System ICT PROTEGE to wysoko skalowalna platforma oferująca zintegrowany system bezpieczeństwa dla obiektu, z możliwością realizacji funkcji automatyki budynkowej oraz z szerokimi możliwościami integracji z zewnętrznymi systemami.

W obrębie systemu są możliwe do wykorzystania następujące moduły funkcjonalne:

* Kontrola Dostępu
* System Sygnalizacji Włamania i Napadu
* Rejestracja Gości
* Zarządzanie windami
* Rejestracja Czasu Pracy
* Interkom (komunikacja)
* Automatyka Budynku
* Integracja REDWALL REDSCAN
* Integracja INOVONICS
* Integracja KABA CENCON O2
* Integracja czytników biometrycznych SUPREMA
* Szerokie możliwości integracji z systemami zewnętrznymi
* CCTV
* Zewnętrzne Systemy BMS
* Systemy Zamków Offline AssaAbloy i SALTO
* Dyspozytornie kluczy
* Usługa Data Sync
* Web SOAP - interfejs www oraz integracje na życzenie
* Protokół Automation & Control (protokół integracji na poziomie kontrolerów głównych PROTEGE)
* MSMQ (Microsoft Message Queue)
* Active Directory, LDAP
* MODBUS IP, BACNet IP

# Normy

System spełnia wymagania norm EN50131 (część SSWiN) oraz EN 60839-11-1:2013 (część KD):

EN50131: Stopień Zabezpieczenia 4, Klasa Środowiskowa II

EN 60839-11-1:2013: Klasa rozpoznania 2 (jeżeli czytniki KD bez klawiatury)  
 Klasa rozpoznania 3 (jeżeli czytniki KD z klawiaturą)  
 Klasa dostępu B

