Mariusz Siczek, Roman Pniewski

Koncepcja bezpieczeństwa systemów pomiarowo-sterujących ze sterownikiem PLC

JEL: R41 DOI: 10.24136/atest.2018.387
Data zgłoszenia: 19.11.2018 Data akceptacji: 15.12.2018

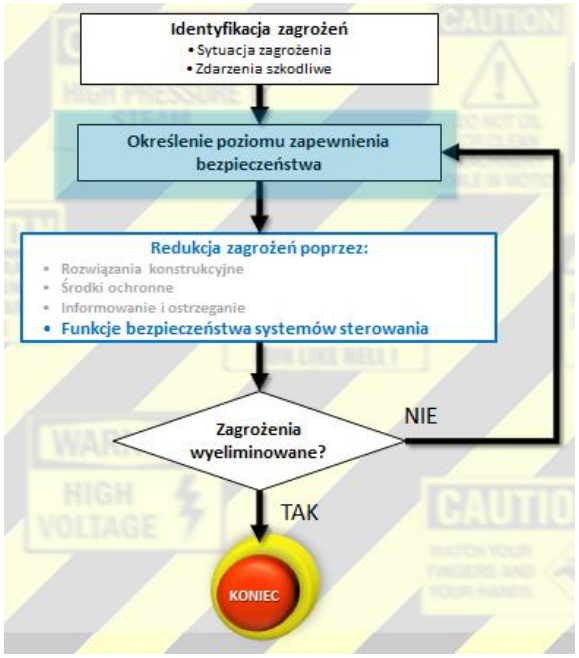
W artykule omówiono koncepcję bezpieczeństwa systemów pomiarowo-sterujących z zastosowaniem sterownika PLC. Zaprezentowano rozwiązanie zastosowane w prostych systemach sterowania, gdzie stosowanie drogich elementów wykonawczych z wysokim stopniem bezpieczeństwa jest niecelowe. Opisane autorskie rozwiązania są stosowane do systemów: elektrycznych, hydraulicznych i pneumatycznych.

Słowa kluczowe: System bezpieczeństwa, bezpieczeństwo, system pomiarowo-sterujący, PLC, HMI.

Wstęp

Wg Dyrektywy Maszynowej 2006/42/WE [1] producent maszyny musi zapewnić przeprowadzenie oceny ryzyka w celu określenia wymagań w zakresie ochrony zdrowia i bezpieczeństwa (rys.1), które mają zastosowanie do maszyny. Zatem maszyna musi być zaprojektowana i wykonana z uwzględnieniem wyników oceny ryzyka [2].

Aby maszyna została zaprojektowana i wykonana z uwzględnieniem wyników oceny ryzyka, ocena ryzyka musi zostać wykonana przed zaprojektowaniem maszyny. W procesie projektowania i budowy może jednak dojść do zmian konstrukcyjnych maszyny, więc w trakcie powstawania maszyny należy zapewnić odpowiedni sposób zarządzania ryzykiem, aby zapewnić zamierzony poziom bezpieczeństwa maszyny, zgodnie z aktualnym stanem wiedzy techniki.[3]



Rys. 1. Procedura identyfikacji i redukcji zagrożeń

Do źródeł wystąpienia tych zagrożeń [4] należą w szczególności:

- ruchome elementy użytkowanych maszyn, narzędzi i innych urządzeń technicznych (ruchome elementy napędu, głowice, uchwyty oraz miejsca zbiegania się obracających się elementów – koła zębate, koła cierne, koła pasowe, koła łańcuchowe – narzędzia poruszające się ruchem posuwisto-zwrotnym lub obrotowym itp.)
- przemieszczające się elementy maszyn i innych urządzeń technicznych (stoły, suporty, głowice narzędziowe, uchwyty itp.)
- ostre, wystające i chropowate elementy materiałów, maszyn i innych urządzeń technicznych oraz wyposażenia miejsca pracy (elementy konstrukcyjne maszyn, narzędzia, chropowate przedmioty, ostre obrabiane przedmioty, ostre elementy urządzeń pomocniczych itp.)
- spadające elementy (obrabiane przedmioty, głowice, narzędzia, uchwyty, imadła itp.)
- śliskie i nierówne powierzchnie w miejscu pracy powstałe wskutek rozprysku lub rozlania się płynów technologicznych (oleje, płyny chłodzące) czy ubytków w posadzkach będących wynikiem wadliwego wykonawstwa lub zużycia technicznego itp.
- powierzchnie gorące (odpryski wiórów powstałe podczas skrawania czy też powierzchnie maszyn, innych urządzeń technicznych, obrabianych przedmiotów lub instalacji technologicznych itp.)
- wyrzuty obrabianych elementów, narzędzi lub przedmiotów podczas procesu skrawania (wióry lub odpryski z obrabianych przedmiotów, uszkodzone lub pęknięte narzędzia lub przedmioty itp.)
- prowadzenie prac konserwatorskich, remontowych i naprawczych na wysokości lub w zagłębieniach
- ograniczone przestrzenie przy maszynach i innych urządzeniach technicznych, zwłaszcza podczas dojścia do nich lub przejścia obok nich
- wytrysk płynów pod ciśnieniem (układy hydrauliczne).

