Fundusze Europejskie dla Rozwoju Społecznego | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Politechnika Świętokrzyska
Wydział Mechatroniki i Budowy Maszyn

Kierunek studiów:
Mechanika i Budowa Maszyn

Szczepan Kostecki

Materiały dydaktyczne do przedmiotu

BEZPIECZEŃSTWO MASZYN

opracowane w ramach realizacji Projektu
„**Dostosowanie kształcenia w Politechnice Świętokrzyskiej do potrzeb współczesnej gospodarki**”
FERS.01.05-IP.08-0234/23

Kielce, 2025

Spis treści

1. Wprowadzenie do bezpieczeństwa maszyn

Współczesne projektowanie maszyn wymaga nie tylko wiedzy z zakresu mechaniki, automatyki i materiałoznawstwa, ale także dogłębnego zrozumienia zasad bezpieczeństwa. Każdy projektant, konstruując urządzenie, powinien postrzegać bezpieczeństwo nie jako dodatkowy wymóg formalny, lecz jako integralny element procesu inżynierskiego. Bezpieczna maszyna to taka, która jest niezawodna, przewidywalna w działaniu oraz przyjazna użytkownikowi**,** a jednocześnie spełnia wymagania obowiązujących przepisów prawnych i norm technicznych.

Bezpieczeństwo maszyn stanowi zatem obszar łączący prawo, inżynierię i ergonomię. To właśnie na styku tych trzech dziedzin kształtuje się współczesne podejście do projektowania urządzeń, w którym kluczową rolę odgrywa analiza ryzyka, ocena niezawodności komponentów oraz zapewnienie zgodności konstrukcji z wymaganiami norm zharmonizowanych. W praktyce oznacza to, że projektant musi nie tylko rozumieć zasady działania maszyny, ale również umieć przewidzieć jej potencjalne zagrożenia i zastosować odpowiednie środki ochronne już na etapie koncepcji.

W dobie dynamicznego rozwoju automatyzacji, robotyzacji i cyfryzacji, odpowiedzialność za bezpieczeństwo spoczywa przede wszystkim na konstruktorach i integratorach systemów, którzy muszą umiejętnie łączyć wiedzę techniczną z wymogami prawnymi. Zapewnienie bezpieczeństwa nie ogranicza się do instalacji osłon czy przycisków awaryjnych — obejmuje cały cykl życia maszyny: od projektu koncepcyjnego, przez montaż i uruchomienie, po eksploatację i wycofanie z użycia.

Najważniejszym dokumentem Unii Europejskiej regulującym wymagania stawiane maszynom i urządzeniom jest Dyrektywa Maszynowa 2006/42/WE, która określa minimalne wymagania zasadnicze dotyczące bezpieczeństwa i ochrony zdrowia w procesie projektowania oraz produkcji maszyn (Dyrektywa 2006/42/WE, Dz.U. UE L 157/24, 2006; European Commission, 2019). W 2023 roku przyjęto nowe Rozporządzenie Maszynowe (UE) 2023/1230, które zastąpi dyrektywę od 20 stycznia 2027 r.

Nowe przepisy rozszerzają dotychczasowe wymagania o kwestie związane z bezpieczeństwem oprogramowania, systemów autonomicznych oraz cyberbezpieczeństwem.

Najważniejsze z nich to:

- rozszerzenie zakresu stosowania – rozporządzenie obejmuje nie tylko klasyczne maszyny, ale również maszyny sterowane oprogramowaniem, systemy autonomiczne i komponenty cyfrowe wpływające na bezpieczeństwo działania,
- bezpieczeństwo cybernetyczne – dodano obowiązek ochrony przed nieuprawnionym dostępem i ingerencją w systemy sterowania. Producent musi zapewnić integralność danych, w tym aktualizacji oprogramowania, które nie mogą obniżać poziomu bezpieczeństwa maszyny,
- oprogramowanie jako element bezpieczeństwa – aktualizacje i modyfikacje oprogramowania są traktowane na równi z modernizacją sprzętową i wymagają ponownej oceny ryzyka,
- cyfrowa dokumentacja techniczna – dopuszczono pełną digitalizację dokumentacji, w tym deklaracji zgodności i instrukcji obsługi, które mogą być dostarczane w formie elektronicznej,
- nowa klasyfikacja maszyn wysokiego ryzyka – w załączniku I określono listę maszyn i komponentów, dla których wymagane jest zaangażowanie jednostki notyfikowanej,
- zastosowanie sztucznej inteligencji i systemów autonomicznych – rozporządzenie obejmuje maszyny wykorzystujące uczenie maszynowe oraz podejmujące decyzje bez bezpośredniego nadzoru człowieka,
- zwiększone obowiązki producentów – konieczność prowadzenia analiz bezpieczeństwa dla całego cyklu życia maszyny, w tym aktualizacji oprogramowania i zdalnego sterowania (Rozporządzenie (UE) 2023/1230; European Commission, 2023 – guidance).

Celem jednolitych wymagań technicznych i norm bezpieczeństwa jest:

- zwiększenie bezpieczeństwa użytkowników i operatorów maszyn,
- ograniczenie liczby wypadków i awarii wynikających z błędów konstrukcyjnych lub eksploatacyjnych,
- zapewnienie swobodnego przepływu maszyn w obrębie rynku wewnętrznego UE,
- podnoszenie jakości technicznej projektowanych i produkowanych urządzeń (EUR-Lex: Machinery Directive 2006/42/WE).

1.1. Znaczenie bezpieczeństwa w cyklu życia maszyny

Bezpieczeństwo jest jednym z kluczowych aspektów, które należy uwzględnić na każdym etapie cyklu życia maszyny — od fazy koncepcji, przez projektowanie, budowę, testy, eksploatację, aż po jej demontaż. W praktyce oznacza to, że już podczas tworzenia projektu konstruktor musi przewidzieć potencjalne zagrożenia

i zaprojektować takie rozwiązania, które wyeliminują lub zminimalizują ryzyko ich wystąpienia. Zasada ta stanowi fundament normy PN-EN ISO 12100:2012, która definiuje proces oceny i redukcji ryzyka jako element integralny projektowania (PN-EN ISO 12100:2012). Odpowiednio zaprojektowana maszyna nie wymaga późniejszego „doposażania" w środki bezpieczeństwa — jest bezpieczna z założenia (safety by design).

Cykl życia maszyny obejmuje wszystkie etapy jej funkcjonowania – od pomysłu i projektu po wycofanie z użytkowania. W każdym z tych etapów można wyróżnić specyficzne działania wpływające na poziom bezpieczeństwa. Na etapie projektowania i koncepcji szczególne znaczenie ma identyfikacja potencjalnych zagrożeń i analiza funkcji maszyny. Już wtedy konstruktor decyduje o tym, czy rozwiązanie będzie bezpieczne z założenia, na przykład poprzez zastosowanie napędów o ograniczonej sile lub mechanicznych blokad zapobiegających niekontrolowanemu ruchowi. W fazie wytwarzania istotne jest zapewnienie odpowiedniej jakości materiałów, prawidłowego montażu i konfiguracji elementów bezpieczeństwa, takich jak czujniki, blokady czy osłony, które muszą być zgodne z projektem i normami. Podczas uruchomienia i eksploatacji należy zadbać o właściwe działanie środków ochronnych, przeprowadzenie szkoleń dla operatorów oraz weryfikację zgodności działania maszyny z deklarowanym poziomem bezpieczeństwa. W trakcie użytkowania maszyny wymaganie jest utrzymanie i modernizacja, obejmujące regularne przeglądy, testy okresowe i ocenę wpływu ewentualnych zmian konstrukcyjnych na bezpieczeństwo. Każda modyfikacja, nawet pozornie drobna, może zmienić charakter zagrożeń i wymaga ponownej oceny ryzyka. W końcu, na etapie wycofania z użytkowania, należy zapewnić bezpieczny demontaż i utylizację komponentów, które mogą stanowić zagrożenie dla środowiska lub ludzi – na przykład zbiorników ciśnieniowych, elementów pod napięciem lub części zawierających substancje niebezpieczne.

Zachowanie bezpieczeństwa na wszystkich etapach cyklu życia maszyny wymaga nie tylko stosowania odpowiednich środków technicznych, lecz także świadomego podejścia projektanta, który od początku odpowiada za jakość i niezawodność rozwiązania. To właśnie w fazie projektowej podejmowane są decyzje mające największy wpływ na bezpieczeństwo użytkowników – wybór koncepcji napędu, rodzaju układów sterowania, sposobu zabezpieczenia dostępu czy rozmieszczenia elementów obsługowych. Na tym etapie nawet drobne błędy konstrukcyjne mogą później skutkować awariami lub wypadkami przy pracy.

Projektant maszyny ponosi więc odpowiedzialność techniczną, prawną i etyczną za zapewnienie zgodności konstrukcji z obowiązującymi przepisami oraz rzeczywistego bezpieczeństwa jej użytkowania. Zgodnie z wymaganiami Dyrektywy 2006/42/WE i Rozporządzenia (UE) 2023/1230, producent lub konstruktor działający w jego imieniu ma obowiązek wykazać, że maszyna spełnia zasadnicze wymagania bezpieczeństwa (Dyrektywa 2006/42/WE, 2006; Rozporządzenie (UE) 2023/1230, 2023). Wymaga to opracowania pełnej dokumentacji technicznej, wykonania oceny ryzyka, przygotowania deklaracji zgodności WE i umieszczenia oznakowania CE potwierdzającego dopuszczenie maszyny do obrotu na rynku europejskim.

Jednocześnie odpowiedzialność projektanta nie kończy się na spełnieniu wymagań formalnych. Etyczny wymiar pracy inżyniera polega na dążeniu do tworzenia rozwiązań, które nie tylko są zgodne z przepisami, ale również rzeczywiście chronią użytkownika. Nawet tam, gdzie przepisy dopuszczają minimalne środki ochronne, projektant powinien kierować się zasadą design for safety – projektowania dla bezpieczeństwa, wybierając rozwiązania techniczne eliminujące ryzyko u źródła (Pamuła, 2011; Dźwiarek, 2012).

Tym samym odpowiedzialność za bezpieczeństwo łączy się nierozerwalnie z dążeniem do niezawodności konstrukcji. Maszyna, która często ulega awariom, nie może być uznana za bezpieczną, ponieważ każdy przestój czy uszkodzenie elementu sterującego zwiększa ryzyko wypadku. Z drugiej strony, nadmiernie skomplikowany system bezpieczeństwa o niskiej niezawodności może sam w sobie generować zagrożenia. Dlatego konstruktor powinien szukać równowagi między poziomem bezpieczeństwa a niezawodnością systemu, uwzględniając parametry techniczne takie jak MTTFd (średni czas do niebezpiecznej awarii), DC_{avg} (średnie pokrycie diagnostyczne) oraz CCF (wspólne przyczyny awarii), zgodnie z normą PN-EN ISO 13849-1:2023-09. Parametry te pozwalają ilościowo ocenić trwałość i odporność systemu bezpieczeństwa, stanowiąc pomost między inżynierią niezawodności a bezpieczeństwem funkcjonalnym.

W praktyce oznacza to, że dobrze zaprojektowana maszyna jest nie tylko efektywna, ale również bezpieczna przez swoją konstrukcyjną niezawodność. Takie podejście, zgodne z zasadą „bezpieczeństwa poprzez niezawodność”, powinno być podstawową ideą towarzyszącą każdemu projektowi inżynierskiemu.

1.2. Podstawy prawne i normatywne

Bezpieczeństwo maszyn w krajach Unii Europejskiej opiera się na wspólnych przepisach prawnych i zharmonizowanym systemie norm technicznych. Celem tego systemu jest zapewnienie jednolitego poziomu bezpieczeństwa, ułatwienie swobodnego przepływu towarów oraz stworzenie jasnych zasad dla projektantów i producentów. W praktyce oznacza to, że każdy konstruktor maszyny musi znać zarówno obowiązujące akty prawne, jak i odpowiednie normy techniczne, ponieważ to ich łączne stosowanie pozwala zaprojektować maszynę zgodną z wymaganiami UE (Dyrektywa 2006/42/WE, 2006; Rozporządzenie (UE) 2023/1230, 2023).

Podstawowym aktem prawnym regulującym bezpieczeństwo maszyn przez wiele lat była Dyrektywa 2006/42/WE, znana jako Dyrektywa Maszynowa. Określała ona zasadnicze wymagania w zakresie bezpieczeństwa i ochrony zdrowia, które muszą zostać spełnione, zanim maszyna zostanie wprowadzona do obrotu lub oddana do użytku. Wymagania te obejmowały między innymi konstrukcję mechaniczną, zabezpieczenia przed zagrożeniami elektrycznymi i termicznymi, ergonomię stanowiska pracy oraz odpowiednie oznakowanie i informowanie użytkownika. Dynamiczny rozwój technologii, automatyzacji i integracji systemów mechatronicznych ujawnił jednak potrzebę aktualizacji tych przepisów, zwłaszcza w obszarze systemów sterowania i oprogramowania.

