



C & C

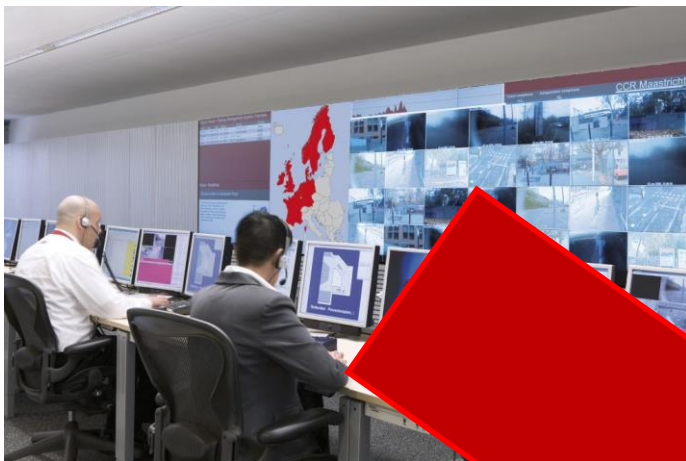
solution
partner

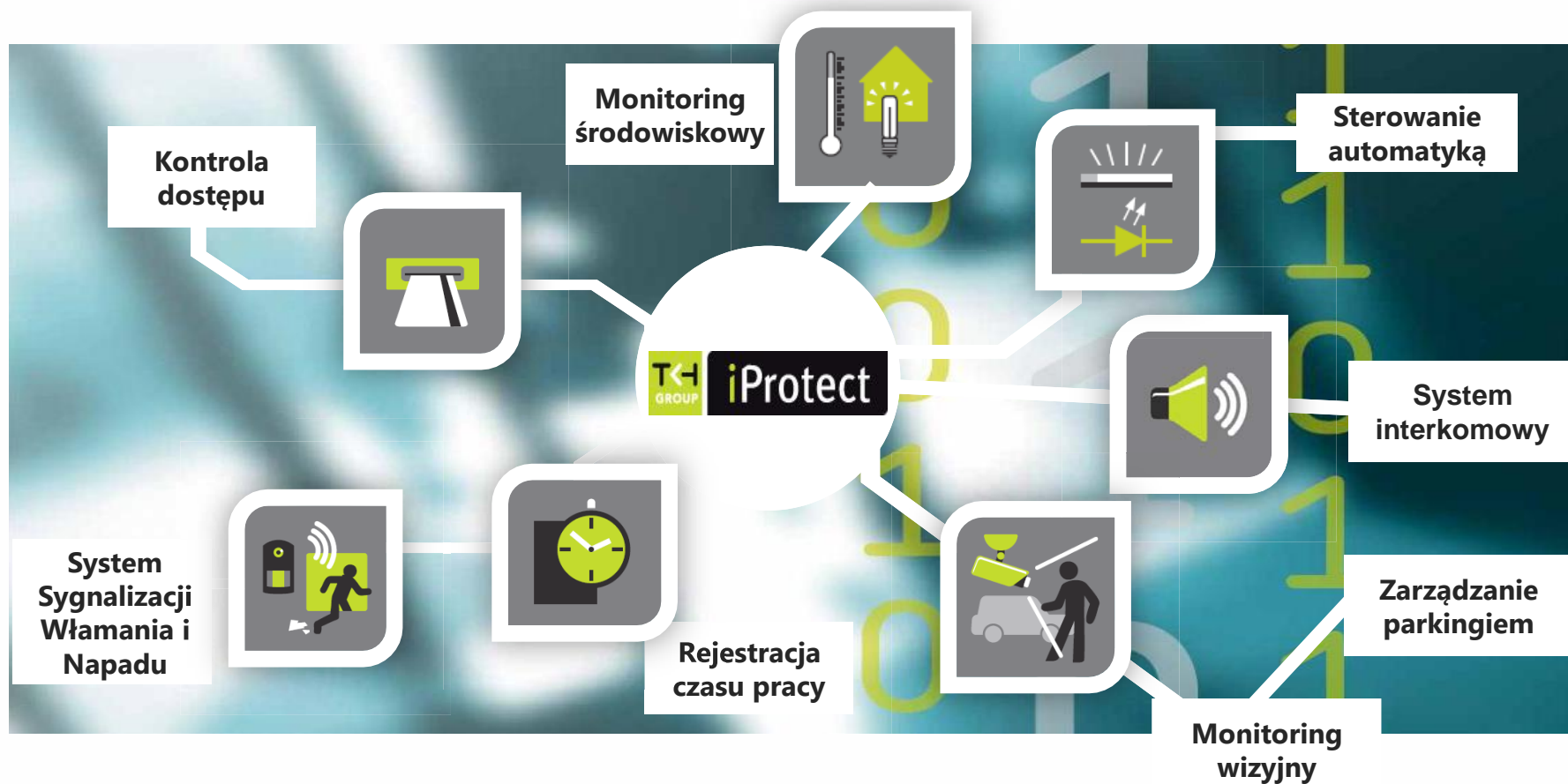
Systemy zabezpieczeń

C&C Partners

Olsztyn, 16 października 2013

Wiele Systemów - Wielu operatorów

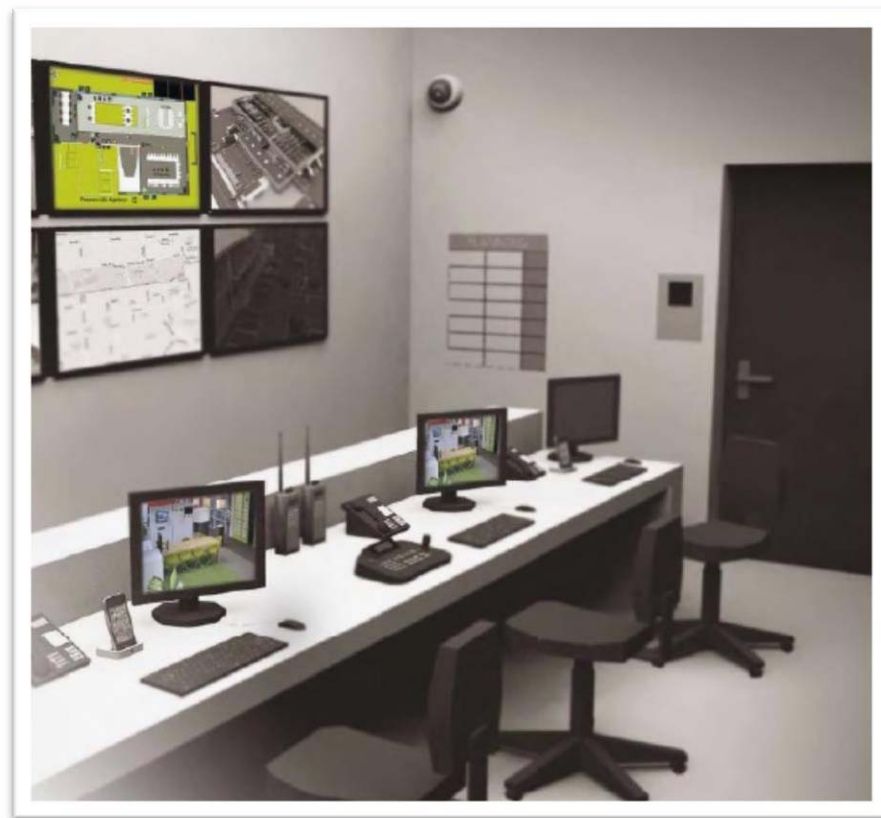




iProtect™

Zintegrowany System Zarządzania

System Zarządzania Bezpieczeństwem





System Zarządzania Bezpieczeństwa

- Jedno stanowisko operatora obsługujące kilka podsystemów, zlokalizowanych w różnych budynkach;
- Niskie koszty utrzymania i serwisu – jeden system;
- Informacja o zdarzeniu alarmowym przesyłana w czasie rzeczywistym – pełna koordynacja działań.

Stanowisko iProtect 1 - Ochrona



Stacja robocza



Interkom

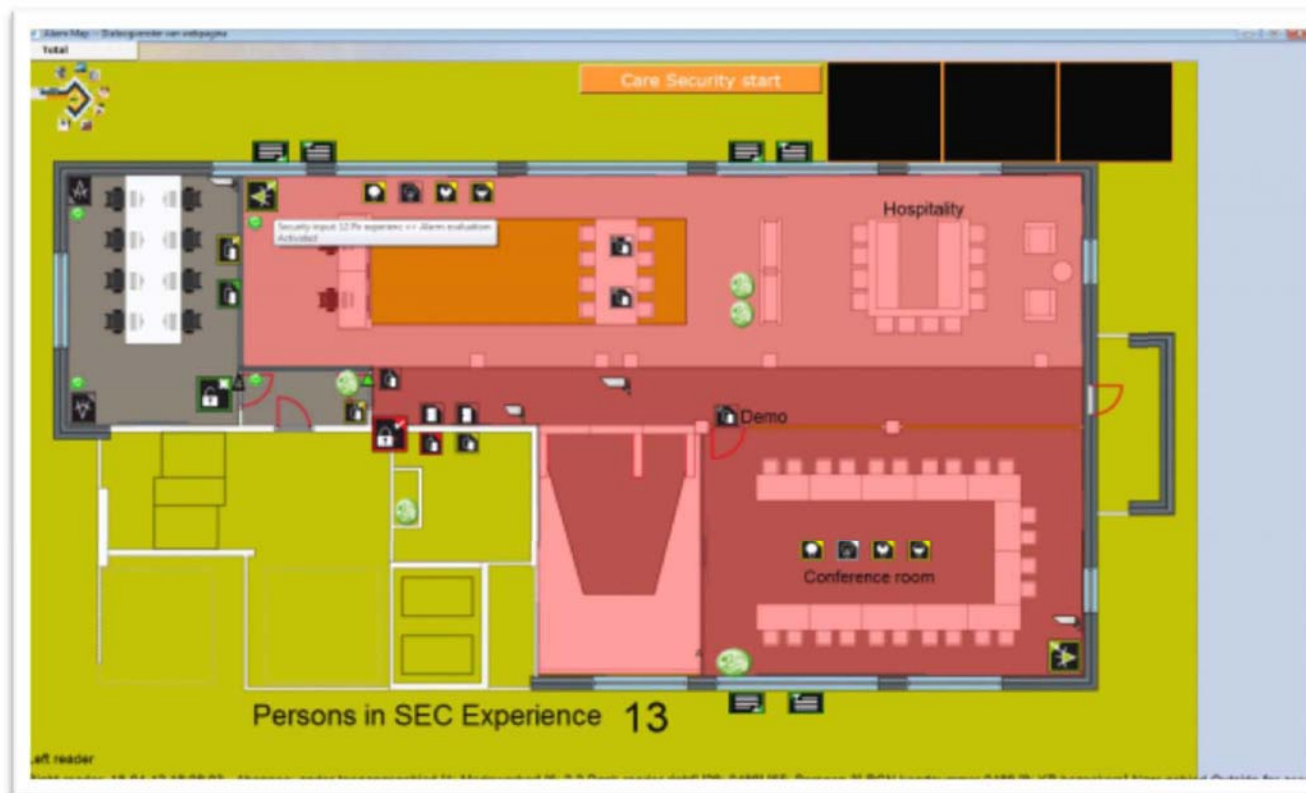


Drukarka kart



System Zarządzania Bezpieczeństwa

- Pełna wizualizacja stanu urządzeń i systemów w czasie rzeczywistym;
- Zarządzanie systemami bezpośrednio z poziomu mapy (np. otwarcie drzwi wejściowych do budynku na stałe).





System Zarządzania Bezpieczeństwa

- Pełne zarządzanie danymi i uprawnieniami poszczególnych użytkowników lub grup użytkowników;
- Możliwość dowolnej gradacji praw administratorów systemu (ochroniarz, pracownik administracyjny, administrator IT).

iProtect™ Aurora

Plik Ogólne Dostęp Goście

Osoba

Szukaj wg:

Wyszukiwanie po słowach kluczowych:

- Baranowski Michał
- C&C Przemek
- d
- Dawidowski Tomasz
- jjj oo
- Jurewicz Tomek
- Karta skradziona
- kkk
- Kowalski Jan
- Kowalski (Centrum) Maciej
- Krakowska Maria
- Kroon Fred
- LAB-EL
- Leszek
- lllll
- Maciej**
- { 1326978265:2 }
- E-mail, Maciej Flis: m.flis@ccpartners.pl
- nnnnnn131

Szczegóły osoby

Nazwisko:

Prefix:

Imię:

Adres:

Kod pocztowy:

Miasto:

Departament:

Ostatnie zdarzenie:

Kraj:

Maksimum kart

Obszar parkingu:

Typ karty

Typ karty:

Zdjęcie:

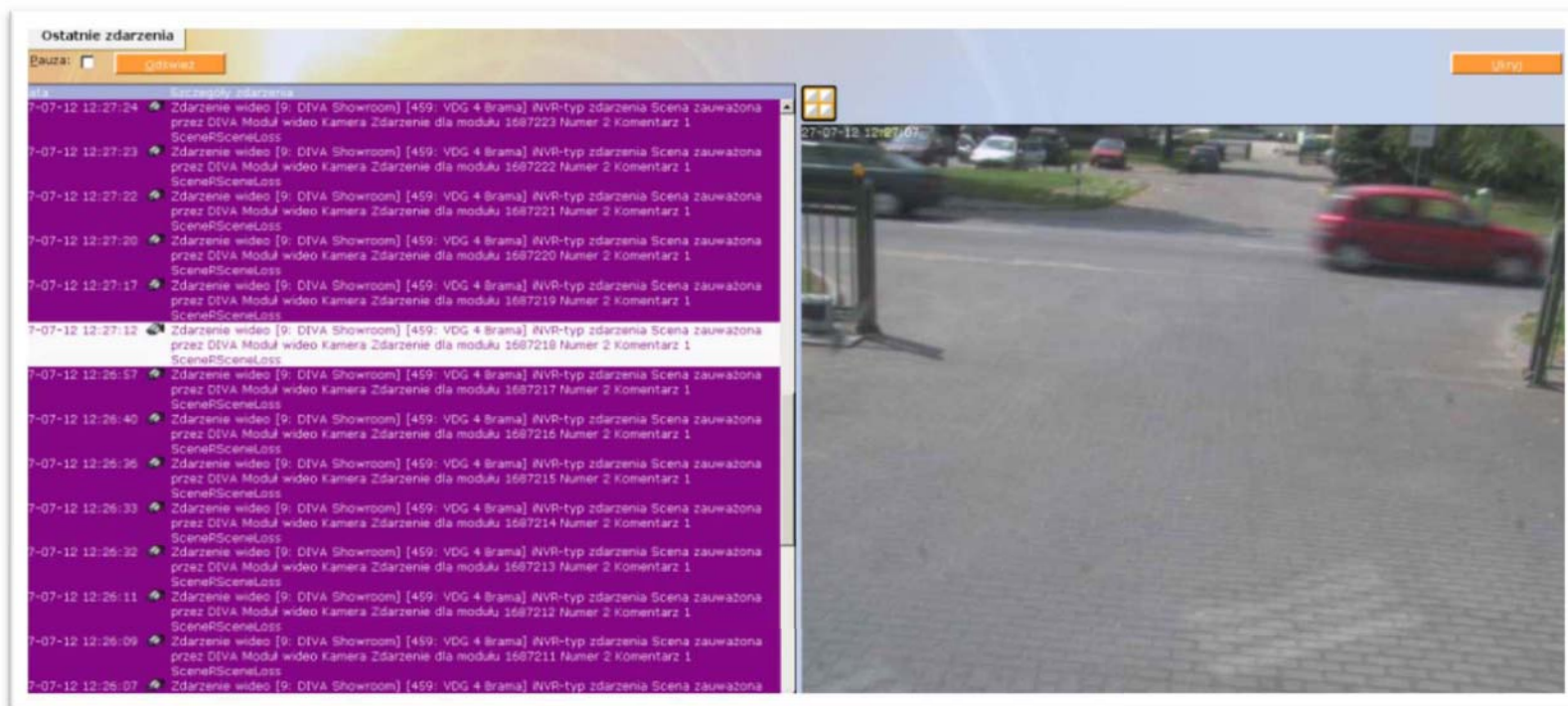
Grupa autoryzacji:

Obszar dostępu:



System Zarządzania Bezpieczeństwa

- Powiązanie zdarzeń między podsystemami (zdarzenie w jednym systemie powoduje wystąpienie zdarzenia w innym systemie);
- Pełna weryfikacja wystąpienia zdarzenia alarmowego (obraz wideo przypisany do zdarzenia).



The screenshot displays a security management interface. On the left, a list titled "Ostatnie zdarzenia" (Recent Events) shows a series of "Zdarzenie wideo" (Video Event) entries. Each entry includes a timestamp, a location (e.g., "DIVA Showroom"), and a description of the event (e.g., "Scena zauważona przez DIVA Moduł wideo Kamera" - Scene detected by DIVA Video Module Camera). The right side of the interface shows a live video feed of a street scene with a red car in motion. The interface also includes a "Pauza" (Pause) button and a "Utrzy" (Hold) button.

Kontrola Dostępu do obiektów i pomieszczeń





Kontrola dostępu

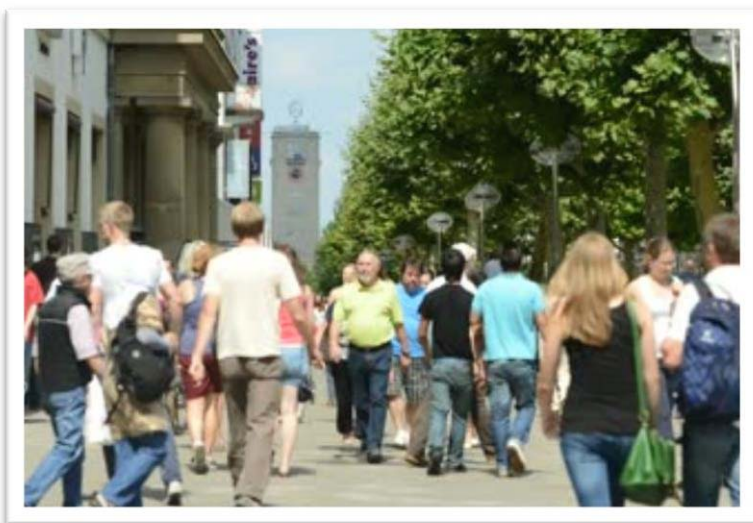
- Zaawansowane zarządzanie dostępem użytkowników / pracowników - Karty ważne terminowo, czasowo, różne poziomy dostępności;
- Zabezpieczenia przed niewłaściwym użyciem kart dostępowych (m.in. Anty Passback, Śluzowość);
- Wsparcie dla różnych typów czytników: karta dostępową (wejście główne), karta + PIN (kancelaria), karta + cecha biometryczna (serwerownia).





Kontrola dostępu

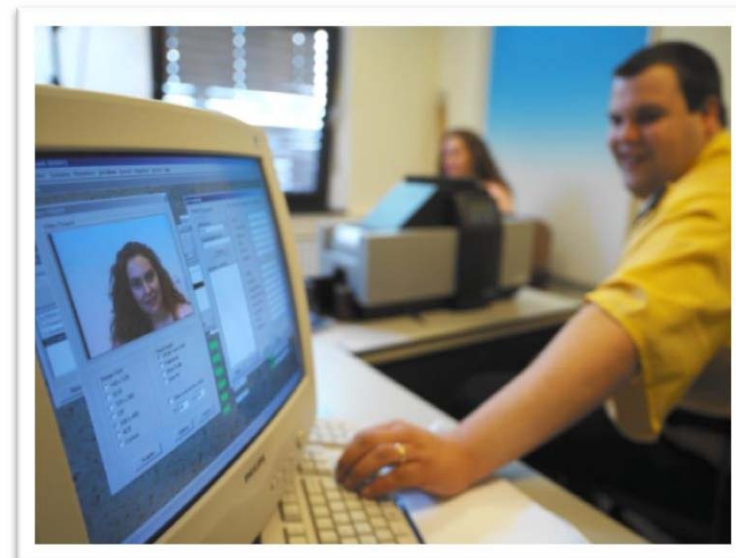
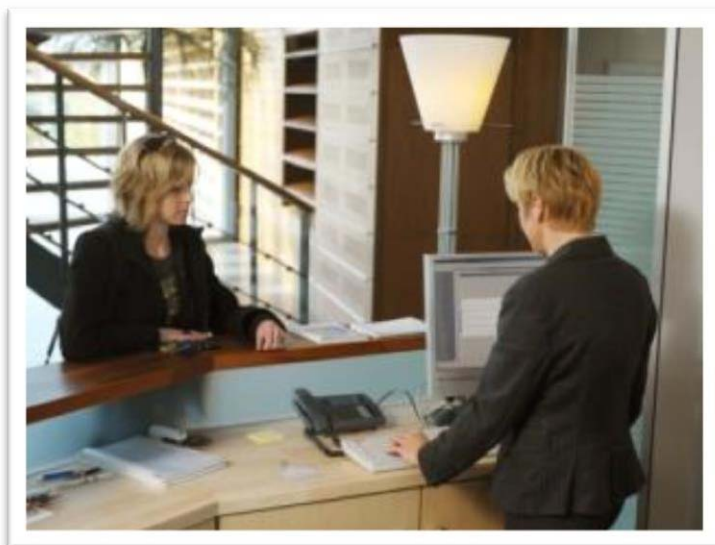
- Kontrola i monitorowanie przepływu użytkowników na terenie obiektu w dowolnym terminie;
- Możliwość weryfikacji obecności użytkowników w pomieszczeniu (np. sali laboratoryjnej) w czasie rzeczywistym i w dowolnym terminie w przeszłości (np. w dniu kradzieży sprzętu);
- Zliczanie osób wchodzących/wychodzących do pomieszczenia (ustanawianie limitów osób, sterowanie zamknięciem pomieszczeń itp.).





Kontrola dostępu

- Funkcja obsługi gości – Możliwość rezerwacji sal i wydawania kart dostępu dla gości, np. w czasie konferencji;
- Karta gościa umożliwia dostęp tylko do wyznaczonych pomieszczeń w odpowiednich godzinach (np. 9.00 – 16.00);
- Funkcja personalizacji identyfikatorów. Zdjęcie użytkownika pobrane z kamery bezpośrednio jest umieszczane na karcie dostępowej.





Kontrola dostępu

- Wszystkie zdarzenia mające miejsce są zapisywane w systemie i wybrane podlegają archiwizacji (np. alarmowe);
- Zróżnicowanie oznaczenia graficznego, w zależności od typu zdarzenia, które ma miejsce (np. czerwony kolor - włamanie);
- Możliwość generowania raportów m.in.: obecność pracowników, praw dostępu itp.(PDF, XLS).

Data	Szczegóły zdarzenia
8-10-12 12:51:15	Wejście jest aktywne [44: 7.1 SecASS Katowice Reader - PIR Ruch] [1: Zarządzanie We/Wy] [1: SecAAS Katowice] [21: 7.1 SacASS Katowice POLYX]
8-10-12 12:51:17	Nowa sytuacja dla elementu logicznego [28: SecASS Katowice] [9: SecASS KATOWICE PIR] Aktywny NIE
8-10-12 12:51:18	Zmiana stanu czujki: CC_Wal stan Alarm
8-10-12 12:51:14	Wejście jest aktywne [80: 5.1 SecASS Warszawa PIR RUCH] [1: Zarządzanie We/Wy] [20: 5.1 SecAAS Warszawa Polyx]
8-10-12 12:51:15	Nowa sytuacja dla elementu logicznego [26: SecASS WWA] [10: SecASS WWA PIR] Aktywny NIE
8-10-12 12:51:12	Wejście jest nieaktywne [44: 7.1 SecASS Katowice Reader - PIR Ruch] [1: Zarządzanie We/Wy] [1: SecAAS Katowice] [21: 7.1 SacASS Katowice POLYX]
8-10-12 12:51:14	Nowa sytuacja dla elementu logicznego [28: SecASS Katowice] [9: SecASS KATOWICE PIR] Aktywny Tak
8-10-12 12:51:11	Wartości zdefiniowane przez użytkownika, zmieniły status [11: Temperatura2] Wartość 338
8-10-12 12:51:11	Wartości zdefiniowane przez użytkownika, zmieniły status [10: Temperatura1] Wartość 243
8-10-12 12:51:11	Zmiana stanu czujki: CC_Wal stan Bezpieczna
8-10-12 12:51:09	Wejście jest nieaktywne [80: 5.1 SecASS Warszawa PIR RUCH] [1: Zarządzanie We/Wy] [20: 5.1 SecAAS Warszawa Polyx]
8-10-12 12:51:09	Nowa sytuacja dla elementu logicznego [26: SecASS WWA] [10: SecASS WWA PIR] Aktywny Tak
8-10-12 12:51:06	Wartości zdefiniowane przez użytkownika, zmieniły status [11: Temperatura2] Wartość 337
8-10-12 12:51:06	Wartości zdefiniowane przez użytkownika, zmieniły status [10: Temperatura1] Wartość 244
8-10-12 12:51:05	Wejście jest aktywne [80: 5.1 SecASS Warszawa PIR RUCH] [1: Zarządzanie We/Wy] [20: 5.1 SecAAS Warszawa Polyx]
8-10-12 12:51:06	Nowa sytuacja dla elementu logicznego [26: SecASS WWA] [10: SecASS WWA PIR] Aktywny NIE

Moduł Sygnalizacji Włamania i Napadu





Sygnalizacja Włamania i Napadu

- Pełna detekcja nieautoryzowanego wejścia do budynku i pomieszczeń;
- Możliwość podłączenia dowolnych detektorów (m.in. ruchu, penetracji, zbitcia szkła, kontaktronów itp.);
- Przesłanie wiadomości o alarmie do stanowiska operatora, dodatkowo przez e-mail lub SMS do dowolnego odbiorcy, np. Dyrektora ds. Technicznych;
- Centrala alarmowa zgodna z EN50131 grade 3, możliwość modułowej rozbudowy (bez ograniczeń).



Pełna ochrona zewnętrzna placówki

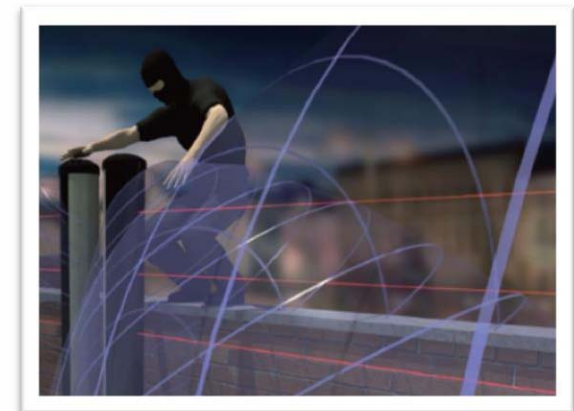
- Zaawansowane bariery mikrofalowe, podczerwieni i hybrydowe;
- Szeroki zasięg działania urządzeń (50m - 500m);
- Ochrona posesji i dachu obiektu.

Zaawansowane technologie

- Niewrażliwość na warunki atmosferyczne;
- Obudowy polikarbonowe z antymaskingiem;
- Precyzyjna lokalizacja intruza.

Pełna integracja z systemem CCTV DIVA

- Automatyczne rozpoczęcie nagrywania w momencie detekcji intruza;
- Skierowanie kamery na strefę detekcji bariery.

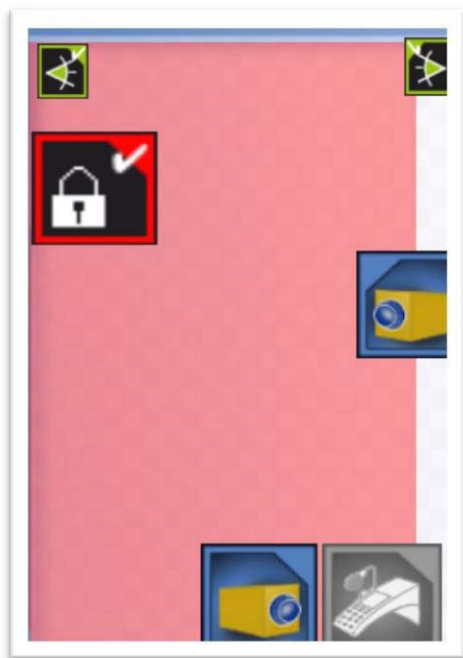




Sygnalizacja Włamania i Napadu

Systemem SWiN można zarządzać (m.in. zazbrajać/rozbrajać strefy) z poziomu:

- Mapy synoptycznej w systemie iProtect (np. na portierni);
- Klawiatury umieszczonej (np. na ostatnim piętrze budynku);
- Czytnika kontroli dostępu (np. automatycznie po wyjściu z pomieszczenia).





Sygnalizacja Włamania i Napadu

- Klarowna procedura działania alarmowego w postaci interaktywnych kroków postępowania;
- Możliwość dowolnej konfiguracji procedury w zależności od rodzaju alarmu (np. zasłonięcie rolet antywłamaniowych w pomieszczeniu).

Szczegóły alarmu

Opis: 18-10-12 13:56:30 - Karta skradziona
 Użytkownik karty nie ma dostępu [5: Karta skradziona] [5: 2 1 1 Sale
 Konferencyjna PIN] [-1725: Błędny pinkod] [34: 1654
 skradziona] Numer karty RCN 1654178 70 [2: 32 BT

Akcje Centrum Rozwiązań Kamera

Nr	Akcja	Status
✓ 1	SSWiN Włącz Stroboskop	wykonana
✓ 2	Commend Skradziona karta ON	wykonana
✓ 3	Stroboskop włączony	wykonana
✓ 4	Czytniki zablokowane	wykonana
→ 5	Próba użycia skradzionej karty !	Do wykonania
UWAGA!		
Próba użycia skradzionej karty !		
Zweryfikuj to zagrożenie !		
→ 6	Commend Skradziona karta OFF	Do w
→ 7	SSWiN Wyłącz Stroboskop Manula	Do w
→ 8	Stroboskop wyłączony	Do w
→ 9	Odblokuj czytniki	Do w
→ 10	Zakończ zdarzenie	Do wykonania

Informacja o rodzaju alarmu i miejscu alarmu

Zaprezentowanie miejsca wystąpienia alarmu na mapie i obrazu z kamery

Lista działań wykonanych (np. zablokowanie czytników, wywołanie komunikatu itp.)

Lista kroków do wykonania (np. odblokuj drzwi, zadzwoń na policję itp.)

Monitoring wizyjny CCTV





Monitoring wizyjny

Korzyści zastosowania monitoringu wizyjnego:

- Zmniejszenie strat spowodowanych wandalizmem i kradzieżami (szczególnie tereny zewnętrzne);
- Usprawnienie działania służb ochrony (weryfikacja);
- Zwiększenie bezpieczeństwa użytkowników;
- Efekt psychologiczny „kamery”.

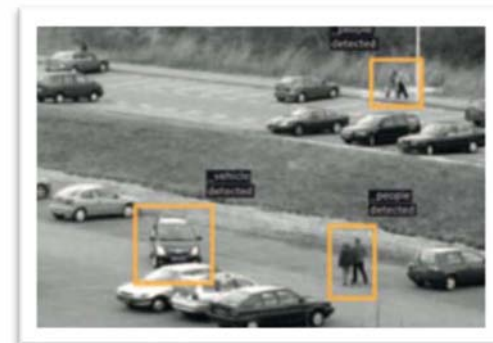




Monitoring wizyjny

Inteligentna analiza materiału wideo (VCA) - realizowana w kamerze lub serwerze:

- Wirtualna ochrona obwodowa obiektu (ObjectR);
- Śledzenie ruchu osób oraz przedmiotów (ObjectR);
- Rozpoznawanie twarzy i tablic rejestracyjnych (FaceR, CarR);
- Zliczanie osób wchodzących do obiektu / pomieszczenia;
- Funkcja Inteligentnego antysabotażu (SceneR).





Monitoring wizyjny

Różnorodność punktów kamerowych pozwala na :

- Dopasowanie do warunków oświetleniowych oraz środowiskowych;
- Dobór obiektywu o odpowiedniej ogniskowej - (odpowiednie kadrowanie obserwowanej sceny);
- Dopasowanie miejsca i metody montażu.

Możliwość podłączenia do systemu kamer różnych producentów (np. w momencie gdy część obiektów posiada już zainstalowane kamery CCTV)

Stacjonarne



Kompaktowe



Kopułkowe



Szybkoobrotowe PTZ

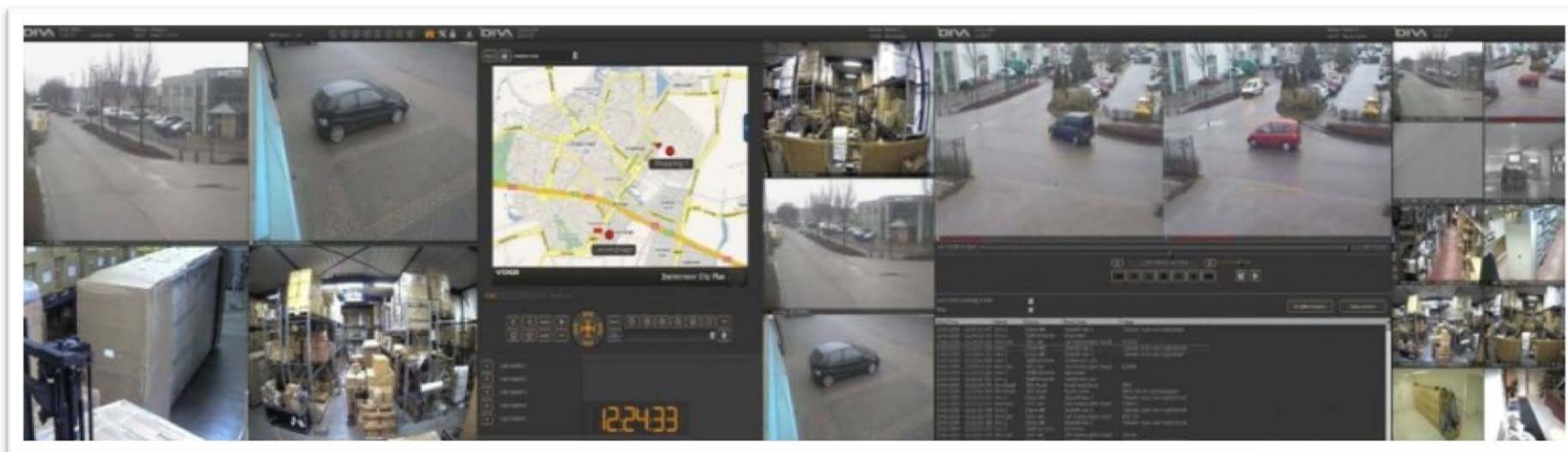




Monitoring wizyjny

Pełna integracja platformy CCTV z SMS iProtect:

- Archiwizacja wideo przypisana do zdarzeń z pozostałych systemów;
- Interakcje zdarzeń wideo (KD, SSWiN, Parking itp.);
- Inteligentna analiza wideo (m.in. analiza ruchu, rozpoznawanie tablic);
- Presety i sterowanie PTZ bezpośrednio z poziomu mapy synoptycznej na stanowisku nadzoru.



Komunikacja głosowa i rozgłoszeniowa





Komunikacja głosowa

System rozgłoszeniowy na terenie obiektu:

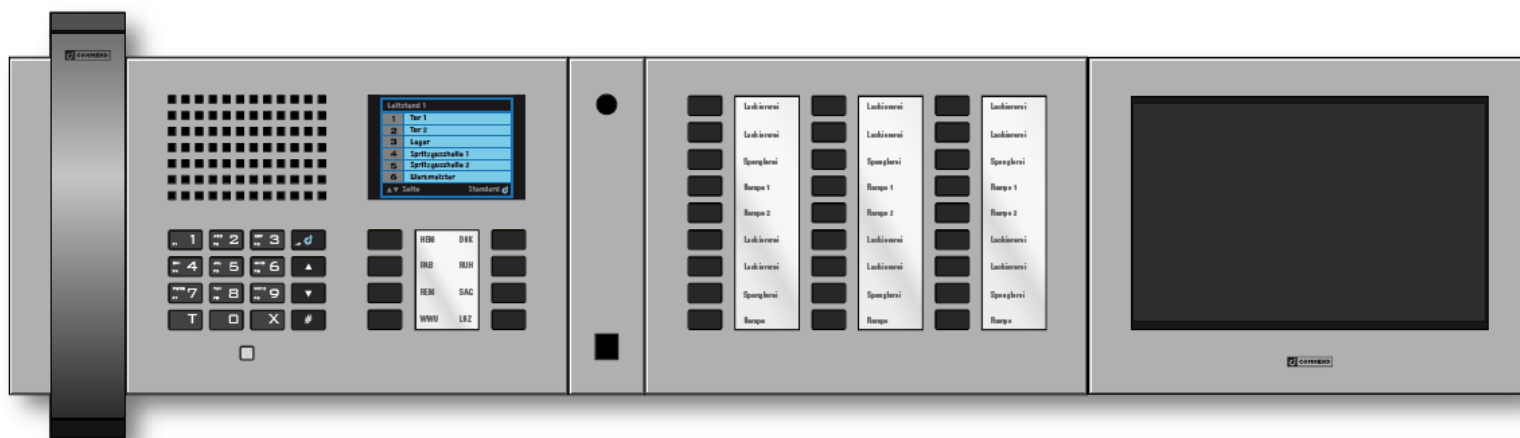
- Wszystkie pomieszczenia i ciągi komunikacyjne
 - Przekazywanie komunikatów alarmowych („Proszę opuścić budynek”);
 - Komunikaty predefiniowane lub przekazywane w czasie rzeczywistym.
- Komunikacja rozgłoszeniowa w obrębie wybranych pomieszczeń, np. „o nowościach produktowych, reklamy itp.”.



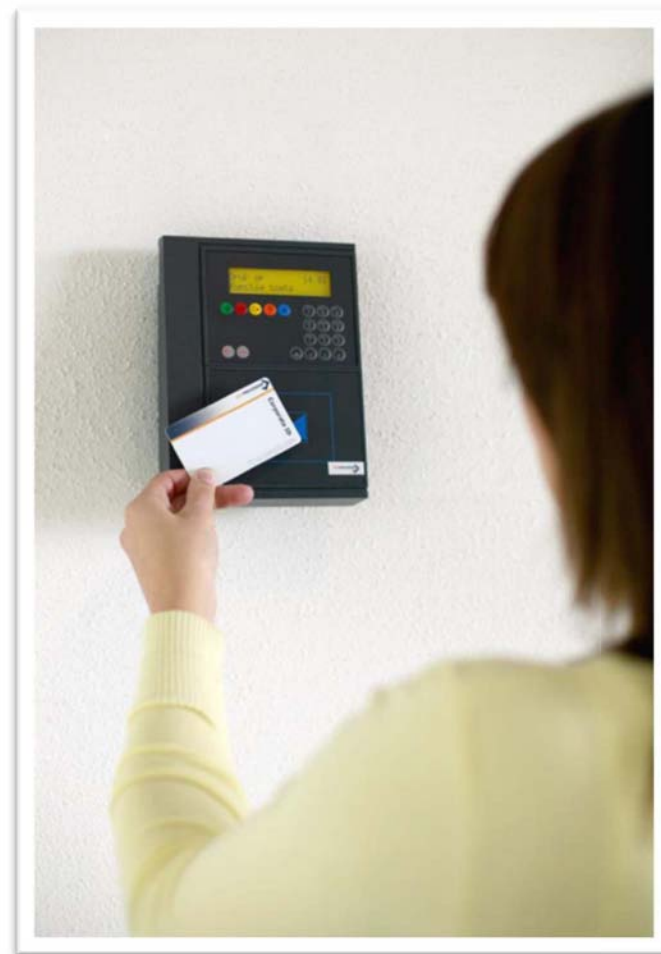


Komunikacja głosowa

- Komunikacja w ramach numerów abonenckich (komunikacja dwukierunkowa jeden do wielu – wiele do jednego, komunikacja dwukierunkowa punkt – punkt);
- Komunikacja z dowolnym innym systemem telekomunikacyjnym (numery zewnętrzne, telefonia DECT);
- Interkomy SOS w obrębie „ciągów komunikacyjnych” (komunikacja dwukierunkowa punkt – punkt);
- Komunikacja dostępowa w obrębie wejść oraz wjazdów na teren uczelni (komunikacja dwukierunkowa punkt – punkt).



Rejestracja Czasu Pracy





Rejestracja Czasu Pracy

- Monitoring i rejestracja czasu pracy pracowników;
- Pełna obsługa różnych rodzajów pracy, np. pracy zmianowej, nienormowanej i dowolnie definiowanych wyjątków np. urlopów, świąt itp.;
- Rozbudowany moduł raportowania (PDF, XLS), możliwość eksportu danych do systemu Kadry-płace.





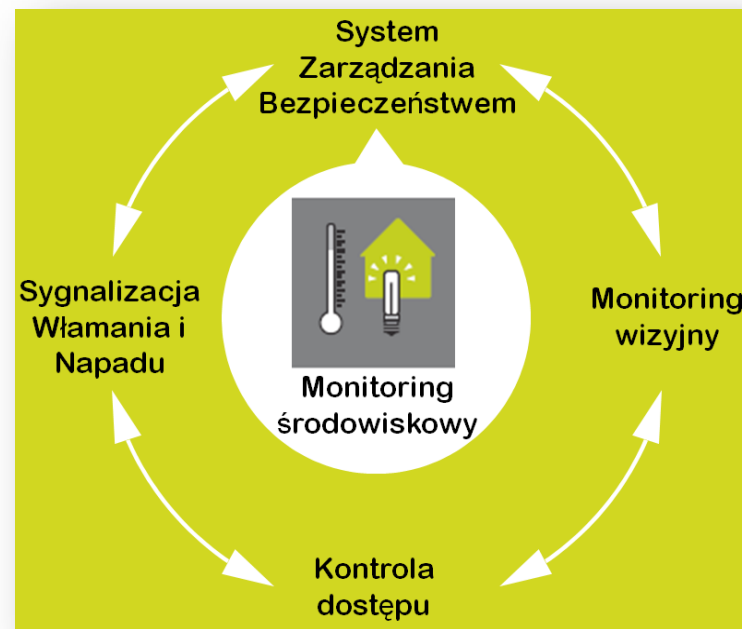
Rejestracja Czasu Pracy

Możliwość realizacji rejestracji w oparciu o:

- Czytniki kontroli dostępu (rejestracja wejść/wyjść);
- Dedykowane czytniki RCP (programowalne przyciski);
- Punkty Infobox (pełna dowolność konfiguracji).



Integracja automatyki i monitoring parametrów środowiskowych





Integracja automatyki

Realizowane funkcjonalności:

- Wizualizacja stanu kluczowych parametrów automatyki (np. stanu / wartości mierników);
- Przesyłanie informacji alarmowych z systemu automatyki do systemu SMS (korelacja zdarzeń, procedura alarmowa);
- Zarządzanie kluczowymi elementami automatyki.

Sposób integracji:

- Twardostykowo w oparciu o dedykowane moduły I/O;
- Wykorzystując protokoły warstw wyższych (np. BACnet).





Monitoring Środowiskowy

Możliwość pełnej kontroli parametrów środowiskowych, rejestrowanych przez szerokie spektrum czujników:

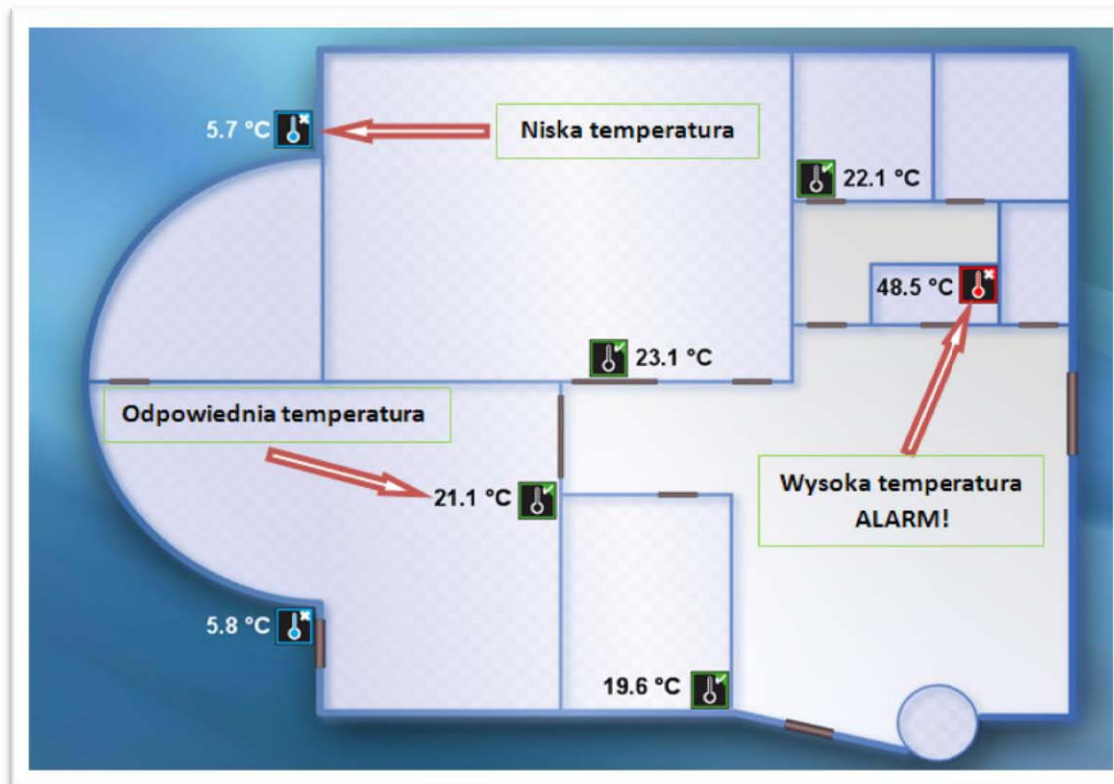
- pomiar temperatura w pomieszczeniu lub szafie serwerowej;
- poziom wilgotności lub czujnik zalania;
- poziom śniegu na dachu budynku;
- poziom deszczu, natężenia słonecznego, siły wiatru.





Monitoring Środowiskowy

- Prezentacja wartości parametrów środowiskowych bezpośrednio z poziomu mapy synoptycznej (wizualizacji);
- Aktualizacja wartości w czasie rzeczywistym (co 1 s.);
- Wywołanie alarmu w momencie przekroczenia wartości progowej – np. „Zbyt wysoka temperatura w szafie serwerowej nr 3 (Budynek 4)”.



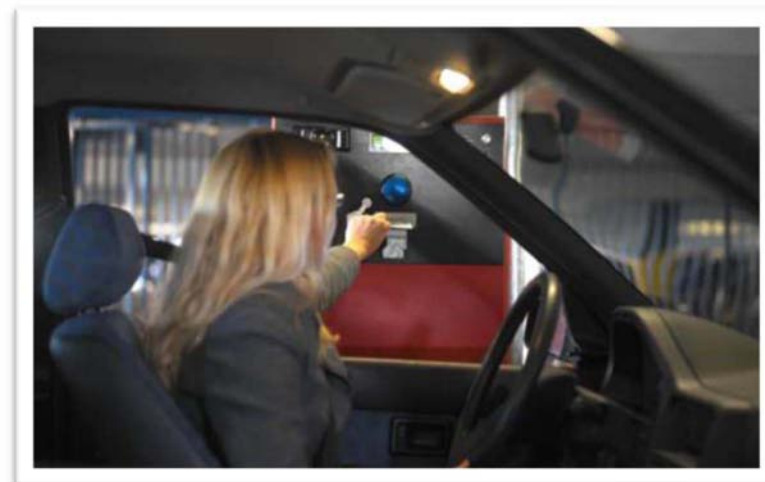
Zarządzanie parkingiem przy obiekcie





Zarządzanie parkingiem

- Zarządzanie dostępem do parkingu przy obiekcie - w oparciu o czytniki dalekiego zasięgu;
- Definiowanie limitu liczby samochodów dla poszczególnych grup użytkowników – pracowników poszczególnych firm, administracyjnych, zarządu itp.;
- Możliwość prezentowania dostępności miejsc (lub braku) na tablicy informacyjnej.





Zarządzanie parkingiem

- Komunikacja w obrębie infrastruktury danego parkingu z portiernią najbliższego budynku (komunikacja interkomowa);
- Integracja funkcji rozpoznania tablic rejestracyjnych (możliwość podwójnej weryfikacji – tablica + karta);
- Możliwość sterowania szlabanem bezpośrednio z poziomu wizualizacji.



Integracja systemów zewnętrznych





Integracje zewnętrzne

- Depozytor kluczy – system zarządzania kluczami do poszczególnych pomieszczeń;
- Zaimplementowana Integracja:
 - Wbudowany czytnik kontroli dostępu zintegrowany z KD iProtect;
 - Sygnał alarmowy przesyłany do SMS iProtect;
 - Sterowanie otwarciem drzwi;
 - Wizualizacja i zarządzanie dostępem do poszczególnych kluczy.





Integracje zewnętrzne

Zaimplementowana Integracja:

- przesyłanie informacji o zdarzeniach alarmowych z centrali SSP do systemu iProtect i rozróżnienie rodzaju alarmu;
- definiowanie dowolnych procedur działania alarmowego w iProtect i kroków, które operator systemu musi wykonać;
- wizualizacja na mapie synoptycznej stanu poszczególnych detektorów i/lub stref SSP.



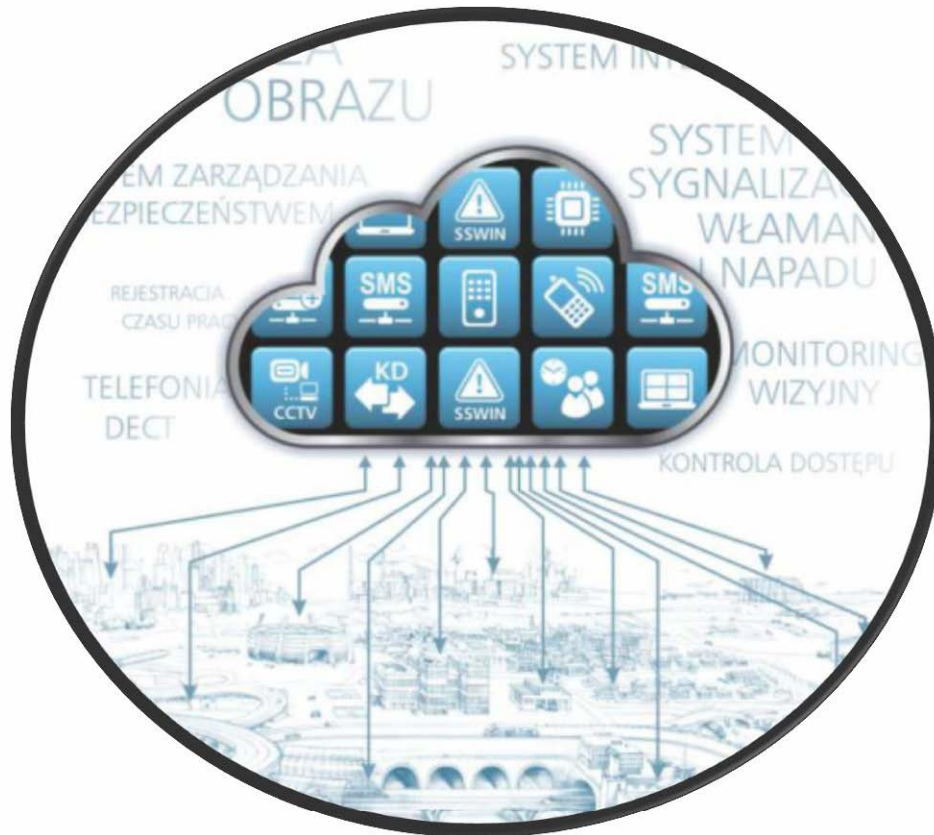
Rozproszony system bezpieczeństwa (SecAAS)

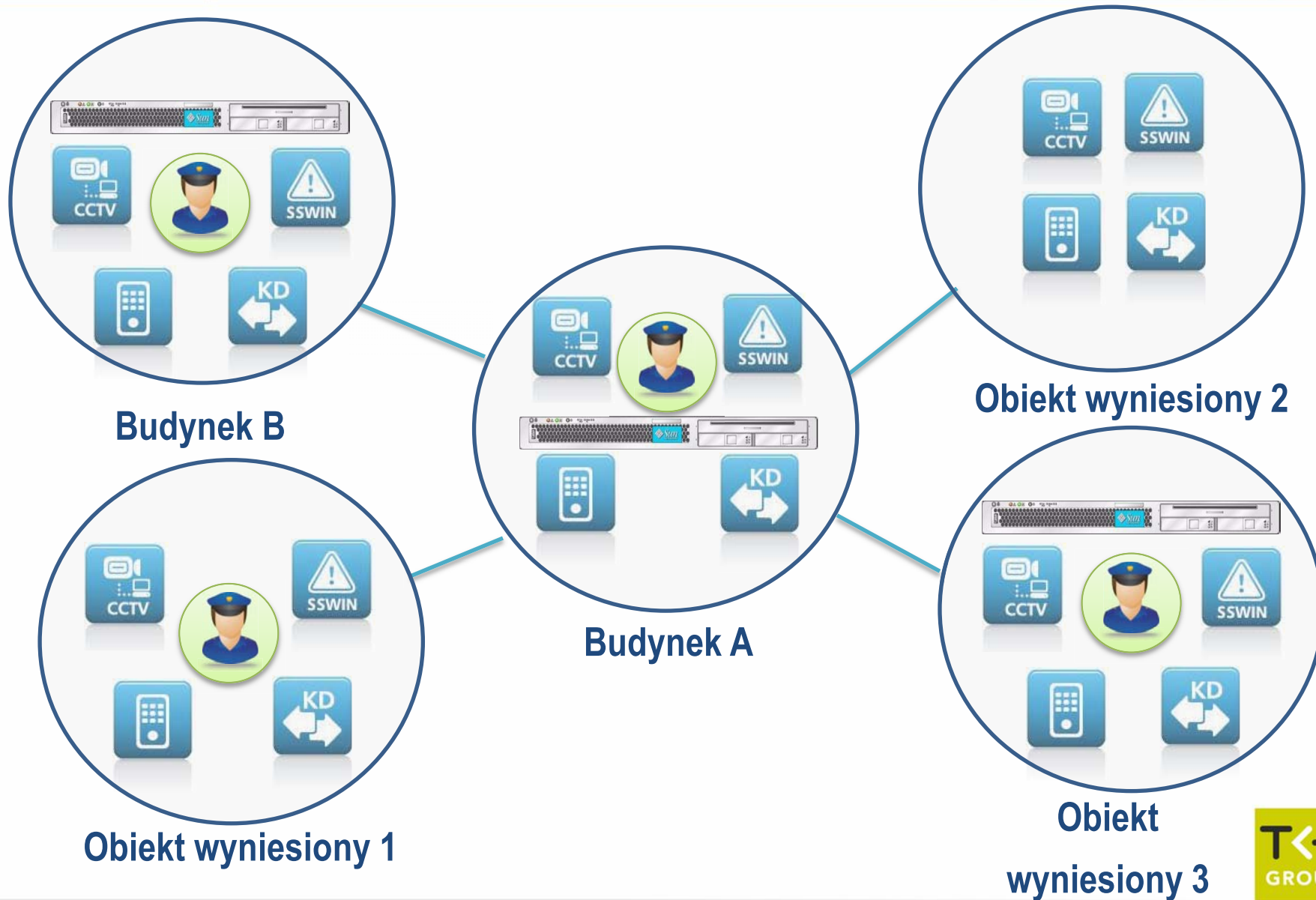




SecAAS

- Możliwość stworzenia zintegrowanego systemu bezpieczeństwa w obrębie budynku, lokalizacji lub nawet wszystkich obiektów wyniesionych
- Serwery zlokalizowane w centralnym punkcie lub rozproszone, z jednym serwerem nadzorującym.





**SecAAS**

Centralny punkt systemu bezpieczeństwa:

- Odbieranie informacji alarmowych z wszystkich lokalizacji – szybka reakcja na zdarzenie alarmowe;
- Wizualizacji urządzeń na mapie synoptycznej dla wszystkich obiektów w punkcie centralnym;
- Automatyczne przełączanie obsługi na centralę w momencie np. zakończenie pracy portiera w jednym z budynków.





SecAAS

- ✔ Redukcja kosztów inwestycyjnych (CapEx)
- ✔ Redukcja kosztów operacyjnych (OpEx)
- ✔ Skalowalność systemu
- ✔ Zdalne monitorowanie
- ✔ Dedykowane urządzenia końcowe
- ✔ Zaawansowane raportowanie zbiorcze
- ✔ Szybkie działanie w sytuacji alarmowej



Wybrane referencje

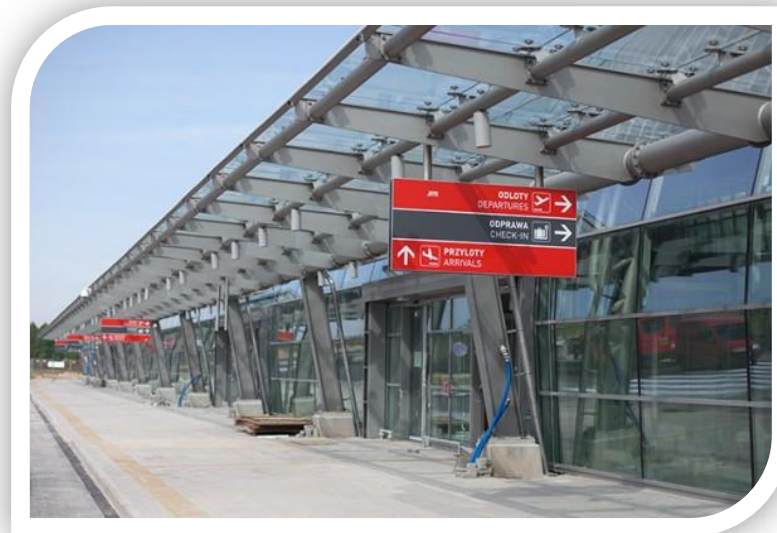
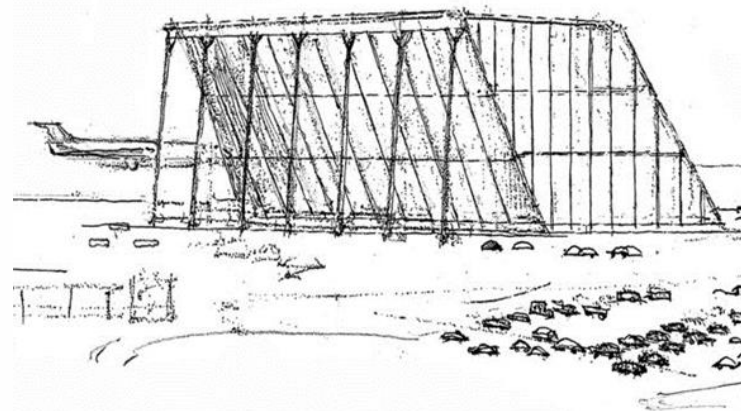


Kluczowe liczby:

- 8 obiektów (SecAAS)
- 240 czytników kontroli dostępu
- 7 central SSWiN (700 detektorów)
- 260 kamer CCTV
- 40 interkomów

Najważniejsze cechy:

- Pełna integracja systemów CCTV + KD + SSWiN + Interkomowy
- SecAAS – cały teren portu lotniczego

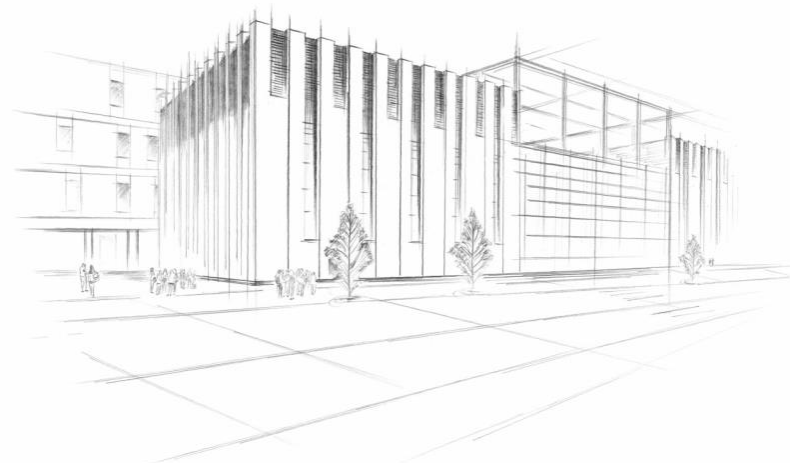


Kluczowe liczby:

- 4 obiekty (SecAAS)
- 100 czytników kontroli dostępu
- 5 central SSWiN (500 detektorów)
- 60 kamer CCTV
- 15 interkomów

Najważniejsze cechy:

- Inteligentne parkingi (zintegrowana analiza tablic rejestracyjnych)
- Pełna integracja systemów CCTV + KD + SSWiN + Interkomy
- SecAAS – lokalizacje oddalone o kilka km od siebie.

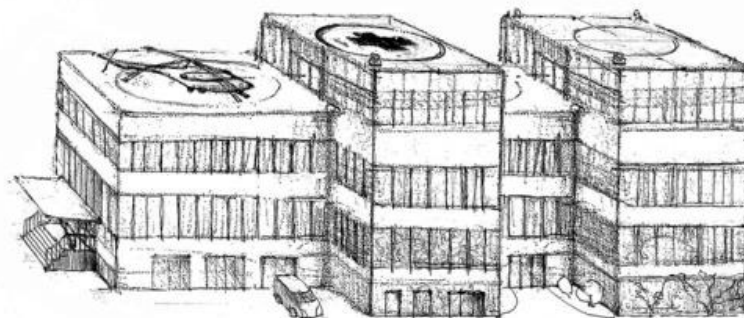


Kluczowe liczby:

- 183 czytniki kontroli dostępu
- 130 interkomów

Najważniejsze cechy:

- Zaawansowana kontrola dostępu do wind;
- Inteligentne parkingi (zintegrowana analiza tablic rejestracyjnych i czytniki dalekiego zasięgu)
- Pełna integracja systemów CCTV + KD + SSWiN + Interkomowy

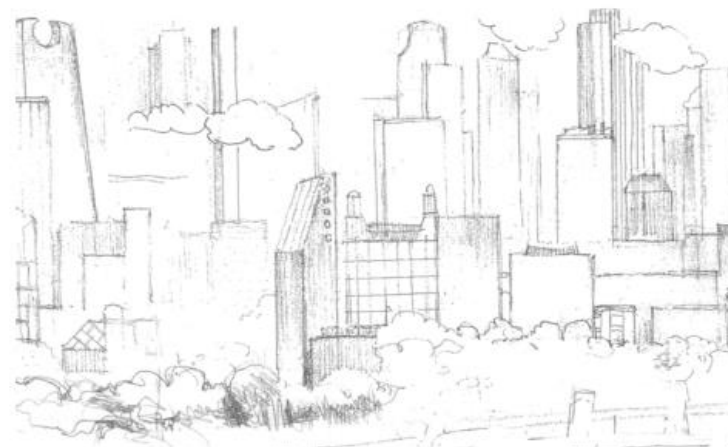


Kluczowe liczby:

- 81 czytników kontroli dostępu
- 2 centrale SSWiN (200 detektorów)
- 48 kamer CCTV
- 8 interkomów

Najważniejsze cechy:

- Inteligentne parkingi (zintegrowana analiza tablic rejestracyjnych i czytniki dalekiego zasięgu)
- Pełna integracja systemów CCTV + KD + SSWiN + Interkomowy



- UMK w Toruniu Collegium Hummanisticum
- Uniwersytet Gdański Wydział Chemii
- Budynek Urzędu Gminy + Szkoła w Wejherowie
- Budynek wyniesiony Polpharma w Gdańsku
- PKP Energetyka (Warszawa)
- Szpital kliniczny CUMRIK (Kraków)
- Dystrybutor energii ENEA (Poznań)
- Zakłady przetwórcze CEDROB (Ciechanów)
- Biurowiec i fabryka WILO (Lesznowola)
- Małopolski Park Technologii Informatycznych (Kraków)
- Targi Kielce



- Obsługa pełnego zakresu podsystemów bezpieczeństwa i komunikacji z poziomu jednej platformy;
- Skalowalność i modułowość systemu;
- Systemy pracujące w IP (SecAAS);
- Integracja podsystemów (Interakcje międzysystemowe);
- Integracja z rozwiązaniami zewnętrznymi;
- Jeden dostawca rozwiązania SMS i wszystkich podsystemów składowych.





DZIĘKUJĘ ZA UWAGĘ



www.ccpartners.pl