Analiza ryzyka kombajnu (ścianowego lub chodnikowego) dla określenia poziomu nienaruszalności bezpieczeństwa SIL. Zagadnienia wybrane

Józef Chmiel

Streszczenie: Artykuł przedstawia analizę ryzyka kombajnu i dotyczy maszyny górniczej do drążenia wyrobisk górniczych w skale płonnej lub pokładach węgla, rudy. Omówiono wybrane zagadnienia związane z analizą ryzyka dla określenia poziomu nienaruszalności bezpieczeństwa SIL elementów systemu sterowania kombajnu związanych z bezpieczeństwem.

Słowa kluczowe: analiza ryzyka, SIL, funkcja bezpieczeństwa, Dyrektywa Maszynowa 2006/42/WE

Abstract: *Risk analysis combine selected issues – applies to the mining machine for digging excavations gangue or seams of coal, ore. The selected issues related to risk analysis for the determination of safety integrity level SIL combine elements of the control system of safety-related.*

Keywords: risk analysis, SIL safety integrity level, Machine Directive 2006/42/WE

Wstęp

Wymagania bezpieczeństwa zasadnicze dla maszyn po raz pierwszy wprowadzanych do obrotu określa Dyrektywa Maszynowa 2006/42/WE. Zharmonizowane z nią standardy PN-EN ISO 13849-1 i 2, PN-EN 62061 oraz niezharmonizowany standard PN-EN 61508 – 1–7, pozwalają stosować konkretne rozwiązania techniczne.

Ogólne zasady projektowania oraz ocenę ryzyka i zmniejszanie ryzyka można znaleźć w normie PN-EN ISO 121OO-1:2012 Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka. Powołują się na te standardy autorzy wielu publikacji, omawiający bezpieczeństwo funkcjonalne [1, 2].

Już w zasadach ogólnych dyrektywa maszynowa podaje, że producent maszyny lub jego upoważniony przedstawiciel musi zapewnić przeprowadzenie oceny ryzyka w celu określenia wymagań w zakresie ochrony zdrowia i bezpieczeństwa, które mają zastosowanie do maszyny; zatem maszyna musi być zaprojektowana i wykonana z uwzględnieniem wyników oceny ryzyka.

Przy analizie zagrożeń i ryzyka należy wziąć pod uwagę wszystkie rodzaje zagrożeń, jakie mogą wystąpić z powodu:

- oddziaływania środowiska – wpływy czynników mechanicznych, elektromagnetycznych, chemicznych, termicznych i ewentualnych innych, jakie niesie środowisko, w omawianym przypadku występowanie metanu, pyłu węglowego, tąpań;
- odchyleń w przebiegu procesu produkcyjnego np. niespodziewana zwyżka prędkości obrotowej silnika napędowego, nieoczekiwana zwyżka ciśnienia w instalacji, powstanie nieszczelności w instalacji.

System związany z bezpieczeństwem powinien zapewnić poziom ryzyka tolerowanego przy działaniu wszystkich zidentyfikowanych zagrożeń.

Wprowadzenie do zagadnień wybranych

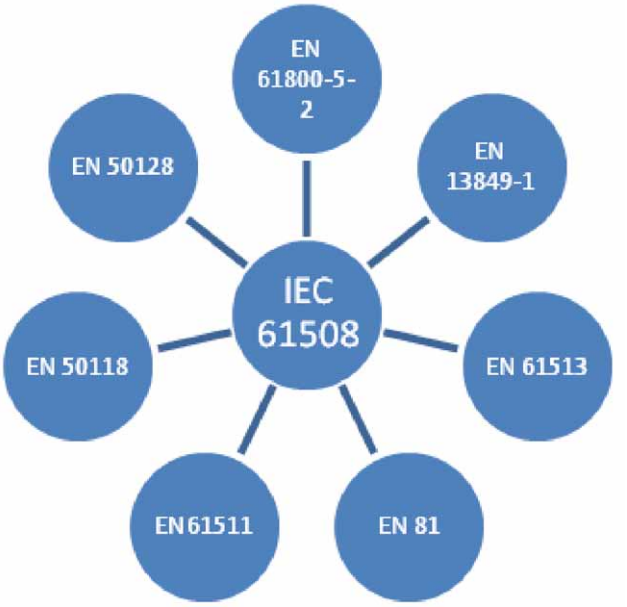
W niniejszym opracowaniu zajmujemy się przede wszystkim systemami E/E/PES, które są stosowane do wypełniania funkcji bezpieczeństwa w maszynach górniczych, jakimi są kombajny ścianowe i chodnikowe, dla spełnienia zadania ograniczenia ryzyka awarii w sytuacji krytycznej.