Odpowiedzią na te potrzeby jest Rozporządzenie (UE) 2023/1230, przyjęte w 2023 roku i obowiązujące od 20 stycznia 2027 r. (Rozporządzenie (UE) 2023/1230, 2023). W odróżnieniu od dyrektywy, rozporządzenie nie wymaga wdrożenia do prawa krajowego – obowiązuje bezpośrednio we wszystkich państwach członkowskich. Nowe przepisy wzmacniają wymogi dotyczące cyberbezpieczeństwa, oprogramowania sterującego, systemów autonomicznych, sztucznej inteligencji oraz zdalnego sterowania (European Commission, 2023). Wprowadzają także pojęcie „maszyn wysokiego ryzyka”, dla których przewidziano rozszerzoną procedurę oceny zgodności z udziałem jednostek notyfikowanych. Dla projektantów oznacza to konieczność szerszego podejścia do bezpieczeństwa, obejmującego już nie tylko elementy mechaniczne, ale również cyfrowe aspekty sterowania.

W praktyce projektowej Dyrektywa Maszynowa i Rozporządzenie Maszynowe bardzo często współistnieją z innymi dyrektywami sektorowymi, które obejmują szczególne grupy zagrożeń lub typy urządzeń.

Oto najczęściej spotykane z nich w kontekście mechaniki i budowy maszyn:

- Dyrektywa Niskonapięciowa (LVD 2014/35/UE) – reguluje kwestie bezpieczeństwa urządzeń elektrycznych pracujących w zakresie napięć od 50 do 1000 V AC oraz od 75 do 1500 V DC. Jej celem jest ochrona przed porażeniem prądem, przegrzaniem, łukiem elektrycznym i innymi zagrożeniami elektrycznymi. Ma zastosowanie m.in. do układów sterowania, napędów elektrycznych oraz urządzeń zasilających w maszynach.
- Dyrektywa Kompatybilności Elektromagnetycznej (EMC 2014/30/UE) – określa wymagania dotyczące odporności i emisji elektromagnetycznej urządzeń elektrycznych i elektronicznych. W kontekście maszyn zapewnia, że układy sterowania nie zakłócają działania innych urządzeń i są odporne na wpływ zakłóceń z zewnątrz. Projektanci muszą więc stosować odpowiednie środki, takie jak ekranowanie przewodów, filtry EMI czy uziemienie konstrukcji.
- Dyrektywa Urządzenia Przeznaczone do Pracy w Atmosferach Potencjalnie Wybuchowych (ATEX 2014/34/UE) – dotyczy urządzeń i systemów ochronnych przeznaczonych do pracy w atmosferach potencjalnie wybuchowych, np. w obecności gazów, pyłów lub oparów. Wymaga oceny ryzyka zapłonu oraz doboru komponentów o odpowiednim poziomie ochrony przeciwwybuchowej.
- Dyrektywa Ciśnieniowa (PED – 2014/68/UE) – obejmuje urządzenia i zespoły, w których występuje nadciśnienie powyżej 0,5 bar. Ma kluczowe znaczenie w konstrukcjach hydraulicznych, pneumatycznych i termicznych, takich jak zbiorniki, siłowniki, zawory czy przewody ciśnieniowe. Dyrektywa PED określa wymagania dotyczące projektowania, materiałów, prób wytrzymałościowych oraz nadzoru technicznego.

Wiele maszyn podlega więc równoczesnemu zastosowaniu kilku dyrektyw. Przykładowo, prasa hydrauliczna z napędem elektrycznym może podlegać zarówno Dyrektywie Maszynowej, jak i PED, LVD oraz EMC. Dlatego konstruktorzy muszą na etapie projektowania zidentyfikować wszystkie obowiązujące dyrektywy i rozporządzenia, a następnie uwzględnić ich wymagania w dokumentacji technicznej i procesie oceny zgodności (PN-EN ISO 12100:2012)
Przepisy prawne określają, co należy osiągnąć, czyli cel bezpieczeństwa, natomiast normy techniczne precyzują, jak ten cel można osiągnąć. To one przekładają zapisy prawne na konkretne rozwiązania konstrukcyjne i metody projektowania.

Zharmonizowany system norm bezpieczeństwa ma charakter hierarchiczny i obejmuje trzy poziomy – A, B i C (PN-EN ISO 12100:2012). Normy typu A definiują ogólne zasady projektowania i podstawowe pojęcia bezpieczeństwa, np. PN-EN ISO 12100:2012. Normy typu B odnoszą się do określonych aspektów bezpieczeństwa

lub środków ochronnych. Normy typu B dzielą się natomiast na normy typu B1 dotyczące ogólnych zagadnień bezpieczeństwa, takich jak odległości ochronne (PN-EN ISO 13855:2025-06) czy bezpieczeństwo elektryczne (PN-EN 60204-1:2018-12) oraz normy typu B2 opisujące konkretne środki ochronne, takie jak kurtyny świetlne, rygle bezpieczeństwa czy przyciski zatrzymania awaryjnego (PN-EN ISO 13850:2016-03). Z kolei normy typu C definiują wymagania dla konkretnych grup maszyn – np. pras, wtryskarek czy suwnic – i mają pierwszeństwo w przypadku rozbieżności z normami typu A lub B.

Szczególne znaczenie wśród norm typu B ma PN-EN ISO 13849-1:2023-09, która zastąpiła wcześniejsze wydanie z 2016 roku. Określa ona zasady projektowania i oceny części systemów sterowania związanych z bezpieczeństwem.
Norma ta wprowadza metodykę obliczania parametrów niezawodnościowych, takich jak MTTFd (średni czas do niebezpiecznej awarii), DC_{avg} (średnie pokrycie diagnostyczne) i CCF (wspólne przyczyny awarii), pozwalających określić osiągany poziom bezpieczeństwa funkcjonalnego (PN-EN ISO 13849-1:2023-09; Dźwiarek, 2012; Pamuła, 2011).

Zrozumienie hierarchii norm i ich powiązań z przepisami prawnymi umożliwia projektantowi płynne przejście od ogólnych zasad bezpieczeństwa do konkretnych rozwiązań technicznych. Normy typu A wyznaczają ramy projektowe, normy typu B wskazują rozwiązania szczegółowe dla funkcji i urządzeń, a normy typu C odnoszą się do konkretnych maszyn. Dzięki temu proces projektowania staje się uporządkowany, a gotowy produkt – zgodny zarówno z wymogami prawnymi, jak i z zasadami dobrej praktyki inżynierskiej.

2. Proces oceny ryzyka wg PN-EN ISO 12100

Projektowanie bezpiecznych maszyn wymaga nie tylko znajomości przepisów prawnych i norm technicznych, ale także umiejętności ich praktycznego zastosowania w procesie inżynierskim. Kluczowym narzędziem, które łączy wymagania prawne z rzeczywistym projektem technicznym, jest ocena ryzyka. To właśnie na jej podstawie projektant podejmuje decyzje dotyczące konstrukcji, doboru środków ochronnych i sposobu użytkowania maszyny.

Norma PN-EN ISO 12100:2012 stanowi podstawowy dokument odniesienia dla oceny bezpieczeństwa w całym cyklu życia maszyny – od etapu koncepcji po demontaż. Zawiera metodyczne zasady identyfikacji zagrożeń, szacowania i redukcji ryzyka, a także opisuje proces decyzyjny, który powinien być stosowany przez

projektantów, producentów i integratorów systemów. Norma ta należy do grupy norm typu A, czyli takich, które formułują ogólne wymagania mające zastosowanie do wszystkich rodzajów maszyn, niezależnie od ich przeznaczenia (PN-EN ISO 12100:2012).

Ocena ryzyka jest procesem iteracyjnym – powtarzanym wielokrotnie w miarę rozwoju projektu. Każda zmiana konstrukcyjna, modernizacja lub aktualizacja oprogramowania może wpływać na poziom ryzyka i wymagać ponownej analizy. Wyniki oceny ryzyka stanowią nie tylko podstawę doboru odpowiednich środków ochronnych, ale także kluczowy element dokumentacji technicznej oraz deklaracji zgodności WE. Dlatego dla projektanta umiejętność prawidłowego przeprowadzenia tego procesu jest równie istotna jak znajomość zasad wytrzymałości materiałów czy analizy naprężeń (Dźwiarek, 2012; Pamuła, 2011)

2.1. Etapy procesu oceny ryzyka

Ocena ryzyka jest podstawowym elementem projektowania bezpiecznej maszyny. Norma PN-EN ISO 12100:2012 definiuje ją jako systematyczny proces identyfikowania zagrożeń, oszacowania ryzyka i podejmowania działań w celu jego redukcji. Celem tego procesu jest zapewnienie, że maszyna będzie bezpieczna w każdym etapie jej cyklu życia – od montażu, przez użytkowanie i konserwację, aż po demontaż (PN-EN ISO 12100:2012).

Proces oceny ryzyka przebiega w czterech głównych etapach:

1) Identyfikacja zagrożeń – polega na rozpoznaniu wszystkich możliwych źródeł zagrożeń związanych z konstrukcją maszyny, jej otoczeniem i sposobem użytkowania. Identyfikacja zagrożeń jest kluczowa, ponieważ pominięcie choćby jednego czynnika może prowadzić do niepełnej oceny bezpieczeństwa. Wyróżnia się m.in. zagrożenia:
   - mechaniczne (np. zmiażdżenie, wciągnięcie, uderzenie przez ruchome elementy),
   - elektryczne (porażenie prądem, przepięcia, łuk elektryczny),
   - termiczne (oparzenie, odmrożenie),
   - ergonomiczne (nieprawidłowa postawa, wymuszone ruchy),
   - hałasem i wibracjami,
   - chemiczne i biologiczne,
   - wynikające z błędów użytkownika.

2) Szacowanie ryzyka – po zidentyfikowaniu zagrożeń należy określić prawdopodobieństwo ich wystąpienia i potencjalne skutki. Norma PN-EN ISO 12100 wskazuje trzy podstawowe parametry, które służą do oszacowania poziomu ryzyka:
   - S – severity (ciężkość skutków, np. uraz lekki, poważny lub śmiertelny),
   - F – frequency (częstotliwość i czas narażenia na zagrożenie),
   - P – possibility (możliwość uniknięcia lub ograniczenia skutków zagrożenia).

   W praktyce wartości tych parametrów wykorzystuje się do oceny poziomu ryzyka, np. w formie grafu lub matrycy.

3) Redukcja ryzyka – po oszacowaniu poziomu ryzyka należy zastosować odpowiednie środki ochronne. Norma określa tzw. hierarchię środków bezpieczeństwa, w której pierwszeństwo mają działania konstrukcyjne:
   - eliminacja zagrożenia u źródła (np. przez zmianę geometrii lub sposobu działania maszyny),
   - zastosowanie środków technicznych zabezpieczających (np. osłony, kurtyny świetlne, wyłączniki awaryjne),
   - środki organizacyjne i informacyjne (instrukcje, szkolenia, oznakowanie).

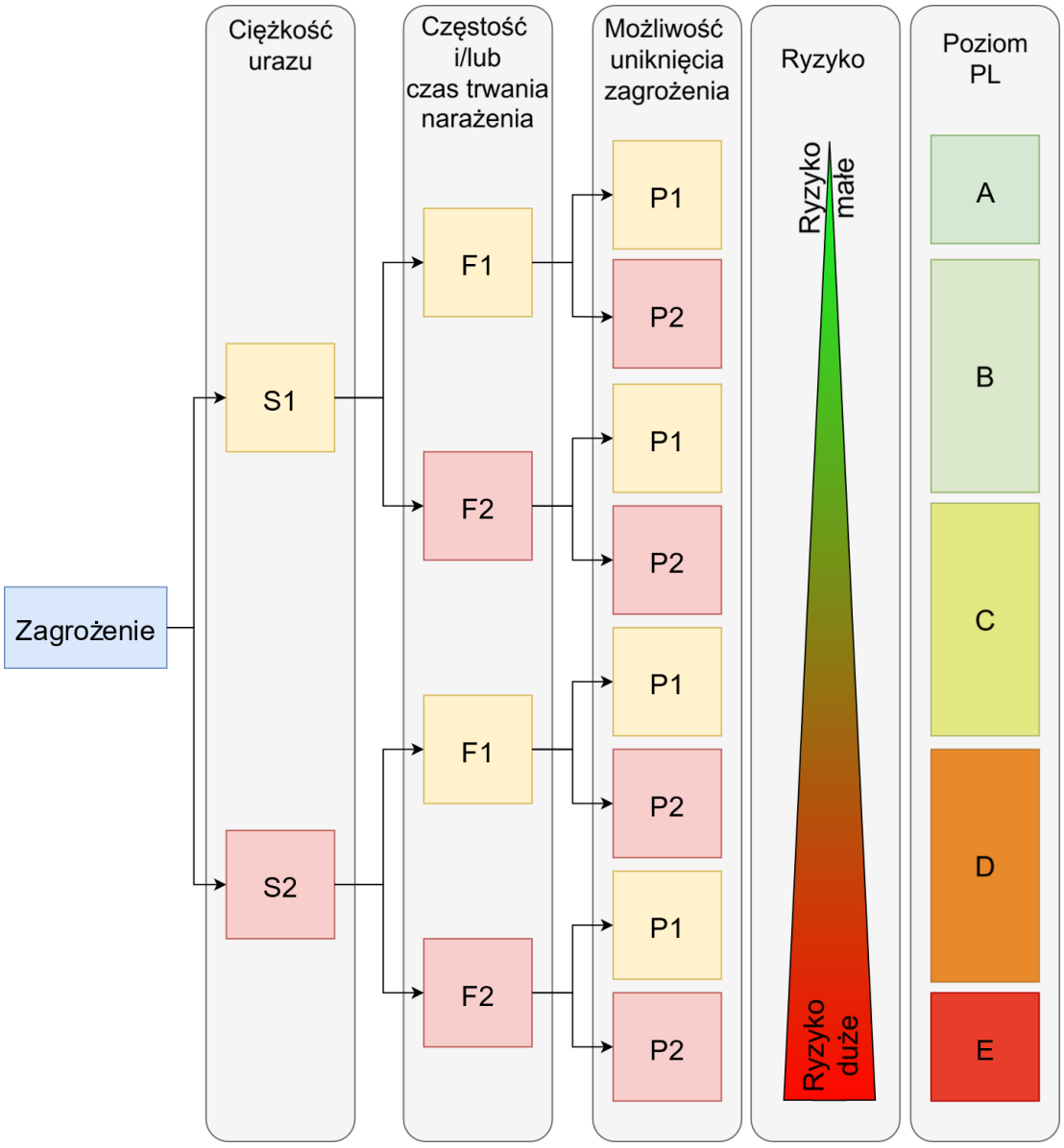
4) Ocena ryzyka resztkowego – po wdrożeniu środków ochronnych należy ocenić, czy pozostałe (resztkowe) ryzyko jest na poziomie akceptowalnym. Jeśli ryzyko jest nadal zbyt wysokie, konieczne jest ponowne przeanalizowanie projektu i wprowadzenie dodatkowych zabezpieczeń. Akceptowalność ryzyka zależy od charakteru maszyny, warunków jej użytkowania oraz społecznych i branżowych standardów bezpieczeństwa (Pamuła, 2011; Dźwiarek, 2012).

