Wstęp do bezpieczeństwa układów sterowania maszyn

TEKST mgr inż. Markus Kusiak, dr inż. Stanisław Kowalewski - ELOKON Polska

Można śmiało powiedzieć, że układy sterowania maszyn to ich systemy nerwowe i możliwości intelektualne. To od nich właśnie zależy, jak napędy i układy wykonawcze maszyn reagują na sygnały pochodzące od operatorów i rozmaitych sensorów. Od budowy ich struktur i cech poszczególnych elementów zależy odporność na działania środowiskowe, ewentualne uszkodzenia i zachowanie się w razie defektów. Dlatego budowa i niezawodność układów sterowania maszyn mają bezpośredni wpływ na poziom bezpieczeństwa (ryzyka) ich obsługi.

Znajduje to od dawna swój wyraz zarówno w europejskich i polskich zasadniczych wymaganiach bezpieczeństwa zawartych w poprzedniej Dyrektywie Maszynowej 98/37/WE, jak i obecnej NMD 2006/42/WE oraz w normach z nimi zharmonizowanych odnoszących się do maszyn „nowych". Praktycznie takie same wymagania stawia się układom sterowania w maszynach od dawna eksploatowanych. W tzw. Dyrektywie Narzędziowej 2009/104/WE dotyczącej wymagań minimalnych podczas użytkowania maszyn „starych", w zał. 1 pkt 2.1 (art. 11 polskiego rozporządzenia z dnia 30.10.2002 r.) sformułowano wymaganie stanowiące o istocie funkcjonalności bezpieczeństwa: „Układy sterowania maszyn powinny zapewniać bezpieczeństwo i być dobierane z uwzględnianiem możliwych uszkodzeń, defektów oraz ograniczeń, jakie można przewidzieć w planowanych warunkach użytkowania maszyny".

Większości wypadków na maszynach można byłoby uniknąć, gdyby układy odpowiedzialne za bezpieczeństwo były projektowane, budowane i użytkowane w pełni świadomie, tzn. na podstawie pełnego rozpoznania konieczności technologicznych, sformułowania ograniczeń konstrukcyjnych, identyfikacji zagrożeń i towarzyszącego im ryzyka oraz sposobów jego redukcji do poziomu tolerowalnego. Uczestnicząc w wielu projektach związanych z oceną i dostosowywaniem maszyn nowych do wymagań zasadniczych i starych do wymagań minimalnych, możemy stwierdzić, że głównym problemem jest niewiedza. Dotyczy to zarówno projektantów układów sterowania maszyn, jak również technologów i służb utrzymania ruchu podczas ich eksploatacji, konserwacji, napraw i modernizacji bez względu na wielkość firm. Niestety ocena ryzyka jest w praktyce warsztatowej wciąż postrzegana jako dolegliwość formalna, a nie jako profesjonalne narzędzie inżynierskie. Od służb odpowiedzialnych za funkcjonowanie maszyn wymaga się powszechnie, aby przede wszystkim realizowały cele technologiczne, dawały tani produkt o określonych cechach jakościowych przy maksymalnej wydajności. Takie uwarunkowania, z natury rzeczy, stoją w sprzeczności z zapewnieniem bezpieczeństwa. Dlatego tak istotna jest wiedza o bezpieczeństwie w ogóle, a o bezpieczeństwie układów sterowania w szczególności. Często inżynierom wydaje się, że wystarczy w układ sterowania włączyć przycisk stopu awaryjnego i sprawa jest załatwiona. Czynią to bez pogłębionych analiz ryzyka, nie znając zasad doboru urządzeń ochronnych i elementów sterowania odpowiedzialnych za bezpieczeństwo. Zasady oparte na szacowaniu i ocenie ryzyka są sformułowane w normach zharmonizowanych z obecną Dyrektywą Maszynową 2006/42/WE:

- PN-EN ISO 13 849-1:2008E. Bezpieczeństwo maszyn. Elementy systemów sterowania związane z bezpieczeństwem. Norma podaje związki pomiędzy parametrami niezawodności i ryzyka a Poziomami Nienaruszalności PL (Performance level) od a do e. Ta norma zastąpiła PN-EN 954-1, która definiowała pięć kategorii od B,1... do 4 opisujących odporność na uszkodzenia i zachowanie obiektu w razie jego wystąpienia. Mimo że została zastąpiona, jeszcze długo będzie funkcjonować w odniesieniu do maszyn zaprojektowanych zgodnie z poprzednią Dyrektywą Maszynową 98/37/WE.

