Niezawodność strukturalna

Eksploatacja Układów Automatyki - Projekt

Tomasz Słabiak
Damian Staroń
Adrian Stępień
Grzegorz Stochel
Michał Strzępek
Grupa 21

1. Wstęp

W celu dokładnej identyfikacji i zdefiniowania czym jest niezawodność strukturalna i znalezienia odpowiedzi na pytanie dlaczego jest tak ważna dla współczesnej techniki, należy rozpocząć od przeanalizowania wszelkich źródeł pochodzenia uszkodzeń, defektów, czyli przyczyn niezdatności systemów lub urządzeń przemysłowych do eksploatacji. Dopiero wówczas będzie można dokładnie odpowiedzieć sobie na pytania dotyczące niezawodności strukturalnej w technice i układach automatyki. Wiedza na temat istoty fizycznej oraz technicznych aspektów procesów związanych z niezawodnością jest niezbędna w rozwiązywani większości zagadnień konstruowania, wytwarzania i eksploatacji. Pozwala ona na racjonalne konstruowanie, wybór odpowiedniej technologii wytwarzanie oraz optymalizacje właściwości eksploatacyjnych maszyn.

2. Podstawowe pojęcia związane z niezawodnością

2.1. Niezawodność techniczna i strukturalna

Niezawodnością techniczną nazywamy zdolność obiektu technicznego do spełnienia stawianych mu wymagań. Jest to własność obiektu informująca o tym, czy pracuje on poprawnie (spełnia powierzone mu funkcje i czynności) przez wymagany czas i w określonych warunkach eksploatacji. Wielkością charakteryzującą zdolności do spełnienia wymagań może być prawdopodobieństwo spełniania wymagań. Stąd definicja wynika kolejna definicja: niezawodność obiektu jest to prawdopodobieństwo spełnienia przez obiekt stawianych mu wymagań.

Niezawodnością strukturalną nazywamy pełną niezawodność układu. Do jej obliczenia niezbędna jest znajomość niezawodności elementów, które tworzą badany układ.

Kiedy wymaganiem jest to, żeby obiekt był zdatny (sprawny) w przedziale (0, t), którego miara może być czas, ilość wykonanej pracy, długość przebytej drogi lub liczba wykonanych czynności to wtedy niezawodnością obiektu jest to prawdopodobieństwo, że obiekt jest zdatny (sprawny) w przedziale (0, t), lub: niezawodność obiektu jest to prawdopodobieństwo, że wartości parametrów określających istotne właściwości obiektu nie przekroczą w ciągu okresu (0, t) dopuszczalnych granic w określonych warunkach eksploatacji obiektu. Wobec czego można zapisać definicję niezawodności jako:

$$R(t) = P\{t \geq \tau\}$$

Gdzie:
$R(t)$ – niezawodność
t – czas pracy bez uszkodzenia
τ – założony (lub wymagany) czas pracy bez uszkodzenia

Dla obiektów nienaprawialnych przyjmuje się następujące założenia:

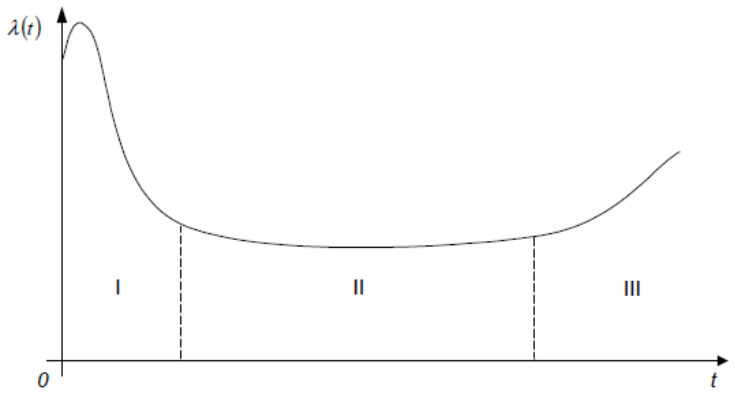
- Dla t = 0 wartość R(0) = 1
- Funkcja niezawodności jest nierosnąca
- Dla t dążącego do nieskończoności lim R(t) = 0

Znaczenie zagadnień niezawodności urządzeń i elementów technicznych znacznie się zwiększyło w przeciągu ostatnich 20 lat. Zostało to spowodowane głównie:

- Wzrostem złożoności współczesnych systemów zawierających niejednokrotnie ponad 1 000 000 elementów,
- Wymaganiami dotyczącymi jakości pracy urządzenia: duże dokładności, efektywności, powtarzalności, itp.,
- Zaostrzeniem się warunków eksploatacji urządzeń lub ich części,
- Zwiększeniem ważności funkcji realizowanych przez system,
- Złożonością warunków eksploatacji systemów technicznych, polegających, na przykład, na jednoczesnym działaniu niskich lub wysokich temperatur, dużej wilgotności, wibracji, dużych przyśpieszeń, promieniowania,
- Automatyzacją i bezpośrednim wyeliminowaniem udziału człowieka w wykonywaniu określonych zadań podczas procesu produkcyjnego, jak i również wyeliminowaniem stałej obserwacji i kontroli ze strony człowieka.

2.2. Uszkodzenia

Ogólnie uszkodzeniem obiektu eksploatacji nazywamy losowy przypadek, powodujący utracenie chwilowe lub stałe zdatności obiektu. Po dokonaniu czynności remontowych lub naprawczych powraca się do pełnej lub częściowej zdatności. Z uszkodzeniem mamy do czynienia, gdy wartości parametrów danego obiektu eksploatacji nie są w normie i przekraczają jego graniczne wartości wytrzymałości.



Rys. 1. Typowy przebieg funkcji intensywności uszkodzeń

Analizując powyższy przebieg intensywności uszkodzeń maszyny podczas czasu eksploatacji możemy wyróżnić trzy okresy jej „życia”:

I. Okres eksploatacji wstępnej (oswajania, dojrzewania)
II. Okres normalnej (właściwej) eksploatacji

III. Okres starzenia się obiektu

Rozwój technik i technologii w budowie maszyn doprowadzają do ciągłego wzrostu osiągów, przy obniżeniu kosztów produkcji i eksploatacji przy równoczesnym zwiększeniu niezawodności i trwałości. Efektem tego typu tendencji produkowane obecnie maszyny cechują się dużym wytężeniem tj. dużym nasileniem oddziaływania czynników cieplnych, mechanicznych i chemicznych, co prowadzi do przyspieszenia czynników mających wpływ na niezawodność materiałów takich jak procesy zużycia i starzenia.

Ogólnie przyjęty podział uszkodzeń prezentuje się następująco:

Rys. 2. Podział uszkodzeń

Czynniki wywołujące uszkodzenia obiektów technicznych związane są z samym obiektem, lub z jego otoczeniem. Spośród najważniejszych możemy wyróżnić:

- Błędy użytkowania
- Błędy konserwacji
- Błędy montażu
- Błędu remontu
- Błędy technologiczne
- Działanie czynników zewnętrznych
- Przekroczenie czasu pracy obiektu

2.3. Starzenie

Jednym z wspomnianych czynników wywołujących uszkodzenia obiektów technicznych jest działanie czynników zewnętrznych. Taki proces powstawania uszkodzeń łączy się z pojęciem starzenia fizycznego.

Starzeniem fizycznym nazywamy proces fizyczny zachodzący w materiałach części maszyn, na skutek wymuszeń wewnętrznych i zewnętrznych, powodujących nieodwracalne zmiany własności użytkowych części. Oddziałuje ono na obiekt w całym procesie jego istnienia, od wytworzenia do likwidacji, nawet wówczas, gdy obiekt nie wykonuje swoich funkcji.

Procesy te zależą od wielu czynników i oddziaływań zewnętrznych i wewnętrznych. Do czynników zewnętrznych należą: wpływ atmosfery, naturalnego podłoża, współpracujących

obiektów itp., natomiast do czynników wewnętrznych zaliczyć można: procesy mechaniczne, mechaniczno-fizyczne i mechaniczno-chemiczne występujące w trakcie funkcjonowania i przechowywania obiektu.

Starzenie fizyczne obiektów zależy od:

- Czynników atmosferycznych (wysokości usytuowania, krainy klimatycznej itp.)
- Opadów atmosferycznych (śnieg, deszcz, wilgotność, ciężar własny pokrywy śnieżnej)
- Ruchu powietrza (siła oddziaływania wiatru, prędkość ruchu powietrza)
- Ciśnienie atmosferyczne (niszczące różnice ciśnień)
- Nagrzewanie słoneczne lub przemysłowe
- Aktywność chemiczna i wilgotność
- Zanieczyszczenia i gazy przemysłowe
- Pole magnetyczne
- Gęstość, spoistośc podłoża
- Ukształtowanie warstwy wierzchniej
- Ruch cieczy
- Struktura warstwy wierzchniej (ziarnistość, kształt i wymiary ziarna)

2.4. Zużycie

Proces stopniowego niszczenia części, pod wpływem czynników fizyko-chemicznych, rodzaju obciążeń i czasu pracy, w całym okresie eksploatacji nazywamy zużyciem. Procesy zużycia, w odróżnieniu od procesów starzenia, zachodzą tylko podczas wykonywania procesów roboczych (funkcjonowania) obiektu.

Procesy zużyciowe obiektów mechanicznych związane są z przetwarzaniem energii w prace mechaniczną i towarzyszącymi im siłami, którymi oddziaływają na siebie jej elementy. W trakcie funkcjonowania obiektu w parach kinematycznych występują reakcje od przyłożonych sił, wynikające z nałożonych więzów geometrycnyczh i kinematycznych. W elementach ogniw i par kinematycznych powstają zmienne naprężenia mechaniczne zależne od obciążanie, obrotów, jakości warstwy wierzchniej itp.

Podstawowe rodzaje zużycia obejmują zużycie:

- Ścierne (mikroskrawanie, rysowanie)
- Adhezyjne (powstawanie i niszczenie połączeń adhezyjnych)
- Zmęczeniowe (cykliczne oddziaływanie naprężeń)
- Przez utlenianie (tworzenie i usuwanie warstewek tlenowych)
- Erozyjne (hydroerozja, erozja gazowa, elektorerozja)
- Kawitacyjne (kawitacja przepływowa, kawitacja falowa)
- Cieplne (metali, niemetali)

2.5. Trwałość

Trwałość i niezawodność są pojęciami różnymi, ale istnieje między nimi zależność. Trwałość jest własnością obiektu, charakteryzująca się pozostawaniem w stanie zdatności do poprawnej pracy z koniecznymi przerwami na obsługę techniczną oraz remonty, aż do granicznego stanu obiektu. Generalizując trwałość to czas, liczba cykli, bądź ilość zrealizowanej pracy przy zachowaniu istotnych własności obiektu w dopuszczalnych granicach.

Natomiast niezawodność, jak już zostało wspomniane, jest zdolnością obiektu do wypełniania określonych funkcji, przy utrzymywaniu swoich wskaźników eksploatacyjnych w zadanych przedziałach, przy zadanych warunkach eksploatacji w ciągu wymaganego czasu lub ilości cykli. Miarą niezawodności jest czas poprawnej pracy liczony od początku użytkowania do pierwszej awarii.

Wyraźnie widać więc, że niezawodność ma pierwszeństwo przed trwałością, gdyż niedopuszczalnym jest by działanie jakiegokolwiek urządzenia lub systemu było nieustannie przerywane, a pożądane funkcje tracone nawet na krótki czas.