2.2. Metody oceny ryzyka

Proces oceny ryzyka, opisany w normie PN-EN ISO 12100:2012, nie wskazuje jednej obowiązującej metody obliczeniowej, lecz dopuszcza różne podejścia w zależności od rodzaju maszyny, dostępnych danych i potrzeb użytkownika. W praktyce inżynierskiej stosuje się zarówno metody jakościowe (ocena opisowa, np. graf lub matryca ryzyka), półilościowe (HRN), jak i ilościowe (LOPA). Wszystkie mają ten sam cel — określenie poziomu ryzyka i wskazanie, czy zastosowane środki ochronne są wystarczające.

[Tekst alternatywny. Graf szacowania ryzyka zgodnie z PN-EN ISO 12100. Schemat przedstawia drzewo decyzyjne (graf) używany do szacowania poziomu ryzyka przy projektowaniu maszyn. Punkt początkowy prowadzi do dwóch gałęzi

odpowiadających ciężkości skutków zagrożenia: *S1 – obrażenia lekkie lub średnie* oraz *S2 – obrażenia ciężkie lub śmiertelne*. Każda z gałęzi rozdziela się następnie na dwa poziomy częstotliwości narażenia: *F1 – rzadkie lub krótkotrwałe narażenie* oraz *F2 – częste lub długotrwałe narażenie*. Od każdego poziomu F odchodzą kolejne rozgałęzienia zależne od możliwości uniknięcia zagrożenia: *P1 – możliwe do uniknięcia w większości przypadków* i *P2 – trudne do uniknięcia lub nieuniknione*. Każda ścieżka kończy się przypisaniem poziomu wymaganego bezpieczeństwa funkcjonalnego oznaczonego literami od **a** (najniższy poziom ryzyka) do **e** (najwyższy poziom ryzyka).]



Rys. 1. Graf szacowania ryzyka zgodnie z PN-EN ISO 12100

Wśród tych metod najbardziej rozpowszechnioną i bezpośrednio opisaną w normie ISO 12100 jest metoda grafu ryzyka (Risk Graph), która stanowi podstawę do określenia wymaganego poziomu bezpieczeństwa (PLr) dla funkcji bezpieczeństwa.

Graf ryzyka to metoda jakościowa, która pozwala w sposób logiczny i uporządkowany oszacować poziom ryzyka na podstawie trzech parametrów opisanych już wcześniej: S, F, P. Każdy z parametrów posiada przypisane poziomy (np. niski / wysoki), które w połączeniu prowadzą do określenia poziomu ryzyka. Na rysunku powyżej (Rys. 1) przedstawiono przykładowy graf ryzyka opracowany zgodnie z PN-EN ISO 12100.

Graf ma strukturę drzewiastą i składa się z trzech kolejnych poziomów decyzyjnych:

1) Ciężkości obrażeń (S) – punkt wyjścia procesu oceny:
   - S1 – obrażenia lekkie (odwracalnie),
   - S2 – obrażenia ciężkie (nie odwracalne poważne urazy, trwałe kalectwo lub śmierć).
2) Częstotliwość narażenia i czas trwania narażenia (F) – określa, jak często i jak długo osoba znajduje się w strefie zagrożenia:
   - F1 – ekspozycja rzadka i/lub krótkotrwała,
   - F2 – ekspozycja częsta i/lub długotrwała.
3) Możliwość uniknięcia zagrożenia lub ograniczenia szkody (P) – uwzględnia czas reakcji operatora, konstrukcję maszyny i prędkość zagrożenia:
   - P1 – możliwe uniknięcie zagrożenia (np. przez cofnięcie się, zatrzymanie maszyny),
   - P2 – trudne lub niemożliwe uniknięcie zagrożenia (np. szybki ruch części, ograniczona widoczność).

Każda ścieżka w grafie prowadzi do określonego poziomu ryzyka, który tanowi punkt wyjścia do określenia wymaganego poziomu bezpieczeństwa PLr (Performance Level required) w normie PN-EN ISO 13849-1:2023-09 lub poziomu SIL (Safety Integrity Level) w normie IEC 62061:2021. Metoda grafu jest więc uniwersalnym i zgodnym z normami narzędziem łączącym etap oceny ryzyka z projektowaniem systemów sterowania bezpieczeństwem.

2.3. Dokumentacja wyników oceny ryzyka

Proces oceny ryzyka ma sens tylko wtedy, gdy jego wyniki są odpowiednio udokumentowane i możliwe do zweryfikowania. Zgodnie z wymaganiami PN-EN ISO 12100:2012 oraz Rozporządzenia (UE) 2023/1230, każdy producent maszyny jest

zobowiązany do sporządzenia dokumentacji technicznej, która potwierdza, że proces oceny ryzyka został przeprowadzony w sposób systematyczny, kompletny i udokumentowany (PN-EN ISO 12100:2012; Rozporządzenie (UE) 2023/1230, 2023). Dokumentacja oceny ryzyka stanowi integralną część dokumentacji technicznej maszyny i jest jednym z kluczowych elementów w procesie oceny zgodności. Powinna umożliwiać osobie trzeciej – np. jednostce notyfikowanej, audytorowi lub organowi nadzoru rynku – prześledzenie toku analizy oraz sposobu, w jaki projektant ograniczył ryzyko do poziomu akceptowalnego.

Nie istnieje jeden sztywny wzór dokumentowania oceny ryzyka, jednak dobra praktyka inżynierska oraz zalecenia ISO 12100 wskazują, że dokumentacja powinna zawierać co najmniej następujące elementy:

- opis maszyny i zakres analizy – identyfikacja maszyny (nazwa, typ, producent, numer seryjny), opis funkcji, przeznaczenia i granic użytkowania (np. środowisko pracy, przewidziane i nieprzewidziane zastosowania).
- identyfikacja zagrożeń – lista wszystkich zidentyfikowanych zagrożeń wraz z ich przyczynami i potencjalnymi skutkami.
- wyniki oceny ryzyka przed zastosowaniem środków ochronnych – przypisanie wartości parametrów S, F, P
- środki redukcji ryzyka – opis zastosowanych rozwiązań technicznych, organizacyjnych i informacyjnych (np. osłony, blokady, oznakowanie, szkolenia).
- ocena ryzyka resztkowego – analiza pozostałych zagrożeń po wdrożeniu środków ochronnych i ocena, czy poziom ryzyka jest akceptowalny.
- wnioski i zalecenia – podsumowanie wyników analizy wraz z rekomendacjami dotyczącymi dalszych działań (np. konieczność testów, walidacji, monitorowania w eksploatacji).

Wyniki oceny ryzyka muszą być jednoznacznie powiązane z dokumentacją techniczną maszyny, a zwłaszcza z:

- rysunkami konstrukcyjnymi i schematami elektrycznymi,
- analizą bezpieczeństwa systemu sterowania (zgodnie z PN-EN ISO 13849-1:2023-09 lub IEC 62061:2021),
- instrukcją obsługi i konserwacji,
- deklaracją zgodności UE.

Dzięki temu możliwe jest prześledzenie logicznego ciągu: zagrożenie → analiza ryzyka → środki ochronne → wynik PL/SIL → potwierdzenie zgodności.
Zgodnie z zasadą przejrzystości, cała dokumentacja powinna być sporządzona w sposób umożliwiający jej ocenę przez osoby trzecie, a producent jest zobowiązany

przechowywać ją przez co najmniej 10 lat od daty wprowadzenia maszyny do obrotu (Rozporządzenie (UE) 2023/1230, 2023).

W praktyce zaleca się stosowanie kilku prostych zasad:

- dokumentować każdą decyzję projektową dotyczącą bezpieczeństwa, nawet jeśli uznasz ryzyko za znikome,
- stosować jednolity formularz lub arkusz oceny ryzyka dla całego projektu,
- korzystać z numeracji zagrożeń i odwołań do rysunków technicznych,
- aktualizować dokumentację po każdej modernizacji maszyny,
- powiąż wyniki z walidacją systemu sterowania (PL/SIL).

Właściwie prowadzona dokumentacja oceny ryzyka stanowi wymóg prawny i umożliwia weryfikację poprawności przyjętych założeń konstrukcyjnych, a w razie potrzeby – stanowi podstawę do weryfikacji oceny zgodności przez organy nadzoru lub jednostki certyfikujące.

3. Bezpieczeństwo funkcjonalne systemów sterowania

Ocena ryzyka stanowi pierwszy krok w zapewnieniu bezpieczeństwa maszyn, ale sama analiza nie wystarcza, jeśli nie zostanie przełożona na konkretne rozwiązania techniczne. Współczesne maszyny są coraz bardziej zautomatyzowane, a ich bezpieczeństwo zależy nie tylko od konstrukcji mechanicznej, lecz przede wszystkim od tego, jak układ sterowania reaguje na zagrożenia. Właśnie ta zdolność systemu do właściwego i niezawodnego działania w sytuacjach awaryjnych stanowi istotę bezpieczeństwa funkcjonalnego.

Bezpieczeństwo funkcjonalne (ang. Functional Safety) obejmuje wszystkie elementy systemu sterowania mające wpływ na bezpieczeństwo – od czujników wykrywających niebezpieczne zdarzenia, przez moduły logiczne, po elementy wykonawcze, które fizycznie zatrzymują ruch lub odcinają energię. To właśnie te układy realizują tzw. funkcje bezpieczeństwa (Safety Functions – SF), które minimalizują ryzyko zidentyfikowane wcześniej podczas oceny zgodnej z PN-EN ISO 12100.

W praktyce bezpieczeństwo funkcjonalne jest określane i weryfikowane przy użyciu dwóch norm zharmonizowanych:

- PN-EN ISO 13849-1:2023-09 – koncentrującej się na częściach systemu sterowania mających wpływ na bezpieczeństwo

- IEC 62061:2021 – obejmującej systemy sterowania bezpieczeństwem oparte na technologiach elektrycznych, elektronicznych i programowalnych.

Obie te normy stosują koncepcję poziomu zapewnienia bezpieczeństwa – odpowiednio PL (Performance Level) i SIL (Safety Integrity Level) – które określają prawdopodobieństwo poprawnego działania funkcji bezpieczeństwa w chwili wystąpienia zagrożenia. Wspólnym celem wyżej wymienionych norm jest zapewnienie, że funkcje bezpieczeństwa będą wykonywane z wymaganą niezawodnością i w odpowiednim czasie reakcji, tak aby ryzyko zostało zredukowane do poziomu akceptowalnego.

3.1. Pojęcie bezpieczeństwa funkcjonalnego oraz funkcji bezpieczeństwa

Bezpieczeństwo funkcjonalne stanowi kluczowy element nowoczesnych systemów sterowania maszynami i urządzeniami. Jego istotą jest zapewnienie, że układ sterowania reaguje w sposób bezpieczny, przewidywalny i niezawodny w sytuacjach zagrożenia, awarii lub błędów eksploatacyjnych. W odróżnieniu od bezpieczeństwa konstrukcyjnego (które wynika z cech fizycznych maszyny, np. osłon czy kształtu elementów), bezpieczeństwo funkcjonalne odnosi się do poprawnego działania systemów elektrycznych, elektronicznych i programowalnych, które mają wpływ na bezpieczeństwo operatora i otoczenia

Zgodnie z normą PN-EN 61508:2010, bezpieczeństwo funkcjonalne to „część ogólnego bezpieczeństwa systemu, która zależy od poprawnego działania funkcji realizowanych przez systemy elektryczne, elektroniczne lub programowalne elektroniczne związane z bezpieczeństwem”. Norma ta wprowadza cykl życia bezpieczeństwa, obejmujący planowanie, analizę ryzyka, projektowanie, walidację, eksploatację i wycofanie systemu, a także określa wymagania dotyczące niezawodności, testowania, redundancji i unikania wspólnych przyczyn awarii (CCF – Common Cause Failures).

