Patrycja Paradowska
numer albumu: 244952

30 kwietnia 2020r.
prowadzący: dr inż. Przemysław Błaśkiewicz

Systemy wbudowane - projekt

System blokady drzwi i kontroli dostępu

Opis przypadków użycia

1 Wstęp

System blokady drzwi i kontroli dostępu do danego pomieszczenia umożliwia niedopuszczenie do chronionych stref osób niemających uprawnień. Jedynie ktoś, kto posiada odpowiednią kartę i zna poprawny numer PIN, jest w stanie odblokować drzwi i wejść do obiektu. Poniżej opisano kilka najważniejszych przypadków użycia tego systemu.

2 Przypadek użycia - "Otwieranie drzwi"

Nazwa przypadku użycia: Otwieranie drzwi	**Numer PU:** 1	**Priorytet:** wysoki
Główny aktor: Użytkownik, System	**Typ PU:** niezbędny	
Kto i co zyskuje na wykonaniu tego PU: Użytkownik dzięki temu przypadkowi użycia może otworzyć drzwi i wejść do danego pomieszczenia, do którego istnieje zabezpieczenie naszym systemem.		
Krótki opis: Ten przypadek użycia opisuje niezbędną czynność, która jest jednym z głównych celów działania systemu.		
Trigger: Użytkownik	**Typ:** zewnętrzny	
Warunki początkowe: Użytkownik znajduje się na zewnwątrz pomieszczenia, posiada odpowiednią kartę oraz swój kod PIN, a urządzenie ma naładowane baterie.		
Scenariusz podstawowy: 1. Użytkownik podchodzi do urządzenia i przykłada kartę do czytnika RFID.(S1) 2. Jeśli dane są poprawne, to użytkownik widzi na wyświetlaczu komunikat "ENTER PASSWORD" oraz może wpisać hasło. 3. Użytkownik wpisuje swój PIN za pomocą klawiatury. 4. Użytkownik wciska przycisk OK, aby zatwierdzić hasło.(S2) 5. Jeśli hasło jest poprawne, to użytkownik widzi na wyświetlaczu komunikat "DOOR OPENED" i może już nacisnąć klamkę, aby otworzyć drzwi. (S3) 6. Użytkownik otrzymuje wiadomość na telefon, że drzwi zostały otwarte.		

Przepływ wewnętrzny:
S1. System odczytuje i weryfikuje dane użytkownika.
S2. System sprawdza wprowadzone hasło, czy jest ono zgodne z tym, które jest przypisane do właściciela wcześniej odczytanej karty.
S3. System odblokowuje blokadę uniemożliwiającą dotychczasowe otwarcie drzwi.

Scenariusz alternatywny/wyjątkowy:
Ex.1. Jeśli użytkownik znajduje się w środku obiektu, to nie musi przechodzić przez ten scenariusz, gdyż drzwi od wewnątrz można otworzyć normalnie (nie są blokowane od wewnątrz).
Ex.2. Jeśli karta jest niepoprawna, to pojawia się sygnał informujący o błędzie w postaci krótkiego dźwięku, migającej na czerwono diody oraz komunikatu na wyświetlaczu "SORRY, WRONG CARD". Nie można dalej kontynuowac procedury otwierania drzwi.
Ex.4. Jeżeli użytkownik przekroczył limit czasowy (30 sekund) na podanie hasła, to system zablokuje możliwość wpisywania PIN-u, pojawi się komunikat o konieczności przyłożenia ponownie karty do czytnika, aby rozpocząć od nowa (od kroku 1.).
Ex.4. Jeżeli użytkownik pomyli się w trakcie wpisywania PIN-u, to może wcisnąć przycisk RESET - resetujący wpisywany numer.
Ex.5. Jeżeli hasło było niepoprawne, to miga czerwona dioda oraz pojawia się komunikat na wyświetlaczu "WRONG PASSWORD". Użytkownik dostaje powiadomienie na telefon, że próbowano otworzyć drzwi jego kartą za pomocą błędnego hasła. Przechdzi on znów do kroku 3. scenariusza podstawowego, może ponownie wprowadzić PIN. Ma na to łącznie 3 próby (każda po 30 sekund) i jeśli trzy razy wpisze numer niepoprawnie, to system zablokuje dostęp temu użytkownikowi na 15 minut (oraz wyśle powiadomienie, że dostęp został zablokowany), a po upływie tego czasu ponownie będzie mógł on skorzystać ze standardowego przebiegu procedury, zaczynając od kroku 1. scenariusza głównego.
Ex.6. Jeżeli użytkownik nie skorzysta z możliwości otwarcia drzwi, to po 10 sekundach ponownie zablokują się one automatycznie.
Ex. Podczas trwania procedury otwierania drzwi może dojść do nagłego braku zasilania i urządzenie wyłączy się, uniemożliwiając otwarcie drzwi użytkownikowi. Wtedy będzie konieczna natychmiastowa wymiana baterii przez użytkownika.

