Kamil SUWAJ[1]

Opiekun naukowy: Jarosław JANUSZ[2]

RFID W PRZEMYŚLE

Streszczenie: W artylule opisano tagi RFID, budowę oraz możliwości programowania transponderów w zależności od standardu. Sposób wykorzystywania czytników RFID do identyfikacji zarówno osób, jak i przedmiotów. Podłączenie czytnika emulującego klawiaturę USB do sterownika PLC.

Słowa kluczowe: RFID, radiowa identyfikacja, tagi RFID, transpondery

RFID IN INDUSTRY

Summary: The article describes RFID tags, structure and programming possibilities of transponders depending on the standard. How to use RFID readers to identify people and objects. Connecting a reader emulating a USB keyboard to a PLC controller.

Keywords: RFID, radio frequency identification, RFID tags, transponders

1. Co to jest technologia RFID?

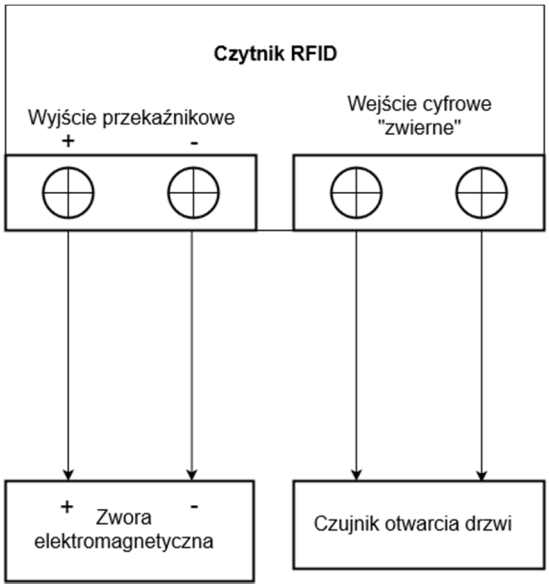
RFID jest to technologia wykorzystująca fale radiowe do identyfikacji zarówno osób jak i przedmiotów na odległość. Budowa systemu RFID jest względnie prosta. Jeżeli mamy zamiar identyfikować ludzi, do konkretnej osoby przypisujemy tag RFID, który może być naklejka, brelok, karta lub jakikolwiek inny przedmiot, który zawiera w sobie układ elektroniczny z anteną pozwalającą na odczyt danych. Aby wykorzystać system RFID do zdalnej kontroli przepływu towarów [1], [4]: do przedmiotu przyczepia się odpowiedni tag RFID z kodem UID odpowiadający określonemu przedmiotowi lub w przypadku tagów RFID z możliwością odczytu bloków pamięci: odczytuje się blok pamięci, na którym zapisane są informacje o produkcie w postaci heksadecymalnej.

---

[1] inż., Wydział Budowy Maszyn i Informatyki, Akademia Techniczno-Humanistyczna w Bielsku-Białej

[2] dr inż., Wydział Budowy Maszyn i Informatyki, Akademia Techniczno-Humanistyczna w Bielsku-Białej, jjanusz@ath.bielsko.pl