# Oprogramowanie

* Architektura klient – serwer z funkcjami kontroli systemu i monitorowania zdarzeń online
* Komunikacja ze Zintegrowanymi Kontrolerami Systemowymi odbywa się poprzez sieć Ethernet, opcjonalnie jako medium rezerwowe można wykorzystywać połączenia modemowe
* Graficzne interaktywne mapy wizualizacyjne z łatwym w użyciu wbudowanym kreatorem, wewnętrzną biblioteką symboli i przyciskami funkcyjnymi
* Oprogramowanie umożliwia automatyczne kasowanie zdarzeń po określonym czasie, np. zdarzenia starsze niż 1 miesiąc, 2 miesiące, 6 miesięcy, 9 miesięcy i 1 rok – pozwala to na uniknięcie zapełnienia bazy danych zdarzeń oraz pozwala na spełnienie wymagań polityki bezpieczeństwa i prywatności danych użytkowników
* Oprogramowanie wykonuje auto archiwizację ustawień każdego dnia, ścieżka zapisu archiwum jest być możliwa do określenia w sposób swobodny
* System loguje aktywność wszystkich operatorów w oprogramowaniu – dzięki temu dostępny jest ciągle pełny audyt systemu, można z łatwością sprawdzić który operatora wykonywał jakie operacje w systemie i jakich zmian dokonał
* System umożliwia odtwarzanie dźwięku alarmowego w oprogramowaniu dla zdarzeń alarmowych
* System posiada możliwość integracji z Active Directory zarówno w zakresie integracji użytkowników jak i operatorów
* System umożliwia integrację z czytnikami biometrycznymi
* Oprogramowanie pozwala na definiowanie dowolnej ilości operatorów z możliwością tworzenia dowolnej ilości profili dostępu i uprawnień dla tych operatorów
* Funkcje i rekordy (np. drzwi, czujki, użytkownicy) niedostępne dla danego operatora są dla niego niewidoczne
* System umożliwia definiowane uprawnień ręcznej kontroli i sterowania stref alarmowych, drzwi KD, zintegrowanych wind, klawiatur, wyjść przez operatorów
* System umożliwia włączenie i / lub wyłączenie widoczności kodów PIN użytkowników dla poszczególnych operatorów
* Dla każdego operatora istnieje możliwość określenia adresu e-mail na który oprogramowanie systemu będzie wysyłało automatycznie generowane raporty
* Oprogramowanie pozwala na automatyczne wylogowanie operatora nieaktywnego przez zadany czas, czas nieaktywności jest możliwy do zdefiniowania indywidualnie dla każdego operatora
* System umożliwia kolorowanie zdarzeń wyświetlanych na listach zdarzeń i listach alarmowych, istnieje możliwość ustalenia koloru tła i czcionki dla każdego możliwego typu zdarzenia z osobna
* Oprogramowanie posiada pełny audyt systemu – wszystkie zmiany wykonywane przez operatorów (np. zmiany użytkowników, poziomów uprawnień, ustawień poszczególnych elementów, itp.) są zapamiętane a system pozwala na wyświetlanie historii zmian dla wszystkich rekordów użytkowników, drzwi, czujek, stref, itp.
* Oprogramowanie umożliwia eksportowanie danych i ustawień do pliku CSV lub PDF, XLS w celu archiwizacji ustawień
* System umożliwia tworzenie dowolnej ilości harmonogramów. W obrębie każdego harmonogramu jest możliwość utworzenia 8 okresów czasowych z dokładnością co do minuty. Każdy z tych okresów czasowych będzie można przypisać do wybranych dni tygodnia (pełna dowolność, do żadnego, kilku lub wszystkich dni). Do każdego harmonogramu można przypisać WAKACJE (dni w roku określone konkretną datą, datami lub przedziałami dat). System umożliwia określenie czy każdy ze zdefiniowanych okresów w ramach poszczególnych harmonogramów jest aktywny w WAKACJE, nieaktywny w WAKACJE lub też ignoruje okresy WAKACJI.
* Zdefiniowany harmonogram jest widoczny w postaci graficznej umożliwiając łatwe zweryfikowanie zdefiniowanych okresów czasowych w poszczególnych dniach tygodnia.
* System umożliwia aktywację i dezaktywację utworzonego harmonogramu uzależnioną od innego elementu systemu np. od wyjścia, w tym od wyjścia wirtualnego
* System wyświetla dla każdego rekordu gdzie ten rekord jest wykorzystywany w systemie, np. okno programowania wejścia alarmowego pokazuje w jakich strefach dane wejście jest używane, okno poziomu dostępu powinno pokazywać do jakich użytkowników dany poziom dostępu został przypisany, itp.
* System powinien umożliwiać zamknięcie, otwarcie na stałe oraz wydłużenie czasu otwarcia z definicją wydłużonego czasu otwarcia drzwi w konkretne dni kalendarzowe w określonych dla tych dni godzinach
* System powinien umożliwiać włączanie i wyłączanie wyjść w konkretne dni kalendarzowe w określonych dla tych dni godzinach
* Wszystkie akcje kalendarza opisane powyżej powinny być widoczne w formie listy, oraz kalendarza tygodniowego i miesięcznego
* System musi umożliwiać synchronizację czasu dla kontrolerów głównych za pomocą co najmniej dwóch serwerów czasu ntp (główny i zapasowy), z określeniem strefy czasowej
* System musi umożliwiać ustawienie okresu czasu letniego
