Industrial Monitor Interviews Edycja 2013
100 pytań od… przedstawicieli działów technicznych, utrzymania ruchu i produkcji

Autor: Mgr inż. Mariusz Głowicki
Z-ca Dyrektora Działu Bezpieczeństwa Maszyn Elokon Polska Sp. z o. o.
Specjalista ds. Inżynierii Bezpieczeństwa Maszyn i Procesów

(Pytanie 1.) Podobno nie powinno się wykorzystywać przemysłowych sterowników PLC do realizacji funkcji bezpieczeństwa – dlaczego?

Bezpieczeństwo maszyn, jako dziedzina techniki niezwykle skrupulatna, wymaga podejścia systemowego na każdym etapie, m.in. podczas konstrukcji obwodów sterowania odpowiedzialnych za ludzkie zdrowie i życie. Punktem wyjścia do doboru urządzeń realizujących funkcje bezpieczeństwa na maszynie zawsze musi być profesjonalna i rzetelna ocena ryzyka.

Niejednokrotnie pominięcie lub marginalizacja oceny ryzyka na maszynie doprowadziły do wypadku z winy jej systemu sterowania (np. poprzez wysterowanie nieoczekiwanych ruchów w wyniku błędów/uszkodzeń komponentów, w tym właśnie przemysłowych sterowników PLC). Sednem problemu jest tutaj brak dostatecznej świadomości lub wiedzy inżynierów w zakresie kiedy konkretne komponenty mogą być stosowane dla zabezpieczenia ryzyka jakie panuje na maszynie. Sprawa jest nagminna bowiem często dotyczy również renomowanych światowych producentów maszyn, którzy przekonani o swojej nieomylności wystawiają deklarację zgodności WE i znak CE dla maszyny. Kluczem do sukcesu jest posiadanie zespołu właściwie przeprowadzającego ocenę ryzyka oraz ich doświadczenie w pogodzeniu potrzeb technologicznych i bezpieczeństwa przy konstrukcji obwodów sterowania.

Rzetelnie przeprowadzona ocena ryzyka (np. według własnej autorskiej metody), powinna poza zidentyfikowaniem zagrożeń i nadaniem im odpowiadającej wartości ryzyka jednocześnie narzucić wymagania na układy sterowania – niezbędne jeżeli później zdecydowano by się na redukcję ryzyka przy wykorzystaniu komponentów włączanych w układ sterowania maszyny. Ocena ryzyka wiąże się z określeniem wymaganych poziomów *Performance Level* wg normy *PN-EN ISO 13849-1* dla funkcji bezpieczeństwa. Pośród szeregu wymagań dla maszyn okazuje się, że nadal poprawne są odwołania do już nieaktualnej normy *PN-EN 954-1* operującej parametrem *Kategorii*.

W zależności od aplikacji i rezultatów procesu oceny ryzyka, a ostatecznie wyznaczonych na podstawie nich wymaganych parametrów *Performance Level* (na jednym z pięciu poziomów a, b, c, d lub e) lub *Kategorii* (na jednym z pięciu poziomów B, 1, 2, 3 lub 4) zastosowanie przemysłowych sterowników PLC może być możliwe. Wiąże się to natomiast już ze szczególnymi oczekiwaniami stawianymi powyższym parametrom na wybranych poziomach. Czasami, np. w przypadku wybranych aplikacji Kategorii 2 wg PN-EN 954-1 czy PN-EN ISO 13849-1 zastosowanie takiego sterownika może być wręcz konieczne (jako jednostki testującej), a w innych, np. większości aplikacji Kategorii 1 wg PN-EN 954-1 czy PN-EN ISO 13849-1 niedopuszczalne.

(Pytanie 2.) Od czego uzależnić wybór metody oceny ryzyka zawodowego – która metoda jest najlepsza?

Zgodnie z definicją, ryzyko to kombinacja prawdopodobieństwa wystąpienia szkody oraz jej ciężkości. W celu zapanowania nad nim przeprowadza się proces jego oceny, w którym na podstawie analizy przy uwzględnieniu takich czynników jak socjalne, ekonomiczne oraz aspekty środowiskowe, zostaje wydane orzeczenie o akceptacji określonego ryzyka. Powyższe hasła są na tyle złożone, że same wymagają odrębnych artykułów.

Przed przystąpieniem do wyboru konkretnej metody oceny ryzyka warto zwrócić uwagę na istotny problem towarzyszący zrozumieniu samego procesu. Bardzo często dobór metody oceny jest mylony z metodą szacowania bądź ewaluacji ryzyka. W celu rozwiania wątpliwości, warto sięgnąć do normy PN-EN ISO 12100 charakteryzującej te zagadnienia.