Funkcją bezpieczeństwa nazywamy każde działanie systemu sterowania, które zapobiega wystąpieniu zdarzenia niebezpiecznego lub ogranicza jego skutki. Funkcje te są realizowane przez tzw. łańcuch bezpieczeństwa, obejmujący trzy podstawowe ogniwa:

- czujnik – wykrywa stan zagrożenia lub zmianę warunków (np. kurtyna świetlna, czujnik pozycji, wyłącznik krańcowy).

- logika – analizuje sygnał wejściowy i podejmuje decyzję o aktywacji reakcji (np. przekaźnik bezpieczeństwa, sterownik PLC Safety).
- element wykonawczy – realizuje fizyczne działanie ochronne, np. zatrzymuje napęd, odcina energię lub blokuje ruch.

System powinien być zaprojektowany zgodnie z zasadą „fail-safe", czyli tak, aby awaria nie prowadziła do utraty funkcji bezpieczeństwa, lecz do przejścia maszyny w stan bezpieczny. Odwrotne zachowanie – „fail-to-danger" – musi być eliminowane już na etapie projektu.

Współczesne napędy i sterowniki bezpieczeństwa realizują szereg funkcji bezpieczeństwa, które można łączyć w zależności od wymaganego poziomu ryzyka i rodzaju zagrożeń. Do najczęściej stosowanych należą:

- STO (Safe Torque Off) – Bezpieczne wyłączenie momentu obrotowego czyli całkowite odłączenie zasilania silnika, uniemożliwiające jego ruch.
- SS1 (Safe Stop 1) – Kontrolowane zatrzymanie maszyny, po którym następuje przejście do stanu STO.
- SS2 (Safe Stop 2) – Zatrzymanie z utrzymaniem sterowania pozycji – po zatrzymaniu aktywny stan SOS.
- SOS (Safe Operating Stop) – Bezpieczne zatrzymanie z utrzymaniem pozycji i gotowością do dalszej pracy.
- SLS (Safe Limited Speed) – Monitorowanie i ograniczenie prędkości do bezpiecznego poziomu.
- SDI (Sade Direction) – Zezwolenie na ruch tylko w bezpiecznym, zdefiniowanym kierunku.
- SLP (Safe Limited Position) – Kontrola granic położenia elementów roboczych.
- SLA/SAR (Safe Limited Acceleration / Safe Acceleration Range) – Monitorowanie i ograniczenie przyspieszenia napędu.

Funkcje bezpieczeństwa, takie jak STO, SS1 czy SLS, zapewniają ochronę podczas normalnej pracy maszyny i reagują automatycznie w razie zagrożenia. Jednak w cyklu życia maszyny występują również sytuacje, w których operator lub technik serwisu musi świadomie ingerować w strefę niebezpieczną – np. podczas czyszczenia, konserwacji lub napraw. W takich przypadkach sam system sterowania, nawet wyposażony w funkcje bezpieczeństwa, nie wystarcza. Konieczne jest wprowadzenie dodatkowych procedur organizacyjnych i środków technicznych, które zapewnią pełne odłączenie energii i uniemożliwią przypadkowe uruchomienie maszyny.

Taką rolę spełnia właśnie procedura LOTO (Lockout–Tagout), stanowiąca praktyczne uzupełnienie systemu bezpieczeństwa funkcjonalnego.

Choć LOTO nie jest funkcją bezpieczeństwa w rozumieniu PN-EN 61800-5-2, stanowi nieodzowny element systemu bezpiecznej eksploatacji maszyny. Procedura ta łączy środki techniczne i organizacyjne, mające na celu całkowite odłączenie źródeł energii (elektrycznej, pneumatycznej, hydraulicznej itp.) przed rozpoczęciem czynności serwisowych, czyszczenia lub konserwacji.

Podstawowe zasady LOTO obejmują:

- identyfikację wszystkich źródeł energii zasilających maszynę,
- ich fizyczne odłączenie i zablokowanie (np. za pomocą kłódek, zaworów blokujących, odłączników),
- oznakowanie miejsca blokady przy pomocy etykiet ostrzegawczych (Tagout),
- sprawdzenie, że energia została skutecznie rozproszona i maszyna nie może się uruchomić.

LOTO jest kluczowym uzupełnieniem systemu bezpieczeństwa funkcjonalnego – gwarantuje, że nawet przy prawidłowo zaprojektowanych funkcjach STO czy SS1, operator nie zostanie narażony na niebezpieczeństwo podczas czynności serwisowych.

3.2. Poziomy zapewnienia bezpieczeństwa

Po określeniu funkcji bezpieczeństwa w systemie sterowania kolejnym krokiem jest zdefiniowanie, z jaką niezawodnością dana funkcja ma być realizowana. W tym celu wprowadzono pojęcia poziomu zapewnienia bezpieczeństwa, które opisują, jak duże jest prawdopodobieństwo, że funkcja bezpieczeństwa zadziała poprawnie w momencie zagrożenia. W praktyce stosuje się dwa równorzędne systemy oceny: Performance Level (PL) zgodnie z normą PN-EN ISO 13849-1:2023-09 oraz Safety Integrity Level (SIL) zgodnie z normą PN-EN IEC 62061:2021. Oba pojęcia odnoszą się do tego samego celu – określenia niezawodności systemu bezpieczeństwa – jednak różnią się sposobem opisu, zakresem wartości i poziomem szczegółowości analizy.

Norma PN-EN ISO 13849-1 odnosi się głównie do maszyn i definiuje poziom zapewnienia bezpieczeństwa PL jako zdolność części systemu sterowania związanego z bezpieczeństwem do wykonywania swojej funkcji bezpieczeństwa w przewidywanych warunkach pracy.

PL określa się na podstawie trzech kluczowych parametrów:

- MTTFd (Mean Time To Dangerous Failure) – średni czas do wystąpienia niebezpiecznej awarii,
- DC_{avg} (Diagnostic Coverage) – średnie pokrycie diagnostyczne,
- CCF (Common Cause Failure) – współczynnik odporności na wspólne przyczyny awarii.

Na podstawie tych wartości oraz architektury systemu (kategorię bezpieczeństwa B, 1–4) wyznacza się osiągany poziom PL od a (najniższy) do e (najwyższy).

W normie PN-EN ISO 13849-1 oprócz parametrów ilościowych (MTTFd, DC_{avg}, CCF) stosuje się także podejście strukturalne, określone przez tzw. kategorie bezpieczeństwa – oznaczone literą B oraz cyframi 1–4. Kategorie te opisują architekturę systemu sterowania, czyli sposób, w jaki układ reaguje na awarie i zapewnia wykonywanie funkcji bezpieczeństwa (Tabela 1). Im wyższa kategoria, tym większa odporność systemu na pojedyncze uszkodzenia i tym mniejsze prawdopodobieństwo utraty funkcji bezpieczeństwa.

Tabela 1. Zestawienie kategorii bezpieczeństwa

Kategoria	Opis ogólny	Charakterystyka działania i zabezpieczenia
B	Podstawowa zasada bezpieczeństwa	Układ zaprojektowany zgodnie z zasadami inżynierskimi, bez redundancji. Utrata funkcji bezpieczeństwa możliwa przy pojedynczej awarii.
1	Zwiększona niezawodność elementów	Wymaga stosowania komponentów o wysokiej jakości i przewidywalności działania. Pojedyncza awaria może spowodować utratę funkcji.
2	Diagnostyka okresowa	System wykonuje okresowe testy, które wykrywają niektóre awarie. Możliwa utrata funkcji między testami.
3	Redundancja i częściowa diagnostyka	Dwa niezależne kanały wykonują tę samą funkcję; pojedyncza awaria nie powoduje utraty bezpieczeństwa, ale musi zostać wykryta.
4	Pełna redundancja i ciągła diagnostyka	Każda pojedyncza awaria jest wykrywana, a funkcja bezpieczeństwa utrzymana. Układ zachowuje bezpieczeństwo nawet w przypadku błędu.

Kategorie bezpieczeństwa stanowią dodatkowy opis architektury systemu, który determinuje sposób obliczania końcowego poziomu PL. Na przykład, system zaprojektowany w kategorii 3 i wysokich wartościach MTTFd oraz DC_{avg} może osiągnąć PL d, natomiast ten sam system z niską diagnostyką uzyska jedynie PL c. Dlatego w praktyce projektant zawsze ocenia zarówno strukturę (kategorię), jak i parametry ilościowe (MTTFd, DC_{avg}, CCF), aby potwierdzić zgodność z wymaganym poziomem bezpieczeństwa PLr.

Natomiast Norma PN-EN IEC 62061 opiera się bezpośrednio na zasadach PN-EN 61508 i stosuje się głównie w przypadku złożonych systemów automatyki, sterowników programowalnych i układów komunikacji sieciowej. W jej przypadku to poziom SIL definiuje integralność bezpieczeństwa funkcji, czyli prawdopodobieństwo, że dana funkcja zadziała poprawnie w momencie, gdy jest potrzebna. Wyróżnia się cztery poziomy SIL (1–4), z których SIL 1 jest najniższym, a SIL 4 najwyższym. Podobnie jak w przypadku ISO 13849-1, w normie IEC 62061 określa się SILr – wymagany poziom integralności bezpieczeństwa – na podstawie wyniku analizy ryzyka i przypisuje go do każdej funkcji bezpieczeństwa.

Oba podejścia – PL i SIL – opisują tę samą właściwość: niezawodność funkcji bezpieczeństwa, lecz stosują różne metodykę i zakres analizy (Tabela 2). Normy jednak nie przewidują bezpośredniego przelicznika między PL a SIL, ponieważ różnią się one założeniami analitycznymi i strukturą oceny.

Tabela 2. Główne różnice pomiędzy PL a SIL

Kryterium	**PL (ISO 13849-1)**	**SIL (IEC 62061)**
Zakres zastosowania	Maszyny i urządzenia przemysłowe	Złożone systemy sterowania (PLC, sieci komunikacyjne)
Liczba poziomów	5 (a–e)	4 (1–4)
Jednostka oceny	PFHd (1/h) + kategorie systemu	PFHd (1/h)
Metoda analizy	Kombinacja kategorii, MTTFd, DC_{avg}, CCF	Model probabilistyczny oparty na PFHd
Typowa złożoność	Prostsze systemy (mechaniczne, elektromechaniczne)	Systemy programowalne i sieciowe
Powiązanie z ISO 12100	Tak (wyznaczenie PLr na podstawie ryzyka)	Tak (wyznaczenie SILr na podstawie ryzyka)

Projektant powinien stosować jedną z norm, zależnie od charakteru systemu sterowania:

- ISO 13849-1 – dla maszyn z klasycznymi układami przekaźnikowymi, elektromechanicznymi lub prostymi PLC,
- IEC 62061 – dla systemów złożonych, opartych na sieciach komunikacyjnych i sterownikach bezpieczeństwa.

3.3. Związek między bezpieczeństwem a niezawodnością

Bezpieczeństwo funkcjonalne systemów sterowania jest ściśle powiązane z ich niezawodnością, ponieważ poprawne działanie funkcji bezpieczeństwa zależy od tego, jak często i w jaki sposób występują awarie komponentów. W praktyce można przyjąć, że im wyższa niezawodność systemu, tym większy poziom bezpieczeństwa – jednak zależność ta nie jest liniowa i wymaga analizy całego łańcucha bezpieczeństwa: czujników, logiki i elementów wykonawczych.

Jednym z kluczowych założeń bezpieczeństwa funkcjonalnego jest koncepcja „fail-safe", czyli projektowania systemu w taki sposób, aby awaria prowadziła do stanu bezpiecznego, a nie do stanu zagrożenia. Oznacza to, że przerwanie przewodu sygnałowego, utrata zasilania, usterka czujnika czy błąd komunikacji nie mogą spowodować uruchomienia niebezpiecznego ruchu lub utraty funkcji bezpieczeństwa.

Przykładowo jeśli kurtyna świetlna nadzorująca strefę pracy operatora zostanie uszkodzona lub odłączona, system sterowania musi automatycznie zatrzymać napęd (np. poprzez aktywację funkcji STO – Safe Torque Off), a nie pozostawić maszynę w stanie aktywnym. Analogicznie, w przypadku zaniknięcia napięcia sterującego w przekaźniku bezpieczeństwa, styk wyjściowy powinien się rozewrzeć, uniemożliwiając zasilanie silnika.