2.6. Naprawialność

Celowe może być niekiedy charakteryzowanie niezawodności obiektu jednocześnie kilkoma rodzajami charakterystyk, np. gdy obiektowi przywraca się sprawność po jej utraceniu. Wtedy niezawodność obiektu jest to jego właściwość określona przez prawdopodobieństwo, że obiekt będzie sprawny w ciągu określonego okresu (0, t) oraz przez prawdopodobieństwo, że gdy stanie się niesprawny, przywrócona mu zostanie sprawność w ciągu określonego okresu (0, τ) mierzonego czasem, ilością wykonanej pracy, kosztem przywracania sprawności itp. Prawdopodobieństwo przywrócenia sprawności obiektowi w określonym czasie (0, τ) jest miarą naprawialności. W przypadku ogólnym naprawialność zależy od właściwości samego obiektu i od warunków w jakich przywraca mu się sprawność.

2.7. Gotowość

Gotowość obiektu naprawialnego - tj. obiektu, któremu przywraca się sprawność gdy ją utraci - może być definiowana w różny sposób, np.

- Gotowość obiektu jest to prawdopodobieństwo, że obiekt będzie gotowy do pełnienia swych funkcji w chwili t.
- Gotowość obiektu jest to frakcja danego okresu (np. 1 roku), w ciągu którego obiekt jest zdolny do pełnienia swych funkcji lub je pełni.
- Gotowość obiektu jest to frakcja sumy okresów eksploatacji obiektu, w ciągu której obiekt pełni swe funkcje lub jest zdolny do pełnienia swych funkcji.

- Gotowość jest to frakcja całego życia obiektu, w ciągu której obiekt jest zdolny do pełnienia funkcji lub ją pełni.

Np. Gotowość $A = \frac{T}{T+Q}$

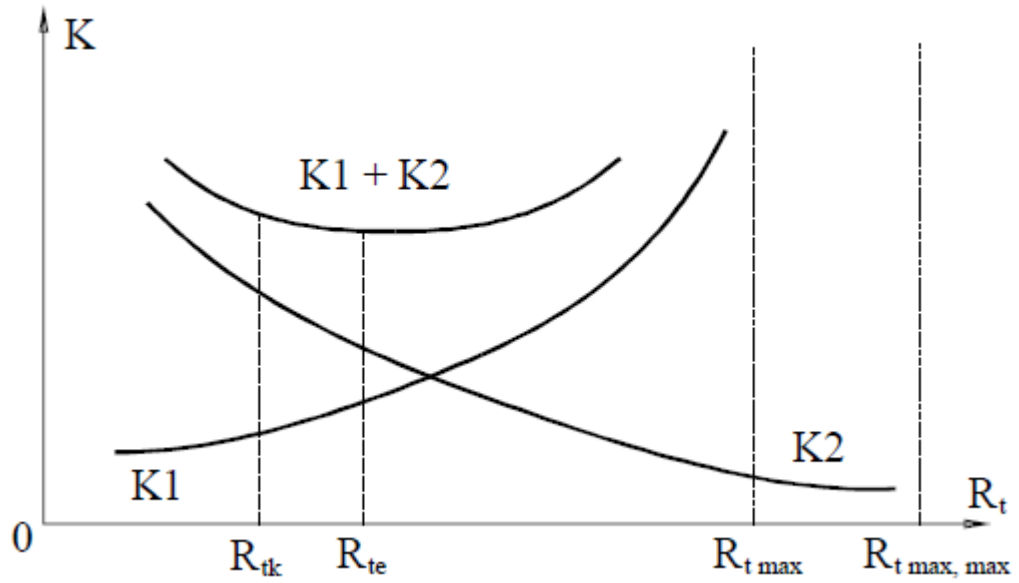
Gdzie:
T - średnia długość okresów sprawności
Q - średnia długość okresów niesprawności

2.8. Wartości szczególne niezawodności

Do wartości szczególnych niezawodności należą:

- $R_{t\,max}$ – wartość maksymalna niezawodności (uzyskiwania lokalnie)
- R_{te} – ekonomicznie optymalna wartość niezawodności
- R_{tk} – wartość krytyczna niezawodności (nietolerowania przez użytkowników)
- $R_{t\,maxmax}$ – największa wartość niezawodności uzyskiwana w technice światowej

Położenie tych wartości niezawodności przedstawia poniższy wykres:

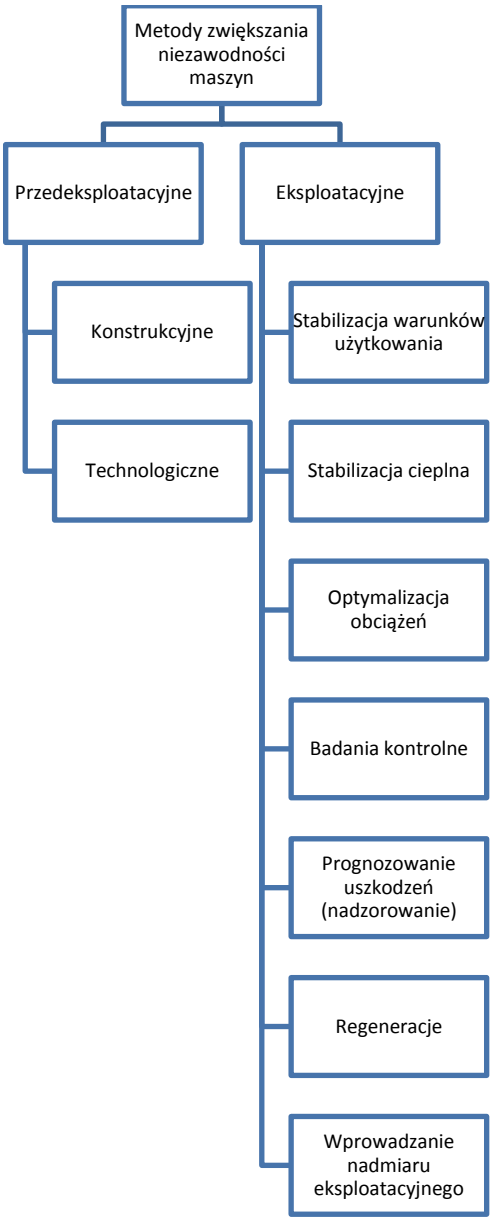


Rys. 3. Zależność kosztów K od niezawodności R_t

Na podstawie wykresu można wnioskować, że koszty K1 uzyskania większej niezawodności R_t rosną, natomiast przy dużej niezawodności maleją koszty K2 postojów, gwarancji, serwisu itp. Istnieje zatem minimalna suma kosztów K1+K2 przy których uzyskuje się ekonomicznie optymalną wartość niezawodności R_{te}.

2.9. Metody zwiększania niezawodności

Przedłużanie okresu użytkowania obiektów technicznych polega głownie na podwyższaniu ich niezawodności. Można to uzyskać metodami przedeksploatacyjnymi lub eksploatacyjnymi.



Rys. 4. Klasyfikacja metod zwiększania niezawodności maszyn.

W **metodach przedeksploatacyjnych** niezawodność uzyskuje się za pomocą metod konstrukcyjnych umożliwiających praktycznie bez większych ograniczeń, stworzenie obiektów o dużej niezawodności z elementów o małej niezawodności – dzięki zastosowaniu elementów rezerwowych.

Mniej skuteczne są metody technologiczne. Wymagają bowiem zróżnicowania parametrów jakościowych elementów, co przeczy unifikacji i w wielu przypadkach jest praktycznie niemożliwe do zrealizowania lub ekonomicznie nieuzasadnione. Często stosowaną odmianą tej metody jest selekcja wyrobów na grupy wymiarowe.

Zwiększenie niezawodności słabych ogniw uzyskuje się dzięki rozpoznaniu procesów niszczących i zwiększeniu odporności elementów na te uszkodzenia w wyniku działań konstrukcyjnych lub eksploatacyjnych polegających na zmianie:

- Materiału elementu,
- Rodzaju smarowania,
- Odporności powierzchni roboczych na zużywanie,
- Grubości warstwy utwardzonej.
- Trwałości powierzchni.
- Założonej sztywności połączenia lub skojarzenia.
- Wartości luzów lub granic tolerancji,
- Wymiarów i kształtu elementów,
- Rodzaju pary trącej.

Każda z metod zwiększania niezawodności polega na pieczołowitym dopilnowaniu wymagań konstruktora (zadanie dla technologa) albo na przewymiarowaniu konstrukcji.

Każdy obiekt techniczny charakteryzuje się **niezawodności potencjalną**, która nabywa w procesie wytwarzania i eksploatacji tylko wówczas, gdy warunki wówczas, gdy warunki wytwarzania i użytkowania nie odbiegają od zakładanych. W praktyce udaje się to niezmiernie rzadko i dlatego rzeczywista niezawodność obiektu jest znacznie niższa od potencjalnej. Należy to brać pod uwagę podczas opracowywania projektu wstępnego i zakładać niezawodność wyższa od wymaganej.

Określone wymagania niezawodności mogą być sprawdzone i potwierdzone wyłącznie podczas użytkowania, np. przez automatyzację kontroli lub nadzorowanie. Miejsce sporządzania takich informacji powinno być usytuowane jak najbliżej źródła ich powstania. W nowoczesnych systemach produkcyjnych powszechne jest nadzorowanie narzędzi i innych, szybko zużywających się elementów. Umożliwia to opracowanie np. metody ustalania czasu wymiany narzędzi przez pomiar siły skrawania luz zużycia. Dzięki zgromadzonym informacjom możliwe jest stosowanie odpowiednich strategii eksploatacyjnych utrzymania maszyn w ruchu i wprowadzenie ulepszeń konstrukcyjnych.

3. Wskaźniki eksploatacyjne niezawodności

Z tematem niezawodności związany jest szereg pojęć. Najważniejsze z nich to:

- **Elementy obliczeń niezawodności** – obiekt rozpatrywany w trakcie obliczeń niezawodności
- **Sprawność** – zdolność do poprawnej pracy
- **Czas eksploatacji** – czas eksploatacji obiektu do momentu wystąpienia stanu granicznego określonego w dokumentacji technicznej
- **Uszkodzenie** – zdarzenie po wystąpieniu, którego obiekt przestaje wypełniać swoje funkcje
- **Trwałość**- własność obiektu charakteryzująca się pozostawaniem w stanie zdolności do poprawnej pracy z koniecznymi przerwami na obsługę techniczną i remonty.
- **Trwałość sumaryczna** - suma okresów, w których obiekt jest sprawny do momentu w którym należy wycofać obiekt z eksploatacji.

Oprócz powyższych wyróżniamy także:

- **Uszkodzenia katastroficzne** – powodują całkowitą utratę zdolności obiektu do poprawnej pracy np. zwarcia i przerwy, połamania, deformacje, zacięcia detali mechanicznych
- **Uszkodzenia parametryczne** – zaliczają się do uszkodzeń częściowych, czyli określają uszkodzenie elementów składowych danego wyrobu. Z biegiem czasu uszkodzenia parametryczne mogą mieć charakter stały lub chwilowy.
- **Uszkodzenia nagłe** - uszkodzenia charakteryzujące się gwałtownymi zmianami pewnych parametrów pod wpływem różnych losowych przyczyn związanych z wewnętrznymi defektami, z niewłaściwymi zmianami warunków eksploatacji, z błędami użytkowania, itp.
- **Uszkodzenia stopniowe** - stopniowa, płynna zmiana parametrów wynikająca ze starzenia się materiałów i zużycia poszczególnych elementów.
- **Uszkodzenia niezależne** - uszkodzenie, które jest nie wynikiem powstania innego uszkodzenia.
- **Uszkodzenia zależne** - uszkodzenie występujące w przypadku, gdy uszkodzenie jednego elementu spowoduje uszkodzenie następnych.
- **Uszkodzenia stałe** - uszkodzenia nieodwracalne, które likwidowane mogą być jedynie przez naprawę, regulację lub wymianę uszkodzonego elementu.
- **Uszkodzenia chwilowe** - charakteryzują się tym, że mogą samodzielnie ustępować bez ingerencji obsługującego.
- **Uszkodzenia chwilowe wielokrotne** - wielokrotnie powtarzające się uszkodzenia chwilowe.

