Urządzenia bezpieczeństwa maszyn wykorzystujące technikę RFID – podstawy, wymagania, badania, stosowanie

Opracował: mgr inż. Tomasz Strawiński – Zakład Techniki Bezpieczeństwa CIOP-PIB

Spis treści:

1. Wprowadzenie

W ostatnich latach nastąpił gwałtowny rozwój technik informatycznych i telekomunikacyjnych. Miniaturyzacja, zmniejszenie pobieranej energii, wzrost precyzji detekcji, wykorzystanie pół elektromagnetycznych wysokiej częstotliwości umożliwia bardziej skuteczne monitorowanie i identyfikowanie obszarów i przedmiotów. Techniki te, obecnie już

szeroko stosowane 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.

Jedną z możliwości jest technika identyfikacji z wykorzystaniem częstotliwości radiowych (ang. Radio Frequency IDentification – RFID). Potwierdzona skuteczność zastosowania techniki RFID do monitorowania stanu zużycia środków ochrony indywidualnej lub w systemach blokady dostępu wskazuje, że można przewidywać możliwość jej zastosowania także w związanych 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.

Zastosowanie techniki RFID w dziedzinie bezpieczeństwa i higieny pracy wymaga określenia wymaganych właściwości wyposażenia bezpieczeństwa stosującego tą technikę i jego parametrów charakterystycznych, w tym szczególnie poziomu pewności działania w warunkach typowych narażeń środowiskowych występujących przy użytkowaniu w środowisku przemysłowym. 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.

Niniejszy poradnik jest poświęcony przedstawieniu zasad wykorzystania techniki RFID w obszarze bezpieczeństwa użytkowania maszyn w charakterze wyposażenia ochronnego uczestniczącego w realizacjach funkcji bezpieczeństwa oraz w charakterze dodatkowych środków bezpieczeństwa pozwalających na identyfikację stanów elementów maszyny związanych z bezpieczeństwem. Rozwiązania stosujące technikę RFID odpowiedzialne za zapewnienie bezpieczeństwa i higieny pracy przy maszynach powinny spełniać wymagania zasadnicze dyrektywy 2006/42/WE (maszynowej).

2. Właściwości techniki RFID w aspekcie zastosowań związanych z bezpieczeństwem użytkowania maszyn

2.1. Stan techniki RFID

Technika RFID została opracowana w celu szybkiej, bezprzewodowej, wykonywanej z relatywnie niewielkiej odległości identyfikacji dowolnych obiektów, w tym przedmiotów, materiałów i osób. Obszar zastosowań techniki RFID stał się na tyle obiecujący, że stał się

przedmiotem prac Komisji Europejskiej zmierzających do wdrożenie techniki RFID 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 swoją stanowisko w tym obszarze [3].

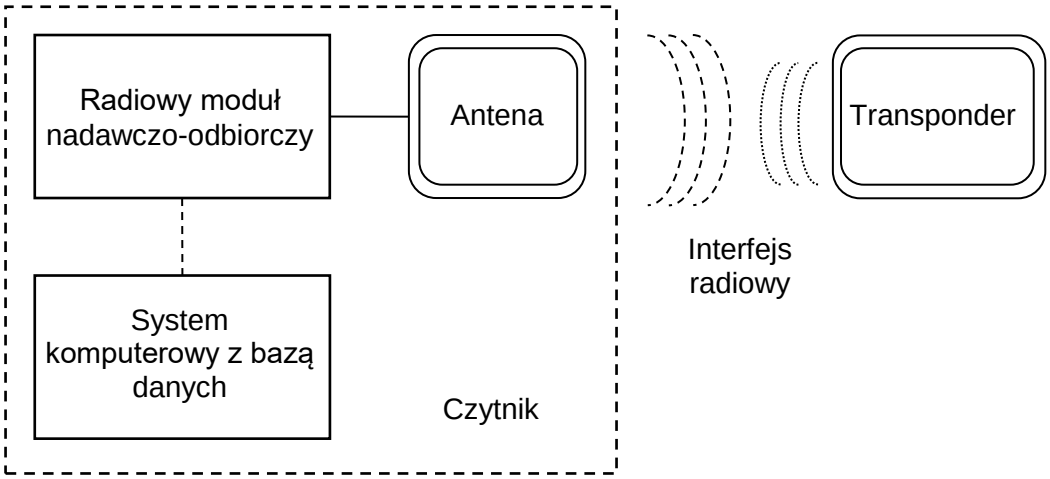
Technika RFID została znormalizowana, głównie w zakresie wykorzystania częstotliwości radiowych, protokołu komunikacyjnego, rodzaju informacji podlegających transmisji i ogólnych wymagań środowiskowych, w szczególności dotyczących kompatybilności elektromagnetycznej (normy [3-9]).

Niektóre możliwości wykorzystania techniki RFID znalazły w pewnych dziedzinach na tyle powszechne zastosowanie, że opracowano już normy szczegółowe z tym związane. Należą do nich na przykład normy dotyczące kart identyfikacyjnych bezkontaktowych (zbliżeniowych i wykrywanych w pobliżu) lub wyposażenia do radiowej identyfikacji zwierząt [10-18].

W obszarze bezpieczeństwa użytkowania maszyn rozważa się dwa aspekty wykorzystania techniki RFID: identyfikacja obiektów w celach związanych z bezpieczeństwem i zastosowania w formie wyposażenia ochronnego do realizacji funkcji bezpieczeństwa w związanych z bezpieczeństwem systemach sterowania maszyn. Pierwszy rodzaj wykorzystania techniki RFID do obniżania ryzyka użytkowania maszyn zawiera się w obszarze dodatkowych środków bezpieczeństwa wykorzystywanych w trybie off-line i nie objętych 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 i komentarzy do nich ([19-22]) oraz norm z nimi zharmonizowanych ([23-28]). Wyposażenie bezpieczeństwa zrealizowane z wykorzystaniem techniki RFID powinno spełniać wymagania analogiczne do wymagań dotyczących wyposażenia ochronnego maszyn (norma [29]).

2.2. Elementy systemu RFID

System RFID funkcjonuje w oparciu o różne techniki komunikacji radiowej realizowane pomiędzy urządzeniem służącym tylko do odczytu danych lub do odczytu i zapisu danych, nazywanym czytnikiem, a urządzeniem przechowującym unikatowe dane, nazywanym transponderem. W skład systemu RFID (rys. 1) wchodzą czytniki i odpowiednie do nich transpondery oraz aplikacja komputerowa z bazą danych, która steruje całym systemem.



Rys. 1. Struktura systemu RFID

2.3. Transponder RFID

Nazwa "transponder" utworzona została w języku angielskim z połączenia dwóch słów: "transmitter" (nadajnik) i "responder" (urządzenie odpowiadające, odzewowe). Nazwa ta oznacza urządzenie nadawcze, które rozpoczyna swoje nadawanie w odpowiedzi na wcześniej odebrany sygnał radiowy.

Transponder systemu RFID przeznaczony jest do umocowania do obiektu, który ma być identyfikowany. W transponderze przechowywany jest jego niepowtarzalny i niezmienny kod identyfikacyjny (identyfikator, numer seryjny, ID) oraz mogą być przechowywane dane dodatkowe, takie jak kod wytwórcy transpondera, informacje identyfikujące użytkownika systemu i dane indywidualne związane z konkretnym transponderem odnoszące się do obiektu, który jest z nim skojarzony. W zależności od systemu część z tych danych może być wielokrotnie zmieniana (zapisywana ponownie). W tym celu transponder dysponuje pewną liczbą bajtów pamięci, z której część zawierająca identyfikator zawsze jest dostępna tylko do odczytu (pamięć typu ROM) a jej zawartość zazwyczaj jest ustalana i kodowana w procesie produkcji. W zależności od rodzaju systemu pozostała część pamięci transpondera może też być tylko odczytywalna (jest wtedy jednokrotnie programowana przez producenta na zamówienie przyszłego użytkownika) lub może być pamięcią nieulotną odczytywalną i zapisywalną przez samego użytkownika (pamięć typu EEPROM).

Oprócz pamięci i urządzenia odbiorczo-nadawczego w transponderze mogą być umieszczone czujniki zmiennych parametrów identyfikowanego obiektu np. temperatury. Informacje z tych czujników mogą być przesyłane do czytnika w procesie komunikacji.

Transponder po uaktywnieniu przesyła drogą radiową zawartą w nim informację (zwykle całą tj. wszystkie jej elementy odpowiednio sformowane w jeden rekord danych) stosując protokół transmisji radiowej odpowiedni w danym systemie RFID.

Transpondery mogą być wykonane jako:

– bierne (passive) - nie mają własnego źródła zasilania, a energię niezbędną do działania i nadawania uzyskują z pola elektromagnetycznego wytwarzanego przez czytnik,
– aktywne - zastosowano bateryjne zasilanie układu elektronicznego transpondera,
– półaktywne - energia do działania i nadawania transpondera pozyskiwana jest z pola elektromagnetycznego czytnika, natomiast zasilanie dodatkowych czujników i ewentualnie zasilanie pamięci danych zmiennych odbywa się z baterii.

Aktywacja transpondera następuje tylko w sytuacji, gdy znajdzie się on w polu (elektromagnetycznym lub magnetycznym) o określonej częstotliwości emitowanym przez antenę czytnika lub odbierze odpowiedni sygnał inicjujący z czytnika. Transpondery aktywne uzyskują większe zasięgi komunikacji.

Transpondery wykonywane są w formie mikroukładów ze zintegrowaną anteną i z wykorzystaniem dedykowanych układów scalonych. Umieszczane są one w różnych obudowach w zależności od przeznaczenia systemu RFID. Mogą to być obudowy w formie kapsułek lub żetonów z tworzywa sztucznego o różnych kształtach, obudowy umożliwiające przyklejenie lub wykonane w formie kart płatniczych.

2.4. Czytnik RFID

Czytnik jest urządzeniem komunikującym się z transponderami znajdującymi się w jego zasięgu za pomocą interfejsu radiowego. Jest to urządzenie nadawczo-odbiorcze emitujące energię wykorzystywaną do uaktywniania transponderów. Łączność z transponderami może być nawiązywana przy wykorzystaniu emisji radiowej (pole elektromagnetyczne) albo przy wykorzystaniu sprzężenia indukcyjnego (poprzez pole magnetyczne). Czytnik odpowiada za inicjację i przebieg łączności z transponderami zgodnie z protokołem transmisji, odczytuje informacje z transponderów, w zależności od rodzaju systemu RFID może również przesyłać informację do transponderów i polecać jej zapisanie w pamięci. Transmisja od czytnika w kierunku transpondera jest określana mianem "łącza w przód" lub "łącza w dół" (ang. forward link, down link"), natomiast w kierunku przeciwnym używa się określenia "łącze powrotne" lub "łącze w górę" (ang. return link, up link).

Czytnik odbierający sygnał transpondera dekoduje informację otrzymywaną z transpondera, a następnie przesyła ją do systemu komputerowego w celu jego identyfikacji. Do identyfikacji wykorzystywane są informacje zawarte w bazie danych systemu. Sposób komunikacji czytnika z systemem komputerowym nie jest objęty standardami dotyczącymi techniki RFID i może być dowolny: przewodowy lub bezprzewodowy (lecz z wykorzystaniem systemów transmisji nie kolidujących z zasadniczą techniką łączności).

Czytnik jest urządzeniem elektronicznym zawierającym antenę, układ nadajnika/odbiornika sygnału radiowego, procesor odpowiadający za realizację protokołu transmisji, interfejs komunikacyjny do systemu komputerowego i układ zasilania. Może być on również wykonany jako jednostka samodzielna i wtedy nie zawiera interfejsu komunikacyjnego, a procesor protokołu transmisji pełni również funkcję systemu komputerowego dokonującego identyfikacji na podstawie niewielkiej bazy danych lub tylko wyświetlającego informację odebraną z transpondera.

Czytnik może być wykonany jako urządzenie stacjonarne, mobilne lub przenośne (z zasilaniem bateryjnym) z zastosowaniem elementów scalonych o wysokim stopniu integracji. Czytniki stacjonarne i mobilne zwykle pracują w sposób ciągły korzystając z dostępnej sieci zasilającej lub lokalnych źródeł energii (instalacja elektryczna pojazdu). Czytniki przenośne zasilane z baterii lub niewielkich akumulatorów zwykle załączane są w momencie wykonywania czynności identyfikacji. Obudowy czytników mogą być dowolne i zazwyczaj są dostosowane do przeznaczenia systemu RFID.

Istotnym elementem czytnika jest antena, której kształt, wielkość i charakterystyka częstotliwościowa w istotny sposób determinuje wielkość i geometrię obszaru, w którym możliwe jest nawiązanie łączności z transponderem. Anteny czytników są optymalizowane pod kątem potrzeb wynikających z przeznaczenia systemu RFID.

Zastosowania systemu RFID mogą przewidywać, że w strefie odczytu czytnika będzie znajdował się jeden lub kilka transponderów. W zależności od wykonania czytnika strefa odczytu może mieć kształt mniej lub bardziej kierunkowy i sięgać na odległość od kilkudziesięciu centymetrów do kilku metrów. Stosownie do przewidywanych sytuacji czytnik powinien realizować właściwy protokół komunikacji w systemie RFID, który w przypadku obecności wielu transponderów będzie również obejmował zasady arbitrażu przy nawiązywania łączności. W podstawowym przypadku łączności pomiędzy jednym transponderem, a czytnikiem realizowany protokół transmisji powinien zapewniać kodowanie sygnału umożliwiające co najmniej wykrywanie pojedynczych błędów. Czytnik i transpondery powinny być kompatybilne pod względem stosowanej techniki RFID (częstotliwość łączności radiowej, rodzaj modulacji, zgodność protokołów transmisji, zgodność zasad kodowania informacji), w przeciwnym przypadku identyfikacja transponderów w systemie nie będzie możliwa.

2.5. Właściwości systemów RFID

Systemy RFID różnią się pod wieloma względami:

- częstotliwością radiową pracy i zasięgiem identyfikacji;
- rodzajem pamięci i pojemnością pamięci transponderów;
- przeznaczeniem danych;

– bezpieczeństwem.

Częstotliwość pracy jest podstawowym parametrem wpływającym na właściwości systemu RFID, takie jak zasięg, szybkość transmisji, odporność na zakłócenia. Większość systemów używanych komercyjnie wykorzystuje albo częstotliwości w zakresie 860 ÷ 960 MHz (zależnie od regionu), albo częstotliwość 13,56 MHz – pasmo HF. Oprócz wymienionych wykorzystywane są również częstotliwości w zakresie do 135 kHz – w paśmie LF oraz 433 MHz i 2,45 GHz – w paśmie UHF.

Sprzężenie indukcyjne

W pasmach LF i HF wykorzystuje się zasadę sprzężenia indukcyjnego. W tym przypadku anteny transponderów i czytnika wykonane są w formie cewek o pewnej liczbie zwojów. Energia jest przekazywana pomiędzy czytnikiem a transponderem za pośrednictwem pola magnetycznego. Wielkość przekazywanej energii jest proporcjonalna do powierzchni anteny nadawczej i powierzchni anteny odbiorczej, zależy też od wzajemnego ustawienia tych anten i możliwości pobudzenia obwodu antenowego transpondera przebiegiem o częstotliwości rezonansowej, ponieważ w stanie rezonansu w obwodzie antenowym płynie maksymalny prąd.

W sprzężeniu indukcyjnym większa dobroć obwodu antenowego wywołuje większy prąd płynący w rezonansie i większą energię wzbudzanego pola magnetycznego. Jednakże wraz ze wzrostem dobroci obwodu zmniejsza się szerokość pasma obwodu, co ogranicza maksymalną szybkość komunikacji danych w systemie. Jednocześnie obwód antenowy o dużej dobroci jest bardziej podatny na rozstrojenie spowodowane bliskością metali oraz zmianami indukcyjności i pojemności obwodu wskutek zmian temperatury otoczenia.

W pasmach LF i HF stosuje się transpondery bierne. W prostych systemach identyfikacji każdy transponder, który znajdzie się w polu aktywującym wytworzonym przez czytnik, o odpowiedniej częstotliwości i dostatecznym natężeniu, wysyła swój kodowany sygnał identyfikacyjny tak długo, jak znajduje się w polu. System działa poprawnie tylko wtedy, gdy w strefie identyfikacji znajduje się jeden transponder. W zaawansowanych systemach, w których czytnik może wydawać polecenia zidentyfikowanym transponderom, są stosowane protokóły komunikacji z arbitrażem kolizji, umożliwiające po wykonaniu sekwencji procedur identyfikację, a następnie odczyt wielu transponderów znajdujących się jednocześnie w strefie kontrolowanej przez czytnik.

Istotnym czynnikiem ograniczającym zasięg strefy identyfikacji są ograniczenia administracyjne limitujące maksymalne natężenie pola magnetycznego wytwarzanego przez antenę czytnika.

W systemach ze sprzężeniem indukcyjnym do przesyłania informacji z transpondera do czytnika stosuje się binarną modulację amplitudy (ASK) pola aktywującego, co jest osiągane poprzez sterowanie zmianami obciążenia obwodu antenowego transpondera z

jego procesora. W czasie przeznaczonym na odbiór sygnału z transpondera czytnik generuje zmienne, sinusoidalne pole magnetyczne o stałej amplitudzie. Istnieją również systemy, w których transponder wysyła sygnał z przełączaniem częstotliwości (FSK) lub z modulacją fazy sygnału.

W celu przesyłania informacji z czytnika do transpondera zawierających polecenia dotyczące transpondera lub dane do zapisania w jego pamięci najczęściej stosowana jest modulacja amplitudy, a rzadziej fazy fali nośnej.