Przeciwieństwem koncepcji fail-safe jest sytuacja określana jako „fail-to-danger", w której awaria prowadzi do stanu niebezpiecznego. Przykładowo:

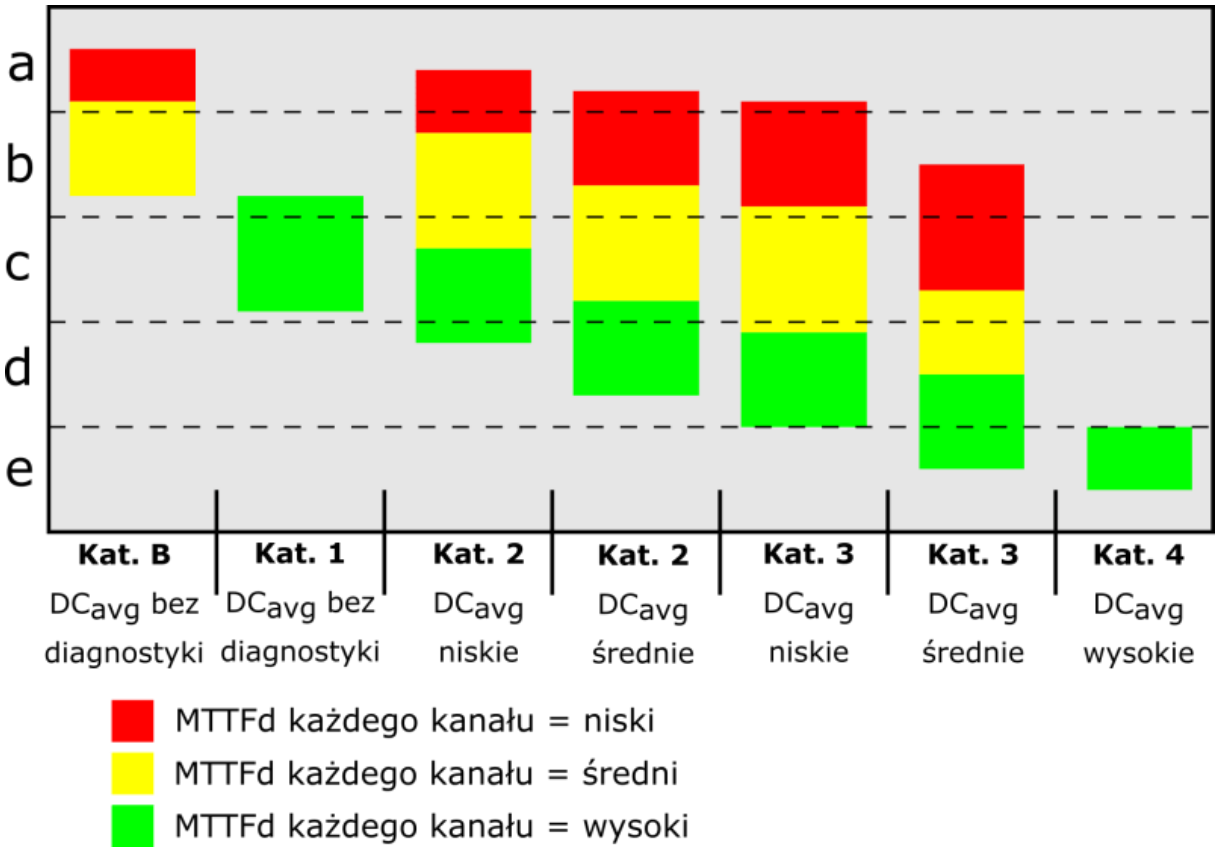
- zwarcie w torze sterowania powoduje samoczynne uruchomienie napędu,
- blokada przekaźnika uniemożliwia zatrzymanie maszyny po naciśnięciu przycisku STOP,
- awaria czujnika nie zostaje wykryta i system nie reaguje na zagrożenie.

Tego rodzaju sytuacje muszą być eliminowane poprzez odpowiednią architekturę (np. redundancję dwukanałową, testy okresowe, ciągłą diagnostykę) oraz stosowanie komponentów o potwierdzonej niezawodności.

Wzrost bezpieczeństwa w systemie sterowania osiąga się głównie poprzez:

- redundancję – stosowanie dwóch niezależnych kanałów wykonujących tę samą funkcję, tak aby pojedyncza awaria nie powodowała utraty bezpieczeństwa.
- diagnostykę – ciągłe lub okresowe testowanie układu w celu wykrycia awarii zanim doprowadzi ona do zagrożenia.

[Tekst alternatywny. Wykres przedstawiający zależność między wartością średniego czasu do niebezpiecznej awarii MTTFd, kategorią systemu i pokrycia diagnostycznego DC_{avg} a możliwym do osiągnięcia poziomem bezpieczeństwa PL. Na osi poziomej oznaczono kategorie systemu bezpieczeństwa: B, 1, 2, 3, 4 z uwzględnieniem poziomu diagnostycznego. Oś pionowa przedstawia możliwy do osiągnięcia PL przy odpowiednich przedziałach wartości MTTFd odpowiadające niskiemu, średniemu i wysokiemu poziomowi niezawodności. Czerwony kolor na słupkach oznacza niski poziom MTTFd. Żółty kolor na słupkach oznacza średni poziom MTTFd. Zielony kolor na słupkach oznacza wysoki poziom MTTFd. Wykres ilustruje, że wyższe wartości MTTFd oraz bardziej złożone kategorie systemu (3 i 4) umożliwiają osiągnięcie wyższych poziomów bezpieczeństwa PL.]



Rys. 2. Korelacja pomiędzy kategorią systemu, MTTFd, DC_{avg} a PL (Bezpieczeństwo w systemach sterowania, 2019)

W praktyce zależność między niezawodnością komponentów, strukturą systemu sterowania a osiąganym poziomem bezpieczeństwa można zobrazować za pomocą korelacji przedstawionej na Rys. 2.

Pokazuje on, jak wzrost średniego czasu do niebezpiecznej awarii (MTTFd) oraz zwiększenie pokrycia diagnostycznego (DC_{avg}) wpływają na możliwy do uzyskania poziom bezpieczeństwa (PL) w zależności od przyjętej kategorii systemu (B–4). Zależność ta stanowi praktyczne potwierdzenie, że wyższe poziomy bezpieczeństwa są osiągane dzięki połączeniu redundancji i diagnostyki, a nie jedynie przez stosowanie komponentów o wysokiej trwałości.

Przykładowo, system kategorii 3 wg ISO 13849-1 składa się z dwóch kanałów oraz częściowej diagnostyki, co pozwala utrzymać bezpieczeństwo w przypadku jednej awarii. W kategorii 4 wprowadzono dodatkowo ciągłą diagnostykę i nadzór wyjść, co umożliwia utrzymanie bezpieczeństwa nawet przy kilku niezależnych błędach.

4. Niezawodność systemów bezpieczeństwa

Niezawodność stanowi fundament bezpieczeństwa funkcjonalnego systemów sterowania. Każda funkcja bezpieczeństwa – niezależnie od tego, czy realizowana jest przez prosty układ przekaźnikowy, czy przez złożony system PLC Safety – musi działać z określonym prawdopodobieństwem poprawnego działania. Parametry niezawodności opisują, jak często mogą występować awarie elementów systemu oraz na ile skutecznie system potrafi je wykryć lub im zapobiec.

W normie PN-EN ISO 13849-1:2023-09 przyjęto trzy główne wskaźniki służące do ilościowego określenia niezawodności systemów bezpieczeństwa:

- MTTFd (Mean Time To Dangerous Failure) – średni czas do wystąpienia niebezpiecznej awarii,
- DC_{avg} (Diagnostic Coverage) – średni poziom pokrycia diagnostycznego,
- CCF (Common Cause Failure) – współczynnik odporności na awarie o wspólnej przyczynie.

Połączenie tych trzech parametrów umożliwia określenie rzeczywistego poziomu bezpieczeństwa systemu, a następnie przypisanie mu odpowiedniego PL (Performance Level).

4.1. Średni czas do wystąpienia niebezpiecznej awarii

Jednym z podstawowych parametrów oceny niezawodności systemów sterowania związanych z bezpieczeństwem jest MTTFd (Mean Time To Dangerous Failure), czyli średni czas do wystąpienia niebezpiecznej awarii. Wartość ta określa oczekiwany czas pracy elementu lub podzespołu do momentu, gdy wystąpi awaria prowadząca do utraty funkcji bezpieczeństwa.

Parametr MTTFd jest kluczowym składnikiem przy obliczaniu poziomu PL (Performance Level) zgodnie z normą PN-EN ISO 13849-1:2023-09, ponieważ pozwala ilościowo ocenić niezawodność komponentów (Bezpieczeństwo w systemach sterowania, 2019).

MTTFd opisuje niezawodność komponentów takich jak czujniki, przekaźniki, zawory, moduły logiczne czy sterowniki PLC Safety. Im większa wartość MTTFd, tym mniejsze prawdopodobieństwo wystąpienia awarii w czasie użytkowania i tym wyższy poziom bezpieczeństwa możliwy do osiągnięcia w całym systemie. Wartość MTTFd jest podawana w latach pracy i wyrażana najczęściej jako przedział (Tabela 3. Przedziały poziomów MTTFdTabela 3). Podział ten jest zgodny z wytycznymi ISO 13849-1 i stosowany przy obliczeniach w oprogramowaniu SISTEMA opracowanym przez IFA (Institute for Occupational Safety and Health, Niemcy).

Tabela 3. Przedziały poziomów MTTFd

Poziom MTTFd	**Zakres [lata]**
Niski	3 < MTTFd ≤ 10
Średni	10 < MTTFd ≤ 30
Wysoki	MTTFd > 30

Dla komponentów mechanicznych i elektromechanicznych, np. przekaźników, czujników, zaworów, aby wyznaczyć MTTFd stosuje się zależność (1).

$$MTTFd = \frac{B_{10d}}{0.1 \cdot n_{op}} \tag{1}$$

gdzie:

B_{10d} – liczba cykli do 10% awarii niebezpiecznych (z danych producenta lub baz danych),

n_{op} – średnia ilość zadziałań w ciągu roku.

Parametr B_{10d} należy pozyskać z dokumentacji technicznej producenta komponentu (np. kart katalogowych przekaźników, czujników czy zaworów) lub, w przypadku jego braku, z baz danych niezawodności określonych w normach (np. ISO 13849-1, ISO 19014-5 lub SN 29500).Natomiast aby wyznaczyć wartość czyli średnią liczbę zadziałań w ciągu roku n_{op}, należy zastosować zależność (2) przedstawiającą sposób obliczenia tej wielkości na podstawie cykli pracy elementu w jednostce czasu.

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600}{t_c} \tag{2}$$

gdzie:

d_{op} – ilość dni roboczych w ciągu roku (~250dni),

h_{op} – ilość roboczogodzin w ciągu doby,

t_c – czas cyklu w sekundach pomiędzy rozpoczęciem dwóch cykli elementów

Przykładowo dla przekaźnika o parametrze $B_{10d} = 2 \cdot 10^6$ cykli i czasie cyklu wynoszącym $t_c = 3,5[s]$ przy systemie 2 zmianowym czyli $h_{op} = 16$ z wyliczeń (3) wynika że taki element zalicza się do elementów o niskim poziomie MTTFd.

$$\begin{aligned} n_{op} &= \frac{250 \cdot 16 \cdot 3600}{3,5} \approx 4,1 \cdot 10^6 \\ MTTFd &= \frac{2 \cdot 10^6}{0.1 \cdot 4,1 \cdot 10^6} \approx 4,87\, roku \end{aligned} \tag{3}$$

Dla układów o architekturze dwukanałowej (redundatnej) w celu wyznaczenia całościowego dla układu średniego czasu do wystąpienia niebezpiecznej awarii $MTTFd_{total}$ stosuje się wzór (4).

$$MTTFd_{total} = \frac{1}{\frac{1}{MTTFd_1} + \frac{1}{MTTFd_2}} \tag{4}$$

gdzie:

$MTTFd_1$ – wyznaczony średni czas do wystąpienia niebezpiecznej awarii kanału pierwszego

$MTTFd_2$ – wyznaczony średni czas do wystąpienia niebezpiecznej awarii kanału drugiego

Przykładowo gdy redundantny układ składa się z dwóch identycznych kanałów dla których $MTTFd_1 = MTTFd_2 = 30$ lat to $MTTFd_{total} = 15$ lat.

Parametr MTTFd stanowi punkt wyjścia do analizy niezawodności i określenia poziomu PL. Im wyższa wartość MTTFd, tym większe prawdopodobieństwo, że system utrzyma funkcję bezpieczeństwa przez cały zakładany okres eksploatacji. W praktyce inżynierskiej dane te uzyskuje się z baz producentów lub z bibliotek programu SISTEMA, co umożliwia szybkie i powtarzalne obliczenia.

4.2. Średnie pokrycie diagnostyczne

Pokrycie diagnostyczne to miara skuteczności mechanizmów diagnostycznych w systemie bezpieczeństwa – określa, jaki odsetek niebezpiecznych uszkodzeń jest wykrywany przez te mechanizmy. W normie PN-EN ISO 13849-1 stosuje się wartość DC_{avg} (średnie pokrycie diagnostyczne) odnoszącą się do całej funkcji bezpieczeństwa, łącząc efekty diagnostyki w czujnikach, logice i elementach wykonawczych.

Pokrycie diagnostyczne wyrażane jest w procentach według wzoru (5):

$$DC = \frac{\lambda_{dd}}{\lambda_d} \cdot 100\% \tag{5}$$

gdzie:

λ_d – intensywność uszkodzeń niebezpiecznych,

λ_{dd} – intensywność wykrywalnych uszkodzeń niebezpiecznych.

