

Formułowanie wymagań dotyczących wyposażenia bezpieczeństwa wykorzystującego technikę RFID

Tomasz Strawiński

Wstęp

W ostatnich latach nastąpił gwałtowny rozwój technik informatycznych i telekomunikacyjnych. Miniaturyzacja, zmniejszenie pobieranej energii, wzrost precyzji detekcji, wykorzystanie pól elektromagnetycznych wysokiej częstotliwości umożliwiają bardziej skuteczne monitorowanie i identyfikowanie obszarów i przedmiotów. Techniki te, obecnie już szeroko używane w transporcie i magazynowaniu, zaczynają być także coraz częściej stosowane w doskonaleniu procesów produkcyjnych, w tym także w obszarze rozwiązań poprawiających bezpieczeństwo na stanowiskach pracy przy maszynach. Potwierdzona skuteczność zastosowania techniki RFID do monitorowania stanu zużycia środków ochrony indywidualnej lub w systemach blokady drzwi dostępu do określonych obszarów wskazuje, że można przewidywać możliwość jej zastosowania także w związanym z bezpieczeństwem systemach sterowania maszyn. Wykorzystanie technik telekomunikacyjnych do monitorowania położenia przedmiotów w magazynach i systemach transportowych pozwalają przypuszczać, że mogą one także być wykorzystywane do monitorowania miejsc pobytu pracowników, także w aspekcie ich przebywania w strefach zagrożenia. Oczekuje się, że stosowanie techniki RFID przyczyni się do poprawy bezpieczeństwa operatorów maszyn, przy jednoczesnym usprawnieniu procesów produkcyjnych.

Propozycje zastosowań techniki RFID w dziedzinie bezpieczeństwa i higieny pracy wymagają gruntownych opracowań w celu określenia wymaganych właściwości wyposażenia ochronnego stosującego tę technikę i jego parametrów charakterystycznych, w tym szczególnie poziomu bezpieczeństwa funkcjonal-

nego w warunkach typowych narażeń środowiskowych występujących przy użytkowaniu maszyn. Cechy te nie były istotne w dotychczasowych zastosowaniach techniki RFID, nie były więc analizowane w wystarczającym zakresie. Wprowadzenie wyposażenia bezpieczeństwa stosującego technikę RFID do realizacji funkcji bezpieczeństwa wymaga także dysponowania informacją o zaleceniach i ograniczeniach w jej stosowaniu w dziedzinie bezpieczeństwa, metodyką oceny typu tych rozwiązań oraz metodyką projektowania funkcji bezpieczeństwa.

Technika RFID została opracowana w celu szybkiej, bezprzewodowej, wykonywanej z relatywnie niewielkiej odległości identyfikacji dowolnych obiektów, w tym przedmiotów, materiałów i osób. Szeroki i perspektywiczny obszar zastosowań techniki RFID stał się przedmiotem prac Komisji Europejskiej zmierzających do wdrożenia tej techniki w wielu dziedzinach gospodarki. W celu wdrożenia tej techniki zgodnie z zasadami wykorzystania częstotliwości radiowych niezbędnych do jej funkcjonowania Komisja Europejska podjęła szereg decyzji mających na celu harmonizację wykorzystania tych częstotliwości w obszarze Unii Europejskiej [1, 2] oraz określiła swoje stanowisko w tym obszarze [3].

Technika RFID została znormalizowana, głównie w zakresie wykorzystania częstotliwości radiowych, protokołu komunikacyjnego, rodzaju informacji podlegających transmisji i ogólnych wymagań środowiskowych, w szczególności dotyczących kompatybilności elektromagnetycznej (normy [4]).

W publikacjach prezentowane są również koncepcje zastosowania techniki RFID w obszarze bezpieczeń-

Streszczenie: W celu uzyskania możliwości implementacji funkcji bezpieczeństwa zgodnie z wymaganiami zasadniczymi dyrektywy 2006/42/WE niezbędne jest określenie wymagań dotyczących wyposażenia bezpieczeństwa wykorzystującego technikę RFID. Wymagania te powinny zmierzać w kierunku zapewnienia spełnienia wymagań zasadniczych w sposób dotyczący elementów bezpieczeństwa wymienionych w ich orientacyjnym wykazie (załącznik V do dyrektywy 2006/42/WE).

