Projektowanie funkcji bezpieczeństwa z wykorzystaniem podsystemu transmisji danych bezpieczeństwa

Tomasz Strawiński

Streszczenie: W artykule omówiono zagadnienia projektowania funkcji bezpieczeństwa realizowanych w układzie sterowania wykorzystującym podsystem transmisji danych bezpieczeństwa. Przedstawiono metodykę projektowania pozwalającą uwzględnić wpływ podsystemu transmisji danych bezpieczeństwa na przyrost prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego całego układu i osiągany poziom nienaruszalności bezpieczeństwa SIL oraz uzyskiwany czas zadziałania funkcji bezpieczeństwa.

Słowa kluczowe: funkcja bezpieczeństwa, podsystem transmisji danych związanych z bezpieczeństwem, prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego, czas zadziałania.

Abstract: *The paper presents the rules of development of safety related control functions which use the safety fieldbus. The presented development methodology specifies the safety fieldbus effect for the estimation of probability increment of dangerous failure per hour and for safety integrity level SIL and also for the safety related control function response time.*

Keywords: safety related control function, safety fieldbus, probability of dangerous failure, response time.

Wstęp

Efektywna realizacja systemów sterowania dużych zespołów maszyn lub linii produkcyjnych jest obecnie możliwa dzięki przyjęciu architektury rozproszonej systemu i wykorzystaniu programowalnych sterowników logicznych połączonych za pomocą elementów podsystemu transmisji danych (magistrali miejscowej). System sterowania w architekturze rozproszonej może również realizować funkcje bezpieczeństwa ograniczające ryzyko użytkowania maszyn. Wymaga to zastosowania sterowników bezpieczeństwa i podsystemów transmisji danych spełniających wymagania bezpieczeństwa funkcjonalnego, tj. elementów charakteryzujących się określonym (bardzo małym) prawdopodobieństwem wystąpienia uszkodzenia niebezpiecznego, tj. uszkodzenia prowadzącego do utraty zdolności systemu do realizacji danej funkcji bezpieczeństwa. Przy projektowaniu związanych z bezpieczeństwem elementów systemów sterowania maszyn należy uwzględniać wymagania dyrektywy 2006/42/WE [1] dotyczące bezpieczeństwa funkcjonalnego w całym cyklu życia.

Związane z bezpieczeństwem elementy systemów sterowania, takie jak programowalne sterowniki bezpieczeństwa czy dedykowane podsystemy transmisji danych bezpieczeństwa, są obecnie wyłącznie układami elektronicznymi i elektronicznymi programowalnymi. Stąd do projektowania związanych z bezpieczeństwem systemów sterowania opartych na tego typu elementach właściwe jest wykorzystanie ogólnej metodyki projektowania przedstawionej w normie [2] zharmonizowanej z dyrektywą 2006/42/WE i pozwalającej na spełnienie wymagań bezpieczeństwa funkcjonalnego odpowiednio do poziomu redukcji ryzyka wynikającego z zastosowania danej funkcji bezpieczeństwa. Opracowania podsystemów transmisji danych związanych z bezpieczeństwem (magistral miejscowych bezpiecznych funkcjonalnie) dodatkowo opierają się na wymaganiach normy [3] i [4]. Norma [4] zawiera również praktyczne wymagania odnośnie do zalecanego ograniczenia przyrostu prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego, spowodowanego wykorzystaniem podsystemu transmisji danych. Zastosowanie tego ograniczenia pozwala w uproszczony sposób podejść do projektowania elementów systemu sterowania realizujących funkcję bezpieczeństwa.

W przewodniku [5] przedstawiono wymagania związane z instalacją podsystemu transmisji danych związanych z bezpieczeństwem, jego konfiguracją i parametryzacją, walidacją powykonawczą podsystemu i sporządzeniem odpowiedniej dokumentacji oraz obsługą, konserwacją i naprawami, w tym również dotyczące niezbędnej informacji dla użytkownika. Spełnienie wymagań przewodnika umożliwia utrzymanie w całym cyklu życia założonego poziomu bezpieczeństwa funkcjonalnego układu sterowania. Dodatkowe wymagania dotyczące podsystemów transmisji danych bezpieczeństwa przedstawiono w pracach [6, 7].

