagające pracę personelu technicznego oraz systemy nadrzędne, który spełniają rolę zarządzająco-administracyjną.

Celem stosowania systemów automatycznego sterowania w elektrowniach jest przede wszystkim polepszenie produkcji energii elektrycznej i cieplnej dostarczanej do użytkownika. Wpływają również dodatnio na zdolności produkcyjne poszczególnych urządzeń elektrowni oraz na ich ekonomiczne uwarunkowania. Przy ich stosowaniu następuje poprawa jakości i warunków pracy personelu technicznego z jednoczesnym ograniczeniem ich liczebności. Jak każdy zakład przemysłowy niosący ze sobą ryzyko występujących zagrożeń, tak i bloki energetyczne są obiektami o podwyższonym ryzyku. W takim przypadku systemy automatyki zwiększają niezawodność i bezpieczeństwo pracy urządzeń elektrowni, jak również zmniejszają negatywne oddziaływanie na otaczające środowisko naturalne.
Do głównych układów regulacji w bloku energetycznym można zaliczyć miedzy innymi [10.8]:

- układ automatycznej regulacji mocy, w którym regulator zmienia stopień otwarcia zaworów regulacyjnych poprzez oddziaływanie na synchronizator, lub bezpośrednio na ciśnienie oleju w układzie elektrohydraulicznym,
- układ automatycznej regulacji ciśnienia pary, który wpływa na zmianę prędkości podajników węgla lub innego paliwa dostarczanego do układu kotłów,



Rys. 10.1: Schemat blokowy układów regulacji bloku kocioł-turbina-generator. R_p – regulator ciśnienia, R_N- regulator obciążenia bloku, R_n – regulator obrotów turbiny, p – ciśnienie, N – obciążenie bloku, f – częstotliwość, B – paliwo, n – obroty turbiny [10.9]

- układy automatycznej regulacji temperatury pary pierwotnej i wtórnej wykorzystujące często wtrysk wody chłodzącej do pary w schładzaczach,
- układy automatycznej regulacji zasilania kotła wodą, których zadaniem jest utrzymanie równowagi między strumieniem dopływu wody a strumieniem pary pobieranej z kotła oddziałując na zawór regulacyjny wody zasilającej lub na prędkość obrotową pompy,
- układ automatycznej regulacji procesu spalania stosowany do utrzymania optymalnej wartość nadmiaru powietrza w celu zapewnienia ekonomicznego spalania,
- układ automatycznej regulacji utrzymującej stałe podciśnienie w komorze paleniskowej za pomocą zmiany wydajności wentylatorów spalin.

Ponadto w bloku energetycznym występuje wiele innych układów sterowania, które są niezbędne do prawidłowego prowadzenia całego procesu. Uszkodzenia poszczególnych podukładów i ich elementów wpływają niekorzystnie na cały proces i mogą być przyczyną różnych uszkodzeń i awarii. Właściwe postępowanie obsługi ruchowej jest w stanie zapobiec dużym awariom, jednak nie wszystkie uszkodzenia są i mogą być wykrywalne.

Systemy sterowania przede wszystkim muszą zapewnić prowadzenie bieżącego ruchu całego bloku z centralnej nastawni w porozumieniu z nadrzędnym centrum dyspozytorskim. W sytuacja awaryjnych muszą dopuszczać uprawnionych operatorów do sterowania ręcznego aparatami lub podukładami wymagającymi zachowania niezbędnych procedur sekwencyjnych. Układy kontrolno-pomiarowe rejestrują istotne parametry turbozespołu i sygnalizują każdą nieprawidłową wykrytą pracę aparatów składowych. Rejestrowane zdarzenia są przechowywane w bazie danych przez okres niezbędny do przeprowadzenia analizy pracy całego bloku energetycznego. Niezbędne są również dane odnośnie sposobów sterowania, zabezpieczeń, obciążenia i awarii innych najbliższych bloków energetycznych. Do celów badań autodiagnostyki i diagnostyki technicznej poszczególne elementy takiego bloku powinny posiadać odpowiednie zestawy czujników, które umożliwią pomiary niezbędnych sygnałów diagnostycznych oraz pozwolą na bezpośrednią (on-line) kontrolę stanu technicznego podzespołów i całego bloku łącznie z wizualizacją tych sygnałów w centralnej nastawni bloku energetycznego. Część układów sterowania i zabezpieczeń pełni funkcje związane z bezpieczeństwem i wymaga stosowania

metod opartych na analizie niezawodności i ryzyka.

Zintegrowana diagnostyka takiego bloku miałaby na celu określenie jego stanu gotowości do realizacji określonych funkcji produkcyjnych oraz funkcji związanych z bezpieczeństwem. Istotne jest uwzględnienie zakłóceń i uszkodzeń wewnętrznych, ale również zakłóceń ze strony systemu elektroenergetycznego. Wynikiem oceny diagnostycznej może być określenie aktualnego stanu bloku, jak również predykcja czasu wejścia systemu w stan zagrożenia, a wiec w stan, w którym praca jest dozwolona tylko przez pewien okres. Przyczynę zakłócenia lub uszkodzenie, należy niezwłocznie zabezpieczyć lub wyeliminować oraz w zależności od sytuacji odizolować od pozostałej części systemu w celu niedopuszczenia do rozprzestrzeniania się awarii. Na bazie zaobserwowanych defektów i uszkodzeń wypracowuje się wskazówki odnośnie dalszych działań prewencyjnych w procesie eksploatacji. Bezpieczna i jednocześnie ekonomiczna praca urządzeń i aparatów elektrowni jest możliwa po zastosowaniu zintegrowanej automatyzacji, w skład której powinny wchodzić układy bezpośrednio wpływające na proces produkcji energii elektrycznej, układy kontrolno pomiarowe, sygnalizacyjne, układy blokad i zabezpieczeń, elementy sterowania napędami podzespołów technologicznych Powinny się tu znaleźć elementy nowoczesnych technik sterowania do których należą m.in. systemy informatyczne SCADA z modułami do centralnej rejestracji i przetwarzania danych (CRPD) oraz do komputerowego wspomagania dyspozytorów bloku (KSWDB) [10.8]

Proces produkcji energii elektrycznej w turbozespołach jest dość specyficznym procesem, gdyż w danej chwili należy wyprodukować tylko tyle tej energii ile są w stanie przejąć odbiorcy – nie ma możliwości zmagazynowania tej energii na przyszły okres. Drugą specyficzną właściwością jest to, że praca poszczególnych urządzeń i zespołów urządzeń jest między sobą ściśle uzależniona i wyłączenie danego urządzenia technologicznego powoduje konieczność dostosowania pracy innego – współpracującego z nim bezpośrednio. Zależności te są jeszcze bardziej skomplikowane przez fakt, iż bardzo istotna jest zarówno kolejność załączeń podczas uruchamiania, jak i zatrzymywania ich pracy. Zabezpieczenia stosowane w blokach turbogeneratorów powodują samoczynne formowanie sygnałów sterujących zapewniających bezpieczeństwo w stanach przejściowych, w stanach normalnej eksploatacji oraz w stanach zakłóceniowych i awaryjnych. Wyróżnia się zabezpieczenia wewnętrzne (lokalne) w odniesieniu do pojedynczych aparatów oraz zabezpieczenia zewnętrzne dotyczące całego turbozespołu. Niezawodności stosowanych zabezpieczeń i blokad jest bardzo istotna w kontekście występowania dużej dynamiki całego bloku, zważywszy na to, iż najczęściej niemożliwa jest właściwa reakcja operatorów podczas sytuacji przejściowych i awaryjnych [10.8].

Dobrym przykładem złożoności urządzeń i podsystemów w blokach energetycznych jest układ regulacji mocy czynnej turbogeneratora działający na strumień pary doprowadzonej do turbiny przez zmianę położenia zaworu regulacyjnego turbiny, bądź przez zmianę wydajności kotła lub poprzez zmianę ilości doprowadzonego paliwa.

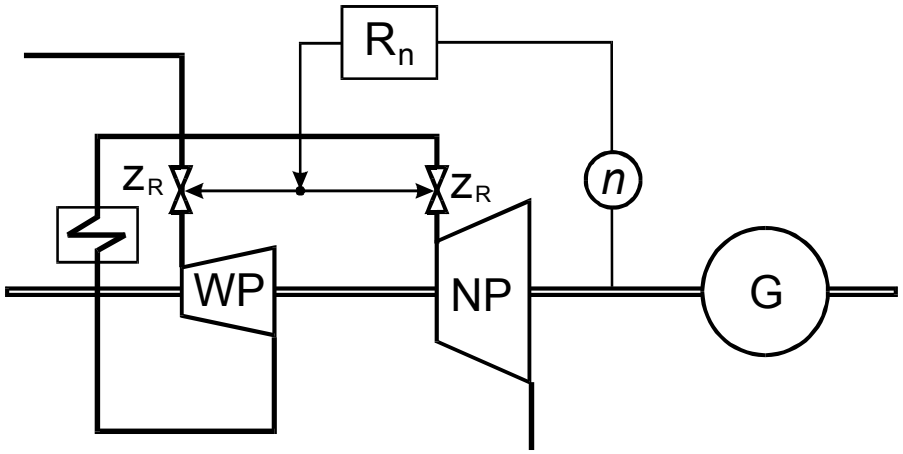
Ważnym i niezbędnym układem jest układ ograniczający szybkość rozruchu i zmian obciążenia, który obejmuje walczak kotła wraz z parownikiem, wężownicami, przegrzewaczem pary, rurociągami oraz z instalacją rozpałową i ruchową. Krytycznym węzłem konstrukcyjnym jest tu połączenie króćca centralnej rury opadowej z płaszczem walczaka, a bezpieczeństwo pracy rur ogrzewanych parownika zapewnia prowadzenie rozruchu z należytym odbiorem pary z kotła. Instalacja ruchowa umożliwia doprowadzenie niezbędnej ilości pary rozruchowej, nagrzewanie komór i rurociągów oraz uzyskiwanie wymaganej temperatury pary świeżej i wtórnie przegrzanej (przy rozruchu turbiny do kontroli pracy kotła wykorzystuje się sygnały o naprężeniach termicznych, informacje o temperaturze wężownic przegrzewacza, informacje o położeniu zaworów regulacyjnych).

Istotne jest bilansowanie się ilości pary produkowanej przez kocioł oraz ilości pary pobieranej przez turbinę (sygnał stałego ciśnienia jest jednoznaczną informacją spełnienia tej równowagi). Klasyczna regulacja obrotów turbiny występuje wówczas, gdy generator jest zsynchronizowany z siecią elektroenergetyczną (przy nadmiernym wzroście obrotów siły odśrodkowe mogą spowodować ocieranie się obluzowanych łopatek o kadłub turbiny). Istotne są charakterystyki układów sterowania, w tym można wyróżnić:

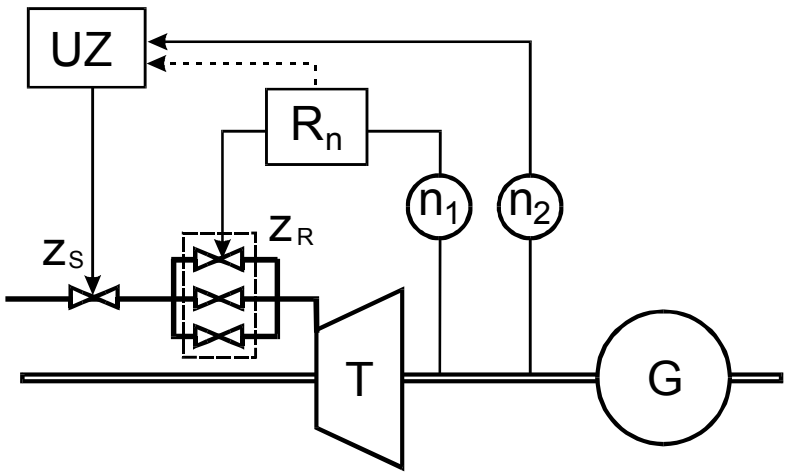
- napędy elektryczne urządzeń pomocniczych kotła,

- napędy elektryczne urządzeń pomocniczych turbiny,
- napędy elektryczne w układach regeneracji, odgazowywania i zasilania pomp wody zasilającej, pomp skroplin z regeneracji oraz pomp oleju do zastosowanych sprzęgieł,
- napędy zestawu klap odcinających, zasuw parowych i wodnych, zasuw elektromagnetycznych i zaworów odcinających,
- napędy organów regulacyjnych (w tym łopatki kierownicze, przekładnie, zawory regulacyjne i inne).

