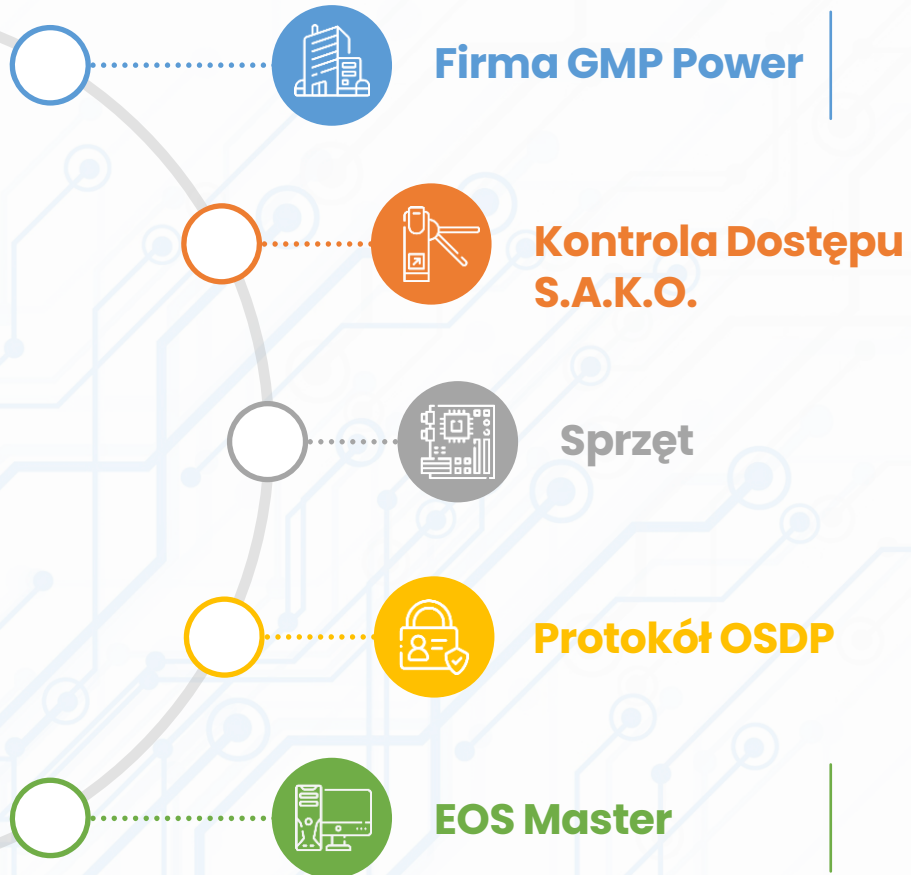




S.A.K.O.

System Autonomicznej Kontroli Obiektu

Spis treści



Firma GMP Power

Firma GMP Power to integrator systemów informatycznych, który oferuje dedykowane oprogramowanie, rozwiązania elektroniczne oraz systemy informatyczne. Nasze rozwiązania mają za zadanie sprostać największym wyzwaniom oraz wysokim standardom bezpieczeństwa, przed którymi stoi Państwa biznes.

Dzięki indywidualnemu podejściu do każdego problemu oprogramowanie będzie posiadać wszystkie potrzebne Państwu funkcjonalności. Daje to nieograniczone możliwości rozwoju przedsiębiorstwa, oszczędność czasu i pieniędzy.

Nasze mocne strony:

- Projektowanie i produkcja w ramach jednej organizacji działającej na rynku krajowym.
- Możliwość dopasowania funkcjonalności do indywidualnych projektów.
- Wsparcie techniczne na etapie projektowania, uruchamiania i użytkowania systemu.
- Ciągły rozwój oferty i oferowanych funkcjonalności.



Nowoczesny system kontroli dostępu

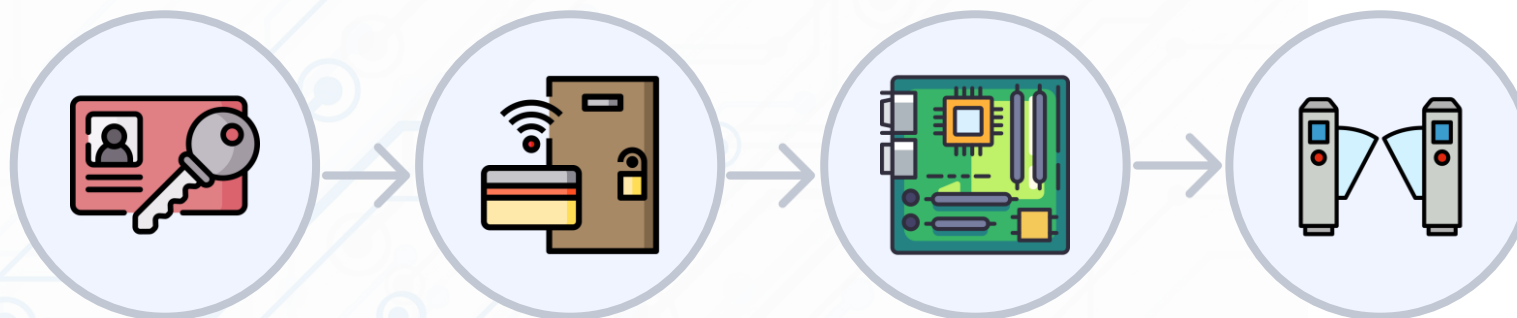
Wychodząc naprzeciw potrzebom naszych klientów, zaprojektowaliśmy nowoczesne oraz elastyczne na etapie projektów rozwiązanie systemu kontroli dostępu.

