

# AUTOMATYKA ZABEZPIECZENIOWA TO NIE TYLKO CERTYFIKOWANE STEROWNIKI

---

**Witold Głodek**

MPCo Polska s.c. Warszawa

[mpco@pol.pl](mailto:mpco@pol.pl)

---

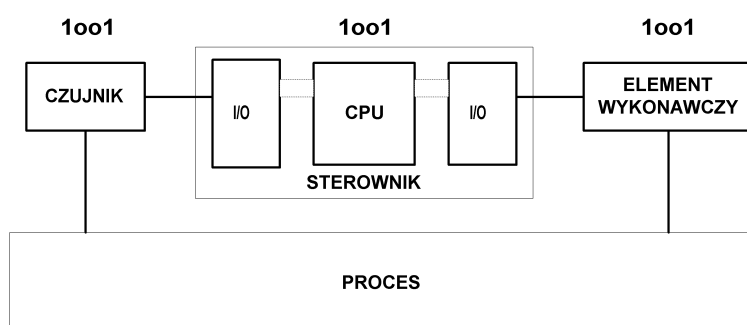
*Abstrakt – Wieloletnie posługiwanie się normą DIN VDE 0801 spowodowało kierowanie całej uwagi projektujących układy automatyki zabezpieczeniowej na część centralną tych obwodów - sterowniki. Tymczasem o parametrach obwodu blokadowego świadczą głównie jego elementy obiektowe, czyli czujniki i elementy wykonawcze*

## **Wprowadzenie**

Jeszcze do niedawna dyskusje dotyczące wyboru właściwego układu automatyki zabezpieczeniowej obracały się głównie wokół wyboru odpowiedniego sterownika i odpowiedniej jego konfiguracji. Głównymi dostawcami informacji na temat zasad tworzenia układów blokadowych byli właśnie producenci sterowników. Dostawcy prezentowali niezawodność sterowników, omawiali możliwości ich redundowania, mówili o łatwości oprogramowywania i serwisowania... Gdy jednak projektant zostawał sam, kiedyś nad deską kreślarską, a ostatnio przed ekranem komputera, stwierdzał, że „sęk tkwi” wcale nie w sterowniku i jego oprogramowaniu - te z reguły były już wybrane, ale w wyborze pozostałych elementów układu blokadowego. Brak prawidłowego, pewnego sygnału z czujnika, który można by było wprowadzić do sterownika, konieczność korzystania z jakiegoś nie bardzo pewnego elementu wykonawczego, czy wreszcie zaprojektowanie odpowiednio pewnych układów zasilających, okazywało się podstawowym problemem technicznym. Do niedawna nie istniały obiektywne kryteria oceny poszczególnych rozwiązań projektowych. Jedyną normą, którą się posługiwano (DIN V VDE0801) dotyczyła praktycznie wyłącznie sterowników. Dopiero pojawienie się normy IEC 61508 i ostatnio IEC 61511 radykalnie zmieniło sytuację. Obie te nowe normy dotyczą bowiem całych obwodów blokadowych, od czujnika, przez układ logiczny (zwykle sterownik), do elementu wykonawczego. W normach wprowadzono parametr będący miarą pewności zabezpieczenia oraz przedstawiono jak ten parametr obliczać. Pewność działania pętli blokadowej określa średnie prawdopodobieństwo jej niezadziałania gdy będzie ono wymagane (PFDavg). Liczbowa ocena istniejących obwodów blokadowych potwierdziła intuicję – pewność działania pętli blokadowej jedynie w 10-15% zależy od pewności działania sterownika. Znacznie większy wpływ mają czujniki (20-40%) i elementy wykonawcze (40-60%).

