KARTA INFORMACYJNA



Opis platformy integrującej – Argus PSIM

Spis treści

1. Opis ogólny 3
2. Wymagania sprzętowe i programowe 3
2.1 Serwer aplikacyjny i bazy danych 4
2.2 Oprogramowanie serwera 4
2.3 Stanowisko operatora 5
2.4 Wymagania sieciowe 5
2.5 System operacyjny: Windows i Linux 5
3. Architektura systemu 6
3.1 Baza ruchowa i baza edycyjna 7
3.2 Wysoka dostępność 7
3.3 Bezpieczeństwo 7
4. Interfejs użytkownika 7
5. Możliwości – moduły funkcjonalne 8
5.1 Panel główny 8
5.2 Moduł map 8
5.3 Moduł dziennika 9
5.4 Moduł procedur 10
5.5 Moduł raportów 10
5.6 Moduł terminarza 11
5.7 Moduł harmonogramów 11
5.8 Moduł warunków i automatyki 11
5.9 Moduł CCTV 11
5.10 Moduł komunikacji: SMS, VoIP, e-mail 11
5.11 Moduł dziennika służby 12
5.12 Moduł wykresów i pomiarów 12
5.13 Moduł ochrony antydronowej i radarowej 12
5.14 Widok syntetyczny (C2) 12
5.15 Moduł administratora 13
6. Integracje – Argus.Drivers 13

1. Opis ogólny

Platforma integrująca Argus PSIM jest głównym elementem rozbudowanej rodziny produktów Argus. Należy do klasy systemów PSIM (Physical Security Information Management): łączy w jednym miejscu systemy ochrony technicznej obiektu, takie jak sygnalizacja włamania i napadu, kontrola dostępu, sygnalizacja pożaru, telewizja dozorowa, ochrona obwodowa, systemy antydronowe czy automatyka budynkowa, i pozwala nimi zarządzać z poziomu jednej, spójnej aplikacji.

Przejrzysty interfejs oraz wysoki poziom ergonomii upraszczają pracę operatorów i pozwalają w krótkim czasie przyswoić obsługę oprogramowania. Aplikacje wyróżnia ciemny motyw kolorów, który w znaczny sposób podnosi komfort długotrwałej pracy w centrum nadzoru.

Platforma Argus PSIM, podobnie jak pozostałe produkty z rodziny Argus, została zaprojektowana i opracowana w całości przez polskich inżynierów, specjalizujących się w programowaniu w języku C# na platformie .NET. Aktualna wersja korzysta z nowoczesnych (.NET 8 i .NET 9), wspieranych przez producenta technologii, co zapewnia wysoką wydajność i bezpieczeństwo.

Platforma składa się z trzech głównych części:

- **Argus.Service** – serwer aplikacyjny, rdzeń systemu. Gromadzi i przetwarza dane z integrowanych urządzeń, uruchamia procedury, warunki i harmonogramy oraz udostępnia dane stanowiskom operatorskim.
- **Argus.Client** – aplikacja operatora dostępna w wersji desktop (Windows) oraz w przeglądarce internetowej. Obie wersje korzystają z tej samej biblioteki interfejsu, dzięki czemu wyglądają i działają identycznie.
- **Argus.Drivers** – zestaw sterowników integracyjnych (ok. 50 integracji), które zapewniają komunikację z centralami i urządzeniami różnych producentów oraz przekształcają ich sygnały na jednolity język systemu.

2. Wymagania sprzętowe i programowe

Wymagania zależą od wielkości instalacji: liczby integrowanych urządzeń i sygnałów, liczby kamer i stanowisk operatorskich, natężenia ruchu zdarzeń oraz wymaganego okresu przechowywania historii. Konfiguracja minimalna jest przeznaczona dla obiektów małych i średnich. Konfiguracja optymalna zapewnia zapas wydajności dla obiektów dużych, rozproszonych, z wieloma stanowiskami i intensywnym ruchem zdarzeń (setki zdarzeń na minutę) oraz długą retencją danych. Ostateczny dobór sprzętu jest ustalany na etapie projektu.

2.1 Serwer aplikacyjny i bazy danych

Parametr	Minimalne	Optymalne
Procesor	8 rdzeni fizycznych, 2,4 GHz (klasa Intel Xeon Silver lub AMD EPYC)	16 rdzeni fizycznych lub więcej, min. 2,8 GHz (aktualna generacja Intel Xeon Silver/Gold lub AMD EPYC)
Pamięć RAM	32 GB	64 GB lub więcej
Dysk systemowy	2 × SSD 480 GB w RAID 1	2 × SSD NVMe 960 GB w RAID 1
Dysk bazy danych	SSD 1 TB (może być wspólny z systemowym)	Osobny wolumen SSD NVMe 2–4 TB w RAID 1 lub RAID 10
Dysk archiwum (kopie zapasowe, załączniki, eksport nagrań)	2 TB	4 TB lub więcej, osobny wolumen lub zasób NAS
Interfejsy sieciowe	2 × 1 Gb Ethernet	4 × 1 Gb Ethernet lub 2 × 10 Gb Ethernet (rozdzielenie sieci urządzeń i sieci operatorów)
Zasilanie	Zasilacz 230 VAC, zasilanie gwarantowane (UPS)	Redundantne zasilacze 230 VAC, UPS
Redundancja	Brak	Drugi serwer

