**Ogólna koncepcja systemu**

Podstawowym urządzeniem systemu jest strefowy kontroler dostępu. Kontroler ten w podstawowej wersji może obsłużyć 1 przejście dwustronne. Po dołączeniu modułów zewnętrznych, kontroler ten może dozorować do 16 przejść dwustronnych. Moduły rozszerzeń są dołączane do kontrolera za pośrednictwem magistrali RS485. Magistrala ta może tworzyć strukturę gwiazdy i mieć długość do 1200 m, licząc od kontrolera do najbardziej odległego modułu. Kontroler może również współpracować z urządzeniami podłączonymi do sieci komputerowej, który pełni rolę interfejsu komunikacyjnego do urządzeń sieciowych.

Przesyłanie ustawień do kontrolerów jest realizowane w tle i nie zatrzymuje bieżącej pracy systemu. Czas przesyłania ustawień zwykle nie przekracza 1 minuty na każdy tysiąc aktywnych użytkowników systemu. Po zakończeniu przesyłania następuje przełączenie systemu na nowe ustawienia, w trakcie, którego system wstrzymuje pracę na kilka sekund.

System umożliwia zarządzanie użytkownikami w trybie online. W trybie tym, aktualizacja danych użytkownika następuje natychmiast po wykonaniu zmian w bazie danych systemu. Przesyłanie zaktualizowanych danych użytkownika nie zatrzymuje działania systemu i zwykle zajmuje kilka sekund. Zdarzenia zarejestrowane w systemie są na bieżąco pobierane z kontrolerów i zapisywane w bazie danych systemu. Pobieranie zdarzeń następuje automatycznie przez serwer komunikacyjny systemu i nie wymaga działania aplikacji zarządzającej systemem.

W przypadku braku połączenia z serwerem komunikacyjnym, kontrolery zapisują zdarzenia w swoich wewnętrznych buforach pamięci. Zasoby sprzętowe kontrolera dostępu mogą być rozszerzane przez dołączanie zewnętrznych modułów i urządzeń. Zewnętrzne zasoby sprzętowe mogą być wykorzystywane wg tych samych zasad, co zasoby płyty głównej kontrolera. Lokalizacja obiektu (linii wejściowej, linii wyjściowej, czytnika itd.), jak i jego rodzaj (typ linii wejściowej, typ linii wyjściowej, typ czytnika) nie mają wpływu na funkcję logiczną, jaką można powiązać z danym obiektem fizycznym.

Oprogramowanie do kontroli dostępu w zależności od wersji powinno umożliwiać tworzenia partycji, czyli logicznych podsystemów zarządzanych przez dedykowanych operatorów oraz umożliwiać integrację z systemami zewnętrznymi poprzez dedykowane API.

**Kontroler**

W zależności od wersji, kontroler umożliwia obsługę do 16 przejść kontrolowanych dwustronnie oraz 32 węzłów automatyki. Koncepcja integracji z systemem alarmowym umożliwia prezentację stanu strefy alarmowej oraz sterowanie jej stanem bezpośrednio z poziomu terminali dostępu. Kontroler udostępnia zaawansowany, a jednocześnie bardzo wydajny sposób zarządzania użytkownikami systemu oraz kształtowania ich uprawnień. Proces konfiguracji kontrolerów systemu jest realizowany współbieżnie, a ilość kontrolerów w systemie nie wpływa na czas jego konfiguracji, który zwykle kończy się przed upływem 1 minuty. Kontroler zarządzany jest z aplikacji narzędziowej, która umożliwia współpracę z serwerową bazą danych Microsoft SQL Server. Zarządzanie systemem może być realizowane z poziomu wielu stacji roboczych z programem narzędziowym przez operatorów o różnym poziomie uprawnień. System udostępnia integrację programową umożliwiającą swobodny dostęp do logu zdarzeń systemu jak i zarządzanie jego użytkownikami. Komunikacja z komputerem zarządzającym jest realizowana za pośrednictwem sieci LAN/WAN z protokołem szyfrowanym metodą AES128 CBC. Pamięć kontrolera pozwala na buforowanie do 8 milionów zdarzeń na wypadek utraty połączenia z bazą danych.

**Terminal dostępu**

Czytnik jest terminalem identyfikacji przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej. Terminal umożliwia w zależności od wersji rozpoznawanie użytkowników za pośrednictwem kart zbliżeniowych standardu 13,56 MHz MIFARE® Ultralight/Classic/DESFire/PLUS (wykorzystując również wartości nośników zapisane w szyfrowanych sektorach SSN) oraz technologii BLE/NFC.

Terminal w zależności od wersji może być instalowany na zewnątrz budynków bez konieczności stosowania dodatkowych zabezpieczeń.