Bezpieczeństwo wg przewodnika ISO/IEC Guide 51 zdefiniowano jako brak nieakceptowanego ryzyka. Ryzyko jest kombinacją prawdopodobieństwa pojawienia się szkody i dotkliwości tej szkody.

Pojęcie bezpieczeństwa funkcjonalnego zostało wprowadzone przez serię norm IEC 61508, która otrzymała status normy podstawowej w zakresie części systemu związanej z bezpieczeństwem, w której wykorzystano do wypełniania funkcji bezpieczeństwa systemy elektryczne, elektroniczne, elektroniki programowalnej. Nie jest zharmonizowaną normą europejską, nie istnieje domniemanie zgodności z żadną dyrektywą, ale wykonana ocena systemu E/E/EP wg tej normy jest akceptowana – spełnienie wymagań tej normy zapewnia bezpieczeństwo. Do tej normy odwołują się wszyscy inżynierowie projektanci i praktycy. Ona jest ogólna nie tylko dla maszyn. Poniżej na diagramie przedstawiono niektóre związki pomiędzy poszczególnymi normami.

O pewnym systemie możemy mówić, że jest bezpieczny wtedy, gdy błędy przypadkowe, systematyczne i błędy o wspólnej przyczynie są wykryte i usunięte. Eliminacja tych błędów ma przede wszystkim zabezpieczyć ludzi przed narażeniami, uszkodzeniami, ma ochraniać środowisko. W technice zabezpieczeń mówi się o tym, żeby maszyna nie została wyłączona z eksploatacji, czyli względy ekonomiczne też są ważne.

Czym jest bezpieczeństwo funkcjonalne? Udzielając odpowiedzi na to pytanie, posłużymy się definicją z PN-EN 61508 część 4, gdzie podano, że:



Bezpieczeństwo funkcjonalne – część bezpieczeństwa całkowitego odnosząca się do wyposażenia sterowanego EUC i systemu sterowania EUC, która zależy od prawidłowego działania systemów E/E/PE związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innych technikach (mechanicznych, pneumatycznych) i zewnętrznych środków do zmniejszania ryzyka.

Związanymi definicjami są pojęcia:

- Nienaruszalność bezpieczeństwa – prawdopodobieństwo, że system związany z bezpieczeństwem wykona w sposób zadowalający wymagane funkcje bezpieczeństwa, we wszystkich określonych warunkach i w określonym przedziale czasu.
- Poziom nienaruszalności bezpieczeństwa SIL – poziom dyskretny (jeden z czterech możliwych) do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które powinny być przypisane w systemach E/E/PE związanych z bezpieczeństwem, przy czym poziom nienaruszalności bezpieczeństwa 4 jest poziomem najwyższym, a poziom nienaruszalności bezpieczeństwa 1 jest poziomem najniższym. Dla maszyn mamy tylko trzy poziomy nienaruszalności bezpieczeństwa.
- Poziom (niezawodności) zapewnienia bezpieczeństwa – PL (ang. *Performance Level*), oznaczany literami od *a* (najniższy) do *e* (najwyższy)
- Funkcja bezpieczeństwa – funkcja maszyny, której uszkodzenie może skutkować natychmiastowym wzrostem ryzyka.

Przywołane definicje dla wielu projektantów maszyn stanowiły istotny problem do rozwiązania, wg jakiej normy ocenić układ elektrycznego sterowania kombajnu ścianowego czy chodnikowego? Czy cały układ sterowania kombajnów powinien posiadać przypisany poziom SIL lub PL, a może obydwa? Pytania te rodziły się z braku zrozumienia norm już przywołanych we wstępie niniejszego opracowania, a przede wszystkim 1 części PN-EN 61508.

To niezrozumienie również było spotykane u przedstawicieli Jednostek Notyfikowanych, którzy prowadzili szkolenia w zakresie bezpieczeństwa funkcjonalnego.