3.1. Charakterystyki niezawodności

W opisie niezawodności korzystamy z sześciu charakterystyk:

- Prawdopodobieństwo poprawnej pracy
- Prawdopodobieństwo uszkodzeń,
- Częstotliwość uszkodzeń
- Intensywność uszkodzeń,
- Średnia częstotliwość uszkodzeń,
- Średni czas poprawnej pracy,
- Średni czas pracy między uszkodzeniami.

3.2. Prawdopodobieństwo poprawnej pracy

Prawdopodobieństwo poprawnej pracy – prawdopodobieństwo nie wystąpienia ani jednego uszkodzenia przy zadanych warunkach eksploatacyjnych. Jest to prawdopodobieństwo tego, że dany obiekt zachowa wartość swych parametrów w wymaganych przedziałach, w określonym czasie przy określonych warunkach eksploatacji.

$$R(t)=P(t\geq T);\ t\geq 0$$

Gdzie:

- t - czas pracy bez uszkodzeń
- T - założony lub wymagany czas pracy bez uszkodzenia

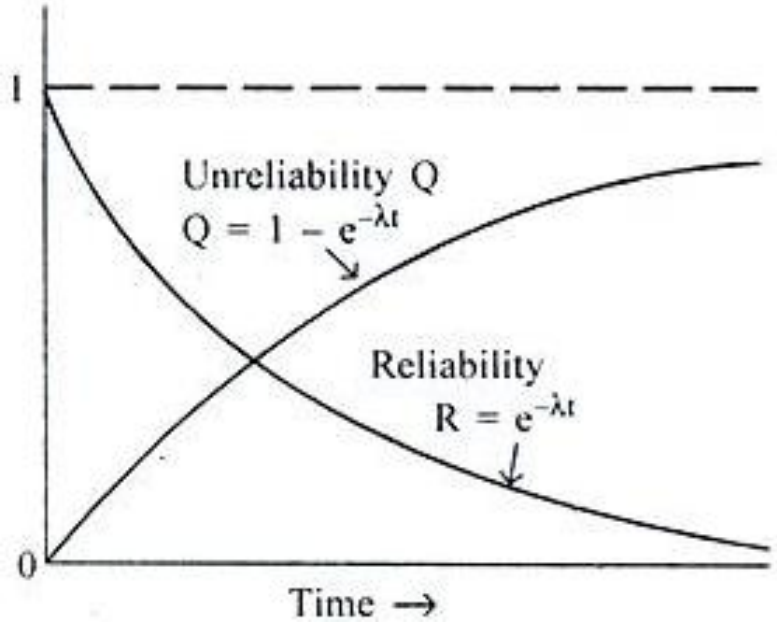
3.3. Prawdopodobieństwo uszkodzeń

Prawdopodobieństwo uszkodzenia – prawdopodobieństwo, że przynajmniej jedno uszkodzenie wystąpi w ustalonym przedziale czasu przy określonych warunkach eksploatacyjnych

$F(t)=1-R(t)$

F(t) – prawdopodobieństwo uszkodzenia,

R(t) – prawdopodobieństwo poprawnej pracy



3.4. Częstotliwość uszkodzeń

Częstotliwość uszkodzeń – stosunek liczby uszkodzonych elementów w jednostce czasu do początkowej liczby elementów badanych.

$$\propto (t) = \frac{\Delta m}{n_0 \Delta t}$$

α(t) - częstotliwość uszkodzeń

Δm - liczba uszkodzonych elementów w przedziale czasu od $(t-\frac{\Delta t}{2})$ do $(t+\frac{\Delta t}{2})$

n_0 - początkowa liczba badanych elementów
Δt - przedział czasu

Częstotliwość uszkodzeń można przedstawić w postaci:

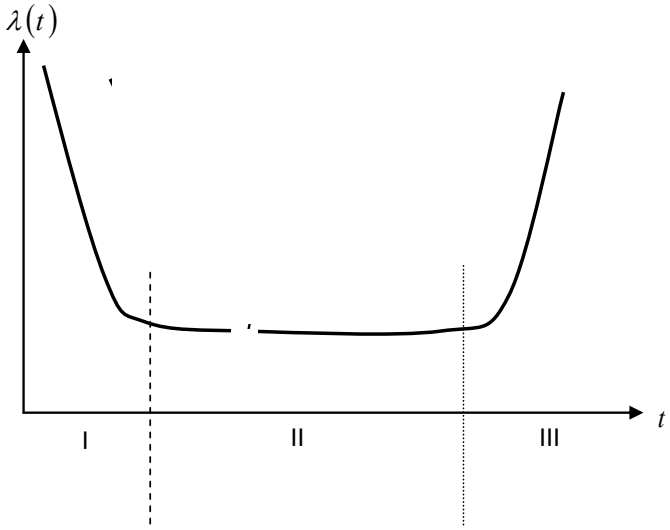
$$\propto (t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$$

F(t) – prawdopodobieństwo poprawnej pracy

R(t) – prawdopodobieństwo uszkodzeń

3.5. Intensywność uszkodzeń

Intensywność uszkodzeń – prawdopodobieństwo, że w danej jednostce czasu po określonym czasie wystąpi nienaprawialne uszkodzenie obiektu, przy spełnionych warunkach (przy braku wcześniejszych uszkodzeń). Intensywność uszkodzeń określa się stosunkiem liczby elementów uszkodzonych w jednostce czasu do średniej liczby elementów pracujących sprawnie w danym przedziale czasowym.



$$\lambda(t) = \frac{\Delta m}{n_{\Delta t} \Delta t}$$

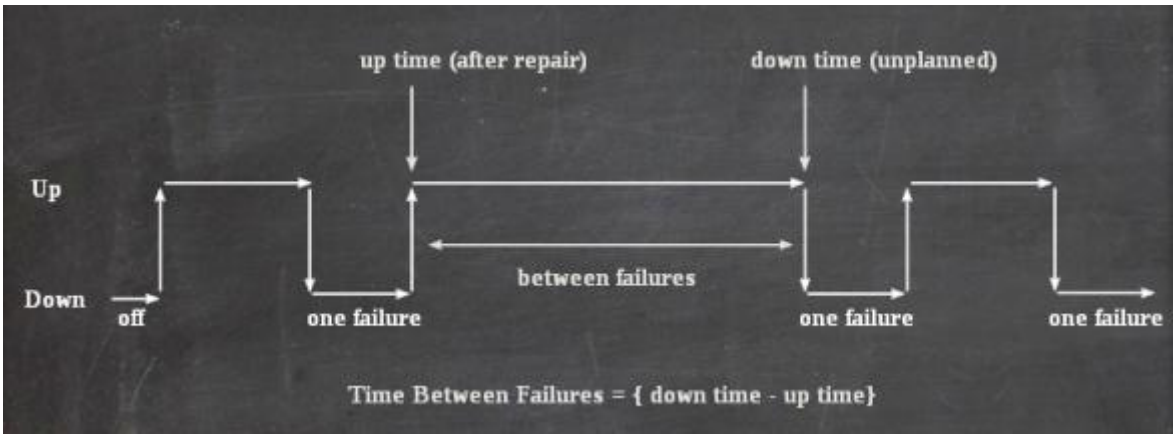
- λ(t) – intensywność uszkodzeń
- Δm – liczba uszkodzonych elementów w przedziale czasu od $(t-\frac{\Delta t}{2})$ do $(t+\frac{\Delta t}{2})$
- $n_{\Delta t}$- średnia liczba elementów pracujących sprawnie w przedziale czasu Δt
- Δt – przedział czasu

$$n_{\Delta t} = \frac{1}{2}[n_{t-\frac{1}{2}\Delta t} + n_{t+\frac{1}{2}\Delta t}]$$

3.6 Współczynnik MTBF

MTBF (z ang. Mean Time Between Failure)

- średni czas wyrażony w godzinach, w którym urządzenie może działać bez przerwy (awarii). MTBF jest stosowany m.in. w informatyce oraz zarządzaniu.



- podstawowa miara niezawodności systemu
- w użyciu od 60 lat
- opracowano ponad 20 metod i procedur do przewidywania cykli życia
- stosowany w projektowaniu obiektów o znaczeniu krytycznym, np. sprzęt IT i telekomunikacyjny

4. Struktury niezawodnościowe systemów

Struktura niezawodnościowa systemu jest to struktura przedstawiająca sposób wzajemnych powiązań elementów określających zależność uszkodzeń systemu od uszkodzeń jego elementów. Niezawodność systemu jest bezpośrednio powiązana z niezawodnością jego elementów składowych.

Podział struktur:

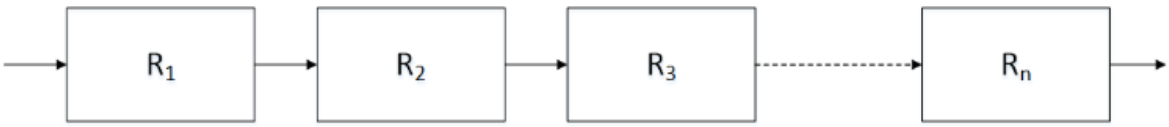
I. Struktury proste:
- 1.1 Struktura szeregowa
- 1.2 Struktura równoległa
- 1.3 Struktura szeregowo-równoległa
- 1.4 Struktura równoległo-szeregowa

II. Stuktury złożone
- 2.1 Struktura typu mostek
- 2.2 Struktura typu siatka
- 2.3 Stuktura typu siec

III. Struktury progowe

4.1. Struktura szeregowa

Mówimy, że system ma szeregową strukturę niezawodnościową, jeżeli niesprawność dowolnego elementu powoduje niesprawność całego systemu. Z definicji struktury szeregowej wynika, że obiekt jest sprawny wtedy i tylko wtedy, kiedy wszystkie jego elementy są sprawne.



Rys. 5. Struktura szeregowa

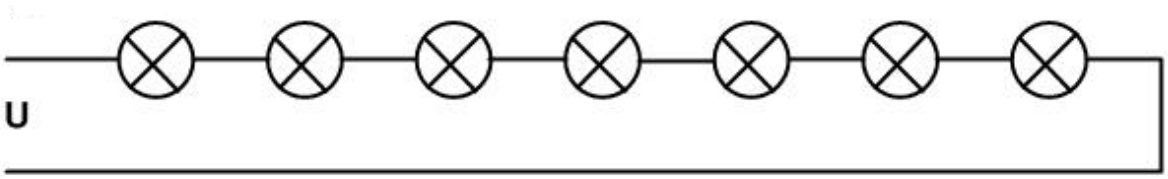
Niezawodność systemu o strukturze szeregowej jest równa iloczynowi niezawodności wszystkich jego elementów składowych:

$$R_s = R_1 R_2 \ldots R_n = \prod_{i=1}^{n} R_i$$

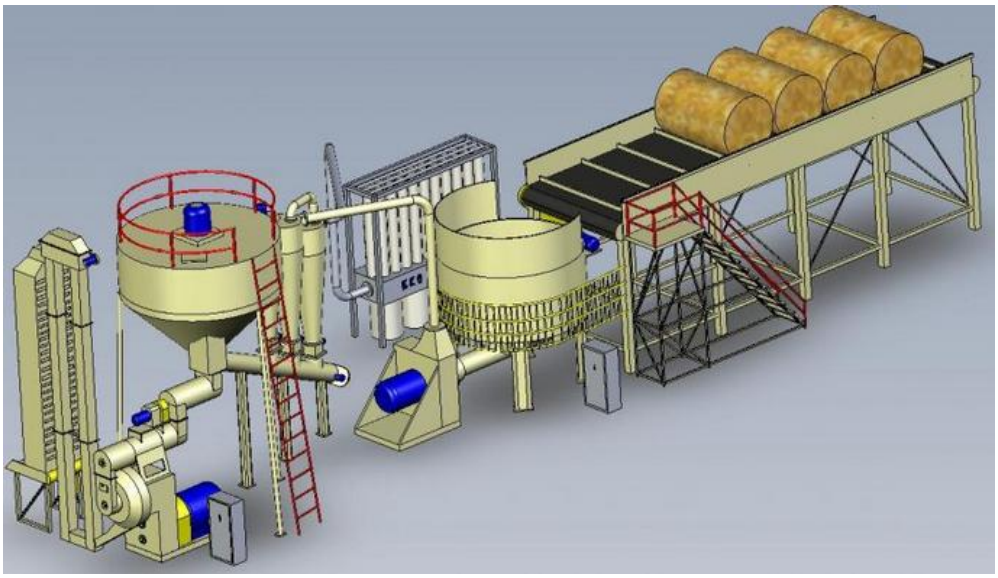
Zawodność obiektu szeregowego wyraża się wzorem:

$$Q_s = 1 - R_s = 1 - \prod_{i=1}^{n} R_i$$

Przykłady obiektów o strukturze szeregowej:



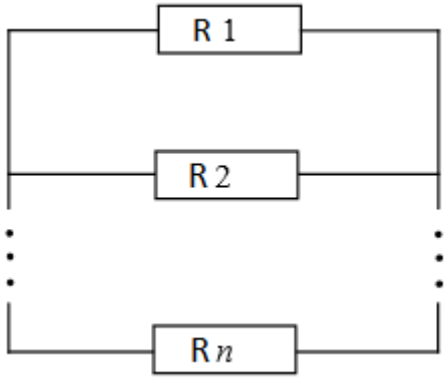
Rys. 6. Szeregowo połączone żarówki



Rys. 7. Linia produkcyjna brykietu

4.2. Struktura równoległa

Obiekt o strukturze równoległej jest zdatny gdy co najmniej jeden z jego elementów składowych jest zdatny



Rys. 8. Struktura równoległa

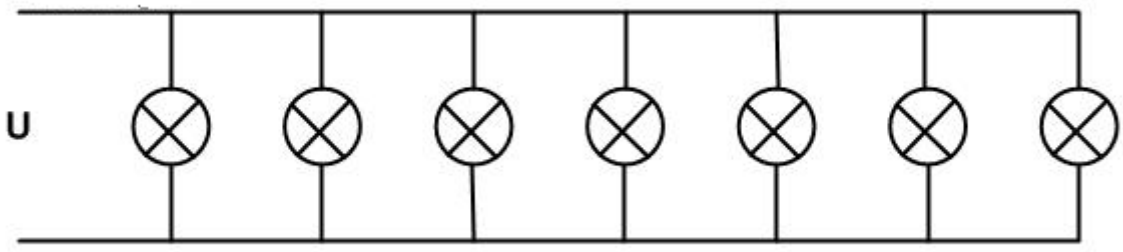
Niezawodność obiektu równoległego wyraża się wzorem :

$$R_r = 1 - \prod_{i=1}^{n}(1-R_i)$$

Zawodność obiektu równoległego wyraża się wzorem :

$$Q_r = Q_1 Q_2 \ldots Q_n = \prod_{i=1}^{n} Q_i$$

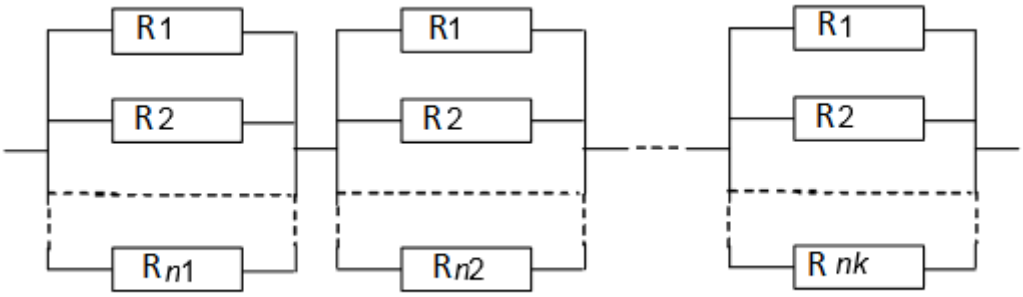
Przykład obiektu o strukturze równoległej :



Rys. 9. Równolegle połączone żarówki

4.3. Struktura szeregowo-równoległa

Struktura szeregowo-równoległa jest strukturą powstałą poprzez szeregowe połączenie kilku zespołów o strukturze równoległej. Obiekt o takiej strukturze działa poprawnie tylko i wyłącznie wtedy gdy wszystkie zespoły działają poprawnie.



Rys. 10. Struktura szeregowo-równoległa

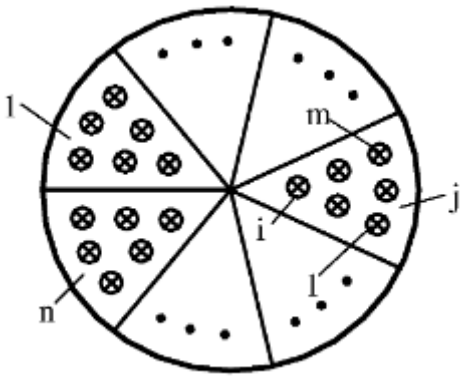
Niezawodność obiektu o strukturze szeregowo-równoległej składającego się z *n* zespołów o *m* równolegle połączonych elementach wyraża się wzorem :

$$R_{sr} = \prod_{j=1}^{n}[1- \prod_{i=1}^{m}(1-R_{ij})]$$

Natomiast zawodność powyższego obiektu wyraża się wzorem :

$$Q_{sr}=1-[1-(1-R)^m]^n$$

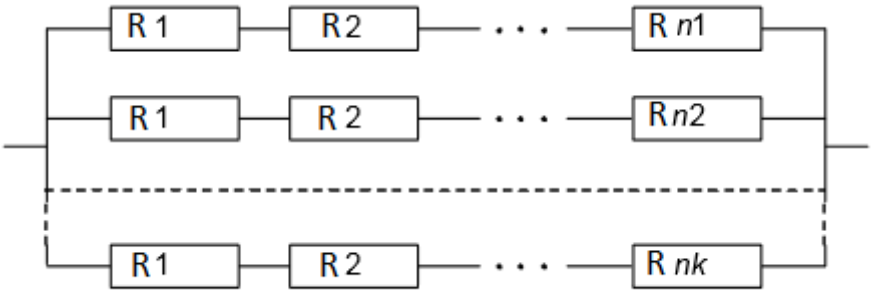
Przykład obiektu o strukturze szeregowo – równoległej :



Rys. 11. Segmentowa lampa elektryczna

4.4. Struktura równoległo-szeregowa

Struktura równoległo-szeregowa jest strukturą powstałą poprzez równoległe połączenie kilku zespołów o strukturze szeregowej. Obiekt o takiej strukturze działa poprawnie gdy przynajmniej jeden z jego zespołów działa poprawnie.



Rys. 12. Struktura równoległo- szeregowa

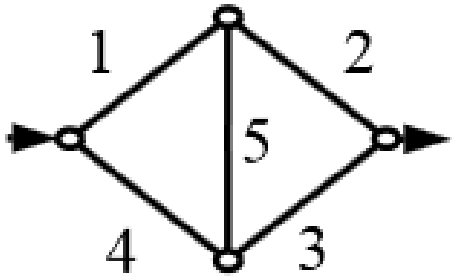
Niezawodność obiektu o strukturze równoległo-szeregowej składającego się z *n* zespołów o *m* szeregowo połaczonych elementach wyraża się wzorem :

$$R_{rs} = 1 - \prod_{j=1}^{n}(1 - \prod_{i=1}^{m} R_{ij})$$

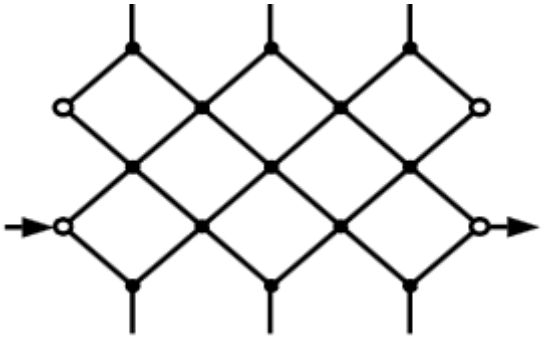
Natomiast zawodność powyższego obiektu wyraża się wzorem :

$$Q_{rs} = (1-R^{m})^{n}$$

4.5. Struktura typu mostek



4.6. Struktura typu siatka



4.7. Struktura typu siec

Przy wyznaczaniu niezawodności obiektów o strukturach złożonych korzystamy z tzn. metody dekompozycji prostej, polegającej na sprowadzeniu obiektów złożonych do obiektów o strukturze prostej, których niezawodność możemy wyliczyć z wyżej wymienionych wzorów.
Dekompozycję prostą przeprowadza się zawsze względem jednego dowolnie wybranego elementu i stosuje się ją aż do momentu kiedy otrzymamy obiekty o strukturze prostej

Niezawodność obiektu n elementowego wyraża się wzorem:

$$R^{(n)} = R_i R_{(i)}^{(n-1)} + (1-R_i) R_{(i)}^{(n-1)}$$

4.8. Struktury progowe

Obiekty o strukturze progowej są sprawne gdy *k* spośród *n* elementów to elementy zdatne. W obiektach tych dopuszcza się uszkodzenie pewnej liczby elementów poniżej której obiekt uznaje się jeszcze za zdatny

Ze względu na parametr p (próg obiektu) obiekty progowe można podzielić na :

1. Obiekty mniejszościowe gdy $0 \leq p < 0.5$
2. Obiekty równościowe gdy $p = 0.5$
3. Obiekty większościowe gdy $0.5 > p \leq 1.0$

Przykładem obiektu o strukturze progowej typu „2 z 3” może być zwykła lampa o trzech żarówkach, którą uznaje się za zdatną gdy działają co najmniej dwie żarówki (dopuszcza się spalenie jednej żarówki)

5. Układy redundantne

5.1. Wstęp

Redundancja (łac. redundantia – powódź, nadmiar, zbytek) – nadmiarowość w stosunku do tego, co konieczne lub zwykłe. Określenie może odnosić się zarówno do nadmiaru zbędnego lub szkodliwego, niecelowo zużywającego zasoby, jak i do pożądanego zabezpieczenia na wypadek uszkodzenia części systemu. Stosuje się ją wszędzie tam gdzie wymagana jest bezawaryjna praca systemu lub ludzi. Znakomicie sprawdza się w przypadku ochrony życia ludzkiego (np. w samolotach, statkach) oraz w przypadku ochrony ważnych danych (bazy danych).

Redundancja pojawia się we współczesnych systemach automatyki w wielu formach, a w niektórych aplikacjach przemysłowych jest wręcz ich integralną częścią. W swej najprostszej postaci redundancja urządzeń wymaga zainstalowania ręcznych, dublowanych przełączników praktycznie dla każdego urządzenia systemowego. W systemach automatyzowanych pracę urządzeń kontrolują odpowiednie, dedykowane sterowniki. W niektórych aplikacjach jednak praca nadmiernie zautomatyzowana może prowadzić do sytuacji groźniejszych niż sterowanie manualne.