Serwer może być maszyną fizyczną lub wirtualną (np. VMware vSphere, Microsoft Hyper-V, Proxmox). W przypadku maszyny wirtualnej należy zagwarantować zarezerwowane zasoby procesora i pamięci oraz szybką macierz dyskową. W dużych instalacjach zaleca się wydzielenie bazy danych na osobny serwer.

2.2 Oprogramowanie serwera

Element	Minimalne	Optymalne
System operacyjny	Microsoft Windows Server 2019 Standard (64-bit)	Microsoft Windows Server 2022 lub 2025 Standard (64-bit)
Baza danych	PostgreSQL 16 z rozszerzeniem TimescaleDB 2.17	PostgreSQL 17 z rozszerzeniem TimescaleDB 2.19 lub nowszym
Środowisko uruchomieniowe	ASP.NET Core Runtime 8.0, .NET Runtime 6.0 i 8.0, .NET Framework 4.8 (dla części sterowników)	Jak w konfiguracji minimalnej, w najnowszych poprawkach
Komponenty dodatkowe	Brak	Apache Kafka (duże instalacje), serwer zapasowy

2.3 Stanowisko operatora

Parametr	Minimalne	Optymalne
Procesor	4 rdzenie, np. Intel Core i5 (10. generacji lub nowszy)	8 rdzeni lub więcej, np. Intel Core i7 / AMD Ryzen 7
Pamięć RAM	16 GB	32 GB
Dysk	SSD 256 GB	SSD NVMe 512 GB
Karta graficzna	Zintegrowana	Dedykowana karta NVIDIA z min. 4 GB pamięci, z obsługą wielu monitorów
Monitory	1 monitor Full HD	2–4 monitory Full HD lub 4K (np. mapa, kamery, dziennik na osobnych ekranach)
Sieć	1 Gb Ethernet	1 Gb Ethernet
Audio	Głośniki	Głośniki lub zestaw słuchawkowy
System operacyjny	Windows 11 Pro (64-bit) lub Windows 10 Enterprise LTSC 2021	Windows 11 Pro / Enterprise 24H2 (64-bit) lub Windows 11 Enterprise LTSC 2024
Oprogramowanie	.NET 9 Desktop Runtime, Microsoft Edge WebView2 Runtime	Jak w konfiguracji minimalnej

Aplikacja przeglądarkowa nie wymaga instalacji. Obsługiwane są aktualne wersje przeglądarek Google Chrome, Microsoft Edge i Mozilla Firefox. Dla komfortowej pracy zaleca się komputer z min. 8 GB pamięci RAM. Aplikacja przeglądarkowa może być uruchamiana na systemach Windows, Linux i macOS.

2.4 Wymagania sieciowe

- Połączenie stanowisk z serwerem w sieci LAN lub WAN o przepustowości min. 100 Mb/s (zalecane 1 Gb/s).
- Dla podglądu wideo należy przewidzieć ok. 2–8 Mb/s na każdy jednocześnie wyświetlany strumień kamery (zależnie od rozdzielczości i kodeka).
- Komunikacja klient - serwer odbywa się szyfrowanym protokołem HTTPS/WebSocket.
- Sterowniki komunikują się z integrowanymi systemami zgodnie z wymaganiami producentów: TCP/IP, łącza szeregowe RS-232/RS-485 (np. przez konwertery), Modbus, SNMP i inne.

2.5 System operacyjny: Windows i Linux

Zalecanym środowiskiem dla platformy Argus PSIM jest Microsoft Windows Server. Wynika to z faktu, że część producentów systemów zabezpieczeń (m.in. systemów telewizji dozorowej VMS, systemów ochrony obwodowej i niektórych central) udostępnia swoje biblioteki integracyjne (SDK) wyłącznie dla systemu Windows. Na systemie Windows działają również usługi platformy, integracja z usługą Active Directory oraz narzędzia administracyjne.