Zasięg identyfikacji zależy od usytuowania (kierunku) anteny transpondera względem anteny czytnika. W przypadku sprzężenia indukcyjnego maksymalny zasięg uzyskuje się, gdy linie pola magnetycznego wytwarzanego przez antenę czytnika są prostopadłe do płaszczyzny zwojów cewki antenowej transpondera. Oznacza to, że antena transpondera powinna być sytuowana w płaszczyźnie równoległej do anteny czytnika. Jeżeli linie pola są równoległe do cewki transpondera, to nie zachodzi sprzężenie między cewkami antenowymi i transponder nie może być odczytywany. Z tych względów w rzeczywistych rozwiązaniach stosuje się systemy antenowe czytnika z wieloma cewkami np. dwoma równoległymi umieszczonymi w pewnej odległości od siebie (strefa identyfikacji znajduje się w obszarze pomiędzy cewkami – tzw. bramka) lub z czterema cewkami tworzącymi tunel (strefa identyfikacji znajduje się wewnątrz tunelu). Stosowanie wielu cewek antenowych wymaga odpowiedniej synchronizacji fazowej prądów wzbudzających.

Sprzężenie propagacyjne

Sprzężenie propagacyjne w komunikacji pomiędzy biernym transponderem i czytnikiem stosowane jest w pasmach UHF. Oba urządzenia wyposażone są wtedy w anteny dipolowe. W tym przypadku zasada komunikacji dotyczy modulacji współczynnika odbicia fali radiowej (tzw. rozproszenia wstecznego, ang. backscatter). Polega to na tym, że część energii fali wytwarzanej przez antenę czytnika jest odbijana w kierunku przeciwnym niż kierunek fali wytwarzanej przez czytnik. Transponder może przesyłać informację zmieniając obciążenie obwodu odbierającego falę, a wskutek tego współczynnik odbicia fali. Czytnik odbierając zmiany natężenia pola może demodulować sygnał i odtwarzać dane.

Systemy RFID mogą pracować w różnych pasmach częstotliwości radiowych. Nie można wskazać najkorzystniejszego pasma ponieważ różne właściwości systemu wynikające ze stosowanej częstotliwości są przydatne w różnych zastosowaniach.

2.6. Właściwości użytkowe transponderów LF

Transpondery LF pracują w paśmie częstotliwości 135 kHz. W tym paśmie częstotliwości, w porównaniu z innymi obserwuje się względnie mały wpływ metali w otoczeniu transpondera na jego charakterystyki. Z tego powodu transpondery te mogą być mocowane jako identyfikatory do obiektów metalowych, takich jak maszyny i ich części. Pole

LF przenika przez różne materiały, w tym przez wodę i tkanki ciała i umożliwia wykorzystanie transponderów LF do identyfikacji zwierząt (implanty), a także osób wkraczających do stref zagrożenia (identyfikatory dostępu w formie kart, żetonów, naklejek i innych). Z drugiej strony przydatność transponderów LF w środowisku przemysłowym może być ograniczona ze względu na poziom zakłóceń wytwarzanych przez maszyny i urządzenia elektryczne.

W większości oferowanych obecnie systemów RFID korzystających z pasma LF w danym momencie możliwy jest odczyt tylko jednego transpondera. Obecność wielu transponderów w strefie identyfikacji może wiązać się z identyfikacją jednego losowo wybranego transpondera lub brakiem możliwości identyfikacji. Pasmo LF nie umożliwia również szybkiej transmisji danych, co wpływa na ograniczenie wielkości danych przesyłanych w jednym cyklu transmisji.

W transponderach LF najczęściej stosowane są częstotliwości fali nośnej 125 kHz i 134,2 kHz. Częstotliwości te są udostępnione do zastosowań RFID praktycznie na całym świecie, w tym oczywiście w Polsce. Podstawowym wymaganiem, które musi spełniać system RFID działający w zakresie częstotliwości 119-135 kHz jest ograniczenie natężenia pola magnetycznego w odległości 10 m od anteny do 66 dBμA/m.

Postać transpondera LF zależy od zastosowania. W systemach kontroli dostępu jest to karta zbliżeniowa lub żeton (brelok) wymagające przyłożenia do czytnika sterującego dostępem (na ogół poprzez odblokowanie drzwi). W immobilizerach samochodowych transpondery zaprasowywane są w główce kluczyka, a przez włożenie kluczyka do stacyjki zbliża się go do umieszczonej współosiowo cewki czytnika. Do identyfikacji zwierząt domowych stosowane są transpondery umieszczone w kapsułkach, które mogą być wstrzykiwane pod skórę, natomiast do identyfikacji zwierząt hodowlanych mogą być również stosowane transpondery wykonane w formie kolczyków do kolczykowania.

2.7. Właściwości użytkowe transponderów HF

Pasywne transpondery HF pracują w paśmie 13,56 MHz (zakres 13,553 - 13,567 MHz), które jest udostępnione na świecie i również w Polsce, jako pasmo do zastosowań przemysłowych, naukowych i medycznych (ISM). Pasmo to jest nielicencjonowane. Powszechna dostępność tego pasma jest jednym z powodów popularności systemów RFID je wykorzystujących. Jednak w różnych regionach świata dopuszczalne wartości mocy promieniowanej lub natężenia pola się różnią.

Pole o częstotliwości 13,56 MHz przenika przez różne materiały, w tym przez wodę i tkanki ciała, lecz transpondery pracujące w tym paśmie są bardziej wrażliwe na oddziaływanie metali w otoczeniu niż transpondery LF. Z kolei systemy HF są mniej podatne na zakłócenia wytwarzane przez urządzenia elektryczne niż systemy LF.

Podstawowymi zaletami systemów HF w porównaniu z systemami LF jest mniejszy koszt wyprodukowania transponderów, większa szybkość komunikacji (możliwe jest zwiększenie rekordu przesyłanych danych) oraz zdolność odczytu wielu transponderów jednocześnie. Ta ostatnia właściwość umożliwia ich stosowanie do automatycznej ewidencji obiektów. Niższy koszt produkcji wynika z możliwości wykonania tańszej anteny transpondera, której w tym zakresie częstotliwości wystarcza kilka zwojów, przez co może być ona wykonana jako nadruk z lakieru przewodzącego na podłożu dielektrycznym. Grubość transpondera łącznie z układem scalonym może być mniejsza niż 0,1 mm. Pozwala to na umieszczanie transponderów w dokumentach, np. w elektronicznych paszportach, czy w naklejkach używanych do naklejania na dokumentach papierowych lub jako etykiety na produktach.

Możliwość wielokrotnego zapisu danych w niektórych rodzajach transponderów HF udostępnia zastosowania z tym związane, np. elektroniczny bilet komunikacji publicznej, karta biblioteczna i inne. Przyczynia się również do zwiększenia bezpieczeństwa w systemach kontroli dostępu (możliwość zapisu danych biometrycznych). Bezstykowe inteligentne karty RFID stają się kartami płatniczymi i kredytowymi następnej generacji. Są one wykorzystywane jako różnego rodzaju karty wstępu i bilety elektroniczne, a jednym z podstawowych powodów ich wprowadzenia jest ochrona informacji. Stosunkowo nową klasą zastosowań systemów RFID w paśmie HF są techniki komunikacji w polu bliskim (Near Field Communication - NFC) promowane jako wygodny i bezpieczny sposób przeprowadzania różnych transakcji i wnoszenia opłat za pomocą osobistego terminala.

Rozmiary transponderów HF są różne. Ogólnie im większa powierzchnia anteny, tym większą energię pola wytworzonego przez czytnik przejmuje transponder, co przekłada się na większy zasięg identyfikacji. W praktyce ze względu na ograniczenia administracyjne dotyczące natężenia pola wytwarzanego przez czytniki zasięg systemów HF jest ograniczony do nie więcej niż 1 m. W Polsce podstawowym warunkiem, który musi spełniać system RFID działający w paśmie częstotliwości 13,56 MHz jest ograniczenie natężenia pola magnetycznego w odległości 10 m od anteny do 66 dBμA/m.

Podobnie jak w systemach LF orientacja transpondera względem anteny czytnika ma istotny wpływ na zasięg identyfikacji. W przypadku transpondera, którego antena jest wykonana w postaci płaskiej cewki, optymalne ze względu na wielkość sprzężenia indukcyjnego jest umieszczenie anteny transpondera równolegle do płaszczyzny anteny czytnika. Jeżeli antena takiego transpondera jest prostopadła, zasięg jest redukowany praktycznie do zera. Ze względu na szybkość transmisji możliwe jest odczytywanie do 50 transponderów w jednym cyklu odczytu (odczyt bezkolizyjny), tj. w okresie 20 ms. W zastosowaniach typu karta płatnicza zasięg identyfikacji jest celowo ograniczany ze względów bezpieczeństwa.

2.8. Właściwości użytkowe transponderów UHF

Zakres UHF obejmuje radiowe częstotliwości od 300 MHz do 3 GHz. Dla potrzeb systemów RFID wykorzystywane są trzy podzakresy: pasmo 433 MHz, różne częstotliwości w podzakresie 860 - 960 MHz i pasmo ISM 2,45 GHz. Spośród trzech wymienionych największe znaczenie ma podzakres 860 – 960 MHz. Jednakże istotnym mankamentem systemów w podzakresie 860 – 960 MHz jest brak wspólnego, światowego zakresu częstotliwości (w odróżnieniu od pasma LF i HF, co do których wymagania obowiązujące w Europie i Ameryce Płn. nie różnią się zasadniczo). W Ameryce systemy UHF pracują w zakresie 902 – 928 MHz, w Europie w zakresie 860 – 868 MHz, a w Japonii 950 – 956 MHz.

Przesyłanie danych pomiędzy biernymi transponderami UHF i czytnikiem jest realizowane z wykorzystaniem techniki rozproszenia wstecznego. Elektrolity i metale znajdujące się w polu czytnika UHF zaburzają działanie systemu. Transponder odbiera sygnał radiowy z czytnika, moduluje go i promieniuje z powrotem w kierunku czytnika. Systemy RFID pracujące w pasmach UHF w porównaniu z systemami HF mają większy zasięg i szybkość działania. Protokóły unikania kolizji stosowane w paśmie UHF różnią się od stosowanych w paśmie HF i umożliwiają w praktyce w jednym cyklu odczyt do 200 transponderów (w paśmie HF tylko do 50-ciu).

Podstawowe właściwości transponderów UHF to:

– typowy zasięg identyfikacji - 3 ÷ 6 m,
– możliwość umieszczania w niemetalowych obudowach np. w etykietach, kartach,
– duża szybkość przesyłania danych,
– szybki protokół antykolizyjny pozwalający na odczyt do 200 transponderów w strefie zasięgu,
– najprostszym wykonaniu (etykiety) mają tylko 96 bitów pamięci dla numeru seryjnego.

2.9. Zastosowania i normalizacja techniki RFID

Identyfikacja z wykorzystaniem częstotliwości radiowych (RFID) jest jedną z najszybciej rozwijających się i przynoszących największe korzyści technik automatycznego gromadzenia danych (Automatic Data Collection, ADC). Do popularyzacji technik RFID przyczyniło się opracowanie standardów, usprawnienia właściwości oferowanych systemów i obniżenie kosztów wdrożenia.

Technika RFID ma kilka istotnych zalet w porównaniu z innymi technikami identyfikacji i gromadzenia danych:

– czytnik nie musi bezpośrednio "widzieć" transpondera, co umożliwia stosowanie RFID tam, gdzie inne sposoby identyfikacji np. za pomocą kodów kreskowych są nieprzydatne,

- eliminacja czynności manualnych wymaganych do identyfikacji,
- możliwość prawie równoczesnego dokonywania identyfikacji wielu obiektów,
- duża szybkość działania – do kilkuset odczytów w ciągu sekundy,
- może być stosowana w środowisku o wysokim poziomie zanieczyszczeń i innych warunkach istotnie odbiegających od normalnych,
- umożliwia automatyzację procesu identyfikacji,
- zapewnia dość wysoką pewność procesu identyfikacji,
- może umożliwić lokalizację obiektów poprzez identyfikację,
- identyfikacja w połączeniu z układem sterowania może być wykorzystana do kontroli dostępu lub zezwolenia na rozpoczęcie procesów przemysłowych,
- możliwość zapisu danych pozwala na aktualizację informacji o obiekcie i śledzenie jego historii,
- możliwość kodowania informacji w transponderze, kodowania protokołu komunikacji i ochrony obiektu przed nieuprawnioną identyfikacją,
- bardzo trudne kopiowanie danych identyfikacyjnych.

Wadami techniki RFID są:

- konieczność umieszczania transpondera na obiekcie podlegającym identyfikacji,
- możliwość utraty transpondera przez identyfikowany obiekt (transponder nie jest trwale skojarzony z obiektem),
- możliwość zniszczenia transpondera i utraty możliwości identyfikacji obiektu,
- uniemożliwienie identyfikacji w wyniku niekorzystnego usytuowania anten czytnika i transpondera,
- uniemożliwienie identyfikacji poprzez zaekranowanie transpondera.

3. Możliwości zastosowania urządzeń RFID do ograniczania ryzyka związanego z użytkowaniem maszyn

System RFID jest przewidziany do identyfikacji za pomocą częstotliwości radiowych. Idea systemu przewiduje wykorzystanie transponderów będących identyfikowanymi elementami. W przypadku systemu RFID identyfikacja oznacza odczyt cyfrowej, unikatowej informacji z transpondera (kod identyfikacyjny) i skojarzenie tej informacji z zawartością komputerowej bazy danych. Wynik tej komputerowej operacji implikuje działanie zdefiniowane w ramach systemu. Działanie systemu niesie informację o tym, że określony transponder znalazł się w polu czytnika związanego z systemem.

Identyfikacja w systemie RFID nie jest wykrywaniem człowieka lub części jego ciała lub innych obiektów o podobnej charakterystyce (np. próbników testowych), tak jak to ma miejsce w przypadku stosowania wyposażenia ochronnego elektroczułego (kurtyny świetlne, skanery laserowe, systemy wizyjne) lub czułego na nacisk (maty, podłogi, krawędzie, listwy,

zderzaki, linki, druty), gdzie oddziaływanie w strefie czułości wyposażenia ochronnego ma charakter bezpośredni. W przypadku systemu RFID identyfikacja dotyczy transpondera i w celu zapewnienia równoważności identyfikacji i wykrywania należy zapewnić wzajemnie jednoznaczne i trwałe przyporządkowanie transpondera do obiektu, który powinien być wykryty za pomocą urządzenia bezpieczeństwa.

Od strony technicznej identyfikacja RFID wymaga zastosowania odpowiednich czytników, w których istotnym elementem jest antena. Możliwość identyfikacji zawsze jest ograniczona limitowaną odległością od transpondera (sięgającą maksymalnie kilku metrów i zależną od zastosowanej częstotliwości). Ograniczenie to wynika z przepisów dotyczących wykorzystania wybranego pasma radiowego oraz konieczności uwzględnienia wymagań kompatybilności elektromagnetycznej. Z drugiej strony warunki uzyskania sprzężenia radiowego mogą ulegać zmianie i powodować zmienność strefy identyfikacji. Należy spodziewać się, że możliwość identyfikacji będzie silnie uwarunkowana czynnikami środowiskowymi.

Przyporządkowanie transpondera do wykrywanego obiektu będzie skuteczne zawsze z prawdopodobieństwem mniejszym od jedności i stąd w zastosowaniach techniki RFID w urządzeniach bezpieczeństwa należy uwzględniać obniżoną pewność ich działania wynikającą z tego faktu. Z kolei właściwość identyfikacji występująca w systemie RFID oraz możliwość wykorzystania transponderów z funkcją zapisu danych stwarza możliwości rozszerzenia działania urządzeń bezpieczeństwa RFID o dotychczas niedostępne funkcjonalności. Dotyczy to możliwości przyporządkowywania identyfikowanym obiektom dodatkowych danych istotnych ze względów bezpieczeństwa, które dodatkowo mogą być aktualizowane stosownie do okoliczności związanych z bezpieczeństwem.

Wskazane w punkcie 2.9 zalety techniki RFID są czynnikiem podnoszącym jej atrakcyjność w aspekcie możliwości zastosowania do ograniczania ryzyka związanego z użytkowaniem maszyn. Natomiast wskazane wady techniki RFID należy traktować jako potencjalne źródła defektów urządzeń wykonanych w tej technice i odpowiednio je analizować pod kątem stwarzania sytuacji niebezpiecznych.

Obecnie rozpatruje sie następujące zastosowania techniki RFID w aspekcie redukcji ryzyka użytkowania maszyn:

– zastosowanie polegające na skojarzeniu stanu identyfikacji w systemie RFID z sytuacją odpowiadającą bezpieczeństwu przy użytkowaniu maszyny,
– zastosowanie polegające na skojarzeniu stanu identyfikacji w systemie RFID z wystąpieniem sytuacji zagrożenia przy użytkowaniu maszyny,
– inne zastosowania techniki RFID do redukcji ryzyka użytkowania maszyny nie powiązane bezpośrednio ze związanym z bezpieczeństwem systemem sterowania maszyny.

3.1. Zastosowanie polegające na skojarzeniu stanu identyfikacji w systemie RFID z sytuacją bezpieczeństwa

Zastosowanie, w którym stan identyfikacji w systemie RFID odpowiada sytuacji bezpieczeństwa stosuje się do uruchamiania ruchów roboczych maszyny związanych z występowaniem zagrożeń. Zastosowanie to szczególnie nadaje się do stwierdzania warunków bezpieczeństwa takich jak wymagane odpowiednie wzajemne położenie określonych części maszyny względem siebie lub odpowiednia pozycja operatora względem strefy zagrożenia maszyny.