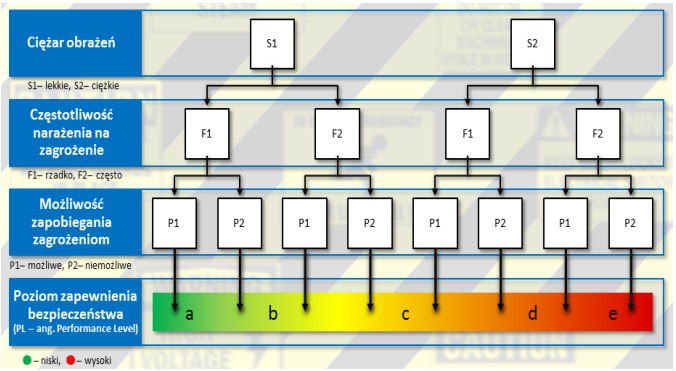
Z praktyki doświadczeń autorów innymi przyczynami występowania zagrożeń mogą być:

- błędne działanie elementów (sklejenie styków, mechaniczne uszkodzenia styczników
- i przekaźników),
- przekroczenie dopuszczalnych prądów pracy silników zasilanych bezpośrednio (bez sterowników lub przemienników częstotliwości),
- wzrost temperatury grzałek lub przestrzeni roboczej,
- diagnostyka torów komunikacji: RS232, RS485, Etherenet, Modbus i Modbus TCP,
- zaniki napięcia.

Dlatego w maszynach ważne jest także monitorowanie zużycia energii i innych czynników.[5]

1.Bezpieczeństwo i jego aspekty w odniesieniu do urządzeń

W normie PN-EN ISO 13849-1 [6] przedstawiono ogólne wymagania i wskazania dotyczące projektowania systemów bezpieczeństwa (rys.2.)



Rys. 2 Określenie żądanego poziomu bezpieczeństwa (PL)

Parametrami technicznymi charakteryzującymi system są:
- średni czas wystąpienia defektu (MTTFd),
- pokrycie diagnostyczne wykrywania defektów (DC),
- współczynnik defektów od wspólnej przyczyny (CCF).

Parametry te są kwalifikowane do grup jakościowych: duży, średni, mały. Przewidywany poziom zapewnienia bezpieczeństwa określany jest na podstawie grafu uwzględniającego oszacowane parametry oraz architekturę systemu (jednokanałowy, redundancja, monitorowanie itp.). Pozwala to, w stosunkowo prosty sposób, dokonać oceny zaprojektowanego systemu. Metoda ta, ze względu na uproszczony sposób oceny nie uwzględnia wielu czynników wpływających na prawdopodobieństwo wystąpienia niebezpiecznego uszkodzenia. Dlatego też zakres jej stosowania jest ograniczony jedynie do systemów niezbyt złożonych. Przewiduje się, że będzie ona stosowana do analizy systemów hydraulicznych, pneumatycznych oraz elektrycznych.

Poziom bezpieczeństwa podsystemu zależy od różnych parametrów bezpieczeństwa technicznego, takich jak:
- Struktura,
- Niezawodność elementów składowych/urządzeń,
- Diagnostyka wykrywania uszkodzeń,
- Odporność na uszkodzenia spowodowane wspólną przyczyną
- Proces

Omówione powyżej zależności zostały przedstawione w tabeli 1 i powiązanej z nią tabeli 2.