* Wsparcie dla różnych typów identyfikatorów: System musi umożliwiać tworzenie niestandardowych identyfikatorów np. tekst Unicode, ASCII lub UTF-8, z możliwością określenia wrażliwości na małe i duże litery, wartość liczbowa lub, Hexadecymalna. Identyfikatory te później będą używane do identyfikacji użytkowników (np. w formie tablicy rejestracyjnej)
* Oprogramowanie musi umożliwiać import użytkowników z pliku CSV (dane oddzielone przecinkiem), import ten musi być możliwy na żądanie (ręczny) jak i automatyczny wg zdefiniowanego harmonogramu (np. każdego dnia o określonej godzinie, lub ciągle co 5 minut), harmonogram importu powinien być definiowany możliwie elastycznie
* System powinien umożliwiać definiowane grup dla użytkowników i wyświetlanie użytkowników w postaci listy lub w grupach
* System powinien wspierać obsługę dowolnej liczby użytkowników, co najmniej 500 000
* System powinien umożliwiać przypisanie do użytkownika kodu PIN, co najmniej 8 identyfikatorów zbliżeniowych (kart, breloków) oraz pilotów systemowych, dodatkowo system musi umożliwiać przypisywanie do użytkowników identyfikatorów niestandardowych, jak np. numer tablicy rejestracyjnej, lub ciąg znaków tekstowych, każdy z identyfikatorów powinien posiadać opcję wyłączenia (bez jego usuwania)
* Oprogramowanie powinno umożliwiać tworzenie dodatkowych pól dla rekordów użytkowników, tak aby zamawiający mógł opisać użytkownika wszystkimi wymaganymi danymi (np. nr rejestracyjny samochodu, dział, nr administracyjny)
* System musi posiadać moduł Photo-ID z kreatorem kart i identyfikatorów, oraz zarządzaniem dystrybucją obrazów do wszystkich lokalizacji zarządzania danymi, zdjęcia użytkowników mają być wyświetlane na listach zdarzeń na żywo
* Dla każdego użytkownika musi być możliwość określenie jego czasu ważności, musi być możliwość wprowadzenie do systemu użytkownika, dla którego okres aktywności będzie zaczynał się dopiero w przyszłości
* Dla każdego użytkownika musi być możliwość przypisania domyślnej strefy alarmowej, która będzie automatycznie rozbrojona po zalogowaniu się użytkownika do klawiatury (bez konieczności wybierania dodatkowych akcji na klawiaturze)
* Do każdego użytkownika można przypisać dowolną liczbę poziomów dostępu
* Każdy poziom dostępu określa uprawnianie użytkownika w zakresie
  + Dostępu do poszczególnych drzwi lub/i grup drzwi
  + Wind i/lub grup wind
  + Pięter w windach
  + Funkcji menu w klawiaturach
  + Uzbrajane strefy
  + Rozbrajane strefy
  + Sterowanych wyjść
  + W zakresie każdego z w/w rekordów przypisywanych do poziomu dostępu musi być możliwość zdefiniowania harmonogramu ważności danego rekordu w danym poziomie dostępu, np. przypisując do poziomu dostępu DRZWI X musi być możliwe określenie że te drzwi w tym poziomie dostępu działają np. tylko od Poniedziałku do Piątku tylko w godzinach od 8:00 do 16:00, itp.
* Do każdego poziomu dostępu można przypisać harmonogram określający jego ważność
* System musi umożliwiać łatwe wyszukiwanie użytkownika wg dowolnego pola używanego w systemie do opisu i ustawień użytkowników, w tym także wg pól własnych zdefiniowanych na etapie uruchomienia systemu, np. jeżeli w systemie zostanie zdefiniowane pole dla użytkownika pod tytułem DOWÓD OSOBISTY, system musi umożliwiać wyszukiwanie użytkowników wg DOWODÓW OSOBISTYCH
* System musi umożliwiać tworzenie pól własnych służących do opisu użytkowników. Pola te będą mogły zawierać następujące dane: tekst, wartość liczbowa, czas, data, czas+data, opcja wyboru, lista rozwijana wyboru, link, obraz
* System musi posiadać moduł umożliwiający tworzenie zadruków kart (identyfikatorów), z możliwością wstawienia na wydruk dowolnego pola opisującego użytkownika
* System musi umożliwiać swobodne wyszukiwanie zdarzeń za wybrany okres, który można zdefiniować datą, godziną i minutą początku oraz datą, godziną i minuta końca, wyszukiwanie zdarzeń powinno umożliwiać wyszukiwanie wszystkich typów zdarzeń lub też ograniczenie wyszukiwania do wybranych typów zdarzeń, jednocześnie musi być możliwość ograniczenia wyszukiwania zdarzeń do wybranych rekordów (np. wybranych drzwi, wejść alarmowych, użytkowników, stref, itp.) przy czym musi być możliwość wybrania co najmniej dwóch różnych typów rekordów, które jednocześnie muszą wystąpić w wyszukiwanym zdarzeniu (np. musi być możliwe wyszukiwanie zdarzeń udzielenia dostępu na drzwiach A i B dla użytkowników X, Y i Z)
* Zaawansowany i łatwy w użyciu generator raportów z szerokimi możliwościami dostosowywania do własnych potrzeb, z możliwościami tworzenia zaawansowanych filtrów, które pokazują tylko wybrane typy zdarzeń z wybranych rekordów (użytkowników, drzwi, czujek, itp.) – raporty muszą mieć możliwość zapisywania co najmniej w formatach PDF, CSV, XLS, XLSX, HTML, MHT, RTF, TXT