Serwer aplikacyjny, baza danych oraz sterowniki oparte na otwartych protokołach (np. ONVIF, Modbus TCP, MQTT, SNMP, REST) mogą pracować w systemie Linux (np. Debian 12, Ubuntu Server

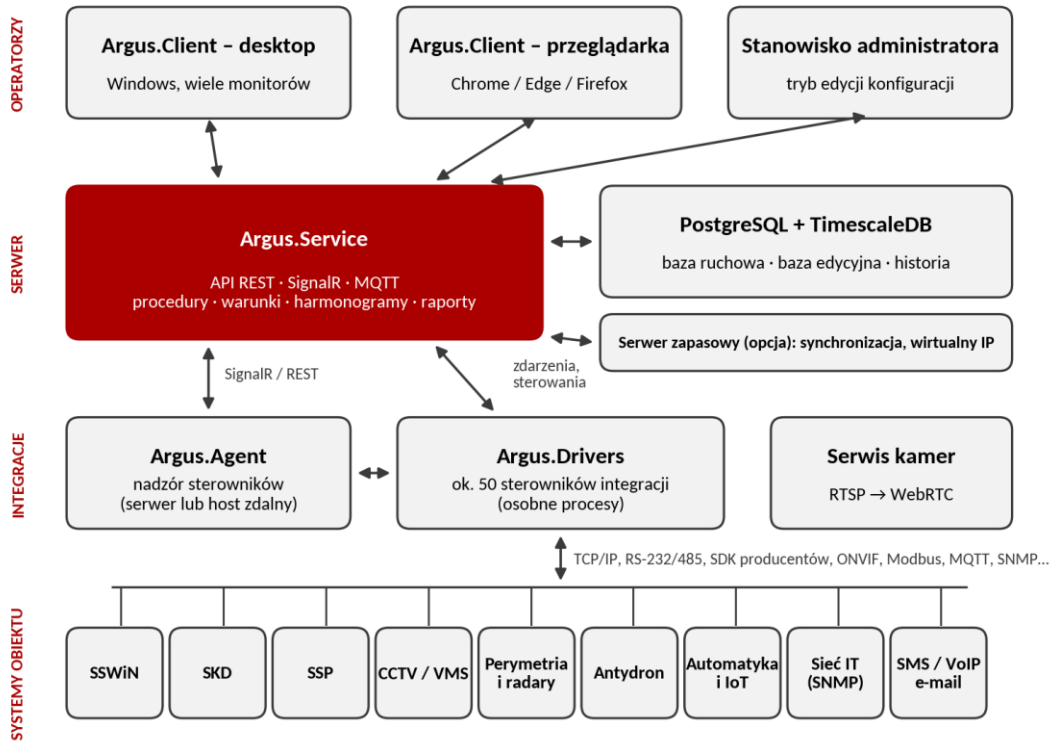
22.04/24.04 LTS). Wdrożenie na Linuksie wymaga jednak dodatkowych prac integracyjnych i jest ustalane indywidualnie dla danego projektu. Możliwe jest też rozwiązanie mieszane: serwer i baza danych na Linuksie, a sterowniki wymagające systemu Windows na osobnym komputerze z usługą.

3. Architektura systemu

Najważniejszym elementem platformy Argus PSIM jest aplikacja serwerowa Argus.Service. Jest to program zainstalowany na fizycznym serwerze lub maszynie wirtualnej, który gromadzi dane spływające z różnych urządzeń, przetwarza je, zapisuje w bazie danych i na żądanie udostępnia stanowiskom operatorskim. Zmiany stanów trafiają do operatorów natychmiast, bez konieczności odświeżania widoku.

Warstwą komunikacyjną pomiędzy aplikacją serwerową, a operatorem jest Argus.Client w wersji desktop lub przeglądarkowej. Dane przechowywane są centralnie w aplikacji serwerowej. Operator w momencie wykrycia zagrożenia zostaje o tym poinformowany odpowiednim wpisem w dzienniku, sygnałem dźwiękowym, oznaczeniem na mapie oraz – w wersji desktop – automatycznym wysunięciem okna aplikacji na pierwszy plan.

Za komunikację z integrowanymi systemami odpowiadają sterowniki (Argus.Drivers), nadzorowane przez usługę Argus.Agent. Agent sprawdza stan sterowników i automatycznie nimi zarządza. Agentów może być wielu – można je instalować na komputerach rozmieszczonych bliżej integrowanych systemów, np. w różnych budynkach, co ogranicza długość połączeń szeregowych i obciążenie sieci.



Rysunek 1. Architektura platformy Argus PSIM

System zbudowano w oparciu o moduły, które można dowolnie włączać i wyłączać dla konkretnego użytkownika. Nie każdy operator musi mieć dostęp do całego systemu. Dodatkowo każdemu operatorowi można przypisać zbiór sygnałów, urządzeń, obszarów, procedur i harmonogramów, które ma nadzorować. Strukturę systemu można podzielić w zależności od typu systemu i przypisać ją różnym operatorom lub podzielić według lokalizacji, np. piętrami.

3.1 Baza ruchowa i baza edycyjna

Argus PSIM posiada dwie bazy danych: ruchową, na której pracują operatorzy, oraz edycyjną do wprowadzania zmian. Administrator może wprowadzać zmiany w systemie bez konieczności wyłączania systemu integrującego. Każda zmiana jest rejestrowana, a przed zatwierdzeniem administrator może ją przejrzeć i w razie potrzeby wycofać. Po zakończonej edycji administrator jednym przyciskiem przesyła zmiany do bazy ruchowej.