Obecnie spotykane są dwa zastosowania takiej funkcji bezpieczeństwa:

– zastosowanie systemu RFID w urządzeniu blokującym osłony ruchomej – dołożenie dodatkowej funkcji identyfikacji „klucza” (transponder) zapobiega obchodzeniu funkcji bezpieczeństwa poprzez użycie drugiego „klucza”. Dodatkową funkcjonalność urządzenia blokującego osłony ruchomej można już znaleźć w produktach kilku znanych producentów wyposażenia bezpieczeństwa maszyn.
– zastosowanie stacyjek z kluczem i systemem RFID do uruchamiania maszyn lub wyboru rodzaju pracy – zastosowanie systemu RFID (transponder w kluczu – system podobny do immobilizera samochodowego) uniemożliwia osobom nieuprawnionym uruchomienie maszyn szczególnie niebezpiecznych lub wybór rodzaju pracy maszyny wiążący się ze zwiększonym ryzykiem, czym zapobiega obchodzeniu funkcji bezpieczeństwa polegającej na ograniczaniu uprawnień do wykonania określonych czynności sterowania.

Wykorzystanie tego rozwiązania wymaga umieszczenia transpondera na obiekcie podlegającym identyfikacji tj. „kluczu” urządzenia blokującego lub kluczu zamka stacyjki oraz odpowiednio zminiaturyzowanego czytnika w urządzeniu ryglującym lub w zamku stacyjki. Identyfikacja transpondera powinna nastąpić tylko po włożeniu „klucza” do urządzenia blokującego lub po włożeniu klucza do zamka stacyjki. Wymaga to zastosowania czytników o bardzo niewielkim zasięgu identyfikacji, co obecnie jest technicznie realizowalne w zadowalający sposób. W rozwiązaniu tym elementy RFID uczestniczą w realizacji dodatkowej funkcji bezpieczeństwa sprawdzającej zgodność wykorzystywanych kluczy z urządzeniem blokady lub zamkiem stacyjki. Podstawowe funkcje bezpieczeństwa realizowane są tradycyjnie.

Wady techniki RFID takie jak: możliwość utraty transpondera przez identyfikowany obiekt (klucz) lub możliwość zniszczenia transpondera prowadzą do sytuacji uniemożliwiającej identyfikację, a więc blokującej możliwość zainicjowania ruchu maszyny. Są to sytuacje odpowiadające uszkodzeniom bezpiecznym. Także uniemożliwienie identyfikacji w wyniku niekorzystnego usytuowania anten czytnika i transpondera oraz

uniemożliwienie identyfikacji poprzez zaekranowanie transpondera nie prowadzą do sytuacji wiążących się z wystąpieniem wysokiego ryzyka.

3.2. Zastosowanie polegające na skojarzeniu stanu identyfikacji w systemie RFID z sytuacją zagrożenia

Zastosowanie, w którym stan identyfikacji w systemie RFID odpowiada sytuacji zagrożenia powinno się odnosić do sytuacji samoczynnego zatrzymania ruchów roboczych maszyny związanych z występowaniem zagrożeń. Takie zastosowanie jest analogiczne do zatrzymania samoczynnego na skutek aktywizacji wyposażenia ochronnego poprzez wykrywanie człowieka lub części jego ciała. Wymaga ono wyposażenia osób chronionych w transpondery i stworzenia warunków stałego ich noszenia w odpowiedni sposób przy sobie.

Czytnik urządzenia RFID powinien charakteryzować się zasięgiem identyfikacji co najmniej kilkadziesiąt centymetrów. Należy rozwiązać problem miejsca noszenia transpondera przez pracownika, położenia anteny czytnika tak, aby transponder mógł znaleźć się w zasięgu identyfikacji przy uwzględnieniu możliwych pozycji pracownika w strefie identyfikacji.

Wszystkie sytuacje zaliczane do wad systemów RFID, takie jak: konieczność zabrania transpondera przez pracownika, możliwość utraty transpondera przez pracownika, możliwość zniszczenia transpondera (przypadkowego lub celowego), niekorzystne usytuowanie się anten czytnika i transpondera uniemożliwiające identyfikację, zaekranowanie transpondera uniemożliwiające identyfikację (przypadkowe lub celowe) są sytuacjami groźnymi ze względu na bezpieczeństwo i powinny być rozpatrywane analogicznie do możliwości wystąpienia defektów niebezpiecznych.

Można spodziewać się, że w związku z powyższym prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego w związanym z bezpieczeństwem systemie RFID wykrywającym sytuację zagrożenia poprzez identyfikację transpondera będzie istotnie wyższe niż w podobnych systemach wykorzystujących urządzenia ochronne. Stąd zastosowanie systemu RFID w funkcjach bezpieczeństwa zatrzymania samoczynnego powinno mieć miejsce tylko w przypadkach szczególnych, ograniczonych do warunków środowiskowych, w których nie sprawdzają się rozwiązania oparte na zastosowaniu wyposażenia ochronnego wykrywającego człowieka lub części jego ciała. Takie rozwiązanie powinno być wyłącznie uzupełniającym środkiem bezpieczeństwa towarzyszącym innym technicznym środkom bezpieczeństwa.

3.3. Inne zastosowania techniki RFID niezwiązane z funkcjami bezpieczeństwa

Technika RFID znajduje również zastosowanie w ograniczaniu ryzyka związanego z użytkowaniem maszyn poprzez działania niezwiązane bezpośrednio ze sterowaniem maszyną. Dotyczą one:

- kontroli i ewidencji dostępu do przemysłowych stref zagrożenia – jest to zastosowanie analogiczne do systemów kontroli dostępu w obiektach biurowych i innych – pozwala na monitorowanie liczby i czasu pobytu pracowników w strefach zagrożenia,
- ewidencja i nadzorowanie czasu użytkowania elementów maszyn istotnych ze względu na bezpieczeństwo, dla których czas ten jest ograniczony – prowadzone jest również monitorowanie parametrów środowiskowych (np. temperatury) i sytuacji, które mają wpływ na przyspieszoną degradację właściwości użytkowych takich elementów.

Kontrola i ewidencja, które wymienione zostały powyżej, prowadzone są w oparciu o identyfikację transponderów, w które wyposażono pracowników, lub które umieszczono na częściach maszyn. Możliwe jest tu bezpośrednie monitorowanie czasu pobytu ludzi w strefach zagrożenia lub eksploatacji elementów maszyn poprzez wykorzystanie transponderów z opcją zapisu danych. Do monitorowania parametrów środowiskowych konieczne jest zastosowanie transponderów wyposażonych w odpowiednie czujniki.

Systemy RFID realizujące powyższe funkcje nie są związane bezpośrednio z systemami sterowania maszyn, więc nie podlegają analizom z punktu widzenia występowania uszkodzeń niebezpiecznych. Niemniej realizowane przez nie funkcje dodatkowe mają istotny walor prewencyjny, obniżający ryzyko użytkowania maszyn. Obecnie są często wdrażane w górnictwie podziemnym.

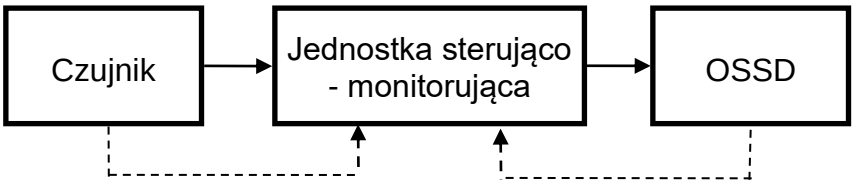
4. Parametry charakterystyczne urządzeń bezpieczeństwa wykorzystujących technikę RFID

Obecnie brak jest opracowań normatywnych określających wymagania szczegółowe w odniesieniu do urządzeń bezpieczeństwa wykorzystujących technikę RFID. Ponieważ ze względu na zasadę działania (bezdotykowe wykrywanie transpondera) urządzenia te najbardziej zbliżone są do elektroczułych urządzeń ochronnych, to za podstawę do określenia ich parametrów charakterystycznych przyjęto metodykę prezentowaną w normie PN-EN 61496-1:2014-02.

4.1. Podstawowe właściwości elektroczułych urządzeń ochronnych

Elektroczułe urządzenie ochronne jest zespołem współpracujących elementów przeznaczonych do wykrywania chwilowego naruszenia jego strefy wykrywania lub stwierdzania w niej stałej obecności obiektów naruszających (wykrywanie obecności). W typowej strukturze elektroczułego urządzenia ochronnego wyróżniane są co najmniej następujące elementy składowe: czujnik, jednostka sterująco-monitorująca i element

przełączający sygnału wyjściowego (OSSD – ang. Output Signal Switching Device) i/lub związany z bezpieczeństwem interfejs transmisji danych (rys. 2). W strukturze urządzenia mogą również występować elementy opcjonalne, takie jak realizujące funkcje mutingu (chwilowe, automatyczne zawieszanie funkcji wykrywania) lub blankingu (umożliwia czasowe przebywanie w strefie wykrywania obiektów większych od progu wykrywania).



Rys. 2. Podstawowa struktura elektroczułego urządzenia ochronnego

Elementy składowe elektroczułego urządzenia ochronnego pełnią następujące funkcje:

– czujnik urządzenia ochronnego – zespół elementów wykorzystujących bezdotykową metodę detekcji sytuacji, które mogą być kojarzone z sytuacjami zagrożenia występującymi podczas użytkowania maszyn. Pobudzenie czujnika jest zdarzeniem interpretowanym jako naruszenie strefy wykrywania urządzenia ochronnego. (np. utworzenie obwodu optycznego z nadajnika i odbiornika promieniowania podczerwonego, którego przerwanie oznacza naruszenie strefy wykrywania optoelektronicznego urządzenia ochronnego);
– jednostka sterująco-monitorująca urządzenia ochronnego – zespół elementów odpowiedzialnych za analizę stanu sygnałów odbieranych z czujnika urządzenia ochronnego i wygenerowanie sygnału wyjściowego przez element (lub elementy) przełączający sygnału wyjściowego. Oprócz monitorowania stanu czujnika i sterowania stanem OSSD jednostka sterująco-monitorująca wykonuje również funkcje diagnostyczne, których celem jest zmniejszenie prawdopodobieństwa wystąpienia defektu niebezpiecznego urządzenia ochronnego;
– element przełączający sygnału wyjściowego (OSSD) i/lub związany z bezpieczeństwem interfejs transmisji danych – OSSD generuje sygnał wyjściowy z urządzenia ochronnego, który przekazany do związanego z bezpieczeństwem systemu sterowania maszyny powoduje jej przejście do stanu bezpieczeństwa. Gdy OSSD jest w stanie ON oznacza to, że strefa wykrywania urządzenia ochronnego nie została naruszona (czujnik nie został aktywowany), i że jednostka sterująco-monitorująca nie stwierdziła defektu urządzenia. Stan OFF oznacza naruszenie strefy wykrywania (czujnik został aktywowany) lub wewnętrzny defekt urządzenia. Związany z bezpieczeństwem interfejs transmisji danych jest połączeniem bezpośrednim do

podsystemu szeregowej transmisji danych bezpieczeństwa, które pełni alternatywną funkcję przesyłania stanów ON i OFF do związanego z bezpieczeństwem systemu sterowania maszyny.

Funkcja bezpieczeństwa układu sterowania maszyny wykorzystująca dane urządzenie ochronne powinna zatrzymywać maszynę i nie zezwalać na jej uruchomienie po przejściu OSSD do stanu OFF oraz zezwalać na jej uruchomienie po przejściu OSSD do stanu ON.

4.2. Podstawowe parametry charakterystyczne elektroczułych urządzeń ochronnych

Podstawowym parametrem charakterystycznym elektroczułych urządzeń ochronnych jest czas zadziałania. Jest to maksymalny czas upływający od momentu wystąpienia zdarzenia prowadzącego do aktywacji czujnika urządzenia ochronnego do momentu przejścia OSSD do stanu OFF. Czas zadziałania powinien zostać określony przez producenta i nie powinien podczas normalnego użytkowania ulegać samoczynnie zmianie. Nastawianie czasu zadziałania, jeżeli jest możliwe, powinno wymagać użycia klucza, słowa kluczowego (hasła) lub specjalnego narzędzia (może być to narzędzie programowe).

Funkcja czułości elektroczułego urządzenia ochronnego powinna być efektywna w strefie wykrywania określonej przez producenta. Do określenia strefy wykrywania zwykle niezbędne jest określenie wymiarów geometrycznych przestrzeni, w której powinno zachodzić wykrywanie (określenie granic strefy wykrywania) oraz tzw. progu wykrywania tj. minimalnych wymiarów geometrycznych obiektu, który powinien zostać wykryty. Przez wykrycie należy rozumieć aktywację czujnika urządzenia ochronnego prowadzącą do przejścia OSSD do stanu OFF w czasie nie większym niż deklarowany czas zadziałania. Strefa wykrywania elektroczułego urządzenia ochronnego powinna zostać określona przez producenta. Jeżeli może ona podlegać nastawianiu, to wymagane jest użycie klucza, słowa kluczowego (hasła) lub specjalnego narzędzia (może być to narzędzie programowe).

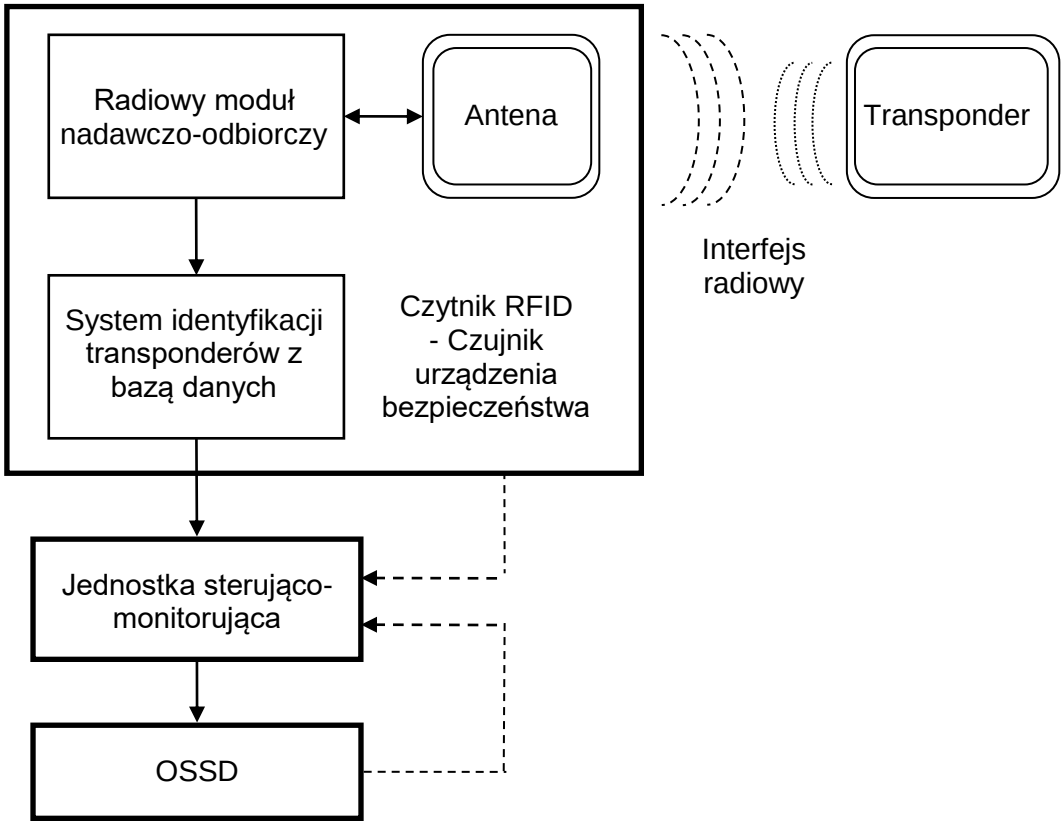
W niektórych rodzajach elektroczułych urządzeń ochronnych przylegle do strefy wykrywania może występować tzw. strefa tolerancji. W strefie tej możliwe jest pobudzenie czujnika urządzenia ochronnego, lecz nie są spełnione (gwarantowane) warunki wykrywania dotyczące czasu zadziałania lub progu wykrywania.

4.3. Urządzenie bezpieczeństwa wykorzystujące technikę RFID

Wykorzystanie techniki „identyfikacji radiowej” (RFID – ang. Radio Frequency IDentification) w budowie urządzenie bezpieczeństwa wymaga połączenia typowej struktury systemu RFID z podstawową strukturą elektroczułego urządzenia ochronnego. W nowo powstałej strukturze elementy systemu RFID powinny pełnić funkcję czujnika (rys. 3).

W czujniku urządzenia bezpieczeństwa wykorzystującego technikę RFID, tak jak w czytniku RFID, zawarte są następujące elementy:

- antena,
- radiowy moduł nadawczo-odbiorczy,
- system identyfikacji transponderów.



Rys. 3 Struktura urządzenia bezpieczeństwa wykorzystującego technikę RFID

Czujnik urządzenia bezpieczeństwa wykorzystującego technikę RFID wykrywa transpondery. Wykrywanie transponderów odbywa się poprzez ich identyfikację, która jest kilkuetapowym procesem. Jeżeli transponder znajdzie się w polu elektromagnetycznym emitowanym stale przez antenę, to korzystając z energii tego pola rozpoczyna jego modulację w sposób określony za pomocą unikatowego kodu identyfikacyjnego w nim zapisanego. Zmodulowany sygnał odbierany jest przez antenę i przekazywany do modułu nadawczo-odbiorczego, który przeprowadza jego demodulację. Zdemodulowany sygnał przesyłany jest do systemu identyfikacji transponderów, w którym sygnał jest dekodowany w celu odczytania kodu identyfikacyjnego transpondera. Odczytany kod transpondera porównywany jest z bazą kodów zawartą w systemie identyfikacji. Jeżeli kod identyfikacyjny odczytywanego transpondera znajduje się w bazie kodów to system identyfikacji generuje sygnał informujący o aktywacji czujnika urządzenia bezpieczeństwa, który przekazywany jest do jednostki sterująco-monitorującej, i która następnie wysyła sygnał zmiany stanu OSSD do stanu ON. Stan ON utrzymywany jest tak długo jak długo podtrzymywany jest stan

identyfikacji transpondera, co wiąże się z koniecznością niezakłóconej obecności transpondera w polu anteny. Przejście do stanu OFF następuje niezwłocznie po usunięciu transpondera z pola anteny lub po wystąpieniu zakłóceń uniemożliwiających poprawne odczytanie kodu identyfikacyjnego transpondera.