W czasie normalnej eksploatacji turbozespołu układ regulacji obrotów wału jest związany z informacjami o aktualnym obciążeniu całego bloku energetycznego. W okresie rozruchu lub odstawiania (zamierzonego lub awaryjnego) można ten układ uprościć do sytuacji przedstawionej na Rys.10.2. przy założeniu występowania zerowego obciążenia. Na tym przykładzie w sposób poglądowy, można przedstawić istotę systemu zabezpieczeń, który ma niezawodnie działać w sytuacjach awaryjnych lub w czasie trwania rzadko stosowanych procedur technologicznych. Na Rys. 10.3. przedstawiono uproszczony schemat zabezpieczeń z zaworem szybkozamykającym ZS, który pełni funkcję bezpieczeństwa, i powinien być w stanie gotowości przez cały okres eksploatacji. Istotne znaczenie ma w tym przypadku struktura całego układu polegająca na zastosowaniu oddzielnego toru pomiarowego, który poprzez układy napędowe jest w stanie zrealizować awaryjne zatrzymanie całego turbozespołu.



Rys. 10.2: Uproszczony układ regulacji obrotów wału turbozespołu



Rys. 10.3: Uproszczony schemat układu zabezpieczeń z zaworem szybkozamykającym ZS

Awarie mogą wystąpić przy sterowaniu wyłącznikami w sposób bezpośredni lub poprzez przekaźniki pośredniczące. Stosowane są różne napędy (pneumatyczne, elektromagnetyczne, zasobnikowe, sprężynowe, silnikowe, itp.. Zabezpieczenia urządzeń cieplnych w elektrowniach stosowane są w celu szybkiego zlokalizowania uszkodzeń występujących w czasie normalnej pracy, jak również w celu niedopuszczenia, aby jakiekolwiek uszkodzenie stało się przyczyną dalszych uszkodzeń lub awarii pozostałych urządzeń technologicznych.

Z przyczyn ruchowych konieczne jest selektywne zabezpieczanie urządzeń eksploatowanych, tzn. odłączanie tylko tych, które są aktualnie niesprawne, np. w przypadku awaryjne wyłączenia generatora nie zawsze jest celowe wyłączenie kotła z pracy. W przypadku zadziałania zabezpieczeń zewnętrznych bloku powinno nastąpić przełączenie po stronie energetycznej, które spowoduje przejście bloku na zasilanie potrzeb własnych. W przypadku odłączenia bloku, turbina może nadal pracować na biegu jałowym; całkowite odłączenie kotła konieczne jest w przypadku zagrożenia kotła (brak wody, lub nie otwarcie stacji redukcyjnych przy tzw. zrzucie mocy).

Stosowane zabezpieczenia bloku dotyczą różnych sytuacji ruchowych, które mogą wystąpić w sposób przypadkowy [10.9]:

- w sytuacji całkowitego odstawienia bloku:
  - wyłączenie wzbudzenia generatora,
  - wyłączenie głównego wyłącznika bloku,
  - odstawienie turbiny z zamknięciem zaworów szybkozamykających,
  - odstawienie kotła,
- w sytuacji awaryjnego odstawienia turbiny:
  - zamknięcie zaworów szybkozamykających,
  - zamknięcie zasuw pary z upustów turbiny na potrzeby pozablokowe,
  - zamknięcie zasuw pary na upustach turbiny na zasilaniu odgazowywacza,
  - załączenie palników rozpałowych kotła,
- w sytuacji wyłączenia generatora i pozostawienia turbiny na biegu luzem,
- w sytuacji zrzutu mocy do poziomu zasilania potrzeb własnych,
- zrzut mocy wywołany utratą wzbudzenia generatora,
- zrzut mocy bloku wywołany wypadnięciem co najmniej jednej pompy wody zasilającej.

Każdy turbozespół wyposażony jest w zbiór wielu zabezpieczeń i blokad technologicznych oraz sekwencji sterowań w przypadku stanów zakłóceniowych lub awaryjnych. Wyróżnić wśród nich można m.in. [10.9]:
zabezpieczenie od wzrostu ciśnienia pary pierwotnej I i II stopnia,

- zabezpieczenie od wzrostu ciśnienia pary wtórnej,
- zabezpieczenie od wzrostu temperatury pary przed wstawkami zrzutowymi do skraplaczy,
- zabezpieczenie od podwyższonego poziomu wody w walczaku (w I stopniu),
- zabezpieczenie od wzrostu temperatury pary wtórnej (w I stopniu),
- zabezpieczenie przy obniżeniu jasności płomienia w komorze paleniskowej,
- zabezpieczenie minimalnego przepływu wody przez pompę zasilającą
- zabezpieczenie ciśnienia oleju łożyskowego w I i II stopniu
- zabezpieczenie ciśnienia oleju regulacyjnego,
- zabezpieczenie temperatury pary za korpusem WP turbiny,

- zabezpieczenie wzrostu poziomu wody w dolnym przegrzewaczu regeneracyjnym,
- zabezpieczenie przy obciążaniu ciśnienia pary w podgrzewaczu regeneracyjnym,
- zabezpieczenie poziomu wody w podgrzewaczach regeneracyjnych,
- zabezpieczenie przy ograniczeniu obciążenia turbiny,
- zabezpieczenie wewnętrzne urządzeń pomocniczych (wentylatory, młyny węglowe, podajniki węgla, podgrzewacze powietrza, pompy zasilające itd.).

Urządzenia i elementy pracujące w sposób ciągły dostarczają informacji na temat ich właściwości dynamicznych, w tym informacje o przebiegach przejściowych istotnych sygnałów technologicznych, informacje o okresowych zmianach parametrów fizycznych oraz informacje o wartościach tych sygnałów w stanach ustalonych. Na podstawie tych informacji można i należy formułować wytyczne będące wskazówką przy projektowaniu podobnych urządzeń oraz przy ewentualnej modernizacji podsystemów lub pojedynczych elementów charakteryzujących się dużą zawodnością w warunkach ruchowych.

Urządzenia prototypowe nie posiadają bazy danych o ich funkcjonowaniu w warunkach rzeczywistych, dlatego też projektant powinien przewidzieć ich pracę na podstawie informacji o pracy urządzeń o podobnych funkcjach i właściwościach. Takie urządzenia powinny mieć szczególnie mocno rozbudowane elementy do prostego i szybkiego diagnozowania ich stanu pracy zarówno w warunkach statycznych, jak i w dynamicznych. Jest rzeczą oczywistą, że określanie stanu technicznego danego urządzenia łączy się nierozerwalnie z różnymi etapami życia zarówno pojedynczego elementu, jak i całego systemu, w tym szczególnie obiektu krytycznego. Obsługa profilaktyczna urządzeń obiektu złożonego ma na celu nie dopuszczenie do wystąpienia zjawisk zużycia lub starzenia.

Maszyny, a szczególnie obiekty krytyczne wyposaża się w system sterowania pełniący funkcje związane z bezpieczeństwem lub w warstwowy system zabezpieczeń. Ryzyko stanów awaryjnych takiego obiektu zależy od zaprojektowanych funkcji oraz niezawodności systemu sterowania, alarmów i automatyki zabezpieczeniowej. Projektowanie i użytkowanie takich systemów odbywa się na podstawie analiz i ocen ryzyka.

Na niezawodność i bezpieczeństwo obiektu krytycznego wpływa więc wiele czynników natury technicznej, ale również organizacyjnej, które wpływają istotnie na kształtowanie czynników ludzkich, a te z kolei determinują jakość pracy i niezawodność personelu operatorskiego w sterowni i personelu obsługi (obsługa profilaktyczna wyposażenia oraz remonty bieżące i planowane). Ryzyko eksploatacji turbozespołu można więc redukować w różny sposób, kształtując czynniki ludzkie i organizacyjne oraz za pomocą systemów związanych z bezpieczeństwem w tym systemów sterowania i automatyki zabezpieczeniowej. Są one realizowane obecnie coraz częściej w technologii programowalnej (w celu uzyskania odpowiedniej elastyczności funkcjonalnej). W ich projektowaniu i eksploatacji powinno się wówczas korzystać z zasad i kryteriów bezpieczeństwa funkcjonalnego.

W związku ze znaczeniem czynników ludzkich, w tym prawidłowego reagowania operatorów w sytuacjach nienormalnych i awaryjnych istotne znaczenie ma opracowanie procedury operacyjnych i awaryjnych, które powinny być weryfikowane w czasie w miarę zdobywania doświadczenia eksploatacyjnego [10.7], [10.5]. Nowe wyzwania dla badań wyłaniają się w związku z coraz szerszym stosowaniem systemów sterowania i automatyki zabezpieczeniowej związanych z bezpieczeństwem. Do przykładowych funkcji związanych z bezpieczeństwem turbozespołu energetycznego realizowanych przez systemy programowalne (BPCS i/lub SIS) oraz operatora w nastawni blokowej, z których część wymaga dalszych pogłębionych analiz i zbadania wpływu na ryzyko eksploatacji, proponuje się zaliczyć następujące funkcje:

A. Funkcja kontroli stanu turbozespołu podczas uruchamiania i obciążenia turbozespołu,

B. Funkcja redukcji mocy turbozespołu przy uszkodzeniach wyposażenia turbozespołu,

C. Funkcja zapewnienia operatorowi informacji i możliwości wpływania na przebieg procesu po awarii podstawowych układów sterowania / regulacji i awarii BPCS,

D. Funkcja przejścia turbozespołu do pracy na potrzeby własne,

E. Funkcja ograniczania prędkości kątowej turbozespołu przy zrzucie obciążenia,

F. Funkcja sterowania turbozespołem przy zakłóceniach przejściowych w systemie elektroenergetycznym,

G. Funkcja odstawienia turbozespołu z powodu uszkodzeń wewnętrznych lub w torze wyprowadzania mocy.

Wybrane z wymienionych wyżej funkcji mogłyby być zaimplementowane w ramach prototypowego systemu doradczego zawierającego system z bazą wiedzy do dynamicznej oceny stanu obiektu i oceny ryzyka do wykorzystania przez operatora zespołu blokowego i służby utrzymania ruchu. Niemniej należy wspomnieć, że istotny wpływ na ryzyko wystąpienia poważniejszej awarii mają systemy sterowania i automatyki zabezpieczeniowej związane z bezpieczeństwem, odpowiednio zaprojektowane i użytkowane zgodnie z zasadami i kryteriami bezpieczeństwa funkcjonalnego.

10.2. Konstruowanie przykładowych sieci stwierdzeń dla celów diagnostycznych

Ryzyko związane z eksploatacja energetycznego bloku turbogeneratora zależy od różnych czynników i rozwiązań natury technicznej i organizacyjnej oraz stosowania odpowiedniego oprogramowania w systemie komputerowym oraz programowalnych systemach sterowania i automatyki zabezpieczeniowej. Analizę ryzyka powinno się przeprowadzać już na etapie projektowania obiektu złożonego, a szczególnie jest ona ważna podczas eksploatacji. Ryzyko takich systemów kształtowane jest w całym cyklu życia obiektu. Opisane metody diagnozowania stanu obiektu opisane w opracowaniach [10.6] mogłyby być wykorzystane w ramach systemu z bazą wiedzy do wspomagania decyzji operatorskich w zakresie funkcji B i G wymienionych powyżej. Mają one związek głównie ze wspomaganiem decyzji operatorskich w systemie zabezpieczeniowo-ochronnym. Ogólne zasady projektowania takiego systemu zawarto w dokumencie technicznym IAEA [10.5].