Nasz zespół własnymi siłami w pełni projektuje zarówno hardware, jak również tworzy firmware oraz oprogramowanie stanowiące interfejs użytkownika.

Dzięki takiemu podejściu jesteśmy w stanie w krótkim czasie dostosować system do indywidualnych wymagań obiektu oraz oczekiwań Klienta co do funkcjonalności systemu.

Dołożyliśmy także wszelkich starań, by rozwiązania przez nas projektowane wykorzystywały najnowocześniejszą technologię.

➤ Jak działa system kontroli dostępu?



Tożsamość

Karta RFID, PIN,
odcisk palca.

Czytniki

Czytniki kart, klawiatury,
skanery odcisków
palców.

Kontroler

Porównanie
tożsamości z listą
uprawnień zapisaną
w pamięci.

Zamki

Zwolnienie blokady
przejęcia, jeśli osoba
jest upoważniona do
wejścia.

4 etapy tworzenia projektu



Projekt

Etap projektowania oraz zbierania informacji o funkcjonalności.



Wdrożenie

Etap instalacji systemu w budynku. Instalacja okablowania oraz osprzętu.



Uruchomienie

Etap programowania urządzeń, tworzenia bazy danych użytkowników oraz nadawania uprawnień.



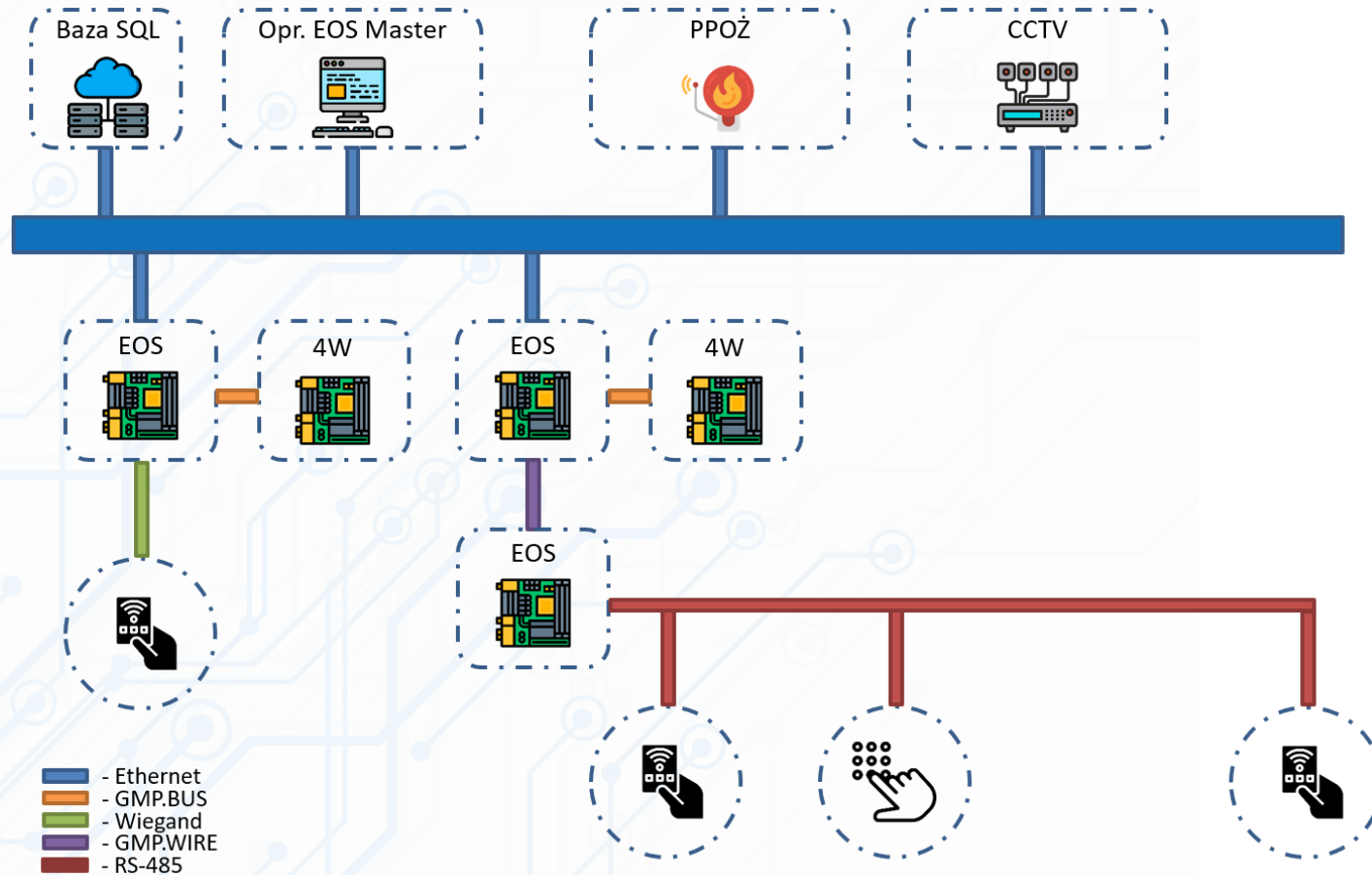
Support

Utrzymanie systemu, dodawanie nowych użytkowników, rozszerzenia systemu oraz konserwacja urządzeń.