W celu umożliwienia działania przedstawionego powyżej urządzenia bezpieczeństwa wykorzystującego technikę RFID wymagane jest zarejestrowanie w systemie identyfikacji transponderów pewnej liczby kodów identyfikacyjnych (co najmniej jednego). W zależności od przyjętych rozwiązań rejestrację kodów identyfikacyjnych przeprowadza producent lub użytkownik urządzenia bezpieczeństwa.

Opisana powyżej zasada działania urządzenia bezpieczeństwa wykorzystującego technikę RFID wymaga zastosowań, w których stan bezpieczeństwa kojarzony jest ze stanem identyfikacji transpondera. Urządzenia tego rodzaju nie są przeznaczone do wykrywania osób lub części ich ciała wnikających do stref zagrożenia maszyn, ponieważ nie można zagwarantować odpowiednio wysokiego prawdopodobieństwa wykrywania poprzez skojarzenie osób lub części ich ciała z transponderem (prawdopodobieństwo naruszenia tego skojarzenia poprzez utratę transpondera, jego przypadkowe lub celowe zniszczenie lub zaekranowanie jest zbyt wysokie).

Natomiast opisane powyżej właściwości funkcjonalne urządzenia bezpieczeństwa wykorzystującego technikę RFID z dobrym rezultatem mogą być wykorzystane w urządzeniach zezwalających na uruchomienie maszyny tj. umożliwiających wprowadzenie jej w stan odpowiadający występowaniu zagrożeń. Wszelkie trudności i zaburzenia w odczycie kodu identyfikacyjnego transpondera lub próba wykorzystania transpondera, którego unikatowy kod identyfikacyjny nie został zarejestrowany w systemie wywołują sytuację braku identyfikacji transpondera (brak aktywacji czujnika, brak przejścia OSSD do stanu ON) i w konsekwencji niemożność uruchomienia maszyny (brak zagrożeń z tym związanych).

Obecnie wyposażenie bezpieczeństwa wykorzystujące technikę RFID o przedstawionych właściwościach funkcjonalnych stosowane jest w:

- urządzeniach bezpieczeństwa zezwalających na uruchomienie maszyny (zastępują dotychczas stosowane stacyjki z unikatowym kluczem) – rozwiązanie to uniemożliwia osobom nieuprawnionym uruchomienie maszyn szczególnie niebezpiecznych lub wybór rodzaju pracy maszyny wiążący się ze zwiększonym ryzykiem, czym zapobiega obchodzeniu funkcji bezpieczeństwa polegającej na ograniczaniu uprawnień do wykonania określonych czynności sterowania;
- urządzeniach bezpieczeństwa blokujących lub blokująco-ryglujących osłony, jako dodatkowy środek bezpieczeństwa ograniczający możliwość obchodzenia - dołożenie dodatkowej funkcji identyfikacji „klucza” (transponder) zapobiega obchodzeniu funkcji bezpieczeństwa poprzez użycie drugiego „klucza”.

4.4. Podstawowe parametry charakterystyczne urządzeń bezpieczeństwa wykorzystujących technikę RFID

Za podstawowe parametry charakterystyczne urządzeń bezpieczeństwa wykorzystujących technikę RFID należy uznać:

- strefę identyfikacji - jest to odpowiednik strefy wykrywania elektroczułego urządzenia ochronnego - strefę tę należy definiować jako największą przestrzeń wokół anteny czytnika RFID, w której możliwe jest utrzymywanie się stanu identyfikacji transpondera;
- czas zaniku identyfikacji - jest to odpowiednik czasu zadziałania elektroczułego urządzenia ochronnego - czas ten należy definiować jako maksymalny czas mierzony od momentu usunięcia transpondera poza strefę identyfikacji do momentu przejścia OSSD do stanu OFF.

W urządzeniach bezpieczeństwa wykorzystujących technikę RFID nie ma potrzeby definiowania parametru odpowiadającego progowi wykrywania elektroczułego wyposażenia ochronnego, ponieważ wymiary anteny transpondera stosowanego w urządzeniu nie są czynnikiem wpływającym na sam proces identyfikacji/zaniku identyfikacji. Natomiast wymiary anteny transpondera i anteny czytnika oraz rodzaj zastosowanego sprzężenia pomiędzy nimi determinują wielkość strefy identyfikacji. Wpływ na możliwość identyfikacji ma również wzajemne usytuowanie anten względem siebie. Najlepsze warunki do identyfikacji występują wtedy, gdy płaszczyzny obu anten są równoległe do siebie. Przy wzajemnie prostopadłych płaszczyznach anten identyfikacja może nie następować. Stąd do uzyskania stanu identyfikacji (OSSD urządzenia jest w stanie ON) wymagane jest odpowiednie pozycjonowanie transpondera w strefie identyfikacji. Uzyskanie stanu identyfikacji (przełączenie OSSD do stanu ON) zwykle wymaga zbliżenia transpondera do czytnika na mniejszą odległość niż potrzebną do uzyskania zdarzenia przeciwnego tj. uzyskania zaniku identyfikacji (przejście OSSD do stanu OFF). Występujące tu zjawisko histerezy odległości identyfikacji wynika z właściwości algorytmu działania systemu identyfikacji i jest korzystne ze względu na pewną stabilność stanów OSSD (zapobiega to przypadkom niezamierzonych zmian stanu identyfikacji np. z powodu drgań i związanym z tym niezamierzonym zatrzymaniom maszyny). Również z tego powodu, w stanie identyfikacji położenie transpondera względem anteny czytnika powinno być stabilizowane.

Sam właściwy proces stwierdzania identyfikacji/zaniku identyfikacji odbywa się w systemie identyfikacji. Stąd na wielkość czasu zaniku identyfikacji wpływ mają parametry transmisyjne łącza radiowego (częstotliwość nośna sygnału i rodzaj modulacji) oraz szybkość przetwarzania systemu identyfikacji.

Zarówno strefa identyfikacji, jak i czas zaniku identyfikacji mogą ulegać zmianie na skutek wpływu czynników środowiskowych, stąd do ich określania należy przyjmować najmniej korzystne wartości (największe zaobserwowane rozmiary strefy identyfikacji i najdłuższy zmierzony czas zaniku identyfikacji).

5. Wymagania związane ze stosowaniem techniki RFID w wyposażeniu bezpieczeństwa maszyn

Uprzednio przedstawiono możliwości wykorzystania stanu identyfikacji w urządzeniach RFID w sytuacjach bezpieczeństwa lub zagrożenia. W związanych z bezpieczeństwem elementach systemu sterowania maszyny jest to związane z realizacją następujących funkcji 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 określono wymagania dotyczące wyposażenia bezpieczeństwa wykorzystującego technikę RFID (wyposażenia RFID). Przy określaniu tych wymagań inne, związane z bezpieczeństwem użytkowania maszyn, zastosowania techniki RFID nie były 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 maszyn znajdują się w dyrektywie 2006/42/WE, lecz są one sformułowane ogólnie bez szczególnego odniesienia do urządzeń wykorzystujących technikę RFID. Wymagania szczegółowe nie zostały dotychczas ujęte w opracowaniach normalizacyjnych. Opracowano jedynie projekt rekomendacji do stosowania opracowany przez grupę VG11 z Europejskiej Koordynacji Jednostek Notyfikowanych w Zakresie Dyrektywy Maszynowej 2006/42/WE [30], który sugeruje wykorzystanie normy PN EN 61496-1:2014-02 *Bezpieczeństwo maszyn - Elektroczułe wyposażenie ochronne - Część 1: Wymagania ogólne i badania* jako podstawę do opracowania metodyki oceny zgodności z wymaganiami zasadniczymi. Wyposażenie

bezpieczeństwa stosujące technikę RFID jakkolwiek technicznie może spełniać definicję elektroczułego wyposażenia ochronnego (zespół urządzeń i/lub elementów współpracujących ze sobą w celu ochronnego wyłączania 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 PN EN 61496-1:2014-02 powinny być odpowiednio zmodyfikowane.

Do określenia wymagań wprowadzono odpowiednio zmodyfikowaną terminologię analogicznie do występującej w normie PN EN 61496-1:2014-02 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.

5.1. Wymagania dyrektywy 2006/42/WE odnoszące się do urządzeń bezpieczeństwa wykorzystujących technikę RFID

W dyrektywie 2006/42/WE w Załączniku I punkt 1.4.1 zawarto następujące wymagania ogólne dotyczące urządzeń ochronnych, które powinny być spełnione również w odniesieniu do wyposażenia bezpieczeństwa wykorzystującego technikę RFID.

„1.4 WYMAGANE WŁAŚCIWOŚCI OSŁON I URZĄDZEŃ OCHRONNYCH

1.4.1. Wymagania ogólne

Osłony i urządzenia ochronne:

- muszą być solidnej konstrukcji,
- muszą być pewnie przymocowane na swoim miejscu,
- nie mogą stwarzać żadnego dodatkowego zagrożenia,
- nie mogą być łatwe do ominięcia lub wyłączenia z działania,
- muszą być umieszczone w odpowiedniej odległości od strefy niebezpiecznej,
- mogą powodować tylko minimalne utrudnienia w obserwacji procesu produkcyjnego, oraz
- powinny umożliwiać wykonanie koniecznych prac związanych z mocowaniem lub wymianą narzędzi oraz konserwacją, przez ograniczenie dostępu wyłącznie do obszaru, w którym dana praca musi być wykonana w miarę możliwości bez konieczności demontażu osłon lub wyłączenia działania urządzeń ochronnych.”

Na etapie projektu, produkcji i wprowadzania na rynek urządzenia bezpieczeństwa wykorzystującego technikę RFID z powyższych wymagań istotne jest zapewnienie solidnej konstrukcji oraz odporności na działania prowadzące do jego ominięcia lub wyłączenia z działania. W kryteriach oceny zgodności z wymaganiami zasadniczymi należy je uwzględnić. Pozostałe wymagania mogą być uwzględnione dopiero na etapie projektowania i produkcji maszyny, w której takie urządzenia bezpieczeństwa zostaną zastosowane.

W dyrektywie 2006/42/WE w Załączniku 1 punkt 1.4.3 zawarto również następujące wymagania szczególne dotyczące urządzeń ochronnych:

„1.4.3. Wymagania szczególne dotyczące urządzeń ochronnych

Urządzenia ochronne muszą być zaprojektowane i wbudowane w układ sterowania tak, aby:

- części ruchome nie mogły zostać uruchomione dopóki znajdują się w zasięgu operatora,
- osoby nie mogły dostać się do części ruchomych znajdujących się w ruchu, oraz
- brak lub uszkodzenie jednego z ich elementów uniemożliwiał uruchomienie części lub zatrzymywał części ruchome.

Urządzenia zabezpieczające muszą być nastawiane tylko poprzez działanie zamierzone.”

Z powyższych wymagań na etapie projektu, produkcji i wprowadzania na rynek urządzenia bezpieczeństwa wykorzystującego technikę RFID wymagane jest zaprojektowanie w sposób zapewniający skuteczną realizację funkcji bezpieczeństwa, i że brak lub uszkodzenie jednego z elementów urządzenia powinien skutkować działaniem uniemożliwiającym uruchomienie tych części maszyny, które stwarzają zagrożenie. Istotne jest również zapewnienie poprzez odpowiednią konstrukcję, że urządzenie bezpieczeństwa wykorzystujące technikę RFID powinno mieć możliwość nastawiania wyłącznie poprzez

działanie zamierzone. Ww. wymagania należy uwzględnić w kryteriach oceny zgodności. Pozostałe wymagania należy uwzględniać dopiero na etapie projektowania i produkcji maszyny, w której takie urządzenia bezpieczeństwa zostaną zastosowane.

Zgodnie z wymaganiami dyrektywy 2006/42/WE niezbędne jest, aby urządzenie bezpieczeństwa wykorzystujące technikę RFID spełniało wymagania dotyczące oznakowania i instrukcji użytkowania. Wymagania zasadnicze dyrektywy są formułowane bardzo ogólnie. Z tego względu niezbędne jest ich uzupełnienie o wymagania szczegółowe, które pozwalają dokładniej sprawdzić spełnienie wymagań zasadniczych.

5.2. Wymagania szczegółowe odnoszące się do urządzeń bezpieczeństwa wykorzystujących technikę RFID

Wymagania szczegółowe odnoszące się do urządzeń bezpieczeństwa wykorzystujących technikę RFID należy sformułować w następujących kategoriach:

– wymagań funkcjonalnych,
– wymagań projektowych,
– wymagań środowiskowych,
– wymagań dotyczących oznakowania w celu bezpiecznego użytkowania,
– wymagań dotyczących zawartości dokumentacji towarzyszącej (instrukcji dla użytkownika).

5.3. Wymagania funkcjonalne

Wymagania funkcjonalne dotyczące wyposażenia RFID należy formułować w następujących obszarach:

– działania normalnego,
– funkcji identyfikacji,
– 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 tramspondera 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 identyfikacji

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.

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 pilotażowe 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.

5.4. Wymagania projektowe

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 (OSSD),
- 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: nie przekraczająca 10% wartości skutecznej napięcia w zakresie harmonicznych od 2-giej do 5-tej i 2% wartości skutecznej napięcia w zakresie harmonicznych od 6-tej do 30-tej,

– 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 przetwornic napięcia:
  - napięcie: 0,9 do 1,1 napięcia znamionowego,
  - tętnienia (międzyszczytowe): nie przekraczające 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 tramspondera 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 PN EN 61496-1:2014-02.

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 przetężeniem.

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 związanego 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 PN EN 61496-1:2014-02. 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 PN EN 61496-1:2014-02.

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, programowanie, 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.

5.5. Wymagania środowiskowe

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

Zaburzenia elektryczne

Urządzenie RFID powinno być odporne na zaburzenia elektryczne, w tym wchodzące w zakres kompatybilności elektromagnetycznej (odporność na serie szybkich elektrycznych stanów przejściowych, odporność na udary elektryczne, odporność na promieniowane pole elektromagnetyczne, odporność na wyładowania elektrostatyczne).

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 wewnętrznie 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 w odniesieniu do pierwotnego napięcia zasilania.

W zakresie kompatybilności elektromagnetycznej 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 PN EN 61496-1:2014-02 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 elektromagnetycznej 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.

5.6. Wymagania dotyczące oznakowania

Wymagania dotyczące oznakowania obudowy w celu bezpiecznego użytkowania, których spełnienie powinno zostać potwierdzone w procesie oceny zgodności urządzeń bezpieczeństwa wykorzystujących technikę RFID dotyczą:

– identyfikacji urządzenia (nazwa, producent, typ, numer seryjny),
– rozmiarów strefy identyfikacji,
– wartości czasu zaniku identyfikacji,
– znamionowych parametrów zasilania,
– znamionowego poboru mocy lub prądu,
– zapewnianego stopnia ochrony obudowy,
– klasy ochronności (ze względu na możliwość porażenia prądem elektrycznym),
– ostrzeżeń o występowaniu wysokich napięć,
– zapewnianego poziomu bezpieczeństwa funkcjonalnego,
– identyfikacji zasilacza (jeżeli dotyczy),
– parametrów zabezpieczeń elektrycznych (jeżeli dotyczy),
– ostrzeżeń o występowaniu wyposażenia elektrycznego pod napięciem,
– identyfikacji elementów sygnalizacyjnych, sterowniczych i nastawczych,
– identyfikacji zacisków przyłączeniowych,

– trwałości i odporności oznakowania na czynniki środowiskowe.

5.7. Wymagania dotyczące instrukcji dla użytkownika

Wymagania dotyczące instrukcji dla użytkownika, które powinny zostać potwierdzone w procesie oceny zgodności urządzeń bezpieczeństwa wykorzystujących technikę RFID dotyczą:

– języka, w którym sporządzono dokumentację,
– informacji o zakazie podłączania innych urządzeń do wewnętrznych źródeł zasilania,
– zaleceń odnośnie przechowywania narzędzi do nastawiania,
– metod testowania doraźnego urządzenia,
– podania czasu zaniku identyfikacji (także w przypadku stosowania interfejsu komunikacyjnego),
– określenia poziomu bezpieczeństwa funkcjonalnego,
– informacji o dopuszczalnych warunkach środowiskowych,
– zaleceń dotyczących możliwości interferencji z funkcją identyfikacji,
– określenia położenia zacisków przyłączeniowych,
– podania wartości znamionowych, granicznych i charakterystyk wejść/wyjść (w tym dotyczących OSSD),
– informacji dotyczących wykonywania prac obsługowych i konserwacyjnych,
– parametrów przewodów podłączanych do urządzenia,
– wymagań związanych z obciążaniem i poborem mocy,
– wymagań związanych z wolną przestrzenią wokół urządzenia i zachowaniem odstępów,
– wykazu części zamiennych,
– wykazu zastosowanych kodów i kolorów oznakowania,
– podania wymiarów całkowitych urządzenia,
– podania usytuowania i wymiarów strefy identyfikacji,
– podania harmonogramów kontroli,
– podania metody testowania w celu potwierdzenia poprawności działania,
– podania informacji o stopniu ochrony obudowy,
– określenia przeznaczenia,
– instrukcji montażu elementów urządzenia,
– instrukcji podłączania urządzenia do systemu sterowania maszyny,
– przeciwwskazań związanych ze stosowaniem urządzenia,
– wymiarów i usytuowania środków do mocowania,

– informacji o środkach do podłączania zasilania i łączeniu oddzielnych elementów urządzenia,
– informacji o prawidłowym podłączaniu wyjść półprzewodnikowych,
– informacji o metodach prawidłowej integracji interfejsu transmisji danych.