Historia zdarzeń, stanów i pomiarów jest przechowywana w tabelach szeregów czasowych (TimescaleDB), co pozwala utrzymywać wieloletnią historię przy zachowaniu szybkiego wyszukiwania i raportowania.

3.2 Wysoka dostępność

W instalacjach o podwyższonych wymaganiach niezawodności, platformę można uruchomić w architekturze wieloserwerowej. Serwery są uszeregowane według priorytetu; serwer główny posiada wirtualny adres IP, pod którym łączą się stanowiska operatorskie i agenci. W razie awarii serwer zapasowy przejmuje ten adres i kontynuuje pracę, a stanowiska automatycznie wznawiają połączenie.

3.3 Bezpieczeństwo

- **Szyfrowana komunikacja** – połączenia klientów, agentów i sterowników z serwerem odbywają się protokołem HTTPS/WSS; certyfikat serwera może być dostarczony przez klienta lub wygenerowany automatycznie.
- **Uwierzytelnianie** – logowanie kontem systemu Argus lub kontem domenowym (Active Directory/LDAP). Grupy z Active Directory mogą być automatycznie synchronizowane z grupami uprawnień systemu.
- **Uprawnienia** – dostęp nadawany do modułów, obszarów, urządzeń, sygnałów, procedur i harmonogramów; dodatkowe potwierdzenie kodem PIN dla wybranych sterowań.
- **Rozliczalność** – rejestr logowań, historia wykonanych sterowań, dziennik audytu i historia zmian konfiguracji.

4. Interfejs użytkownika

Oprogramowanie posiada górny pasek nawigacji z modułami i opcjami dodatkowymi, lewy panel boczny prezentujący na bieżąco liczniki aktywnych stanów urządzeń według priorytetów, obszar centralny, w którym zmienia się zawartość w zależności od wybranego modułu, oraz pasek dolny z informacjami o stanie serwera, stanie licencji, aktualnie zalogowanym użytkowniku i aktualnym czasie.

Kliknięcie w licznik stanów w panelu bocznym otwiera listę zdarzeń przefiltrowaną według wybranego priorytetu.

Na pasku dolnym umieszczono przełącznik, który umożliwia zmianę interfejsu z trybu ruchowego do trybu edycji (dla uprawnionych użytkowników).

Aplikacja desktop obsługuje pracę na wielu monitorach. Każdy użytkownik może przypisać moduły do poszczególnych ekranów, a konfiguracja ta jest przechowywana na serwerze i odtwarzana po zalogowaniu na dowolnym stanowisku. Dostępny jest także tryb pracy z kartami graficznymi NVIDIA łączącymi wiele monitorów w jedną powierzchnię (np. ściany wizyjne). Dla najczęstszych czynności przewidziano skróty klawiszowe, a sygnały alarmowe mogą mieć przypisane własne dźwięki, które operator wycisza jednym przyciskiem.

5. Możliwości – moduły funkcjonalne

Poniżej opisano możliwości, jakie oferuje platforma Argus PSIM, z podziałem na moduły funkcjonalne. Dostępność modułów zależy od licencji oraz uprawnień użytkownika.

5.1 Panel główny

Każdy z użytkowników ma dostęp do panelu głównego, który może spersonalizować w wygodny dla siebie sposób. Panel składa się z widżetów, które można dowolnie rozmieszczać, np. mapy, podglądu kamer, dziennika zdarzeń, dziennika kontroli dostępu, wiadomości, zegara, kalendarza czy stanu systemu. Dzięki temu w jednym momencie można mieć podgląd na mapę, kamery i dziennik.

Użytkownik może utworzyć wiele paneli i przełączać się między nimi, np. osobny panel na zmianę dzienną i nocną. Administrator może przygotować panele dla całych grup użytkowników. Ustawienia są zapamiętywane w bazie i po zalogowaniu odtwarzane na dowolnym stanowisku.

5.2 Moduł map

Moduł map służy do wizualnego przedstawienia lokalizacji elementów na podkładach graficznych. Osoba konfigurująca system wgrywa podkłady, które reprezentują rzut z góry integrowanego obszaru; mapy wykonane są w technice wektorowej (SVG), dzięki czemu zachowują ostrość przy dowolnym powiększeniu. Moduł pozwala zagnieżdżać podkłady, tworząc strukturę od ogółu do szczegółu. Na podkładach rozmieszczane są elementy zgodnie z ich faktyczną lokalizacją.

Rozmieszczone elementy zmieniają kolory zgodnie ze stanem faktycznym. Kolory stanów/priorytetów mogą być edytowane i dostosowywane do zasad panujących na obiekcie. Każdy kolor musi jednoznacznie definiować zdarzenie, które jest odbierane przez system integrujący. W systemie wbudowano edytor map oraz edytor ikon, dzięki którym administrator samodzielnie przygotowuje podkłady i symbole urządzeń. Na mapach można także wyrysować strefy dozorowe oraz przebieg kabli i czujek systemów ochrony obwodowej; strefa w momencie wystąpienia w niej alarmu zmienia kolor zgodnie z priorytetem zdarzenia.