Określenie poziomu nienaruszalności bezpieczeństwa układu elektrycznego

Producent maszyny (układu sterowania maszyny) powinien udokumentować poziom nienaruszalności bezpieczeństwa. Wiele SIWZ (przyszłych użytkowników tych maszyn) wymagało, aby kombajny ścianowe/chodnikowe posiadały poziom nienaruszalności bezpieczeństwa SIL 3. W praktyce okazało się to niemożliwe do osiągnięcia!

Każdy cykl życia maszyny powinien być określony i udokumentowany, aby był łatwy do odtworzenia. Wymaganie to również dotyczy udokumentowania przez producenta kombajnu (układu jego sterowania) poziomu nienaruszalności bezpieczeństwa. W tym celu producent powinien:

- przeprowadzić analizę ryzyka, analizę niezawodności układu w celu określenia pokrycia diagnostycznego DC, który jest określany z poniższej zależności:
  DC = ilość uszkodzeń niebezpiecznych wykrytych/ilości wszystkich uszkodzeń niebezpiecznych;
- obliczyć współczynnik SFF, który jest określany z niżej podanej zależności:
  SFF = ilość wszystkich uszkodzeń bezpiecznych i rozpoznanych niebezpiecznych/ilości wszystkich uszkodzeń;
- określić współczynnik β, który jest określany z niżej podanej zależności:
  β = udział uszkodzeń niebezpiecznych wykrytych (o wspólnej przyczynie)/wszystkich uszkodzeń niebezpiecznych;
- określić intensywność uszkodzeń na godzinę λ(t), w FITACH (FIT = 1E-09);
- określić czas bezawaryjnej pracy czujnika, systemu logicznego, systemu wykonawczego, całego elektrycznego układu sterowania maszyny;
- z otrzymanego czasu bezawaryjnej pracy systemu przyporządkować SIL w zależności od częstości przywołania (np. wg PN-EN 61508-6 przy braku norm sektorowych, wg PN-EN ISO 13849-1 dla niezłożonych podsystemów, wg PN-EN 62061 dla maszyn z systemami programowalnymi).

Postępowanie zgodne z którąkolwiek z norm (bezpieczeństwa funkcjonalnego) powinno prowadzić do bardzo podobnego rezultatu i wynikowe poziomy nienaruszalności bezpieczeństwa (*Safety Integrity Level* – SIL) i poziomy zapewnienia bezpieczeństwa (*Performance Level* – PL) są porównywalne (tabela 1 poniżej).

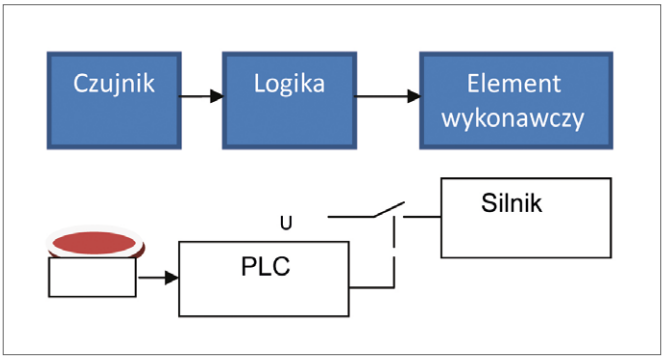
Tabela 1. Porównanie wartości SIL i PL [ISO 13849-1:2006(E)]

SIL	PL
brak odpowiednika	a
SIL 1	b
SIL 2	c
SIL 3	d
SIL 4	e

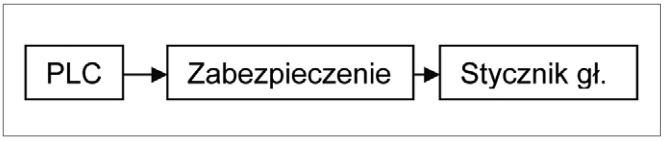
Typowy schemat układu sterowania maszyny

Przykładowy prosty układ, który zazwyczaj w maszynie występuje, składa się z czujnika, połączeń z elementem logiki i wykonawczym. Poniżej przedstawiono go na rysunku 1.

