Systemy bezpieczeństwa w automatyce

mgr inż. MARIUSZ GŁOWICKI
specjalista ds. Inżynierii Bezpieczeństwa Maszyn i Procesów
ELOKON Polska Sp. z o.o.

Powiązanie sterowania z bezpieczeństwem w maszynach i urządzeniach wprowadzanych na rynek stanowi częsty problem, z którym nie mogą poradzić sobie projektanci. Z czego najczęściej wynikają błędy projektowe w tej materii? Na co należy zwrócić szczególną uwagę, jeśli chcemy mieć zagwarantowane bezpieczeństwo w rozwiązaniach z zakresu automatyki? Jakie ryzyko wiąże się z wykorzystywaniem przemysłowych sterowników PLC do realizacji funkcji bezpieczeństwa? Jakie mogą być konsekwencje takich rozwiązań? W niniejszym artykule znajdą Państwo odpowiedzi na te i inne pytania dotyczące systemów bezpieczeństwa w automatyce.

Błędy projektowe w zakresie powiązania sterowania z bezpieczeństwem w maszynach i urządzeniach najczęściej są wynikiem nieświadomości, czasem mogą być też skutkiem nieodpowiedzialnych i pozornych oszczędności. Jednak podstawowym problemem dotyczącym sterowania funkcjami bezpieczeństwa maszyn jest niewystarczająca wiedza projektantów dotycząca zasad koncepcyjnych opartych na ocenie ryzyka i brak znajomości wymagań szczegółowych zawartych w normach, jakim podlegają tego typu rozwiązania. Przyczyn takiego stanu rzeczy jest wiele. Za główną można jednak uznać brak zrozumienia potrzeb i problemów, z jakimi muszą się zmierzyć projektanci, producenci i użytkownicy maszyn przez instytucje państwowe, które odpowiadają za kształtowanie bezpieczeństwa maszyn w Polsce, a nigdy nie przeprowadziły i nie prowadzą odpowiednich działań edukacyjnych i informacyjnych w tej dziedzinie. Szkolenia z zakresu bezpieczeństwa maszyn są oferowane tylko przez nieliczne firmy z branży lub przez niektórych producentów podzespołów bezpieczeństwa. Często poziom szkoleń jest niski. Brak jest praktycznych przewodników do oceny ryzyka jako narzędzia przy projektowaniu układów sterowania, a rozwój inżynierii bezpieczeństwa w tej dziedzinie jest wręcz burzliwy.

Brak podstawowej wiedzy w zakresie prawa i norm

Do tej pory, mimo że istnieje od 2006 r., nie została przetłumaczona na język polski podstawowa norma PN-EN ISO 13849-1 dotycząca wymagań bezpieczeństwa układów sterowania. Z początkiem 2012 r. jest ona podstawową normą w tym obszarze zastosowań, ponieważ w pełni zastąpiła normę PN-EN 954-1, która nota bene też nigdy nie została opublikowana po polsku, mimo że jako Polska Norma została opublikowana już w 2001 r. W tych normach zostały sformułowane wymagania bardzo trudne, często niejednoznaczne. Nawet dobra znajomość angielskiego, francuskiego czy niemieckiego (w tych językach norma jest dostępna) nie gwarantuje poprawnego zrozumienia słownictwa, definicji, zakresu i w sumie wymagań, które decydują o zachowaniu się maszyn i tym samym wprost o bezpieczeństwie ludzi je obsługujących. Trudno pojąć, że obszar bezpieczeństwa zawodowego, który jest związany ze zdrowiem, czasami życiem ludzi, jest tak niepoważnie traktowany przez państwo, które tylko wymaga i niewiele wspiera – zarówno producentów, jak i pracodawców jasnymi przepisami, czytelnymi normami, przewodnikami i opracowaniami, które umożliwią spełnienie wymagań im stawianych.