* Wygenerowany raport zdarzeń musi umożliwiać następujące działania:
  + Raport przedstawiony w formie tabeli z co najmniej następującymi kolumnami: ID zdarzenia, opis zdarzenia, czas wystąpienia zdarzenia, czas zapisu do bazy danych, użytkownik (jeżeli występuje w zdarzeniach), drzwi (jeżeli występują w zdarzeniach), kontroler główny z którego pochodzi zdarzenie, czas potwierdzenia alarmu (jeżeli zdarzenie alarmowe), komentarz dla alarmu (jeżeli zdarzenie alarmowe), instrukcje dla alarmu (jeżeli zdarzenie alarmowe), osoba potwierdzająca alarm (jeżeli zdarzenie alarmowe)
  + Wyszukiwanie ciągu znaków w wybranej kolumnie tabeli zdarzeń za pomocą pisania w górnym wierszu
  + Przestawianie kolejności kolumn
  + Grupowanie zdarzeń za pomocą danych w jednej lub wielu kolumnach, np. grupowanie zdarzeń wg drzwi, a następnie wg użytkowników
  + Łatwa zmiana kolejności grupowania za pomocą „przeciągnij i upuść”
  + Sortowanie rosnąco i malejąco w każdej z kolumn
  + Tworzenie własnych filtrów wyszukiwania zdarzeń w raportach, z co najmniej 10 warunkami (równe, różne, większe, mniejsze, zawiera, nie zawiera, zaczyna się od, kończy się na, jedno z , żaden z, puste, niepuste) i zależnością między warunkami (AND, OR, NOTAND, NOTOR), filtry muszą wspierać wielostopniowość (np. utworzony filtr wyszukuje wszystkie zdarzenia na drzwiach zaczynających się na BUDYNEK i w tych zdarzeniach wyszukuje tylko takie zdarzenia, które wystąpiły po określonej dacie i zawierały określonych użytkowników)
  + Zapisywanie utworzonych filtrów do późniejszego wykorzystania
* Oprócz wyszukiwania zdarzeń system musi oferować możliwość zapisywania określonych typów raportów ze zdefiniowanymi już właściwościami, tak aby można było je wywołać w przyszłości z podaniem tylko okresu za który raport ma być wykonany
* System musi umożliwiać wykonywanie raportów ewakuacyjnych, pokazujących osoby przebywające w określnych obszarach lub strefach, z informacja o ostatnich drzwiach na których została odbita karta (lub inny identyfikator) użytkownika, raport ewakuacyjny musi mieć możliwość automatycznego wysłania do wybranych operatorów jeżeli wystąpi zdarzenie zagrożenia (definiowane)
* System powinien umożliwiać definiowanie raportów obecności lub rejestracji czasu pracy, które pokazują godziny wejść i wyjść użytkowników na teren określonego obszaru, wraz z czasem ich przebywania, do tych raportów musi być możliwe definiowanie dziennych harmonogramów czasu pracy (kiedy użytkownik jest spodziewany na obiekcie)
* System musi umożliwiać generowanie następujących raportów o użytkownikach:
  + Raport o wszystkich użytkownikach z wybranymi danymi oraz sortowaniem wg wybranej kolumny
  + Raport na temat wszystkich użytkowników, którzy posiadają dostęp do wybranych drzwi (więcej niż jedne drzwi do wyboru w raporcie)
  + Raport o wszystkich użytkownikach uwzględnionych w wybranych poziomach dostępu (więcej niż jeden poziom dostępu dla raportu)
  + Raport o użytkownikach występujących w określonych typach zdarzeń za wybrany okres czasowy
  + Raport o użytkownikach występujących w określonych typach zdarzeń i jednoczęsnie w określonych drzwiach za wybrany okres czasowy, np. raport pozwalający znaleźć wszystkich użytkowników, którym został odmówiony dostęp na wybranej grupie drzwi za ostatni miesiąc
  + Raport o użytkownikach, których ważność wygaśnie w ciągu określonej ilości dni, ilość dni do wygaśnięcia ważności może być swobodnie definiowana
  + Raport o użytkownikach, który przeszli jako ostatni przez określone drzwi (możliwość wyboru więcej niż jednych drzwi)
  + Raport o użytkownikach, którzy nie występują w zdarzeniach za wybrany okres czasowy (użytkownicy nieaktywni)
  + Wszystkie z w/w raportów musza umożliwiać wybranie danych użytkownika, które mają znaleźć się w raporcie oraz kolumny wg której nastąpi sortowanie raportu, kolejność kolumn raportu musi być możliwa do przestawienia
* System musi mieć możliwość automatycznego wysyłania raportów za pomocą e-mail do wybranych operatorów (więcej niż jednego) wg harmonogramu tygodniowego, raport ma być wysyłany w formacie PDF, XLS lub CSV
* System musi umożliwiać automatyczne wysyłanie zdarzeń poprzez e-mail do wybranych operatorów (więcej niż jednego) w sytuacji kiedy nastąpi określone zdarzenie w systemie
* System musi umożliwiać definiowanie dowolnych zdarzeń jako zdarzeń ALARMOWYCH
* Na listach zdarzeń zdarzenia alarmowe muszą być oznaczone kolorem (np. czerwony kolor tła i biały kolor czcionki) oraz znakiem graficznym (np. wykrzyknik)