6. Badania wyposażenia bezpieczeństwa opartego na technice RFID

6.1. Zakres badań

Wprowadzane na rynek wyposażenie bezpieczeństwa oparte na technice RFID powinno przejść badania typu obejmujące: badania właściwości funkcjonalnych, sprawdzenie cech projektowych oraz badania w zakresie odporność i wytrzymałość na czynniki środowiskowe. Zakres badań powinien obejmować:

– sprawdzenie wymagań dotyczących działania normalnego - pomiary czasu zadziałania i pomiary geometrii strefy identyfikacji,
– sprawdzenie wymagań dotyczących nastawiania parametrów i programowania bazy danych do identyfikacji - oględziny, analiza dokumentacji i próby praktyczne,
– sprawdzenie wymagań dotyczących osiąganego poziomu bezpieczeństwa funkcjonalnego - analiza dokumentacji i typowych zastosowań systemu RFID,
– sprawdzenie wymagań dotyczących zasilania elektrycznego - badania i pomiary w warunkach zasilania znamionowego i na granicach przedziału napięć dopuszczalnych,
– sprawdzenie funkcjonowania systemu RFID w stanie defektu - badania poprzez próby symulacji defektów niebezpiecznych,
– sprawdzenie wymagań dotyczących wyposażenia elektrycznego - oględziny, pomiary i próby funkcjonalne,
– sprawdzenie wymagań dotyczących funkcjonowania elementów przełączających sygnału wyjściowego (OSSD) - wykonanie testów funkcjonalnych,
– sprawdzenie wymagań dotyczących wskaźników i wyświetlaczy - sprawdzenie dokumentacji, elementów sygnalizacyjnych i próby działania,
– sprawdzenie wymagań dotyczących środków do nastawiania parametrów – analiza dokumentacji oraz próby praktyczne,
– sprawdzenie wymagań dotyczących rozłączania elementów składowych – próby funkcjonalne,
– sprawdzenie wymagań dotyczących elementów nieelektrycznych – oględziny,
– sprawdzenie środków zapobiegających uszkodzeniom pochodzącym od wspólnej przyczyny – sprawdzenie dokumentacji i oględziny,
– sprawdzenie wymagań dotyczących elementów scalonych programowalnych lub o dużej złożoności – sprawdzenie dokumentacji i oględziny,

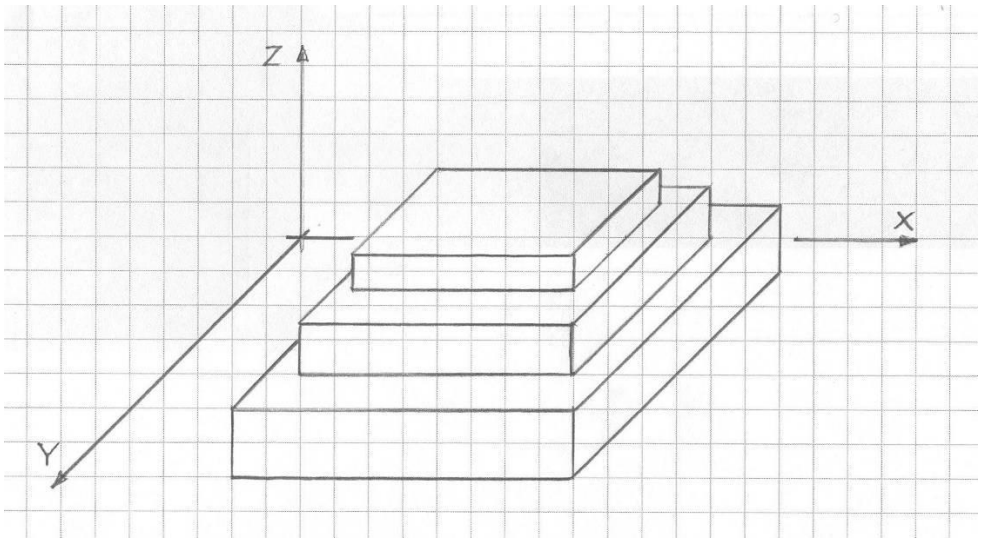
- sprawdzenie oprogramowania, programowania, projektowania funkcjonalnego obwodów scalonych – sprawdzenie dokumentacji,
- sprawdzenie wymagań dotyczących temperatury otoczenia i wilgotności względnej – pomiary czasu identyfikacji i geometrii strefy identyfikacji w warunkach narażeń na temperaturę i wilgotność,
- sprawdzenie wymagań dotyczących odporności i wytrzymałości na zaburzenia elektryczne – badanie odporności na zaniki napięcia zasilania – pomiary czasu zadziałania i geometrii strefy wykrywania w warunkach występowania zaników (badania wchodzące w zakres kompatybilności elektromagnetycznej, w tym: odporności na szybkie elektryczne stany przejściowe, zaburzenia przewodzone indukowane obcymi polami magnetycznymi i wyładowania elektrostatyczne powinny być wykonane w wyspecjalizowanym laboratorium badawczym - w ramach badań pilotażowych nie przewiduje się ich wykonania),
- sprawdzenie wymagań dotyczących odporności o wytrzymałości na środowiskowe czynniki mechaniczne – próby badawcze z zastosowaniem narażeń na wibracje i udary, pomiary czasu identyfikacji i geometrii strefy identyfikacji po zastosowaniu narażeń,
- sprawdzenie wymagań dotyczących obudów i zapewnianego przez nie stopnia ochrony – zgodnie z procedurami badań odpowiednimi do deklarowanego kodu IP, pomiary czasu identyfikacji i geometrii strefy identyfikacji po przeprowadzeniu narażeń wynikających z kodu IP.

Badania typu urządzenia bezpieczeństwa wykorzystującego technikę RFID, zgodnie z przedstawionymi wymaganiami i zakresem badań wymagają stanowisk badawczych do pomiaru czasu zaniku identyfikacji i pomiaru geometrii strefy identyfikacji. Stanowiska te mogą wymagać dostosowania do konkretnych realizacji urządzeń RFID. Z użyciem tych stanowisk należy przeprowadzić badania laboratoryjne w warunkach normalnych oraz w warunkach narażenia na czynniki środowiskowe. Pozostałe właściwości urządzenia sprawdzane są na podstawie oględzin, prób działania i analizy dokumentacji.

6.2. Pomiar geometrii strefy identyfikacji i czasu zaniku identyfikacji

Strefa identyfikacji urządzenia bezpieczeństwa wykorzystującego technikę RFID ma charakter przestrzenny, co implikuje konieczność wykonywania pomiarów w trzech osiach współrzędnych X, Y i Z układu kartezjańskiego. W badaniach pilotażowych przyjęto, że modelem strefy identyfikacji będzie piramida prostopadłościanów przedstawiona na rys. 4. Do wykonywania pomiarów niezbędne jest wykonanie stanowiska badawczego, w którym wyznaczone zostaną trzy płaszczyzny referencyjne, prostopadłe do każdej z osi współrzędnych i wyznaczające punkty zerowe każdej z nich. Podczas badania transponder

powinien być pozycjonowany na stanowisku badawczym w sposób umożliwiający określenie jego współrzędnych.



Rys. 4. Model geometryczny strefy identyfikacji urządzenia bezpieczeństwa wykorzystującego technikę RFID

Podczas badania geometrii strefy identyfikacji poprzez przemieszczanie transpondera należy wyznaczyć punkty graniczne strefy identyfikacji poprzez wyznaczenie wierzchołków i krawędzi założonego modelu geometrycznego.

Pomiar czasu zaniku identyfikacji może być wykonywany różnymi technikami. W badaniach pilotażowych wykorzystywano pomocniczy mikroprzełącznik ze stykiem NO mocowany do specjalnej podkładki. Do transpondera mocowano sprężyste cięgno pozwalające na jego szybkie usunięcie ze strefy identyfikacji. Transponder umieszczano na podkładce z mikroprzełącznikiem w taki sposób, aby zamknąć styki przełącznika. Następnie podkładka z transponderem umieszczana była w strefie identyfikacji urządzenia tak, aby transponder znajdował się na możliwie najbliżej jej granicy, przy czym napinano sprężyste cięgno. W momencie uwolnienia transpondera był on usuwany ze strefy identyfikacji przez sprężyste cięgno, przy czym następowała zmiana stanu mikroprzełącznika. Przyjęto, że jest to źródło sygnału informującego o przekroczeniu przez transponder granicy strefy identyfikacji i opuszczeniu tej strefy. Sygnał z mikroprzełącznika oraz sygnał z OSSD urządzenia doprowadzono do dwóch kanałów pomiarowych oscyloskopu. Za pomocą kursorów podstawy czasu oscyloskopu mierzono jest odstęp czasowy pomiędzy zboczami obserwowanych sygnałów, który przyjmowany był za czas zaniku identyfikacji.

6.3. Badania laboratoryjne właściwości urządzenia bezpieczeństwa wykorzystującego technikę RFID

Pilotażowe badania laboratoryjne właściwości urządzenia bezpieczeństwa wykorzystującego technikę RFID obejmowały:

- pomiar czasu zaniku identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 230 V 50 Hz (warunki klimatyczne normalne, zasilanie znamionowe);
- pomiar strefy identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 230 V 50 Hz (warunki klimatyczne normalne, zasilanie znamionowe);
- pomiar czasu zaniku identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 195,5 V 50 Hz (warunki klimatyczne normalne, zasilanie 0,85 wartości znamionowej);
- pomiar strefy identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 195,5 V 50 Hz (warunki klimatyczne normalne, zasilanie 0,85 wartości znamionowej);
- pomiar czasu zaniku identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 253 V 50 Hz (warunki klimatyczne normalne, zasilanie 1,1 wartości znamionowej);
- pomiar strefy identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 253 V 50 Hz (warunki klimatyczne normalne, zasilanie 1,1 wartości znamionowej);
- pomiar czasu zaniku identyfikacji w temperaturze (0±3) °C bez kontroli wilgotności względnej, przy zasilaniu 230 V 50 Hz (temperatura graniczna dolna, zasilanie znamionowe);
- pomiar strefy identyfikacji w temperaturze (0±3) °C bez kontroli wilgotności względnej, przy zasilaniu 230 V 50 Hz (temperatura graniczna dolna, zasilanie znamionowe);
- pomiar czasu zaniku identyfikacji w temperaturze (50±3) °C i wilgotności względnej (95±2)%, przy zasilaniu 230 V 50 Hz (temperatura graniczna górna, maksymalna wilgotność względna, zasilanie znamionowe);
- pomiar strefy identyfikacji w temperaturze (50±3) °C i wilgotności względnej (95±3)%, przy zasilaniu 230 V 50 Hz (temperatura graniczna górna, maksymalna wilgotność względna, zasilanie znamionowe);
- badanie odporności na zmiany napięcia zasilającego (w temperaturze (20±5) °C i wilgotności względnej (25÷75)%) - zmiana napięcia zasilającego od wartości znamionowej 230 V 50 Hz do 0 V w czasie (10÷20) s, a następnie analogicznie od 0 V do wartości znamionowej - obserwacja, czy występuje uszkodzenie niebezpieczne;
- pomiar czasu zaniku identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 230 V 50 Hz z generowanymi przerwami w zasilaniu (spadek napięcia w przerwie do 0 V, czas przerwy 10 ms, częstotliwość powtarzania przerwy 10 Hz);

- pomiar strefy identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 230 V 50 Hz z generowanymi przerwami w zasilaniu (spadek napięcia w przerwie do 0 V, czas przerwy 10 ms, częstotliwość powtarzania przerwy 10 Hz);
- pomiar czasu zaniku identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 230 V 50 Hz z generowanymi przerwami w zasilaniu (spadek napięcia w przerwie do 115 V, czas przerwy 20 ms, częstotliwość powtarzania przerwy 5 Hz);
- pomiar strefy identyfikacji w temperaturze (20±5) °C i wilgotności względnej (25÷75)%, przy zasilaniu 230 V 50 Hz z generowanymi przerwami w zasilaniu (spadek napięcia w przerwie do 115 V, czas przerwy 20 ms, częstotliwość powtarzania przerwy 5 Hz);
- badanie odporności na przerwę w napięciu zasilającym (w temperaturze (20±5) °C i wilgotności względnej (25÷75)%) (spadek napięcia w przerwie do 115 V, czas przerwy 500 ms, częstotliwość powtarzania przerwy 0,2 Hz) - obserwacja, czy występuje uszkodzenie niebezpieczne;

6.4. Sprawdzanie właściwości urządzenia bezpieczeństwa wykorzystującego technikę RFID

Sprawdzenie właściwości urządzenia bezpieczeństwa wykorzystującego technikę RFID dotyczyło następujących zagadnień:

- programowanie bazy danych do identyfikacji transponderów,
- zapewniany poziom nienaruszalności bezpieczeństwa SIL (poziom bezpieczeństwa funkcjonalnego),
- funkcjonowania systemu RFID w stanie defektu,
- wymagania dotyczące wyposażenia elektrycznego,
- wymagania dotyczące funkcjonowania elementów przełączających sygnału wyjściowego (OSSD),
- wymagania dotyczące związanych z bezpieczeństwem interfejsów danych i interfejsów komunikacyjnych,
- wymagania dotyczące wskaźników i wyświetlaczy,
- wymagania dotyczące rozłączania elementów składowych,
- wymagania dotyczące środków do nastawiania,
- wymagania dotyczące elementów nieelektrycznych,
- środki zapobiegające uszkodzeniom pochodzącym od wspólnej przyczyny,
- wymagania dotyczące elementów scalonych programowalnych lub o dużej złożoności,
- oprogramowanie, programowanie, projektowanie funkcjonalne obwodów scalonych,
- wymagania dotyczące obudów i zapewnianego przez nie stopnia ochrony (kod IP).

7. Ocena zgodności z wymaganiami zasadniczymi w odniesieniu do urządzeń bezpieczeństwa wykorzystujących technikę RFID

Ocena zgodności z wymaganiami zasadniczymi urządzeń bezpieczeństwa wykorzystujących technikę RFID powinna być dokonywana na podstawie kryteriów wynikających z przepisów dyrektywy 2006/42/WE oraz kryteriów wynikających z wymagań opracowanych na podstawie norm zharmonizowanych z dyrektywą. Podstawą do przeprowadzenia oceny powinny być wyniki przeprowadzonych badań typu.

Do oceny zgodności z wymaganiami zasadniczymi urządzeń bezpieczeństwa wykorzystujących technikę RFID opracowano listę kontrolną. Opracowana lista kontrolna zawiera pytania ogólne odnoszące się bezpośrednio do wymagań zasadniczych i pytania szczegółowe wynikające z opracowanych wymagań szczegółowych.

W liście kontrolnej udziela się odpowiedzi na pytania związane ze spełnieniem wymagania poprzez wybór pola "tak lub nie dotyczy" albo pola "nie". Przyjęta konstrukcja listy kontrolnej pozwala zakwalifikować odpowiedzi potwierdzające spełnienie wymagania i pytania, które nie dotyczą danego rozwiązania konstrukcyjnego do tej samej grupy ocen cząstkowych, które nie przeczą ogólnej ocenie dotyczącej zgodności z wymaganiami zasadniczymi. Oznacza to, że negatywną ocenę spełnienia wymagań zasadniczych przez urządzenie bezpieczeństwa wykorzystujące technikę RFID otrzymuje się, gdy udzielono co najmniej jednej, negatywnej odpowiedzi na pytanie cząstkowe, a ocenę pozytywną potwierdzającą spełnienie wymagań zasadniczych, gdy wszystkie odpowiedzi cząstkowe są pozytywne lub pytanie nie dotyczy urządzenia. W kolumnie "Uwagi" listy kontrolnej można zamieścić notatkę uzasadniającą ocenę cząstkową.

Lista kontrolna oceny zgodności z wymaganiami zasadniczymi urządzeń bezpieczeństwa wykorzystujących technikę RFID została dostosowana do urządzeń przeznaczonych do realizacji funkcji bezpieczeństwa blokowania uruchomienia, ponieważ obecnie tylko ten rodzaj urządzeń spełnia wymagania bezpieczeństwa funkcjonalnego. Llistę kontrolną przedstawiono w tablicy 1.

Tablica 1 Lista kontrolna oceny zgodności z wymaganiami zasadniczymi urządzeń bezpieczeństwa wykorzystujących technikę RFID.