Taki schemat obejmuje cały zakres bezpieczeństwa funkcjonalnego dla wszystkich urządzeń (tj. kompletny system bez-



Rys. 1. Schemat układu sterowania maszyny



Rys. 2. Schemat poglądowy obwodu zabezpieczeń

pieczeństwa: sensor – sterowanie – człon wykonawczy). Dla zrozumienia i mówienia o bezpieczeństwie całkowitym, należy widzieć całość takiego systemu.

Analiza ryzyka

Obejmuje określenie ograniczeń dla kombajnu, identyfikację zagrożeń występujących oraz oszacowanie ryzyka.

Rozpatruje się problem uzyskania wystarczającego zmniejszenia ryzyka wynikającego z pracy kombajnu, jak i zastosowanych układów logicznych w układach sterowania kombajnu.

Układami logicznymi zapewniającymi funkcje bezpieczeństwa są:

- układy logiczne dla oburęcznych urządzeń sterujących;
- sterowniki bezpieczeństwa PLC;
- elementy przeznaczone do przetwarzania związanych z bezpieczeństwem sygnałów systemów magistrali SafetyBus.

Kombajn ścianowy/chodnikowy jest źródłem zagrożeń wynikających z jego ruchów roboczych (przy pracy normalnej może przejeżdżać w dwóch przeciwnych kierunkach, urabiając i transportując urabiany urobek). Każde nieprawidłowe wykonanie dowolnej czynności może wywołać sytuację zagrażającą dla operatora, jak i innych współpracowników. Błędy (uszkodzenie lub nieprawidłowe działanie) w układach logicznych, np. magistrali SafetyBus, zagrażają bezpieczeństwu zatrudnionych osób.

Elementy bezpieczeństwa – analizują co najmniej jeden sygnał wejściowy i generują, według ustalonego algorytmu, co najmniej jeden sygnał wyjściowy oraz są przeznaczone do działania w połączeniu z układem sterowania maszyny lub jego części w celu wykonania co najmniej jednej funkcji bezpieczeństwa.

Wymagania bezpieczeństwa

Nienaruszalność bezpieczeństwa dotyczy systemów E/E/PE związanych z bezpieczeństwem, a odpowiada koniecznemu zmniejszaniu ryzyka.

Przyjęto wyrażanie poziomu wymagań bezpieczeństwa w kategoriach:

- zapewnianych funkcji bezpieczeństwa,
- nienaruszalności bezpieczeństwa tych funkcji.

Funkcjami bezpieczeństwa są:

- wszystkie funkcje związane z realizacją ruchu kombajnu, ochrona obsługi (personelu obsługującego lub współpracującego); elementy przeznaczone do przetwarzania związanych z bezpieczeństwem sygnałów magistrali SafetyBus.

Poziom nienaruszalności bezpieczeństwa (SIL) jest zdefiniowany w przypadku kombajnu (rodzaj pracy ciągły), intensywność uszkodzeń na godzinę według tablicy 2 [3].

Tabela 2. Poziomy nienaruszalności bezpieczeństwa: docelowe miary uszkodzeń funkcji bezpieczeństwa działających w rodzaju pracy na częste przywołanie lub ciągłym

Poziom nienaruszalności bezpieczeństwa (SIL)	Rodzaj pracy na częste przywołanie lub ciągły (Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę (PF H))
4	od $\geq 10^{-9}$ do$< 10^{-8}$
3	od $\geq 10^{-8}$ do$< 10^{-7}$
2	od $\geq 10^{-7}$ do$< 10^{-6}$
1	od $\geq 10^{-6}$ do$< 10^{-5}$

Określenie poziomu nienaruszalności bezpieczeństwa oraz kategorii

W analizie rodzaju i skutków uszkodzeń FMEA [4]określono poziomy nienaruszalności bezpieczeństwa układów logicznych zapewniających funkcje bezpieczeństwa, wybrano np. tor wyłączenia awaryjnego związanego z zadziałaniem zabezpieczeń. Poszczególne elementy wyposażenia elektrycznego posiadają określone wartości $PFH_D(\lambda_D)$. Poglądowy schemat z rys. 2 przedstawia sposób realizacji wyłączenia awaryjnego po zadziałaniu zabezpieczeń. Przyjęto częstotliwość przywołania funkcji 6 razy na godzinę (najgorszy przypadek, gdy zadziała zabezpieczenie o najwyższym poziomie uszkodzeń na godzinę).

