

# **Bezpieczeństwo funkcjonalne programowalnych układów sterowania maszyn**

---

**Marek Dźwiarek**

---

Zakład Techniki Bezpieczeństwa

## Podstawa prawna

Dyrektywa Maszynowa 98/37/EC, w Załączniku 1 p.1.2.7  
"Uszkodzenia obwodu sterowania" wymaga:

*"Uszkodzenie logicznych obwodów sterowania, defekt lub uszkodzenie obwodu sterowania nie mogą prowadzić do sytuacji niebezpiecznych"*

## Podstawa prawna

p. 1.4.3 "Wymagania specjalne dotyczące urządzeń ochronnych,, mówi:

*"Urządzenia ochronne powinny być tak zaprojektowane i włączone w układ sterowania maszyny, aby brak lub uszkodzenie jednego z ich elementów uniemożliwiało uruchomienie lub zatrzymywało ruch części ruchomych"*

## Projektant systemu sterowania powinien zrealizować dwa cele:

- zaprojektować system który umożliwi realizowanie zadań funkcjonalnych maszyny, uwzględniając przy tym kwestie bezpieczeństwa
- zaprojektować system który będzie realizował swoje funkcje w warunkach uszkodzenia w sposób przewidywalny, na określonym poziomie niezawodności, w całym cyklu życia maszyny

## Normy uszczegóławiające wymagania dyrektywy

- PN-EN 954-1:2000. Maszyny. Bezpieczeństwo. Związane z bezpieczeństwem elementy systemów sterowania. Ogólne zasady projektowania
- PN-EN 61508:2003(U). Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych programowalnych elektronicznych systemów wiążących się z bezpieczeństwem
- pr. IEC 62061. Safety of machinery - functional safety - electrical, electronic and programmable electronic control systems

## Norma PN-EN 954-1

- stosuje jakościowe podejście do oceny odporności systemu sterowania na defekty
- wprowadza podział systemów sterowania na 5 kategorii w zależności od ich zachowania się w warunkach defektu
- wprowadza podział systemów sterowania na 5 kategorii w zależności od ich zachowania się w warunkach defektu
- doboru kategorii dokonuje się na podstawie oceny ryzyka

## Norma PN-EN 954-1

- ocena poprawności zastosowanych rozwiązań konstrukcyjnych dokonywana jest poprzez analizę FMEA lub FTA
- w przypadkach szczególnych wykonuje się badania laboratoryjne polegające na symulacji defektów
- norma nie uwzględnia uszkodzeń systematycznych, nie może więc być stosowana do oceny złożonych (programowalnych) systemów sterowania

## Norma PN-EN 954-1

Zakres stosowania:

- wymagany jest niewielki poziom zapewnienia bezpieczeństwa („a” lub „b”,)

lub

- funkcja bezpieczeństwa realizowana jest przy zastosowaniu sprzętu którego potencjalne uszkodzenia są jasno określone i możliwe do oceny

lub

- udział elementów programowalnych w całym systemie realizującym funkcje bezpieczeństwa jest niewielki i wymagany jest poziom zapewnienia bezpieczeństwa „a” do „d”

## Norma PN-EN 954-1

lub

- funkcja bezpieczeństwa jest realizowana przez dwa oddzielne systemy programowalne z różnym oprogramowaniem, różnymi systemami operacyjnymi i różnym sprzętem oraz wymagany jest poziom zapewnienia bezpieczeństwa „a” do „d”