### Przykład

Przeanalizujemy przykład z typowymi parametrami urządzeń stosowanych w układach blokadowych. Trzeba stanowczo podkreślić, że nie da się stworzyć układu blokadowego, zgodnego z normami IEC bez posiadania podstawowych parametrów niezawodnościowych użytych w nim elementów. Skąd wziąć te dane, to temat rzeka. W zasadzie normy amerykańskie wymagają ich od producentów urządzeń.. Schemat analizowanej pętli blokadowej przedstawia rysunek 1. Dla uzyskania efektu dydaktycznego przy obliczeniach prawdopodobieństw zastosowano poważne uproszczenia. Wyniki obliczeń prezentuje tabela 1. Widać z niej, że „wszystko” zależy od aparatury obiektowej. Co zrobić aby poprawić pewność całego zabezpieczenia?



Rys.1 Prosty układ zabezpieczający

Tabela 1.

Parametr	jednostki	Czujnik	Sterownik 1001D (beta=0.0)			Element wykonawczy	Cała pętla
			Wejścia	CPU	Wyjścia		
MTBF	lata	50	50	15	50	20	
Udział awarii groźnych	%	40	25	50	25	25	
Autodiagnostyka	%	0	97	97	97	0	
Przeglądy	miesiące	12	12	12	12	12	
Czas przeglądu (on line)	godziny	1	1			1	
Czas naprawy (on line)	godziny	8	8			8	
PFDavg		0.00413	0.00082			0.0064	0.01135
Udział w PFDavg	%	36.4	7.2			56.4	100
RRF = 1/PFDavg							88 (SIL1)

Zajmijmy się czujnikami i elementami wykonawczymi. Jakie są sposoby poprawienia pewności ich zadziałania?

Już z pobieżnej analizy tabeli nr 1 widać, że czas między awariami (MTBF) prostych czujników i zaworów wykonawczych jest zbliżony do czasów między awariami sterowników. 50-20-15 lat to wielkości tego samego rzędu i nie w nich należy szukać głównego czynnika, wpływającego na pewność działania zabezpieczenia. Znacząca różnica występuje w poziomie autodiagnostyki tych urządzeń. Proste czujniki, takie jak presostaty, czy termostaty są trwałe, ale całkowicie pozbawione możliwości automatycznego testowania. Podobnie z prostymi zaworami odcinającymi. Ze względu na istnienie części

ruchomych, kontaktujących się na dodatek z medium procesowym są bardziej zawodne od czujników. Wymuszanie ich awaryjnego zadziałania przy pomocy sprężyny powoduje, że przeważnie psują się w „bezpieczny”, przewidywalny sposób. Autodiagnostyki jednak z reguły nie posiadają. W przypadku sterowników sytuacja jest inna. Psują się one stosunkowo często – w naszym przykładzie średnio co 15lat, ale za to aż 97% ich awarii wykrywa ich wewnętrzny układ diagnostyczny. O awarii informuje on operatora lub sam sprowadza instalację do stanu bezpiecznego. Są to więc w 97 procentach przypadków awarie bezpieczne, powodujące w najgorszym przypadku odstawienie instalacji i straty w produkcji. Tylko 3% ze zdarzających się średnio co 15lat awarii uniemożliwia zadziałanie zabezpieczenia. Są to awarie groźne.

Mamy kilka metod na poprawienie pewności działania aparatury obiektowej. Są to:

- poprawa parametrów niezawodnościowych używanych urządzeń,
- redundowanie urządzeń,
- zwiększenie poziomu diagnozowania tych urządzeń,
- zwiększenie częstotliwości przeglądów,

Jak stosowane są te metody?

## **Czujniki**

***Poprawa parametrów niezawodnościowych czujników.*** Poprawa taka, w ramach jednego typu urządzeń, jest możliwa w zaledwie w niewielkim zakresie. Przy wyborze czujnika kierować się trzeba własnymi doświadczeniami z poprzednich aplikacji i danymi od producentów. Należy przy tym pamiętać, że awarie w dużej mierze wynikają w warunków zabudowy czujników i informacje od producentów należy modyfikować o pewne eksperckie współczynniki korekcyjne.