Uszkodzenie niebezpieczne to każde uszkodzenie, które prowadzi lub może prowadzić do utraty funkcji bezpieczeństwa. Do tej kategorii zalicza się zarówno defekty wykryte, jak i te, które nie zostały zidentyfikowane. Największe zagrożenie stanowią oczywiście uszkodzenia niewykryte, ponieważ mogą one pozostać niezauważone podczas eksploatacji systemu. Natomiast wykryte uszkodzenie niebezpieczne to defekt, który prowadzi lub może prowadzić do utraty funkcji bezpieczeństwa, ale może zostać zidentyfikowany przez system diagnostyczny. Po jego wykryciu uruchamiana jest funkcja zabezpieczająca, która powoduje przejście systemu do stanu bezpiecznego, minimalizując ryzyko wystąpienia zagrożenia (Rockwell Automation, 2019).

Norma ISO 13849-1 wyróżnia cztery podstawowe zakresy pokrycia diagnostycznego (DC) (Tabela 4) dla kategorii systemu bezpieczeństwa które posiadają diagnostykę (kategorie 2, 3 i 4), a w kategoriach B i 1 diagnostyka nie jest brana pod uwagę.

Tabela 4. Zakresy pokrycia diagnostycznego

Pokrycie diagnostyczne	**Zakres**
Bez diagnostyki	DC < 60%
Niskie	60% ≤ DC ≤ 90%
Średnie	90% ≤ DC ≤ 99%
Wysokie	99% ≤ DC

Dla osiągnięcia wyższych poziomów bezpieczeństwa (PL d, PL e), zazwyczaj wymagane jest stosowanie przynajmniej wysokiego pokrycia diagnostycznego, zwłaszcza w architekturze kategorii 3 i 4 (norma zaleca $DC_{avg} \geq 99$ % dla kategorii 4)(ABB, 2012)

Pokrycie diagnostyczne (DC) należy wyznaczyć dla całego układu bezpieczeństwa, obejmującego jego wszystkie elementy – część wejściową, logiczną oraz wyjściową. Jeżeli system bezpieczeństwa realizuje kilka funkcji (np. zatrzymanie awaryjne oraz blokadę osłony ruchomej), to wartości DC poszczególnych funkcji należy uśrednić. Podczas określania poziomu zapewnienia bezpieczeństwa (PL) uwzględnia się więc jedno, wspólne – średnie pokrycie diagnostyczne (DC_{avg}) – odnoszące się do całej części sterującej odpowiedzialnej za daną funkcję bezpieczeństwa. Wartość DC_{avg} oblicza się zgodnie ze wzorem(6).

$$DC_{avg} = \frac{\sum\left(\frac{DC_i}{MTTFd_i}\right)}{\sum\left(\frac{1}{MTTFd_i}\right)} \tag{6}$$

gdzie:

DC_i – pokrycie diagnostyczne i-tego elementu,

$MTTFd_i$ – średni czas do wystąpienia niebezpiecznej awarii i-tego elementu,

Wprowadzenie normy PN-EN ISO 13849-1 wiązało się początkowo z dużym wyzwaniem dla projektantów systemów sterowania, głównie ze względu na konieczność wykonywania czasochłonnych i złożonych obliczeń. Dla wielu inżynierów była to sytuacja frustrująca – ich głównym zadaniem jest bowiem projektowanie rozwiązań technicznych, a nie prowadzenie szczegółowych analiz matematycznych. Normy powinny wspierać proces projektowy, a nie go utrudniać.

Znacznym ułatwieniem okazało się oprogramowanie SISTEMA, które automatyzuje część obliczeń i pomaga w ocenie poziomu zapewnienia bezpieczeństwa (PL). Mimo to zarówno sama norma, jak i narzędzia wspomagające, wciąż bywają źródłem nieporozumień i wymagają dokładnego zrozumienia zasad ich stosowania. Warto jednak podkreślić, że PN-EN ISO 13849-1 została opracowana w taki sposób, aby wprowadzić metody probabilistyczne w możliwie najbardziej przystępnej formie. Choć początkowo może wydawać się skomplikowana, w praktyce – po poznaniu zasad – umożliwia szybkie i efektywne przeprowadzenie obliczeń, wspierając bezpieczne projektowanie układów sterowania.

4.3. Wspólne przyczyny awarii

Wielokanałowe systemy bezpieczeństwa, w których ta sama funkcja realizowana jest przez dwa lub więcej niezależnych torów (np. czujniki, przekaźniki, elementy wykonawcze), mogą być podatne na tzw. awarie o wspólnej przyczynie – Common Cause Failures (CCF). Zjawisko to polega na tym, że dwa niezależne kanały ulegają awarii jednocześnie lub w krótkim odstępie czasu wskutek tego samego czynnika, co w praktyce może doprowadzić do całkowitej utraty funkcji bezpieczeństwa mimo redundancji (Bezpieczeństwo w systemach sterowania, 2019)

CCF to zjawisko, które obniża rzeczywistą niezawodność systemu, ponieważ niweluje korzyści wynikające z zastosowania dwóch kanałów. Typowymi przyczynami wspólnych awarii są:

- drgania i wibracje powodujące jednoczesne uszkodzenie złączy lub przewodów,
- wspólne źródło zasilania, którego awaria wyłącza oba kanały,
- przegrzanie lub zalanie modułów pracujących w jednym środowisku,
- błędy konstrukcyjne (np. identyczne komponenty w tym samym otoczeniu),
- zakłócenia elektromagnetyczne (EMC) lub przepięcia,
- błędy programistyczne powielone w identycznych układach PLC.

Norma PN-EN ISO 13849-1 wymaga, aby projektant wdrożył konkretne środki techniczne i organizacyjne ograniczające prawdopodobieństwo wystąpienia CCF. Do najczęściej stosowanych należą:

- separacja fizyczna kanałów – prowadzenie przewodów w oddzielnych wiązkach lub korytach, oddzielne zasilanie, brak wspólnych elementów mechanicznych,
- różnorodność komponentów (diversity) – użycie elementów różnych producentów lub technologii (np. czujnik optyczny + czujnik magnetyczny),
- ekranowanie i ochrona EMC – stosowanie kabli ekranowanych, filtrów, dławików i uziemienia zapobiegającego zakłóceniom,

- kontrola temperatury i innych warunków środowiska pracy – unikanie wspólnego wpływu czynników termicznych, wilgotności lub drgań,
- oddzielne źródła energii – zasilanie każdego kanału z niezależnego obwodu lub zasilacza,
- niezależna diagnostyka – zapewnienie, że awaria jednego kanału nie uniemożliwi wykrycia uszkodzenia drugiego.

Norma PN-EN ISO 13849-1:2023-09 określa uproszczony sposób oceny odporności systemu na CCF za pomocą metody punktowej (Tabela 5), gdzie projektant przyznaje punkty za zastosowane środki techniczne. Aby uznać system za odporny, suma punktów powinna wynosić co najmniej 65!

Tabela 5. Punktacja oceny odporności systemu na CCF

Nr	Kategoria działań	Środek zapobiegania CCF	Punkty
1	Separacja kanałów	Kanały prowadzone oddzielnie, brak wspólnych elementów	15
2	Różnorodność komponentów	Różni producenci / technologie / typy czujników	20
3.	Projekt – zastosowanie - doświadczenie	Zabezpieczenie przepięciowe, nadciśnieniowe, nadprądowe, temperaturowe	15
		Zastosowanie sprawdzonych elementów	5
4	Ocena i analiza	Dla każdego elementu związanego z bezpieczeństwem wykonano analizę rodzajów a także skutków uszkodzeń i uwzględniono wyniki w projekcie w celu uniknięcia CCF	5
5	Szkolenia i kwalifikacje	Szkolenie projektantów dotyczące przyczyn i skutków CCF	5
6	Czynniki środowiskowe	Dla układów elektrycznych: Ochrona przed EMC. Ekranowanie, uziemienie, filtry przeciwzakłóceniowe. Dla układów płynowych: filtracja, zapobieganie zanieczyszczeniom medium energii	25
		Przeciwdziałanie warunkom środowiskowym. Ochrona przed temperaturą, wilgocią, wibracjami	10

Przykładowo, system kategorii 3, który korzysta z sprawdzonych elementów, ma zastosowaną separacje, niezależne zasilanie, zabezpieczenia i ekranowanie, osiągnie wynik ok. 70 pkt, co spełnia wymogi normy. Jeśli jednak oba kanały korzystają z tego samego zasilacza i pracują w tym samym module sterownika, wartość ta może spaść poniżej 50 pkt. Wówczas projekt wymaga modyfikacji.

W praktyce projektanci często popełniają błąd, zakładając, że „redundancja automatycznie eliminuje CCF". W rzeczywistości, bez wdrożenia środków różnorodności i separacji, redundancja może wręcz zwiększać ryzyko awarii o wspólnej przyczynie. Z tego powodu ocena CCF jest obowiązkowym elementem analizy, które wymaga od użytkownika wpisania punktacji oraz uzasadnienia przyjętych środków.

5. Kategorie systemów bezpieczeństwa

Kategorie systemów bezpieczeństwa określają strukturę i odporność architektury systemu sterowania na uszkodzenia komponentów. Stanowią one podstawowy sposób opisu organizacji układu bezpieczeństwa w normie PN-EN ISO 13849-1, a ich dobór ma kluczowy wpływ na końcowy poziom PL (Performance Level). Każda kategoria (oznaczona jako B, 1, 2, 3 lub 4) opisuje, jak system reaguje na pojedynczą awarię i czy potrafi utrzymać funkcję bezpieczeństwa mimo jej wystąpienia. Im wyższa kategoria, tym większa niezawodność i odporność systemu, ale także większa złożoność konstrukcyjna oraz wymagania diagnostyczne. Norma PN-EN ISO 13849-1 definiuje pięć kategorii architektury systemu bezpieczeństwa. Są one uporządkowane rosnąco – od najprostszej B do najbardziej zaawansowanej Kat. 4.

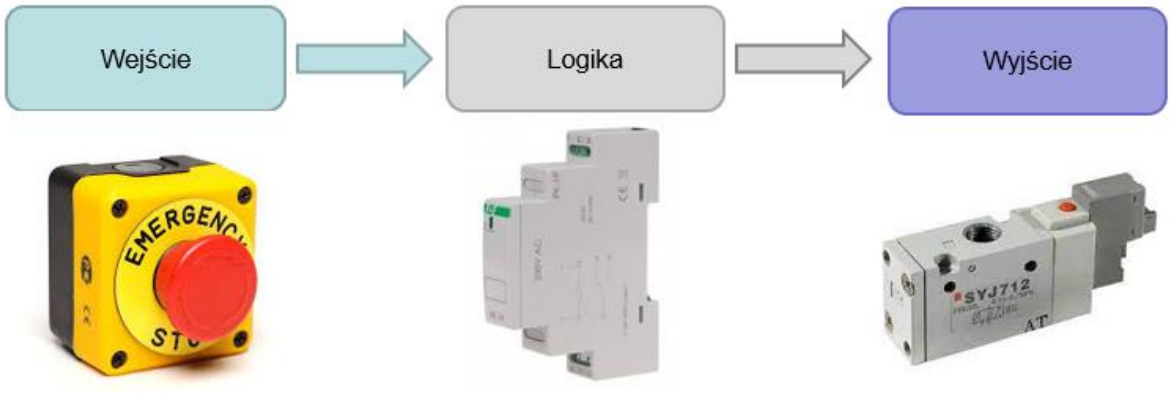
5.1. Kategoria B

Kategoria B stanowi najprostszy poziom architektury systemu bezpieczeństwa. Zgodnie z normą PN-EN ISO 13849-1, układy tej kategorii projektowane są zgodnie z ogólnymi zasadami inżynierskimi, jednak nie zawierają żadnych środków redundancji ani diagnostyki. Oznacza to, że funkcja bezpieczeństwa jest realizowana przez pojedynczy tor, którego prawidłowe działanie zależy wyłącznie od niezawodności zastosowanych komponentów. System kategorii B działa poprawnie tak długo, jak długo wszystkie jego elementy są sprawne. Pojedyncza awaria któregokolwiek z komponentów, np. czujnika lub przekaźnika, może bezpośrednio doprowadzić do utraty funkcji bezpieczeństwa. Z tego względu kategoria ta jest stosowana wyłącznie w układach, w których poziom ryzyka jest niski, a skutki potencjalnej awarii nie zagrażają życiu lub zdrowiu operatora.

Schemat takiego systemu jest jednokanałowy i obejmuje podstawowy łańcuch elementów: czujnik – logika – element wykonawczy, w którym brak jest zarówno diagnostyki, jak i redundancji (Rys. 3). Przykładowo w realizacji funkcji bezpieczeństwa odpowiadającej kategorii B zastosowano podstawowe elementy

układu sterowania, takie jak przycisk awaryjnego zatrzymania z pojedynczym stykiem rozwiernym, zwykły przekaźnik elektromechaniczny oraz zawór pneumatyczny odcinający dopływ sprężonego powietrza. Układ ten działa zgodnie ze sprawdzonymi zasadami inżynierskimi, jednak nie posiada żadnych mechanizmów diagnostyki ani redundancji a niezawodność elementów jest na standardowym poziomie, dlatego nie zapewnia ochrony w przypadku pojedynczej awarii. Ze względu na prostą strukturę i ograniczoną odporność na awarie, systemy kategorii B umożliwiają osiągnięcie jedynie najniższych poziomów bezpieczeństwa – PL a lub PL b. W kategorii B najczęściej stosuje się elementy o niskim i średnim poziomie MTTFd. Aby poprawić bezpieczeństwo, projektant może zastosować komponenty o wyższej jakości (wysoki poziom MTTFd) czyli przejść do kategorii 1, jednak wciąż nie eliminuje to ryzyka utraty funkcji w przypadku pojedynczej awarii (ABB, 2012; Rockwell Automation, 2019)..