* Występujący alarm musi być sygnalizowany za pomocą wyskakującego okienka lub innego elementu oprogramowania zwracającego jednoznacznie uwagę operatora, jednocześnie przy wystąpieniu zdarzenia alarmowego lub innego zdefiniowanego zdarzenia oprogramowanie musi odtwarzać dźwięk alarmowy do momentu wyciszenia alarmu lub jego potwierdzenia
* Oprogramowanie musi umożliwiać zablokowanie wyskakujących okien z alarmami oraz dźwięków alarmowych na pewien czas oraz do następnego logowania operatora, ta funkcja musi być dostępna tylko dla wybranych operatorów ze specjalnymi uprawnieniami, operatorzy bez tych specjalnych uprawnień nie będą mieli możliwości wyciszania alarmów
* Oprogramowanie musi posiadać funkcję potwierdzania zdarzeń alarmowych oraz innych zdarzeń z możliwością wprowadzania komentarzy
* Liczba nieobsłużonych alarmów powinna być widoczna w każdym momencie pracy z oprogramowaniem niezależnie od wyświetlanego okna
* Po wystąpieniu alarmu na drzwiach, czujkach oraz w strefach system musi umożliwiać łatwe i szybkie przejście do mapy wizualizacji gdzie znajduje się element generujący alarm, bezpośrednie przejście do odpowiedniej mapy wizualizacji musi być możliwe z wyskakującego okna z alarmem oraz z listy zdarzeń (np. po kliknięciu prawym przyciskiem myszy na zdarzenie alarmowe)
* System musi umożliwiać przypisywanie priorytetów różnym typom alarmów, wyższy priorytet powoduje występowanie zdarzenia alarmowego wyżej na liście, w ten sposób można osiągnąć pożądaną gradacje ważności zdarzeń alarmowych
* System musi umożliwiać routing zdarzeń alarmowych na wybrane stacje robocze systemu, dla każdego typu alarmu taki routing może być inny, routing pozwala na transferowanie zdarzenia na wybrane stacje po określonym czasie jeżeli alarm nie został potwierdzony na stacji roboczej
* Oprogramowanie musi umożliwiać utworzenie co najmniej 100 map wizualizacji
* Mapy wizualizacji zawierać mają wszystkie drzwi objęte kontrolą dostępu, czujki alarmowe, strefy
* Widok mapy wizualizacji powinien zawierać:
  + Graficzną reprezentację piętra z zaznaczonymi drzwiami, czujkami i strefami SSWiN
  + Elementy na mapie powinny pokazywać swój aktualny stan dla drzwi, czujek, stref i problemów
  + Widok musi zawierać listę elementów na mapie z opisaniem stanów poszczególnych elementów
  + System musi mieć możliwość wskazania gdzie znajduje się element na mapie (np. poprzez kliknięcie prawym przyciskiem myszy na elemencie na liście i wybraniu odpowiedniej funkcji z podręcznego menu – wówczas element na mapie zaczyna migać)
  + Widok musi zawierać listę zdarzeń ale tylko dla elementów znajdujących się na danej mapie wizualizacji, jednocześnie musi być możliwość wyświetlania pełnej listy zdarzeń bez wyłączania widoku mapy wizualizacji
  + Mapy wizualizacji muszą umożliwiać oddalania i zbliżania widoku, powinien być również dostępny przycisk pozwalający na szybkie ustalenie widoku 100% mapy
* Oprogramowanie musi umożliwiać przypisywanie map wizualizacji do elementów, które znajdują się na tych mapach, w szczególności do drzwi, czujek i stref
* Mapy wizualizacji musza mieć możliwość pokazywania temperatury i wilgotności w pomieszczeniach gdzie te parametry są mierzone
* Na mapach wizualizacji musi być możliwość umieszczania napięć i prądów pobieranych z zasilaczy
* System musi umożliwiać budowanie dowolnej ilości widoków, które będą zawierały różne elementy systemu. Widok będzie pozwalał na podział okna aplikacji na maksymalnie 16 pól. W każdym z pól będzie można wyświetlać:
  + Listy statusów urządzeń (np. statusy wybranych drzwi, wejść alarmowych, stref)
  + Mapy wizualizacji
  + Kamery CCTV
  + Zdarzenia (wybrane wg filtrów lub wszystkie)
  + Zmienne (np. temperatura, wilgotność, prądy i napięcia zasilaczy, ilości wejść, wyjść, itp.)
  + Strony www
  + Raporty ewakuacyjne
* Oprogramowanie powinno umożliwiać rozbudowę systemu o dodatkowe przejścia KD, czujniki alarmowe, strefy, wyjścia sterujące, itp do nielimitowanej ilości, ważnym aspektem oprogramowania jest możliwość zarządzania w przyszłości poprzez sieć Ethernet lokalnymi oddziałami organizacji, tak aby można było utworzyć jeden globalny system zarządzania bezpieczeństwem i dostępem do poszczególnych obiektów organizacji
* Łączność pomiędzy lokalizacjami (kontrolerami) a oprogramowaniem za pomocą połączenia Ethernet TCP/IP
* Oprogramowanie musi umożliwiać odłączanie okien od głównej aplikacji, tak aby raz zalogowany użytkownik mógł na kilku monitorach wyświetlić różne okna aplikacji (np. monitor 1 – mapa wizualizacji, monitor 2 – lista użytkowników, monitor 3 – lista zdarzeń na żywo)
* System musi umożliwiać ustawienie dwóch różnych czasów otwarcia dla każdych drzwi, jeden z czasów (np. 5 sekund) dotyczy większości użytkowników, drugi czas (np. 30 sekund) dotyczy użytkowników niepełnosprawnych