Projektowanie funkcji bezpieczeństwa

W przypadku maszyn, stwierdzenie ryzyka związanego z ich użytkowaniem na poziomie wyższym niż dopuszczone przepisami dyrektywy 2006/42/WE wymaga zastosowania środków bezpieczeństwa zmniejszających to ryzyko do wymaganego poziomu. Funkcje bezpieczeństwa i odpowiednie układy sterowania przeznaczone do ich realizacji są jednym z rodzajów środków bezpieczeństwa powszechnie implementowanych w maszynach w celu redukcji ryzyka. Środki bezpieczeństwa powinny być skuteczne w redukcji ryzyka w całym cyklu życia

maszyny. W przypadku środków bezpieczeństwa opartych na sterowaniu wymaganie to osiąga się poprzez zapewnienie ich bezpieczeństwa funkcjonalnego poprzez odpowiednie projektowanie, wykonanie i eksploatację.

Ogólna metodyka projektowania układów sterowania elektrycznych/elektronicznych/elektronicznych programowalnych przewidzianych do realizacji funkcji bezpieczeństwa przedstawiona została w normie [2]. Metodyka ta zakłada, że cały związany z bezpieczeństwem układ sterowania maszyny składa się z systemów realizujących poszczególne funkcje bezpieczeństwa, a te z kolei składają się z podsystemów dedykowanych do pełnienia wybranych zadań. Typowymi podsystemami są:

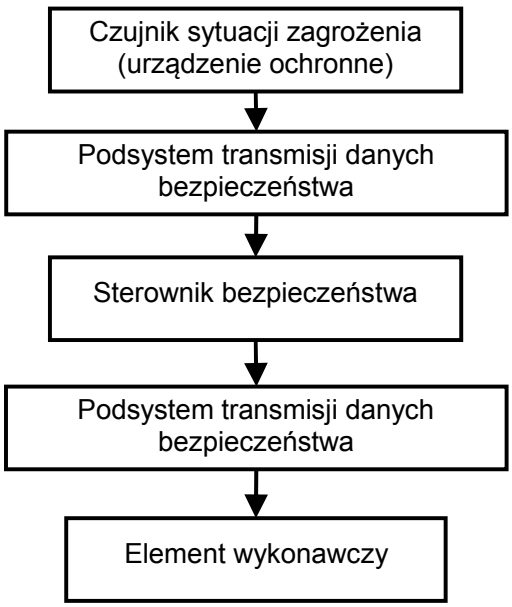
- czujnik sytuacji zagrożenia (np. urządzenie ochronne wykrywające człowieka, czujnik/miernik wielkości fizycznych) – wykrywa sytuację zagrożenia i generuje sygnał o jej występowaniu;
- sterownik bezpieczeństwa (obecnie bardzo często programowalny) – na podstawie sygnału z czujnika (czujników) generuje sygnały do elementu wykonawczego (elementów wykonawczych);
- element wykonawczy – na podstawie sygnału ze sterownika oddziałuje na stan energetyczny maszyny poprzez sterowanie zasilaniem napędów i innych elementów, w tym odbiorem energii z nich (np. poprzez uruchamianie/zatrzymywanie napędów, sterowanie dopływem/odpływem czynników, itp.).

Danymi bezpieczeństwa są wszystkie zmienne logiczne występujące w funkcjach bezpieczeństwa. Część z nich (lub wszystkie) może być przesyłana za pomocą podsystemu transmisji danych, który powinien zapewniać wewnętrznie odpowiednio wysoki poziom bezpieczeństwa funkcjonalnego.

Zastosowanie podsystemu transmisji danych bezpieczeństwa w realizacji układowej funkcji bezpieczeństwa wymaga uwzględnienia tego podsystemu w ogólnej konfiguracji (architekturze) systemu sterowania. Na ogólnym poziomie rozważań zakłada się, że podsystem transmisji danych będzie wykorzystany dwukrotnie: pierwszy raz przy przekazywaniu sygnałów z czujnika sytuacji zagrożenia do sterownika bezpieczeństwa i drugi raz przy przekazywaniu sygnałów ze sterownika do elementu wykonawczego (możliwa jest budowa systemu z niepełnym wykorzystaniem podsystemu transmisji danych). Ogólny schemat systemu sterowania o architekturze jednokanałowej przedstawiono na rys. 1.