[Tekst alternatywny. Schemat przedstawia uproszczoną strukturę systemu bezpieczeństwa maszyny składającą się z trzech podstawowych bloków funkcjonalnych: Wejście – Logika – Wyjście. Po lewej stronie znajduje się przycisk awaryjnego zatrzymania (Emergency Stop) oznaczony kolorem żółtym i czerwonym, pełniący rolę elementu wejściowego, inicjującego sygnał bezpieczeństwa. W środku pokazano moduł przekaźnikowy odpowiadający za logikę sterowania, czyli przetwarzanie sygnału wejściowego i decyzyjne sterowanie układem. Po prawej stronie znajduje się elektrozawór pneumatyczny, reprezentujący element wyjściowy, który reaguje na sygnał z modułu logicznego i zatrzymuje przepływ energii w układzie. Strzałki między blokami wskazują kierunek przepływu sygnału od wejścia przez logikę do wyjścia.]



Rys. 3. Schemat struktury kategorii B z przykładowymi elementami

5.2. Kategoria 1

Kategoria 1 stanowi rozwinięcie kategorii B poprzez zastosowanie komponentów o zwiększonej niezawodności oraz potwierdzonej jakości działania. Zgodnie z normą PN-EN ISO 13849-1, układy tej kategorii mają strukturę jednokanałową, jednak różnią się od kategorii B tym, że wykorzystują elementy o wysokim poziomie MTTFd oraz projektowane są zgodnie z rygorystycznymi zasadami inżynierskimi i kontrolą jakości. Podstawowa architektura nie zmienia się – funkcja bezpieczeństwa realizowana jest przez pojedynczy tor: czujnik – logika – element wykonawczy, ale wzrasta przewidywalność działania i trwałość komponentów.

System kategorii 1 funkcjonuje poprawnie tak długo, jak długo jego elementy pozostają sprawne. W przeciwieństwie do kategorii B, ryzyko awarii jest znacznie mniejsze, gdyż wykorzystuje się komponenty certyfikowane, o wysokiej trwałości mechanicznej i elektrycznej. W dalszym ciągu jednak brak jest diagnostyki i redundancji, dlatego awaria pojedynczego elementu – np. sklejenie styków przekaźnika czy uszkodzenie czujnika – może skutkować utratą funkcji bezpieczeństwa. Z tego względu kategoria 1 jest stosowana w systemach, gdzie ryzyko jest niskie lub umiarkowane, a potencjalne skutki awarii nie powodują poważnych obrażeń, lecz mogą wymagać ponownego uruchomienia maszyny lub kontroli operatora.

Schemat struktury kategorii 1 (Rys. 4) jest zbliżony do kategorii B i obejmuje pojedynczy tor sygnałowy. Przykładowo, funkcja bezpieczeństwa może być zrealizowana przez przycisk awaryjnego zatrzymania, certyfikowany przekaźnik bezpieczeństwa o zwiększonej żywotności (np. z pozłacanymi stykami i wymuszoną separacją), oraz zawór elektromagnetyczny o wysokiej trwałości eksploatacyjnej (MTTFd > 30 lat). W takim układzie uzyskuje się większą niezawodność w porównaniu do kategorii B, jednak nadal pojedyncza awaria może spowodować utratę funkcji bezpieczeństwa, ponieważ system nie monitoruje swojego stanu ani nie posiada redundantnych torów.

Kategoria 1 pozwala zazwyczaj osiągnąć poziom bezpieczeństwa PL b, w wyjątkowych przypadkach PL c, jeśli zastosowane komponenty charakteryzują się bardzo wysokim MTTFd. W praktyce stanowi ona pośredni etap między prostymi układami kategorii B a bardziej zaawansowanymi systemami kategorii 2 i 3, w których pojawia się diagnostyka okresowa lub redundancja (ABB, 2012; Rockwell Automation, 2019)...

[Tekst alternatywny. Schemat przedstawia strukturę systemu bezpieczeństwa w kategorii 1, składającą się z trzech głównych bloków funkcjonalnych: Wejście – Logika – Wyjście. Po lewej stronie znajduje się przycisk awaryjnego zatrzymania, pełniący rolę elementu wejściowego. W centralnej części widoczny jest przekaźnik bezpieczeństwa reprezentujący logikę sterowania, odpowiedzialny za przetwarzanie sygnału wejściowego i kontrolę działania układu. Po prawej stronie umieszczono zawór elektromagnetyczny o zwiększonej trwałości, będący elementem wykonawczym zatrzymującym dopływ energii. Strzałki między blokami wskazują kierunek przepływu sygnału – od wejścia przez logikę do elementu wykonawczego.]

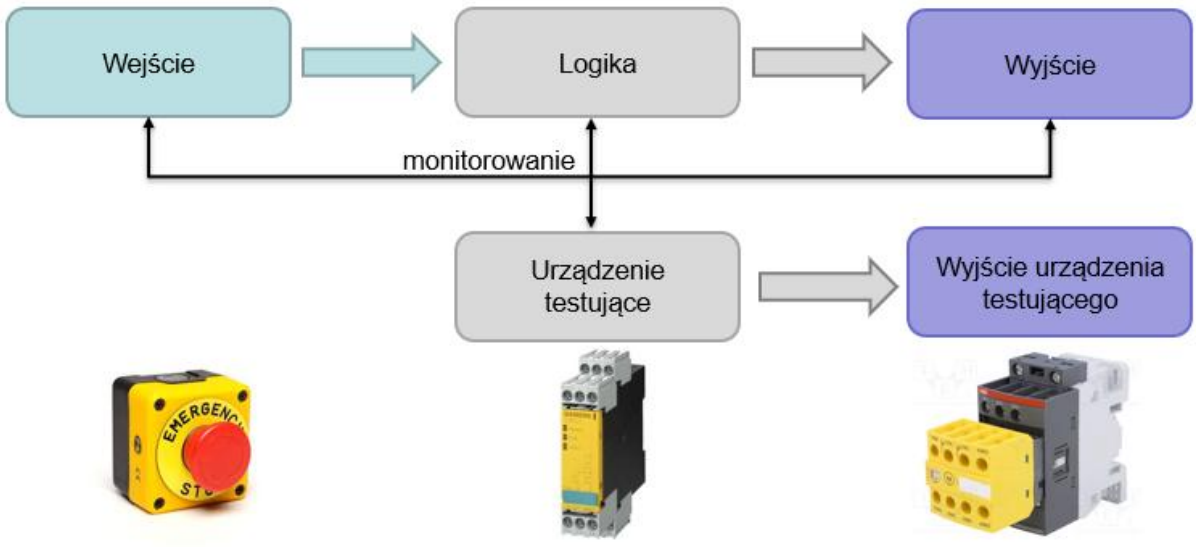
Rys. 4. Schemat struktury kategorii 1 z przykładowymi elementami

5.3. Kategoria 2

Kategoria 2 stanowi rozwinięcie architektury jednokanałowej (znanej z kategorii 1) o możliwość okresowego testowania i monitorowania elementów systemu bezpieczeństwa. Zgodnie z normą PN-EN ISO 13849-1, układy tej kategorii wykorzystują diagnostykę realizowaną przez urządzenie testujące lub funkcje samego sterownika, które cyklicznie sprawdzają poprawność działania czujników, logiki i elementów wykonawczych. Diagnostyka nie jest ciągła, lecz wykonywana w określonych odstępach czasu – np. przy każdym uruchomieniu maszyny, po zakończeniu cyklu roboczego lub w ustalonych interwałach testowych. W odróżnieniu od kategorii 1, w której system działa bez nadzoru, w kategorii 2 dodano mechanizmy testujące, które mogą wykrywać typowe uszkodzenia, takie jak przerwanie przewodu, sklejenie styków czy nieprawidłowe przełączenie przekaźnika. W przypadku wykrycia błędu układ powinien przejść do stanu bezpiecznego, czyli np. zatrzymać napęd, odciąć energię lub zablokować możliwość ponownego uruchomienia, dopóki nie zostanie wykonana naprawa.

Schemat struktury systemu kategorii 2 (Rys. 5) obejmuje trzy podstawowe bloki funkcjonalne: Wejście – Logika – Wyjście, oraz dodatkowy tor urządzenia testującego, które nadzoruje poprawność działania toru głównego. Sygnały z urządzenia testującego mogą być przetwarzane przez układ logiczny (np. przekaźnik bezpieczeństwa lub sterownik PLC Safety), który porównuje wyniki testów z oczekiwanym stanem. Jeżeli wykryte zostanie odchylenie od wartości referencyjnych, system generuje polecenie zatrzymania lub uniemożliwia uruchomienie maszyny (ABB, 2012; Rockwell Automation, 2019).

[Tekst alternatywny. Schemat przedstawia strukturę systemu bezpieczeństwa w kategorii 2.Po lewej stronie znajduje się blok wejściowy z przyciskiem awaryjnego zatrzymania (Emergency Stop) reprezentującym źródło sygnału bezpieczeństwa. W centralnej części znajduje się blok logiki – przekaźnik bezpieczeństwa – odpowiedzialny za przetwarzanie sygnału i sterowanie wyjściem. Po prawej stronie widoczny jest blok wyjściowy, w którym umieszczono stycznik odcinający energię maszyny. Pod głównym torem pokazano dodatkowe urządzenie testujące, połączone z blokiem logiki, które okresowo monitoruje stan elementów wejściowych i wyjściowych. Strzałki przedstawiają przepływ sygnału oraz kierunek monitorowania i testowania poszczególnych bloków.]



Rys. 5. Schemat struktury kategorii 2 z przykładowymi elementami

Przykładowo, w realizacji funkcji bezpieczeństwa odpowiadającej kategorii 2 zastosowano przycisk awaryjnego zatrzymania, moduł przekaźnikowy bezpieczeństwa z funkcją autotestu oraz stycznik z monitorowanymi stykami pomocniczymi. Urządzenie testujące okresowo sprawdza, czy styki przekaźnika

poprawnie rozłączają obwód, a logika porównuje sygnał sprzężenia zwrotnego z aktualnym stanem wejść. W ten sposób wykrywana jest część potencjalnych awarii – choć nie wszystkie, ponieważ testy wykonywane są w odstępach czasowych, co pozostawia możliwość wystąpienia awarii pomiędzy cyklami testowymi.

Systemy kategorii 2 umożliwiają osiągnięcie poziomu bezpieczeństwa PL c, a w niektórych przypadkach – przy wysokiej niezawodności komponentów i skutecznej diagnostyce – nawet PL d. Są one często stosowane w maszynach o średnim poziomie ryzyka, gdzie konieczna jest kontrola stanu elementów bezpieczeństwa, ale nie wymaga się pełnej redundancji.

5.4. Kategoria 3

Kategoria 3 wprowadza kluczową zmianę w architekturze systemu bezpieczeństwa – pojawia się redundancja, czyli zastosowanie dwóch niezależnych kanałów realizujących tę samą funkcję bezpieczeństwa. Zgodnie z normą PN-EN ISO 13849-1, systemy tej kategorii muszą być zaprojektowane w taki sposób, aby pojedyncza awaria któregokolwiek z kanałów nie prowadziła do utraty funkcji bezpieczeństwa. Dodatkowo wymagane jest zastosowanie częściowej diagnostyki, umożliwiającej wykrycie błędów w jednym z kanałów przed wystąpieniem kolejnych awarii.

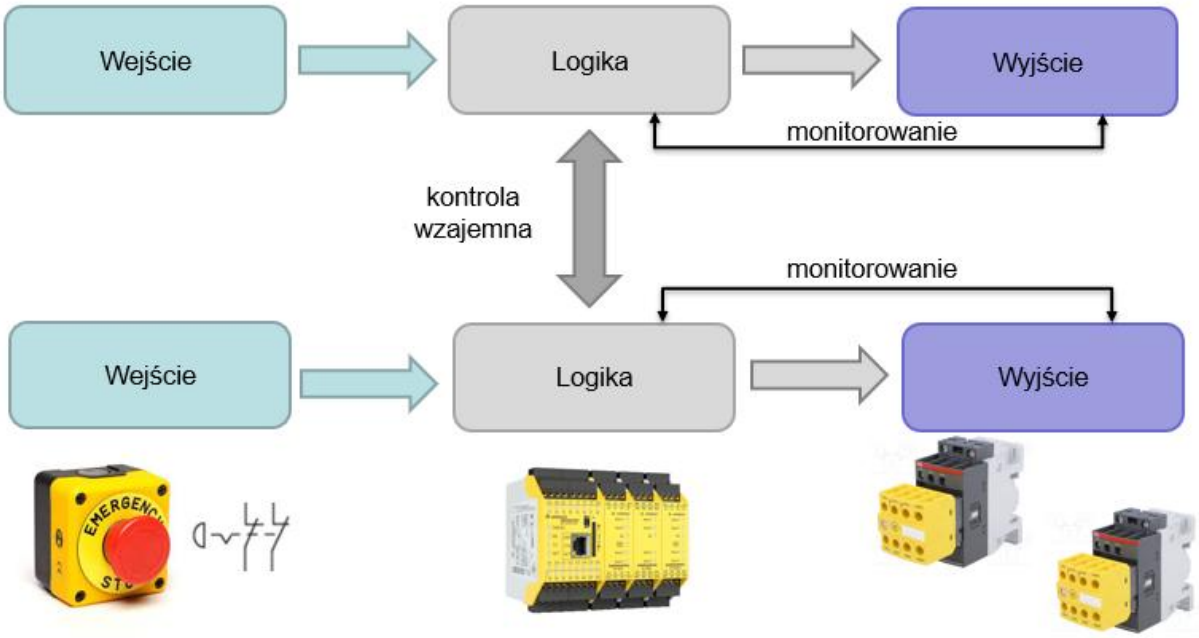
W przeciwieństwie do kategorii 2, gdzie testy są wykonywane okresowo, w kategorii 3 monitorowanie odbywa się w sposób ciągły lub cykliczny. Oba kanały pozostają aktywne podczas normalnej pracy i wzajemnie kontrolują swoje stany, co pozwala na wczesne wykrycie niespójności sygnałów lub uszkodzeń elementów. W przypadku wykrycia błędu system powinien przejść do stanu bezpiecznego lub zablokować możliwość ponownego uruchomienia, dopóki awaria nie zostanie usunięta.