Co ciekawe, kilka-kilkanaście lat temu uważano, że technologia RFID nie ma szans na to, aby była stosowana masowo w aplikacjach, ponieważ cena pojedynczego tagu RFID (dla jednej osoby, bądź na jeden towar) kosztowała ok. 1 euro. W połączeniu z relatywnie drogimi czytnikami dyskwalifikowało systemy RFID już na starcie [2].
W dzisiejszych czasach, gdy ceny transponderów i czytników przestały decydować o tym czy wdrożyć system, czy nie, największym hamulcem rozwoju tej technologii jest brak pomysłu na aplikację lub rozwiązanie dla którego technologia zdalnej identyfikacji radiowej mogłaby przynieść zysk i oszczędności dla przedsiębiorstwa. Jednak coraz częściej udaje się obejść ten problem, ponieważ wartość całego rynku RFID z roku na rok rośnie.
Najczęściej spotykanym rynkiem RFID jest kontrola czasu pracy [3]. Pracownicy w momencie przyjścia do zakładu pracy oraz po zakończonym dniu przykładają kartę RFID do czytnika, dzięki temu przedsiębiorca nie musi prowadzić fizycznej listy obecności.
Również szkolnictwo rozpoczęło wdrażanie systemów RFID do szkół, aby tylko osoby upoważnione (posiadające tag RFID) mogły wejść do budynku szkoły. W takim przypadku można zastosować czytniki z wbudowanymi wyjściami i wejściami. Dzięki temu jeżeli czytnik rozpozna tag RFID, czasowo wyłączy wyjście przekaźnikowe, które zwolni magnes. Natomiast do wejścia cyfrowego może zostać podłączony czujnik otwarcia drzwi, który zasygnalizuje zbyt długi stan otwarcia drzwi.



Rysunek 1. Przykładowe wykorzystanie czytnika RFID w szkołach

2. Rodzaje standardów RFID

Na rynku istnieje coraz więcej różnych standardów RFID. Dodatkowo z biegiem czasu systemy RFID przenoszą się do coraz wyższych częstotliwości pracy, dzięki

czemu można uzyskać większy zasięg oraz możliwość odczytu kilku tagów jednocześnie umieszczonych obok siebie.
Podział tagów ze względu na zakres częstotliwości pracy prezentuje się następująco:

- LF (ang. low frequency) – tagi działające w częstotliwości 124 kHz, 125 kHz lub 135 kHz,
- HF (ang. high frequency) – tagi działające w częstotliwości 13,56/27 MHz,
- UHF (ang. ultrahigh frequency) – tagi działające w częstotliwości 865-868 MHz oraz 2,4-5,8GHz.

W zależności od wykorzystywanej częstotliwości, tagi używane są w różnych obszarach zastosowań. Transpondery LF są najczęściej wykorzystywane do kontroli dostępu, czy znakowania zwierząt. Wadą tagów LF jest to, że w zasięgu czytnika można znajdować się tylko jeden transponder. W przypadku znaczników HF rośnie zasięg odczytu do nawet 1m. Zastosowanie technologii HF RFID to różne programy lojalnościowe, karty miejskie, karty biblioteczne, identyfikatory i przepustki, a także karty płatnicze. Stosując chip UHF można uzyskać zasięg odczytu do 8m. Co więcej UHF RFID pozwala na niezwykle szybką transmisję danych oraz na odczyt kilku znaczników jednocześnie. Te chipy są wykorzystywane do kontroli procesów logistycznych, kontroli stanów magazynowych czy nawet do pomiaru czasu w rywalizacjach sportowych.
Należy pamiętać, że nie wszystkie standardy RFID pozwalają na zapis danych. Wiele tagów to karty tylko do odczytu. Taki znacznik posiada jedynie kod UID (unikalny numer identyfikacyjny) zapisany w pamięci karty przez producenta, którego użytkownik nie może zmienić, ani zmodyfikować. Korzystając z takich transponderów, należy napisać program, który po odczycie karty przez czytnik, będzie porównywał kod UID z bazą danych.
Innym rozwiązaniem jest zakup czytnika z wbudowaną pamięcią wewnętrzną. Wielu producentów zapewnia możliwość zdalnego wprowadzania kodów UID do pamięci czytnika, dzięki czemu administrator nie musi posiadać fizycznego transpondera, a jedynie numer UID, do którego przypisze odpowiedniego użytkownika.
W niniejszym artykule zostaną poruszone kwestie struktury danych, możliwości odczytu i zapisu oraz bezpieczeństwa dla 2 standardów:

- Unique,
- Mifare® Classic 1k.