Metodyka projektowania funkcji bezpieczeństwa przedstawiona w normie [2] przewiduje szereg etapów postępowania obejmujących:

- identyfikację zagrożeń i sytuację zagrożenia;
- oszacowanie i ocenę ryzyka (w wyniku końcowym powinna być wykazana potrzeba zastosowania środków bezpieczeństwa, które zmniejszą ryzyko – w przeciwnym przypadku dalsze działania nie są potrzebne);



Rys. 1. Architektura jednokanałowa związanego z bezpieczeństwem systemu sterowania wykorzystującego podsystem transmisji danych

- wstępne podjęcie decyzji o zastosowaniu środka bezpieczeństwa opartego na sterowaniu;
- opracowanie specyfikacji funkcji bezpieczeństwa uwzględniającej ograniczenia związane z maszyną i obejmującej: określenie funkcji logicznej i wymaganego czasu zadziałania, wstępny wybór urządzenia ochronnego (lub innego czujnika sytuacji zagrożenia), określenie wymagań związanych z bezpieczeństwem funkcjonalnym (SIL) i innymi cechami układu (architektura, pokrycie diagnostyczne), określenie ograniczeń;
- opracowanie planu realizacji projektu;
- opracowanie planu walidacji projektu (powinien przewidywać prowadzenie walidacji równolegle do procesu projektowania i badania układu sterowania oraz zakładać wykorzystanie wyników zakończonych etapów prac – w celu możliwie szybkiego wykrywania i korygowania błędów);
- projektowanie związanych z bezpieczeństwem elementów systemu sterowania;
- opracowanie oprogramowania elementów systemu sterowania związanych z bezpieczeństwem (o ile w projekcie wykorzystano elementy programowalne);
- analizy i badania w celu potwierdzenia wymaganych właściwości z zakresu bezpieczeństwa funkcjonalnego;
- sporządzenie dokumentacji technicznej;
- sporządzenie informacji dla użytkownika (stanowiącej fragment instrukcji maszyny) odnośnie do rodzaju funkcji bezpieczeństwa realizowanych w systemie sterowania maszyny, ich podstawowych parametrów, wymagań związanych z kontrolami okresowymi oraz wymagań związanych z ich eksploatacją i utrzymaniem założonego poziomu bezpieczeństwa funkcjonalnego w całym cyklu życia maszyny;
- walidację układu sterowania;
- ponowne oszacowanie i ocenę ryzyka w celu wykazania, że ryzyko zostało zmniejszone do wymaganego poziomu, lub powrót do ponownego oszacowania i oceny ryzyka z uwzględnieniem zastosowania dotychczas zaprojektowanych środków bezpieczeństwa (proces iteracyjny).

Zastosowanie podsystemu transmisji danych związanych z bezpieczeństwem wymaga uzupełnienia metodyki projektowania funkcji bezpieczeństwa w następujących aspektach:

- analiza możliwości, ograniczeń i celowości zastosowania podsystemu transmisji danych związanych z bezpieczeństwem do realizacji funkcji bezpieczeństwa (przed opracowaniem pełnej specyfikacji funkcji bezpieczeństwa);
- uwzględnienie w specyfikacji funkcji bezpieczeństwa dodatkowych informacji związanych z zastosowaniem podsystemu transmisji danych związanych z bezpieczeństwem (liczba i rodzaj zmiennych przesyłanych w ramach podsystemu, wymagany limit poziomu nienaruszalności bezpieczeństwa SILCL, dopuszczalne opóźnienia transmisji w kontekście wymagań dotyczących czasu zadziałania funkcji bezpieczeństwa i dodatkowych środków bezpieczeństwa związanych z tym parametrem, wymagania związane z konfiguracją i parametryzacją, wymagania związane z monitorowaniem defektów i sygnalizacją sytuacji alarmowych, wymagania związane z zapewnieniem bezpieczeństwa funkcjonalnego w przypadku wykrycia defektu elementów systemu sterowania, wymagania środowiskowe, kryteriów wyboru podsystemu);
- uwzględnienie w planie realizacji projektu dodatkowych etapów związanych z zastosowaniem podsystemu transmisji danych związanych z bezpieczeństwem (wybór podsystemu, projektowania jego konfiguracji i parametrów działania, szacowania wpływu na poziom nienaruszalności bezpieczeństwa SIL, szacowanie wielkości opóźnień związanych z transmisją danych i ich wpływu na czas zadziałania funkcji bezpieczeństwa, określenie parametrów monitorowania defektów i zasad działania podsystemu w przypadku ich wykrycia, projektowanie instalacji podsystemu w maszynie obejmujące dobór podzespołów, projekt okablowania zgodny ze specyfikacją podsystemu, projekt zasilania);
- uwzględnienie w planie walidacji działań wynikających z wystąpienia dodatkowych etapów projektowania oraz działań związanych z instalacją i uruchamianiem podsystemu transmisji danych związanych z bezpieczeństwem (walidacja kompetencji osoby odpowiedzialnej za konfigurację i parametryzację podsystemu oraz jego przygotowanie do działania, sprawdzenie przed załączeniem zasilania, sprawdzenie po załączeniu zasilania, próby funkcjonalne i testy jakości transmisji, walidacja sposobu zachowania danych referencyjnych);
- wykonanie w procesie projektowania i opracowywania oprogramowania związanych z bezpieczeństwem elementów systemu sterowania prac dotyczących zastosowania podsystemu transmisji danych (wybór podsystemu, opracowanie jego konfiguracji sprzętowej, określenie jego parametrów działania, określenie zasad monitorowania i kryteriów wystąpienia defektów związanych z działaniem podsystemu transmisji i innych podsystemów uczestniczących w realizacji funkcji bezpieczeństwa, określenie zasad działania podsystemu