Operator, posługując się mapą, wybiera ikonę, która reprezentuje prawdziwy element integrowanego systemu. Wskazana ikona otwiera dodatkowe okno, które umożliwia sprawdzenie stanu tego elementu, dla kamery możliwe jest podejrzenie obrazu. Dla elementu dostępne jest wywołanie sterowania, czyli wydanie polecenia integrowanemu systemowi. Przykładowo:

- **SSWiN** – uzbrojenie, rozbrojenie i kasowanie alarmu w strefie, blokada czujnika, wysterowanie wyjść przekaźnikowych,
- **kontrola dostępu** – otwieranie, zamykanie i blokowanie przejścia,
- **CCTV** – podgląd na żywo, sterowanie PTZ, przywołanie presetu,
- **automatyka i oświetlenie** – załączanie i wyłączanie wyjść, ustawianie wartości.

Dla obszarów zewnętrznych dostępne są także mapy geograficzne (GIS), wykorzystywane m.in. do prezentacji obiektów wykrytych przez radary i czujniki systemów antydronowych.

System pożarowy w systemie niecertyfikowanym polega jedynie na wizualizacji i nie ma możliwości wywoływania na nim sterowań. W celu zapewnienia sterowania systemami pożarowymi należy skorzystać z systemu, któremu wydano Krajową Ocenę Techniczną (KOT) i świadectwo dopuszczenia CNBOP-PIB, jak Argus SIUP (system integrujący urządzenia przeciwpożarowe).

5.3 Moduł dziennika

Moduł dziennika służy do podglądu wszystkich zdarzeń, które zostały przetworzone przez system integrujący. Komunikat w dzienniku zaprojektowano tak, aby był jak najbardziej czytelny. Każdy wpis posiada oznaczenie kolorystyczne odpowiadające priorytetowi zdarzenia oraz ikonę powiązaną z priorytetem i sygnałem zdarzenia, taką samą jak na mapie. Zawarte są w nim również informacje o typie oraz adresie urządzenia, które zgłosiło komunikat, lokalizacja oraz data rozpoczęcia i zakończenia zdarzenia. Daty te mówią operatorowi, czy zdarzenie jeszcze trwa w systemie chroniącym obiekt, czy zostało już zakończone.

Wszystkie wpisy do dziennika mogą podlegać kwitowaniu. Oznacza to, że operator prowadzący służbę musi potwierdzić, że komunikat przyjął do wiadomości i podjął działania. Status potwierdzenia jest zapamiętywany w bazie danych i nie podlega zmianie. Do każdego wpisu można dodać notatkę, wyfiltrować wszystkie wcześniejsze zdarzenia dla wskazanego elementu, pokazać urządzenie na mapie oraz otworzyć sygnaturę elementu, aby sprawdzić konfigurację sygnału. W zakładce dziennika można skorzystać z gotowych filtrów:

- **lista alarmowa** – wszystkie zdarzenia alarmowe, zarówno trwające, jak i zakończone, które nie zostały jeszcze skwitowane,
- **lista ostrzegawcza** – zdarzenia alarmowe, sabotaże, zagrożenia oraz rozbrojenia, które ciągle trwają w systemach ochrony,
- **lista aktywnych stanów** – aktualny stan wszystkich elementów dodanych do systemu Argus PSIM,
- **nieskwitowane** – wszystkie wpisy w dzienniku, które nie zostały jeszcze skwitowane, bez rozróżnienia na typ sygnału.

Dziennik daje możliwość zaawansowanego filtrowania, w którym można ustawić zakres dat, obszar obiektu, typ zdarzenia, typ systemu, typ urządzenia oraz stan zdarzenia. Filtry można zapisywać i wykorzystywać ponownie. Po filtracji zdarzenia można wydrukować lub wyeksportować do formatu PDF lub Excel.

Oprócz głównego dziennika zdarzeń moduł zawiera dzienniki tematyczne:

- **dziennik alarmów** – z podglądem nagrań z kamer powiązanych z alarmem,
- **dziennik kontroli dostępu** – przejścia użytkowników kart, odmowy dostępu i zdarzenia systemu kontroli dostępu,
- **dziennik obecności** – zliczanie osób przebywających w strefach obiektu,
- **depozytory kluczy** – wydania i zwroty kluczy z depozytorów,
- **komunikaty systemowe** – informacje o pracy samej platformy, np. utracie komunikacji ze sterownikiem.