Najczęściej stosowanym ostatnio sposobem na powiększenie niezawodności czujników jest zastępowanie, powszechnie używanych czujników dwustanowych, przetwornikami pomiarowymi. Ze względu na brak części mechanicznych są one bardziej niezawodne (MTBF ponad 100lat) i posiadają pewną autodiagnostykę.

Innym sposobem jest rezygnacja z barier lub separatorów iskrobezpiecznych i zastępowanie ich układami w wykonaniu Exd. Wprowadzenie do obwodu blokadowego dodatkowych elementów w oczywisty sposób powoduje zmniejszenie niezawodności układu.

***Redundowanie czujników*** jest najdroższą metodą uzyskiwania pewności działania układów zabezpieczających. Metoda ta musi być stosowana w układach klasy SIL3 i wyższej. Trzeba pamiętać, że zwiększanie liczby czujników w proporcjonalny sposób zwiększa liczbę awarii bezpiecznych.

***Autodiagnozowanie czujników*** pozwala na wykrywanie ich awarii. Dostępne są dwie techniki postępowania:

- używanie urządzeń z wbudowanymi układami diagnozującymi. Jest ich stosunkowo mało. Niektóre z nich posiadają diagnostykę obejmującą ponad 95% możliwych awarii.
- wykorzystywanie redundancji. Porównywanie sygnałów ze zwielokrotnionych czujników pozwala na wyciąganie wniosków na temat poprawności ich działania

## **Elementy wykonawcze**

**Niezawodność elementów wykonawczych** w dużej mierze zależy od prawidłowego ich doboru i dbania o to aby pracowały w warunkach przewidzianych przez producenta. Wybierać należy zawory pozwalające na przeprowadzanie testów on-line oraz te, wyposażone w układy diagnostyczne. Dalsza poprawa parametrów niezawodnościowych już wybranego zaworu praktycznie nie jest możliwa. Do dyspozycji mamy wtedy jedynie możliwość wpływania na jakość powietrza automatyki.

**Diagnozowanie zaworów** on-line pozwala na sprawdzaniu na ruchu, czy zawory nie utraciły możliwości zadziałania. Niektóre zawory wyposażane są w **automatyczne układy diagnostyczne**, pozwalające na testowanie poprzez wykonywanie częściowych ruchów zaworem. Dotyczy to oczywiście jedynie zaworów w normalnych warunkach pracy instalacji otwartych, czyli otwieranych powietrzem i zamykanych sprężyną. Poprzez wykonywanie częściowych ruchów zaworem sprawdzić można 70-80% potencjalnych awarii zaworu. W przypadku zaworów odcinających, będących jednocześnie zaworami regulacyjnymi w układach automatyki procesowej (BPCS), do takiego diagnozowania służyć mogą informacje z inteligentnych ustawników pozycyjnych. Pamiętać jednak należy, że dodawanie pozycjonerów do zaworów odcinających, tylko w celach diagnostycznych, może być przyczyną niepotrzebnych pełnych przesterowań zaworów i kosztownych odstawiń instalacji.

**Zwiększenie częstotliwość przeglądów** pozwala na poprawę pewności pracy zabezpieczenia. Awarie nie wykryte przez autodiagnostykę, jeżeli ona w ogóle istnieje, mogą zostać wykryte podczas przeglądów okresowych. Podstawowym problemem pojawiającym się przy wykorzystywaniu tej metody jest pytanie o możliwość wykonywania takich przeglądów podczas pracy instalacji. Odstawienie instalacji wiąże się ze znacznymi kosztami i przeważnie nie jest dopuszczalne. Podczas ręcznego testowania on-line, szczególnie układów bez redundancji, obwód zabezpieczający nie działa. Dodatkowym zagrożeniem jest możliwość błędnego przesterowania zaworu i odstawienie instalacji podczas testu. Znane są także przypadki pozostawienia po zakończeniu testów blokad ograniczających ruchy zaworów, co całkowicie uniemożliwiało zadziałanie zabezpieczeń.