Państwo, które powołało i ma do dyspozycji instytuty naukowo-badawcze, wyższe uczelnie techniczne, studia podyplomowe, wypuszcza na rynek magistrów inżynierów: mechaników, mechatroników, automatyków, elektryków, niewiedzących, że istnieje np. Dyrektywa Maszynowa. Obecnie uczelnie nie mają kontaktu z przemysłem i nie potrafią dostosować się do potrzeb rynku. Obszary bezpieczeństwa technicznego w konstrukcjach maszyn nie są objęte programami kształcenia. To można stwierdzić po braku wiedzy absolwentów czołowych polskich politechnik, których zatrudniamy i z którymi mamy do czynienia w przemyśle. To także problem braku kadry naukowej w tej dziedzinie. W rezultacie młodzi inżynierowie nie znają wymagań stawianych układom sterowania oraz nie są w pełni świadomi swojej odpowiedzialności prawnej w roli projektantów. Dyrektywy Maszynowe – począwszy od 89/392/EWG, potem 98/37/WE i 2006/42 – obowiązują w Europie już od ponad 20 lat (w Polsce od lipca 2002 r.), mimo to absolwenci renomowanych uczelni technicznych rozpoczynają pracę bez elementarnej wiedzy formalnej i technicznej na ten temat.

Wymagania dla układów sterowania funkcjami bezpieczeństwa

Normami dotyczącymi bezpośrednio układów sterowania funkcjami bezpie-

czeństwa są PN-EN 954-1 oraz PN-EN ISO 13849-1 – Maszyny – Bezpieczeństwo – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania. Dla maszyn wyprodukowanych przed dniem 1 lipca 2007 r. obowiązujące są wymagania zawarte w normie PN-EN 954-1. Dla maszyn, które wyprodukowano w okresie od 1 lipca 2007 r. do 31 grudnia 2011 r., akceptowalne jest spełnienie wymagań jednej z powyższych norm (tzw. okres przejściowy). Natomiast dla maszyn, które wyprodukowano od dnia 1 stycznia 2012 r., aktualne są wymagania zawarte w PN-EN ISO 13849-1. Ponadto dla maszyn wyprodukowanych po dniu 29.12.2009 r. istotne jest spełnienie wymagań Dyrektywy Maszynowej 2006/42/WE, w której w załączniku 1 zostały sformułowane ogólne wymagania związane ze sterowaniem.

Norma PN-EN ISO 13849-1 powstała na bazie PN-EN 954-1. Istotną różnicą pomiędzy nimi jest zakres oceny obwodów. W PN-EN 954-1 obwody podlegały analizie jakościowej opisywanej tzw. Kategoriami, czyli architekturą obwodu sterowniczego odpowiedzialnego za realizowanie funkcji bezpieczeństwa.

Z Kategorią (architekturą) mamy również do czynienia w PN-EN ISO 13849-1, ale dodatkowo, oprócz parametrów jakościowych, pojawiły się tam parametry ilościowe dotyczące elementów wykorzystanych w obwodach i niezawodności struktury układu.

Parametrem oceniającym cały obwód bezpieczeństwa i jego odporność na utratę funkcji bezpieczeństwa jest Performance Level (PL), czyli Poziom Zapewniania Bezpieczeństwa. Na PL oprócz Kategorii znanej z PN-EN 954-1, składają się również wspomniane parametry związane z niezawodnością, jakością i zasadami działania wykorzystanych elementów: Mean Time To Dangerous Failure ($MTTF_d$) – Średni Czas do Niebezpiecznego Uszkodzenia, Diagnostic Coverage (DC) – Pokrycie Diagnostyczne i Common Cause Failure (CCF) – Uszkodzenia Spowodowane Wspólną Przyczyną.

Przy projektowaniu maszyn należy dołożyć wszelkich starań, aby sposób obsługi maszyny sam w sobie, jak to tylko możliwe, ograniczał możliwość niebezpiecznego zdarzenia. Ważne jest więc przemyślenie aspektów funkcjonalnych maszyny, staranne opracowanie koncepcji obsługi maszyny, jej uruchamiania, regulacji, konserwacji i wyłączania. Następnie należy zastanowić się nad sposobami zabezpieczeń maszyn. Projekt systemu sterowania funkcjami bezpieczeństwa maszyny powinien rozpocząć się od oceny ryzyka, jakie panuje w danych strefach na maszynie. Jeżeli proces ten został przeprowadzony w sposób prawidłowy, możliwe jest skuteczne zastosowanie zasad konstrukcyjnych obwodów bezpieczeństwa opisanych w normach PN-EN 954-1 i PN-EN ISO 13849-1.