# Urządzenia i topologia systemu

Dobór urządzeń i topologia systemu do ustalenia. Poniżej podaję tylko przykłady.

## 3.4 ZINTEGROWANY KONTROLER SYSTEMOWY

Zintegrowany Kontroler Systemowy jest jednostką centralą odpowiedzialną za system alarmowy oraz kontrolę dostępu. Cechą charakterystyczną Zintegrowanego Kontrolera jest **pełna funkcjonalność off-line**: wszystkie zaprogramowane funkcje (łącznie z integracją w obrębie modułów systemowych jak i z wieloma systemami zewnętrznymi) są realizowane bez udziału serwera. Kontrolery główne pomiędzy budynkami muszą wymieniać między sobą informacje niezależnie od działań użytkowników. Musi być możliwość sterowania dowolnym wyjściem PGM i drzwiami poprzez stan dowolnego wejścia alarmowego czy strefy w obrębie całego systemu.

* Wbudowany port TCP/IP 10/100 Ethernet
* Komunikacja z innymi modułami systemowymi za pomocą sieci LAN, WAN, sieci korporacyjnej i szyfrowanej magistrali RS485
* Wbudowany dialer telefoniczny (Contact ID, SIA)
* Zawansowany, 32bitowy procesor w RISC, 2GB RAM
* Szyfrowanie AES 256 Bit
* 8 wejść
* 1 wyjście wysokoprądowe monitorowane, 2 wyjścia przekaźnikowe oraz 4 wyjścia niskoprądowe
* Możliwość aktualizacji oprogramowania za pomocą standardowych technologii IT, FTP
* Szyfrowana magistrala do modułów systemu, używająca komunikacji RS-485, z optyczną izolacją od sieci 230V ( w tym od transformatorów)
* 2 x port Wiegand i RS485 do podłączenia czytników kontroli dostępu, każdy port obsługuje jedno przejście jedno- lub dwustronne
* Funkcje programowalne
* Wirtualizacja elementów
* Realizacja wszystkich funkcji systemowych offline (bez połączenia z serwerem)

## KONTROLER PRZEJŚĆ

Kontroler przejść w obudowie DIN rozszerza funkcjonalność Zintegrowanego Kontrolera Systemowego o obsługę dodatkowych 2 przejść kontroli dostępu. Pozwala na podłączenie do 4 czytników w konfiguracji 2 przejść dwustronnych lub 2 czytników w konfiguracji 2 przejść jednostronnych.

* Obsługa 2 czytników w trybie przejść jednostronnych lub 4 czytników w trybie 2 przejść dwustronnych
* 3 wyjścia na każdy port czytnika do kontroli diody czerwonej, zielonej i buzzera
* Wsparcie dla technologii inteligentnej kontroli sabotaży czytnika, system monitoruje obecność czytnika za pomocą specjalnego protokołu
* Wskaźniki informacyjne pokazujące otrzymywanie danych na portach czytników
* Monitorowane i zabezpieczone wyjście zasilania czytników
* Obudowa przemysłowa dedykowana do montażu na szynę DIN
* Urządzenie w sposób jasny i przejrzysty powinno pokazywać stan wejść (naruszenie, stan bezpieczny, sabotaż i zwarcie/awaria) np. za pomocą wskaźników LED wyprowadzonych na obudowę urządzenia
* Urządzenie powinno posiadać kostki zaciskowe zdejmowane z urządzenia, co ułatwi serwisowanie i konserwację
* Obsługa czytników Wiegand oraz ICT RS485, które ofertują bezpieczne szyfrowane połączenie

## CZYTNIK KART ZBLIŻENIOWYCH

Czytniki kart zbliżeniowych bezpiecznej technologii DESFire MIFARE EV1 i EV2. Wejścia sterowania dualną diodą LED oraz buzzerem pozwalają na integrację tego czytnika w różnych instalacjach, nowych i już istniejących. Urządzenie powinno posiadać możliwość konfiguracji parametrów pracy takich jak klucz szyfrujący oraz sektor pamięci w którym on się znajduje.