■ PN-EN 62 061:2008P. Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem. Jest w niej odniesienie do tzw. bezpieczeństwa zintegrowanego oznaczanego SIL (Safety integrity level) na trzech poziomach od 1 do 3. Symbolem SIL powinny być oznakowane wszystkie elektroczułe urządzenia ochronne. Norma bardzo ważna dla producentów maszyn i elementów bezpieczeństwa.

Najczęściej występującym błędem w układach sterowania jest wykorzystywanie przemysłowych sterowników PLC do realizacji funkcji bezpieczeństwa. Do tych sterowników podłączane są wszelkie urządzenia i czujniki odpowiedzialne za procesy technologiczne, ale również urządzenia ochronne (osłony blokujące z/bez ryglowania, kurtyny i bariery świetlne, głowice skanujące, oburęczne sterowanie, listwy, maty i inne) i stopy awaryjne. Często brak jest nadzorowania osłon ruchomych lub nadzorowanie to posiada niewystarczającą odporność na utratę funkcji bezpieczeństwa. Rysunek 1 ilustruje przykład niewłaściwego podłączenia do układu sterowania osłon ruchomych – do sterownika PLC.

Prawidłowy układ pokazany został na rysunku 2, gdzie wykorzystano do nadzorowania dodatkowy moduł bezpieczeństwa/sterownik bezpieczeństwa, który bezpośrednio odcina energię dostarczaną do napędu.

Można sobie zadać pytanie, czym różni się zwykły sterownik PLC od sterownika bezpieczeństwa i czy jest rzeczywiście uzasadnione ponoszenie dodatkowych kosztów, skoro sterownik PLC całkiem dobrze poradzi sobie z realizacją funkcji nie tylko technologicznych, ale też i bezpieczeństwa. Jest w tym dużo prawdy, ponieważ przemysłowe sterowniki PLC z reguły pod względem możliwości przewyższają sterowniki bezpieczeństwa, które jednak należy stosować. Istnieje kilka podstawowych różnic, o których warto pamiętać, zanim podejmie się decyzję o wykorzystaniu w obwodach bezpieczeństwa sterowników przemysłowych PLC. Sterowniki bezpieczeństwa mają zawsze dwukanałową strukturę. W przypadku, gdy jeden z kanałów ulegnie uszkodzeniu, drugi kanał musi doprowadzić maszynę do stanu bezpiecznego. Często producenci sterowników stosują zasadę, by w jednym kanale znalazł się inny procesor (podzespoły) niż w drugim. Chodzi o uniknięcie błędów wynikających ze wspólnej przyczyny (np. w przypadku, gdy cała seria procesorów została wypuszczona na rynek z wadą, która może w pewnych warunkach się ujawnić). Ponadto, aby uniknąć błędów programowania, software jest tak skonstruowany i przebadany przez jednostki notyfikowane, żeby uniknąć takich błędów, jak np. zapętlenia. Również bloki funkcyjne oraz możliwości ich połączeń są narzucone w bardzo restrykcyjny sposób. Kolejną istotną różnicą jest zdecydowanie wyższa odporność na zewnętrzne zakłócenia środowiskowe. Również wyjścia i wejścia sterowników bezpieczeństwa są inaczej skonstruowane. Jest w nich ciągła, dynamiczna kontrola uszkodzeń, zwarć.

Na rysunkach 3, 4 i 5 pokazany jest układ połączeń na prasie, na której całkowicie wymieniono i zmodernizowano sterowanie w sposób nieodpowiedni, w wyniku czego operator stracił dłoń.

Na pierwszy rzut oka wygląda, że układ jest prawidłowy. Przekaźnikowy moduł bezpieczeństwa wysterowuje styczniki K15 i K16 (rys. 3), których styki odcinają zawór Y1 odpowiedzialny za ruch suwaka w dół (rys. 4). Wadliwe jest podłączenie, które zostało na rysunku 3 podkreślone na czerwono.