Słowa kluczowe: identyfikacja za pomocą częstotliwości radiowych (RFID), funkcja bezpieczeństwa, bezpieczeństwo funkcjonalne, środki bezpieczeństwa wykorzystujące technikę RFID.

Abstract: *In case of intention to implement safety function according to the essential requirements of directive 2006/42/WE, the safety equipment which applies the RFID technology shall satisfy the suitable particular requirements. These requirements directed be directed on the essential requirements of safety elements listed in Annex V do directive 2006/42/WE. (Preparation of Papers for VIII Symposium of Paragraf 34 – The setting of requirements for safety equipment using RFID technology).*

Keywords: *radio frequency identification (RFID), safety function, functional safety, safety measures with RFID technology.*

stwa użytkowania maszyn (prace [5, 6, 7]) w dwóch aspektach: identyfikacji obiektów w celach związanych

z bezpieczeństwem i zastosowań w formie wyposażenia ochronnego do realizacji funkcji bezpieczeństwa w związanych z bezpieczeństwem systemach sterowania maszyn. Pierwszy rodzaj wykorzystania techniki RFID do obniżania ryzyka użytkownika maszyn zawiera się w obszarze dodatkowych środków bezpieczeństwa wykorzystywanych w trybie *offline* i nieobjętych istotnymi wymaganiami zasadniczymi dyrektywy 2006/42/WE. Natomiast zastosowania techniki RFID w środkach bezpieczeństwa opartych na sterowaniu podlega istotnym wymaganiom w zakresie zapewnianego bezpieczeństwa funkcjonalnego, co wynika z przepisów prawa [8, 9] oraz norm z nimi zharmonizowanych [10, 11, 12]. Wyposażenie bezpieczeństwa zrealizowane z wykorzystaniem techniki RFID powinno spełniać wymagania szczególne dotyczące elementów bezpieczeństwa, analogicznie do tych, które zostały wymienione w załączniku V do dyrektywy 2006/42/WE. Wzorcem do sformułowania tych wymagań może być norma [13].

Wyposażenie RFID jako środek bezpieczeństwa

Wyposażenie RFID może realizować następujące funkcje bezpieczeństwa:

- funkcja blokady uruchomienia – wymaga skojarzenia stanu identyfikacji w systemie RFID z sytuacją odpowiadającą bezpieczeństwu – stan identyfikacji pozwala na zniesienie blokady uruchomienia;
- funkcja zatrzymania samoczynnego – wymaga skojarzenia stanu identyfikacji w systemie RFID z sytuacją zagrożenia – stan identyfikacji powinien spowodować samoczynne przejście maszyny do stanu bezpieczeństwa (np. zatrzymanie ruchów roboczych).

W obu przypadkach wykorzystanie techniki RFID powinno być uzupełniającym środkiem bezpieczeństwa skojarzonym z zastosowaniem innych środków bezpieczeństwa o charakterze podstawowym.

W celu uzyskania możliwości implementacji powyższych funkcji bezpieczeństwa zgodnie z wymaganiami zasadniczymi dyrektywy 2006/42/WE niezbędne jest określenie wymagań dotyczących wyposażenia bezpieczeństwa wykorzystują-

cego technikę RFID. Przy określaniu tych wymagań inne, związane z bezpieczeństwem użytkownika maszyn, zastosowania techniki RFID nie będą brane pod uwagę. Zastosowania te nie są związane z systemem sterowania maszyny, a ich aplikacja mieści się w kategorii dodatkowych środków bezpieczeństwa opartych na rozwiązaniach organizacyjnych.

Wymagania dotyczące wyposażenia bezpieczeństwa wykorzystujące technikę RFID nie były dotychczas formułowane. Dotychczasowe próby wypełnienia tej luki opierały się na zastosowaniu normy [13]. Jest to zgodne z projektem rekomendacji do stosowania opracowanej przez grupę VG11 z Europejskiej Koordynacji Jednostek Notyfikowanych w Zakresie Dyrektywy Maszynowej 2006/42/WE. Wyposażenie bezpieczeństwa stosujące technikę RFID, jakkolwiek technicznie może spełniać definicję elektroczułego wyposażenia ochronnego (zespół urządzeń i/lub elementów współpracujących ze sobą w celu ochronnego wyłączenia samoczynnego lub wykrywania obecności, składający się co najmniej z urządzenia czujnikowego, urządzenia sterująco-monitorującego oraz urządzenia przełączającego sygnału wyjściowego i/lub związanego z bezpieczeństwem interfejsu transmisji danych), to nie realizuje swoich funkcji bezpośrednio, odnosząc je do człowieka lub części jego ciała, lecz do transpondera, którego skojarzenie z obiektem wykrywanym wnosi dodatkowy obszar niepewności działania, niewątpliwie obniżający poziom bezpieczeństwa funkcjonalnego. Z tego względu wymagania normy [13] powinny być odpowiednio zmodyfikowane.