4 filary bezpieczeństwa systemu KD



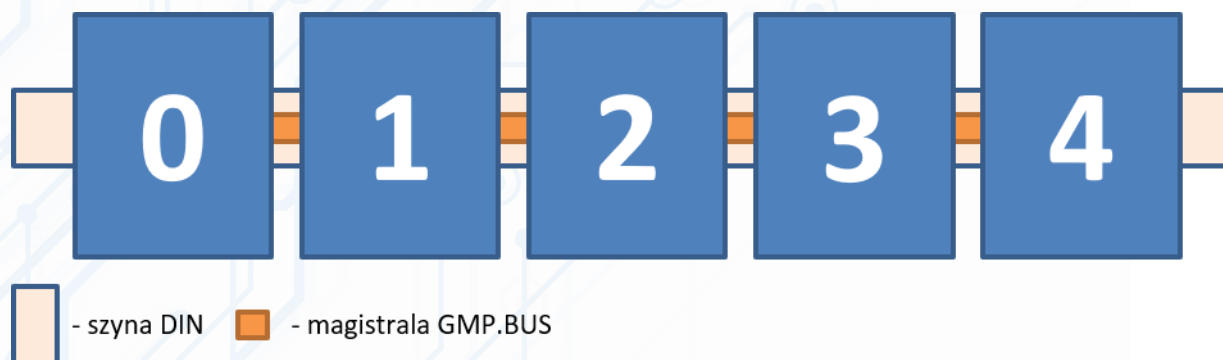
Topologia systemu



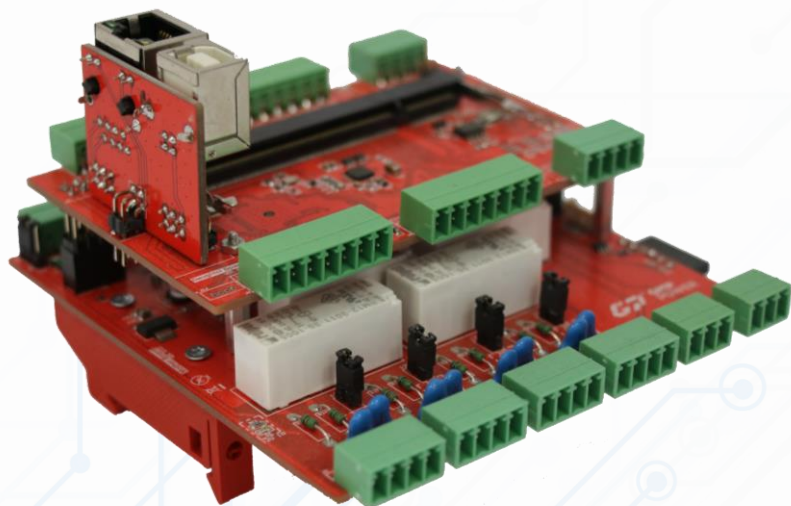
Kontroler EOS – podstawowa jednostka

Kontroler EOS jest podstawowym modułem wykonawczym w systemie kontroli dostępu Power S.A.K.O. Pojedynczy kontroler umożliwia sterowanie 4 pojedynczymi drzwiami. Dzięki modułowej budowie systemu w prosty sposób jesteśmy w stanie rozszerzyć możliwości kontrolera bez potrzeby instalowania dodatkowego okablowania. Na ten moment istnieje możliwość dołączenia kart rozszerzeń oferującej dodatkowo:

- 4 magistrale Wiegand,
- 4 lub 16 przekaźników,
- 8 parametryzowanych wejść analogowych,
- magistrale MBUS do pomiarów liczników.



➤ Co oferuje kontroler EOS?



Peryferia:

- 4 magistrale Wiegand,
- magistrala RS485,
- magistrala GMP.WIRE,
- 3 wejścia cyfrowe dla sygnałów pochodzących np. od zasilacza oraz styku sabotażowego obudowy,
- 4 przekaźniki bezpotencjałowe lub zasilane napięciem 12V z zab. nadprądowym,
- 12 wejść w pełni parametryzowanych (alarm, czuwanie, zwarcie, sabotaż).



Responsywność

Zdarzenia z systemu wyświetlane w czasie rzeczywistym.



Bezpieczeństwo

Szyfrowanie danych przechowywanych w pamięci kontrolera.



Lokalny bufor

Lokalny bufor kontrolera mogący przechować do 30 mln zdarzeń.



Modułowa budowa

Możliwość szybkiej rozbudowy dzięki szerokiej ofercie modułów rozszerzeń.



Harmonogramy

Praca według wcześniej zaplanowanych harmonogramów. Użytkownik może zadeklarować nieograniczoną liczbę harmonogramów w systemie.



Wizualizacja

Pełna i intuicyjna wizualizacja stanu systemu.