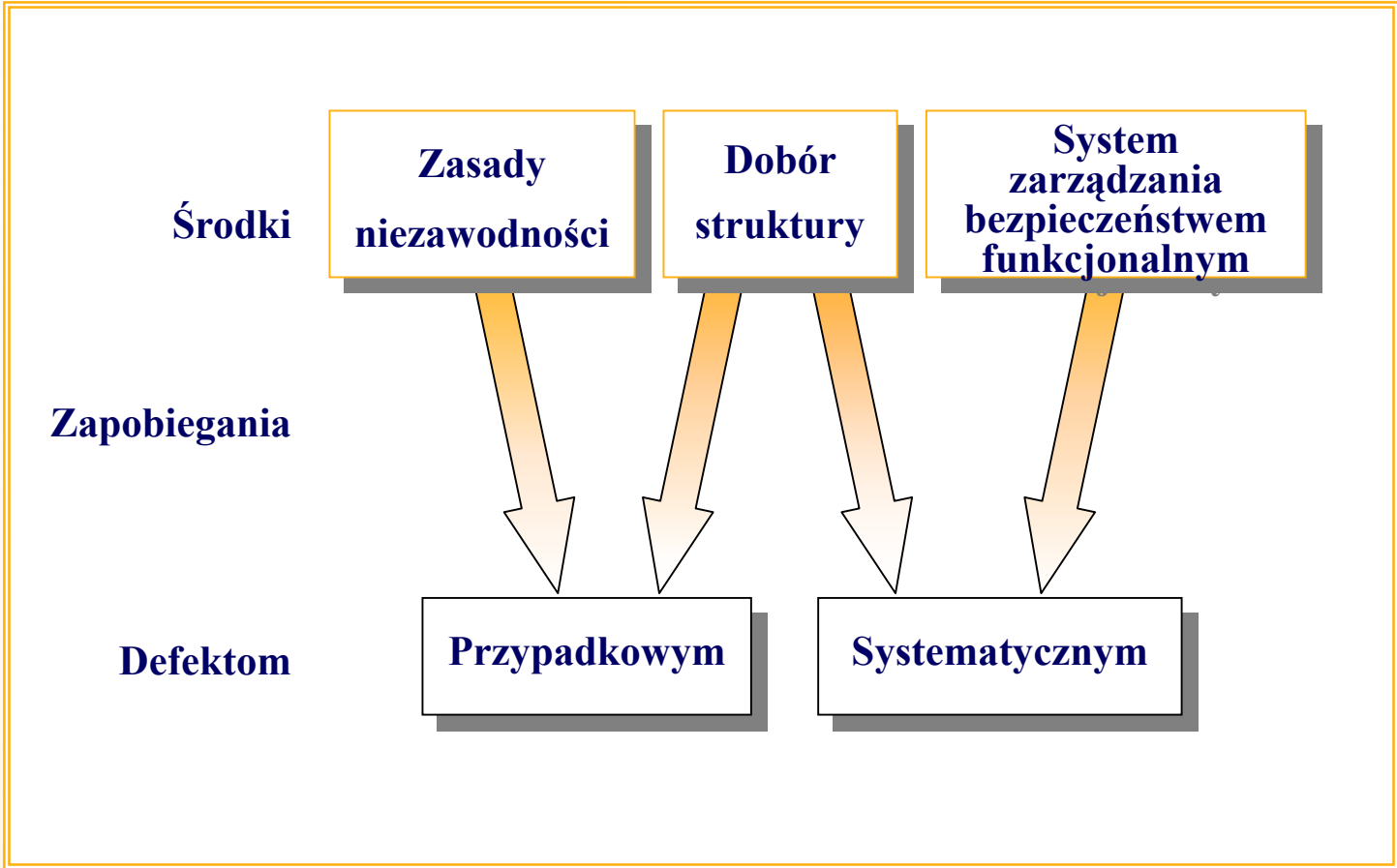
lub

- zastosowany sprzęt (z uwzględnieniem oprogramowaniem użytkownika) był badany i certyfikowany przez jednostki niezależne (np. jednostki notyfikowane) pod kątem spełnienia wymagań odpowiednich norm

## Cechy charakterystyczne systemów sterowania maszyn

- stosunkowo niski poziom ryzyka (odpowiadający co najwyżej SIL 3)
- prosta struktura sprzętowa (zwykle nie więcej niż dwa proste sterowniki PLC)
- proste oprogramowanie (zwykle w pisane w językach niskiego rzędu, niewielkie programy do kilkuset rozkazów)