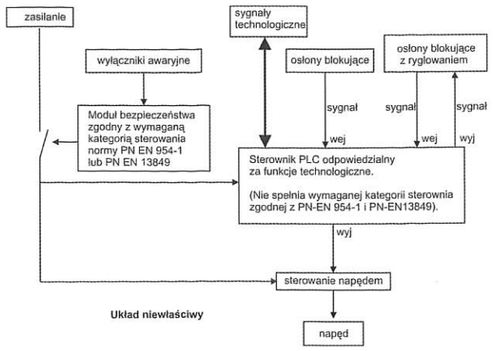
Połączenie to jest Q16 i Q17 i miało poprawić pewne właściwości technologiczne (rys. 5). Jest to klasyczny błąd występujący często na maszynach. Sterownik PLC przejął nadzór nad bezpieczeństwem. Do wypadku doszło podczas bardzo niekorzystnego zbiegu wypadków. W momencie, gdy operator zmieniał element pod stemplem prasy, w pobliżu przejeżdżał elektryczny wózek widłowy, który zwykle jeździł inną trasą. Zakłócenia z wózka były tak silne (po wypadku udało się tę sytuację zasymulować), że spowodowały zakłócenie pracy sterownika PLC, na którego wyjściach pojawił się sygnał wysoki i wysterował zawór. Nastąpił niezamierzony ruch suwaka w dół. Oczywiście istotną rolę odegrało tu również nieprawidłowe położenie kabli zasilających i brak ekranów, poprzez które zakłócenie dotarło do sterownika.

Innym częstym błędem jest wykorzystywanie w obwodach odpowiedzialnych za bezpieczeństwo styczników bez nadzorowania położenia styków. Jest to istotne ze względu na wczesne wykrycie takich błędów, jak sklejenie styków, pęknięcia sprężyn prowadzących itp. Warto zalecić zastosowanie w obwodach bezpieczeństwa tzw. Przekaźnikowych Modułów Bezpieczeństwa, które są coraz powszechniej wykorzystywane, są dostępne i coraz tańsze.

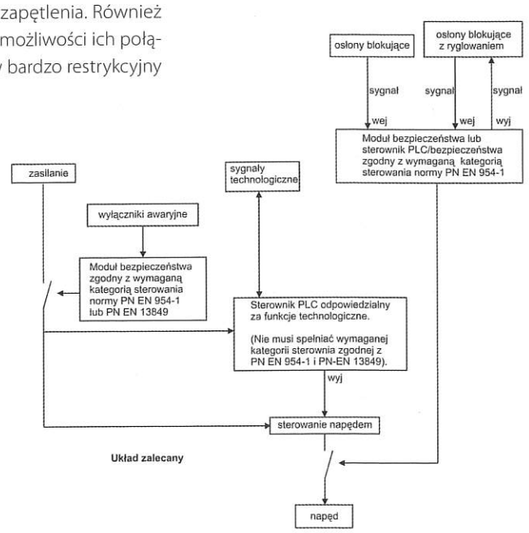
W całym procesie doboru środków bezpieczeństwa, tworzeniu odpowiednich schematów, doborze styczników, sterowników, modułów bezpieczeństwa itd. niezmiernie ważna jest prawidłowa ocena maszyn, zwłaszcza starych, przy których często brakuje dostępnych, aktualnych dokumentacji układów sterowania. Wtedy należy postępować bardzo ostrożnie, ponieważ wystarczy nieprawidłowe włączenie jednego z elementów, aby mogło dojść do tragicznego w skutkach wydarzenia wypadkowego. W naszej praktyce często jesteśmy powoływani do oceny stanu technicznego maszyn, na których takie zdarzenia miały miejsce. W zdecydowanej większości stwierdzaliśmy błędy w układach sterowania, gdzie nieprawidłowe połączenia były jedną z przyczyn wypadku. Zaprojektowane układy muszą mieć jeszcze dwie istotne cechy. Pierwsza z nich to nie przeszkadzać w normalnej obsłudze. Druga – nie powinny dawać się w prosty sposób obchodzić. Niestety często jest to czynione za wiedzą i przyzwoleniem nadzoru po to, aby np. zwiększyć wydajność pracy. Dlatego nie do przecenienia jest rola świadomych wymagań i odpowiedzialności służb utrzymania ruchu.