Funkcje kontrolera



Metody autoryzacji

- karta,
- PIN,
- biometria,
- karta + PIN,
- karta + biometria,
- numer tablicy rejestracyjnej.



Bezpieczeństwo

- dane szyfrowane na kontrolerze,
- szyfrowana komunikacja pomiędzy czytnikami,
- szyfrowana komunikacja pomiędzy kontrolerami i aplikacją zarządzającą,
- funkcja anti-passback.



Dodatkowo

- lokalny bufor 30 milionów zdarzeń,
- praca w trybie offline,
- elastyczna architektura,
- zgodność z normą obronną NO-04-A004-6.

Parametry kontrolera EOS

Funkcjonalności

Wyjścia	4 przekaźniki, styki beznapięciowe lub zasilane 12V z bezpiecznikiem elektronicznym
Wejścia dodatkowe	sabotaż, awaria zasilania, niski poziom baterii, 12 wejść parametryzowanych
Czytniki	4 x standardowy Wiegand lub szyfrowane przez magistrale RS485
Pamięć nieulotna	4 [GB] , 8 [GB], 16 [GB], 32 [GB]
Pamięć operacyjna	1GB LPDDR2 RAM
Pamięć kart użytkowników	do 250 000 kart
Pamięć zdarzeń	do 30 000 000 operacji w trybie offline

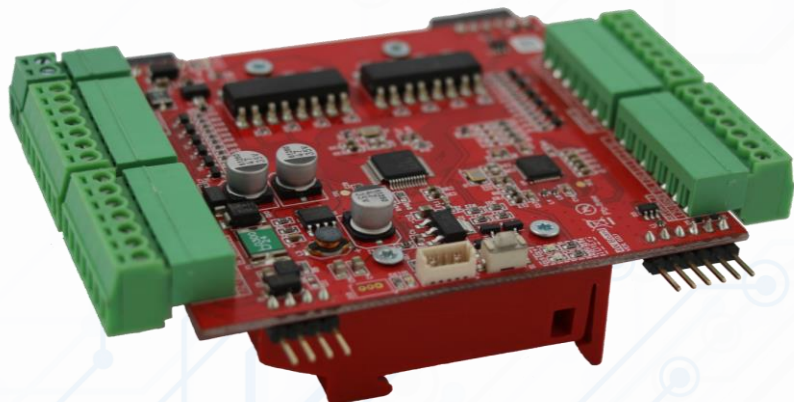
Zasilanie

Napięcie (tylko płyta PCB)	12 VDC
Pobór prądu (bez podpiętych zwór)	350 mA
Napięcie (obudowa - całość)	Wejście 220-230 V AC 50/60 Hz
Bateria RTC	CR2032

Parametry fizyczne

Wymiary kontrolera	100 mm x 85 mm x 66 mm
Obudowa	montaż ścienny, blacha Dc01 1.2mm, kolor RAL7035 (szary)
Waga kontrolera (bez obudowy)	0.16 kg
Waga z obudową	5.00 kg

➤ Co oferuje moduł 4W?



Rozszerza kontroler EOS:

- 4 magistrale Wiegand



Komunikacja

Obsługa GMP.BUS.



Szybkość

Błyskawiczna rozbudowa systemu. Moduł montowany na szynie DIN.



Zabezpieczenia

Wbudowane zabezpieczenie nadprądowe.



Bezpieczeństwo

Wejścia danych izolowane galwanicznie.



Interfejs

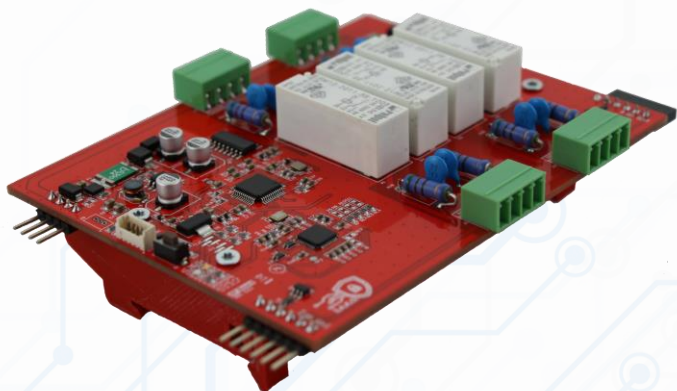
Sterowanie dwoma LED-ami oraz dodatkowo buzzer-em.



Elastyczność

Współpraca z wieloma typami czytników dostępnych na rynku.

➤ Co oferuje moduł 4P?



Rozszerza kontroler EOS:

- 4 przekaźniki bezpotencjałowe



Komunikacja

Obsługa GMP.BUS.



Szybkość

Błyskawiczna rozbudowa systemu. Moduł montowany na szynie DIN.



Niski pobór prądu

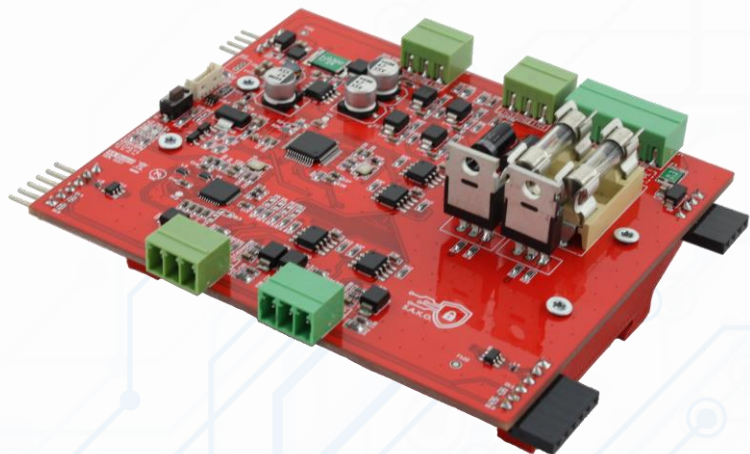
Średni pobór prądu 30 mA (plus 30 mA na każdy włączony przekaźnik).



Obciążalność

Wyjścia przekaźnikowe z jednym stykiem NO/NC obciążalne 8A/24 VDC lub 8A/250 VAC.

➤ Co oferuje moduł 8A?



Rozszerza kontroler EOS:

- 12 wejść w pełni parametryzowanych (alarm, czuwanie, zwarcie, sabotaż)
- 2 wyjścia syrenowe zasilane 12V z płytki PCB lub z zewnętrznego zasilania



Komunikacja

Obsługa GMP.BUS.



Szybkość

Błyskawiczna rozbudowa systemu. Moduł montowany na szynie DIN.



Bezpieczeństwo

Wejścia analogowe buforowane.



Zabezpieczenia

Wbudowane zabezpieczenie nadprądowe.

Rozszerzenie zasobów za pomocą RS-485

Kontroler EOS można wyposażyć w dodatkowy sprzęt dzięki wbudowanej magistrali RS485.

Zalety:

- możliwość dołączenia dodatkowych 16 urządzeń,
- maksymalna długość magistrali aż do 1000 m,
- możliwość używania szyfrowanej transmisji OSDP*, OSDPv2*, Idesco RS485 with AES.



*OSDP (Open Supervised Device Protocol), to protokół komunikacji dla urządzeń peryferyjnych z kontrolerem. Specyfikacja protokołu oferuje dwukierunkową zabezpieczoną transmisję. Wykorzystanie tego protokołu z silnym szyfrowaniem AES128 eliminuje ryzyko podsłuchiwania sygnału Wiegand.

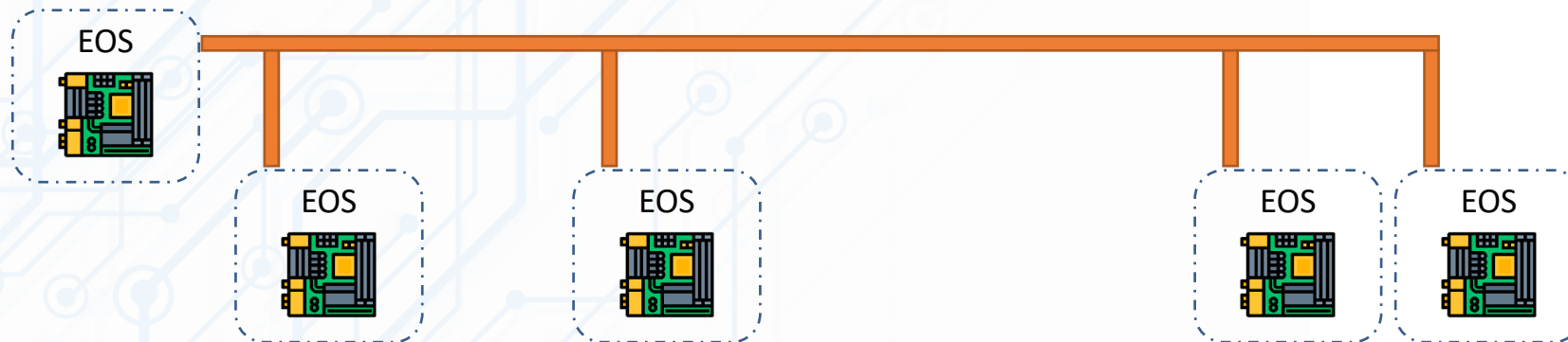
Rozszerzenie zasobów za pomocą GMP.WIRE

Dodatkowo kontrolery EOS oferują możliwość komunikacji pomiędzy urządzeniami tego samego typu tj. kontroler-kontroler za pośrednictwem magistrali GMP.WIRE.

Magistrala ta sprawdza się idealnie w przypadku, gdy do kontrolera nie może zostać doprowadzony przewód sieciowy Ethernet. GMP.Wire wykorzystuje transmisję różnicową, dzięki czemu do jej instalacji potrzebne są tylko dwa przewody. Umożliwia ona w pełni przesyłanie informacji do kontrolera, a także raportowanie zdarzeń zaistniałych na kontrolerze do oprogramowania zarządczego. Komunikacja za pomocą tej magistrali jest szyfrowana, dzięki czemu informacje przesyłane pomiędzy kontrolerami są w pełni bezpieczne.