Przy opisie wymagań dotyczących wyposażenia bezpieczeństwa wykorzystującego technikę RFID stosowany będzie skrót „wyposażenie RFID”. Zastosowano również odpowiednio zmodyfikowaną terminologię analogicznie do zdefiniowanej w normie [13] oraz zastosowano następujące definicje:

- wyposażenie RFID – zespół urządzeń stosujący technikę RFID do realizacji funkcji identyfikacji, składający się z czytnika lub zespołu czytników oraz zgodnych z nimi transponderów. Czytnik składa się co najmniej z: urządzenia nadawczo-odbiorczego

pracującego z ustaloną częstotliwością radiową wraz z anteną lub zespołem anten, systemu komputerowego z bazą danych identyfikatorów transponderów, realizującego funkcję identyfikacji oraz urządzenia przełączającego sygnału wyjściowego (OSSD) i/lub związanego z bezpieczeństwem interfejsu transmisji danych. Transponder jest ruchomym przenośnym elementem z unikatowym identyfikatorem, na podstawie którego przeprowadzana jest identyfikacja aktywowanym sygnałem radiowym z czytnika;

- identyfikacja wykonywana przez wyposażenie RFID – proces polegający na aktywowaniu transpondera sygnałem o częstotliwości radiowej, odbiorze przez czytnik unikatowego identyfikatora zawartego w transponderze i porównaniu identyfikatora z zawartością bazy danych czytnika;
- strefa identyfikacji – strefa, w której określony transponder może być zidentyfikowany przez wyposażenie RFID;
- czas identyfikacji – największy czas pomiędzy wystąpieniem zdarzenia prowadzącego do identyfikacji i przejściem OSSD do stanu OFF.

Wymagania funkcjonalne dotyczące wyposażenia RFID

Wymagania funkcjonalne dotyczące wyposażenia RFID należy formułować w następujących obszarach:

- działania normalnego;
- funkcji wykrywania;
- wymaganego poziomu bezpieczeństwa funkcjonalnego.

Działanie normalne

Podczas działania normalnego, gdy nie są wykrywane defekty, OSSD wyposażenia RFID może przyjmować stan ON lub OFF stosownie do wyniku identyfikacji i wybranego rodzaju pracy.

Wyposażenie RFID powinno wysyłać sygnał wyjściowy odpowiedni do wyniku identyfikacji transpondera w strefie identyfikacji. Czas identyfikacji nie powinien przekraczać czasu zadeklarowanego przez producenta (dostawcę). Nastawianie czasu identyfikacji nie powinno być możliwe bez zastosowania specjalnego narzędzia przeznaczonego do tego celu.

Nastawianie identyfikatora w transponderze nie powinno być możliwe. Zmiana zawartości bazy danych w czytniku nie powinna być możliwa bez zastosowania specjalnego narzędzia przeznaczonego do tego celu.

Funkcja wykrywania

Funkcja identyfikacji powinna być skuteczna w całym obszarze strefy identyfikacji określonej przez producenta. Nastawianie strefy identyfikacji nie powinno być możliwe bez zastosowania specjalnego narzędzia przeznaczonego do tego celu.

Wymagany poziom bezpieczeństwa funkcjonalnego

Osiągany poziom bezpieczeństwa funkcjonalnego wyposażenia RFID powinien wynosić nie mniej niż SIL 1, z zastrzeżeniem weryfikacji możliwości spełnienia tego wymagania poprzez badania wybranych przykładów wyposażenia RFID, z uwzględnieniem pewności posiadania (noszenia) transpondera przez człowieka oraz jego odporności na zniszczenie, próby zaekranowania i inne równorzędne działania uniemożliwiające identyfikację.