3. Struktura danych, odczyt, zapis i bezpieczeństwo

Analiza zostanie rozpoczęta od standardu UNIQUE, który jest kompatybilny z układami EM4100 i EM4102 [5]. Ten znacznik charakteryzuje się pracą w zakresie LF, a dokładniej 125kHz. Kod UID, czyli unikalny numer identyfikacyjny w przypadku standardu UNIQUE to 5 bajtów, czyli 10 znaków hex. Cała pamięć standardu wynosi 64 bity. Transpondery UNIQUE posiadają pamięć tylko do odczytu. Od użytkownika nie jest wymagane kodowanie tych znaczników. Wszystkie dane zapisane na karcie są tam umieszczane przez producenta. Zasięg takiego transpondera wynosi do 15cm, aby osiągnąć taką odległość odczytu konieczna jest duża antena czytnika i dobrej jakości chip, dlatego najczęściej spotykany zasięg kart UNIQUE wynosi do 5cm.
UNIQUE to jeden z najprostszych standardów RFID oraz jeden z najczęściej stosowanych z uwagi na jego łatwość wdrażania. Użytkownik otrzymuje transponder,

który jest już zaprogramowany. Wystarczy, że nowe znaczniki zostaną wprowadzone do bazy danych.
Standard ten głęboko zakorzenił się w systemach rejestracji czasu pracy, ponieważ jest niezwykle tani, a pracodawcy najczęściej patrzą na niewielkie koszty wprowadzenia nowych systemów. Wykorzystanie systemu RFID do rejestrowania czasu pracy opartych na standardzie UNIQUE wiąże się z kosztami zakupu czytnika z pamięcią wewnętrzną. Ceny takich urządzeń niejednokrotnie nie przekraczają 1000zł netto, przy pamięci wbudowanej do 10 000 kart. Krok w stronę automatyzacji zakładu pracy pomaga kontrolować czas produktywny pracowników, długość trwania przerw, a na koniec dnia lub miesiąca pomaga automatycznie sporządzić listę obecności lub wygenerować odpowiednie raporty.
Transpondery UNIQUE są wykorzystywane w systemach kontroli dostępu. Jest to o tyle ciekawe, że jest on niezwykle niebezpieczny. Jak zostało wyżej opisane karty posiadają typ pamięci tylko do odczytu (Read Only), jednak skopiowanie numeru tagu na inną, jeszcze niezaprogramowaną kartę trwa zaledwie kilka sekund.
Aby skopiować transponder UNIQUE wystarczy kupić czytnik, który posiada funkcję programowania oraz niezaprogramowaną kartę. Przebieg operacji kopiowania tagu polega na tym, że kartę którą chcemy skopiować przykładamy do czytnika, w którym zostanie zapisany odczytany numer UID. W przypadku niektórych programatorów jest możliwość ręcznego wprowadzenia kodu. Następnie włączamy funkcję programowania i przykładamy do czytnika czystą kartę. Od tego momentu na obu kartach będzie ten sam numer.
Z uwagi na to, że tak łatwo można skopiować kod UID, coraz więcej przedsiębiorców decyduje się na przejście na bardziej zabezpieczone systemy RFID, takie jak te oparte na standardzie Mifare.
Standard UNIQUE jest niezwykle powszechnie stosowany, jednak transpondery te są niezwykle niebezpieczne z uwagi na łatwość kopiowania. Zasięg takiego chipa wynosi jedynie około 5cm. Jednak plusem tego standardu jest jego niewysoka cena: zarówno czytników jak i znaczników.
Standard Mifare Classic 1k [8], [9], [10] został opracowany już w 1994r. przez firmę Philips, dzisiaj NXP Semiconductors (wersja 1k). Transponder podobnie jak standard UNIQUE posiada unikalny numer identyfikacyjny jednak w tym przypadku długość kodu UID to 4 lub 7 bajtów, czyli 8 lub 14 znaków hex. Cała pamięć standardu wynosi 1024 bajty w przypadku Mifare Classic 1k lub 4096 bajtów dla Mifare Classic 4k. Porównując wymienione standardy do 64 bitów (8 bajtów) tagu UNIQUE pamięć EEPROM transpondera Mifare jest ponad 100-krotnie większa. Chipy Mifare posiadają funkcję zarówno odczytu jak i zapisu. Producenci gwarantują do 10 lat przechowywania danych na karcie oraz nawet do 200 000 operacji zapisu danych.
Transpondery Mifare działają w zakresie częstotliwości 13.56MHz, co oznacza, że należą do grupy HF. Zasięg działania transponderów wynosi do 10 cm. Znaczniki Mifare przejmują rynek systemów zabezpieczeń po transponderach UNIQUE z uwagi na możliwość zabezpieczenia zawartości karty. Dodatkowo, standard ten stosowany jest jako:

- karty biblioteczne,
- karty miejskie,
- karty parkingowe,
- identyfikatory systemów bezpieczeństwa opartych na RFID,
- legitymacje studenckie.

Rysunek 2. Przykładowa karta Mifare – legitymacja studencka

Struktura transponderów Mifare Classic 1k składa się z 1024 bajtów pamięci EEPROM (16 sektorów po 4 bloki, każdy o długości 16 bajtów).

SEKTOR	BLOK	0 1 2 3 4 5	6 7 8 9	10 11 12 13 14 15	OPIS	
15	3	klucz A	BITY DOSTĘPU	klucz B	SEKTOR TRAILER 15	63
4 bloki	2				DANE	62
	1				DANE	61
	0				DANE	60
:	:					•
:	:					•
:	:					•
1	3	klucz A	BITY DOSTĘPU	klucz B	SEKTOR TRAILER 1	7
4 bloki	2				DANE	6
	1				DANE	5
	0				DANE	4
0	3	klucz A	BITY DOSTĘPU	klucz B	SEKTOR TRAILER 0	3
4 bloki	2				DANE	2
	1				DANE	1
	0	DANE PRODUCENTA			BLOK PRODUCENTA	0

Rysunek 3. Struktura tagu Mifare Classic 1k (na podstawie materiałów NXP)

Dla danych użytkownika przeznaczono 752B z 1024B. Pozostałe 272B to 16 bloków o nazwie „Sector Trailer" oraz jeden blok przeznaczony na dane producenta (blok 0 w sektorze 0) . W skład bloku producenta wchodzi kod UID oraz pozostałe dane producenta. W przypadku bloków Sector Trailer jest to:

- klucz A o długości 6 bajtów,
- klucz B o długości 6 bajtów,
- Access Bits, czyli bity dostępu o długości 4 bajtów.

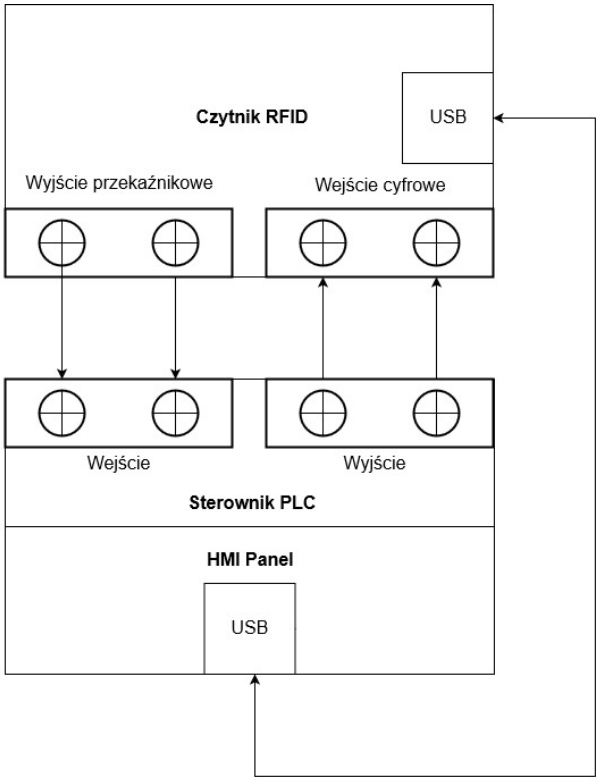
Domyślnymi kluczami nowych transponderów Mifare są wartości FFFFFFFFFFFF zarówno dla klucza A oraz klucza B.
W przypadku bitów dostępu, domyślnymi wartościami są 0xFF 0x07 0x80 oraz jeden bajt przeznaczony dla użytkownika. Modyfikując wartości bitów dostępu można całkowicie zablokować dostęp do zawartości sektora lub zezwolić tylko na odczyt danych kluczem B, natomiast zapis zablokować. Zezwolenie na zmianę kluczy A lub B również zależy od bitów dostępu. Nieumiejętna modyfikacja tego bloku może całkowicie zablokować sektor.