Mówiąc o metodzie oceny ryzyka, najczęściej mamy na myśli jej fragment czyli sposób analizy ryzyka. Metod jest wiele, natomiast wybór najlepszej powinien być uzależniony od szeregu czynników, m.in. zakresu analizy, stopnia jej szczegółowości, charakteru wyników które chce się osiągnąć, adekwatność względem obiektu z uwagi chociażby na jego wielkość i typ, czy fazę życia. Te kroki pozwolą na wybór z grupy metod ilościowych lub jakościowych.

Duże obiekty przemysłowe wymagają metod oceny globalnej, dających najczęściej wyniki o charakterze jakościowym np. HAZOP, FMEA, CCA, listy kontrolne. Dla poszczególnych fragmentów instalacji czy urządzeń technicznych bardziej odpowiednie są ilościowe metody oparte na strukturach drzewiastych pozwalające w sposób liczbowy określić wartość ryzyka.

W analizie ryzyka na stanowiskach pracy, przy maszynach powinno się stosować metody ilościowe podczas projektowania i budowy stanowisk pracy. Dla maszyn już używanych jako najbardziej adekwatne do tego typu obiektów ze względu na charakter zagrożeń są metody mieszane, zwłaszcza grafy ryzyka. Analiza ryzyka w oparciu o metody drzewiaste lub stosujące metodologię MORT uzupełnione o modelowanie zachowania człowieka lub oceny niezawodności ludzkiej są najbardziej odpowiednie dla stanowisk pracy. Dla szybkiego oszacowania ryzyka mogą być tu zastosowane metody kalkulatora ryzyka, różne metody wskaźnikowe lub listy kontrolne.

Analiza ryzyka prowadzona w uporządkowany sposób zgodnie z wymaganiami norm europejskich stanowi punkt wyjścia do oceny i podejmowania decyzji o przyjęciu lub odrzuceniu ryzyka, czyli do ewaluacji ryzyka. W jej trakcie zapada decyzja o akceptacji, bądź dyskwalifikacji stanu bezpieczeństwa w środowisku pracy.

Każda z metod ma pewne zalety i wady. Niestety wśród nich nie ma takiej, która dotyczy wszystkich maszyn podlegających dyrektywie 2006/42/WE (wymagania zasadnicze) czy dyrektywie 2009/104/WE (wymagania minimalne). Praktycznie najlepiej wybrać taką, która swoim zakresem umożliwi objęcie jak największej ilości dzięki możliwości doboru odpowiednich wskaźników dla określonych grup maszyn. To oczywiście wymaga doświadczenia, bowiem źle ustalone wartości mogą poprzez niepoprawnym dobór zabezpieczeń skutkować zdarzeniami zagrażającymi ludziom. W razie

konieczności, zawsze można szukać wsparcia wśród firm mających takie doświadczenie i biorących odpowiedzialność za zastosowane metody i wykonane analizy ryzyka.

(Pytanie 3.) Co to jest bezpieczeństwo funkcjonalne systemów sterowania dla maszyn i jakie normy regulują tę kwestię?

Dobrze przeprowadzony proces oceny ryzyka w pewnym momencie stawia przed jego wykonawcą zakres wymagań co do niezawodności, jakim musi podołać część układu sterowania odpowiedzialna za bezpieczeństwo na maszynie. Czasami takie wymagania wynikają w prosty sposób z norm typu C dla maszyn.

Specyfikację, co do konstrukcji i potwierdzenia wydajności obwodów sterownia odpowiedzialnych za bezpieczeństwo określają obecnie dwie normy (obie zharmonizowane z dyrektywą 2006/42/WE): PN-EN ISO 13849-1, operującą parametrem niezawodności *Performance Level (PL)* , oraz PN-EN 62061, gdzie tą rolę pełni *Safety Integrity Level (SIL)*, czyli poziom nienaruszalności bezpieczeństwa. Decyzja, która z norm zostanie wybrana powinna być uzależniona od możliwości aplikacji, ale i wiedzy konstruktora.