Ocena ryzyka to podstawa

Ocena ryzyka przy projektowaniu maszyny jest istotna, gdyż dzięki niej konstruktor wie, jakie optymalne wymagania powinien postawić obwodom odpowiedzialnym za realizację funkcji bezpieczeństwa. Brak świadomości ryzyka, jakie panuje w wybranych strefach maszyny i jego umiejętnego zestawienia z możliwymi rozwiązaniami, niejednokrotnie przejawia się w sposobach konstrukcji obwodów bezpieczeństwa.

Często spotykanymi przypadkami jest wykorzystywanie czujników technologicznych (np. czujników zbliżeniowych – indukcyjnych) do nadzorowania położenia osłon odpowiedzialnych za ograniczanie dostępu do stref niebezpiecznych. Działanie takich czujników może być bardzo łatwo zakłócone lub nawet świadomie „oszukanie". Innym błędem jest wykorzystanie zwykłych sterowników PLC do realizacji obwodów bezpieczeństwa, przy jednoczesnym niezachowaniu obostrzeń ustalonych w normach dla tego typu aplikacji. Technicznie funkcje te są spełnione, natomiast odporność na utratę funkcji bezpieczeństwa (niezależnie, z jakiego powodu) jest najczęściej niewystarczająca lub nieokreślona. Ważne jest więc, aby przy realizacji obwodów bezpieczeństwa wykorzystywać komponenty przeznaczone do tego celu i podłączać je zgodnie z zaleceniami norm i producentów.

Przy projektowaniu obwodów funkcji bezpieczeństwa istotne jest, by zachowały one swoje właściwości w całym łańcuchu, czyli od elementów wejściowych, przez logiczne, aż po wykonawcze.

Każde słabsze ogniwo powoduje obniżenie odporności całego układu. Należy więc mieć świadomość, że dołożenie czujnika bezpieczeństwa na osłonie ochraniającej strefę niebezpieczną nie jest rozwiązaniem wystarczającym. Czujnik ten w zależności od wymaganej Kategorii lub PL powinien być nadzorowany przez jednostkę logiczną bezpieczeństwa lub odpowiednio zaprojektowany układ logiczny, który wpływa na prawidłowe odłączenie komponentu zasilającego element niebezpieczny na maszynie. Często zdarza się (co potwierdzają analizy przeprowadzane przez naszych ekspertów), że nieświadomy konstruktor, mając dobre intencje, zabezpiecza niebezpieczną strefę poprzez właściwy element bezpieczeństwa, jednak realizacja części logicznej i wykonawczej obwodu jest niezgodna z wymaganiami norm. Taka sytuacja niesie ze sobą duże zagrożenia, ponieważ nieprawidłowe zachowanie elementu bezpieczeństwa może nie zostać wykryte przez system sterowania i w rezultacie doprowadzi to do wypadku. Konieczne jest więc wyraźne oddzielenie obwodów sterowania funkcjami bezpieczeństwa maszyny od obwodów sterowania funkcjami technologicznymi maszyny.

Innym niebezpiecznym aspektem jest zaufanie użytkownika do zainstalowanych zabezpieczeń. Przykładowo operator, widząc kurtynę świetlną zainstalowaną przed strefą narzędziową prasy wyłączającą niebezpieczne ruchy po wtargnięciu w pole ochronne kurtyny, ma wrażenie pełnej ochrony. Jego czujność jest o wiele niższa niż byłaby, gdyby kurtyna nie została tam zainstalowana. W takich przypadkach nieprawidłowe obwody sterowania na odcinku logicznym i wykonawczym niejednokrotnie doprowadziły do ciężkiego wypadku.