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
Wymagania zasadnicze dyrektywy 2006/42/WE				
1.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest solidnej konstrukcji - urządzenie jest odporne i wytrzymałe na czynniki środowiskowe występujące w warunkach przemysłowych			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
2.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID może być pewnie zamocowane na swoim miejscu - zastosowano rozwiązania konstrukcyjne obudowy pozwalające na pewne zamocowanie			
3.	Transponder identyfikowany przez urządzenie bezpieczeństwa wykorzystujące technikę RFID może być pewnie umieszczony w strefie identyfikacji urządzenia			
4.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID nie stwarza dodatkowego zagrożenia			
5.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID nie jest łatwe do ominięcia lub wyłączenia z działania			
6.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID może być umieszczone w odpowiedniej odległości od strefy zagrożenia			
7.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID może być usytuowane w sposób nie powodujący utrudnień w obserwacji procesu produkcyjnego			
8.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID może być usytuowane w sposób nie utrudniający wykonania koniecznych prac związanych z mocowaniem lub wymianą narzędzi oraz konserwacją			
Wymagania szczegółowe - funkcjonalne				
9.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID może być usytuowane w sposób nie powodujący utrudnień w obserwacji procesu produkcyjnego			
10.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID może być wbudowane do układu sterowania maszyny tak, że zanik identyfikacji transpondera powoduje zatrzymanie części ruchomych maszyny			
11.	Identyfikacja transpondera urządzenia bezpieczeństwa wykorzystującego technikę RFID może nastąpić tylko, gdy transponder został umieszczony w strefie identyfikacji			
12.	Identyfikacja transpondera urządzenia bezpieczeństwa wykorzystującego technikę RFID może nastąpić tylko, gdy transponder został zarejestrowany w jego systemie identyfikacji			
13.	Jeżeli czytnik urządzenia bezpieczeństwa wykorzystującego technikę RFID składa się z wielu elementów to brak lub uszkodzenie jednego z nich powoduje uniemożliwienie identyfikacji			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
14.	Nastawianie transpondera urządzenia bezpieczeństwa wykorzystującego technikę RFID jest uniemożliwione (w szczególności nastawianie identyfikatora transpondera)			
15.	Nastawianie czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID jest możliwe tylko poprzez działanie zamierzone (w szczególności programowanie bazy danych identyfikatorów transponderów, nastawianie czasu zaniku identyfikacji, nastawianie strefy identyfikacji)			
16.	OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID przyjmuje stan ON podczas działania normalnego, gdy osiągany jest stan identyfikacji			
17.	OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID przyjmuje stan OFF, gdy nie jest osiągany jest stan identyfikacji			
18.	OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID przyjmuje stan OFF, gdy wykryty zostanie defekt			
19.	OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID utrzymuje stan OFF do czasu usunięcia defektu			
20.	Funkcja identyfikacji transpondera jest skuteczna w całej określonej przez producenta strefie identyfikacji urządzenia bezpieczeństwa wykorzystującego technikę RFID			
21.	Przejście OSSD ze stanu ON do stanu OFF po usunięciu transpondera ze strefy identyfikacji urządzenia bezpieczeństwa wykorzystującego technikę RFID odbywa się w czasie zaniku identyfikacji (zadziałania) nie większym niż zadeklarowany przez producenta			
22.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID spełnia wymagania co najmniej poziomu nienaruszalności bezpieczeństwa SIL 1			
Wymagania szczegółowe - projektowe				
23.	Wyposażenie elektryczne czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID funkcjonuje w warunkach zasilania określonych przez p. 4.2.1 normy PN-EN 61496:2014-02			
24.	Wyposażenie elektryczne transpondera urządzenia bezpieczeństwa wykorzystującego technikę RFID nie wymaga zasilania ze źródeł energii			
25.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID powinno wykrywać defekty prowadzące do fałszywej identyfikacji transponderów			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
26.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID powinno wykrywać defekty prowadzące do przejścia OSSD do stanu ON w warunkach braku identyfikacji			
27.	Wyposażenie elektryczne urządzenia bezpieczeństwa wykorzystującego technikę RFID jest odpowiednie do zamierzonego zastosowania			
28.	Wyposażenie elektryczne urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania normy PN-EN 60204-1:2010 w zakresie ochrony przed przepięciami.			
29.	Wyposażenie elektryczne urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania normy PN-EN 60204-1:2010 w zakresie ochrony przed przetężeniami			
30.	Wyposażenie elektryczne urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania normy PN-EN 60947-1:2010 w zakresie 2 stopnia ochrony przed zanieczyszczeniami			
31.	Wyposażenie elektryczne urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania normy PN-EN 60947-1:2010 w zakresie odstępów izolacyjnych			
32.	Wyposażenie elektryczne urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania normy PN-EN 60204-1:2010 w zakresie oprzewodowania			
33.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID ma oddzielne elementy przyłączeniowe dla każdego OSSD			
34.	OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID jest zdolne przełączać zadeklarowane obciążenie bez zastosowania elementów gaszenia łuku			
35.	Jeżeli urządzenie bezpieczeństwa wykorzystujące technikę RFID jest wyposażone w związany z bezpieczeństwem interfejs transmisji danych, to zmiana stanu OSSD powoduje jego adekwatne działanie			
36.	Przekaźnikowe OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID wyposażone jest w środki (dodatkowe styki sprzężone mechanicznie) do monitorowania jego stanu			
37.	Półprzewodnikowe OSSD urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania dotyczące napięcia zasilającego oraz minimalnych i maksymalnych wartości napięcia w stanach OFF i ON			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
38.	Jeżeli urządzenie bezpieczeństwa wykorzystujące technikę RFID ma dwa półprzewodnikowe OSSD, to zapewniono środki do wykrywania zwarć pomiędzy nimi			
39.	Producent wyposażenia bezpieczeństwa wykorzystującego technikę RFID wyposażonego w półprzewodnikowe OSSD zamieścił w instrukcji użytkownika wymagane informacje dotyczące nominalnego i maksymalnego prądu wyjściowego, maksymalnego napięcia w stanie OFF, maksymalnego prądu wyjściowego wstanie OFF, maksymalnej dopuszczalnej pojemności obciążenia oraz maksymalnej dopuszczalnej rezystancji połączeń pomiędzy OSSD i obciążeniem			
40.	Związany z bezpieczeństwem interfejs transmisji danych urządzenia bezpieczeństwa wykorzystującego technikę RFID spełnia wymagania bezpieczeństwa funkcjonalnego na poziomie nie niższym niż samo urządzenie			
41.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID wyposażone jest we wskaźniki świetlne stanu OSSD (zielony dla stanu ON, czerwony dla stanu OFF) – zmiana stanu wskaźników odbywa się z opóźnieniem nie większym niż 100 ms w stosunku do zmian stanu OSSD			
42.	Jeżeli urządzenie bezpieczeństwa wykorzystujące technikę RFID jest wyposażone w inne wskaźniki świetlne o tej samej barwie co wskaźniki stanu OSSD, to ich funkcje są oznakowane w sposób jednoznaczny			
43.	Wskaźniki urządzenia bezpieczeństwa wykorzystującego technikę RFID mogą być widoczne z pozycji operatora maszyny			
44.	Środki do nastawiania urządzenia bezpieczeństwa wykorzystującego technikę RFID są wykonane w sposób zapobiegający wystąpieniu uszkodzenia niebezpiecznego			
45.	Jeżeli czytnik urządzenia bezpieczeństwa wykorzystującego technikę RFID składa się z elementów, które mogą być rozłączane, to takie rozłączenie powoduje przejście przynajmniej jednego OSSD do stanu OFF			
46.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID wyposażone jest w niezbędne elementy nieelektryczne			
47.	W urządzeniu bezpieczeństwa wykorzystującym technikę RFID zastosowano środki minimalizujące możliwość powstania uszkodzeń pochodzących od wspólnej przyczyny - wywołanych wpływami środowiskowymi			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
48.	W urządzeniu bezpieczeństwa wykorzystującym technikę RFID zastosowano środki minimalizujące możliwość powstania uszkodzeń pochodzących od wspólnej przyczyny - wywołanych zastosowaniem systemu wielokanałowego z częścią wspólną			
49.	W urządzeniu bezpieczeństwa wykorzystującym technikę RFID zastosowano środki minimalizujące możliwość powstania uszkodzeń pochodzących od wspólnej przyczyny – wywołanych zwarciami pomiędzy kanałami systemu wielokanałowego			
50.	Zastosowaniu w urządzeniu bezpieczeństwa wykorzystującym technikę RFID układów scalonych programowalnych lub o wysokim stopniu złożoności towarzyszy zastosowanie zdwojonych środków do monitorowania wystąpienia defektów			
51.	Oprogramowanie urządzenia bezpieczeństwa wykorzystującego technikę RFID zostało opracowane zgodnie z wymaganiami odpowiedniego poziomu SIL			
Wymagania szczegółowe - środowiskowe				
52.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID zostało przystosowane do działania w przedziale temperatur co najmniej od 0 ºC do 50 ºC i przy wilgotności względnej 95% (bez kondensacji, w zakresie temperatur od 20 ºC do 50 ºC)			
53.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na zmiany napięcia zasilającego			
54.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na przerwy w zasilaniu			
55.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na serie szybkich elektrycznych stanów przejściowych zgodnie z wymaganiami PN-EN 61000-4-4:2013-05			
56.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na udary elektryczne zgodnie z wymaganiami PN-EN 61000-4-5:2014-10			
57.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na promieniowane pole elektromagnetyczne zgodnie z wymaganiami PN-EN 61000-4-3:2007			
58.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na zaburzenia przewodzone, indukowane przez pola o częstotliwości radiowej zgodnie z wymaganiami PN-EN 61000-4-6:2014-04			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
59.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na wyładowania elektrostatyczne zgodnie z wymaganiami PN-EN 61000-4-2:2011			
60.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na drgania			
61.	Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest odporne na udary			
62.	Obudowa czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID przeznaczona do montażu w maszynie zgodnie z zaleceniami producenta zapewnia stopień ochrony co najmniej IP54			
63.	Obudowa czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID przeznaczona do montażu w obudowie układu sterowania maszyny zapewnia stopień ochrony co najmniej IP20			
64.	Przejścia kablowe w obudowie czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID zapewniają stopień ochrony nie gorszy niż obudowa			
65.	W obudowie czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID nie zastosowano połączeń z zastosowaniem mas uszczelniających, jeżeli połączenia te mogą być rozłączane w celach serwisowych			
66.	Obudowa czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID jest pozbawiona ostrych krawędzi			
67.	Obudowa czytnika urządzenia bezpieczeństwa wykorzystującego technikę RFID jest wyposażona w odpowiednie środki dostępu do nastawiania			
68.	Obudowa transpondera urządzenia bezpieczeństwa wykorzystującego technikę RFID jest monolityczna, zapewnia stopień ochrony co najmniej IP54 i jest pozbawiona ostrych krawędzi			
Wymagania szczegółowe – znakowanie w celu bezpiecznego użytkowania				
69.	Identyfikacja urządzenia (nazwa urządzenia, nazwa i adres producenta, typ lub seria, numer seryjny i rok budowy)			
70.	Wymiary strefy identyfikacji			
71.	Czas zaniku identyfikacji			
72.	Znamionowe napięcie i częstotliwość zasilania			
73.	Znamionowy pobór mocy (jeżeli większy niż 25 W) lub pobór prądu			
74.	Stopień ochrony obudowy			
75.	Symbol urządzenia II klasy ochronności (jeżeli dotyczy)			
76.	Znak ostrzeżenia o występowaniu wysokich napięć (jeżeli dotyczy)			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
77.	Poziom nienaruszalności bezpieczeństwa SIL			
78.	Oznaczenie zasilacza, jeżeli do zasilania wymagany jest określony zasilacz			
79.	Wartość znamionowa bezpiecznika, jeżeli zasilanie czytnika odbywa się z wewnętrznych źródeł zasilania			
80.	Symbol wg normy PN-EN 60204-1:2010 p. 16.2.1 umieszczony na obudowie zawierającej wyposażenie elektryczne			
81.	Oznaczenia przełączników, wskaźników, elementów sterowniczych umieszczone w ich pobliżu			
82.	Oznaczenia elementów do nastawiania parametrów z oznaczeniem kierunku zwiększania/zmniejszania wartości			
83.	Oznaczenie zacisków wymagających podczas instalacji podłączenia przewodów zgodnie ze schematem			
84.	Oznaczenie zacisków przewidzianych do podłączenia zasilania			
85.	Oznaczenie zacisku przewidzianego do podłączenia przewodu ochronnego			
86.	Oznakowanie jest odporne na przemysłowe warunki środowiskowe (próba trwałości oznakowania)			
Wymagania szczegółowe – zawartość dokumentacji towarzyszącej				
87.	Do urządzenia bezpieczeństwa wykorzystującego technikę RFID dołączono dokumentację w języku uzgodnionym pomiędzy dostawcą i odbiorcą			
88.	Stwierdzenie, że do wewnętrznych źródeł zasilania nie należy podłączać innych urządzeń			
89.	Zalecenie przechowywania narzędzi do nastawiania pod specjalnym nadzorem			
90.	Opis metody testowania doraźnego urządzenia i funkcji identyfikacji			
91.	Określenie czasu zaniku identyfikacji			
92.	Określenie zapewnianego poziomu nienaruszalności bezpieczeństwa SIL lub informacje równoważne (np. PFHD)			
93.	Jeżeli stosowany jest interfejs komunikacyjny, to określenie metodyki wyznaczania całkowitego czasu zaniku identyfikacji			
94.	Informacja o znamionowych warunkach środowiskowych (zakres temperatury, wilgotność, zakres napięć zasilania, wymagane odległości pomiędzy elementami urządzenia i maksymalna długość przewodów połączeniowych)			
95.	Zalecenia dotyczące możliwości interferencji z funkcją identyfikacji			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
96.	Schematy blokowe, opis funkcjonalny przedstawiający sekwencję operacji związanych z przełączaniem przekaźników			
97.	Położenie wszystkich zacisków wejściowych i wyjściowych			
98.	Wartości znamionowe i charakterystyki wszystkich wejść i wyjść			
99.	Wartości minimalne i maksymalne napięć i prądów dotyczące OSSD oraz inne parametry związane z ich obciążaniem			
100.	Informacja dotycząca możliwości wykonywania przez użytkownika czynności konserwacyjnych i obsługowych we własnym zakresie			
101.	Szczególne wymagania dotyczące przewodów podłączanych do zacisków (jeżeli dotyczy urządzenia)			
102.	Wymagania dotyczące obciążania i poboru mocy			
103.	Wymagania dotyczące utrzymania wolnej przestrzeni wokół urządzenia w celu wyjmowania i konserwacji			
104.	Wykaz części zamiennych wymienialnych przez użytkownika			
105.	Wykaz kolorów i kodów zastosowanych do oznakowania			
106.	Całkowite wymiary urządzenia			
107.	Instrukcja działania			
108.	Usytuowanie i wymiary strefy identyfikacji			
109.	Harmonogram sprawdzeń urządzenia po zainstalowaniu, konserwacji i kontroli okresowej			
110.	Metoda regularnego testowania w celu potwierdzenia poprawności działania i częstość jej stosowania			
111.	Określenie stopnia ochrony IP obudowy urządzenia lub minimalne wymagania dotyczące obudowy dodatkowej			
112.	Wyraźne określenie zastosowań, do których urządzenie jest przeznaczone			
113.	Instrukcja instalacji i montażu wszelkich elementów składowych urządzenia			
114.	Instrukcja podłączania urządzenia do systemu sterowania maszyny			
115.	Szczegóły przeciwwskazań, które powinny być wzięte pod uwagę przy stosowaniu urządzenia			
116.	Wielkość odstępów, które należy zapewnić urządzeniu			
117.	Wymiary i usytuowanie środków do mocowania urządzenia			
118.	Minimalne i maksymalne odstępy pomiędzy różnymi elementami urządzenia i elementami otaczającymi			

Lp.	Wymaganie	Ocena		Uwagi
		Tak lub nie dotyczy	Nie	
119.	Środki do podłączania zasilania i łączenia oddzielnych elementów urządzenia			
120.	Informacje o prawidłowym podłączaniu wyjść półprzewodnikowych			
121.	Informacje dotyczące prawidłowej integracji interfejsu transmisji danych			

8. Metodyka projektowania związanych bezpieczeństwem systemów sterowania maszyn wykorzystujących technikę RFID

Metodyka projektowania funkcji bezpieczeństwa z wykorzystaniem techniki RFID powinna uwzględniać i zapewnić spełnienie wymagań bezpieczeństwa funkcjonalnego wynikających z dyrektywy 2006/42/WE. Wymagania dyrektywy w tym zakresie są bardzo ogólne, stąd należy sięgnąć do odpowiedniej normy zharmonizowanej z dyrektywą w celu uzyskania wymagań szczegółowych. Urządzenie bezpieczeństwa wykorzystujące technikę RFID jest układem elektronicznym zawierającym system identyfikacji transponderów z bazą danych programowalnym. Związany z bezpieczeństwem element systemu sterowania maszyny oparty na zastosowaniu urządzenia bezpieczeństwa wykorzystującego technikę RFID również należy rozpatrywać, jako urządzenie elektroniczne programowalne. Stąd odpowiednią normą do wykorzystania będzie PN-EN 62061:2008 *Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem*. Norma ta jest dostępna w języku polskim. Do normy tej opublikowano również dwie zmiany A1 i A2 (PN-EN 62061:2008/A1:2013-06 i PN-EN 62061:2008/A2:2016-01), które dostępne są tylko w języku angielskim.

Norma PN-EN 62061 formułuje wymagania bezpieczeństwa funkcjonalnego w odniesieniu do związanego z bezpieczeństwem systemu sterowania maszyny (SRECS) zasilanego energią elektryczną, zawierającego części elektryczne, elektroniczne lub elektroniczne programowalne. SRECS jest definiowany jako elektryczny system sterowania maszyny, którego uszkodzenie może skutkować bezpośrednim wzrostem ryzyka. Taki system sterowania składa się z podsystemów. Uszkodzenie dowolnego podsystemu powoduje uszkodzenie jakiejś funkcji sterowania związanej z bezpieczeństwem (SRCF). SRCF jest funkcją sterowania realizowaną przez SRECS, o określonym poziomie nienaruszalności bezpieczeństwa (SIL), przeznaczoną do utrzymywania warunków bezpieczeństwa maszyny lub zapobiegania bezpośredniemu wzrostowi ryzyka. Nienaruszalność bezpieczeństwa jest to prawdopodobieństwo, że SRECS lub jego podsystem wykona w sposób zadowalający wymagane funkcje sterujące związane z

bezpieczeństwem we wszystkich określonych warunkach. Na nienaruszalność bezpieczeństwa składają się nienaruszalność bezpieczeństwa sprzętu (część nienaruszalności bezpieczeństwa SRECS lub jego podsystemu zawierająca zarówno wymagania dotyczące prawdopodobieństwa niebezpiecznych przypadkowych uszkodzeń sprzętu, jak i ograniczenia architektury) i nienaruszalność bezpieczeństwa oprogramowania (część systematycznej nienaruszalności SRECS lub jego podsystemu odnosząca się do zdolności oprogramowania elektronicznych systemów programowalnych do realizacji funkcji sterowania związanej z bezpieczeństwem we wszystkich ustalonych warunkach w ustalonym czasie).

Elementem podsystemu SRECS jest jego część, która może zawierać pojedyncze składniki lub dowolną grupę składników. W szczególności elementem podsystemu może być inny podsystem. Norma określa bezpieczeństwo funkcjonalne jako część bezpieczeństwa maszyny i jej systemu sterowania, która zależy od poprawnego funkcjonowania SRECS, systemów związanych z bezpieczeństwem wykonanych w innych technikach oraz zewnętrznych środków redukcji ryzyka.