Norma PN-EN 62061 jest tzw. normą sektorową dla normy PN-EN 61508 poruszającej w szerokim zakresie zagadnienie *bezpieczeństwa funkcjonalnego*. PN-EN 62061 dotyczy wyłącznie specyfiki sektora maszynowego. Ma ułatwiać określanie niezawodności działania systemów elektrycznego sterowania związanych z bezpieczeństwem w odniesieniu do znaczących zagrożeń generowanych przez maszyny. Dzięki temu może być stosowana wymiennie (z pewnymi ograniczeniami dla różnych technologii sterowania) z normą PN-EN ISO 13849-1, nie mówiącą wprost o bezpieczeństwie funkcjonalnym.

Próbując w jak najbardziej przystępny sposób zdefiniować *bezpieczeństwo funkcjonalne* należy powiedzieć, że jest to część całkowitego bezpieczeństwa maszyny i jej systemu sterowania, która zależy od poprawnego działania elementów tegoż systemu sterowania wykonanych wyłączenie w technice elektrycznej. Uszkodzenie tych elementów może doprowadzić do bezpośredniego wzrostu ryzyka na maszynie.

Ponieważ norma PN-EN 61508, a tym bardziej PN-EN 62061 rozpatruje obwody bezpieczeństwa wykonane wyłączenie w technice elektrycznej nie może ona w pełni zapanować nad bezpieczeństwem maszynowym. Wszędzie tam, gdzie w obwodach bezpieczeństwa konieczne jest wykorzystanie elementów nieelektrycznych – np. zaworów pneumatycznych w celu zatrzymania określonych siłowników, konieczne jest stosowanie normy PN-EN ISO 13849-1. Obie normy umożliwiają wzajemne – wymienne stosowanie, ale niestety każda z nich przedstawia odrębną metodę oceny ryzyka. Często doprowadza to do ustalania różnych wymagań dla obwód bezpieczeństwa. Jak wskazuje praktyka, aby świadomie zapanować nad tą sytuacją, najlepszym krokiem jest stosowanie jednej spójnej metody oceny ryzyka (np. opracowanej na własne potrzeby).

(Pytanie 4.) Zatrzymanie bezpieczne, zatrzymanie awaryjne i reset – jakie wymagania techniczne zgodnie z obowiązującymi normami powinny być spełnione aby można było zagwarantować bezpieczeństwo w każdej z ww. sytuacji? Jakie normy regulują tę kwestię?

Pojęcie zatrzymania i resetowania pojawia się w kilku istotnych dokumentach związanych z bezpieczeństwem maszyn. Ogólnie rzecz ujmując można te terminy sklasyfikować jako funkcje bezpieczeństwa realizowane przez układ sterowania maszyny. W konsekwencji dobór parametrów dla obwodów sterowania, a przez to określenie wymagań technicznych dla sprzętu je realizującego powinien być poprzedzony rzetelną oceną ryzyka przeprowadzoną na maszynie.

W przypadku nowych maszyn pierwszych informacji na temat obu funkcji należy naturalnie poszukiwać w dyrektywie 2006/42/WE. Klasyfikuje ona rodzaje zatrzymania na normalne, eksploatacyjne i awaryjne. Niestety nie napotkamy w niej wymagań co do resetowania po konkretnym zatrzymaniu. W tym celu należy odwołać się do norm zharmonizowanych z dyrektywą, m.in. PN-EN 60204-1, PN-EN ISO 13849-1 oraz PN-EN ISO 13850, gdzie w spójny sposób opisuje się konieczność resetowania po określonym zatrzymaniu.

Mówiąc o zatrzymaniu bezpiecznym musimy myśleć o zatrzymaniu normalnym i eksploatacyjnym. Zgodnie z wspomnianymi powyżej dokumentami, reset nie jest wymagany – jeżeli oczywiście nie wynika to oceny ryzyka lub najczęściej ze sposobu realizacji technologicznego systemu sterowania maszyny. Po takim zatrzymaniu ponowny rozruch (restart) maszyny jest możliwy przez element przeznaczony do uruchamiania. W przypadku funkcji zatrzymywania awaryjnego (ale w większości przypadków również w wyniku zatrzymania wyzwolonego przez inne urządzenia ochronne na maszynie – np. osłony blokujące), zawsze konieczne jest ręczne zresetowanie systemu sterowania przez element przeznaczony do tego celu (tzw. reset manualny), przed ponownym rozruchem systemu. Należy zwrócić szczególną uwagę, że reset manualny nie może bezpośrednio powodować uruchomienia.