Istotną przyczyną wielu problemów jest niestosowanie zasad walidacji dla przeprowadzonych prac. Przed wdrożeniem systemu sterowania w życie należy dokonać sprawdzenia wykonanego układu. Zaleca się, aby proces walidacji był wykonywany przez osoby niezależne, niebiorące udziału w projekcie i wykonaniu obwodów sterowania funkcjami bezpieczeństwa. Zasady walidacji przedstawiono w normie PN-EN ISO 13849-2. Na szczęście ta norma od kilku lat jest przetłumaczona na język polski.

Podsumowując, większość problemów z implementacją funkcji bezpieczeństwa na maszynach wynika z niepełnej znajomości i niedokładnego stosowania wymagań właściwych norm w zakresie realizacji obwodów bezpieczeństwa dla konkretnych maszyn. Istotne jest również zaznajomienie się z oceną ryzyka maszyn, jak i przestrzeganie podstawowych zasad związanych z budową obwodów bezpieczeństwa, a w rezultacie dokonywanie walidacji rozwiązań. Jednak aby dostęp do wiedzy z zakresu bezpieczeństwa maszyn był prostszy i efektywniejszy, konieczne jest wprowadzenie jej do programów nauczania technicznych uczelni wyższych i wymuszenie na instytucjach państwowych rozwoju kultury bezpieczeństwa maszyn.

Na co zwrócić uwagę?

Na co należy zwrócić szczególną uwagę, jeśli chcemy mieć zagwarantowane bezpieczeństwo w rozwiązaniach z zakresu automatyki? Na to pytanie ciężko jest odpowiedzieć kilkoma zdaniami. Automatyka przemysłowa zajmuje się tak wieloma dziedzinami, że nie sposób podać kilku konkretnych i zawsze skutecznych rozwiązań. Dlatego też podstawowym zadaniem projektanta powinno być dokonanie oceny ryzyka dla danej maszyny czy konstrukcji: określenie zagrożeń i skutków, gdy zabezpieczenia będą niewłaściwe, a w konsekwencji dobór takich urządzeń i odpowiednio zaprojektowanego obwodu sterowania, aby nie doszło do wypadku. Oprócz wystrzegania się błędów konstrukcyjnych obwodów sterowania odpowiadających za realizację funkcji bezpieczeństwa, ważne jest zwrócenie uwagi na sposób zachowania się maszyny po wyzwoleniu funkcji bezpieczeństwa lub przy przywracaniu jego funkcjonalności po takim zdarzeniu. Skupmy się tu na trzech pojęciach, które są powiązane praktycznie z każdą maszyną, są to zatrzymywanie bezpieczne, zatrzymywanie awaryjne oraz reset.

Zatrzymywanie bezpieczne, zatrzymanie awaryjne i reset

W normie PN-EN 60204-1 zostały zdefiniowane trzy kategorie funkcji bezpiecznego zatrzymania wraz z wymaganiami ich dotyczącymi:

- kategoria 0, czyli zatrzymanie poprzez bezzwłoczne odłączenie zasilania od napędów maszyny. Jest to zatrzymanie niekontrolowane. Zatrzymywanie niekontrolowane w tej samej normie jest definiowane jako „zatrzymanie poprzez odłączenie napędów maszyny od zasilania, z jednoczesnym uruchomieniem wszystkich hamulców i innych mechanicznych urządzeń zatrzymujących",
- kategoria 1, czyli zatrzymanie kontrolowane przy zasilaniu napędów maszyny aż do jej zatrzymania, a następnie odłączenie zasilania po zatrzymaniu. Zatrzymanie kontrolowane jest w tej samej normie definiowane jako „zatrzymywanie ruchu maszyny za pomocą np. redukcji sygnału sterującego do wartości zerowej, gdy tylko sygnał zatrzymania został rozpoznany przez sterownik, ale z pozostawieniem dopływu energii elektrycznej do elementów napędowych maszyny podczas procesu zatrzymania",
- kategoria 2, czyli zatrzymanie kontrolowane przy pozostawieniu zasilania napędów maszyny.