Wymagania projektowe dotyczące wyposażenia RFID

Wymagania projektowe istotne w odniesieniu do wyposażenia RFID należy przedstawić w odniesieniu do następujących właściwości i elementów konstrukcyjnych:

- zasilanie elektryczne;
- zachowania w stanie defektu;
- wyposażenie elektryczne;
- element przełączający sygnału wyjściowego;
- wskaźniki i wyświetlacze;
- środki do nastawiania;
- rozłączanie elementów składowych;
- elementy nieelektryczne;
- uszkodzenia pochodzące od wspólnej przyczyny;
- elementy scalone programowalne lub o dużej złożoności;
- oprogramowanie, programowanie, projektowanie funkcjonalne obwodów scalonych.

Zasilanie elektryczne

Czytnik wyposażenia RFID powinien funkcjonować poprawnie w poniższych

warunkach zasilania odniesionych do wartości znamionowych:

- zasilanie napięciem przemiennym:
 - napięcie: 0,85 do 1,1 napięcia znamionowego,
 - częstotliwość: 0,99 do 1,01 częstotliwości znamionowej (w warunkach pracy ciągłej) oraz 0,98 do 1,02 częstotliwości znamionowej (krótkookresowo),
 - zawartość harmonicznych: nieprzekraczająca 10% wartości skutecznej napięcia w zakresie harmonicznych od 2. do 5. i 2% wartości skutecznej napięcia w zakresie harmonicznych od 6. do 30.;
- zasilanie napięciem stałym z baterii:
 - napięcie: 0,85 do 1,15 napięcia znamionowego (0,7 do 1,2 napięcia znamionowego w przypadku wyposażenia przeznaczonego do pojazdów zasilanych z akumulatorów);
- zasilanie napięciem stałym z przetworzonego napięcia:
 - napięcie: 0,9 do 1,1 napięcia znamionowego,
 - tętnienia (międzyszczytowe): nieprzekraczające 0,05 napięcia znamionowego

Transpondery wyposażenia RFID powinny być pasywne (aktywowane polem czytnika, bez własnego źródła zasilania).

Zachowanie w stanie defektu

O ile to możliwe, wyposażenie RFID powinno wykrywać defekty związane z nieprawidłowym działaniem transpondera i/lub czytnika, w tym dotyczące: nieprawidłowego kodu identyfikacyjnego, błędów transmisji, uszkodzenia nadajnika odbiornika w czytniku, uszkodzenia lub błędów podłączenia anteny czytnika, funkcjonowania systemu komputerowego obsługującego bazę danych i inne racjonalnie uzasadnione.

W stanie defektu wyposażenia RFID jego OSSD powinno przechodzić do stanu OFF i utrzymywać ten stan do czasu usunięcia defektu. Po włączeniu zasilania wyposażenie RFID powinno inicjować procedurę testową sprawdzającą wystąpienie defektów wykrywalnych. Przejście wyposażenia RFID znajdującego się w stanie defektu do normalnego działania nie powinno być możliwe.

Należy prowadzić analizę FMEA w celu ustalenia listy potencjalnych

uszkodzeń (w tym uszkodzeń niebezpiecznych). W analizie należy uwzględnić możliwe sytuacje związane z przypadkowym lub celowym uszkodzeniem transpondera lub uniemożliwieniem jego identyfikacji.

Wyposażenie elektryczne

Należy spełnić wymagania punktu 4.2.3 normy [13].

Element przełączający sygnału wyjściowego (OSSD)

Należy zapewnić oddzielne zaciski do przyłączania obwodu każdego OSSD. OSSD powinno być zaprojektowane w sposób pozwalający na przyłączanie obciążenia bez stosowania elementów gaszenia łuku. Obwód wyjściowy OSSD powinien być zabezpieczony przed przecięciem.

W przypadku zastosowania więcej niż jednego OSSD należy stosować środki minimalizujące prawdopodobieństwo wystąpienia uszkodzeń niebezpiecznych spowodowanych wspólną przyczyną.

Działanie wyposażenia RFID skutkujące zmianą stanu OSSD powinno powodować odpowiednie działanie związane z bezpieczeństwem interfejsu transmisji danych.

Charakterystyki prądowo-napięciowe OSSD wykonanych jako przekaźnikowe lub półprzewodnikowe powinny spełniać wymagania punktów 4.2.4.2 i 4.2.4.3 normy [13]. Związany z bezpieczeństwem interfejs transmisji danych powinien spełniać wymagania punktu 4.2.3.4.