w warunkach wystąpienia defektu zapewniających bezpieczeństwo funkcjonalne, opracowanie zbioru parametrów do konfiguracji i parametryzacji podsystemu);
- uwzględnienie w fazie analiz i badań projektu (prototypu) związanych z bezpieczeństwem elementów systemu sterowania sprawdzenia funkcjonowania podsystemu transmisji danych (testy łączy komunikacyjnych, określenie stopy błędów transmisji, sprawdzenie poprawności konfiguracji i parametryzacji podsystemu, wyznaczenie osiągniętego poziomu nienaruszalności bezpieczeństwa SIL);
- dołączenie do dokumentacji technicznej elementów systemu sterowania związanych z bezpieczeństwem dokumentacji związanej z zastosowanym podsystemem transmisji danych (dokumentacja ogólna podsystemu i szczegółowa dotycząca zastosowanych elementów, sposobu wykonania połączeń między elementami, rodzaju zastosowanych przewodów i tras ich poprowadzenia, dokumentacja zasilania i uziemiania elementów podsystemu, dokumentacja narzędzi przeznaczonych do testowania i wykrywania uszkodzeń podsystemu);
- dołączenie do instrukcji maszyny informacji niezbędnej do jej prawidłowego użytkowania i wynikającej z wykorzystania w systemie sterowania podsystemu transmisji danych związanych z bezpieczeństwem (informacja o funkcjach bezpieczeństwa realizowanych z wykorzystaniem podsystemu transmisji danych, ogólnych informacje o zasadach funkcjonowania podsystemu i monitorowania jego defektów, informacje szczegółowe o sposobie sygnalizacji stanów normalnej pracy podsystemu i sytuacji wystąpienia defektów, wymagania dotyczące kwalifikacji operatorów maszyny związane z użytkowaniem podsystemu transmisji danych, wymagania dotyczące kwalifikacji personelu odpowiedzialnego za prowadzenie kontroli okresowych i serwisowanie elementów systemu sterowania związanych z bezpieczeństwem, w tym podsystemu transmisji, zasady prowadzenia kontroli okresowych funkcji bezpieczeństwa wykorzystujących podsystem transmisji, opisy i instrukcje stosowania narzędzi specjalistycznych do diagnostyki podsystemu transmisji danych związanych z bezpieczeństwem);
- wykonanie w procesie walidacji analiz i sprawdzeń wynikających z zastosowania podsystemu transmisji danych związanych z bezpieczeństwem poprzez: sprawdzenie poprawności założeń projektowych (w tym dotyczących określenia wymagań związanych z bezpieczeństwem funkcjonalnym, czasem zadziałania i wymaganiami środowiskowymi), sprawdzenie poprawności procesu projektowania i przygotowania oprogramowania (w tym: doboru podsystemu, jego konfiguracji i parametrów działania, użycia odpowiednich narzędzi do programowania, stosowania właściwej dokumentacji producenta podsystemu), potwierdzenie osiągnięcia założonych właściwości funkcjonalnych, poziomu nienaruszalności bezpieczeństwa SIL i czasu zadziałania, potwierdzenie poprawności wykonania podsystemu i połączeń jego elementów (w tym: użycie odpowiednich podzespołów, zastosowanie przewodów o wymaganych właściwościach, prowadzenie przewodów i ich połączenia, wykonanie zasilania i uziemienia elementów podsystemu), sprawdzenie wyników testów funkcjonalnych, sprawdzenie kompletności dokumentacji technicznej (w tym: dokumentacji producenta podsystemu, dokumentacji wytworzonej w następstwie prac projektowych, danych dotyczących konfiguracji i parametryzacji), sprawdzenie informacji dotyczącej podsystemu transmisji danych w instrukcji maszyny (w tym: opis podsystemu i związanych z nim funkcji bezpieczeństwa, zamieszczenie niezbędnych schematów i wykazów elementów, zasady monitorowania i sygnalizacji normalnego działania i defektów, wymagania dotyczące obsługi, serwisu i napraw z uwzględnieniem kontroli okresowych).