Na przykład w utleniających rowach cyrkulacyjnych automatyczne sterowanie procesem może doprowadzić do nadmiernego nasycenia tlenem przez aeratory. W trybie ręcznym najlepszym wyjściem w takiej sytuacji może się okazać szybkie wyłączenie wszystkich aeratorów, co zapewni właściwy poziom nasycenia powietrzem, bez konieczności stałego monitoringu wskaźników procesowych. Jednakże może to również zaowocować większymi stratami energii. Rozwiązaniem alternatywnym jest zastosowanie obejścia – bypassu – w formie kanału omijającego urządzenie filtrujące, co zapewnia poprawne funkcjonowanie linii procesowej. Może jednak prowadzić do pojawienia się w nadmiernej ilości szkodliwych cząstek zanieczyszczeń w dalszych etapach oczyszczania – odstojnikach, klarownicach, zbiornikach.

Innym sposobem realizacji redundancji jest tzw. nadmiarowość urządzeń, a więc instalacja większej ich liczby niż niezbędna w procesie. Na przykład montaż trzech pomp, gdy konieczne są tylko dwie. Tego typu rozwiązania są bardzo popularne. Zwykle każda z takich pomp ma swój własny układ rozruchowy, moduł falownikowy i sterownik, dzięki czemu idea redundancji systemu dotyka też sfery automatyki i sterowania takim układem. Realizacja idei redundancji może być również osiągnięta poprzez budowę kilku osobnych ciągów produkcyjnych/przetwórczych, z których każdy ma zazwyczaj niezależny system sterowania lub są one częściowo powiązane funkcjonalnie.

W przypadku gdy podczas awarii zagrożone jest ludzkie życie elementy zapewniające bezpieczeństwo przez prawidłowe działanie mogą być potrojone, mimo tego że formalnie występują jako pojedynczy element. W takim przypadku wszystkie trzy komponenty

musiałyby ulec awarii żeby cały układ przestał działać poprawnie. Prawdopodobieństwo takiego zdarzenia jest bardzo niewielkie.

Wreszcie redundancja może być oparta na odpowiednim projekcie, strukturze i funkcjonalności systemu automatyki.

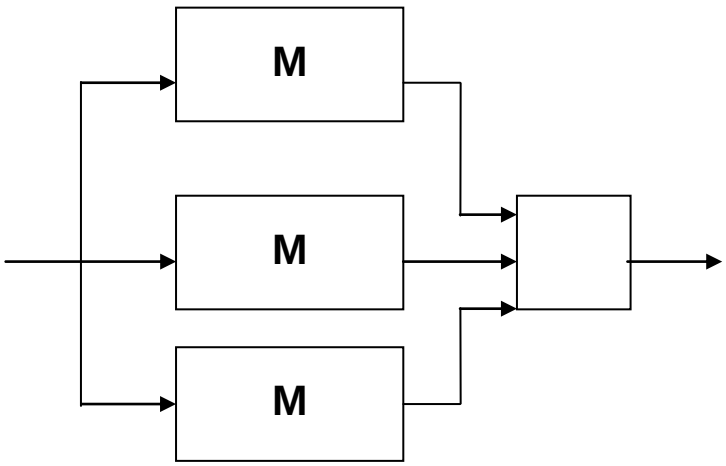
5.2. Statyczna redundancja sprzętowa.

Przykładem zastosowania statycznej redundancji sprzętowej jest używany w samolotach całkowicie skomputeryzowany system sterowania fly-by-wire. W tym systemie elementy, które podejmują decyzje są potrojone. Część, która będzie wysyłać błędną decyzję zostanie przegłosowana przez dwa pozostałe. Dzięki temu układ będzie działał niezawodnie mimo uszkodzeniu jednego z elementów.

Założenia potrzebne do prawidłowego działania układu:

- sprawny układ głosujący,
- niezależne uszkodzenia modułów,
- większa ilość modułów działających od niedziałających.

Schemat systemu statycznej redundancji sprzętowej:



M – moduł, który może ulec awarii

V – układ głosujący

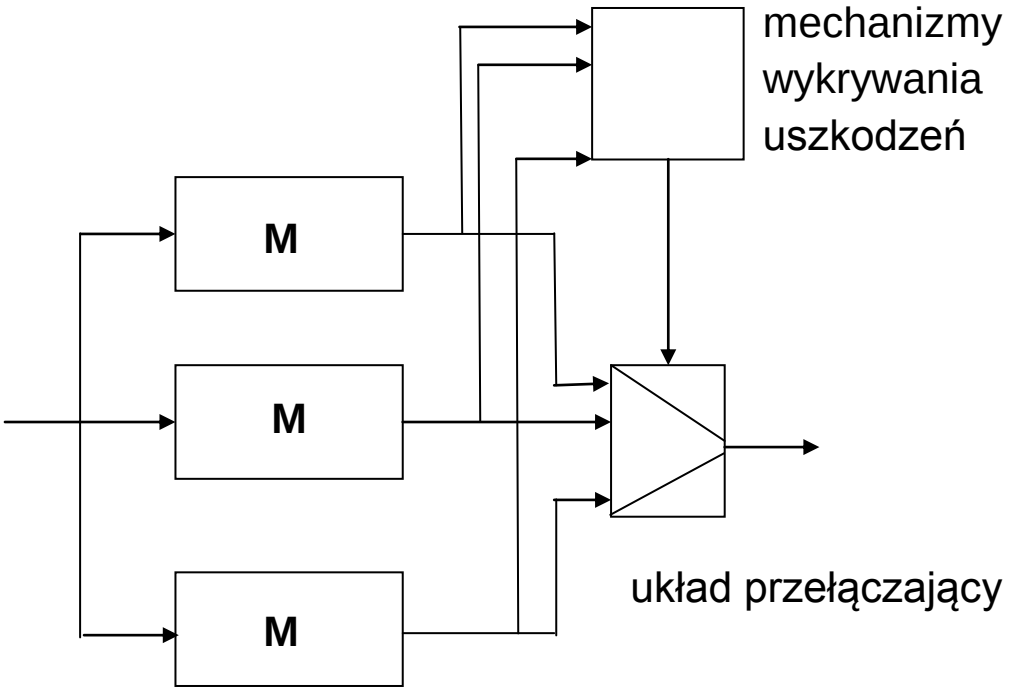
5.3. Dynamiczna redundancja sprzętowa

System dynamicznej redundancji sprzętowej zawiera kilka modułów. Tylko jeden z nich jest wystarczający do poprawnego działania całego systemu. Pozostałe moduły są zapasowe.

Założenia potrzebna do prawidłowego działania układu:

- idealne mechanizmy wykrywania uszkodzeń,
- sprawny układ przełączający,
- niezależne uszkodzenia modułów.

Schemat systemu dynamicznej redundancji sprzętowej:



Układy dynamicznej redundancji sprzętowej dzielą się na:

- układy redundancji typu cold,
- układy redundancji typu warm,
- układy redundancji typu hot.

Podział ten odnosi się do szybkości reakcji (przejęcia funkcji uszkodzonego elementu przez zapasowy) systemu redundantnego.

5.4. Redundancja typu cold

Ten rodzaj redundancji stosuje się do sterowania procesami, gdzie czas reakcji ma minimalne znaczenie, a obsługa systemu zwykle wymaga interwencji operatora, który wykonuje funkcję układu przełączającego. Przykładem może być instalacja dwóch pras, z których każda ma własny panel sterowania. W przypadku awarii jednej z nich operator przywraca funkcjonalność procesu przez załączenie drugiej prasy. W takiej aplikacji wyłączenie prasy głównej może skutkować brakiem wytłoczenia co najwyżej kilku elementów, jednakże nie prowadzi do całkowitego zablokowania produkcji. Dlatego też taka redundancja może bazować na czynniku ludzkim, a więc interwencji operatora.

5.5. Redundancja typu warm

Ten typ redundancji spotykany jest w aplikacjach, gdzie czas reakcji jest parametrem znaczącym, jednak wciąż dopuszczalne są bardzo krótkie zatrzymania procesu, skutkujące nagłymi uderzeniami (w układach wodnych, gazowych itp.). W czasie takich uderzeń zawory, silniki pomp i inne urządzenia mogą podlegać krótkotrwałym wyłączeniom, a związane z nimi czujniki mogą nie przekazywać przez pewien czas informacji o swoim stanie do np. sterowników PLC.

Ten typ redundancji może być zobrazowany na przykładzie systemu ATAD (autotermicznej tlenowej stabilizacji osadu), w którym w czasie przemian biologicznych powstaje ciepło. Do jego rozproszenia wykorzystuje się zwykle mieszalniki, aeratory i reduktory piany, dostarczające powietrze i ograniczające gromadzenie się piany. Przy nagłym pojawieniu się przerwy, okresu przejściowego, wartość ciepła w procesie może pozostawać na stałym poziomie, co z kolei prowadzi do zmniejszenia jego wydajności energetycznej. Trzeba jednak pamiętać, że wyłączenie mikserów, aeratorów, reduktorów piany na dłużej niż kilka minut powoduje nadmierny, nieprzewidziany przyrost piany i rozwarstwienie osadów, na skutek czego procesy przemian biologicznych mogą przejść w niekorzystną fazę beztlenową. Dlatego też w systemie sterowania dla takich aplikacji dopuszcza się kilkusekundowe przerwy w pracy urządzeń, które jednak powinny być jak najszybciej automatycznie przywrócone do pracy, by uniknąć zaburzeń procesów tlenowej stabilizacji osadu.

Systemy redundantne typu *warm* zbudowane są zwykle w oparciu o dwa mikrokontrolery (sterowniki) włączone jako główny i zapasowy (w trybie oczekiwania standby). Sterownik główny steruje układami we/wy obsługującymi sygnały procesowe, podczas gdy zapasowy jest zasilony i otrzymuje okresowo sygnały nastaw ze sterownika głównego, oczekując na jego ewentualne wyłączenie na skutek awarii itp. Jeżeli awaria nastąpi, sterownik zapasowy przejmuje proces sterowania wszystkimi modułami w miejsce sterownika głównego, który w tym czasie może być serwisowany. Sygnały nastaw/stanów sterownika głównego przekazywane są zwykle na zakończenie każdej sekwencji programowej w postaci najbardziej istotnych danych, niezbędnych do podtrzymania ciągłości sterowanych procesów. Dlatego też w momencie przejęcia sterowania przez sterownik

zapasowy, w procesach mogą nastąpić małe przerwy i uderzenia, zanikające po kilku sekundach i unormowaniu wszystkich bieżących nastaw.

5.6. Redundancja typu hot

Redundancja *hot*. Tego typu redundancję stosuje się, gdy w obsługiwanej aplikacji w żadnych okolicznościach niedopuszczalna jest nawet najmniejsza przerwa w sterowaniu. Przykładem mogą być ciśnieniowe układy membranowe i zaworowe. W obu przypadkach te procesy technologiczne nie wymagają same z siebie sterowania w układzie redundancji typu *hot,* jednak w przypadku prowadzenia strumieni zwrotnych jest już ona niezbędna. W czasie odwracania strumienia może bowiem nastąpić odwrócenie zaworów, zaburzenie ich sekwencji działania lub zatrzymanie silników, przez co proces odwracania może być niekompletny. Na skutek tego do czystej wody mogą się dostać zanieczyszczenia, a niektóre z urządzeń mogą ulec nieodwracalnym zniszczeniom. Takie sytuacje są niedopuszczalne – dlatego też w tego typu aplikacji konieczne jest zastosowanie redundancji *hot*.

Sfera sprzętowa układów z redundancją *hot* jest identyczna jak w przypadku typu *warm,* z tą jednak podstawową różnicą, że w systemach *hot* nie ma żadnego opóźnienia, przerw i uderzeń w momencie przełączania sterowania między sterownikiem głównym a zapasowym. Aby to było możliwe, konieczne jest odpowiednie zarządzanie transmisją danych, ustawień pomiędzy dwoma sterownikami, które w rzeczywistości przekazywane są na bieżąco, czyli w każdym cyklu logicznym pracy układu sterującego. Organizację transmisji danych w takim reżimie realizuje się zwykle według dwóch dostępnych metod.