Wskaźniki i wyświetlacze

Należy spełnić wymagania punktu 4.2.5 normy [13].

Środki do nastawiania

Jeżeli w wyposażeniu RFID przewidziano możliwość nastawiania zasięgu i/lub czasu identyfikacji, to środki do nastawiania powinny być tak zaprojektowane, aby uszkodzenie niebezpieczne nie było możliwe w dowolnym punkcie zakresu nastawiania. Jeżeli nastawianie wiąże się ze zmianą konfiguracji, to powinny być to zmiany zamierzone.

Rozłączanie elementów składowych

Jeżeli w wyposażeniu RFID możliwe jest odłączanie elementów składowych

(np. anteny od czytnika), to takie odłączenie powinno skutkować przejściem co najmniej jednego OSSD do stanu OFF.

Transponder zawsze powinien być wykonany w postaci jednego modułu, bez możliwości odłączania jakichkolwiek elementów składowych.

Elementy nieelektryczne

Elementy nieelektryczne wyposażenia RFID powinny być odpowiednie do zamierzonego zastosowania.

Uszkodzenia pochodzące od wspólnej przyczyny

Projekt wyposażenia RFID powinien minimalizować możliwość wystąpienia jakiegokolwiek defektu niebezpiecznego spowodowanego wspólną przyczyną pochodzącą od czynników środowiskowych.

Elementy scalone programowalne lub o dużej złożoności

Stosowaniu elementów scalonych programowalnych lub o dużej złożoności powinna towarzyszyć implementacja funkcji diagnostycznych zdolnych do wykrywania defektów w możliwie największym stopniu.

Oprogramowanie, projektowanie funkcjonalne obwodów scalonych

Przygotowanie oprogramowania, zaprogramowanie elementów programowalnych i projektowanie funkcjonalne obwodów scalonych wyposażenia RFID powinno być prowadzone zgodnie z wymaganiami bezpieczeństwa funkcjonalnego odpowiednimi do zapewnianego poziomu nienaruszalności bezpieczeństwa SIL.

Wymagania środowiskowe dotyczące wyposażenia RFID

Wymagania środowiskowe dotyczące wyposażenia RFID należy określić w odniesieniu do następujących czynników środowiskowych:

- temperatura otoczenia i wilgotność;
- zaburzenia elektryczne;
- czynniki mechaniczne;
- ochrona zapewniana przez obudowy.

Temperatura otoczenia i wilgotność

Czytnik i transponder systemu RFID powinny pracować normalnie co naj-

mniej w zakresie temperatur otoczenia od 0°C do 50°C i wilgotności względnej do 95% (bez kondensacji pary wodnej).

Zaburzenia elektryczne

Czytnik systemu RFID nie powinien ulegać defektom niebezpiecznym podczas zmian napięcia (napięć) zasilania. Defekty niebezpieczne nie powinny wystąpić podczas próby polegającej na jednostajnym i ciągłym obniżaniu zewnętrznego napięcia zasilania od wartości znamionowej do zera w czasie od 10 s do 20 s, a następnie na podwyższaniu tego napięcia do wartości znamionowej w tym samym tempie. Podczas analogicznej próby prowadzonej w odniesieniu do napięć zasilających wytwarzanych wewnątrz również nie powinny wystąpić defekty niebezpieczne.

Czytnik systemu RFID powinien kontynuować działanie normalne lub odpowiednio nie ulegać uszkodzeniom niebezpiecznym podczas zaniku napięcia zasilania zewnętrznego. Należy przeprowadzić testy polegające na wymuszeniu spadku napięcia zasilania o zadany procent wartości znamionowej na zadany czas i z określoną częstotliwością powtórzeń próby (% spadku napięcia, czas trwania spadku, liczba powtórzeń próby). Podczas testów według prób (100%, 10 ms, 10 Hz) i (50%, 20 ms, 5 Hz) powinna być kontynuowana normalna praca systemu RFID. Podczas testów według próby (50%, 500 ms, 0,2 Hz) system RFID nie powinien ulec uszkodzeniu niebezpiecznemu.

W przypadku zasilania systemu RFID ze szczególnych źródeł zasilania (np. zasilanie poprzez sieć transmisji danych) próby należy prowadzić w odniesieniu do pierwotnego napięcia zasilania.