Norma [2] i przewodnik [5] przedstawiają wiele szczegółów postępowania objętego przedstawioną powyżej metodyką projektowania funkcji bezpieczeństwa z zastosowaniem podsystemu transmisji danych bezpieczeństwa, co pozwala bezpośrednio zastosować te dokumenty do organizacji procesu projektowania i wykonania związanego z bezpieczeństwem układu sterowania maszyny. Wykorzystanie tych dokumentów jest zalecane w celu kompleksowego spełnienia wymagań bezpieczeństwa funkcjonalnego systemów sterowania maszyn.

Wpływ podsystemu transmisji danych na poziom zapewnienia bezpieczeństwa SIL i czas zadziałania

Jednym z ważnych elementów powyższej metodyki projektowania funkcji bezpieczeństwa jest określenie wpływu zastosowania podsystemu transmisji danych na osiągany poziom nienaruszalności bezpieczeństwa SIL. Znajomość tego wpływu pozwala już na początku procesu projektowania na podjęcie decyzji o wyborze rozwiązania z zastosowaniem podsystemu transmisji danych bezpieczeństwa lub bez niego.

Podsystemy realizujące funkcję bezpieczeństwa w szeregowej architekturze jednokanałowej i nieobjęte dodatkowymi funkcjami diagnostycznymi (rys. 1) wnoszą swój udział w ogólnym prawdopodobieństwie wystąpienia uszkodzenia niebezpiecznego systemu zgodnie ze wzorem:

$$PFH_D = PFH_{Dcz} + PFH_{Dsb} + PFH_{Dew} + 2\,PFH_{Dtr} \qquad (1)$$

gdzie:
- PFH_D – prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego systemu sterowania realizującego funkcję bezpieczeństwa;
- PFH_{Dcz}, PFH_{Dsb}, PFH_{Dew}, PFH_{Dtr} – prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego odpowiednio w podsystemach: czujnika sytuacji zagrożenia, sterownika bezpieczeństwa, elementu wykonawczego oraz jednego odcinka przesyłu danych bezpieczeństwa za pośrednictwem podsystemu transmisji.

Wielkość tak obliczonego prawdopodobieństwa jest podstawą do określenia poziomu nienaruszalności bezpieczeństwa SIL (tablica 3 w [2]).

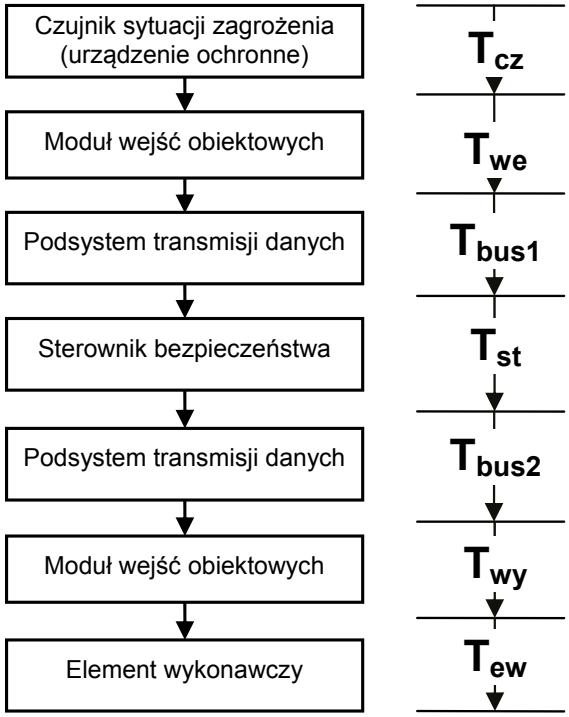
Opracowania podsystemów transmisji danych związanych z bezpieczeństwem (magistral miejscowych bezpiecznych funkcjonalnie) mogą opierać się na wymaganiach norm [3] i [4]. Norma [4] zawiera również praktyczne wymagania odnośnie