Norma PN-EN 62061 formułuje wymagania odnoszące się do SRECS poprzez przedstawienie następujących zagadnień:

- określenie terminów, definicji i skrótów,
- wymagania dotyczące zarządzania bezpieczeństwem funkcjonalnym,
- wymagania dotyczące specyfikacji związanych z bezpieczeństwem funkcji sterowania (SRCF),
- wymagania dotyczące projektowania i integracji SRECS,
- sporządzenie informacji dla użytkownika,
- walidacja SRECS,
- procedury zarządzania modyfikacjami SRECS.

W przypadku SRECS stosującego technikę RFID wymagania normy PN-EN 62061 można uwzględnić przy projektowaniu następujących podsystemów:

- podsystem urządzenia bezpieczeństwa wykorzystującego technikę RFID – jest to układ czujnika RFID wykrywającego sytuacje zagrożenia o strukturze (patrz p. 4.3) zawierającej następujące elementy: czytnik RFID (ze zintegrowaną funkcją identyfikacji transponderów), jednostkę sterująco-monitorującą i element przełączający sygnału wyjściowego (OSSD). SRCF realizowana przez ten podsystem polega na wykrywaniu zaniku identyfikacji transpondera (jest równoważne ze stwierdzeniem sytuacji zagrożenia) i sygnalizacji tego faktu (możliwość wykorzystania przez kolejne podsystemy SRECS do realizacji kolejnych SRCF). Wymagania szczegółowe dotyczące podsystemu urządzenia bezpieczeństwa wykorzystującego technikę RFID sformułowano w oparciu o normę PN-EN 61496 (patrz p. 5), lecz nie określają one

szczegółów metodyki wyznaczenia poziomu nienaruszalności bezpieczeństwa zapewnianego przez tak określony podsystem. Zatem w tym aspekcie należy dodatkowo wykorzystać normę PN-EN 62061. Szczególnie dotyczy to zapewnienia nienaruszalności bezpieczeństwa oprogramowania i wyznaczenia granicy poziomu nienaruszalności bezpieczeństwa dla tak określonego podsystemu SRECS;

- podsystem SRECS wykorzystujący możliwości oferowane przez technikę RFID – ze względu na specyfikę techniki RFID (patrz p. 3) racjonalne jest wykorzystanie techniki RFID do realizacji SRCF polegającej na blokowaniu możliwości uruchomienia maszyny po stwierdzeniu zaniku identyfikacji transpondera. Elementami struktury podsystemu SRECS realizującego powyższą SRCF będą: podsystem urządzenia bezpieczeństwa wykorzystującego technikę RFID (czujnik sytuacji zagrożenia), element logiczny (np. PLC – odpowiada za logiczną realizację funkcji bezpieczeństwa) i element wykonawczy (blokujący możliwość przejścia maszyny w stan energetyczny związany z zagrożeniem np. blokowanie uruchomienia napędów). W tym przypadku norma PN-EN 62061 powinna być wykorzystana do określenia wymaganego poziomu nienaruszalności bezpieczeństwa SIL i do zapewnienia, że projektowany podsystem spełni to wymaganie.

Ogólna metodyka projektowania związanych z bezpieczeństwem systemów sterowania przedstawiona w normie PN-EN 62061 zakłada prowadzenie etapowych działań według wcześniej przygotowanego planu, który powinien:

- identyfikować odpowiednie działania;
- opisywać strategię spełnienia określonych wymagań bezpieczeństwa funkcjonalnego;
- opisywać strategie osiągania bezpieczeństwa funkcjonalnego dotyczące opracowania, scalania, weryfikacji i walidacji oprogramowania użytkowego;
- identyfikować osoby, działy i inne jednostki i zasoby w celu zapisywania oraz utrzymywania właściwych informacji dla bezpieczeństwa funkcjonalnego związanych z bezpieczeństwem elementów systemu sterowania;
- identyfikować lub ustanawiać procedury i zasoby w celu zapisywania oraz utrzymywania właściwych informacji dla bezpieczeństwa funkcjonalnego;
- opisywać strategię zarządzania konfiguracją, z uwzględnieniem odpowiednich środków organizacyjnych, takich jak autoryzowany personel i wewnętrzna struktura organizacji,
- ustanawiać plan weryfikacji zawierający: szczegółowe określenie, kiedy weryfikacja powinna mieć miejsce, szczegółowe określenie osób, działów lub jednostek, które powinny przeprowadzać weryfikację, wybór strategii i technik prowadzenia weryfikacji, wybór i stosowanie urządzeń probierczych, określenie działań weryfikacyjnych, kryteria oceny i środki, które powinny być stosowane przy ocenie wyników weryfikacji;

- ustanawiać plan walidacji uwzględniający: szczegóły, kiedy walidacja powinna mieć miejsce, identyfikację odpowiednich rodzajów działania maszyny (np. praca normalna, ustawianie), wymagania będące przedmiotem walidacji związanych z bezpieczeństwem elementów systemu sterowania, strategię techniczną walidacji (np. metody analityczne lub badania statystyczne), kryteria oceny i działania, jakie powinny być podejmowane w przypadku uszkodzenia, aby spełnić kryteria oceny.

8.1. Specyfikacja wymagań dotyczących SRCF wykorzystującej technikę RFID

Na wstępnym etapie projektowania urządzenia bezpieczeństwa wykorzystującego technikę RFID należy sporządzić oraz udokumentować i zweryfikować specyfikację realizowanej SRCF. Powinna ona zawierać:

- specyfikację wymagań funkcjonalnych,
- specyfikację wymagań dotyczących nienaruszalności bezpieczeństwa.

Przy sporządzaniu specyfikacji wymagań dotyczących SRCF należy korzystać z dostępnych informacji, w tym:

- wyników oceny ryzyka dotyczącej sytuacji zagrożenia, dla której podjęto decyzję o redukcji ryzyka metodami sterowania i określono stosowną funkcję bezpieczeństwa;
- charakterystyki działania maszyny uwzględniające: rodzaje pracy, czas cyklu, czas zadziałania (odpowiedzi), warunki środowiskowe, zasady współdziałania człowieka z maszyną;
- wszystkie informacje dotyczące funkcji bezpieczeństwa, które mogą mieć wpływ na projekt związanych z bezpieczeństwem elementów systemu sterowania, w tym: opis zachowania się maszyny w sytuacjach związanych z funkcją bezpieczeństwa, interfejsy pomiędzy elementami uczestniczącymi w realizacji funkcji bezpieczeństwa, wymagane funkcje reagowania na uszkodzenia funkcji bezpieczeństwa.

Specyfikacja wymagań funkcjonalnych dla SRCF powinna opisywać szczegóły jej działania, o ile to odpowiednie, obejmujące następujące informacje:

- warunki pracy maszyny, w których SRCS powinna być aktywna lub nieaktywna,
- pierwszeństwo wśród tych funkcji, które mogą być równocześnie aktywne i które mogą powodować konflikty działania,
- częstość aktywowania SRCF,
- wymagany czas zadziałania (reakcji),
- interfejsy do innych funkcji maszyny i wymagane czasy odpowiedzi urządzeń wejścia/wyjścia,
- opis SRCF,
- opis funkcji reagowania na defekty i wszelkie ograniczenia,

- opis środowiska pracy,
- procedury badania i związane z tym wyposażenie badawcze,
- znamionową liczbę cykli działania.

Specyfikacja wymagań dotyczących nienaruszalności bezpieczeństwa SRCF powinna być określona na podstawie oceny ryzyka, co pozwoli zapewnić osiągnięcie odpowiedniego stopnia redukcji ryzyka. Wymagania dotyczące nienaruszalności bezpieczeństwa należy określić poprzez podanie poziomu nienaruszalności bezpieczeństwa SIL zgodnie z tablicą 2.

Tablica 2 Poziomy nienaruszalności bezpieczeństwa SIL wyrażone wartością prawdopodobieństwa wystąpienia niebezpiecznych uszkodzeń na godzinę.

Poziom nienaruszalności bezpieczeństwa	Prawdopodobieństwo wystąpienia niebezpiecznych uszkodzeń na godzinę (PFH_D)
3	$10^{-8} \leq PFH_D < 10^{-7}$
2	$10^{-7} \leq PFH_D < 10^{-6}$
1	$10^{-6} \leq PFH_D < 10^{-5}$

Do oceny ryzyka można zastosować dowolną sprawdzoną metodę. Norma PN-EN 62061 w załączniku A określa przykładową metodykę jakościowego oszacowania ryzyka. Zgodnie z tą metodyką pod uwagę brane są następujące elementy ryzyka, których wartość należy określić na podstawie poniższych tablic:

- ciężkość szkody Se,

Tablica 3. Klasyfikacja ciężkości szkody (Se)

Konsekwencje	Ciężkość szkody (Se)
Nieodwracalne: śmierć, utrata oka lub ręki	4
Nieodwracalne: złamania kończyn(-y), utrata palca(-ów)	3
Odwracalne: wymagana interwencja personelu medycznego	2
Odwracalne: wymagana pierwsza pomoc	1

- częstotliwość i czas trwania ekspozycji osób na zagrożenie Fr,

Tablica 4. Klasyfikacja częstotliwości i czasu trwania ekspozycji (Fr)

Częstotliwość ekspozycji (wyrażona okresem T pomiędzy zdarzeniami zagrażającymi) przy czasie ekspozycji > 10 min	Częstotliwość i czas trwania ekspozycji (Fr)
T ≤ 1 h	5
1 h < T ≤ 1 dzień	5
1 dzień < T ≤ 2 tygodnie	4
2 tygodnie < T ≤ 1 rok	3

1 rok < T	2

– prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego Pr,

Tablica 5. Klasyfikacja prawdopodobieństwa (Pr)

Możliwość wystąpienia zdarzenia niebezpiecznego	Prawdopodobieństwo (Pr)
Bardzo wysokie	5
Dogodne	4
Możliwe	3
Rzadkie	2
Pomijalne	1

– możliwość uniknięcia lub ograniczenia szkody Av.

Tablica 6. Klasyfikacja prawdopodobieństwa uniknięcia lub ograniczenia szkody (Av)

Możliwość uniknięcia lub ograniczenia szkody	Prawdopodobieństwo (Av)
Niemożliwe	5
Rzadkie	3
Prawdopodobne	1

Po ustaleniu wartości elementów ryzyka należy określić klasę prawdopodobieństwa wystąpienia szkody Cl wg wzoru:

$$Cl = Fr + Pr + Av$$

a następnie przypisać poziom nienaruszalności bezpieczeństwa SIL zgodnie z tablicą 7.

Tablica 7. Matryca przypisywania SIL

Ciężkość (Se)	Klasa prawdopodobieństwa wystąpienia szkody (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	**SIL 2**	**SIL 2**	**SIL 2**	**SIL 3**	**SIL 3**
3		**(OM)**	**SIL 1**	**SIL 2**	**SIL 3**
2			**(OM)**	**SIL 1**	**SIL 2**
1				**(OM)**	**SIL 1**

Obszar ciemno szary wskazuje SIL przypisany SRCF jako celowy. Obszar jasno szary powinien być stosowany jako zalecany, jeżeli są stosowane inne środki (OM).

Wyraźna niedogodność techniki RFID z punktu widzenia techniki bezpieczeństwa polegająca na tym, że identyfikacja transpondera nie jest całkowicie równoważna z identyfikacją człowieka/operatora dysponującego tym transponderem powoduje, że stopień

redukcji ryzyka, który może być zapewniony przez urządzenia bezpieczeństwa wykorzystujące technikę RFID nie jest wysoki. Zatem ich zastosowanie jako jeden z podstawowych środków bezpieczeństwa może być rozpatrywane tylko w przypadkach wymagających niskiego poziomu SIL = 1 lub tam, gdzie zalecane jest stosowanie innych środków bezpieczeństwa. Obecne zastosowania techniki RFID w realizacji SRECS mają charakter uzupełniający w stosunku do podstawowych środków bezpieczeństwa i potwierdzają powyższe spostrzeżenie.

Nie mniej wyspecyfikowanie wymagań dla SRCF wykorzystującego technikę RFID na poziomie SIL = 1 lub nawet nieco poniżej tego poziomu wiąże się z koniecznością odpowiedniej realizacji tego wymagania w procesie projektowania SRECS i następnie jego walidacji. Należy również spodziewać się, że dążenie do wykorzystania zalet techniki RFID w dziedzinie bezpieczeństwa użytkowania maszyn doprowadzi do istotnego zredukowania wpływu powyższej niedogodności na zapewniany poziom nienaruszalności bezpieczeństwa, co utoruje drogę tej technice do realizacji SRECS o wyższych poziomach nienaruszalności bezpieczeństwa.

8.2. Projektowanie i integracja SRECS wykorzystującego technikę RFID

SRECS wykorzystujący technikę RFID należy dobrać lub zaprojektować tak, aby spełniał specyfikację wymagań bezpieczeństwa i specyfikację wymagań oprogramowania. W zakresie dotyczącym nienaruszalności bezpieczeństwa sprzętu należy uwzględnić:

- ograniczenia architektury w odniesieniu do nienaruszalności bezpieczeństwa sprzętu,
- wymagania dotyczące prawdopodobieństwa niebezpiecznych uszkodzeń przypadkowych sprzętu,
- wymagania dotyczące nienaruszalności bezpieczeństwa systematycznej zawierające wymagania dotyczące unikania uszkodzeń i dotyczące kontroli defektów systematycznych,
- wymagania dotyczące zachowania się SRECS w przypadku wykrycia defektów,
- wymagania dotyczące projektowania i wytwarzania oprogramowania związanego z bezpieczeństwem.

W projekcie SRECS wykorzystującego technikę RFID należy uwzględnić wymagania i możliwości samej techniki RFID. Źródłem tych wymagań powinny być normy przedmiotowe odpowiednie do rodzaju techniki RFID, która zostanie zastosowana.

W projekcie SRECS należy uwzględnić możliwości i ograniczenia człowieka (w tym rozsądnie przewidywane niewłaściwe użytkowanie). Projekt SRECS powinien być odpowiedni do działań przypisywanych operatorowi, personelowi utrzymania ruchu i innym osobom. Projekt interfejsu operatorskiego powinien nawiązywać do dobrej praktyki ergonomicznej. W przypadku wykorzystania techniki RFID powinien on uwzględniać

geometrię strefy identyfikacji i wynikający z niej zasięg identyfikacji oraz potencjalne uciążliwości wynikające z konieczności pozycjonowania transpondera w strefie identyfikacji.

Wykrycie niebezpiecznego defektu w podsystemie, w którym przewidziano jakąkolwiek tolerancję na defekty sprzętu powinno powodować wykonanie określonej funkcji reakcji na defekty. Jeżeli konieczne jest wprowadzenie funkcji diagnostycznej ze względu na osiągnięcie wymaganego prawdopodobieństwa przypadkowych uszkodzeń sprzętu i podsystem nie ma tolerancji na uszkodzenie sprzętu, wtedy należy zapewnić, że wykrycie defektu i reakcja na niego nastąpi zanim wystąpi sytuacja zagrożenia spowodowana defektem SRCF.

Defektów systematycznych SRECS (projektowych i wynikających z niewłaściwego wykonania) należy unikać poprzez stosowanie następujących środków:

- projektowanie i wdrażanie SRECS zgodnie z planem bezpieczeństwa funkcjonalnego,
- właściwy dobór, połączenie, rozmieszczenie, montaż i instalowanie podsystemu łącznie prowadzeniem kabli i wykonywaniem połączeń,
- stosowanie SRECS zgodnie ze specyfikacją producenta,
- stosowanie wskazówek producenta dotyczących zastosowania i instalowania oraz zasad dobrej praktyki inżynierskiej,
- stosowanie podsystemów o kompatybilnych charakterystykach pracy,
- stosowanie zabezpieczeń oraz zapobieganie utracie połączeń uziemienia funkcjonalnego zgodnie z normą PN-EN 60204-1 *Bezpieczeństwo maszyn – Wyposażenie elektryczne maszyn –m Część 1: Wymagania ogólne*,
- nie należy wykorzystywać nieudokumentowanych rodzajów pracy stosowanych komponentów,
- należy przewidywać niewłaściwe użycie, zmiany środowiska pracy lub modyfikacje.

W projektowaniu należy dodatkowo stosować następujące techniki:

- przeglądy projektu sprzętu SRECS w celu wykrywania rozbieżności pomiędzy specyfikacją i wdrożeniem,
- komputerowe narzędzia wspomagające projektowanie, w tym funkcje symulacji i analizy.

W celu kontroli defektów systematycznych należy stosować odpowiednie rozwiązania obejmujące:

- SRECS jest tak zaprojektowane, że po odłączeniu zasilania elektrycznego maszyna osiąga lub utrzymuje stan bezpieczny,
- zmiany napięcia zasilającego (np. przerwy, zapady) nie powodują zagrożenia,
- efekty zaburzeń elektromagnetycznych w środowisku lub podsystemie nie powodują zagrożenia,

- skutki szeroko rozumianych błędów w podsystemach transmisji danych bezpieczeństwa nie powodują zagrożenia,
- wystąpienie defektów w interfejsie, jest wykrywane, a funkcja reagowania na defekty jest w stanie zadziałać zanim wystąpi zagrożenie związane z tym defektem.

W zakresie kompatybilności elektromagnetycznej podsystem SRECS powinien spełniać wymagania dotyczące niewprowadzania warunków niebezpiecznych lub zagrożeń dla innych podsystemów, nie powinna następować utrata SRCF związanej z podsystemem, w przypadku występowania chwilowych lub ciągłych zakłóceń stan bezpieczeństwa maszyny jest osiągany zanim wystąpi zagrożenie lub jest utrzymywany do czasu ustąpienia zakłóceń.