Tab. 1. Pięć filarów poziomu zapewnienia bezpieczeństwa PL dla układu sterowania

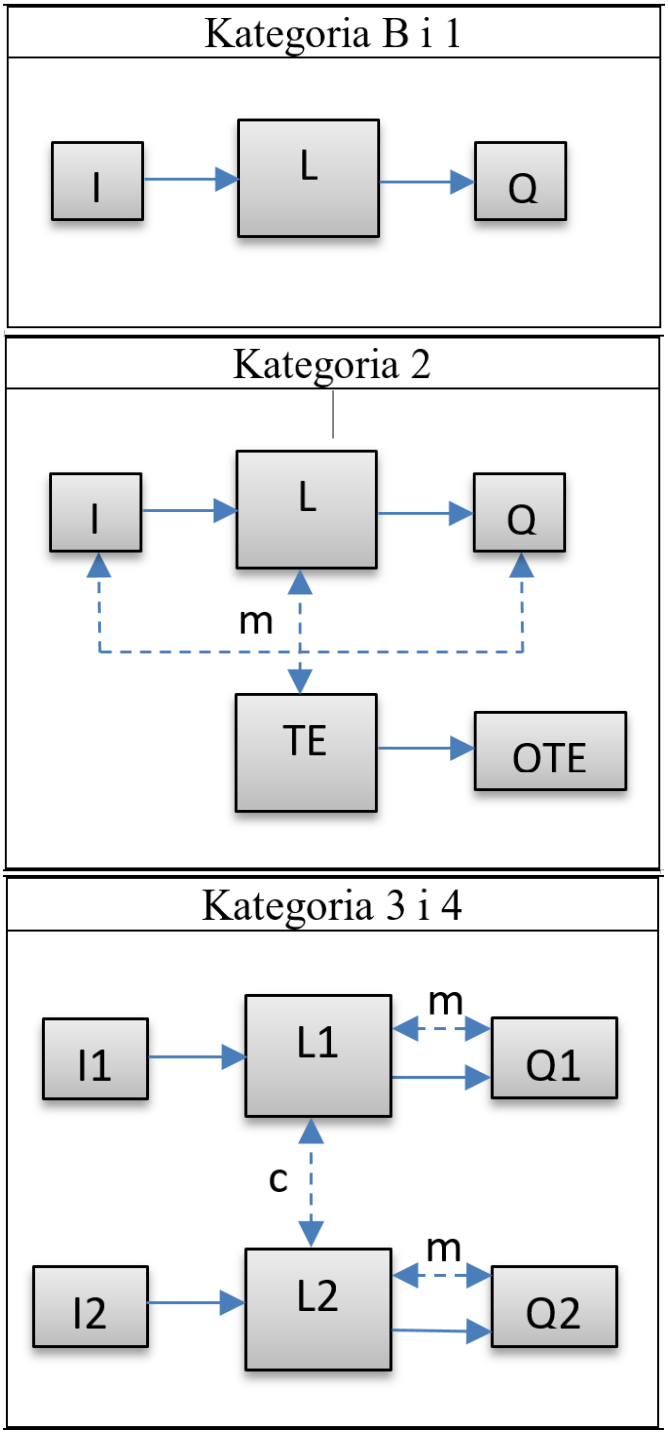
PL – Poziom bezpieczeństwa				
Kategoria	MTTFd	DC	CCF	Weryfikacja
STRUKTURA	NIEZAWODNOŚĆ	DIAGNOSTYKA	ODPORNOŚĆ	PROCES

Tab. 2. Poziomy zapewnienia bezpieczeństwa [7]

Poziomy zapewnienia bezpieczeństwa	Średnie prawdopodobieństwo uszkodzenia niebezpiecznego na godz.	Poziom nienaruszalności bezpieczeństwa SIL
a	≥ 10-5 do < 10-4	brak specjalnych wymagań
b	≥ 3·10-6 to < 10-5	1
c	≥ 10-6 to < 3·10-6	1
d	≥ 10-7 do < 10-6	2
e	≥ 10-8 do < 10-7	3

Kategoria B i kategoria 1 według PN-EN ISO 13849-1 jest architekturą szeregową, bez środków wykrywania defektów. W kategorii 2. system zawiera urządzenie monitorujące okresowo poprawność jego pracy. Kategoria 3. jest systemem z redundancją, a kategoria 4. redundancja z monitorowaniem krzyżowym.

Na rysunku 3 przedstawiono warianty architektury sprzętowej realizujące funkcje bezpieczeństwa.