System RFID powinien być odporny na szybkie elektryczne stany przejściowe, zaburzenia przewodzone indukowane obcymi polami magnetycznymi i wyładowania elektrostatyczne. W tym zakresie należy dążyć do spełnienia wymagań punktów 4.3.2.3.1, 4.3.2.4.1, 4.3.2.5.1, 4.3.2.6.1 i 4.3.2.7.1 normy [13] i przywołanych w tych punktach norm: PN-EN 61000-4-4:2013-05, PN-EN 61000-4-5:2014-10, PN-EN 61000-4-3:2007, PN-EN 61000-4-6:2014-04, PN-EN 61000-4-2:2011 (wymagania dotyczące kompatybilności elektroma-

gnetycznej urządzeń elektrycznych) przy uwzględnieniu wymagań norm serii ISO/IEC 18000 dotyczących interfejsu radiowego.

Czynniki mechaniczne

Czytnik i transponder systemu RFID powinny pracować normalnie w środowisku, w którym występują narażenia na drgania i udary. Odporność i wytrzymałość na te narażenia należy potwierdzić poprzez odpowiednie próby.

Ochrona zapewniana przez obudowy

Czytnik i transponder systemu RFID powinny mieć swoje własne obudowy.

Obudowa czytnika powinna mieć stopień ochrony IP54. Wszelkie otwory do wprowadzania kabli powinny zachowywać ten stopień ochrony. Nie należy stosować mas uszczelniających pomiędzy elementami obudowy, które powinny być odłączane podczas serwisu. Obudowa czytnika powinna być pozbawiona ostrych krawędzi. Obudowa powinna umożliwiać dostęp do elementów do nastawiania parametrów i programowania informacji wykorzystywanych do identyfikacji, jeżeli takie funkcje zostały przewidziane.

Obudowa transpondera powinna być monolityczna, nierozbieralna, pozbawiona ostrych krawędzi i dostosowana do konkretnych aplikacji systemu RFID.

Podsumowanie

Przedstawione wymagania szczególnie dotyczące wyposażenia ochronnego wykorzystującego technikę RFID mogą być stosowane do jego badań i oceny typu. Na ich podstawie można wykazać


zgodność tego wyposażenia z wymaganiami zasadniczymi dyrektywy 2006/42/WE.

Literatura

- [1] Commission Decision (2006/804/EC) of 23 November 2006 on harmonization of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band. OJ L 329 25.11.2006.
- [2] Commission Decision (2006/771/EC) of 9 November 2006 on harmonization of the radio spectrum for use by short-range devices. OJ L 312 11.11.2006.
- [3] Commission of the European Communities. Brussels, 15.3.2007. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Radio Frequency Identification (RFID) in Europe: steps towards a policy framework.
- [4] Normy serii ISO/IEC 18000-x Information technology – Radio frequency identification for item management.
- [5] TIHAY D.: *Application de la RFID a la prevention des risques professionnels en entreprise*. INRS – Hygiene et securite du travail 2012 – 226/25.
- [6] FABRIZIO I. I INNI: *Wireless Sensing Based on RFID and Capacitive Technologies for Safety in Marble Industry Process Control*. Journal of Computer Networks and Communications Vol 2013, Article ID 392056;
- [7] STRAWIŃSKI T.: *Wykorzystanie techniki RFID do ograniczania ryzyka użytkownika maszyn*. Maszyny elektryczne - Zeszyty problemowe 105 (1/2015), s. 119–124.
- [8] 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, str. 24.
- [9] Rozporządzenie Ministra Transportu z dn. 3 lipca 2007 r. w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego (Dz. U. 2007 nr 138, poz. 972 ze zmianą z dn. 29 lutego 2008 r. Dz. U. 2008 nr 47, poz. 277).
- [10] PN-EN ISO 12100:2012P Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka.
- [11] PN-EN ISO 13849-1,2 Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem.
- [12] PN-EN 62061:2008 Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
- [13] PN-EN 61496-1:2014-02 Bezpieczeństwo maszyn – Elektroczułe wyposażenie ochronne – Część 1: Wymagania ogólne i badania.

Opracowanie wykonane na podstawie wyników zadania realizowanego w ramach III etapu Programu Wieloletniego pn. „Poprawa bezpieczeństwa i warunków pracy”

Artykuł pochodzi z materiałów konferencji Paragraf 34 z 2015 roku.

 mgr inż. Tomasz Strawiński – Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy