

1 Możliwości Terminali Biometrycznych

Możliwości terminali możemy podzielić ze względu na dwa rodzaje:

- Funkcjonalności dla pracownika
- Funkcjonalności dla administratora systemu

1.1 Funkcjonalność dla pracownika

Rejestracja czasu pracy indywidualnie dla każdego pracownika

Proces rejestracji jest bardzo prosty i szybki w obsłudze. Pracownik rejestruje się w systemie poprzez przyłożenie palca do czytnika i ewentualnym wyborze rodzaju zdarzenia tj. wyjście służbowe, powrót z wyjścia służbowego. Skanowanie i wybór rodzaju zdarzenia trwa ok. 2s

Podgląd własnych zdarzeń przez pracownika

Po poprawnej weryfikacji istnieje możliwość podglądu ostatnio zarejestrowanych zdarzeń przez pracownika bezpośrednio przy terminalu. Oczywiście pracownik nie ma możliwości korekty tych zdarzeń, ani podglądu zdarzeń innych pracowników. Takie uprawnienia posiada administrator systemu.

Komunikaty głosowe

Urządzenie sygnalizuje fakt poprawnej weryfikacji na 3 sposoby:

- Zapaleniem zielonej diody
- Wyświetleniem komunikatu na ekranie
- Komunikatem głosowy np. Dziękuję

W przypadku błędnej weryfikacji komunikatem „Proszę spróbować ponownie”. Jest to bardzo przydatna funkcja sprawiająca, że żaden pracownik nie ma problemu z obsługą terminala

1.2 Funkcjonalność dla administratora systemu

Komunikacja TCP/IP

Terminale wyposażone są w moduł TCP/IP najpopularniejszy moduł komunikacji. Każde urządzenie posiada własne (konfigurowalne) IP umożliwiające współpracę i tworzenie sieci. Ponadto wyposażone są w moduł komunikacji RS232/RS485. Daje to praktycznie nieograniczone możliwości zdalnego zarządzania systemem.



Integracja z innymi systemami

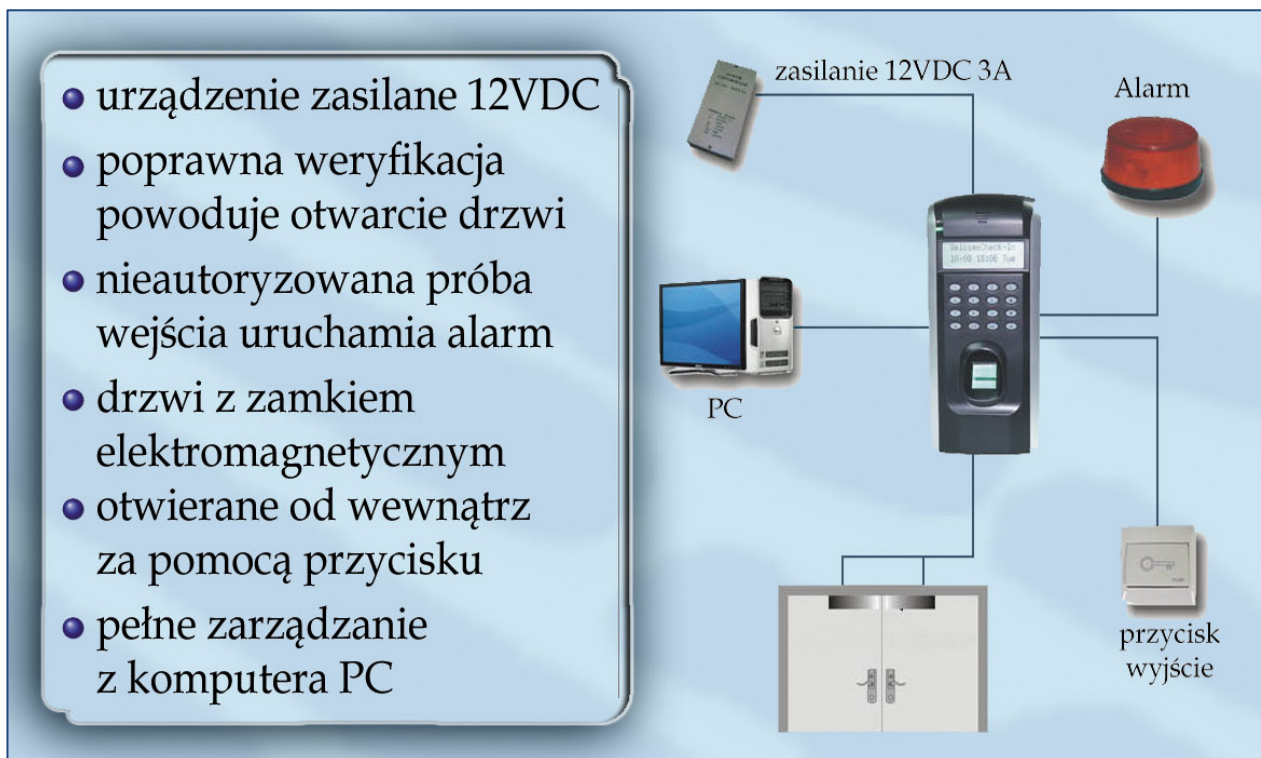
Terminale oprócz komunikacji sieciowej TCP/IP wyposażone są w protokół Wiegand 24/26. Dzięki temu mogą współpracować praktycznie z każdym systemem obsługującym ten standard. Daje to możliwość integracji z systemami kontroli dostępu, alarmowymi i innymi oraz do implementacji dodatkowych zewnętrznych czytników do systemu biometrycznego.

Kontrola dostępu

Terminale wspierające KD posiadają możliwość bezpośredniego podłączenia zamka elektromagnetycznego, czujnika otwartych drzwi czy czujki alarmu. Wyposażone są w czujnik anty-demontażowy.

Odcisk palca i karty zbliżeniowe

Prawie każdy terminal Biometryczny (na odcisk palca) może zostać wyposażony w czytnik kart zbliżeniowych. Czytnik taki jest umieszczany wewnątrz urządzenia (wygląd urządzenia nie ulega zmianie) i jest całkowicie niewidoczny. Rejestracja odbywa się poprzez zbliżenie karty (karty EM Unique 125kHz lub Mifare 13,56 MHz) do czytnika na odległość mniejszą niż 5cm. Weryfikacja trwa ułamek sekundy (<0.35ms). Zdarzenie zapisane jest do bazy. Wybór rodzaju zdarzenia (wejście, wyjście, przerwa itd) jest analogiczny jak w przypadku biometrycznej weryfikacji. Użytkownik może posługiwać się zarówno kartą, PIN-em, odciskiem palca - wybór jednego bądź wszystkich opcji zależy tylko od administratora.



2 Projektowanie sieci biometrycznych

2.1 Okablowanie

2.1.1 Zasilanie

Terminale biometryczne zasilane są napięciem 12V DC (12V prąd stały). Doprowadzenie zasilanie do miejsc montażu odbywa się poprzez zasilacz 12V umieszczone gdziekolwiek „po drodze” pomiędzy źródłem napięcia a terminalem.

Pobór prądu w zależności od modelu waha się pomiędzy 300 – 500 mA.

Zasilanie awaryjne w postaci zasilacza UPS wpinamy w dowolne miejsce pomiędzy zasilaczem 12DC a urządzeniem.

2.1.2 Komunikacja TCP/IP

Komunikacja z komputerem odbywa się poprzez port TCP/IP. Doprowadzenie kabla sieciowego UTP w standardzie 5E to kluczowy element w projekcie i instalacji sieci. Kabel sieciowy doprowadzamy do urządzenia z dowolnego routera pracującego w sieci lub bezpośrednio z serwerowni. Urządzenia posiadają możliwość konfiguracji ustawień sieciowych (adres IP, brama, maska). Odległość terminala od Access Pointa nie może przekraczać „teoretycznie” 100 metrów, lecz w praktyce jest to dystans krótszy ok. (70 metrów). Tek podpięte urządzenie jest pingowalne z dowolnej stacji znajdującej się w sieci.