Jak wiadomo, system zabezpieczeniowo-ochronny traktowany jako system związany z bezpieczeństwem, ze względu na swoją złożoność, umożliwia redukcję ryzyka tylko na poziomie nienaruszalności bezpieczeństwa SIL1. Ponadto, w analizie ryzyka należy również uwzględnić operatora w sterowni i odpowiedni system SIS (lub E/E/PE). Ich ocena probabilistyczna oparta jest odpowiednio na modelu niezawodności człowieka i modelu probabilistycznym systemu SIS (lub E/E/PE). Poprawnie zaprojektowany system doradczy (z bazą wiedzy) wykorzystujący sieci bayesowskie mógłby przyczynić się do zmniejszenia prawdopodobieństwa błędu człowieka, a tym samym redukcji ryzyka.

W przypadku stwierdzenia trendu niekorzystnej zmiany stanu obiektu lub wystąpienia uszkodzeń częściowych celowe byłoby podejmowanie decyzji opartych na dynamicznym systemie oceny ryzyka. W przypadku przejścia obiektu w obszar stanów niedopuszczalnych lub przekroczenia odpowiednio zdefiniowanych wartości progowych ryzyka (ryzyko definiowane probabilistycznie) powinna nastąpić decyzja o wyłączeniu obiektu lub jego przejściu w odpowiedni stan. W tym drugim przypadku niezbędna jest znajomość stanów elementów (zdatny lub niezdatny), które byłyby uwzględnione w uprzednio opracowanym modelu ryzyka (prawdopodobieństwa przebywania elementu w stanie niezdatności równe 1 dla niezdatnego elementu). Spowoduje to znaczny wzrost prawdopodobieństwa i ryzyka związanego z danym scenariuszem awaryjnym a zatem przesunięcie do góry punktu odpowiadającego temu scenariuszowi na matrycy ryzyka.

Przy projektowaniu takiego systemu doradczego należy przeanalizować obowiązujące dla danego obiektu procedury operacyjne/awaryjne, gdyż operator jest zobowiązany prawnie do ich przestrzegania [10.5]. Wspomniany system doradczy mógłby obejmować te procedury, docelowo również dla pozostałych funkcji związanych z bezpieczeństwem (A, C, D, E i F). W opracowywaniu takich procedur (np. zorientowanych na symptomy lub przyczynę stanu nienormalnego) warto skorzystać z wiedzy zgromadzonej podczas eksploatacji turbozespołów w elektrowniach jądrowych [10.4], [10.3].

Coraz częściej do sterowania złożonymi instalacjami technologicznymi stosuje się systemy doradcze o różnych strukturach wykorzystujących bazę wiedzy pozyskiwaną z różnych źródeł w tym

również dane pomiarowe (gdy jest dostępna maszyna rzeczywista), eksperckie oraz wiele innych relacji przyczynowo-skutkowych. Systemy te zalicza się do metod sztucznej inteligencji, które coraz częściej i chętniej są stosowane w różnorodnych rozwiązaniach technicznych. Główna zaletą takich systemów jest bezpośrednie i wielokrotne korzystanie z zapisanych danych w sytuacjach, gdy podjęcie decyzji wiąże się z różnymi aspektami zaistniałego zdarzenia. Wiele systemów doradczych wykorzystuje wnioskowanie zgodne z zasadami logiki klasycznej. Powstaje wówczas baza wiedzy złożona z reguł o strukturze przesłanka-konkluzja. Złożone reguły wnioskowania mogą tworzyć dowolne łańcuchy, w których konkluzja danej reguły jest jednocześnie przesłanką w następnej regule. Odpowiednio zbudowane moduły objaśniające pozwalają weryfikować proponowane wnioski z własną wiedzą i utwierdzić w przekonaniu o ich prawdziwości. Wiedza zapisana w tych systemach może dotyczyć zaistniałych faktów lub procedur postępowania w sytuacjach nienormalnych.

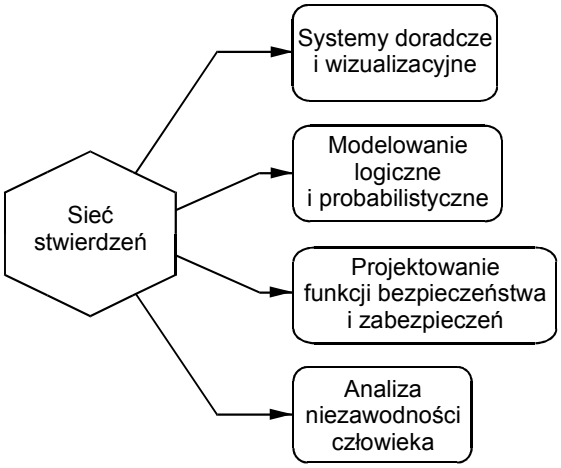
Systemy doradcze oparte o dokładne reguły wnioskowania są jednak mocno ograniczone, gdyż nie pozwalają na korzystanie z niedokładnych opinii ekspertów. W takim przypadku tylko stosowanie przybliżonych systemów doradczych umożliwia wykorzystanie przybliżonych lub niepełnych reguł łączących przesłanki z konkluzjami. W literaturze opisywane są różne metody wnioskowania w tym różnorodne grafy, sieci Markowa, jak również sieci przekonań i stwierdzeń [10.1].

W sieciach stwierdzeń wyróżniane są stwierdzenia pierwotne i wtórne mające postać zdań logicznych z dokładnym opisem ich interpretacji. Sieć ta ma możliwość korzystania z przybliżonych warunków koniecznych i dostatecznych. Dzięki temu wnioskowanie w takiej sieci uwzględnia przedziały wartości stopnia prawdziwości stwierdzenia lub stopnia przekonania o jego prawdziwości. Sieci stwierdzeń można zastosować do budowania systemów doradczych i wizualizacyjnych wspomagających podejmowanie decyzji operatorom instalacji krytycznych. Nagromadzona baza wiedzy pomocna jest również przy modelowaniu logicznym oraz probabilistycznym obiektów wymagających pozyskiwanie danych z różnych źródeł. Projektowanie funkcji bezpieczeństwa i zabezpieczeń nie powinno być pozbawione danych uzyskanych z sieci stwierdzeń, szczególnie przy posługiwaniu się metodami jakościowych analiz ryzyka. Sieć stwierdzeń jest również pomocna przy analizowaniu niezawodności człowieka, który w wielu przypadkach jest istotnym czynnikiem sprawczym przy awariach i poważniejszych uszkodzeniach.

Ostatnio powstał system DiaDyn [10.1] przy zastosowaniu oprogramowania Dragonfly CMS (ang. Content Management System), należącego do z grupy *systemów zarządzania treścią*. System pracuje na zasadzie aplikacji serwerowej z dostępem dozwolonym tylko dla zarejestrowanych użytkowników z poziomu dowolnej przeglądarki internetowej zainstalowanej na sieciowej końcówce roboczej (dopuszczona jest praca w dowolnym systemie operacyjnym). W systemie DiaDyn mamy możliwość redagowanie i tworzenie sieci stwierdzeń oraz ich analizowania. Podstawowym elementem reprezentacji wiedzy przyjętym w systemie DiaDyn jest stwierdzenie. Do wprowadzenia zestawu stwierdzeń oraz ich uporządkowania w słownikach stwierdzeń służy moduł Dia_Wiki, stworzony na bazie dystrybucji systemu PmWiki (system zastosowany przy konstruowaniu np. Wikipedii). Użytkownik ma dodatkowo możliwość dokładnego opisywania zasobów wiedzy za pomocą systemu haseł łączonych w tematy typu: opis bibliografii i opis autorów stwierdzeń. Zadania analizy oraz uruchomienia procesów wnioskowania zostały zrealizowane w module Dia_Sta, w którym mamy możliwość stworzenia (na podstawie wcześniej przygotowanych słowników stwierdzeń) sieci stwierdzeń oraz drzew stwierdzeń. W sieci stwierdzeń określamy sposób połączenia i wzajemnego wpływu na siebie poszczególnych stwierdzeń-węzłów sieci. Wpływ węzłów nadrzędnych na podrzędne określamy za pomocą tablic prawdopodobieństw warunkowych. W celu uruchomienia i przeprowadzenia procesu wnioskowania należy zdefiniować zadanie na podstawie utworzonej sieci stwierdzeń oraz określić parametry początkowe węzłów tej sieci.

Opracowany system można wykorzystać w wielu celach, m.in. do budowy systemów doradczych i wizualizacyjnych, w modelowaniu probabilistycznym, w analizie niezawodnościowej człowieka w projektowaniu funkcji bezpieczeństwa, funkcji zabezpieczeń itp. (Rys.10.4).

Dobrym przykładem zastosowania tego systemu jest wynik prostego wnioskowania na bazie słownika stwierdzeń zbudowanego dla zaworu szybkozamykającego przeznaczonego do eksploatowania w



Rys. 10.4: Zastosowania dla sieci stwierdzeń i reguł wnioskowania

turbozespołach (Rys.10.5). Kolejne stwierdzenia są zdaniami oznajmującymi, np.:

- główny trzpień zaworu w położeniu górnym,
- brak sygnału z czujnika górnego położenia trzpienia głównego zaworu,
- rygiel w położeniu aktywnym,
- brak sygnału z czujnika sterowania ryglem,
- brak ciśnienia zasilającego,
- zawór szybkozamykający jest otwarty,
- medium robocze przepływa,
- sprawdzić źródło zasilania ciśnieniem,
- występują drgania zaworu.

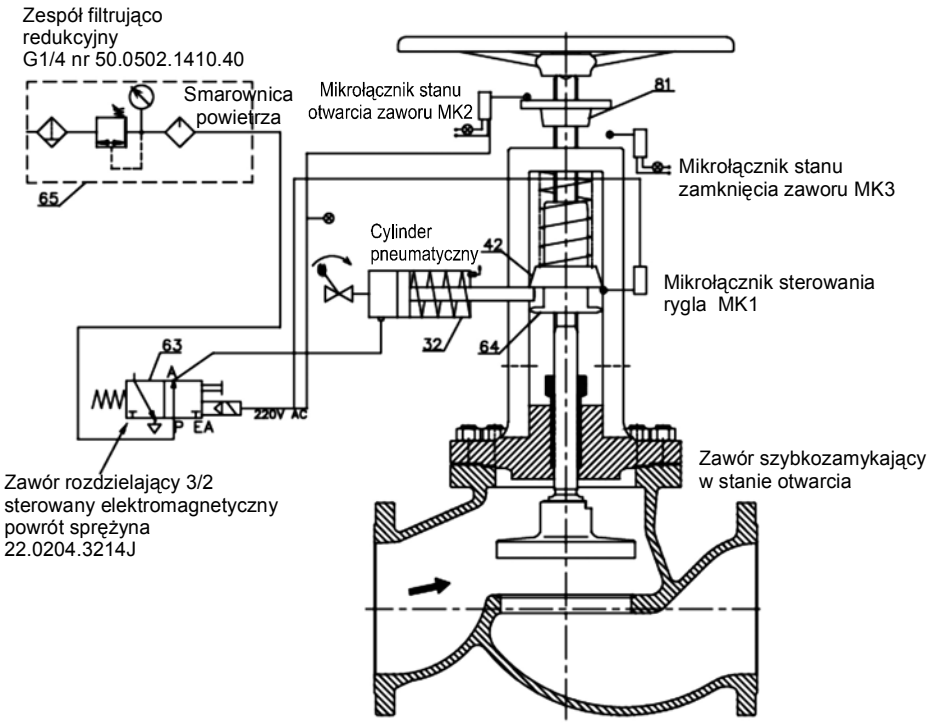
Zawór taki stosuje się do szybkiego odcięcia przepływu czynnika w instalacjach technologicznych. Zadziałanie zaworu powinno nastąpić po wysłaniu sygnału inicjującego, np. po zaniku sprężonego powietrze lub po zaniku sygnału elektrycznego.

W czasie produkcji zawór jest sprawdzany i doszczelniany na stanowiskach testowych i nie wymaga dodatkowej obsługi. Jednak w przypadku zaobserwowania niepokojących symptomów, należy niezwłocznie przeprowadzić dodatkowe testy a w razie potrzeby wymienić na nowy.