Schemat systemu kategorii 3 (Rys. 6) przedstawia dwa równoległe tory: Wejście – Logika – Wyjście, pracujące niezależnie, lecz połączone mechanizmem kontroli wzajemnej. Sygnały z obu kanałów są monitorowane i porównywane – wszelkie rozbieżności między nimi (np. różny stan wejść, brak reakcji jednego z wyjść, błąd logiczny) są traktowane jako awaria i powodują zatrzymanie maszyny. Taka konstrukcja pozwala utrzymać funkcję bezpieczeństwa w przypadku uszkodzenia jednego kanału, o ile drugi pozostaje sprawny (ABB, 2012; Rockwell Automation, 2019).

Przykładowo, funkcja bezpieczeństwa zatrzymania awaryjnego w kategorii 3 może być zrealizowana poprzez podwójny przycisk awaryjnego zatrzymania (z dwoma

zestawami styków), dwa niezależne tory przekaźnikowa bezpieczeństwa lub PLC Safety oraz podwójne styczniki odcinające zasilanie napędu. Każdy z torów realizuje identyczną funkcję, a ich stany są porównywane w logice układu. Dodatkowo, styki pomocnicze styczników są monitorowane przez przekaźnik, co umożliwia wykrycie sklejenia styków lub braku rozwarcia toru mocy po zatrzymaniu.

[Tekst alternatywny. Schemat przedstawia strukturę systemu bezpieczeństwa w kategorii 3, składającą się z dwóch równoległych torów: Wejście – Logika – Wyjście. Każdy tor ma własny przycisk awaryjnego zatrzymania, moduł logiczny i element wykonawczy w postaci stycznika z monitorowaniem styków. Pomiędzy torami zaznaczono kontrolę wzajemną, umożliwiającą porównywanie stanów logicznych obu kanałów. Strzałki oznaczają kierunek przepływu sygnałów oraz monitorowanie i komunikację pomiędzy torami, które pozwalają na wykrycie różnic w działaniu. Dodatkowe strzałki łączą bloki logiki z wyjściami, wskazując na ciągłe monitorowanie poprawności działania styczników.]



Rys. 6. Schemat struktury kategorii 3 z przykładowymi elementami

Systemy kategorii 3 zapewniają wysoki poziom bezpieczeństwa i odporności na pojedyncze awarie, umożliwiając osiągnięcie poziomu PL d, a przy wysokiej niezawodności komponentów i dobrze zaprojektowanej diagnostyce – nawet PL e. Ze względu na większą złożoność konstrukcyjną, wymagają starannego projektowania ścieżek sygnałowych, kontroli wzajemnej oraz zapewnienia

odporności na awarie o wspólnej przyczynie (CCF). W praktyce stosowane są powszechnie w maszynach przemysłowych o średnim lub wysokim poziomie ryzyka.

5.5. Kategoria 4

Kategoria 4 stanowi najwyższy poziom architektury systemu bezpieczeństwa opisany w normie PN-EN ISO 13849-1. Układy tej kategorii charakteryzują się pełną redundancją oraz ciągłym monitorowaniem działania wszystkich kluczowych elementów systemu sterowania. Celem takiego rozwiązania jest zapewnienie, aby żadna pojedyncza awaria nie prowadziła do utraty funkcji bezpieczeństwa, a każda usterka była natychmiast wykrywana i odpowiednio sygnalizowana.

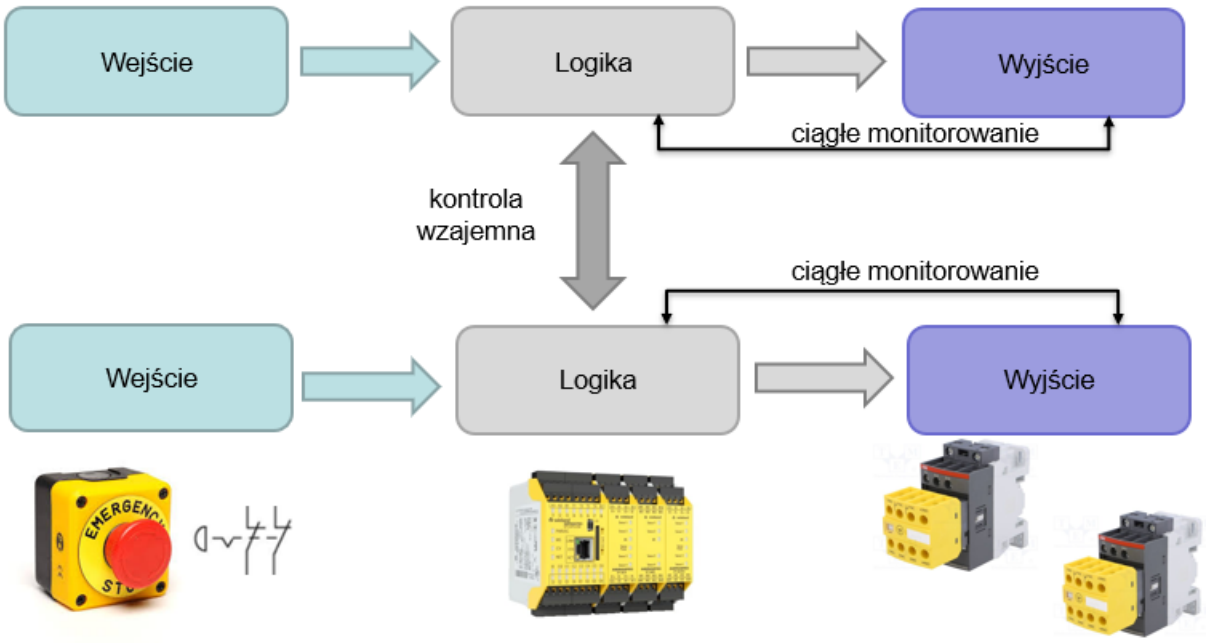
System kategorii 4 składa się z dwóch niezależnych torów bezpieczeństwa, które wzajemnie się kontrolują oraz stale monitorują swoje stany wejść, logiki i wyjść. Oznacza to, że w przeciwieństwie do kategorii 3, gdzie diagnostyka może być częściowa, w kategorii 4 występuje pełna, ciągła diagnostyka, obejmująca zarówno elementy wejściowe (czujniki), jak i wykonawcze (styczniki, zawory). Dzięki temu układ jest w stanie natychmiast wykryć każdą niespójność sygnałów lub błąd działania i przejść do stanu bezpiecznego bez opóźnienia (ABB, 2012; Rockwell Automation, 2019).

Schemat przedstawiony na rysunku poniżej (Rys. 7) ilustruje budowę systemu kategorii 4, w którym zastosowano dwa równoległe kanały Wejście – Logika – Wyjście. Każdy kanał działa niezależnie, a między nimi zachodzi ciągła kontrola wzajemna, umożliwiająca porównywanie sygnałów w czasie rzeczywistym. Dodatkowo, w każdym z kanałów prowadzony jest ciągły monitoring stanu elementów wykonawczych – np. sprawdzanie pozycji styków styczników, poprawności działania czujników oraz integralności sygnałów w torach logicznych. Taka struktura sprawia, że system pozostaje funkcjonalny nawet w przypadku wystąpienia jednej lub kilku awarii, o ile nie są one współzależne (nie pochodzą z tej samej przyczyny).

W praktyce funkcja bezpieczeństwa realizowana w kategorii 4 może obejmować np. podwójny obwód zatrzymania awaryjnego, moduł przekaźnikowy z wymuszoną separacją i testowaniem wyjść, a także styczniki z nadzorowanymi stykami połączone z kontrolą wzajemną w sterowniku PLC Safety. Każdy element jest kontrolowany w sposób ciągły, a układ potrafi zidentyfikować zarówno przerwanie obwodu, jak i sklejenie styków, błąd transmisji czy niezgodność logiczną. Takie rozwiązania są typowe dla maszyn o najwyższym poziomie ryzyka, w których

bezpieczeństwo operatora zależy bezpośrednio od poprawnego działania systemu sterowania.

[Tekst alternatywny. Schemat przedstawia strukturę systemu bezpieczeństwa w kategorii 4. Układ składa się z dwóch równoległych torów: Wejście – Logika – Wyjście, które działają niezależnie, lecz pozostają ze sobą w stałej komunikacji. Między torami zaznaczono kontrolę wzajemną, umożliwiającą porównywanie sygnałów w czasie rzeczywistym. Oba kanały realizują ciągłe monitorowanie zarówno stanu wejść (czujników), jak i wyjść (styczników), dzięki czemu każda awaria jest natychmiast wykrywana. Po lewej stronie widoczny jest podwójny przycisk awaryjnego zatrzymania, w centralnej części moduł logiczny bezpieczeństwa z funkcją kontroli wzajemnej, a po prawej podwójny zestaw styczników odpowiadających za odcięcie zasilania. Strzałki wskazują kierunek przepływu sygnałów oraz ścieżki monitorowania między kanałami.]



Rys. 7. Schemat struktury kategorii 4 z przykładowymi elementami

Systemy kategorii 4 umożliwiają osiągnięcie najwyższego poziomu bezpieczeństwa – PL e. Osiągnięcie tego poziomu wymaga nie tylko zastosowania odpowiedniej architektury, lecz także komponentów o wysokiej niezawodności (MTTFd > 30 lat), bardzo wysokim pokryciu diagnostycznym ($DC_{avg} \geq 99\%$) oraz odporności na wspólne przyczyny awarii (CCF ≥ 65 pkt). Takie systemy stosuje się w aplikacjach o krytycznym znaczeniu dla bezpieczeństwa – np. w prasach hydraulicznych,

robotach współpracujących, systemach zautomatyzowanych linii montażowych czy urządzeniach transportowych o dużej mocy.

6. Literatura

ABB. (2012). Bezpieczeństwo w systemach sterowania według normy ISO EN 13849-1. ABB Sp. z o.o.

Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn i zmiany dyrektywy 95/16/WE. Dziennik Urzędowy Unii Europejskiej, L 157, 24–86.

Dźwiarek, M. (2012). Bezpieczeństwo funkcjonalne systemów sterowania maszynami. Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

European Commission. (2019). Guide to application of the Machinery Directive 2006/42/EC. Publications Office of the European Union.

European Commission. (2023). Guide to application of the Machinery Regulation (EU) 2023/1230. Publications Office of the European Union.

IEC 62061:2021. (2021). Safety of machinery – Functional safety of safety-related control systems. International Electrotechnical Commission.

Pamuła, W. (2011). Niezawodność i bezpieczeństwo: wybór zagadnień. Wydawnictwo Politechniki Śląskiej.

PN-EN 60204-1:2018-12. (2018). Bezpieczeństwo maszyn – Wyposażenie elektryczne maszyn – Część 1: Wymagania ogólne. Polski Komitet Normalizacyjny.

PN-EN ISO 12100:2012. (2012). Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka. Polski Komitet Normalizacyjny.

PN-EN ISO 13849-1:2023-09. (2023). Bezpieczeństwo maszyn – Części systemów sterowania związanych z bezpieczeństwem – Część 1: Ogólne zasady projektowania. Polski Komitet Normalizacyjny.

PN-EN ISO 13850:2016-03. (2017). Bezpieczeństwo maszyn – Funkcja zatrzymania awaryjnego – Zasady projektowania. Polski Komitet Normalizacyjny.

PN-EN ISO 13855:2025-06. (2025). Bezpieczeństwo maszyn – Pozycjonowanie środków ochronnych w zależności od prędkości zbliżania się ciała człowieka. Polski Komitet Normalizacyjny.

Rockwell Automation. (2016). Bezpieczna konstrukcja maszyn – przewodnik po zasadach projektowania systemów bezpieczeństwa funkcjonalnego zgodnie z normą ISO 13849-1. Rockwell Automation, Inc.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230 z dnia 29 czerwca 2023 r. w sprawie maszyn oraz uchylenia dyrektywy 2006/42/WE. Dziennik Urzędowy Unii Europejskiej, L 165/1.

Bezpieczeństwo w systemach sterowania, MTTFd wg ISO 13849-1 (https://bezpieczenstwowsystemachsterowania.pl/2019/07/mttfd-wg-iso-13849-1/ dostępny 10.09.2025)