Istnieje możliwość podpięcia urządzenia bezpośrednio do komputera za pomocą kabla sieciowego UTP w połączeniu krzyżowym. Oczywiście w takim układzie do urządzenia mamy dostęp tylko z jednego komputera.

2.1.3 Czujnik alarmu

Do urządzenia podpinamy syrenę alarmową (sygnalizator świetlny i dźwiękowy). Każde urządzenie wyposażone jest w przycisk antysabotażowy (antydemontażowy). Przy zdjęciu urządzenia ze ściany wyzwalany jest sygnał alarmowy.

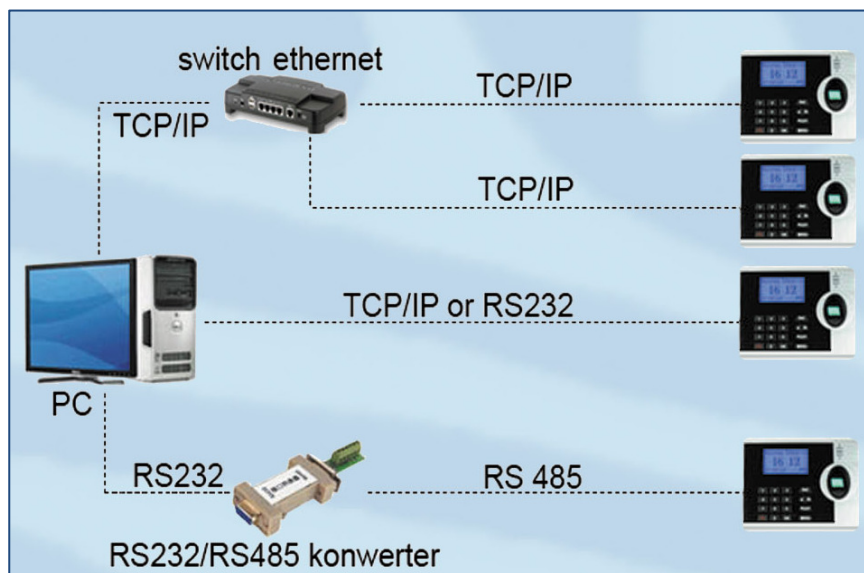
Sygnalizator zasilany jest stale i przerwanie obwodu wyzwala sygnał. Do obsługi sygnalizatora urządzenie wyposażone jest w dodatkowe wyjście przekaźnikowe (niezależne od przekaźnika do otwierania drzwi).

2.1.4 Umiejscowienie urządzenia

Urządzenie powinno zostać przytwierdzone do ściany za pomocą kołków rozporowych w stabilny sposób. W systemach kontroli dostępu, gdzie czytnik steruje otwarciem drzwi

okablowanie powinno być doprowadzone przez otwór w ścianie z wnętrza pomieszczenia (aby uniemożliwić ewentualną próbę sanotażu).

Terminale przystosowane są do pracy wewnątrz budynku w temperaturze powyżej 0°C
Urządzenie może być położone na biurku, jednak zalecamy przytwierdzenie go do ściany na wys. ok.120-140cm w miejscu nie narażonym na ciągłe promieniowanie słoneczne.



Wiele pojęć zostało wyjaśnionych w dziale FAQ na naszej stronie. (<http://biosys.pl/faq.html>)

Zapraszamy na naszą stronę
Zespół BioSys

Witryny branżowe, w których znaleźć można informacje o szeroko pojętej biometrii i jej zastosowaniu w zintegrowanych systemach (pod patronatem BioSys):

<http://www.odcisk-palca.pl/>

<http://www.kontrola-dostepu.pl/>

<http://www.rejestracja-czasu-pracy.eu/>

<http://www.kontroladostepu.pl/>