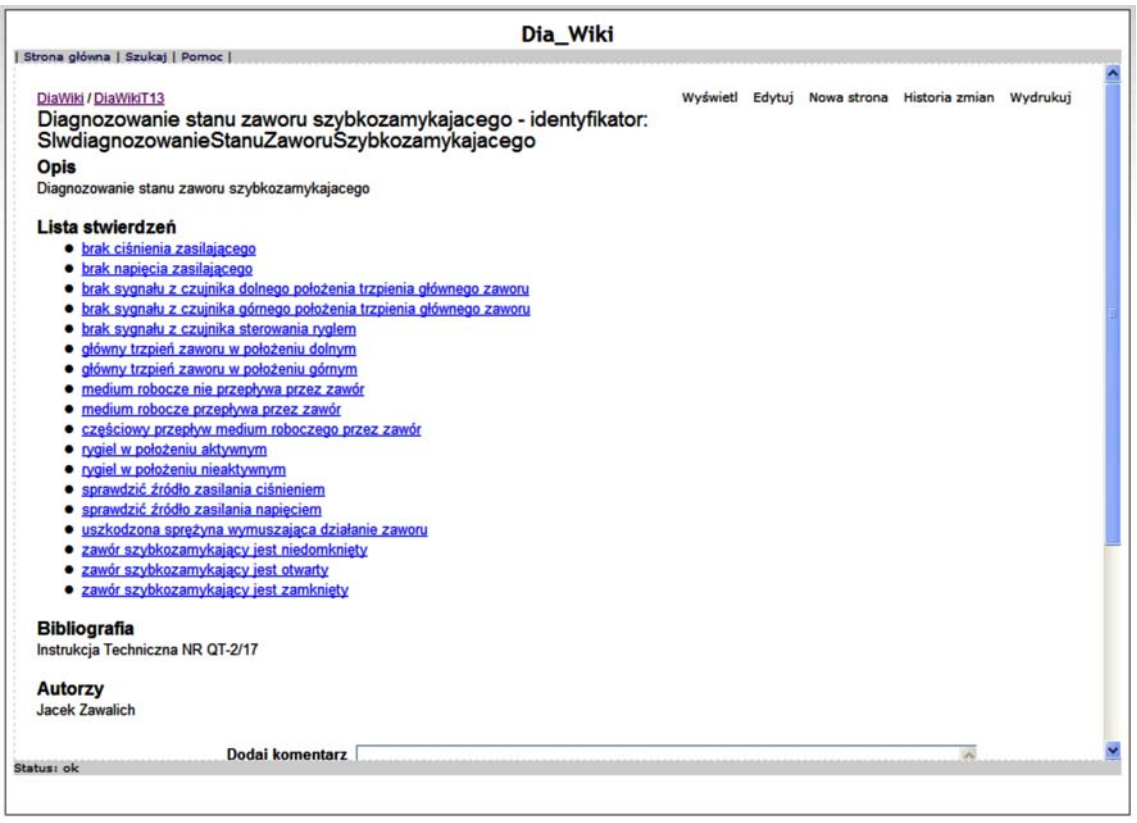
Dla każdego zaworu szybkozamykającego niezbędne jest prowadzenie właściwej konserwacji i obsługi ruchowej przez uprawniony do tego, wykwalifikowany personel techniczny. Ponadto należy przestrzegać zasad wymaganych w instrukcji w celu uniknięcia awarii samego zaworu oraz całej instalacji związanej z bezpieczeństwem całej turbiny. Firma produkującą urządzenie przestrzega przyszłych użytkowników przed niewłaściwą eksploatacja aparatu, która może prowadzić do wystąpienia zarówno szkód materialnych jak i ciężkich obrażeń wśród personelu obsługi. Przykładowa sieć stwierdzeń może stanowić podstawę do budowy bazy danych w systemie ekspertowym.

Pełną postać słownika można wizualizować w oknie systemu Dia_Wiki łącznie z dokładnymi opisami każdego z nich (Rys.10.6).

Wprowadzona lista stwierdzeń pozwoliła na zbudowanie sieci stwierdzeń, którą można traktować jako element bazy wiedzy o właściwościach i funkcjach krytycznego elementu wykonawczego, czyli zaworu szybkozamykającego, czuwającego nad bezpieczeństwem całej turbiny. Od jego niezawodności i gotowości zależy prawidłowe i bezawaryjne prowadzenie procesów przejściowych i awaryjnych całego turbozespołu. Na podstawie przygotowanego w module Dia_Wiki słownika stwierdzeń, przygotowano sieć stwierdzeń w module Dia_Sta *diagnozowanie stanu zaworu szybkozamykającego.* Na Rys.10.7 przedstawiono okno z wprowadzonym przykładowym węzłem *medium robocze nie przepływa przez*

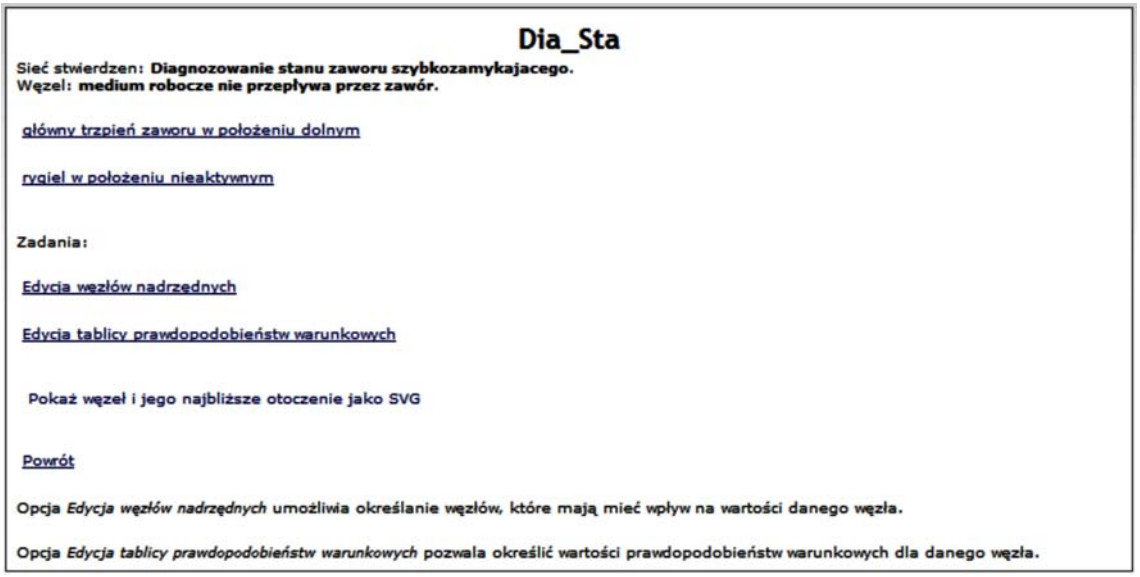


Rys. 10.5: Schemat sterowania zaworu szybkozamykającego [10.2]

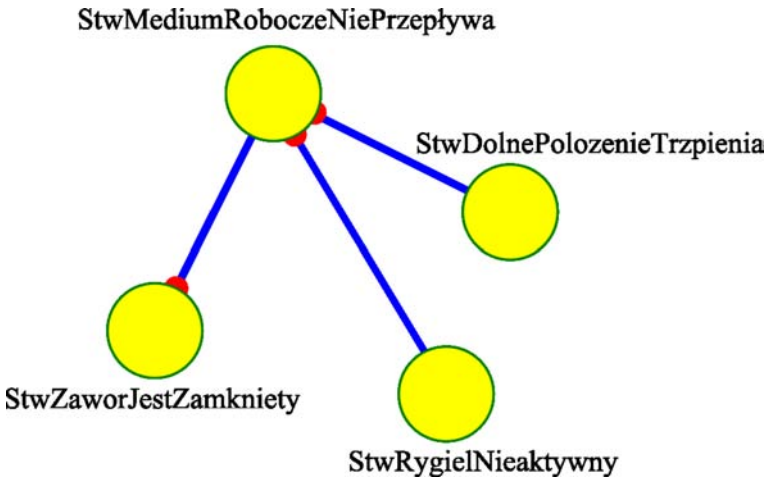


Rys. 10.6: Okno systemu Dia_Wiki z wprowadzoną listą stwierdzeń dla zaworu szybkozamykającego

zawór oraz dwoma węzłami nadrzędnymi: *główny trzpień zaworu w położeniu dolnym* oraz *rygiel w położeniu nieaktywnym*. Tak utworzoną sieć stwierdzeń można przedstawić graficznie w oknie wizualizacji (Rys.10.8, Rys.10.9).



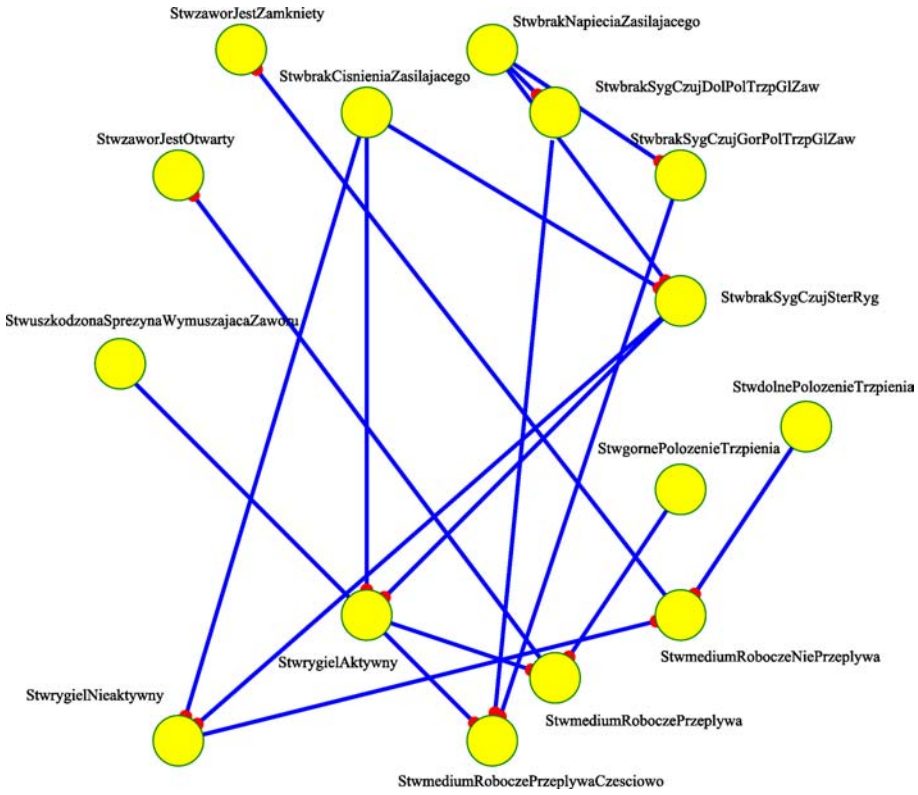
Rys. 10.7: Okno systemu Dia_Sta z wprowadzonymi węzłami sieci stwierdzeń



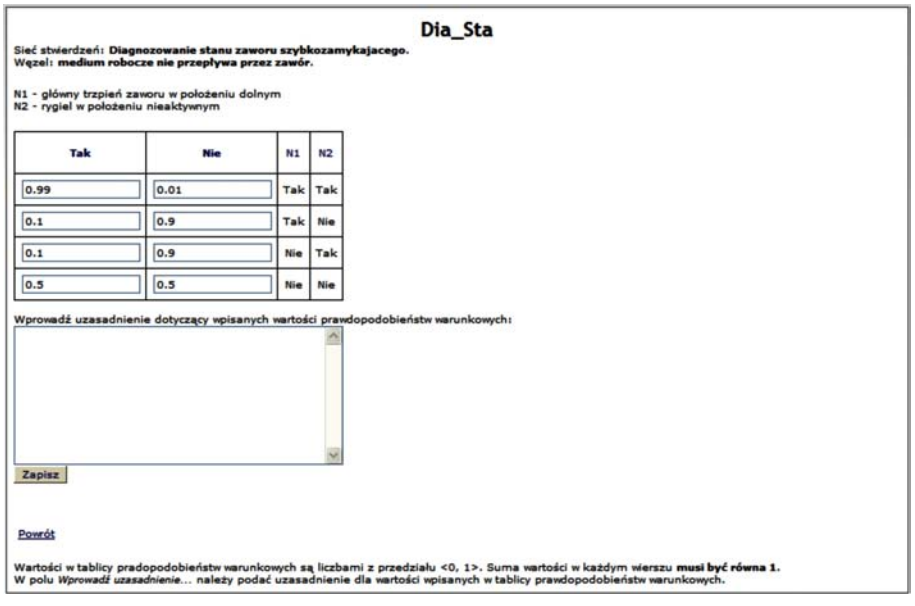
Rys. 10.8: Wizualizacja sieci stwierdzeń dla pojedynczego węzła nadrzędnego

Projektowanie i realizacja systemów eksperckich i diagnozujących dla nowoprojektowanych bloków energetycznych jest zagadnieniem bardzo złożonym. Różnorodne struktury systemów, z różną ich wewnętrzną filozofią funkcjonowania, mogą powstawać w zależności od konkretnych zespołów projektowych. Jednak w każdym przypadku systemy z bazą wiedzy, oparte o długookresowe doświadczenia w istniejących obiektach technicznych o podobnych strukturach, są niezbędne do wspomagania decyzji podejmowanych przez operatorów w konkretnych warunkach ruchowych obarczonych różnymi zakłóceniami wewnętrznymi i zewnętrznymi.