Pewność działania prostego układu blokadowego testowego on-line w przybliżeniu opisać można poniższą zależnością

$$PFD_{AVG} = \frac{1}{2} \lambda_D (\text{Tip D} + \text{Tic (1-D)}) + \text{TT/Tip}$$

Gdzie:

$\lambda_D$  - częstotliwość występowania uszkodzeń groźnych - takich, które uniemożliwiają zadziałanie zabezpieczenia,

**TT** - czas trwania testu sprawności zabezpieczenia,

**Tip** - okres między przeglądami częściowymi,

**Tic** - okres między przeglądami pełnymi,

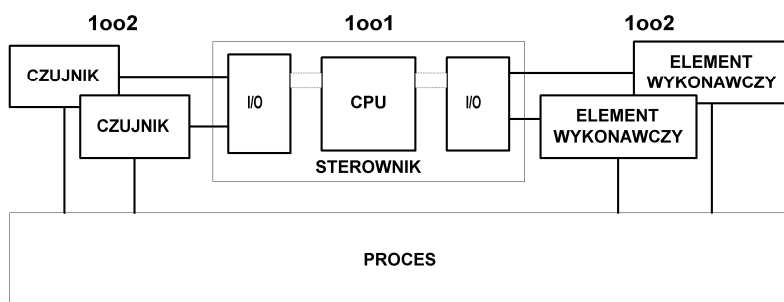
**D** - stopień efektywności przeglądów częściowych (pokrycie diagnozowaniem)

Przy częstych (małe Tip) i długich przeglądach (duże TT), czynnik TT/Tip może zniweczyć zyski wynikające z możliwości szybszego wykrycia awarii (małe  $\lambda_D$  Tip).

W przypadku testowania automatycznego, i to bez ograniczania funkcji bezpieczeństwa, duża częstotliwość testów eliminuje wpływ składników Tip D i TT/Tip. Pozostaje jedynie składnik  $\frac{1}{2} \lambda_D \text{Tic (1-D)}$  i to on właśnie świadczy o pewności tej części zabezpieczenia ( $PFD_{AVG}$ ). Następuje wtedy D/(1-D) krotna pewności zadziałania.

**Powróćmy do przykładu** obliczeniowego i dokonajmy modyfikacji obwodu. Obliczmy bezpieczeństwo następujących wariantów (rys. 2):

- 1 – zastosowanie redundancji czujników (1oo2)
- 2 – zastosowanie cyfrowego inteligentnego przetwornika pomiarowego
- 3 – zastosowanie cyfrowego przetwornika inteligentnego pomiarowego z certyfikatem TÜV SIL2.



Rys.2 Układ zabezpieczający z redundancją czujników i elementów wykonawczych

Tabela 2.

Parametr	jednostki	Czujniki 1oo1	Czujniki 1oo2 (beta=0)	Czujniki 1oo2 (beta=2)	Przetwornik pomiarowy	Certyfikowany przetwornik pomiarowy
MTBF	lata	50	50	50	176.77	147.6
Udział awarii groźnych	%	40	40	40	34.1	65
Autodiagnostyka	%	0	0	0	60	94.2
Przeglądy	miesiące	12	12	12	12	12
Czas przeglądu (on line)	godziny	1	1	1	1	1
Czas naprawy (on line)	godziny	8	8	8	8	8
PFDavg		0.00413	0.000041	0.00010	0.000991	0.000242

Z tabeli 2 wysnuć można następujące wnioski:

- już pojedynczy czujnik dwustanowy z reguły pozwala na zbudowanie układu klasy SIL2,
- dwa zredundowane czujniki dwustanowe pozwalają na zbudowanie układu klasy SIL3,
- możliwość pojawienia się błędów wspólnej przyczyny ( ich udział we wszystkich możliwych błędach określa współczynnik beta ) znacząco pogarsza parametry bezpieczeństwa układu zabezpieczeń,
- inteligentny przetwornik pomiarowy powszechnego stosowania, w porównaniu z przetwornikiem dedykowanym do pracy w układach zabezpieczeń, ma kilkakrotnie wyższe prawdopodobieństwo wystąpienia błędu groźnego, czyli takiego który uniemożliwia zadziałanie zabezpieczenia.
- przetworniki inteligentne powszechnego stosowania, zgodnie z normą IEC 61508, należą do urządzeń typu B. O możliwości zastosowania urządzeń tego typu w obwodach zabezpieczeniowych świadczy procentowy udział awarii bezpiecznych we wszystkich awariach. Przedstawiony w przykładzie przetwornik pomiarowy ogólnego stosowania posiada co prawda niską wartość PFDavg ( $PFD_{avg} = 0.000991$  /rok), jednak ze względu na wysoki, procentowy udział nie wykrytych awarii groźnych (21%), może być samodzielnie wykorzystywany jedynie w zabezpieczeniach klasy SIL1.
- w przetworniku certyfikowanym autodiagnostyka jest tak rozbudowana (94.2% funkcji jest diagnozowane), że pomimo gorszego MTBF, udział nie wykrytych awarii groźnych wynosi jedynie około 5% , co łącznie z dobrym PFDavg pozwala na jego stosowanie w obwodach klasy SIL2 nawet bez redundancji.

W kolejnym przykładzie pokazano jaki wpływ na pewność zabezpieczenia ma częstotliwość testów polegających na częściowym przesterowaniu zaworu. Założono, że efektywność testu częściowego wynosi 75% awarii.

Tabela 3.

Parametr	jednostki	Zawór 1oo1 (test co 12m)	Zawór 1oo1 (test co 4m)	Zawór 1oo1 (test co 1m)	Zawory 1oo2 (beta=5%)
MTBF	lata	20	20	20	20
Udział awarii groźnych	%	25	25	25	25
Autodiagnostyka	%	0	0	0	0
Przeglądy część/całk	miesiące	12/12	3/12	1/12	12/12
Czas przeglądu (on line)	godziny	1	1	1	-
Czas naprawy (on line)	godziny	8	8	8	-
PFDavg		0.0064	0.0032	0.0019	0.000117

Wnioski z obliczeń są proste:

- zwiększenie częstotliwości testów częściowych poprawia pewność zabezpieczenia,

- pojedyncze zawory odcinające z prostymi zaworkami elektromagnetycznymi można stosować nawet do układów klasy SIL2 . Według normy IEC 61508 należą one do urządzeń klasy A. Wyjątek stanowią urządzenia z cyfrowymi ustawnikami pozycyjnymi, które należą do urządzeń typu B.

### **Podsumowanie**

Pewność pracy układów blokadowych w dużej mierze zależy od pewności działania aparatury obiektowej,

Projektowanie obwodów zabezpieczających napotyka na liczne trudności, szczególnie gdy w grę wchodzi aparatura obiektowa. Najważniejsze z nich to:

- duża różnorodność dostępnych konfiguracji i związane z tym kłopoty obliczeniowe,
- brak danych o parametrach niezawodnościowych urządzeń składowych,

Wpływ jakości i częstotliwości wykonywanych testów w proporcjonalny sposób przyczynia się poprawy do bezpieczeństwa instalacji.

Literatura:

- 1- ANSI/ISA S84,01-1996 Application of Safety Instrumented Systems for Process Industry  
ISBN- 1-55617-590-6
- 2- IEC 61508 Functional Safety of electrical/electronic/programmable electronic safety-related systems  
Parts 1-7
- 2- ISA-TR84.00.03.2002 Guidance for testing of Process Sector Safety Instrumented Functions  
ISBN- 1-55617-801-8
- 4- ISA-TR84.00.02.2002 Safety Instrumented Functions (SIF) Safety Integrity Level evaluation  
Techniques Parts 1-5, ISBN- 1-55617-802-6
- 5- Failure Modes, Effects and Diagnostic Analysis Summary - Rosemount 3051T Pressure Transmitter  
Exida 2001
- 6- Safety Integrity Level Verification, Failure Rate Data for the 345 Critical transmitter  
Moore Process Co. 2000

Witold Głodek  
mpco@pol.pl