Składniki obwodu: zabezpieczenie z poziomem uszkodzeń niebezpiecznych na godzinę $PFH_{D1} = 8{,}5 \cdot 10^{-7}$, DC = 60%, stycznik (pomocniczy i główny) o $PFH_{D2} = 5{,}1 \cdot 10^{-8}$, DC = 90%, $PFH_{D3} = 5 \cdot 10^{-7}$, DC = 90%.

Poziom uszkodzeń niebezpiecznych na godzinę dla całego obwodu wyznaczono z zależności:

$$PFH_D = PFH_{D1} + PFH_{D2} + PFH_{D3} =$$
$$= 8{,}5 \cdot 10^{-7} + 5{,}1 \cdot 10^{-8} + 5 \cdot 10^{-7} = 14 \cdot 10^{-7}$$

Dla minimalnego SFF = 67,6% (tablica 6 normy [5]), poziom nienaruszalności bezpieczeństwa nie może być wyższy niż SIL 1. Wymagana kategoria 2 podana w tabeli 1 wg normy typu C [6], dla elementów elektrycznych/elektonicznych została zachowana. Zastosowane układy są standardowo jednokanałowe. Posiadają funkcje diagnostyczne (samotestujące). Do funkcji diagnostycznych zastosowano dodatkowo sterownik PLC, do którego doprowadzone są informacje o stanie styków wyjściowych (o wymuszonym prowadzeniu) poszczególnych komponentów składowych systemu.

Wnioski

Decyzja o zastosowaniu funkcji bezpieczeństwa powinna być podjęta przez zespół projektantów aplikacji na podstawie wyników analizy ryzyka, jakie może wystąpić w danej aplikacji (maszynie). Projektant decyduje następnie o wyborze właściwego poziomu zapewnienia bezpieczeństwa i realizuje zakładany SIL lub PL za pomocą określonych komponentów lub za pomocą dodatkowych środków.

Analiza ryzyka dostarcza informacji do oceny ryzyka, która z kolei pozwala na osądzenie, czy zmniejszenie ryzyka jest wymagane czy też nie. To osądzenie będzie poparte przez jakościowe lub – gdzie to ma zastosowanie – ilościowe oszacowanie ryzyka związanego z zagrożeniami obecnymi na kombajnach.

Układu sterowania kombajnu jako całości nie uznaje się za układ logiczny.

Powierzenie zadania analizy bezpieczeństwa osobom nieposiadającym odpowiednio szerokiego doświadczenia w ocenie ryzyka i określenia zagrożeń oraz stosowania właściwych środków ochronnych nie jest wskazane.

Producenci kombajnów powinni wybrać, którą z norm reprezentujących dwa systemy bezpieczeństwa zastosować (PN-EN ISO 13849-1 czy PN-EN 62061). Dla zapewnienia spójności prowadzonej analizy słuszne wydaje się stanowisko zalecające kierowanie się tą samą, wybraną normą od początku do końca procesu projektowania i produkcji.

Literatura

[1] Missala T.: *Bezpieczeństwo funkcjonalne – awers i rewers.* „Pomiary – Automatyka – Robotyka" 1/2008.

[2] Trajdos M.: *Wprowadzenie do projektowania bezpiecznych systemów sterowania maszyn.* Partner Serwis Sp. z o.o. – Elbląg.

[3] PN-EN 61508 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych systemów związanych z bezpieczeństwem – Część 1–7.

[4] PN-EN 60812 Techniki analizy nieuszkadzalności systemów. Procedura analizy rodzajów i skutków uszkodzeń (FMEA).

[5] PN-EN 62061 Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.

[6] PN-EN 12111 Maszyny do drążenia tuneli. Kombajny chodnikowe, maszyny do urabiania ciągłego i maszyny udarowe. Wymagania bezpieczeństwa.

Artykuł został przedstawiony podczas Konferencji Bezpieczeństwa Przemysłowego – Klub Paragraf 34, 5–6 grudnia 2013, Wolbórz

dr inż. Józef Chmiel – CBiDGP Sp. z o.o. w Lędzinach, e-mail: j.chmiel@cbidgp.pl; jch56@wp.pl

artykuł recenzowany