Pierwsza z nich to wysłanie danych ze sterownika głównego po zeskanowaniu nastaw programowych po każdym cyklu pracy programu. W takim trybie, zwanym „skanuj i wyślij", tylko po potwierdzeniu transmisji danych do sterownika zapasowego możliwy jest kolejny krok programu i w efekcie na jego końcu ponowne skanowanie parametrów. Technika ta po raz pierwszy była zastosowana przez firmę Modicon przy budowie pierwszych redundantnych sterowników PLC. Z powodzeniem stosowana jest również w wielu współczesnych aplikacjach i jak wskazuje praktyka, gwarantuje właściwy poziom niezawodności oraz szybkości działania. Jednakże przy stosowaniu tej metody trzeba zwrócić uwagę na kilka istotnych kwestii. Po pierwsze rzeczywisty czas skanu parametrów między sterownikami jest połączeniem czasu skanowania programu oraz czasu transmisji zeskanowanych danych między sterownikami. Ponieważ czas skanowania może być parametrem krytycznym w niektórych aplikacjach, dostawcy systemów redundantnych zwracają uwagę w dokumentacji swoich urządzeń, że program sterownika powinien być zoptymalizowany pod kątem jak największej szybkości skanowania. Niejednokrotnie sugerują w nich również, jak ograniczyć zbędne kroki i operacje skanowania tylko do niezbędnych, związanych bezpośrednio z bieżącymi faktycznymi zmianami parametrów. Jeżeli sugestie te nie zostaną właściwie uwzględnione, może to doprowadzić do nadmiernego obciążenia łączy komunikacyjnych i w momencie awarii do nieprawidłowego przejęcia sterowania przez układ zapasowy. Układy redundancji typu *hot* bazujące na wspomnianej metodzie funkcjonują już

od dłuższego czasu w automatyce przemysłowej i dobrze się sprawdzają. Trzeba jednak mieć świadomość ich wspomnianych ułomności.

Postęp technologiczny w dziedzinie układów sterujących pozwolił w ostatnim czasie na opracowanie nowej metody transmisji danych w układach redundantnych *hot*, tym razem niezależnej od czasu skanowania parametrów programu w sterowniku głównym. Ta nowa metoda zwana jest transmisją asynchroniczną. Do jej realizacji niezbędny jest sterownik główny wyposażony w dwa wbudowane mikroprocesory, z których pierwszy zajmuje się obsługą kolejnych procedur programowych. Po każdym zakończeniu cyklu programu wszystkie dane, nastawy są przekazywane do drugiego mikroprocesora, który z kolei ma za zadanie obsługę transmisji danych, podczas gdy procesor pierwszy już uruchamia kolejny cykl programowy. W ten sposób w sterowniku pracują dwa procesory – jeden wykonujący program sterowania, drugi odpowiedzialny za obsługę transmisji danych do sterownika zapasowego, a sama transmisja przebiega asynchronicznie w stosunku do realizowanego algorytmu sterowania. Dzięki temu możliwe jest przesyłanie kompletnych tabel parametrycznych, bez wpływu na opóźnienie realizacji obsługi sterowania urządzeń procesowych. Sam program sterowania nie musi być już zatem rygorystycznie optymalizowany pod kątem szybkości skanowania niezbędnych parametrów i nastaw. Dlatego też w większości przypadków ta metoda obsługi redundancji *hot* jest lepsza do zastosowań w zakładach uzdatniania wody, gdzie większość procesów funkcjonuje w trybie wysokiej niezawodności, ze względu na krytyczność parametrów czystości wody.

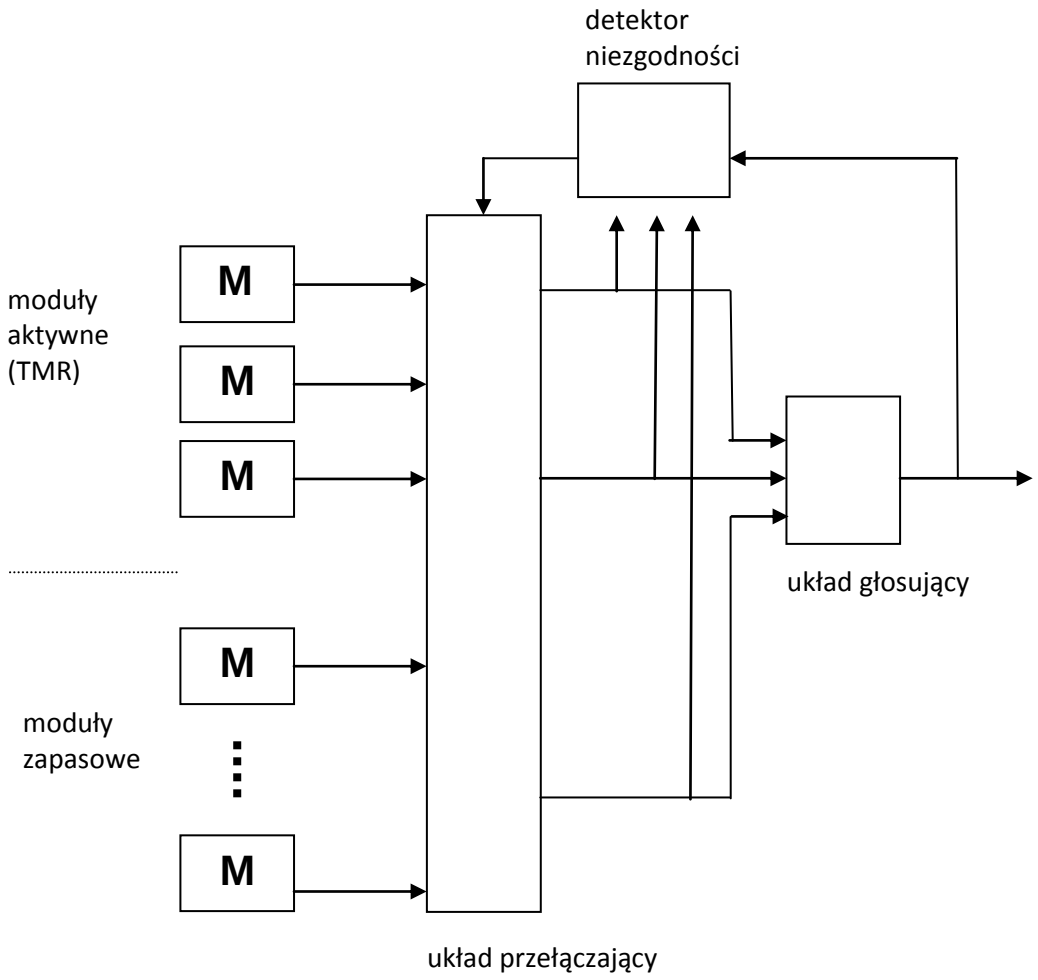
5.7. Hybrydowa redundancja sprzętowa

System hybrydowej redundancji sprzętowej to połączenie statycznej i dynamicznej redundancji. Zawiera detektor niezgodności, układ głosujący i układ przełączający.

Założenia potrzebne do prawidłowego działania układu:

- niezależne uszkodzenia modułów,
- sprawny układ przełączający,
- sprawny układ głosujący,
- sprawny detektor niezgodności.

Schemat systemu hybrydowej redundancji sprzętowej:



6. Zasady budowy modelu niezawodnościowego

Rodzaj struktury niezawodnościowej systemu (obiektu złożonego) zależy od:

- struktury funkcjonalnej obiektu, tzn. od sposobu konstrukcyjnego połączenia elementów i od wzajemnego oddziaływania tych elementów na siebie,
- zadania, jakie ma dany obiekt wykonać.

Podstawą tworzenia struktur niezawodnościowych są odpowiednie schematy technologiczne obiektów złożonych. Ze względu na specyfikę problemu oraz różnice w rozwiązaniach projektowych różnych obiektów należy określać strukturę niezawodnościową indywidualnie dla każdego analizowanego obiektu.

Strukturę niezawodnościową można przedstawić w postaci stabelaryzowanej lub analitycznej. Jednak najlepszym i najbardziej obrazowym sposobem jest przedstawienie

struktury niezawodnościowej obiektu jako schemat graficzny, na przykład jako graf, schemat blokowy niezawodności lub schemat niezawodnościowy obiektu.

Każdy system należy analizować indywidualnie ze względu na specyfikę problemu oraz różnice w rozwiązaniach projektowych. Podczas tworzenia schematu niezawodnościowego należy:

- przeanalizować schemat topologiczny funkcjonowania systemu,
- wyróżnić w systemie elementy, których niezawodność ma wpływ na niezawodność systemu,
- odwzorować wyróżnione elementy w postaci bloków,
- odwzorować graficznie zależności między stanami niezawodnościowymi elementów, a stanem niezawodnościowym systemu.

W celu ułatwienia graficznego odwzorowania struktury niezawodnościowej systemu można wykorzystać następujące wskazówki:

- elementy niepowtarzalne przedstawia się w postaci oddzielnych i różnych bloków,
- elementy powtarzalne przedstawia się w postaci jednego typu bloku,
- jeżeli niesprawność danego elementu powoduje niezdatność całego systemu, to element ten wchodzi w skład podsystemu o szeregowej strukturze niezawodnościowej,
- jeżeli niesprawność systemu jest spowodowana jednocześnie zdatnością kilku elementów, to elementy te wchodzą w skład podsystemu o równoległej strukturze niezawodnościowej.

Wyróżnienia elementów w systemie dokonuje się w procesie dekompozycji. Dekompozycja systemu polega na stopniowym podziale obiektu na mniejsze części (podsystemy), które z kolei dzieli się na podsystemy prostsze. Na danym stopniu podziału wyróżnione podsystemy traktuje się jako niepodzielne elementy. Podział jest wykonywany ze względu na funkcje (wg kryteriów technologicznych), jakie pełni dany podsystem podczas realizacji zadania obiektu. Dekompozycji dokonuje się do takiego stopnia szczegółowości, jaki narzuca cel i zakres oceny niezawodności analizowanego systemu. Oznacza to, że z punktu widzenia potrzeb oceny niezawodności dalszy podział na elementy nie jest celowy.

W niektórych wypadkach struktura funkcjonalna obiektu złożonego odpowiada wprost jego strukturze niezawodnościowej. W większości wypadków jednak tak nie jest. Związane jest to z wpływem postawionego zadania, które ma wykonać obiekt, na jego strukturę niezawodnościową.

7. Niezawodność w przypadku bezpieczeństwa w systemach sterowania

Budowa systemu zabezpieczeń, który sprawdza się w praktyce i oferuje wystarczający poziom bezpieczeństwa wymaga doświadczenia w wielu obszarach. Podstawą jest zaprojektowanie funkcji bezpieczeństwa dla systemu, który będzie gwarantował odpowiedni poziom niezawodności. W tej kwestii z pomocą przychodzi norma EN ISO 13849-1.

Zmiana norm dotyczących bezpieczeństwa w systemach sterowania wprowadza nowe koncepcje i obliczenia dla konstruktorów i użytkowników maszyn. Norma EN 954-1 (kategorie) jest stopniowo zastępowana przez EN ISO 13849-1(PL-Performance Level) i EN 62061 (SIL-Safety Integrity Level).

Tak więc projektując system mamy do wyboru dwie normy i dwie technologie:

- PL (Performance Level – poziom działania) to neutralna pod względem technologicznym koncepcja, którą można stosować w stosunku do elektrycznych, mechanicznych, pneumatycznych oraz hydraulicznych rozwiązań służących poprawie bezpieczeństwa.

- SIL (Safety Integrity Level – poziom nienaruszalności bezpieczeństwa) może z drugiej strony, być zastosowany wyłącznie w stosunku do elektrycznych, elektronicznych i programowalnych rozwiązań służących poprawie bezpieczeństwa.

Czym jest PL (Performance Level)?