3 Przypadek użycia - ”Blokowanie drzwi”

Nazwa przypadku użycia: Blokowanie drzwi	**Numer PU:** 2	**Priorytet:** wysoki
Główny aktor: Użytkownik, System	**Typ PU:** kluczowy	
Kto i co zyskuje na wykonaniu tego PU: Użytkownik dzięki temu przypadkowi użycia uzyskuje zamknięcie i blokadę drzwi. Ma to na celu uniknięcie wtargnięcia do danego pokoju lub budynku osób niepożądanych, które nie mają do tego praw.		
Krótki opis: Ten przypadek użycia opisuje niezbędną czynność, która jest jednym z głównych celów działania systemu. Podczas ”spoczynku” klamka zamka przy zamkniętych drzwiach znajdująca się po zewnętrznej stronie pomieszczenia jest nieaktywna. Oznacza to, że jej naciśnięcie nie powoduje schowania się elementu blokującego i otwarcia drzwi. Może to zrobić dopiero użytkownik za pomocą PU nr 1.		
Trigger: Użytkownik	**Typ:** zewnętrzny	
Warunki początkowe: Drzwi nie mogą być otwarte/niedomknięte, a urządzenie musi mieć naładowane baterie.		
Scenariusz podstawowy: 1. Użytkownik wchodzi do lub wychodzi z pomieszenia i zamyka za sobą drzwi. 2. System zablokowuje drzwi za pomocą elementu blokującego. 3. Na ekranie pojawia się komunikat ”DOOR CLOSED” i dioda miga raz na zielono.		
Scenariusz alternatywny/wyjątkowy: Ex.1.1. Jeśli drzwi są otwarte lub przez przypadek niedomknięte przez dłużej niż 3 minuty, to system po tym czasie wyświetla na ekranie komunikat ”PLEASE, CLOSE THE DOOR!” oraz dioda miga na czerwono, dopóki ktoś nie zamknie drzwi, a do użytkownika zostaje wysłane powiadomienie na telefon o zaistniałej sytuacji i konieczności zamknięcia drzwi. Ex.1.2. Użytkownik po wykonaniu PU nr 1. mógł nie skorzystać z otwarcia drzwi w ciągu 10 sekund i są one wtedy automatycznie blokowane. Ex.2. Może dojść do nagłego braku zasilania i urządzenie wyłączy się, uniemożliwiając blokadę drzwi. Wtedy będzie konieczna natychmiastowa wymiana baterii przez użytkownika.		

4 Przypadek użycia - ”Zmiana numeru PIN”

Nazwa przypadku użycia: Zmiana numeru PIN	**Numer PU:** 3	**Priorytet:** średni
Główny aktor: Użytkownik, System	**Typ PU:** opcjonalny	
Kto i co zyskuje na wykonaniu tego PU: Użytkownik dzięki temu przypadkowi użycia uzyskuje możliwość zmiany obecnego hasła, na przykład początkowo do danej karty jest przypisany domyślny kod PIN ”123456” i użytkownik może od razu przy pierwszym skorzystaniu z systemu, ale także w poźniejszym czasie, zmienić go na swój własny.		
Krótki opis: Ten przypadek użycia opisuje czynność, która jest opcjonalna, ale usprawnia działanie systemu i wygodę w użytkowaniu przez klienta.		
Trigger: Użytkownik	**Typ:** zewnętrzny	
Warunki początkowe: Użytkownik posiada już obecne hasło, system jest gotowy działania i podłączony do zasilania.		

Scenariusz podstawowy:
1. Użytkownik podchodzi do urządzenia i przykłada kartę do czytnika RFID.(S1)
2. Jeśli dane są poprawne, to użytkownik widzi na wyświetlaczu komunikat "ENTER PASSWORD".
3. Zamiast standardowego podania numeru PIN, użytkownik klika na klawiaturze trzy razy z rzędu "*".
4. Na ekranie wyświetla się komunikat "ENTER CURRENT PASSWORD" i użytkownik musi wpisać obecne hasło.
5. Użytkownik wciska przycisk OK, aby zatwierdzić hasło.(S2)
6. Na ekranie wyświetla się komunikat "ENTER NEW PASSWORD".
7. Użytkownik podaje nowy numer PIN (którego ilość cyfr musi zawierać się w przedziale 6-10).
8. Użytkownik wciska przycisk OK, aby zatwierdzić hasło.(S3)
9. Użytkownik otrzymuje powiadomienie na telefon, że numer PIN został zmieniony.

Przepływ wewnętrzny:
S1. System odczytuje i weryfikuje dane użytkownika.
S2. System sprawdza wprowadzone hasło, czy jest ono zgodne z tym, które jest przypisane do właściciela wcześniej odczytanej karty.
S3. System zapamiętuje nowe hasło użytkownika