**Bezpieczeństwo w systemie**

System w zależności od wersji oferuje wysoki, wielopoziomowy system bezpieczeństwa, na który składają się:

* Zastosowanie kart standardu MIFARE® z programowalnym numerem zapisanym w szyfrowanych sektorach karty (SSN - Secure Sector Number).
* Obsługa kart MIFARE® DESFire® i MIFARE Plus® oraz technologii mobilnej NFC/BLE.
* Obsługa czytników biometrycznych.
* Złożone tryby identyfikacji wymagające użycia kombinacji identyfikatorów (np. karta + PIN, karta + biometria + PIN itp.).
* Komunikacja w sieci LAN/WAN szyfrowana metodą AES128 z dynamicznie zmienianym kluczem szyfrującym (CBC).
* Szyfrowana komunikacja z terminalami dostępu i ekspanderami dołączonymi do magistrali RS485.
* Autoryzacja zewnętrzna - umożliwiająca uzależnienie zgody na dostęp na konkretnym punkcie identyfikacji od decyzji zewnętrznej. Decyzja ta może być wydana przez operatora monitorującego system lub z poziomu dedykowanego do tego celu punktu identyfikacji (czytnika).
* Możliwość wizualizowania w module map oprogramowania zarządzającego zintegrowanych systemów bezpieczeństwa (KD, CCTV, SSWiN, SSP) oraz elementów automatyki budynkowej.
* Integracja bazodanowa z wybranymi systemami dystrybucji i monitorowania obiegu kluczy z funkcjonalnością blokowania dostępu uzależnioną od zdeponowania kluczy w depozytorze.
* Integracja z systemami włamaniu i napadu z funkcjonalnością blokowania dostępu do pomieszczeń z uzbrojoną strefą alarmową.
* Wielopoziomowy dostęp do oprogramowania zarządzającego z rejestracją działań operatorów

**Przykładowe funkcje systemu**

Kontrola dostępu do pomieszczeń

Głównym zadaniem systemu jest realizacja fizycznej kontroli dostępu do pomieszczeń. System w zależności od wersji jest skalowalny i umożliwia obsługę nieograniczonej ilości przejść. Przejścia mogą być kontrolowane jedno lub dwustronnie. Ilość użytkowników systemu nie jest ograniczona. Ograniczeniu podlega ilość użytkowników na poszczególnych kontrolerach dostępu. System przesyła do kontrolera tylko tych użytkowników, którzy posiadają uprawnienie do wykonania jakiejkolwiek akcji na danym kontrolerze.

Raportowanie czasu obecności

System rejestruje zdarzenia związane z ruchem użytkowników na terenie objętym elektroniczną kontrolą dostępu. Rejestr zdarzeń może być wykorzystany do analizy czasu przebywania użytkowników w poszczególnych częściach dozorowanego obiektu. Program narzędziowy umożliwia wyznaczenie czasu przebywania użytkowników w dowolnie zdefiniowanych obszarach systemu (tzw. strefy obecności) i w dowolnym zakresie czasowym. Raportowanie czasu obecności osób może odbywać się przez sumowanie cząstkowych czasów przebywania w określonym obszarze lub jako czas, który upłynął od momentu pierwszego wejścia aż do momentu ostatniego wyjścia z obszaru w ramach tego samego dnia.

Integracja z telewizją przemysłową

W ramach integracji z telewizją przemysłową CCTV system udostępnia możliwość pobrania i odtworzenia filmu lub zdjęcia zarejestrowanego przez kamerę skojarzoną z danym typem zdarzenia oraz miejscem jego wystąpienia. Opcjonalnie, film lub zdjęcie pobrane z rejestratora może zostać zachowane w bazie danych systemu. Podgląd z kamer może odbywać się w osobnym oknie programu zadokowanym na dodatkowym monitorze. Okno z podglądem kamery może się automatycznie przełączać na tą kamerę, która jest skojarzona z ostatnio zarejestrowanym zdarzeniem.

Awaryjne sterowanie przejściem

System umożliwia zarówno otwarcie jak i zablokowanie dowolnej grupy przejść w trybie awaryjnym. Tryb ten ma najwyższy priorytet i nie może być zmieniony przez żaden inny dostępny w systemie mechanizm z wyjątkiem dedykowanej do tego celu funkcji kasującej tryb awaryjny. Sterowanie trybem awaryjnym przejścia może być realizowane zarówno lokalnie z poziomu urządzeń systemu, jaki i zdalnie z programu narzędziowy.

Rejestracja zdarzeń

Zdarzenia, które wystąpiły w systemie są na bieżąco ściągane z kontrolerów i zapisywane w bazie danych systemu. Proces ściągania jest realizowany przez Serwer komunikacyjny, który jest usługą systemu operacyjnego Windows i nie wymaga uruchomienia programu narzędziowego zarządzającego systemem. W przypadku, gdy połączenie z kontrolerem jest nieosiągalne, zdarzenia są rejestrowane w wewnętrznym buforze zdarzeń kontrolera i są pobierane automatycznie po przywróceniu komunikacji.