4. Komunikacja z czytnikami RFID

Z uwagi na stale zwiększające się grono producentów aparatury RFID oraz walkę o klienta, użytkownik dysponujący odpowiednim budżetem może kupić czytnik z takim protokołem komunikacji, jaki jest mu potrzebny. Wielu producentów czytników RFID nadal umieszcza w swoich urządzeniach RS485 w celu łatwej integracji ze sterownikami PLC poprzez Modbus RTU. Niezwykle często spotykane są czytniki posiadające wbudowany serwer WWW, w którym można ustawić wymagany protokół komunikacji [6].
Protokoły komunikacji występujące w czytnikach RFID ze złączem RJ45:

- protokół HTTP w trybie klient,
- protokół HTTP w trybie serwer,
- protokół Modbus TCP,
- protokół Modbus RTU,
- sterowanie przez SNMP.

Najnowsze czytniki RFID posiadają wbudowane wejścia oraz wyjścia, aby urządzenia mogły autonomicznie sterować i kontrolować np. drzwi zewnętrzne. Bardziej zaawansowane modele posiadają wbudowany czujnik temperatury oraz wilgotności. Z takiej konfiguracji urządzeń korzystają firmy transportujące różne produkty. Jeżeli na produkcie zostanie umieszczony znacznik RFID posiadający możliwość zapisu danych (np. Mifare lub ICODE®) to w momencie dojazdu do miejsca przeładunku, czytniki odczytują dane z chipa, dopasowują towary do odpowiednich baz danych i sprawdzają czy np. aktualna temperatura nie jest nieodpowiednia dla danego produktu. W przypadku przekroczenia dopuszczalnej wartości, czytnik może to zakomunikować sygnałem dźwiękowym lub wizualnym. Dodatkowo na transponderach przymocowanych do produktów zostają zapisane dane z czujników, w celu późniejszej ich archiwizacji i ewentualnych badań statystycznych [7].
Niektórzy producenci systemów RFID posiadają w swojej ofercie czytniki oferujące emulację klawiatury USB. Polega to na tym, że po zbliżeniu karty do czytnika, urządzenie może wysłać do komputera / sterownika PLC (panelu HMI) kod UID lub zawartość transpondera w postaci znaków wprowadzanych z klawiatury.



Rysunek 4. Przykładowa konfiguracja sterownika PLC, panelu HMI z czytnikiem RFID emulującym klawiaturę USB.

W momencie odczytania nowego transpondera, czytnik włącza swoje wyjście, powodując włączenie się wejścia w sterowniku PLC. W tym czasie użytkownik może np. ustawić kursor we właściwym polu tekstowym, aby dokonać autoryzacji. Po ustawieniu się w odpowiednim polu, użytkownik włącza wyjście w sterowniku PLC, które powoduje pojawienie się stanu wysokiego na wejściu czytnika RFID. Urządzenie RFID wysyła dane do panelu operatorskiego, po czym następuje autoryzacja użytkownika. W czytniku zostaje wyłączone wyjście, pojawia się stan niski na wejściu w sterowniku PLC i można zbliżyć kolejną kartę do czytnika.
W taki sposób producenci zwiększają możliwości na przeprowadzenia komunikacji ze sterownikami PLC i wdrażanie nowego systemu. Nie tylko „tradycyjne" protokoły komunikacji takie jak Modbus RTU są aktualnie dostępne. Czytniki emulujące klawiaturę również mogą odpowiadać za interakcje z użytkownikiem.