Rys. 3 Warianty architektury sprzętowej realizacji funkcji bezpieczeństwa zgodne z normą PN-EN ISO 13849-1

Wyróżnione elementy oznaczono następująco:
I (DI, AI) – wejścia cyfrowe i analogowe,
L (L1, L2) – logika (realizacja funkcji np. PLC),
Q (DQ, AQ) – wyjścia cyfrowe i analogowe,
TE – moduł testujący (oprogramowanie, inny sterownik zabezpieczeń, itp.)
OTE – wyjście modułu TE (sygnalizacja świetlna lub akustyczna, pulpit operatora HMI)

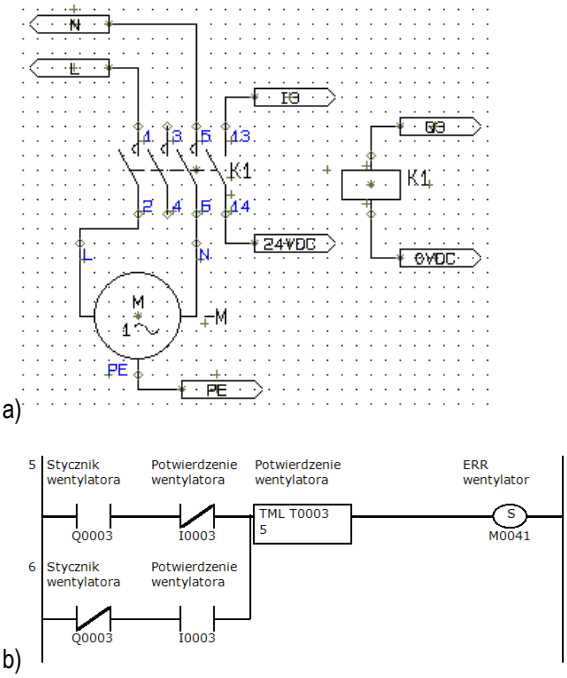
m – monitoring wyjść (procedury diagnostyczne torów analogowych i cyfrowych, np. w sterowniku PLC; elementy wykonawcze z diagnostyką – dodatkowe sygnały lub poprzez protokoły komunikacyjne),
c – monitoring krzyżowy (wzajemna diagnostyka).

2.Wybrane elementy bezpieczeństwa technicznego w systemach z PLC

Stosowany sterownik PLC posiada diagnostykę wejść i wyjść analogowych(AI/AQ). Diagnostyka ta dotyczy inicjalizacji i parametrów poszczególnych torów, przekroczenia dopuszczalnych wartości sygnałów – co jest wystarczające w praktyce inżynierskiej i pozwala programowo zapewnić bezpieczeństwo działania systemu pomiarowo-sterującego.

W przypadku wystąpienia błędu jest realizowana procedura awaryjnego wyłączenia. Ten mechanizm mimo iż wygląda że jest stosowany w kategorii B i 1 może być zaliczony do kategorii 2. Moduł TE jest niewidoczny (zrealizowany programowo), a jako moduł OTE jest wykorzystany pulpit operatora HMI.

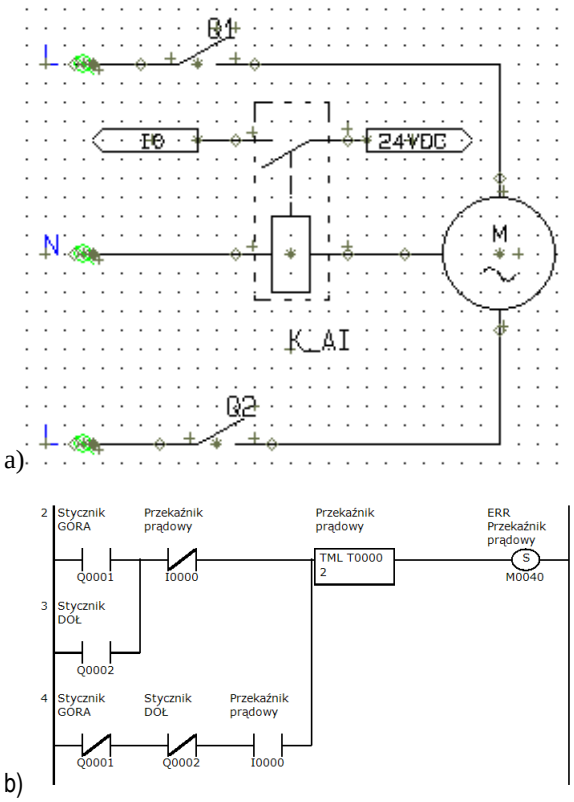
Na rysunku 4 przedstawiono kontrolę załączenia silnika za pomocą stycznika. Brak prawidłowych stanów styku pomocniczego i wyjścia sterującego cewką stycznika po pewnym czasie, odmierzanym przez licznik TML, powoduje zapalenie flagu błędu M0000. Ta prosta diagnostyka z doświadczeń autora jest niezwykle skuteczna. Może być stosowana do wszelkich urządzeń załączanych stycznikami lub przekaźnikami. W przypadku załączania grzałek można dodatkowo kontrolować temperaturę grzałek, co jest wymogiem normy maszynowej. Zapobiega to przepalaniu grzałek oraz dodatkowo po przez kontrolę wzrostu temperatury można stwierdzić poprawne działanie obwodu. Ten mechanizm realizacji funkcji bezpieczeństwa odpowiada kategorii B i 1 oraz kategorii 2.].