5.4 Moduł procedur

Procedury ułatwiają pracę operatora w momencie zagrożenia. Dzięki takiemu podejściu operator może działać zgodnie z określonymi krokami przygotowanymi przez administratora systemu, co ogranicza ryzyko popełnienia błędu. Argus PSIM został przystosowany do działania wielopoziomowego, co oznacza, że operatorzy mogą się uzupełniać w wykonywaniu procedur. Każda procedura automatyczna jest odkładana na stos, z którego operator ją pobiera i przypisuje do siebie. W trakcie wykonywania procedury operator może opuścić stanowisko pracy i odłożyć niedokończoną procedurę z powrotem na stos. W tym momencie wyższy nadzór, zlokalizowany w innym miejscu, może dokończyć wykonywanie wcześniej rozpoczętej procedury.

Argus PSIM nie opiera się na mechanizmie predefiniowanych procedur – tworzy się je w graficznym edytorze w postaci schematu blokowego. Dostępne bloki to m.in.: podgląd kamery, sterowanie urządzeniem, decyzja operatora (rozgałęzienie scenariusza), wysłanie wiadomości e-mail, SMS lub komunikatu głosowego, potwierdzenie kodem PIN, odliczanie czasu, automatyczne wygenerowanie raportu oraz odwołanie do innej procedury. Wewnątrz procedury operator może wprowadzać komentarze, wyświetlać obraz z kamery przypisanej do elementu, który wywołał procedurę, oraz otworzyć podgląd mapy, aby zlokalizować miejsce zdarzenia.

Procedury mogą być wywoływane ręcznie lub automatycznie przez zdarzenie spływające do dziennika. Przed udostępnieniem operatorom procedurę można przetestować w trybie testowym, bez wpływu na pracę systemu.

5.5 Moduł raportów

Moduł raportów umożliwia generowanie raportów na podstawie wszystkich pojawiających się w systemie zdarzeń. Raporty mogą być tworzone ręcznie przez użytkownika lub generowane automatycznie. Przy ręcznym generowaniu raportu użytkownik ustawia filtry, które określają jego zawartość, i może dodać załączniki. Możliwe jest tworzenie szablonów raportów wykonywanych cyklicznie.

Raporty można odtwarzać w systemie, zapisywać na dysku (PDF, Excel, CSV), drukować lub udostępniać innym użytkownikom w zakładce raportów udostępnionych. Każdy operator ma możliwość utworzenia raportu ze swojej zmiany. Moduł raportów jest powiązany z modułem harmonogramów, dzięki czemu podczas wykonywania zadania może zostać utworzony raport z jego przebiegu. Moduł raportów jest też powiązany z modułem procedur, co umożliwia generowanie raportu po każdym wykonanym kroku lub podsumowanie procedury po jej ukończeniu.

5.6 Moduł terminarza

Moduł terminarza umożliwia administratorowi i użytkownikom planowanie zdarzeń w oparciu o kalendarz, np. prac serwisowych, przeglądów czy obchodów. Zdarzenia posiadają nazwę, priorytet, zakres dat i przypisanych użytkowników. Priorytety są ustalane przez administratora, a następnie mogą być przypisane do zdarzenia. Dodane zdarzenia pokazują się na siatce kalendarza i są widoczne tylko dla użytkowników, których dotyczą. Moduł umożliwia modyfikację i usuwanie zdarzeń. Terminarz wysyła przypomnienia przed zaplanowanym terminem; odstęp przypomnień można ustawić podczas tworzenia zdarzenia.

5.7 Moduł harmonogramów

Harmonogramy umożliwiają tworzenie zaplanowanych czynności, które system ma wykonać automatycznie, np. uzbrajanie i rozbrajanie stref, załączanie oświetlenia czy automatyczne generowanie raportów. Zadanie harmonogramu może być cykliczne lub jednorazowe oraz może wywoływać sterowanie na jednym lub wielu elementach systemu. Harmonogram umożliwia skonfigurowanie wszystkich sterowań dostępnych z poziomu mapy. Zadania oświetleniowe mogą być powiązane z zegarem astronomicznym (wschód i zachód słońca).

Każde zadanie posiada status informujący, czy zostało wykonane prawidłowo, a także priorytet, według którego zadania są kolejkowane – zadania o wyższym priorytecie są wykonywane w pierwszej kolejności. Rejestr zmian oraz rejestr wykonanych sterowań pozwalają w każdej chwili sprawdzić, kto i kiedy zmienił harmonogram oraz jakie sterowania zostały wykonane.

5.8 Moduł warunków i automatyki

Warunki to mechanizm tworzenia połączeń logicznych pomiędzy sygnałami pochodzącymi z różnych systemów. Administrator definiuje wyrażenia logiczne (np. „czujka w strefie A w alarmie i strefa A uzbrojona”), których wynik prezentowany jest jako nowy sygnał o ustawionym priorytecie. Wynik warunku może również automatycznie wywołać sterowanie, uruchomić procedurę lub wysłać powiadomienie. Dzięki temu możliwe jest budowanie powiązań między systemami różnych producentów bez ingerencji w ich konfigurację.