PL to miara niezawodności funkcji bezpieczeństwa, czyli poziom zapewnienia bezpieczeństwa lub poziom działania. PL dzieli się na pięć poziomów (a-e). PL e oznacza najlepszą niezawodność i jest równoznaczny z wymaganym przy najwyższym poziomie zagrożenia.

Aby obliczyć poziom PL systemu, trzeba znać:

- Strukturę systemu (kategorie B, 1-4)
- Mean Time To dangerous Failure, czyli średni czas międzyawaryjny (MTTFd)
- Diagnostic Coverage, czyli pokrycie diagnostyczne systemu (DC)

Konieczne będą także:

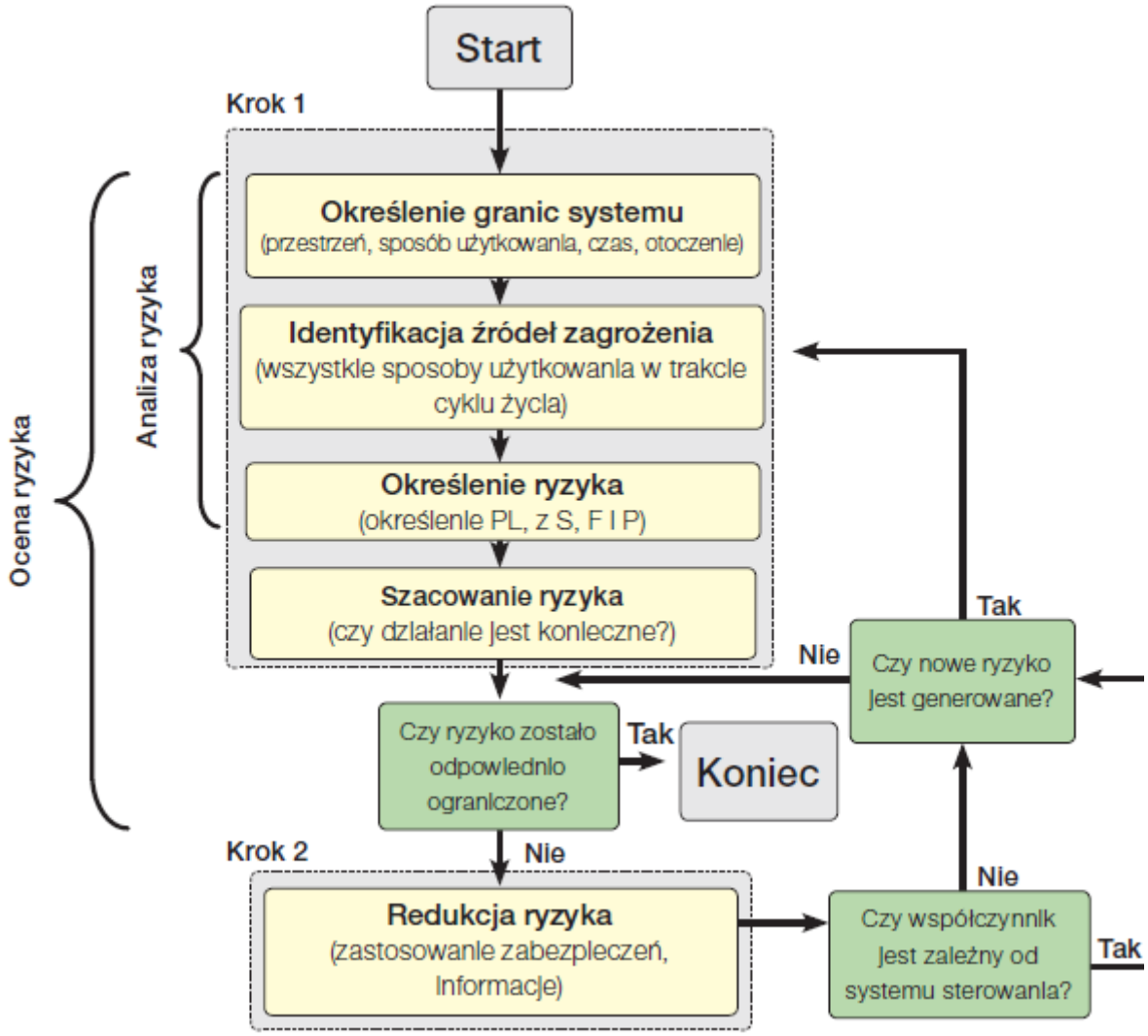
- ochrona systemu przed usterką, która wyeliminuje obydwa kanały (CCF)
- ochrona systemu przed błędami systematycznymi wynikającymi z jego konstrukcji
- przestrzeganie określonych zasad w celu zapewnienia prawidłowego rozwoju oraz walidacji oprogramowania

Pięć poziomów PL (a-e) odpowiada określonym zakresom wartości PFHD (Probability of dangerous Failure per Hour – prawdopodobieństwo niebezpiecznego defektu na godzinę). Mówią one, jak prawdopodobne jest wystąpienie niebezpiecznej awarii w okresie jednej godziny. Przy obliczeniach zaleca się stosowanie bezpośrednio wartości PFHD, gdyż PL jest pewnego rodzaju uproszczeniem, które nie zapewnia zawsze takiej samej dokładności wyników.

Pojęcia zgodnie z nomenklaturą EN ISO 13849-1

- **PL -** Performance Level (poziom działania) - podział (od a do e)
- $\boldsymbol{PL_r}$ - Required Performance Level. Wymagany poziom zapewnienia bezpieczeństwa dla danej funkcji
- $\boldsymbol{MTTF_d}$ - Średni czas międzyawaryjny. Podział na niski, średni i wysoki
- $\boldsymbol{B_{10d}}$ - Średnia ilość cykli roboczych, osiągniętych przed czasem, w którym 10% urządzeń testowych ulegnie defektowi prowadzącemu do niebezpiecznego uszkodzenia (dotyczy komponentów pneumatycznych i elektromechanicznych).
- $\boldsymbol{T_{10d}}$ - Średni czas do momentu, w którym 10% komponentów ulegni defektowi prowadzącemu do uszkodzenia niebezpiecznego (czas pracy komponentu jest ograniczony do T10d).
- $\boldsymbol{CCF}$ - Common Cause Failure (uszkodzenie wywołanewspólną przyczyną)
- $\boldsymbol{DC}$ - Diagnostic Coverage (pokrycie diagnostyczne). Podział na niskie, średnie i wysokie
- $\boldsymbol{PFH_D}$ - Probability of Dangerous Failure per Hour. Prawdopodobieństwo defektu na godzinę

Schemat postępowania:

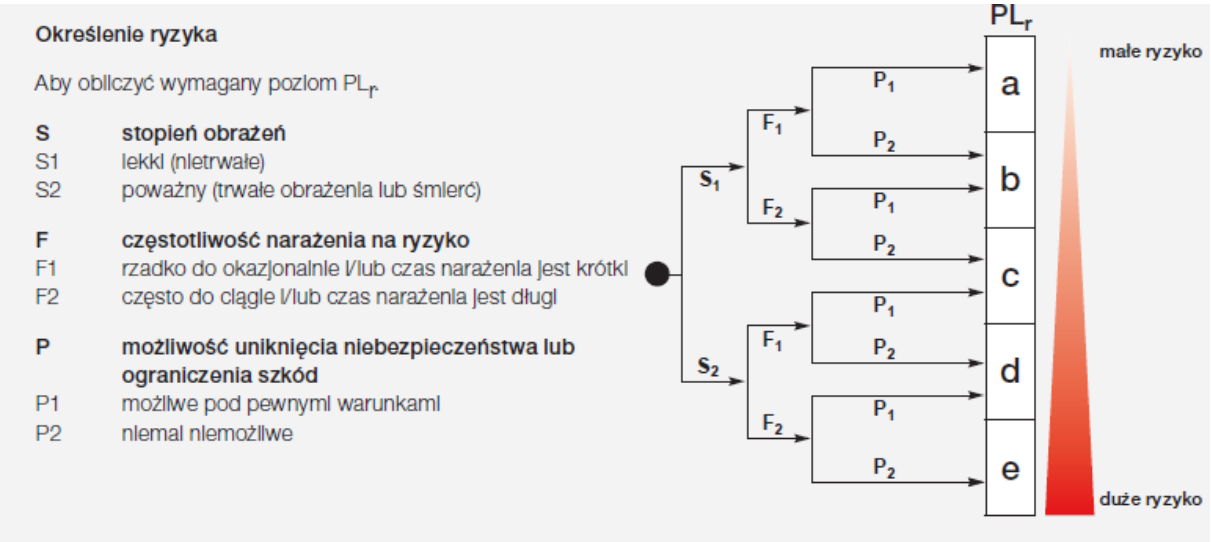


Krok 1: Ocena i minimalizacja ryzyka

Według EN ISO 13849-1 ryzyko określane jest na podstawie trzech czynników: stopnia obrażeń (S, severity), częstotliwości narażenia na ryzyko (F, frequency) oraz możliwości uniknięcia lub ograniczenia obrażeń (P, possibility). Dla każdego czynnika podane są dwie możliwości. Granica między nimi nie jest sprecyzowanaw normie, ale stosuje się następujące ogólnie przyjęte interpretacje:

- S1 obrzęki, otarcia, rany kłute i niewielkie zmiażdżenia
- S2 urazy kostne, amputacje i śmierć
- F1 rzadziej, niż co dwa tygodnie
- F2 częściej, niż co dwa tygodnie
- P1 powolne ruchy maszyny, dużo miejsca, mała moc
- P2 szybkie ruchy maszyny, ciasno, duża moc

Określając wartości S, F i P, można uzyskać wymagany parametr PLr konieczny dla oszacowania źródła ryzyka. Ocena ryzyka uwzględnia także szacowanie ryzyka. Określa się w niej, czy istnieje konieczność redukcji ryzyka, czy też zapewnione jest wystarczające bezpieczeństwo.



Krok 2

Jeżeli wymagana jest redukcja ryzyka, należy przestrzegać kolejności działań zgodnych z Dyrektywą Maszynową:

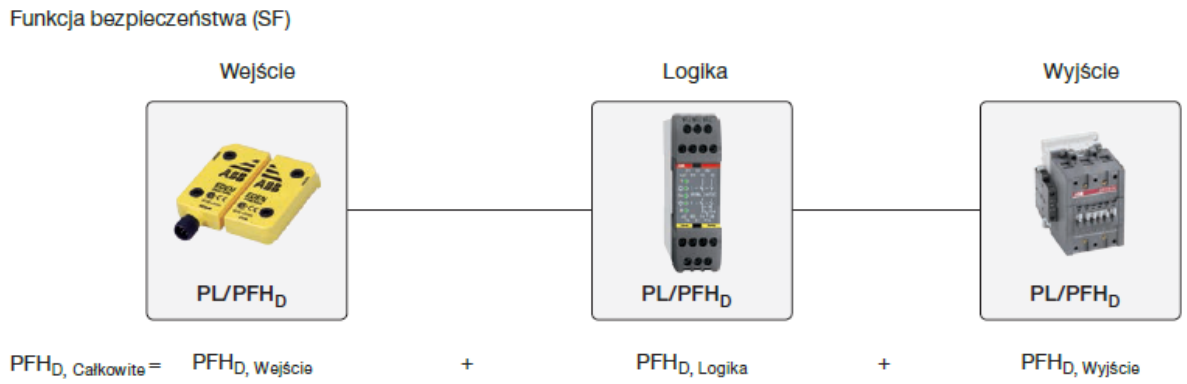
- Uniknięcie ryzyka już na etapie projektowania. (np. zmniejszenie mocy, uniknięcie interferencji w strefie zagrożenia.)
- Zastosowanie ochrony i/lub urządzeń bezpieczeństwa. (np. wygrodzenie, fotokomórki lub urządzenia sterujące.)
- Udostępnienie informacji o bezpiecznym sposobie użytkowania maszyny. (np. w instrukcjach lub na oznaczeniach.)