a) b)

Rys. 4 Diagnostyka załączenia silnika a) schemat ideowy, b) fragment programu.

Na rysunku 5 przedstawiono kontrolę załączenia silnika z potwierdzeniem za pomocą kontroli prądu. Ten sposób został zastosowany do sterowania siłownikiem prądu przemiennego, który pracuje w ciężkich warunkach środowiska – wysoka wilgotność i zmiany temperatury w dużym zakresie -20 ÷ +80ºC. Załączenie stycznika Q1 i Q2, podobnie jak w poprzednim przykładzie jest kontrolowane za pomocą styków pomocniczych. Położenie siłownika jest sygnalizowane jego krańcówkami. Dodatkowo w torze neutralnym umieszczono przekaźnik prądowy, który działa w momencie, gdy jest załączony jeden ze styczników Q1 lub Q2. Jest to informacja o tym, że silnik pracuje. Mierząc czas działania siłownika Q1 i Q2 możemy dodatkowo aproksymować stan położenia siłownika. Ten mechanizm realizacji funkcji bezpieczeństwa odpowiada kategorii B i 1 oraz kategorii 2.



a) b)

Rys. 5 Diagnostyka załączenia silnika z kontrolą prądu a) schemat ideowy, b) fragment programu.

Podsumowanie

Funkcja bezpieczeństwa musi być uwzględniana na etapie projektowania i utrzymana w następnych etapach życia urządzenia: produkcji, instalacji, montażu, działania, konserwacji itd. Funkcja bezpieczeństwa realizowana przez elementy systemów sterowania ogranicza zagrożenia w sytuacji krytycznej.

Głównym zadaniem projektanta systemu bezpieczeństwa jest zapobieganie występowaniu sytuacji zagrożenia oraz niezamierzonemu uruchomieniu urządzenia poprzez implementację zabezpieczeń programowych i/lub sprzętowych.

Utrudnieniem dla projektantów systemów sterowania jest brak wystarczająco przejrzystych dokumentów normalizacyjnych, zatem istotne znaczenie mają prace badawcze prowadzone w tym zakresie.

Bibliografia:

1. Dyrektywa 2006/42/WE z dn. 17 maja 2006r (PL) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:pl:PDF.
2. https://bezpieczenstwowsystemachsterowania.pl/category/bezpieczna-maszyna-zasady-projektowania/.
3. https://bezpieczenstwowsystemachsterowania.pl/2018/05/rola-i-znaczenie-oceny-ryzyka/
4. Zawieska W.M. (2008) Ryzyko zawodowe – metodyczne podstawy oceny CIOP-PIB, Warszawa.

5. https://www.ciop.pl/CIOPPortalWAR/appmanager/ciop/pl?_nfpb=true&_pageLabel=P312001232514435415140 96&html_tresc_root_id=11518&html_tresc_id=11526&html_klucz=11518&html_klucz_spis
6. PN-EN ISO 13849-1:2008/AC:2009 Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania.
7. Bezpieczeństwo funkcjonalne systemów sterowania maszynami w świetle przepisów wprowadzających dyrektywy UE - dr inż. MAREK DŹWIAREK Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, BEZPIECZEŃSTWO PRACY 12/2004.

The concept of the safety of measurement and control systems with a PLC

The article presents the concept of safety of measurement and control systems with the use of a PLC controller. The solution presented in simple control systems was presented, where the use of expensive executive elements with a high degree of security is pointless. The proprietary solutions described are used for electrical, hydraulic and pneumatic systems.

Keywords: Security system, security, measurement and control system, PLC, HMI..

Autorzy:

mgr inż. **Mariusz Siczek** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki (student studiów III stopnia).

dr hab. inż. **Roman Pniewski** prof. nadz. – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, r.pniewski@uthrad.pl