Warto również dodać jeszcze jedna uwagę. Często nie jest uwzględniany rzeczywisty czas zatrzymywania elementów niebezpiecznych maszyny po zadziałaniu urządzeń ochronnych. Brak jest udokumentowanych pomiarów świadczących o prawidłowych odległościach bezpieczeństwa urządzeń ochronnych od stref niebezpiecznych. Niestety bardzo często nie tylko nie są one wykonane przed pierwszym uruchomieniem, ale mimo obowiązku, jaki ciąży na pracodawcy (użytkowniku maszyny) również podczas eksploatacji nie są dokonywane wymagane kontrole okresowe. Do tego celu służą specjalne skalibrowane dobiegometry.

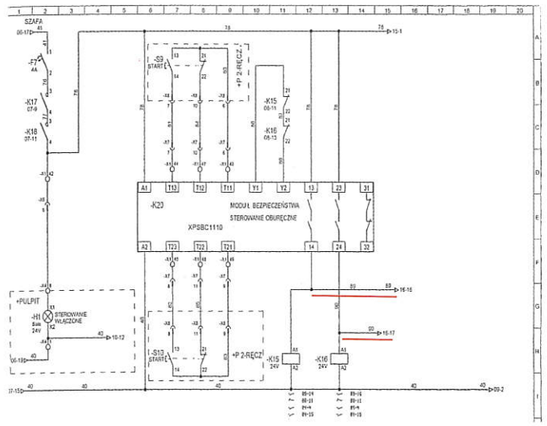
Podsumowując, warto powtórzyć, że od struktury układów sterowania w maszynach bezpośrednio zależy bezpieczeństwo ich obsługi. Od układów sterowania zależy to, jak maszyny się zachowują, jak są odporne na uszkodzenia i jak na nie reagują. Od poprawnego zaprojektowania, zainstalowania i utrzymywania w stanie zdatności układów sterowania zależy także skuteczność technicznych środków bezpieczeństwa, odgradzających (osłon) i nieodgradzających (urządzeń ochronnych).



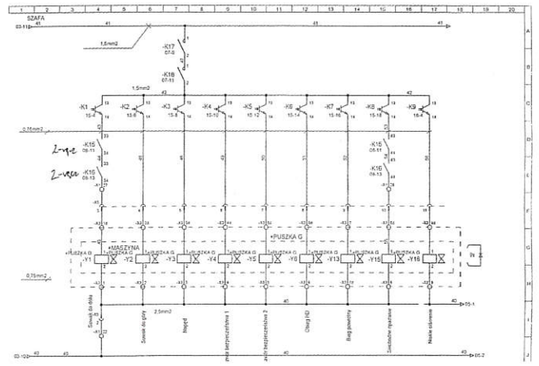
Rys. 1. Przykład niewłaściwego podłączenia osłon do układu sterowania



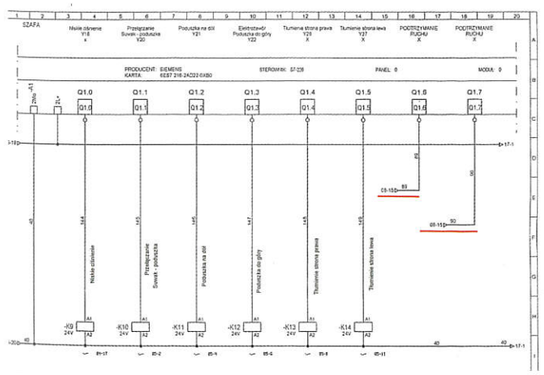
Rys. 2. Prawidłowe podłączenie osłon do układu sterowania



Rys. 3. Układ połączeń na prasie



Rys. 4. Układ połączeń na prasie



Rys. 5. Układ połączeń na prasie