do zalecanego ograniczenia przyrostu prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego spowodowanego wprowadzeniem do architektury systemu podsystemu transmisji danych bezpieczeństwa. Zalecane jest, aby:

$$PFH_{Dtr} < 1\% \, (PFH_{Dcz} + PFH_{Dsb} + PFH_{Dew}) \qquad (2)$$

Spełnienie zależności (2) pozwala w praktycznych obliczeniach pominąć wpływ podsystemu transmisji danych bezpieczeństwa na wynikowy poziom nienaruszalności bezpieczeństwa SIL. Z tego względu zastosowanie podsystemów transmisji danych związanych z bezpieczeństwem o deklarowanej przez producenta zgodności z wymaganiami normy [4] jest rozwiązaniem istotnie ułatwiającym projektowanie związanych z bezpieczeństwem systemów sterowania.

W projektowaniu funkcji bezpieczeństwa, oprócz spełnienia wymagań bezpieczeństwa funkcjonalnego, istotne jest również zapewnienie czasu zadziałania nieprzekraczającego pewnego limitu narzuconego warunkami bezpieczeństwa (np. odległością bezpieczeństwa od strefy zagrożenia). Z punktu widzenia analizy wpływu dodatkowego podsystemu transmisji danych bezpieczeństwa na łączny czas zadziałania funkcji bezpieczeństwa należałoby wziąć pod uwagę strukturę funkcjonalną systemu, wnoszącą określone składowe do tego czasu (rys. 2). Dodatkowe składowe czasu zadziałania wynikające z zastosowania podsystemu transmisji danych związane są z przetwarzaniem w modułach wejść i wyjść obiektowych oraz dwukrotnie z przesyłaniem informacji poprzez interfejsy i łącza komunikacyjne. Składowe te odpowiadają wydłużeniu czasu zadziałania funkcji bezpieczeństwa w porównaniu z realizacjami niestosującymi podsystemu transmisji danych.



Rys. 2. Struktura funkcjonalna związanego z bezpieczeństwem systemu sterowania, wykorzystującego podsystem transmisji danych bezpieczeństwa i składowe czasu zadziałania funkcji bezpieczeństwa

Podsumowanie

Stosowanie podsystemów transmisji danych w związanych z bezpieczeństwem systemach sterowania jest obecnie atrakcyjnym rozwiązaniem pozwalającym na efektywną realizację układową całego systemu sterowania złożonych maszyn i linii technologicznych. Jednak zapewnienie bezpieczeństwa funkcjonalnego w całym cyklu życia tych systemów wymaga wielu dodatkowych działań w fazie projektowania, wykonania i późniejszej eksploatacji.

Literatura

[1] Dyrektywa 2006/42/WE *Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE (przekształcenie)*, Dziennik Urzędowy Unii Europejskiej L. 157 z 9.06.2006, s. 24.

[2] PN-EN 62061:2008P+A1:2013-6E *Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.*

[3] PN-EN 61784-1:2011E *Przemysłowe sieci komunikacyjne – Profile – Część 1: Profile magistrali miejscowej.*

[4] PN-EN 61784-3:2010E *Przemysłowe sieci komunikacyjne – Profile – Część 3: Magistrale miejscowe bezpieczne funkcjonalnie – Ogólne zasady i definicje profili.*

[5] IEC/TR 62513:2008E *Safety of machinery – Guideline for use of communication systems in safety related applications.*

[6] Missala T.: *Bezpieczeństwo funkcjonalne komunikacji w sieciach przemysłowych – stan normalizacji.* Materiały Konferencji Automation 2007, Warszawa 2007.

[7] Strawiński T.: *Wymagania dotyczące bezpieczeństwa funkcjonalnego podsystemów transmisji danych stosowanych w systemach sterowania maszyn*. 14 Międzynarodowa Konferencja Naukowo-Techniczna KOMTECH 2013 pt. „Innowacyjne Techniki i Technologie dla Górnictwa – Bezpieczeństwo – Efektywność – Niezawodność" – Kliczków 2013, s. 325–335.

Opracowanie wykonane na podstawie wyników zadania realizowanego w ramach II Programu Wieloletniego pn. „Poprawa bezpieczeństwa i warunków pracy".

Artykuł został przedstawiony podczas VI Konferencji Bezpieczeństwa Maszyn, Urządzeń i Instalacji Przemysłowych organizowanej przez „Klub Paragraf 34", 5–6 grudzień 2013, Bolesławów.

Tomasz Strawiński – Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy

artykuł recenzowany