# Strategia Zapobiegania Defektom



## Ogólne zasady bezpieczeństwa funkcjonalnego według pr. IEC 62061

- rozdzielenie systemów funkcjonalnych od systemów bezpieczeństwa
- dekompozycja systemów realizujących poszczególne funkcje bezpieczeństwa na podzespoły, tak głęboka jak to jest tylko możliwe:
  - w sprzęcie
  - w oprogramowaniu
- określenie SIL dla poszczególnych podzespołów
- SIL funkcji bezpieczeństwa jest mniejszy lub równy najniższemu SIL poszczególnych podzespołów

## Określanie SIL sprzętu

Podzespoły wykonane i przebadane według PN-EN 954-1

Kategoria wg EN 954-1	Liczba tolerowanych uszkodzeń	Procent defektów niegroźnych	Maksymalny osiągalny SIL
<b>1</b>	<b>0</b>	<b>&lt;60%</b>	zależnie od niezawodności elementów
<b>2</b>	<b>0</b>	<b>60...90%</b>	<b>SIL 1</b>
<b>3</b>	<b>1</b>	<b>&lt;60%</b>	<b>SIL 1</b>
		<b>60...90%</b>	<b>SIL 2</b>
<b>4</b>	<b>&gt;1</b>	<b>60...90%</b>	<b>SIL 3</b>
	<b>1</b>	<b>&gt;90%</b>	<b>SIL 3</b>

## Zakres zaleceń pr. IEC 62061

- zarządzanie bezpieczeństwem funkcjonalnym
- określanie funkcji bezpieczeństwa
- definiowanie funkcji bezpieczeństwa
- projektowanie, wykonywanie i oprogramowanie elektronicznych systemów sterowania
- informacje dla użytkownika
- walidacja systemów wiążących się z bezpieczeństwem
- modyfikacje
- dokumentacja

## Przykłady zastosowań pr. IEC 62061

- proste systemy sterowania maszyn, takich jak:
  - maszyny do obróbki drewna
  - prasy
  - maszyny do przetwarzania papieru, itp.
- proste systemy ochronne, np.:
  - systemy oburęcznego sterowania
  - kontrola dostępu do stref niebezpiecznych
  - blokada osłon, itp.

## Przykłady zastosowań PN - EN 61508

- złożone systemy sterowania dużymi maszynami lub grupami maszyn
- sterowniki programowalne dedykowane do realizacji funkcji bezpieczeństwa
- elektroczułe urządzenia ochronne, takie jak:
  - kurtyny świetlne
  - skanery laserowe

## Certyfikacja bezpieczeństwa funkcjonalnego

- maszyny i urządzenia ochronne wymienione w załączniku IV do Dyrektywy Maszynowej podlegają obowiązkowi oceny z udziałem jednostki notyfikowanej
- ocena ta obejmuje także ocenę systemu sterowania (p. 1.2.7 i p. 1.4.3 dyrektywy)
- w przypadku braku norm zharmonizowanych systemy te powinny być badane i oceniane wg PN-EN 954-1 lub w aspekcie bezpieczeństwa funkcjonalnego (pr. IEC 62061 lub PN-EN 61508)

## Certyfikacja bezpieczeństwa funkcjonalnego

Ocena bezpieczeństwa obejmuje trzy podstawowe aspekty:

- zarządzanie bezpieczeństwem funkcjonalnym
- wyznaczenie SIL sprzętu
- wyznaczenie SIL oprogramowania

## Certyfikacja bezpieczeństwa funkcjonalnego

Podstawowe problemy przy ocenie bezpieczeństwa funkcjonalnego sterowników maszyn:

- brak metodologii oceny ryzyka umożliwiającej wyznaczenie wymaganego SIL
- brak danych o niezawodności stosowanych podzespołów
- brak jednolitych kryteriów oceny SIL oprogramowania

# **Bezpieczeństwo funkcjonalne programowalnych układów sterowania maszyn**

**Dziękuję za uwagę**

---

**Marek Dźwiarek**

---

Zakład Techniki Bezpieczeństwa