Krok 3

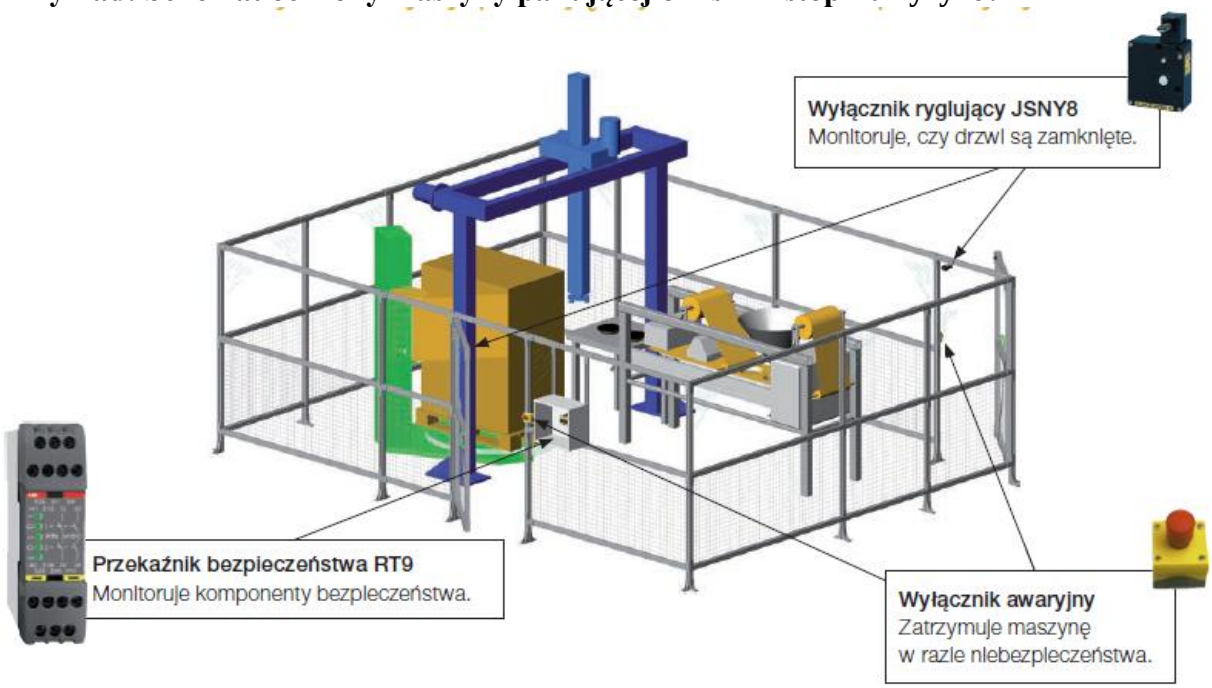
Przy obliczaniu PL dla funkcji bezpieczeństwa systemu, najłatwiej jest podzielić go na osobne, dobrze zdefiniowane bloki (zwane także podsystemami). Często logicznym jest dokonanie podziału ze względu na wejście, logikę i wyjście (np. Wyłącznik – przekaźnik bezpieczeństwa - styczniki), ale bloków może być też więcej, niż trzy, w zależności od połączenia i liczby zastosowanych komponentów (przekaźnik rozszerzenia może tworzyć dodatkowy blok logiczny).

Dla każdego bloku oblicza się wartość PL lub PFHD. Najłatwiej jest pozyskać te wartości od producenta komponentu, aby nie trzeba było ich obliczać samodzielnie. Producent wyłączników, czujników i urządzeń logiki często jest w posiadaniu wartości PL i PFHD dla swoich komponentów, ale dla urządzeń wyjściowych (takich jak styczniki i zawory) zwykle nie określa się tych wartości, gdyż zależą one od częstotliwości użytkowania komponentu. Można je zatem obliczyć samodzielnie według EN ISO 13849-1 lub skorzystać z przykładowych, gotowych i obliczonych rozwiązań, takich jak te od ABB Jokab Safety.

Aby obliczyć PL lub PFHD dla bloku, konieczna jest znajomość jego kategorii, DC i MTTFD. Ponadto, należy wystrzegać się błędów systematycznych i upewnić się, że błąd nie wyeliminuje obydwu kanałów, a także nie będzie generować i dokonywać walidacji oprogramowania. Poniższy tekst w skrócie omawia to zagadnienie.



Przykład: Schemat ochrony maszyny pakującej o niskim stopniu ryzyka.



Krok 1 (ocena ryzyka):

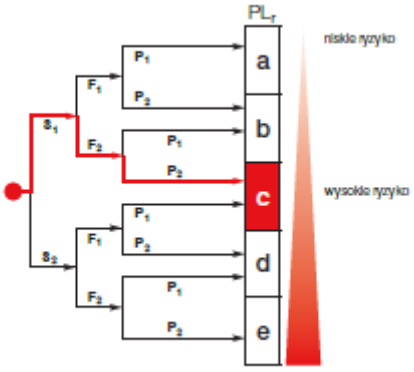
Żywność do zapakowania jest ładowana do klatki ręcznie tylnymi drzwiami. Następnie w zasobniku przygotowywana jest partia dla przenośnika pakującego. Klatka jest resetowana i restartowana. Maszyna pakująca z przenośnikiem taśmowym działa tylko wtedy, gdy zarówno jedne jak i drugie drzwi są zamknięte i gdy system zabezpieczający został zresetowany.
Podczas szacowania ryzyka ustalono, że maszyna ma pracować w trybie trójzmianowym (8 godzin na zmianę), 365 dni w roku. Zakłada się, że zaburzenia w pracy maszyny udaje się usunąć w czasie poniżej jednej minuty w strefie zagrożenia. Może to mieć miejsce dwa razy w ciągu godziny (F2). Nieoczekiwane uruchomienie nie może być przyczyną poważnych

obrażeń, a co najwyżej niewielkich, uleczalnych urazów (S1). Operator z założenia nie ma możliwości uniknięcia obrażeń, gdyż maszyna porusza się szybko (P2).

Ocena dla funkcji bezpieczeństwa wymaganej do uzyskania dostępu do maszyny wynosi PL_r= c (S1, F2, P2). Oprócz tej funkcji bezpieczeństwa, konieczna jest funkcja zatrzymania awaryjnego. Jest ona także oceniana jako PL_r

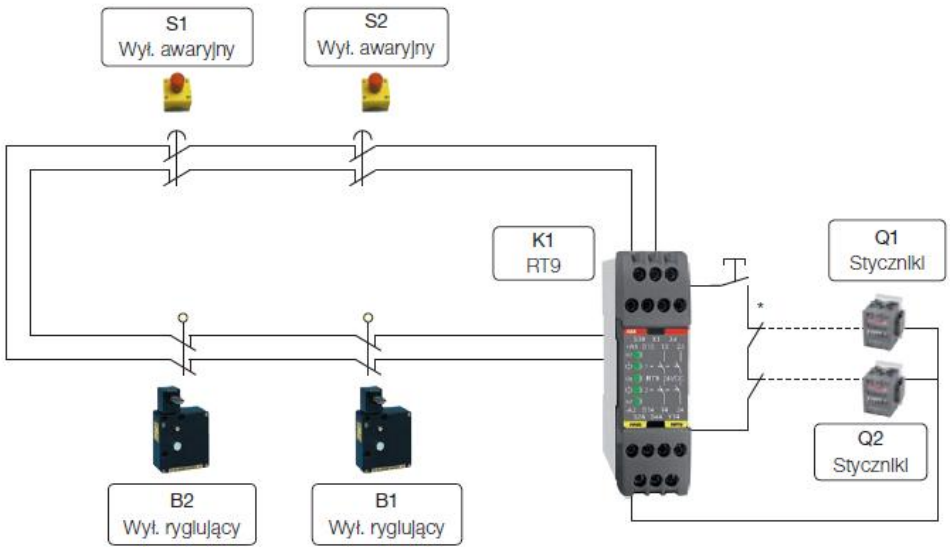
Krok 2 (redukcja ryzyka):

Jako zabezpieczenie wybrano drzwi blokowane z wyłącznikiem ryglującym JSNY8. Czas dobiegu jest na tyle krótki, że dojdzie do zatrzymania niebezpiecznego ruchu zanim operator będzie mógł uzyskać dostęp do maszyny. Wyłącznik awaryjny jest umiejscowiony w zasięgu ręki, po obu stronach klatki w pobliżu zamkniętych drzwi.



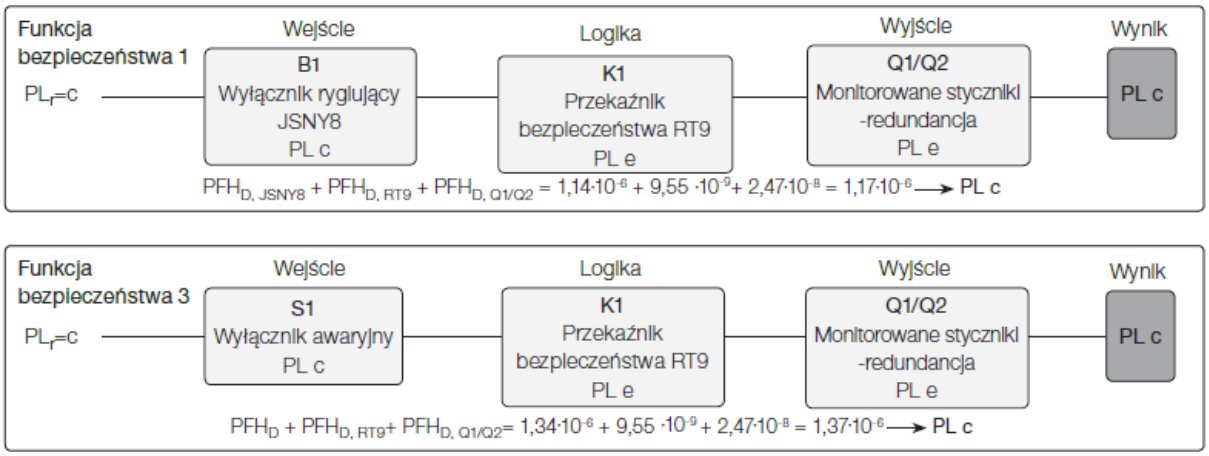
Ocena PLr wymaganego dla funkcji bezpieczeństwa z blokadą drzwi dla tego przykładu.

Krok 3 (obliczanie funkcji bezpieczeństwa):



Blok startowy składający się z podwójnych niemonitorowanych styczników został obliczony na 2.47·10-8. Funkcje bezpieczeństwa są reprezentowane przez schematy blokowe.

Funkcje bezpieczeństwa 1 i 2 są identyczne, dlatego też pokazana jest tylko funkcja 1.
Funkcje bezpieczeństwa 3 i 4 są identyczne, dlatego też pokazana jest tylko funkcja 3.



Powodem uzyskania tylko PL c przy tym rozwiązaniu jest fakt zastosowania jednego wyłącznika ryglującego na drzwi. Gdyby zastosowano dwa wyłączniki ryglujące na drzwi, możliwe byłoby uzyskanie PL d, ale wiązałoby się to z koniecznością dodatkowego monitoringu każdego z wyłączników.

Uwaga: Gdyby ocena ryzyka wykazała możliwość zaistnienia poważnych obrażeń S2, rezultatem tego byłoby PLr=e. Oznaczałoby to, że powyższe rozwiązanie jest niewystarczające. Dla funkcji zatrzymania awaryjnego możliwe jest uzyskanie PL d, jednak przy założeniu, że można wykluczyć niektóre typy usterek.