5.9 Moduł CCTV

Moduł CCTV służy do obsługi strumieni wideo z kamer i rejestratorów. Umożliwia podgląd na żywo oraz odtwarzanie nagranego materiału, sterowanie kamerami obrotowymi PTZ (również za pomocą joysticka), przywoływanie presetów oraz eksport nagrań. Operator może tworzyć i zapisywać własne układy siatek kamer. Obraz jest przekazywany w technologii WebRTC, dzięki czemu działa bez dodatkowych wtyczek również w przeglądarce internetowej.

Integracja z rejestratorami i systemami zarządzania wideo (VMS) zapewnia informacje o stanie systemu CCTV (np. utrata sygnału wideo, detekcja ruchu, zdarzenia analityki).

5.10 Moduł komunikacji: SMS, VoIP, e-mail

Moduł służy do definiowania odbiorców końcowych, grup komunikacyjnych oraz do konfiguracji wiadomości. Obsługiwane kanały to:

- **SMS** – przez bramkę SMS,

- **połączenia głosowe TTS** – przez centralę telefoniczną, z komunikatami odczytywanymi przez syntezator mowy,
- **e-mail** – przez serwer pocztowy klienta,
- **wiadomości systemowe** – wewnętrzne komunikaty między użytkownikami platformy, możliwość dołączania załączników.

Odbiorcy i wiadomości są powiązani z modułem procedur i warunków, gdzie jednym z kroków może być wysłanie powiadomienia. Rejestr wysłanych wiadomości zapisywany jest w bazie danych i przedstawiany na liście dostępnej dla administratora.

5.11 Moduł dziennika służby

Moduł przeznaczony jest dla pracowników pełniących służbę na terenie obiektu. Administrator posiadający uprawnienia edycji może dodać dziennik przeznaczony dla konkretnej grupy użytkowników, np. ochrony oraz zdefiniować posterunki, typy stanowisk, rodzaje czynności i rodzaje notatek. Każde rozpoczęcie i zakończenie służby jest odnotowywane w systemie wraz z imieniem i nazwiskiem osoby pełniącej służbę, jej identyfikatorem oraz stanowiskiem lub posterunkiem.

Każdy wpis do dziennika ma swojego opiekuna, który pełni rolę dyżurnego. Do wpisu można dodać opis przebiegu zmiany oraz informacje o tym, co wydarzyło się na poprzedniej zmianie. Zakończenie służby jest dokonywane przez dyżurnego, który jako jedyny, poza administratorem, może zmienić stan wpisu w dzienniku. Po zakończeniu generowany jest automatyczny raport z liczbą odstępstw od normalnego układu systemu, zaistniałych podczas pełnionego dyżuru. Zakończone dzienniki trafiają do archiwum dostępnego dla koordynatora.

5.12 Moduł wykresów i pomiarów

Moduł prezentuje dane systemu w formie wykresów: liczbę i rodzaje zdarzeń w czasie, stan systemu, historię logowań oraz wartości pomiarowe z urządzeń (np. temperatury, jakości powietrza, parametrów zasilania czy wejść analogowych). Wykresy pozwalają szybko wychwycić trendy i nietypowe sytuacje, np. rosnącą liczbę awarii w danym systemie.

5.13 Moduł ochrony antydronowej i radarowej

Moduł prezentuje na mapie geograficznej obiekty wykrywane przez radary i czujniki systemów antydronowych z klasyfikacją (np. dron, pojazd, zwierzę, samolot), historią trasy, odległością i azymutem. Dla detekcji radiowych (RF) wyświetlana jest również szacowana pozycja operatora drona. Operator może definiować strefy ochronne, automatycznie naprowadzać kamery na wykryty obiekt oraz, w ramach uprawnień, uruchamiać środki przeciwdziałania, np. jammer.

5.14 Widok syntetyczny (C2)

Widok syntetyczny przedstawia stan całego obiektu na jednym, animowanym schemacie. Uzupełniają go zestawienia liczby alarmów, zagrożeń, sabotaży, uszkodzeń, awarii komunikacji, akcji serwisowych i przekroczeń w wybranym okresie oraz automatycznie generowane podsumowanie sytuacji. Widok jest przeznaczony przede wszystkim dla kadry kierowniczej i centrów dowodzenia.