Zatrzymanie kategorii 0, 1 i/lub 2 należy przewidzieć, jeśli wynika to z oszacowania ryzyka i wymagań funkcjonowania maszyny. Funkcje zatrzymania kategorii 0 i 1 powinny pozostawać w gotowości niezależnie od rodzaju pracy, przy czym zatrzymanie kategorii 0 powinno mieć pierwszeństwo. Oczywiste jest, że funkcje zatrzymania powinny mieć pierwszeństwo przed odpowiednimi funkcjami uruchomienia, a reset funkcji zatrzymania nie powinien powodować jakichkolwiek sytuacji zagrożenia.

Pojęcie zatrzymania awaryjnego zostało zdefiniowane również w normie PN-EN 60204-1 i 13850 i oznacza funkcję przeznaczoną do:

– odwrócenia narastania zagrożenia dla osób i szkód w maszynach lub strat w wykonywanych pracach,

– zainicjowania jednym działaniem człowieka.

Zawarto tam także szczegółowe postanowienia dotyczące tej funkcji bezpieczeństwa:

- Zatrzymanie awaryjne powinno działać jako zatrzymanie kategorii 0 lub 1. W przypadku, gdy funkcję zatrzymania awaryjnego pełni zatrzymanie kategorii 1, powinno być zapewnione ostateczne odłączenie zasilania napędów maszyny za pomocą elementów elektromechanicznych. W przypadku, gdy funkcję zatrzymania awaryjnego pełni zatrzymanie kategorii 0, układ powinien być zmontowany wyłącznie z części elektromechanicznych, a działanie zatrzymania awaryjnego nie powinno zależeć od stanu elektronicznych elementów logicznych (sprzętowych lub programowych). Zatrzymanie awaryjne kategorii 2 nie jest stosowane.
- Zatrzymanie awaryjne powinno jak najszybciej odcinać zasilanie od napędów maszyny powodujących stany zagrożeń. Odcięcie zasilania nie może powodować innych zagrożeń (zatrzymaniem kategorii 1 może być hamowanie przeciwprądem).
- Zatrzymanie awaryjne powinno mieć pierwszeństwo przed innymi funkcjami i działaniami we wszystkich rodzajach pracy, a reset nie powinien powodować ponownego uruchomienia maszyny.

Analiza powyższych trzech wymagań nasuwa wnioski, że funkcja zatrzymania awaryjnego ma za zadanie odcięcie jednym ruchem wszystkich źródeł energii dostarczanych do urządzeń, które mogą spowodować ruch. Ponadto energia zgromadzona w tych urządzeniach powinna zostać rozładowana. Oznacza to, że np. w przypadku napędów pneumatycznych po zadziałaniu funkcji zatrzymania awaryjnego nie może pozostać sprężone powietrze w siłowniku. Należy siłownik doprowadzić do takiego stanu, aby zresetowanie stopu nie powodowało zagrożeń związanych z nieoczekiwanym uruchomieniem. Często spotykanym przypadkiem jest użycie stopu awaryjnego przez operatora, gdy jakiś detal jest nieprawidłowo obrabiany. W przypadku próby uwolnienia detalu spod siłownika zgromadzona energia wyzwala nieoczekiwany ruch, co prowadzi do zmiażdżeń czy utraty palców.

Z wymaganiami dotyczącymi resetowania układów po wyzwoleniu funkcji bezpieczeństwa mamy do czynienia w wielu normach. Aspekty resetowania zależą niekiedy od rodzaju maszyny i jej specyficznych wymagań opisanych w normach szczegółowych. Generalnie możemy wyróżnić dwa rodzaje funkcji resetu: ręczny i automatyczny.

Ręczny reset wymaga oddzielnej akcji od operatora, np. naciśnięcia przycisku, aby przygotować maszynę po zaistniałym sygnale od układów bezpieczeństwa. Ten typ resetu jest podatny na uszkodzenie, np. gdy nastąpi zwarcie – uszkodzenie przewodów lub zatrzaśnięcie przycisku.