Za pomocą czytników KD powinno być możliwe uzbrojenie oraz rozbrojenie stref (uzbrojenie po dwukrotnym lub trzykrotnym przyłożeniu karty do czytnika). Musi istnieć możliwość otwarcia drzwi KD na stałe i ich zamknięcia poprzez przyłożenie podwójnie karty do czytnika. Są to funkcje systemu nie czytnika.

* Podłączenie czytnika za pomocą interfejsu RS485 lub Wiegand
* Dwukolorowa dioda LED (czerwona i niebieska) z niezależnym lub pojedynczym sterowaniem.
* Programowalne formaty danych Wiegand od 26 bitów do 128 bitów, RS485
* Transmisja sygnału obecności co 30 sekund dla inteligentnego zarządzania detekcją sabotażu.
* Szczelna obudowa pozwala na pracę wewnątrz i na zewnątrz budynków. Wymagana klasa IP65.
* Buzzer nie przerywa operacji odczytu.
* Szerokie możliwości programowania za pomocą komputera
* Możliwość określania (ograniczania i rozszerzania) odczytywanych formatów
* Możliwość własnoręcznego definiowania sektorów pamięci z kluczami zabezpieczającymi
* Czytniki powinny być dostępne z klawiaturą PIN lub bez
* Czytniki dostępne w kolorze białym lub czarnym

Wymagana obsługa następujących formatów kart:

- HID - 125KHz – aktualnie używane

- DESFire:

* DESFire MIFARE EV1 lub EV2

- MIFARE:

* Secured Mifare – karty zabezpieczone kluczem AES256 bit
* Sector – odczyt zawartości sektora pamięć karty MIFARE, możliwość zabezpieczenia
* CSN – numer seryjny
* CSN Reversed – odwrócony nr seryjny

Zaleca się wymianę używanego standardu kart na format szyfrowany i zabezpieczony typu DESFire MIFARE EV1 lub Secured Mifare (karty zabezpieczone kluczem AES256 bit).

Aby umożliwić inwestorowi stopniową wymianę kart na karty bezpieczne projektuje się czytnik który jednocześnie obsługuje standard nie zabezpieczony MIFARE CSN jak i standard wysokiego bezpieczeństwa DESFire MIFARE EV1 (szyfrowany).

UWAGA: Ze względu na znaczne odległości w niektórych miejscach projektowanego systemu, odległość pomiędzy czytnikiem a jego kontrolerem może przekraczać 150m (maksymalna odległość dla standardu WIEGAND). Z tego względu zastosowane czytniki muszą umożliwiać podłączanie na kablach o długości znacznie przekraczającej 150m (STANDARD RS485).

Z powodu podniesienia poziomu bezpieczeństwa czytniki muszą być podłączone do kontrolerów za pomocą szyfrowanego interfejsu (np. RS485).

## INTELIGENTNY ZASILACZ SYSTEMOWY 2A/4A/8A

Inteligentny zasilacz systemowy wersja DIN 12VDC/2A lub DIN 12VDC/4A lub 12VDC/8A dostarcza zasilanie dla urządzeń kontroli dostępu, systemu alarmowego, elementów automatyki oraz dużej liczby modułów systemu (SKD). Zasilacz jest zaprojektowany w standardowej obudowie pozwalającej na łatwy montaż na szynie DIN. Zasilacze 4A i 8A nie wymagają transformatora i są bezpośrednio przyłączane do sieci 230VAC. Zasilacz 2A do prawidłowej pracy wymaga transformatora TOR80VA/16V.  
Dwa wyjścia przekaźnikowe Form B, które mogą być wykorzystane jako standardowe wyjścia programowalne. Inteligentne algorytmy ładowania i monitorowania baterii oraz zasilania AC. Komunikacja z systemem za pośrednictwem magistrali RS-485.   
Inteligentne źródło zasilania w kontrolerach powinno raportować (w czasie rzeczywistym) do systemu następujące problemy:

- brak zasilania AC

- słaba bateria

- błąd zasilania wyjściowego dla urządzeń zewnętrznych (czytniki, czujki, elektro zaczepy)

- przeciążenia wyjścia

Zasilacze dedykowane do zasilania kontrolerów głównych i magistrali systemowej będą monitorowane w systemie również w sposób analogowy. System powinien pokazywać następujące informacje na temat tych zasilaczy:

* wartość napięć na wyjściach
* wartość napięcia baterii
* całkowity pobór prądu z zasilacza
* przeciążenie wyjścia
* przekroczenie temperatury pracy urządzenia

Sygnały te maja być przesyłane do systemu przez magistralę systemową a nie przez wyjścia zasilacza. Każda z w/w informacji służy do monitorowania warunków pracy urządzeń. Przekroczenie założonych lub dopuszczalnych parametrów powoduje wystąpienie alarmu w systemie.