Gwarancją bezpieczeństwa dla określonych form zatrzymania, a jednocześnie spisem wymagań technicznych dla ich realizacji są dwa kluczowe parametry. Pierwszy z nich to *„Kategorie Zatrzymania”* (0,1 lub 2), a drugi to *„Kategorie”* lub *„Performance Level”* dla funkcji sterowania odpowiedzialnej za bezpieczeństwo. Oba te parametry powinny być dobrane poprawnie na podstawie oceny ryzyka dla określonej aplikacji. Co ważne - drugi z nich powinien być określony i zrealizowany również dla funkcji resetu manualnego.

Mówiąc o aspektach zatrzymania i resetowania na maszynach starych, warto spojrzeć do zapisów dyrektywy 2009/104/WE. Podobnie jak w przypadku nowych maszyn, konieczne będzie tutaj jednak wsparcie się normami, jako źródłem sprawdzonej wiedzy technicznej. Ostatecznie z punktu widzenia praktyki dla maszyn strych zaleca się dochowanie zapisów norm PN-EN 60204-1, PN-EN 954-1 (poprzedniczka PN-EN ISO 13849-1) czy PN-EN ISO 13850 (następczyni PN-EN 418) przedstawionych w poprzednim akapicie.

(Pytanie 5.) Jakie normy szczegółowe w zakresie bezpieczeństwa maszyn regulują wymagania odnośnie umiejscowienia i działania elementów sterowniczych a jakie wymagania dotyczące sygnałów wizualnych, akustycznych i dotykowych? Jakie to wymagania?

W zakresie wymagań dotyczących umiejscawiania i działania elementów sterowniczych pewne zapisy spotkamy już w samych dyrektywach 2006/42/WE i 2009/104/WE oraz normie PN-EN ISO 12100. Mówiąc najogólniej o usytuowaniu każdy z elementów sterowniczych powinien m.in. być umiejscowiony w sposób zapewniający bezpieczną obsługę, poza strefami niebezpiecznymi oraz tak aby jego obsługa nie powodowała dodatkowego zagrożenia. W zakresie działania warto zwrócić uwagę na zapisy o kierunkowości działania zgodnej z zamierzonym skutkiem, czy o uwzględnieniu zasad ergonomii przy ich operowaniu. Oczywiście od każdej z tych zasad istnieją pewne odstępstwa, które najlepiej omawiać na określonym przypadku, przy ocenianiu maszyny.

Pośród innych norm poruszających kwestię rozmieszczenia elementów sterowniczych przede wszystkim warto odwołać się do normy PN-EN 60204-1. Poruszono tam aspekty związane z ich umiejscowieniem, kolorystyką, oznakowaniem i zasadami działania. Dla integrowanych systemów produkcyjnych, ciekawe zapisy możemy spotkać w normie PN-EN ISO 11161. W przypadku wybranych typów maszyn, np. maszyny pakujące (seria norm PN-EN 415) warto odwoływać się do norm szczegółowych typu C, gdzie znajdziemy informacje o konieczności i zasadach stosowania wybranych elementów sterowniczych.

O konieczności sygnalizacji różnych zdarzeń i stanów na maszynie, przede wszystkim mówią obie dyrektywy i norma PN-EN ISO 12100. Stosowanie takich sygnałów zaleca się chociażby gdy z określonych przyczyn wyeliminowanie pewnych sytuacji niebezpiecznych na maszynie jest niemożliwe. Kluczową normą szczegółową w zakresie sygnałów wizualnych, akustycznych i dotykowych jest seria norm PN-EN 61310. Znajdziemy tam liczne wskazówki, co do sposobów dobierania typów sygnałów i ich symboliki dla określonych zagrożeń czy funkcji.

Przykładowo, dla sygnałów wizualnych barwa żółta powinna być używana w celu ostrzegania przed zagrożeniami dla ludzi lub stanami nienormalnymi na maszynie. W zakresie sygnałów dotykowych napotkamy tam znormalizowane kształty dla elementów sterowniczych mogących służyć do uruchamiana określonych funkcji maszyny. W przypadku sygnałów dźwiękowych warto również sięgnąć do normy PN-EN ISO 7731, gdzie wymagania im stawiane zostały pogłębione.

ELOKON Polska Sp. z o.o.
Tytoniowa 22
04-228 Warszawa

Tel (+48 22) 812 71 38
Fax (+48 22) 613 36 32

elokon@elokon.pl
www.elokon.pl

Bank Zachodni WBK S.A.
23 Oddział Warszawa
50 1090 1030 0000 0001 2244 0365

NIP 5270202006
REGON 010088180
KRS 0000145346
Sąd Rejonowy dla m.st. W-wy w Warszawie
XX Wydział Gospodarczy
Kapitał Zakładowy 100.000 PLN