Ręczny reset może być zrealizowany w wyższej kategorii, czyli jego stan może być monitorowany przez sterownik bezpieczeństwa lub przekaźnikowy moduł bezpieczeństwa. Taki układ w przeciwieństwie do zwykłego sterownika PLC jest odporniejszy na uszkodzenia oraz sprawdza, czy elementy wykonawcze maszyny odpowiedzialne za stany niebezpieczne są gotowe na to, aby układ mógł bezpiecznie wznowić pracę.

Zaleca się, aby funkcja resetu nie powodowała bezpośredniego uruchomienia maszyny. Reset powinien przygotować maszynę do pracy, jednak uruchomienie cyklu obróbki powinno nastąpić poprzez jego osobne zainicjowanie, np. z przycisku „start cyklu".

Reset automatyczny oznacza, że nie jest wymagane od operatora żadne dodatkowe potwierdzenie o ustaniu niebezpieczeństwa lub skasowania stanu nienormalnego. Ta funkcja jest realizowana przez przekaźnik bezpieczeństwa lub sterownik bezpieczeństwa.

Automatycznego resetu nie można używać, gdy możliwe jest przedostanie się całym ciałem do obszaru niebezpiecznego i pozostanie w nim. Natomiast gdy zabezpieczenia umożliwiają tylko częściową ingerencję w obszar niebezpieczny, np. gdy system bezpieczeństwa wie, że kurtyna świetlna nadzorująca strefę jest wciąż przecięta, wówczas zabrania maszynie wykonać ruchy niebezpieczne i wtedy reset automatyczny może być zastosowany.

Wybór odpowiedniego typu resetu zależy od maszyny, jej stref niebezpiecznych oraz od sposobu ich nadzorowania. W przypadkach, gdy ciężko dokonać wyboru właściwej formy resetowania systemu bezpieczeństwa warto kierować się troską o bezpieczeństwo każdej z osób pracujących z daną maszyną.

Podsumowując, wybór właściwej formy zatrzymania maszyny oraz przywracania jej funkcjonalności, przy jednoczesnym zachowaniu zasad konstrukcji układów bezpieczeństwa, w dużej mierze prowadzi do maksymalnego, przy obecnym stanie wiedzy technicznej, sposobu zabezpieczenia osób pracujących z maszynami.

W celu zwiększenia bezpieczeństwa w rozwiązaniach automatyki przemysłowej należałoby poruszyć szereg innych istotnych aspektów, do których możemy m.in. zaliczyć: bezpieczny wybór trybu pracy (niejednokrotnie traktowany po macoszemu, a często przyczyniający się do zaistnienia sytuacji niebezpiecznych), czasy zatrzymania elementów niebezpiecznych w powiązaniu z prawidłowym doborem odległości bezpieczeństwa urządzeń zabezpieczających, dobór komponentów bezpieczeństwa i ich charakterystyki, funkcje ryglowania i blokowania, konstrukcje osłon stałych i ruchomych.

Uwaga na wykorzystanie PLC do realizacji funkcji bezpieczeństwa

Wykorzystanie przemysłowych sterowników PLC jako jedynych elementów logicznych do realizacji funkcji bezpieczeństwa jest niestety częstym błędem. Niejednokrotnie na maszynach spotyka się sytuację, że przemysłowy sterownik PLC odpowiada za wszystkie obszary sterowania – technologiczne i bezpieczeństwa. Do sterowników podłączane są nie tylko przyciski zatrzymania awaryjnego, ale i inne urządzenia ochronne, takie jak urządzenia oburęcznego sterowania, wyłączniki bezpieczeństwa osłon blokujących, kurtyny świetlne czy skanery laserowe.

Można zadać sobie pytanie, czym różni się zwykły sterownik PLC od sterownika bezpieczeństwa i czy rzeczywiście uzasadnione jest ponoszenie dodatkowych kosztów, skoro sterownik PLC całkiem dobrze poradzi sobie z logiczną stroną realizacji funkcji nie tylko technologicznych, ale i bezpieczeństwa.