Powiadamianie o wystąpieniu zdarzenia

Wystąpienie dowolnego zdarzenia może automatycznie uruchamiać akcję powiadomienia. Powiadomienie może odbywać się przez wyświetlenie komunikatu na ekranie monitora, wysłanie wiadomości email lub wysłanie pakietów danych przy pomocy protokołu TCP pod zdefiniowany adres sieciowy. Korzystając z uniwersalnego mechanizmu filtru zdarzeń można określić dodatkowe warunki (m.in. czas i miejsce wystąpienia zdarzenia), które muszą wystąpić, aby system wykonał powiadomienie. Powiadamianie protokołem TCP może być użyte to integracji programowej z innymi rodzajami programów (np. BMS).

Monitorowanie zdarzeń

Zdarzenia, które wystąpiły w systemie mogą być na bieżąco wyświetlane w oknach Monitorowania online. Każde z okien może być skonfigurowane do wyświetlania wybranej grupy zdarzeń i dokowane na dodatkowych monitorach.

Monitorowanie obecności

System umożliwia monitorowanie osób zalogowanych w dowolnie zdefiniowanych obszarach systemu. Możliwe jest monitorowanie wielu obszarów jednocześnie. W szczególnym przypadku monitor obecności może być użyty w celu prezentacji listy osób, które zarejestrowały się na wybranym punkcie dostępu w następstwie ogłoszenia ewakuacji budynku.

Monitorowanie przejść

System umożliwia monitorowanie wybranych przejść i podgląd zdarzeń, które na nich wystąpiły. W momencie wystąpienia zdarzenia system może automatycznie wyświetlić podgląd z kamery CCTV skojarzonej z miejscem wystąpienia zdarzenia lub zdjęcie osoby, która została zarejestrowana na tym miejscu.

Mapy

W systemie w zależności od wersji można tworzyć wizualizację zintegrowanych systemów bezpieczeństwa (KD, CCTV, SSWiN, SSP) oraz elementów automatyki budynkowej. Na dowolnych podkładach graficznych w procesie konfiguracji można nanosić symbole reprezentujące wybrane elementy ww. systemów, którymi na etapie użytkowania możemy, w odpowiednim dla nich zakresie, sterować.

Harmonogramy

Harmonogramy umożliwiają uzależnienie działania systemu od konkretnego dnia tygodnia i pory dnia. Harmonogramy mogą być wykorzystane przy konfigurowaniu działania wielu funkcji systemu, a w szczególności uprawnień dostępu. Stan harmonogramu może być prezentowany na linii wyjściowej i umożliwić w ten sposób sprzętowe uzależnienie działania systemu od dnia tygodnia i pory dnia.

Uprawnienia

W systemie wykonanie dowolnej akcji może być uwarunkowane wymogiem posiadania właściwego Uprawnienia. Uprawnienie określa, kiedy i gdzie dana akcja (funkcja) może być wykonana. Uprawnienia mogą być przypisywane bezpośrednio do Identyfikatora, Użytkownika lub Grupy użytkowników. Uprawnienia przypisane do Grupy dostępu przechodzą automatycznie na wszystkich Użytkowników należących do danej Grupy. Uprawnienia przypisane do Identyfikatora automatycznie przechodzą na Użytkownika, do którego dany Identyfikator należy.

Szczególne w zależności od wersji cechy systemu kontroli dostępu:

* możliwość definiowania wielofunkcyjnych linii wejściowych,
* możliwość definiowania wielofunkcyjnych linii wyjściowych (z możliwością ustawienia priorytetu dla funkcji),
* możliwość definiowania sposobu modulacji linii wyjściowej,
* możliwość zastosowania czytników obsługujących standard BLE, NFC, QR podłączanych do kontrolera po szyfrowanej magistrali RS485,
* definiowanie własnych złożonych trybów identyfikacji,
* logowanie zwykłe, specjalne (np. długie przyłożenie karty), podwójne; na jednym punkcie identyfikacji możliwość wywoływania wielu funkcji,
* programowa (po protokole) integracja z windami KONE (DCS, Kone Access), Otis (Compas), Schindler (PORT),
* integracja z ActiveDirectory, AssaAbloy Aperio, Milestone, Galaxy, Satel
* komendy globalne wywoływane: dowolnym zdarzeniem w systemie lub komendą ze stacji roboczej,
* autoryzacja zewnętrzna (potwierdzenie tożsamości na ekranie Ochrony),
* integracja bazodanowa z wybranymi systemami dystrybucji i monitorowania obiegu kluczy,
* integracja bazodanowa z wybranymi systemami rejestracji czasu pracy.