Konstrukcja i opracowanie SRECS również powinny w pełni uwzględniać specyfikację wymagań bezpieczeństwa, procesy z tym związane powinny być udokumentowane. W projekcie architektury SRECS należy uwzględnić dekompozycję układu na bloki funkcjonalne (struktura systemu). Architektura SRECS powinna zostać opisana poprzez podanie opisu struktury, wymagań bezpieczeństwa (w tym poziomu nienaruszalności bezpieczeństwa SIL) dotyczących każdego bloku funkcjonalnego oraz przez określenie wejść i wyjść każdego bloku.

Jeżeli projektowanie SRECS wykorzystującego technikę RFID oparte jest o wymagania normy PN-EN 61496, to w zakresie wymagań konstrukcyjnych i dotyczących kompatybilności elektromagnetycznej spełnienie wymagań tej normy jest odpowiednie w miejsce wymagań wynikających z normy PN-EN 62061.

Nienaruszalność bezpieczeństwa sprzętu należy określać poprzez prawdopodobieństwo wystąpienia uszkodzeń niebezpiecznych na godzinę w odniesieniu do każdej realizowanej SRCF. Prawdopodobieństwo to powinno być szacowane z uwzględnieniem architektury SRECS związanej z każdą rozpatrywaną SRCF oraz na podstawie szacowania strumienia uszkodzeń związanego z każdym blokiem funkcjonalnym (podsystemem, elementem SRECS) uczestniczącym w realizacji SRCF i z uwzględnieniem procesów przesyłania danych cyfrowych pomiędzy blokami funkcjonalnymi. W architekturze (strukturze) szeregowego połączenia bloków funkcjonalnych defekt jednego z bloków skutkuje defektem całej SRCF. W tym przypadku, dla konkretnej SRCF oszacowanie prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego PFH_D na godzinę może być obliczone ze wzoru:

$$PFH_D = PFH_{D1} + \ldots + PFH_{Dn} + P_{TE}$$

gdzie: $PFH_{D1},\ldots,PFH_{Dn}$ – prawdopodobieństwa wystąpienia defektów niebezpiecznych na godzinę związane z poszczególnymi blokami funkcjonalnymi,

P_{TE} – prawdopodobieństwo niebezpiecznego błędu transmisji na godzinę.

Powyższe obliczenie jest słuszne tylko w przypadku struktury szeregowej. W przypadku innych struktur np. równoległych z uwzględnieniem defektów pochodzących od wspólnej przyczyny, czy struktur z wprowadzoną funkcją diagnostyczną obowiązują inne procedury obliczeniowe (patrz punkt 6.7.8.2 normy PN-EN 62061).

Wyznaczenie parametru PFH_D dla SRCF jest równoznaczne z określeniem poziomu nienaruszalności bezpieczeństwa SIL dla podsystemu realizującego SRCF (na podstawie tablicy 2). W SRECS zawierającym szeregowo połączone podsystemy o różnych SILCL (granica osiągnięcia SIL dla podsystemu) SIL wynikowy jest co najwyżej równy najniższemu SILCL zaangażowanemu w realizację SRCF.

W przypadku projektowania podsystemów SRECS obowiązują podobne wymagania do tych przedstawionych dla całego SRECS (szczegóły w p. 6.7 normy PN-EN 62061).

Często projektowanie SRECS wiąże się z potrzebą realizacji funkcji diagnostycznych, które są konieczne do spełnienia wymagań wynikających z ograniczeń architektury i prawdopodobieństwa wystąpienia uszkodzeń niebezpiecznych na godzinę. Funkcje diagnostyczne uważa się za oddzielne funkcje, które mogą mieć inne struktury niż SRCF i mogą być wykonywane przez: ten sam system, który wymaga diagnozowania lub przez inne podsystemy SRECS lub przez podsystem SRECS nie wykonujący SRCF. Funkcje diagnostyczne, które są stosowane łącznie z powiązanymi z nimi SRCF powinny spełniać wymagania dotyczące unikania uszkodzeń systematycznych i wymagania dotyczące kontroli uszkodzeń systematycznych. Prawdopodobieństwo uszkodzeń funkcji diagnostycznej należy brać pod uwagę przy szacowaniu PFH_D dla SRCF.

Wdrożenie SRECS powinno nastąpić zgodnie z udokumentowanym projektem. Należy przy tym zapewnić zgodność z odpowiednimi częściami specyfikacji wymagań bezpieczeństwa SRECS oraz spełnić odpowiednie wymagania dotyczące oprzewodowania.

8.3. Specyfikacja wymagań bezpieczeństwa oprogramowania SRECS wykorzystującego technikę RFID

W podsystemach SRECS wykorzystujących technikę RFID zawsze występuje, realizowana programowo, funkcja identyfikacji transponderów na podstawie odpowiedniej bazy danych oraz funkcje towarzyszące pozwalające na zarządzanie tą bazą. Również inne elementy tych podsystemów mogą wykorzystywać elementy programowalne.

Specyfikację wymagań bezpieczeństwa oprogramowania należy opracować dla każdego podsystemu w oparciu o specyfikację wymagań bezpieczeństwa SRCF i architekturę SRECS. W specyfikacji wymagań bezpieczeństwa oprogramowania należy uwzględnić:

- logikę wszystkich bloków funkcjonalnych przypisanych każdemu podsystemowi,
- interfejsy wejścia/wyjścia przypisane blokowi funkcjonalnemu,

- format i zakresy danych wejściowych i wyjściowych i ich odniesienie do bloków funkcjonalnych,
- dane istotne do opisania ograniczeń bloku funkcjonalnego,
- funkcje diagnostyczne innych urządzeń wchodzących w skład SRECS,
- funkcje umożliwiające maszynie osiągnięcie stanu bezpieczeństwa,
- funkcje odnoszące się do wykrywania, komunikowania i postępowania z defektami,
- funkcje odnoszące się do testów okresowych maszyny,
- funkcje zapobiegające nieautoryzowanym zmianom oprogramowania SRECS,
- interfejsy inne niż do SRCF,
- pojemności oraz czasy odpowiedzi.

Należy także stosować się do wymagań (specyfikacji) w zakresie parametryzacji oprogramowania SRECS. Jest to aspekt projektu traktowany jako związany z bezpieczeństwem i opisany w specyfikacji wymagań bezpieczeństwa oprogramowania. Należy zapewnić nienaruszalność wszystkich danych stosowanych do parametryzacji. W tym celu należy stosować odpowiednie narzędzia programowe, wykonywać odpowiednie analizy i badania (testy funkcjonalne i testy dynamiczne) oraz sporządzać dokumentację.

8.4. Informacja dla użytkownika SRECS wykorzystującego technikę

Wymagania opracowane na podstawie normy PN-EN 61496 dla urządzenia bezpieczeństwa wykorzystującego technikę RFID uwzględniają wymagania dotyczące informacji dla użytkownika. Niżej podane wymagania wynikające z normy PN-EN 62061 należy stosować uzupełniająco i odpowiednio. W przypadku podsystemów SRECS wykorzystujących możliwości techniki RFID poniższe wymagania dotyczące informacji dla użytkownika należy przyjąć za podstawowe i uzupełnić je odpowiednio wymaganiami uwzględniającymi specyfikę techniki RFID.

Informacja dla użytkownika SRECS, zgodnie z wymaganiami normy PN-EN 62061, powinna zawierać dokumentację dotyczącą instalowania, użytkowania i konserwacji, w tym:

- zwięzły opis wyposażenia, instalowania i montażu z zaznaczeniem specyfiki wykorzystanej techniki RFID,
- określenie przewidywanego zastosowania SRECS i wskazanie przypadków niewłaściwego użycia, szczególnie ze względu na ograniczenia techniki RFID,
- informacje o ograniczeniach środowiskowych z uwzględnieniem specyfiki techniki RFID,
- schematy poglądowe (blokowe) i schematy obwodów,
- określenie testów sprawdzających, częstości ich stosowania lub czasu życia,

- opis współdziałania między funkcjami SRECS i funkcjami sterowania elektrycznego maszyny,
- opis ochrony i środków koniecznych do zapewnienia separacji funkcji SRECS od funkcji systemu elektrycznego maszyny,
- opis ochrony i środków służących utrzymaniu bezpieczeństwa, jeżeli jest to konieczne do zawieszenia działania SRCF (np. w celu programowania bazy danych systemu identyfikacji transponderów),
- informacje dotyczące oprogramowania urządzeń bezpieczeństwa wykorzystujących technikę RFID (jeżeli jest to właściwe),
- opis wymaganych konserwacji obejmujący wprowadzanie zapisów do dziennika konserwacji maszyny, opis rutynowych czynności, procedury diagnostyki defektów, procedury sprawdzania po naprawie, opis narzędzi stosowanych do konserwacji.

8.5. Walidacja SRECS wykorzystującego technikę RFID

Walidacja jest potwierdzeniem przez sprawdzenie (tj. badania i analizy), że SRECS spełnia wymagania bezpieczeństwa funkcjonalnego w określonych zastosowaniach. Istotnym elementem walidacji SRECS wykorzystującego technikę RFID powinny być sprawdzenia zgodności przyjętych rozwiązań z odpowiednimi normami przedmiotowymi dotyczącymi techniki RFID.

Walidacja SRECS powinna być przeprowadzana zgodnie z wcześniej przygotowanym planem walidacji, który powinien obejmować walidację sprzętu i walidację oprogramowania. Walidacji należy poddać każdą SRCF, która została określona w specyfikacji wymagań SRECS oraz wszystkie procedury działania i konserwacji. Walidacja powinna zostać udokumentowana poprzez zapisy zawierające:

- identyfikację SRECS i identyfikację planu walidacji,
- identyfikację SRCF poddaną badaniom lub analizom z powołaniem się na wymagania,
- stosowane narzędzia i wyposażenie, w Tyn dane dotyczące wzorcowania,
- wyniki każdego badania,
- rozbieżności między oczekiwaniami i osiągniętymi wynikami.

Przy walidacji systematycznej nienaruszalności bezpieczeństwa SRECS należy stosować:

- badania funkcjonalne w celu wykrycia nieprawidłowości powstałych w fazie specyfikacji, projektowania i integracji oraz wykrycia defektów systematycznych,
- badania odporności na zaburzenia elektromagnetyczne w celu potwierdzenia spełnienia wymagań kompatybilności elektromagnetycznej,

- badania z zastosowaniem metody symulacji uszkodzeń, jeżeli oczekiwany wskaźnik uszkodzeń bezpiecznych ma przekraczać 90%.

W badaniach mogą być przydatne techniki analizy statycznej, analizy dynamicznej, analizy uszkodzeń i ich skutków, badania czarnej skrzynki, badania symulacyjne uszkodzeń, badania „najgorszego przypadku", a także zebrane doświadczenia eksploatacyjne i inne metody odpowiednie do zastosowanych rozwiązań technicznych.

8.6. Modyfikacje SRECS wykorzystujących technikę RFID

Modyfikacje SRECS mogą wynikać, między innymi, z: zmian wymagań specyfikacji bezpieczeństwa, warunków aktualnego użytkowania, doświadczeń zebranych podczas analizy wypadków lub zdarzeń prawie wypadkowych, wprowadzenia zmian materiałowych, modyfikacji maszyny lub sposobu jej działania.

Modyfikacje należy prowadzić w oparciu o przygotowany plan działania uwzględniający stosowanie procedur sterujących wprowadzaniem modyfikacji oraz należy je dokumentować poprzez zapisy zawierające: powody przeprowadzania modyfikacji, analizę skutków modyfikacji w zakresie jej wpływu na bezpieczeństwo funkcjonalne i dokumentację przeprowadzonych prac modyfikacyjnych.

SRECS wykorzystujące technikę RFID należy modyfikować w sposób nie naruszający wymagań dotyczących wykorzystywanych rozwiązań z dziedziny techniki RFID.

9. Podsumowanie

Wprowadzenie na rynek urządzenia bezpieczeństwa wykorzystującego technikę RFID i przeznaczonego do zmniejszania ryzyka związanego z użytkowaniem maszyn jest związane z obowiązkiem spełnienia wymagań wynikających z przepisów, w tym szczególnie wymagań zasadniczych dyrektywy 2006/42/WE (tzw. maszynowej, wdrożonej do prawa krajowego na mocy rozporządzenia Ministra Gospodarki z dnia 21 października 2008 r. w sprawie zasadniczych wymagań dla maszyn – Dz. U. Nr 199, poz. 1228). Przepisy te wymagają, aby takie urządzenia bezpieczeństwa były zaprojektowane i wykonane zgodnie z ustalonymi wymaganiami oraz poddane badaniom w kompetentnym laboratorium i ocenie typu przez jednostkę notyfikowaną w ramach procedury oceny zgodności z wymaganiami zasadniczymi w zakresie ochrony zdrowia i bezpieczeństwa. Po dopełnieniu procedur urządzenie może być oznakowane znakiem CE i można dla niego sporządzić deklarację zgodności WE.

Późniejsze zastosowanie urządzenia bezpieczeństwa wykorzystującego technikę RFID w związanych z bezpieczeństwem elementach systemów sterowania maszyn także poddane jest wymaganiu zapewnienia odpowiedniego poziomu bezpieczeństwa funkcjonalnego. Spełnienie tego wymagania jest możliwe w oparciu o istniejące normy

zharmonizowane z dyrektywą 2006/42/WE.

Powyższe wymagania przepisów są ogólne, nie wskazują szczegółowej ścieżki postępowania i dlatego wymagają uzupełnienia wymaganiami szczegółowymi. Na obecnym etapie rozwoju urządzeń bezpieczeństwa wykorzystujących technikę RFID nie są dostępne uznane dokumenty (normy, specyfikacje techniczne, raporty techniczne) formułujące takie wymagania. Powinny być one opracowane na zasadzie analogii do wymagań szczegółowych dotyczących podobnych urządzeń i podobnych zastosowań.

W niniejszym opracowaniu przedstawiono zagadnienia wypełniające lukę w zakresie wymagań szczegółowych dotyczących urządzeń bezpieczeństwa do maszyn wykorzystujących technikę RFID. Zaprezentowana analiza możliwości zastosowania techniki RFID w aplikacjach związanych z bezpieczeństwem użytkowania maszyn, opracowane wymagania szczegółowe pozwalające na odpowiednie zaprojektowanie, wykonanie i ocenę urządzeń bezpieczeństwa wykorzystujące tę technikę, a także metodyka badania i oceny typu tych urządzeń pozwalają na ich wprowadzanie na rynek w kategorii układów logicznych zapewniających funkcje bezpieczeństwa. Odpowiednia implementacja tych urządzeń w oparciu o przedstawioną metodykę projektowania związanych z bezpieczeństwem elementów systemów sterowania maszyn pozwala na spełnienie wymagań dotyczących bezpieczeństwa funkcjonalnego.

Niniejsze opracowanie zostało przygotowane w ramach zadania realizowanego w III etapie Programu Wieloletniego pn. „Poprawa bezpieczeństwa i warunków pracy” w Centralnym Instytucie Ochrony Pracy – Państwowym Instytucie Badawczym (CIOP-PIB). CIOP-PIB jako jednostka notyfikowana w obszarze dyrektywy 2006/42/WE może również podjąć się badań i oceny typu urządzeń bezpieczeństwa wykorzystujących technikę RFID i aplikacji tych urządzeń w związanych z bezpieczeństwem systemach sterowania maszyn.

10. Piśmiennictwo

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. ISO/IEC 18000-1:2004. Information technology – Radio frequency identification for item management – Part 1: Reference architecture and definition of parameters to be

standardized;
5. ISO/IEC 18000-2:2004. Information technology – Radio frequency identification for item management – Part 2: Parameters for air interface communications below 135 kHz;
6. ISO/IEC 18000-3:2004. Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz;
7. ISO/IEC 18000-4:2004. Information technology – Radio frequency identification for item management – Part 4: Parameters for air interface communications at 2,45 GHz;
8. ISO/IEC 18000-6:2004. Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz;
9. ISO/IEC 18000-7:2004. Information technology – Radio frequency identification for item management – Part 7: Parameters for active air interface communications at 433 MHz;
10. ISO/IEC 14443-1:2008. Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics;
11. ISO/IEC 14443-2:2001. Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface;
12. ISO/IEC 14443-3:2001. Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision;
13. ISO/IEC 14443-4:2008. Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol;
14. ISO/IEC 15693-1:2000. Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 1: Physical characteristics;
15. ISO/IEC 15693-2:2006. Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 2: Air interface and initialization;
16. ISO/IEC 15693-3:2001. Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 3: Anticollision and transmission protocol;
17. PN-ISO 11784:2008 Radiowa identyfikacja zwierząt -- Struktura kodowa
18. PN-ISO 11785:2008 Radiowa identyfikacja zwierząt -- Koncepcja techniczna
19. 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;
20. Rozporządzenie Ministra Gospodarki z dnia 21 października 2008 r. w sprawie zasadniczych wymagań dla maszyn – Dz. U. Nr 199, poz. 1228;
21. Przewodnik do stosowania dyrektywy 2006/42/WE;
22. 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);

23. PN-EN ISO 12100:2012P Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka;
24. PN-EN ISO 13849-1:2008E Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1. Ogólne zasady projektowania;
25. PN-EN ISO 13849-2:2013-04 Bezpieczeństwo maszyn -- Elementy systemów sterowania związane z bezpieczeństwem -- Część 2: Walidacja;
26. PN-EN 62061:2008 Bezpieczeństwo maszyn -- Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem;
27. PN-EN 62061:2008/A1:2013-06 Bezpieczeństwo maszyn -- Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem;
28. PN-EN 62061:2008/A2:2016-01 Bezpieczeństwo maszyn -- Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem;
29. PN-EN 61496-1:2014-02 Bezpieczeństwo maszyn -- Elektroczułe wyposażenie ochronne -- Część 1: Wymagania ogólne i badania;
30. Projekt "Recommendation for use" przygotowany przez: Vertical Group No 11 - Safety Components of European Co-ordination of Notified Bodies - Machinery Directive 2006/42/EC + Amendment, dotyczący: RFID based protective devices (Urządzenia bezpieczeństwa wykorzystujące technikę RFID);