## KONTROLER 8 WYJŚĆ PRZEKAŹNIKOWYCH

Rozszerza liczbę wyjść dostępnych w systemie o 8 wyjść z przekaźnikami typu Form-C. 8 wyjść z przekaźnikiem typu Form-C. Kontrolery te służą do sterowania windą.

* Wskaźniki LED pokazujący stan przekaźników
* Wskaźnik LED pokazujący status urządzenia

## KONTROLER 16 WEJŚĆ IZOLOWANYCH

Rozszerza liczbę wejść dostępnych w systemie o 16 wejść izolowanych. Kontrolery te służą do sterowania windą.

* Wskaźnik LED pokazujący stan przekaźników
* Wskaźnik LED pokazujący status urządzenia
* 16 wejść izolowanych

## STEROWANIE WINDĄ

System pozwala na integrację typu HLI (High Level Interface) z systemami windowymi OTIS, KONE, SCHNDLER, Thyssen Krupp oraz MCE (Motion Control Engineering).

Uprawnienia użytkowników do poszczególnych kabin windowych i pięter są ustawiane w systemie PROTEGE. Następnie kontroler PROTEGE przesyła w trybie online te ustawienia do systemu windowego (do kontrolera wind lub serwera systemu windowego w zależności od systemu). Wówczas uprawnienia użytkownika są analizowane w systemie windowym po jego identyfikacji na panelu wyboru piętra.

## SERWER

Oprogramowanie serwerowe PROTEGE może być zainstalowane na komputerze lub maszynie wirtualnej. Serwer odpowiedzialny jest za programowanie systemu, wysyłanie aktualnych ustawień do kontrolerów w trybie rzeczywistym oraz za zbieranie i logowanie zdarzeń w bazie danych Microsoft SQL.

## STACJA ROBOCZA

Aplikacja interfejsu użytkownika może być zainstalowana na dowolnej ilości komputerów. Ilość jednocześnie zalogowanych do systemu operatorów zależna jest od ilości posiadanych licencji klienckich oraz od wydajności maszyny serwerowej.

**Niezawodność pracy systemu**

Ze względu na konieczność zapewnienia ciągłej pracy systemu i orientację na minimalizację możliwych punktów awarii proponowany system powinien realizować wszystkie lub większość zaprogramowanych funkcji na **kontrolerach sprzętowych, a nie na serwerze**. Nie dotyczy to wizualizacji systemu i jego programowania, a także generowania raportów. Wszystkie funkcje związane z kontrolą dostępu, systemem alarmowym, oraz integracją pomiędzy tymi systemami a także integracją z systemami zewnętrznymi powinny być realizowane na kontrolerach głównych systemu (SKD).

Wszystkie funkcje związane z dostępem do konkretnych drzwi KD powinny być realizowane przez dedykowane dla danych drzwi kontrolery, które w przypadku braku komunikacji z kontrolerem nadrzędnym (głównym) będą w stanie zapewnić prawidłowe funkcjonowanie przejścia (w ramach możliwych do zapamiętania ilości użytkowników). Dzięki takiemu rozwiązaniu funkcjonowanie systemu będzie niezależne od sprawności połączeń sieciowych, magistrali RS485, działania serwerów i komputerów monitorujących system. System musi umożliwiać lokalny (w ramach jednego kontrolera głównego/centrali) i globalny anty-passback (w ramach wszystkich kontrolerów i central w systemie). Błąd APB użytkownika musi być możliwy do skasowania poprzez oprogramowanie lub po upłynięciu czasu oraz na zadziałanie harmonogramu. Do każdego użytkownika powinna być możliwość przypisania co najmniej 100 poziomów dostępu. Urządzenia systemu muszą w łatwy sposób pokazywać stan wejść i wyjść, np. za pomocą ikon diodowych na urządzeniach – tak aby po otwarciu obudowy konserwator w łatwy sposób mógł widzieć w jakim stanie jest dane urządzenie.

## KOMUNIKACJA URZĄDZEŃ W SYSTEMIE

**TCP/IP:**

* Główne kontrolery systemowe do serwera
* Komputery klienckie do serwera systemu
* Ewentualne inne zewnętrzne systemy zintegrowane do kontrolerów głównych

**RS485:**

* Kontrolery przejść, klawiatury alarmowe, ekspandery wejść i wyjść do kontrolerów głównych, czytniki

UWAGA:

Do zasilania portów komunikacyjnych oraz magistrali RS485 powinno być dedykowane osobne inteligentne źródło zasilania z pełnym monitoringiem parametrów pracy w sposób analogowy (wartości napięć i prądów) oraz cyfrowy (komunikaty o problemach i awariach).