Dla każdego utworzonego węzła podrzędnego można zbudować tablicę prawdopodobieństw warunkowych. Przykładowo na Rys.10.10 umieszczono okno dla węzła sieci stwierdzeń *medium robocze nie przepływa przez zawór* z przykładowymi danymi dla węzłów nadrzędnych N1- *główny trzpień zaworu w położeniu dolnym* oraz N2- *rygiel w położeniu aktywnym*.



Rys. 10.9: Wizualizacja sieci stwierdzeń dla kilku węzłów nadrzędnych



Rys. 10.10: Okno wprowadzania prawdopodobieństw warunkowych z dwoma węzłami nadrzędnymi

Bibliografia

[10.1] Cholewa W. Materiały seminaryjne z warsztatów diadyn. Raport instytutowy, Katedra Podstaw Konstrukcji Maszyn, Politechnika Śląska, Gliwice, 06.11.2007 2007.

[10.2] FAP WAKMET. *Instrukcja techniczna nr QT-2/17 Dokumentacja techniczno-ruchowa. Zawór szybkozamykający kołnierzowy prosty sterowany pneumatycznie. Nr katalogowy 231/S*.

[10.3] International Atomic Energy Agency, Vienna. *IAEA-Safety Series No. 50-P-4: Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)*, 1992.

[10.4] International Atomic Energy Agency, Vienna. *IAEA-TECDOC-658: Safety related maintenance in the framework of the reliability centered maintenance concept*, 1992.

[10.5] International Atomic Energy Agency, Vienna. *IAEA-TECDOC-1019: Use of computers to enhance nuclear power plant diagnosis and operator response*, 1998.

[10.6] Kiciński J. *Modelowanie i diagnostyka oddziaływań mechanicznych, areodynamicznych i magnetycznych w turbozespołach energetycznych*. IMP-PAN, Gdańsk, 2005.

[10.7] Kosmowski K.T. *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Monografie 33. Wydawnictwo Politechniki Gdańskiej, Gdańsk, 2003.

[10.8] Laudyn D., Pawlik M., Strzelczyk F. *Elektrownie*. WNT, 2000.

[10.9] Rakowski J. *Automatyka cieplnych urządzeń siłowych*. WNT, Warszawa, 1976.

Rozdział 11

Zarządzanie bezpieczeństwem w złożonych obiektach i instalacjach krytycznych

Kazimierz T. KOSMOWSKI, Jacek ZAWALICH

11.1. Metody wspomagające zarządzanie bezpieczeństwem

Wzrasta znaczenie metod zarządzania bezpieczeństwem obiektów technicznych, opartych na systematycznej analizie zagrożeń i ryzyka. Metody oparte na ocenie ryzyka wykorzystuje się coraz szerzej w podejmowaniu decyzji w różnych obszarach techniki, zarówno podczas projektowania, jak i eksploatacji złożonych instalacji technologicznych [11.6], [11.7]. Dotyczy to szczególnie metod opartych na ocenach bezpieczeństwa funkcjonalnego, przedstawionych w niniejszym rozdziale. Są one stosowane również w przypadku systemów sterowania maszyn różnej wielkości [11.2]. Poniżej scharakteryzowano wybrane metody wspomagające zarządzanie bezpieczeństwem w systemach technicznych i kierunki prac badawczych.

Obsługa profilaktyczna zorientowana na nieuszkadzalność RCM

Metodyka RCM (*reliability-centered maintenance*) została przedstawiona szerzej w pracach [11.1], [11.3]. Polega ona nie tylko na tym, aby poprzez proaktywną obsługę unikać nie tylko samych uszkodzeń, ale przede wszystkim nie dopuszczać lub przynajmniej ograniczać skutki potencjalnych uszkodzeń. W procesie RCM klasyfikuje się cztery grupy konsekwencji:

A. *Konsekwencje spowodowane uszkodzeniami ukrytymi* – chociaż uszkodzenia ukryte nie mają bezpośredniego wypływu na określony skutek, jednak wystawiają one system na uszkodzenia wielokrotne, często z konsekwencjami katastroficznymi. Większość tych uszkodzeń jest związana z urządzeniami katastroficznymi urządzeń zabezpieczających, które nie są typu *fail-safe*.

B. *Konsekwencje bezpieczeństwa i środowiskowe* – uszkodzenie ma konsekwencje bezpieczeństwa, jeśli mogłoby spowodować zranienie osób lub zejścia śmiertelne; ma ono konsekwencje środowiskowe, jeśli może doprowadzić do naruszania standardów korporacyjnych, regionalnych, państwowych lub środowiskowych.

C. *Konsekwencje (straty) produkcyjne*– uszkodzenie powoduje konsekwencje eksploatacyjne, jeśli wpływa na efektywność produkcji (wielkość, jakość produktu, koszty obsługi i koszty eksploatacyjne, oprócz bezpośrednich kosztów naprawy).

D. *Konsekwencje poza produkcyjne* – uszkodzenie nie wpływa ani na bezpieczeństwo, ani na straty produkcji; obejmują, więc one tylko bezpośredni koszt naprawy.

Kategorie te są uwzględniane w wypracowaniu struktury dla podejmowania decyzji odnośnie obsługi wyposażenia.

Działania w procesie zarządzania obsługą dzieli się na dwie kategorie [11.1]:

- *działania proaktywne*, które podejmowane są przed wystąpieniem uszkodzenia, w celu zapobieżenia przejścia obiektu w stan uszkodzenia; obejmują one obsługę określaną tradycyjnie jako *predykcyjną* (ang. *predictive*) lub *prewencyjną* (ang. *preventive*), chociaż w metodzie RCM stosuje się również takie określenia jak: *planowana odnowa* (ang. *scheduled restoration*), *zaplanowana wymiana* (ang. *scheduled discard*) i *obsługa zorientowana na stan* (ang. *on-condition maintenance*);
- *działania domyślne*, które dotyczą sytuacji po wystąpieniu uszkodzenia; mają one zastosowanie wówczas , kiedy nie jest możliwe określenie efektywnego działania proaktywnego; działania domyślne obejmują: *wykrycie uszkodzenia* (ang. *failure-finding*), *przeprojektowanie* (ang. *redesign*) i funkcjonowanie obiektu do wystąpienia uszkodzenia (ang. *run-to-failure*).

W metodzie RCM proponuje się zasady selekcji działań zależnych od charakterystyk technicznych i rodzaju uszkodzenia, któremu ma się zapobiegać. Istota procesu selekcji zadań polega na:

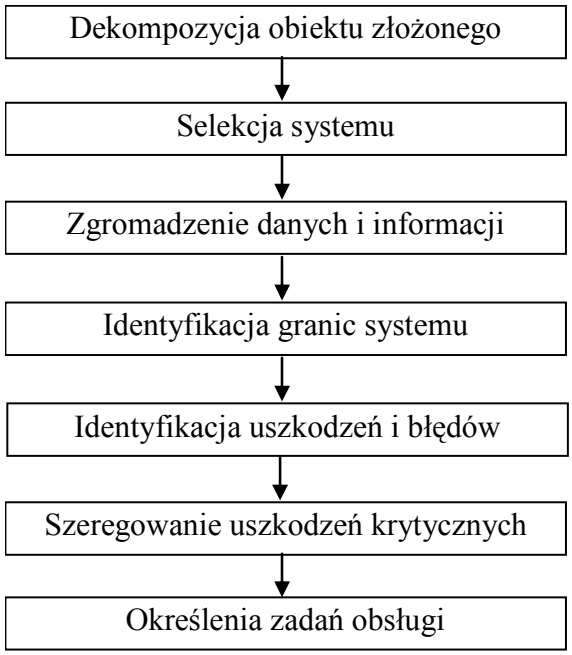
- w przypadku uszkodzeń utajonych, działanie proaktywne jest uzasadnione, jeśli przyczynia się one do redukcji ryzyka, związanego z daną funkcją, do poziomu tolerowanego; jeśli takiego działania nie można określić, wówczas należy wykonać działanie *wykrywania uszkodzenia*; jeśli i takie działanie nie może być określone, należy rozważyć przeprojektowanie obiektu;
- w przypadku uszkodzeń powodujących skutki utraty bezpieczeństwa i środowiskowe, działanie proaktywne jest uzasadnione tylko wówczas, jeśli przyczynia się ono do redukcji ryzyka do odpowiednio niskiego poziomu; jeśli takie działanie nie może być określone, wówczas dany obiekt powinien być przeprojektowany lub powinien być zmieniony proces;
- jeśli uszkodzenie powoduje konsekwencje (straty) produkcyjne, działania proaktywne są uzasadnione tylko wówczas, jeśli sumaryczny koszt ich przeprowadzania w danym przedziale czasu jest mniejszy niż straty produkcji i koszty naprawy w rozważanym okresie - działanie musi być więc uzasadnione ekonomicznie; jeśli to nie zachodzi, wstępną decyzją jest *obsługa niezaplanowana* (ang. *no scheduled maintenance*); jeśli to występuje i potencjalne straty produkcyjne są nadal nie do zaakceptowania, wówczas decyzją powinno być przeprojektowanie obiektu;
- jeśli występują konsekwencje poza produkcyjne, działanie proaktywne jest uzasadnione tylko wówczas, jeśli koszt działania w danym przedziale czasu jest mniejszy niż koszt naprawy w tym samym okresie – działania powinny być uzasadnione na gruncie ekonomicznym; jeśli nie jest to uzasadnione wówczas decyzją domyślną jest *obsługa niezaplanowana*, a jeśli koszty naprawy są zbyt wysokie, następną decyzja domyślną jest przeprojektowanie obiektu.

Na Rys.11.1 przedstawiono schematycznie zakres analizy RCM. Metoda RCM ma związek z ocenami ryzyka, chociaż sama w sobie nie obejmuje formalnej metody analizy ryzyka. Za metodę analizy rodzajów i skutków uszkodzeń przyjmuje się FMEA (*Failure Mode and Effect Analysis*) [11.8], przy czym w analizie krytyczności uszkodzeń stosuje się metodę FMECA (*Failure Mode, Effect and Criticality Analysis*). Analizę FMEA / FMECA przeprowadza się w kontekście wyróżnionych funkcji systemu, przyczyn ich utraty w procesie eksploatacji systemu oraz dostępnych lub proponowanych środków zaradczych. Metoda FMECA jest również bardzo przydatna w analizie systemów związanych z bezpieczeństwem.

11.1.1. Metoda obsługi profilaktycznej oparta na ryzyku RBM

Metoda RBM (*risk-based maintenance*) obejmuje [11.5]:

- zastosowanie technik analitycznych w celu identyfikowania krytycznych, ze względu na ryzyko, jednostek rozważanej instalacji;
- wyznaczenie częstości wystąpienia ważniejszych rodzajów uszkodzeń tych jednostek;
- ocenę konsekwencji każdego rodzaju uszkodzenia, to jest kosztów uszkodzenia z włączeniem zarówno kosztów naprawy, jak i kosztów związanych z utratą produkcji; określenie całkowitego ryzyka związanego z każdym elementem wyposażenia.



Rys. 11.1: Zakres typowej analizy RCM

Nadzorujący przebieg obsługi profilaktycznej wyposażenia uwzględniają wyniki analizy ryzyka i opracowują strategię obsługi szeregując elementy wyposażenia względem składowych ryzyka dla rozważanych rodzajów uszkodzeń. Potencjalne zdarzenia awaryjne i ich skutki można wyznaczyć na przykład na podstawie metody analizy drzew zdarzeń ETA (*Event Tree Analysis*).
Strategię RBM określa się w pięciu krokach:

1. Analiza i dekompozycja systemu z definiowaniem podsystemów / elementów.
2. Identyfikacja potencjalnych rodzajów uszkodzeń.
3. Oszacowanie częstości i konsekwencji (skutków) zdarzeń awaryjnych.
4. Oszacowanie ryzyka i szeregowanie składowych.
5. Wypracowanie strategii obsługi.

Szeregowanie elementów obiektu złożonego według ważności obsługi przeprowadza się na podstawie miary względnego zmniejszenia ryzyka z uwzględnieniem ich potencjalnych rodzajów uszkodzeń. Analizy wykazały, że udział w ryzyku zagregowanym nie jest równomierny i zależy istotnie od elementów i nielicznych rodzajów uszkodzeń. Obsługę elementów o mniejszym udziale w ryzyku można przeprowadzać rzadziej.

11.1.2. Procedura RIMAP w zarządzaniu bezpieczeństwem obiektów i maszyn krytycznych

Jedną z ciekawszych prac badawczych związanych tematyczne z PBZ DIADYN jest projekt RIMAP (*Risk-Based Inspection and Maintenance Procedures*) [11.5]. Projekt ten został zakończony w 2005 roku i jego rezultatem ma być norma europejska poświęcona „*Procedurze inspekcji i obsługi opartej na ocenie ryzyka*". Procedura RIMAP uwzględnia wybrane elementy następujących metod: RBI (*Risk-Based Inspection*), RBIM (*Risk-Based Inspection and Maintenance*), RBLM (*Risk-Based Life Management*), RBM (*Risk-Based Maintenance*) oraz RCM (*Reliability Centered Maintenance*).

Procedura RIMAP obejmuje następujące podstawowe kroki analizy:

1. Praca przygotowawcza i określenie celu.

2. Zgromadzenie danych i walidacja.
3. Wielopoziomowa analiza ryzyka.
4. Podejmowanie decyzji i optymalizacja.
5. Wdrożenie planów eksploatacji i obsługi.
6. Ocena i zbadanie efektywności.

W procedurze tej wyróżniono dwa rodzaje analizy prowadzące do określenia zadań inspekcji, obsługi i testu na podstawie oceny ryzyka:

- RBI (*Risk-Based Inspection*), uwzględnianej w analizie integralności (nienaruszalności).
- RCM (*Reliability Centered Maintenance*) uwzględnianej w analizie funkcjonalności.

Ogólne wymagania dotyczącej oceny ryzyka wspierającej RBIM i RBLM obejmują następujące zasady:

1. Cele i kryteria ryzyka powinny być jasno definiowalne.
2. Musi być określony wymagany poziom szczegółowości informacji wejściowej.
3. Ocena i zastosowana procedura muszą być zgodne z odpowiednimi przepisami prawnymi, regulacjami i normami.
4. Ocena musi być przeprowadzana (audytowana, jeśli to celowe) przez personel o określonej kompetencji z zastosowaniem procedury i narzędzi zapewniających wymaganą informację do podejmowania decyzji.
5. Ocena i zastosowana procedura powinny zapewnić wyniki, które są godne zaufania (zapewniając poprawę bezpieczeństwa systemu), mierzalne, audytowalne oraz zgodne z celami i przejętymi kryteriami oceny ryzyka.

Twórcy tej metody uważają, że zadawalające jakościowo wyniki oceny ryzyka obiektów złożonych zapewni tylko zespół interdyscyplinarny, którego członkowie reprezentują zależnie od potrzeb określone zakresy kompetencji, na przykład:

- Inspekcja i obsługa urządzeń technicznych;
- Dyscypliny związane ze szczególnym wyposażeniem (np. elektrotechnika, oprzyrządowanie pomiarowe i automatyka, zbiorniki i instalacje, maszyny i napędy, itd.);
- Bezpieczeństwo i higiena pracy;
- Eksploatacja instalacji i przebieg procesów (korozji, zużycia, itd.);
- Niezawodność;
- Ocena ryzyka.

Przyjęto, że zarządzający procesem analiz powinni jasno określić jej cele i stosować procedurę w uzgodnieniu z zespołem oceniającym. Cele analiz i ocen są przeważnie określone z uwzględnieniem wymagań bezpieczeństwa oraz ochrony zdrowia i środowiska SHE (*safety, health and environment*) i obejmują niekiedy analizę ekonomiczną skutków zdarzeń awaryjnych. W szczególności plan inspekcji i obsług, który ma być zastosowany w konkretnym obiekcie powinien ujmować jeden lub więcej następujących celów:

- Wypełnienie wymagań dotyczących zdrowia, bezpieczeństwa i środowiska zawartych w regulacjach poprzez redukowania ryzyka do poziomu akceptowalnego,
- Poprawę bezpieczeństwa i niezawodności obiektu,
- Redukowanie kosztów inspekcji i obsługi przez optymalizowanie korzystania z dostępnych zasobów,
- Wydłużenie użytecznego czasu życia obiektu, na przykład poza czas życia obiektu przyjęty w założeniach projektowych.

RIMAP, podobnie jak inne metody analizy ryzyka, przyjmuje w ocenie ryzyka systemów technicznych trzy obszary:

- Obszar ryzyka nieakceptowanego, jeśli w przypadku danego systemu wyznaczone ryzyko znajduje się w tym obszarze, należy podjąć bezwarunkowo działania, aby ryzyko zredukować do poziomu akceptowanego,
- Obszar ryzyka akceptowanego warunkowo, w którym należy dążyć do redukcji ryzyka zgodnie z zasadą ALARP (*as low as reasonably practicable*), korzystając pomocnico z metody analizy kosztów i efektów CBA (*cost-benefit analysis*),
- Obszar ryzyka tolerowanego, w którym nie wymaga się podejmowania działań mających na celu redukowanie ryzyka.

W opracowaniach projektu RIMAP [11.5] dokonuje się przeglądu, proponowanych w literaturze lub stosowanych w niektórych krajach regulacji i kryteriów ryzyka. Uwzględnia się przy tym zarówno miarę ryzyka indywidualnego i miarę ryzyka społecznego.

Istnieje więc szereg metod zarządzania bezpieczeństwem systemów technicznych opartych na analizach i ocenach ryzyka. Prace badawcze prowadzone w Europie (RIMAP i inne) świadczą o aktualności i znaczeniu problematyki zarządzania bezpieczeństwem, wskazując na kierunki integrowania dostępnej wiedzy na ten temat. Celem tych projektów jest opracowanie norm technicznych w formie dostosowanej do oczekiwań przemysłu europejskiego, a więc komunikatywnych i jednoznacznych w interpretacji. W proces ten wpisuje się również projekt DIADYN, którego dalszym etapem powinna być synteza wyników badań w formie oczekiwanej przez krajowy przemysł.

Poniżej przedstawiono wybrane aspekty metodyczne zarządzania bezpieczeństwem złożonych obiektów technicznych podwyższonego ryzyka w cyklu życia z uwzględnieniem zagadnień bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń. Propozycja ta jest rozszerzeniem idei zawartych w metodach opisanych powyżej w niniejszym podrozdziale.

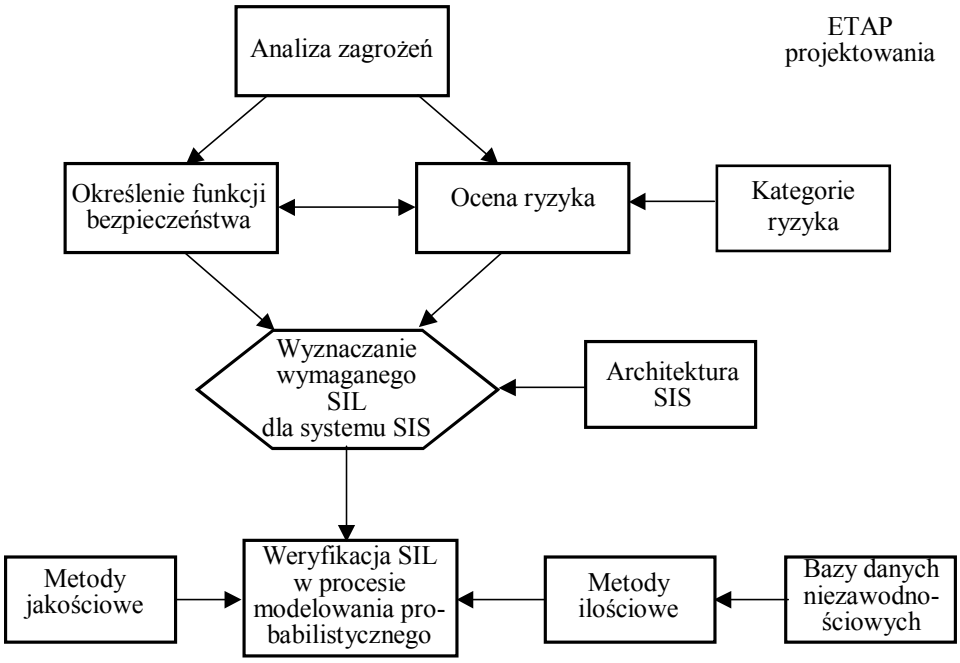
11.2. Zarządzanie bezpieczeństwem w cyklu życia

Zarządzanie bezpieczeństwem w obiekcie krytycznym przeprowadza się w jego cyklu życia, w dwóch podstawowych etapach: w etapie projektowania i etapie eksploatacji. Istotny wpływ na ryzyko związane z eksploatacją takiego obiektu mają systemy sterowania i systemy zabezpieczeniowe. Przyjęto, że projektowanie programowalnych systemów sterowania i automatyki zabezpieczeniowej odbywa się zgodnie z koncepcją bezpieczeństwa funkcjonalnego zarysowaną w rozdz. 3.5. niniejszego opracowania. Przebieg projektowania systemu E/E/PE lub SIS według tej koncepcji przedstawiono na Rys.11.2.

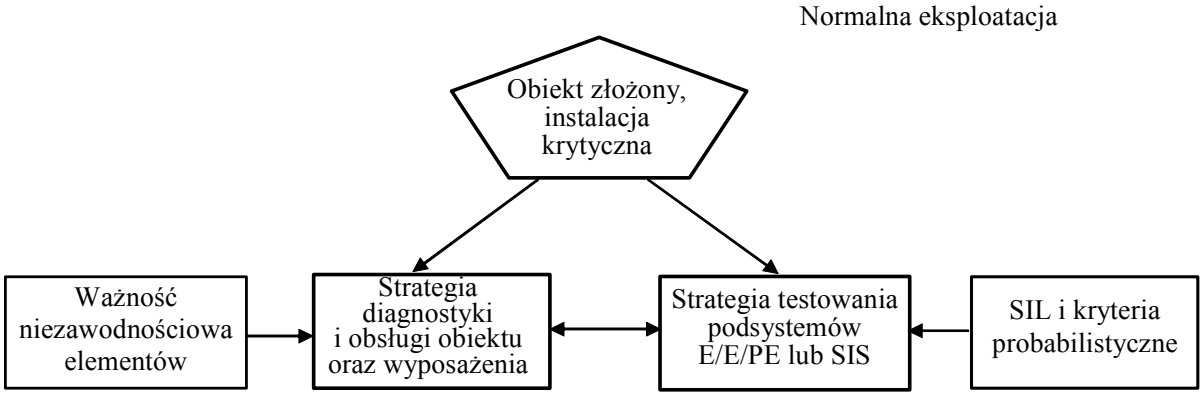
Każdy projekt nowej instalacji lub maszyny krytycznej powinien być poprzedzony analizą występujących zagrożeń i możliwości ich eliminowania. Wyznaczenie wymaganego poziomu nienaruszalności bezpieczeństwa SIL uwarunkowane jest określeniem funkcji bezpieczeństwa i oceną ryzyka po przyjęciu odpowiednich kategorii ryzyka przy jednoczesnej znajomości architektury SIS. W procesie modelowania probabilistycznego można wykonać weryfikację SIL stosując metody jakościowe lub ilościowe korzystając z niezawodnościowych baz danych.
Etap eksploatacji dzieli się na: normalną eksploatację oraz sytuacje po wystąpieniu stanów nienormalnych lub awaryjnych. W czasie normalnej eksploatacji realizuje się wypracowane strategie (Rys.11.3):

- strategię diagnostyki obiektu krytycznego i wyposażenia na podstawie metod analiz niezawodności i ryzyka zarysowanych w rozdz. 3.2 i 3.3 miar ważności niezawodnościowej elementów,
- strategię testowania podsystemów E/E/PE na podstawie wymaganego SIL oraz kryteriów probabilistycznych bezpieczeństwa funkcjonalnego i zakresu analizy zarysowanej w rozdz. 3.5.

Jak widać na Rys.11.2 i Rys.11.3 do przeprowadzania analiz niezawodności i ryzyka eksploatacji takiego obiektu niezbędne są dane niezawodnościowe i inne parametry modeli probabilistycznych. Dane niezawodnościowe o charakterze ogólnym można znaleźć w opracowaniach [11.11], [11.10]. Dane



Rys. 11.2: Przebieg projektowania systemu E/E/PE lub SISzgodnie z koncepcji bezpieczeństwa funkcjonalnego

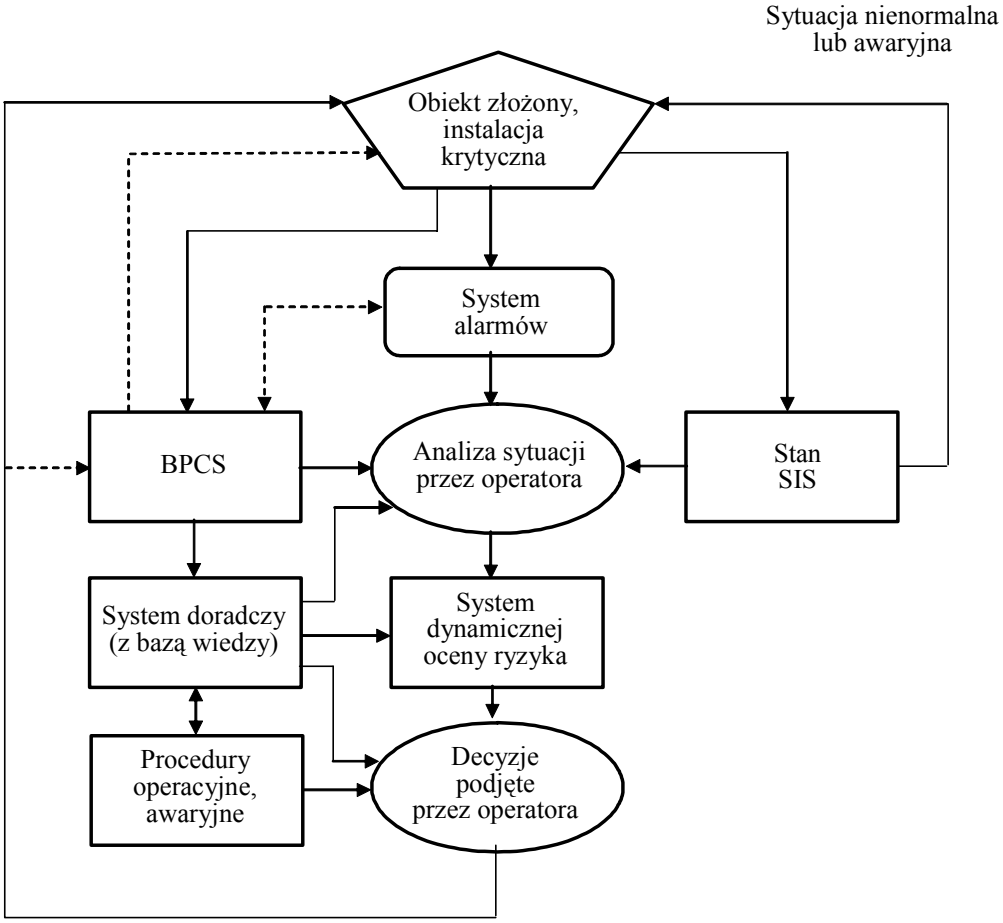


Rys. 11.3: Zarządzanie ryzykiem podczas normalnej eksploatacji

te wymagają odpowiedniej korekty przy wykonywaniu analiz o charakterze ogólnym dla konkretnego obiektu krytycznego [11.8].

Podczas sytuacji nienormalnej lub awaryjnej obiektu złożonego (instalacja krytyczna) istotne znaczenie mają decyzje podejmowane przez operatora, otrzymującego informacje o stanie obiektu z systemu BPCS lub systemu alarmów. Gdyby operatorowi nie udało się odwrócić niekorzystnej tendencji i zostaną przekroczone wartości progowe wielkości charakteryzujących proces awaryjny, powinno nastąpić zadziałanie systemu SIS. Analizę ryzyka dla takich sytuacji odbywa się według metody LOPA. Częstość występowania zdarzeń inicjujących (od zakłóceń wewnętrznych) zależy od strategii diagnostyki i obsługi profilaktycznej wyposażenia (Rys.11.3). Skuteczność działań operatora jest uwarunkowana różnymi czynnikami [11.4] i wymaga analiz niezawodności człowieka-operatora. Propozycję metody uwzględniania czynników ludzkich i organizacyjnych w analizie ryzyka przedstawiono w monografii [11.6].

Podstawowym zagadnieniem w zarządzaniu ryzykiem eksploatacji obiektu krytycznego ma wy-



Rys. 11.4: Elementy wpływające na bezpieczeństwo obiektu krytycznego podczas sytuacji nienormalnej lub awaryjnej

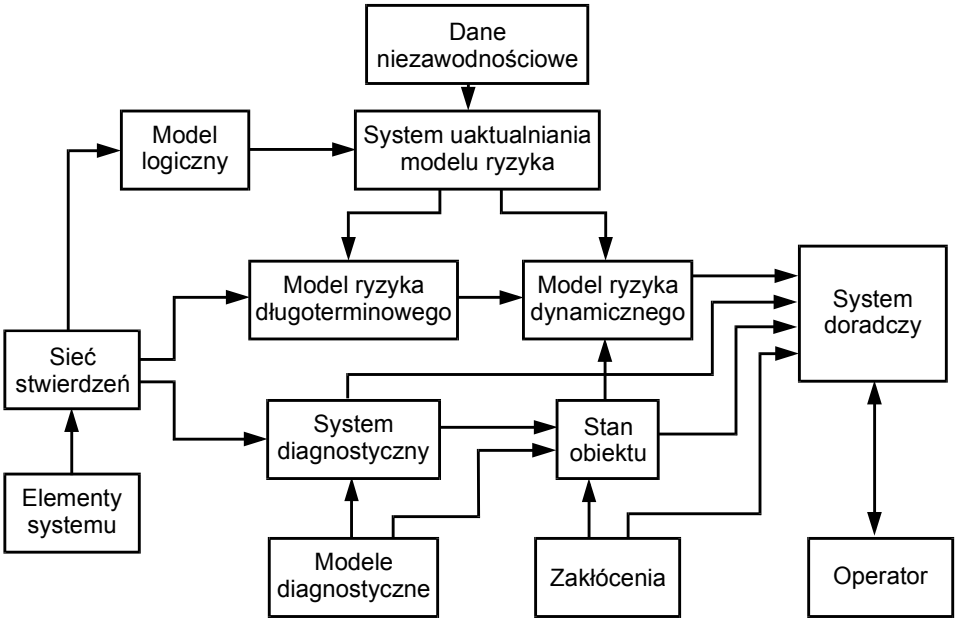
różnienie funkcji bezpieczeństwa. W przypadku energetycznego zespołu blokowego kocioł-turbina-geretator wyróżnić można funkcje sterowania i zabezpieczeń wpływające na niezawodność i bezpieczeństwo, które są realizowane przez odpowiednie układy technologiczne oraz oprzyrządowanie kontrolno-sterownicze i zabezpieczające [11.9]. Podstawowe układy sterowania i regulacji zespołu blokowego elektrowni przedstawiono na Rys.10.1. Zagadnienia funkcjonalne wpływające na niezawodność i bezpieczeństwo eksploatacji turbozespołu energetycznego opisano poniżej.

Audyt bezpieczeństwa funkcjonalnego (*functional safety audit*) - systematyczne i niezależne badanie w celu stwierdzenia, czy konkretne procedury bezpieczeństwa funkcjonalnego są zgodne z procedurami przewidzianymi, czy są skutecznie wprowadzone do stosowania i czy są odpowiednie do osiągnięcia konkretnych celów. Audyt bezpieczeństwa funkcjonalnego może być częścią oceny bezpieczeństwa funkcjonalnego.

Ocena bezpieczeństwa funkcjonalnego (*functional safety assessment*) - badanie oparte na dowodach, podjęte w celu oceny bezpieczeństwa funkcjonalnego osiągniętego przez jeden lub kilka systemów E/E/PE wiążących się z bezpieczeństwem.

Na zarządzanie bezpieczeństwem w instalacjach i obiektach krytycznych można popatrzeć w sposób kompleksowy tworząc zintegrowany system oceny ryzyka i zarządzania bezpieczeństwem (Rys. 11.5). Uwzględnia się tu wówczas modele ryzyka długoterminowego oraz modele ryzyka dynamicznego, które może w sposób diametralny zmienić bezpieczeństwo danej maszyny w bardzo krótkim czasie. Konieczny jest wówczas system uaktualniania modelu ryzyka oparty o dane niezawodnościowe i aktualny stan techniczny obiektu. System diagnostyczny korzystając z aktualnych pomiarów oraz

przyjętych modeli diagnostycznych wypracowuje dane dla systemu doradczego operatora. Bardzo istotne jest uwzględnienie zakłóceń zewnętrznych, które mają duży wpływ na pełną ocenę ryzyka i sposób zarządzania bezpieczeństwem. Sieci stwierdzeń, które w dość łatwy i przystępny sposób można budować w systemie DiaDyn mogą być pomocne przy modelowaniu ryzyka długoterminowego oraz przy budowaniu systemów diagnostycznych. Tak zbudowany system doradczy dla operatora maszyn krytycznych będzie zawierał niezbędne informacje skutecznie wspomagające podejmowanie decyzji.



Rys. 11.5: Zintegrowany system oceny ryzyka i zarządzania bezpieczeństwem

11.3. Wnioski końcowe

Problematyka bezpieczeństwa ma istotne znaczenie w eksploatacji systemów technicznych, w tym instalacji i maszyn krytycznych, gdyż nie ma takiego systemu, o którym można powiedzieć, że jest w pełni bezpieczny. Zagadnienia związane z zarządzaniem bezpieczeństwem zaczynają coraz częściej ujmować dyrektywy europejskie i krajowe akty prawne w postaci ustaw i rozporządzeń. Opracowywane są normy międzynarodowe i krajowe w kontekście wymagań dotyczących szeroko rozumianej jakości (projekt, wyrób, usługa itd.), ochrony środowiska przyrodniczego i bezpieczeństwa (pracy, systemu, działalności gospodarczej, informacji itd.). W przedsiębiorstwach wprowadza się coraz częściej zintegrowane systemy zarządzania jakością, środowiskiem i bezpieczeństwem. W takim szerokim ujęciu należy również spojrzeć na system zarządzania procesem eksploatacji i bezpieczeństwem w przedsiębiorstwie, który powinien obejmować zagadnienia oceny ryzyka, diagnostyki technicznej i niezawodności. Każdy współczesny obiekt techniczny wyposaża się w systemy sterowania i zabezpieczeń, które wpływają istotnie na niezawodność i bezpieczeństwo całego systemu. Zarządzanie bezpieczeństwem złożonego obiektu przeprowadza się w całym cyklu życia.