Scenariusz alternatywny/wyjątkowy:
Ex.2. Jeśli karta jest niepoprawna, to pojawia się sygnał informujący o błędzie w postaci krótkiego dźwięku, migającej na czerwono diody oraz komunikatu na wyświetlaczu "SORRY, WRONG CARD".
Ex.3. Użytkownik nie naciśnie trzykrotnie "*" tylko inną sekwencję klawiszy, którą system potraktuje jako błędne wpisanie numeru PIN.
Ex.5. Jeżeli użytkownik przekroczył limit czasowy (30 sekund) na wpisanie hasła, to system zablokuje możliwość podawania numeru PIN, pojawi się komunikat o konieczności przyłożenia ponownie karty do czytnika i rozpoczęcie od nowa (od 1. kroku scenariusza).
Ex.6. Jeżeli wpisane obecne hasło było niepoprawne, to miga czerwona dioda oraz pojawia się komunikat na wyświetlaczu "WRONG PASSWORD", użytkownik dostaje powiadomienie na telefon, że próbowano zmienić kod PIN, używając błędnego hasła. Może on ponownie wprowadzić obecny PIN. Ma na to łącznie 3 próby (każda po 30 sekund) i jeśli trzy razy wpisze numer niepoprawnie, to system zablokuje dostęp temu użytkownikowi na 15 minut (oraz wyśle powiadomienie, że dostęp został zablokowany), a po upływie tego czasu ponownie będzie mógł on skorzystać ze standardowego scenariusza PU zmiany numeru PIN, zaczynając od kroku 1. scenariusza głównego.
Ex.7. Ilość cyfr jest niepoprawna (najmniej 6, najwięcej 10), na ekranie pokazuje się komunikat o błędzie i prośbie ponownego wpisania nowego hasła. Po 3 błędnych próbach ustawienia nowego numeru PIN, system zablokuje dostęp temu użytkownikowi na 15 minut (oraz wyśle powiadomienie, że dostęp został zablokowany), a po upływie tego czasu ponownie będzie mógł on skorzystać ze standardowego scenariusza PU zmiany numeru PIN, zaczynając od kroku 1. scenariusza głównego.

5 Przypadek użycia - ”Przypomnienie numeru PIN”

Nazwa przypadku użycia: Przypomnienie numeru PIN	**Numer PU:** 4	**Priorytet:** średni
Główny aktor: Użytkownik, System	**Typ PU:** opcjonalny	
Kto i co zyskuje na wykonaniu tego PU: Użytkownik dzięki temu przypadkowi użycia uzyskuje możliwość przypomnienia obecnego hasła w sytuacji, gdy nie pamięta ustalonego wcześniej PIN-u.		
Krótki opis: Ten przypadek użycia opisuje czynność, która jest opcjonalna, ale usprawnia działanie systemu i wygodę w użytkowaniu przez klienta.		
Trigger: Użytkownik	**Typ:** zewnętrzny	
Warunki początkowe: Użytkownik posiada już obecne hasło, system jest gotowy działania i podłączony do zasilania.		
Scenariusz podstawowy: 1. Użytkownik podchodzi do urządzenia i przykłada kartę do czytnika RFID.(S1) 2. Jeśli dane są poprawne, to użytkownik widzi na wyświetlaczu komunikat ”ENTER PASSWORD”. 3. Zamiast standardowego podania numeru PIN, użytkownik klika na klawiaturze trzy razy z rzędu ”#”. 4. Na ekranie wyświetla się komunikat ”PASSWORD HAS BEEN SENT”. 5. Użytkownik otrzymuje powiadomienie na telefon ze starym hasłem.		
Przepływ wewnętrzny: S1. System odczytuje i weryfikuje dane użytkownika.		
Scenariusz alternatywny/wyjątkowy: Ex.2. Jeśli karta jest niepoprawna, to pojawia się sygnał informujący o błędzie w postaci krótkiego dźwięku, migającej na czerwono diody oraz komunikatu na wyświetlaczu ”SORRY, WRONG CARD”. Ex.3. Jeżeli użytkownik przekroczył limit czasowy (30 sekund) na wpisanie znaków na klawiaturze, to system zablokuje możliwość wpisywania, pojawi się komunikat o konieczności przyłożenia ponownie karty do czytnika i rozpoczęcie od nowa (od 1. kroku scenariusza).		

6 Przypadek użycia - ”Informowanie i niskim poziomie naładowania baterii”

Nazwa przypadku użycia: Informowanie o niskim poziomie naładowania baterii	**Numer PU:** 6	**Priorytet:** średni
Główny aktor: System	**Typ PU:** istotny	
Kto i co zyskuje na wykonaniu tego PU: Użytkownik dzięki temu przypadkowi użycia uzyskuje ważną informację od systemu, że poziom naładowania baterii jest bardzo niski i ma odpowiednio dużą ilość czasu, aby wymienić baterie, zanim rozładują się one całkowicie i system przestanie działać.		
Krótki opis: Ten przypadek użycia opisuje czynność, która jest pomocna do komunikacji z użytkownikiem o stanie urządzenia. Gdyby wymieniony PU nie istniał, to użytkownik mogłby za późno zorientować się o niedziałającym poprawnie urządzeniu, co mogłoby naruszać kwestie bezpieczeństwa.		
Trigger: System	**Typ:** wewnętrzny	
Scenariusz podstawowy: 1. Baterie rozładowują się wraz z upływem czasu i ich poziom naładowania w pewnym momencie przekracza ustaloną przez system granicę. 2. Dioda zaczyna migać na niebiesko. 3. System wysyła powiadomienie na telefon o konieczności wymiany baterii.		