Jest w tym dużo prawdy. Przemysłowe sterowniki PLC z reguły pod względem możliwości zastosowań przewyższają sterowniki bezpieczeństwa, dlaczego więc ich nie 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 wewnętrzną strukturę. W przypadku, gdy jeden z kanałów ulegnie uszkodzeniu, drugi kanał musi doprowadzić maszynę do stanu bezpiecznego. Często producenci sterowników bezpieczeństwa stosują zasadę, by w jednym kanale znalazł się inny procesor (oraz jego podzespoły) niż w drugim. Wynika to z chęci uniknięcia ewentualnych błędów wynikających ze wspólnej przyczyny (np. cała seria procesorów ma wadę, która może ujawnić się dopiero w pewnych warunkach).

Aby uniknąć błędów programowania, software jest tak skonstruowany i przebadany przez jednostki notyfikowane, aby uniknąć takich błędów, jak np. zapętlenia programu.

Dodatkową formą zabezpieczenia jest sposób programowania sterowników bezpieczeństwa. Restrykcyjne zasady połączeń bloków funkcyjnych eliminują możliwe błędy przy pisaniu aplikacji. Bloki funkcyjne posiadają ograniczenia podłączeń wewnętrznych, co wpływa na przejrzystość struktury.

Kolejną istotną różnicą jest wymóg dużo wyższej odporności na zakłócenia elektromagnetyczne. W przypadku przemysłowych sterowników PLC zdarzają się bowiem sytuacje, że na wyjściach możliwe jest pojawienie się wysokiego stanu pod wpływem silnych zewnętrznych oddziaływań elektromagnetycznych (często przypadkowych, zazwyczaj niewystępujących w pobliżu miejsca instalacji sterownika PLC). Niespodziewane pojawienie się wysokiego sygnału na wyjściu sterownika PLC może doprowadzić do wysterowania niebezpiecznego dla operatora w danym momencie ruchu.

Ważnym faktem technicznym jest konstrukcja wejść i wyjść w sterowniku bezpieczeństwa. Sposób ich obsługi zapewnia ciągłą dynamiczną kontrolę uszkodzeń i zwarć.

Absolutne wykluczanie przemysłowych sterowników PLC w obwodach bezpieczeństwa nie jest konieczne, jednak należy mieć na uwadze, że większość aspektów realizacji obwodów sterowania funkcji bezpieczeństwa jest zarezerwowana wyłącznie dla sterowników lub przekaźników bezpieczeństwa. Ograniczenia wynikają tutaj m.in. z definicji parametrów kategorii w normie PN-EN ISO 13849-1. Przykładowo norma ta nie dopuszcza możliwości wykorzystania sterownika PLC do realizacji obwodów o architekturze kategorii 1, ze względu na fakt, że sterownik przemysłowy PLC nie jest sprawdzonym elementem bezpieczeństwa.

Sterownik PLC w niektórych aplikacjach, np. obwodach o architekturze kategorii 3 według PN-EN ISO 13849-1, może być wykorzystywany jako element pomocniczy realizujący proste dodatkowe funkcje związane z bezpieczeństwem, np. monitorowanie reakcji maszyny na przełączenie elementów bezpieczeństwa. W przypadku wykrycia błędu sterownik przemysłowy PLC powinien mieć wówczas możliwość przełączenia maszyny w stan bezpieczny bez spowodowana nowych lub dodatkowych zagrożeń.

Podsumowując, stosowanie przemysłowych sterowników PLC do realizacji obwodów bezpieczeństwa niesie ze sobą ryzyko powiązane z ich dużą podatnością na warunki zewnętrzne. W związku z tym nie zaleca się stosowania ich jako jedynych elementów logicznych w obwodach bezpieczeństwa. Mogą one pełnić funkcje wspomagające dla podstawowych komponentów logicznych bezpieczeństwa. Jednak przy takich realizacjach należy pamiętać o najważniejszej zasadzie – ciągłej wyższości wpływania na zachowanie maszyny przez elementy logiczne bezpieczeństwa nad przemysłowymi sterownikami PLC.