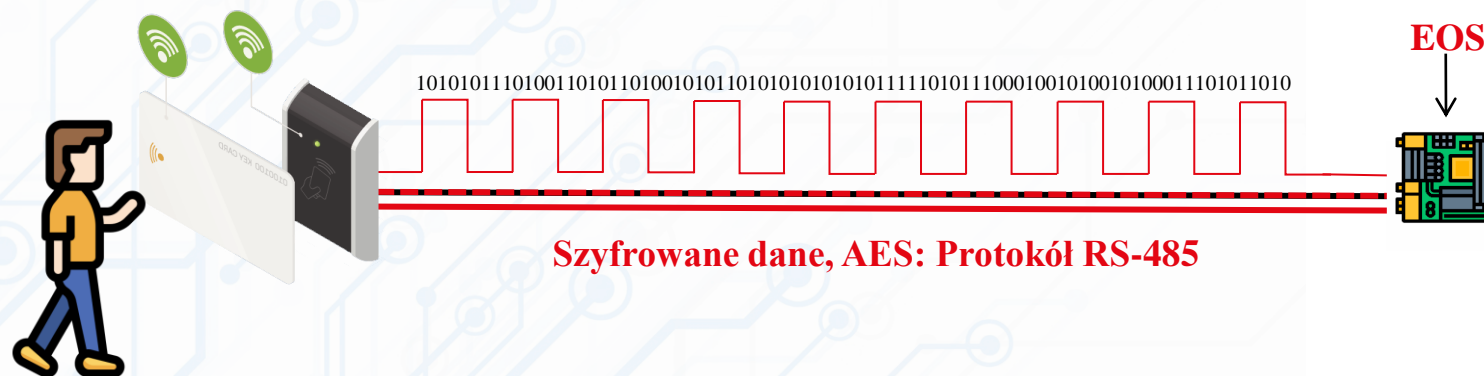
Zalety:

- możliwość dołączenia dodatkowych 128 urządzeń,
- maksymalna długość magistrali aż do 250 m.



Protokół OSDP

Dane z karty, szyfrowanie AES



Rozwiązanie to wymaga użycia protokołu OSDP przez magistrale RS-485 w kontrolerze EOS.

Takie rozwiązanie zapewnia szyfrowanie danych w całym torze transmisyjnym. Nie wymaga instalacji dodatkowego sprzętu.

Protokół OSDP - zalety



Zwiększone bezpieczeństwo

OSDP obsługuje zaawansowane koncepcje bezpieczeństwa, w tym szyfrowaną komunikację AES-128. Oznacza to, że Twój system bezpieczeństwa jest daleki od potencjalnych włamań i naruszeń, dzięki czemu Twoja siedziba pozostaje zabezpieczona.



Komunikacja dwukierunkowa

W przeciwieństwie do komunikacji jednokierunkowej w systemach magistrali Wiegand, funkcja dwukierunkowa protokołu OSDP umożliwia komunikowanie się paneli kontrolnych i czytników. Ta dwukierunkowa interakcja daje możliwość korzystania z bardziej zaawansowanych funkcji takich jak: wykrywanie sabotażu, nadzór nad urządzeniami i bezpośrednie wysyłanie konfiguracji do czytnika.



Skalowalność i interoperacyjność

Protokół OSDP jest niezwykle skalowalny, co oznacza, że system można łatwo dostosować do rosnących potrzeb w zakresie bezpieczeństwa. Dzięki standaryzacji zapewnianej przez OSDP nasz system jest kompatybilny z urządzeniami i systemami innych producentów, które również są zgodne z protokołem OSDP.



Sprawne instalacje i aktualizacje

Zastosowanie przez OSDP uniwersalnego standardu pozwala na usprawnienie instalacji i aktualizacji, zmniejszając koszty i złożoność wdrożenia. Jeśli dokonujesz aktualizacji z systemu opartego na magistrali Wiegand na protokół OSDP, system S.A.K.O. ułatwia to przejście oszczędzając czas i pieniądze.

Rekomendowane czytniki 125 kHz



Quattro

Basic

Slim



Quattro Pin
S

Quattro Pin
N

Slim Pin

Desktop

Obsługiwane technologie:

- EM4102
- Sokymat Unique
- Hitag2
- HIDProx

Interfejsy komunikacyjne:

- RS-232
- Wiegand
- USB
- Clock&Data
- USB HI
- 2 x wyjście FET
- 1 x wejście ogólnego przeznaczenia

Przewód o długości 3 m lub złącze z kostką połączeniową, podstawki montażowe.