Prace badawcze w kierunku opracowania i wdrożenie technologii innowacyjnych w przemyśle, dotyczących urządzeń, instalacji, systemów sterowania i zabezpieczeń, oprogramowania i wspomaganych komputerowo systemów zarządzania, powinny uwzględniać wymagania o charakterze ogólnym oraz kryteria formułowane w normach zharmonizowanych i innych normach technicznych, szczególnie krajowych. Europejskie normy techniczne nie zawsze mają charakter obligatoryjny. Jednak, jeżeli dotyczą zagadnień bezpieczeństwa, powinny być one respektowane, szczególnie wówczas, gdy zawierają wskazania dobrej praktyki inżynierskiej.

Zarządzanie bezpieczeństwem opiera się na analizie i ocenie ryzyka. Analiza ryzyka obejmuje

wyznaczenie miary prawdopodobieństwa lub częstości rozważanych scenariuszy awaryjnych. Każdemu zdefiniowanemu scenariuszowi awaryjnemu przypisuje się określone straty, które szacuje się na podstawie odpowiednich metod modelowania procesów (tzw. modelowanie deterministyczne procesów fizycznych i/lub chemicznych), przy czym korzysta się często z opinii ekspertów. Jakość tych opinii, wpływa zwykle istotnie na założenia dotyczące modelu ryzyka i jego parametrów, a zatem jego wiarygodność i przydatność uzyskanych wyników w podejmowaniu decyzji. Zaproponowano, aby zarządzanie bezpieczeństwem oparte na analizie ryzyka odbywało się na podstawie ocen ryzyka statycznego (szacowanego w dłuższych horyzontach czasowych, na przykład roku) oraz oceny ryzyka dynamicznego, dotyczącego stosunkowo krótkich horyzontów czasu, po wystąpieniu zdarzeń nienormalnych. Ryzyka związanego z eksploatacją złożonych obiektów technicznych nie można w pełni wyeliminować, ale można je redukować i utrzymywać na racjonalnym poziomie.

Postęp techniczny oraz ciągle zmieniające się otoczenie wymaga wyróżnienia ryzyka statycznego i ryzyka dynamicznego. Ryzyko statyczne występuje niezależnie od postępu technicznego i związane jest przede wszystkim ze zjawiskami przyrody, np. sztormami, huraganami, trzęsieniami ziemi itp. Natomiast ryzyko dynamiczne ma bezpośredni związek ze zmianami technicznymi, ekonomicznymi i organizacyjnymi, czyli jest nieodłącznym elementem postępu cywilizacyjnego świata i zachodzących zmian społecznych.

W ocenie ryzyka długoterminowego (statycznego) systemów technicznych wyróżniono m.in. obszar ryzyka nieakceptowanego. Jeśli wyniki analizy ryzyka znajdują się w tym obszarze, należy podjąć niezwłocznie działania, wprowadzając odpowiednie opcje sterowania ryzykiem, aby zredukować ryzyko do poziomu akceptowanego. Jeśli znajdują się one w obszarze ryzyka akceptowanego warunkowo, należy dążyć do redukcji ryzyka zgodnie z zasadą ALARP, korzystając pomocniczo z metody analizy kosztów i efektów CBA (*cost-benefit analysis*). W przypadku wyników znajdujących się w obszarze ryzyka tolerowanego nie wymaga się podejmowania działań zmniejszających ryzyko.

Szacowanie ryzyka dynamicznego w czasie eksploatacji, szczególnie po wystąpieniu zdarzenia nienormalnego, jest poważnym wyzwaniem, co wynika z niepewności oceny stanu elementów systemu i możliwych błędnych działań człowieka-operatora. Podstawowe znaczenie ma tutaj odpowiednio zaprojektowany system diagnostyczny. Zaproponowano w niniejszym rozdziale funkcje systemu doradczego, uwzględniającego ocenę ryzyka dynamicznego. Ryzyko dynamiczne jest wyznaczane z wykorzystaniem elementów modelu ryzyka statycznego z odpowiednio uaktualnianymi parametrami (zmienne logiczne i liczbowe). System doradczy powinien obejmować procedury awaryjne opracowane na wypadek sytuacji nienormalnych i awaryjnych, określając zakres wymaganych obserwacji wielkości procesu i działań.

Strategie sterowania ryzykiem realizuje się poprzez projektowanie funkcji bezpieczeństwa i implementowanie ich za pomocą systemów E/E/PE związanych z bezpieczeństwem oraz systemów związanych z bezpieczeństwem wykonanych w innej technice lub za pomocą zewnętrznych urządzeń do zmniejszania ryzyka. Analizy ryzyka przeprowadza się uwzględniając system E/E/PE, którym jest zwykle zestaw elementów funkcjonujących zgodnie z projektem. Zestaw ten może być systemem sterującym lub systemem sterowanym i obejmuje sprzęt, oprogramowanie i współdziałanie człowieka.

W większości instalacji krytycznych odpowiedni poziom bezpieczeństwa uzyskuje się za pomocą pewnej liczby systemów zabezpieczeń, które wykorzystują różne techniki (na przykład mechaniczną, hydrauliczną, pneumatyczną, elektryczną, elektroniczną, programowalną elektroniczną). Dlatego też każda strategia bezpieczeństwa oparta na zarządzaniu ryzykiem musi rozpatrzyć nie tylko elementy wchodzące w skład danego systemu (na przykład czujniki, urządzenia sterujące i urządzenia wykonawcze), lecz także inne systemy związane z bezpieczeństwem tworzące całościowy zestaw systemów wiążących się z bezpieczeństwem.

W modelowaniu bezpieczeństwa dużą rolę odgrywają systemy diagnostyczne. Diagnostyka maszyn w dużym stopniu opiera się na wykonywaniu pomiarów bezpośrednich oraz na badaniach pośrednich, które głównie wykorzystują procesy resztkowe towarzyszące funkcjonowaniu danej maszyny. Procesy te mają charakter elektryczny, mechaniczny, lub cieplny. Z pośród tej kategorii najczęściej stosuje się metody wibroakustyczne, ultradźwiękowe oraz termowizyjne.

Diagnostykę techniczną można podzielić na diagnostykę uszkodzeniową, która zajmuje się identyfikacją i lokalizacją uszkodzeń i defektów maszyny lub jego podzespołów oraz na diagnostykę weryfikacyjną, której zadaniem jest kontrola i ciągła weryfikacja istotnych parametrów z przyjętym modelem, traktowanym jako wzorcowy. Dzięki diagnostyce weryfikacyjnej można określić czy dany obiekt jest zdatny do wykonywania postawionych zadań, czyli czy wartości wybranych istotnych parametrów zawierają się w dopuszczalnych granicach. Odstępstwa od wzorcowego modelu są wówczas informacją o nieprawidłowej pracy maszyny lub przebiegu danego procesu. Na podstawie ciągłej rejestracji dostępnych parametrów obiektu rzeczywistego jest również możliwość prognozowania zmian jego stanu w danym horyzoncie czasowym.

Diagnostykę techniczną należy brać po uwagę w każdym etapie życia systemu technicznego, dowolnej maszyny lub instalacji technicznej. Głównym jej celem jest wypracowanie oceny dotyczącej gotowości urządzeń do wypełnienia postawionych zadań lub przypisanych funkcji. Istotne jest tu zapewnienie dyspozycyjności danej maszyny krytycznej, zabezpieczenie przed uszkodzeniami prowadzącymi do poważnych awarii raz prognozowanie czasu sprawności, okresów prowadzenia przeglądów i testów sprawdzających.

Ocena diagnostyczna powstaje na podstawie aktualnego stanu systemu technicznego przyjętego modelu oraz bazy danych o szczegółowych właściwościach poszczególnych elementów. Każdy etap życia systemu ma inne wymagania i możliwości pozyskiwania informacji. W rezultacie wybór metody diagnostycznej wiąże się z wieloma czynnikami, m.in. warunkami zewnętrznymi urządzeń ich stanem technicznym, rodzajem wykonywanych funkcji, możliwością wykonywania pomiarów, nakładami ekonomicznymi i innymi.

Stawiane diagnozy odnośnie sprawności i niezawodności oraz bezpieczeństwa poszczególnych elementów są podstawą do wydania kompleksowej oceny całego systemu technicznego oraz prowadzonego procesu. W ocenie diagnostycznej istotne są elementy związane z przewidywaniem okresu dyspozycyjności i gotowości pojedynczych elementów i całych układów, które wpływają, często w sposób drastyczny, na okres dyspozycyjności całego systemu oraz koszty eksploatacji i obsługi remontowo-naprawczej. Poszczególne funkcje urządzeń, w tym również funkcje związane z bezpieczeństwem muszą być szczegółowo określone wraz z powiązaniami sprzętowymi, aby oceny diagnostyczne, wytyczne eksploatacyjne, jak również zalecenia dla projektantów były wiarygodne i miały pożądany efekt końcowy.

Identyfikacja rzeczywistych przedziałów wartości wielkości fizycznych, w których występuje generacja sygnałów zewnętrznych, poprzez wykonanie odpowiednich pomiarów napotyka na trudności technologiczne. Na przykład wykonanie standardowego pomiaru prędkości obrotowej oraz wykonanie kontroli tej samej prędkości obrotowej ma zupełnie inny charakter. Sens tej różnicy polega na konieczności zastosowania przyrządów o zwiększonej dokładności oraz na innym interpretowaniu przeprowadzonego pomiaru, aby w sposób obiektywny wykonać rzeczywiste badanie.

Celowe jest, aby prace badawcze dotyczące zagadnień bezpieczeństwa, w nawiązaniu do praktyki zarządzania ryzykiem z uwzględnieniem zagadnień diagnostyki technicznej, były przydatne w opracowaniu lub uaktualnianiu norm technicznych, na które oczekuje przemysł. Przykładem takiej pracy badawczej finansowanej z programu badawczego UE jest projekt RIMAP, którego drugi etap ma zakończyć się opracowaniem normy europejskiej. Wyniki uzyskane podczas realizacji projektu DIADYN można wykorzystać w opracowaniu części takiej normy, w zakresie zintegrowanego zarządzania bezpieczeństwem w cyklu życia dużych maszyn i instalacji krytycznych.

Bibliografia

[11.1] Bahrami K., Price J. RBM, a risk-based maintenance case study. *Maintenance & Asset Management*, 16(1), 2001.

[11.2] Dźwiarek M. Bezpieczeństwo funkcjonalne systemów sterowania maszynami w świetle wymagań dyrektyw ue. Gdańsk / Jurata, 16-18.09. 2004. Politechnika Gdańska, Polskie Towarzystwo Bezpieczeństwa i Niezawodności.

[11.3] International Atomic Energy Agency, Vienna. *IAEA-TECDOC-658: Safety related maintenance in the framework of the reliability centered maintenance concept*, 1992.

[11.4] International Atomic Energy Agency, Vienna. *IAEA-TECDOC-1019: Use of computers to enhance nuclear power plant diagnosis and operator response*, 1998.

[11.5] Ivanovic A. et al. *Risk-Based Inspection and Maintenance Procedures for European Industry*. RIMAP CEN Workshop Document, MPA, 2005.

[11.6] Kosmowski K.T. *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Monografie 33. Wydawnictwo Politechniki Gdańskiej, Gdańsk, 2003.

[11.7] Kosmowski K.T., redaktor. *Functional Safety Management In Critical Systems*. Politechnika Gdańska. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk, 2007.

[11.8] *PN-IEC 812:1994: Techniki analizy niezawodności systemu - Procedura analizy postaci i skutków uszkodzeń (Procedure for Failure Mode and Effects Analysis - FMEA)*.

[11.9] Rakowski J. *Automatyka cieplnych urządzeń siłowych*. WNT, Warszawa, 1976.

[11.10] Washington: U.S. Department of Defence. *MIL-HDBK-217F. Reliability Prediction of Electronic Equipment*, 1991.

[11.11] Wiley, New York. *IEEE Standard 500: IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*, 1984.