5.15 Moduł administratora

Moduł administratora służy do zarządzania całym systemem. Obejmuje m.in.:

- **Zmiany w bazie** – zatwierdzanie zmian wprowadzonych w trybie edycji, z możliwością ich podejrzenia i wycofania; tworzenie kopii zapasowej bazy danych oraz jej przywracanie.
- **Zasoby systemowe** – rozmiar zajmowany przez bazę danych i zajętość dysków, z ostrzeżeniami o kończącym się miejscu.
- **Użytkownicy i uprawnienia** – tworzenie i archiwizowanie kont, grupy uprawnień do modułów, obszarów, urządzeń, sygnałów, procedur i harmonogramów, powiązanie kont z kontami domenowymi Windows.
- **Aktywni użytkownicy i historia logowań** – kto jest aktualnie zalogowany oraz rejestr logowań z datą, adresem IP, rezultatem i opisem.
- **Agenci i sterowniki** – nadzór nad pracą agentów i sterowników komunikacyjnych, ich uruchamianie, zatrzymywanie i konfiguracja.
- **Urządzenia i architektura urządzeń** – lista integrowanych elementów, z których każdy posiada sygnaturę (adres, ikona, rzeczywisty typ elementu), oraz graficzna prezentacja zależności między urządzeniami (np. centrala – moduł – czujka). Konfiguracja sygnałów tłumaczy adresację różnych producentów na jednolitą postać systemu.
- **Grupy urządzeń i grupy szybkiego dostępu** – grupowanie elementów w celu wspólnego sterowania i szybkiego wyszukiwania oraz podglądu stanu czy pomiaru.
- **Sygnały** – zarządzanie priorytetami/stanami, kolorami i dźwiękami sygnałów.
- **Serwis kamer** – zarządzanie serwisem przekazującym obraz z kamer do aplikacji.
- **Integracje** – konfiguracja integracji z systemami zewnętrznymi, synchronizacja kont z SSWiN itp.
- **Import i eksport danych** – masowe wprowadzanie i eksport konfiguracji z plików Excel/CSV, co znacząco przyspiesza uruchomienie dużych obiektów.
- **Historia sterowań i audyt** – rejestr wszystkich sterowań oraz dziennik audytu działań użytkowników i systemu.
- **Wersja** – numery wersji wszystkich składników platformy.

6. Integracje – Argus.Drivers

Argus.Drivers to zestaw sterowników, które zapewniają komunikację platformy z systemami różnych producentów. Każdy sterownik działa jako osobny proces nadzorowany przez usługę Argus.Agent; odbiera stany i zdarzenia z integrowanego systemu, tłumaczy je na jednolity model sygnałów Argus PSIM i przekazuje do serwera, a w przeciwnym kierunku realizuje sterowania wydawane przez operatorów, procedury i harmonogramy. Poniższa tabela przedstawia aktualnie dostępne integracje.

Rodzaj systemu	Integrowane systemy i urządzenia
Sygnalizacja włamania i napadu (SSWiN)	Satel INTEGRA, Honeywell Galaxy, Aritech ATS / Advisor Master, Vanderbilt SPC

Rodzaj systemu	Integrowane systemy i urządzenia
Kontrola dostępu (SKD)	Nedap AEOS, Roger RACS, Unicard, Compas, Schneider Andover Continuum, Argus KD (TELBUD), depozytory kluczy SAIK
Sygnalizacja pożaru (SSP) – wizualizacja	Polon-Alfa (Polon 4000, POLON 6000), Schrack Seconet, moduły Neuron, ESSER i BOSCH
Telewizja dozorowa (CCTV / VMS)	Genetec Security Center, Bosch BVMS, Avigilon Control Center, Geutebrück G-Core / GeViScope, Mirasys VMS, Hikvision, BCS, kamery zgodne z ONVIF (wykrywanie, podgląd, PTZ), analityka kamer Axis (MQTT), kamery Vortex
Ochrona obwodowa i radary	radary Axis, radary Magos, Future Fibre Technologies (FFT CAMS), FiberSenSys, CIAS SIOUX, sterowniki stref Stekop HF-500R
Ochrona antydronowa	radary OWL, detektory RF Rantelon i SkyCope, głowice obserwacyjne MOOG, systemy APFLYER, jammer, platforma dowodzenia IMCP, dane radarowe w standardzie ASTERIX
Automatyka budynkowa, oświetlenie, I/O	Modbus RTU / Modbus TCP (także wiele urządzeń), MQTT, Echelon i.LON SmartServer (sterowanie oświetleniem), sterowniki EWIO, bramy Advantech ECU-1251D, moduły DCM100, moduły wejść/wyjść komputerów przemysłowych, moduł Argus Control (TELBUD)
Środowisko	czujniki jakości powietrza uHoo
Nagłośnienie	głośniki sieciowe Axis
Infrastruktura sieciowa (IT)	dowolne urządzenia SNMP (v1/v2c/v3, pułapki i odczyt), przełączniki Extreme Networks i Bitstream
Lokalizacja pojazdów (GPS)	system Radiolok AVL
Komunikacja	bramki SMS (SMSEagle), centrale telefoniczne Slican, poczta e-mail
Inne instancje Argus	wymiana stanów, zdarzeń i pomiarów między instalacjami Argus PSIM (np. obiekt lokalny – centrum nadzoru)

Lista integracji jest stale rozwijana. Nowe sterowniki powstają na wspólnej bibliotece, co pozwala szybko dodawać kolejne systemy na potrzeby konkretnego projektu.