 **IDESCO**

Rekomendowane czytniki 13,56 MHz



Quattro



Basic



Slim

!!! IP 67 – dla wersji z przewodem



Quattro Pin S



Quattro Pin N



Slim Pin



Desktop

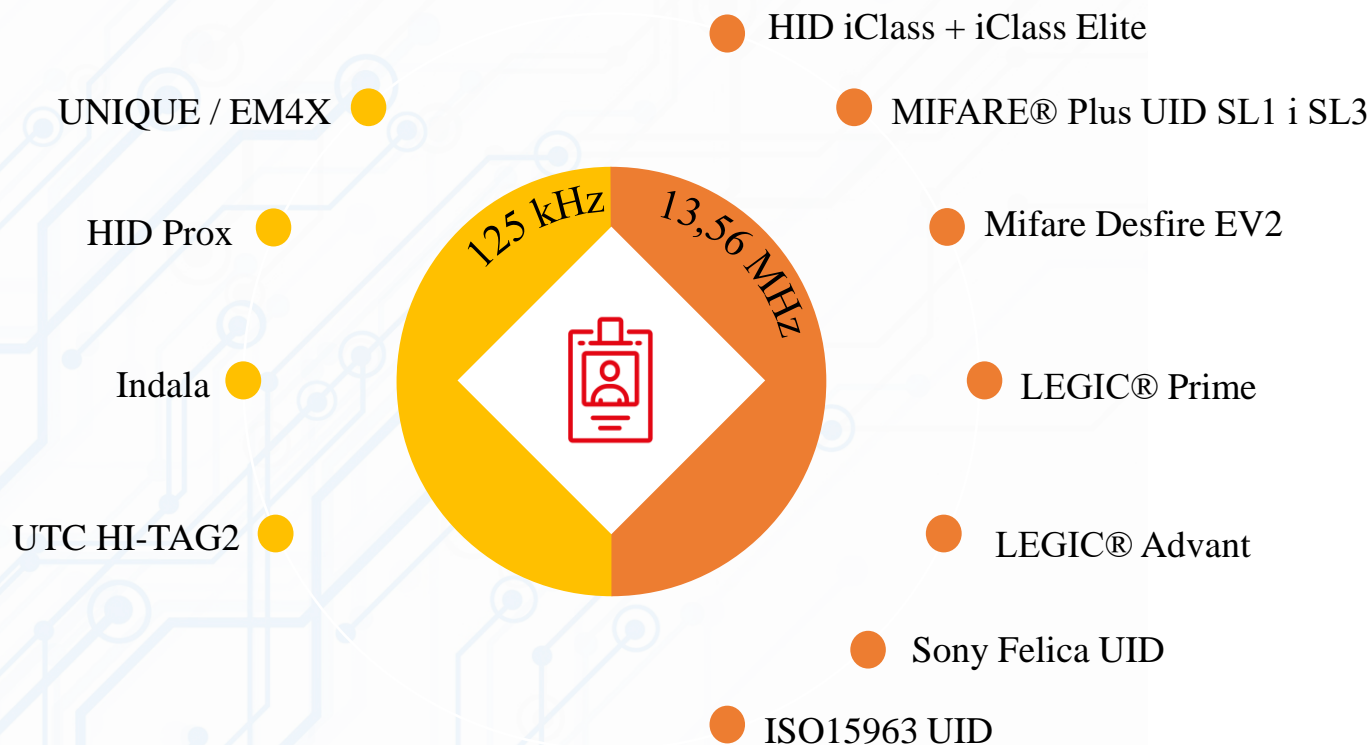
Obsługiwane technologie:

- MIFARE® Classic: UID
- MIFARE® Ultralight UID
- MIFARE® SmartMX (MIFARE® Classic emulation)
- NFC (UID)
- Mifare Classic 7 byte UID
- MIFARE® DESFire Ev1: UID
- **MIFARE® DESFire EV2: UID**
- MIFARE® Plus UID SL1 oraz SL3

Interfejsy komunikacyjne:

- RS-232
- Wiegand
- USB
- USB HI
- Clock & Data: 10 BCD-format dla Mifare® Classic z sektorami oraz Mifare® DESfire aplikacje
- RS-485
- Idesco RS-485
- Idesco RS-485 z AES
- OSDP
- **OSDP v2**
- 2 x wyjście FET
- 1 x wejście ogólnego przeznaczenia

Obserwowane standardy kart zbliżeniowych



EOS MASTER

Nasza aplikacja komputerowa została specjalnie zaprojektowana tak, aby jak najbardziej uprościć system zarządzania dostępem, zapewniając bezpieczeństwo i wygodę. Wierzymy, że nasi klienci mogą korzystać z zaawansowanych rozwiązań technologicznych, które są łatwe w nawigacji, wydajne i wysoce bezpieczne.

Najważniejsze funkcjonalności

Tryb nadzoru operatorskiego do stref i pomieszczeń

Operatorzy mogą zdalnie kontrolować kto, kiedy i w jakich strefach się znajduje oraz szybko reagować na ewentualne sytuacje awaryjne lub naruszenia bezpieczeństwa.



Obsługa wielu kart dla jednego użytkownika

Użytkownik może posiadać więcej niż jedną kartę, ale także inne rodzaje identyfikatorów jak PIN, odcisk palca, tablica rejestracyjna.



Antypassback lokalny, globalny

Zwiększa bezpieczeństwo poprzez eliminację możliwości przekazania karty innym osobom i zapewnia lepszą kontrolę nad ruchem wewnątrz monitorowanego obszaru. Uniemożliwia, aby na jedną kartę wpuszczono więcej osób.



Ciągle wyświetlanie zdarzeń

Obejmuje to takie informacje jak wejścia, wyjścia, próby nieautoryzowanego dostępu oraz wszelkie alarmy i wyjątki. Ta funkcjonalność zwiększa świadomość sytuacyjną i pozwala na natychmiastową reakcję w przypadku naruszeń bezpieczeństwa.



Praca według harmonogramów

Pozwala na zaprogramowanie przedziałów czasowych, w których określone osoby lub grupy osób mają dostęp do różnych stref i pomieszczeń. Na przykład, pracownicy działu sprzedaży mogą mieć dostęp do biura tylko w dni robocze od 8:00 do 18:00, podczas gdy zespół ochrony może mieć dostęp całą dobę.



Najważniejsze funkcjonalności

Szybka propagacja uprawnień

Pozwala na niemal natychmiastowe zaktualizowanie uprawnień dla użytkowników w całej sieci punktów dostępu. Ta funkcja jest szczególnie użyteczna w dynamicznych środowiskach, gdzie wymagane jest szybkie reagowanie na zmiany w strukturze organizacyjnej lub zabezpieczeniach.

Rozszerzone raporty

Kompleksowe raporty pomagają analizować strukturę dostępu, monitorować incydenty związane z bezpieczeństwem i podejmować decyzje w oparciu o dane.

Strefy przebywania ludzi

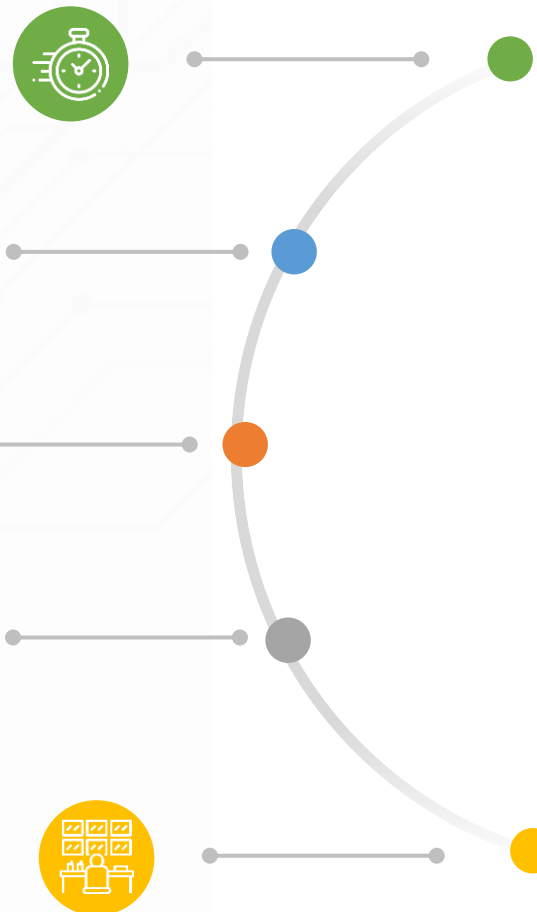
Strefy są monitorowane w czasie rzeczywistym, co pozwala na identyfikację i śledzenie osób znajdujących się w danym obszarze.

Zarządzanie pojazdami

Funkcja ta jest szczególnie przydatna na dużych obiektach przemysłowych, parkingach czy w innych miejscach, gdzie kontrola dostępu pojazdów jest równie ważna jak kontrola dostępu osób. Zarządzanie tym aspektem zwiększa bezpieczeństwo i efektywność operacyjną.

Monitor stref

Dzięki dziennikom zdarzeń i natychmiastowym alertom można przeglądać informacje o obiektach w czasie rzeczywistym. Dowiedz się kto, gdzie i kiedy przebywa w Twoim budynku.



Najważniejsze funkcjonalności

Praca wielostanowiskowa:

W systemie możliwe jest zainstalowanie wielu aplikacji EOS Master na różnych komputerach. Umożliwia to zarządzania systemem przez Administratora z różnych komputerów.

Operatorzy aplikacji:

Systemem może zarządzać wiele osób, każda z nich posiada własny profil uprawnień. Każdy z tych profili można dowolnie modyfikować w aplikacji EOS Master. Działania operatorów są magazynowane i w każdym momencie dostępne dla Administratora systemu.

Rejestracja zdarzeń z systemu:

Zdarzenia, które miały miejsce na terenie obiektu są na bieżąco pobierane z kontrolerów i przenoszone do głównej bazy danych. Proces ten jest realizowany pomimo braku włączenia aplikacji EOS Master. W przypadku braku połączenia z kontrolerem, zdarzenia są zapisywane w wewnętrznym buforze. Po powrocie komunikacji z aplikacją zarządzająca zdarzenia są natychmiast przenoszone do głównej bazy danych.

Aplikacja EOS Master – wymagania systemu

Minimalne wymagania komputera, na którym ma być zainstalowane oprogramowanie:

Nazwa	Serwer kontroli dostępu
System operacyjny	Windows 10 (64 bit) lub nowszy
Procesor	Intel Core i5, 5 generacji lub nowszy
Pamięć RAM	4 GB RAM
Karta graficzna	HD minimum 1GB pamięci
Dysk	100GB HDD

EOS MASTER porównanie wersji

	BASIC	PRO
	BEZPŁATNY	Zapytaj handlowca
Liczba kontrolerów w systemie	Do 4 kontrolerów	∞
Liczba użytkowników w systemie	∞	∞
Liczba przejść w systemie	Do 16 przejść	∞
Identyfikacja LPR	✓	✓

Wsparcie produktów firmy GMP Power

- Prezentacja systemu kontroli dostępu u Inwestora.
- Pomoc w doborze odpowiedniego sprzętu.
- Usługa projektowania całego systemu kontroli dostępu jak i CCTV.
- Usługa montażu i uruchomienia systemu na obiekcie inwestora.

Kontakt



ul. Ewy 1,
03-641 Warszawa



info@sakokd.pl