5. Podsumowanie i wnioski

Zagadnienie dotyczące systemów RFID jest tak rozległym tematem, że może dotyczyć niemalże każdej dziedziny życia codziennego. Może się okazać, że w niedalekiej przyszłości większość ludzi będzie korzystać z identyfikacji radiowej

w celu dostania się do swojego miejsca pracy lub po odbiór dziecka ze szkoły.
Porównując standard UNIQUE oraz Mifare Classic 1k pod względem bezpieczeństwa, lepiej jest zastosować standard Mifare, ponieważ w tym przypadku mamy przynajmniej niewielką ochronę danych zawartych na karcie przez wymaganie wprowadzenia klucza autoryzującego. Oczywiście dla osób pracujących z tagami RFID na co dzień, złamanie czystej karty Mifare (bez żadnego procesora szyfrującego) nie będzie wielkim problem. Natomiast nieporównywalnie łatwiej i szybciej jest skopiować tag w standardzie UNIQUE.
Rozwój techniki oraz powstawanie nowych producentów systemów RFID wpływa korzystanie na możliwości tworzenia systemów zarządzenia opartych na identyfikacji radiowej. Na rynku istnieje wiele osób specjalizujących się w dziedzinie RFID, dlatego jednymi problemami z zaprojektowaniem systemu zdalnej identyfikacji mogą być kwestie finansowe oraz ewentualny brak pomysłu na rozwój.
Ważnymi czynnikami podczas projektowania systemu RFID jest wybór zakresu częstotliwości pracy transpondera, na którym będzie się opierać projekt. Oprócz kwestii związanej z bezpieczeństwem, należy się zastanowić, czy nie będzie wymagane odczytywanie danych z kilku znaczników jednocześnie. W przypadku transponderów LF mamy do czynienia z niewielkim zasięgiem odczytu oraz można odczytywać tylko jeden transponder, aktualnie znajdujący się w polu czytnika. W przypadku zakresu pracy UHF takie problemy nie występują. Dodatkowym atutem są znacznie większe szybkości odczytu danych, przez co możemy zastosować takie tagi przy produkcji masowej Minusem jest to, że takie rozwiązania są znacznie droższe.

LITERATURA

1. BARTCZAK K.: Zastosowanie RFID w logistyce. Logistyka 4/2015,s.55-63.
2. BESZ B.: Czy technologia RFID pozwala zaoszczędzić pieniądze? Elektronik, lipiec 2019, s.40-41.
3. JAKUBSKI B., ŻYCIAK M., Rozwój oraz obszary zastosowań technologii RFID, Pomiary, Automatyka, Kontrola, 7/ 2009.
4. RFID, NFC, czyli zdalna identyfikacja radiowa. Elektronik, lipiec 2019, s.26-37.
5. Serwis internetowy *https://www.nfc24.pl*/, dostęp: 11.11.2019r.
6. Serwis internetowy *https://www.fidpolska.pl*/, dostęp: 11.11.2019r.
7. Serwis internetowy *https://www.inveo.com.pl*/, dostęp: 11.11.2019r.
8. Serwis internetowy *https://rfid.zone*/, dostęp: 11.11.2019r.
9. Serwis internetowy *http://rfid-lab.pl*/, dostęp: 12.11.2019r.
10. Dokumentacja techniczna kart Mifare Classic firmy NXP *https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf*, dostęp:11.11.2019.