



# ARGUS RV

WYSOKOWYDAJNY SYSTEM KLASY PSIM

KARTA INFORMACYJNA



## INFORMACJE OGÓLNE

ARGUS RV jest zaawansowaną platformą komputerowego systemu nadzoru i sterowania z oprogramowaniem klasy PSIM (Physical Security Information Management) o rozbudowanej funkcjonalności i dużej niezawodności, wykorzystywaną do zarządzania bezpieczeństwem obiektów.

Stanowi jednolite rozwiązanie dla integracji wszystkich rodzajów systemów ochrony technicznej (SOT) różnych producentów:

- sygnalizacji włamania i napadu (SWiN) wraz z ochroną obwodową,
- kontroli dostępu (KD),
- telewizji dozorowej (CCTV),
- detekcji wtargnięć i ochrony powierzchni (systemów radarowo-kamerowych),
- wykrywania i sygnalizacji pożaru (SSP),
- wentylacji pożarowej i oddymiania grawitacyjnego,
- stałych urządzeń gaśniczych (SUG),
- dźwiękowych systemów ostrzegawczych (DSO),
- oświetlenia awaryjnego,
- detekcji CO i LPG
- oraz innych instalacji istotnych dla zapewnienia bezpieczeństwa ludzi i mienia (zasilających, teleinformatycznych, komunikacyjnych, itp.).

ARGUS RV może przy tym pełnić równocześnie funkcje SCADA w systemach BMS (Building Management System) i automatyki.

System jest rozwijany przez TELBUD S.A. we współpracy z firmą MIKRONIKA na bazie sprzętowo-programowych rozwiązań automatyki z oprogramowaniem dyspozytorskim SYNDIS RV, które są powszechnie wykorzystywane do zarządzania rozległymi systemami elektroenergetycznymi na terenie całej Polski, a także poza jej granicami. Zastosowanie rozwiązań, które zostały sprawdzone w sytuacjach krytycznych w czasie wieloletniego użytkowania, jest gwarancją dużej pewności i stabilności działania systemu, co w połączeniu z rozbudowanymi mechanizmami ochrony komunikacji i programowej autokontroli, pracą w czasie rzeczywistym z rozdzielczością do 1 ms oraz brakiem ograniczeń dla ilości nadzorowanych sygnałów i urządzeń stanowi istotną przewagę konkurencyjną nad innymi rozwiązaniami tego typu oferowanymi obecnie na rynku.

Dostęp do kodów źródłowych oprogramowania systemowego pozwala na szybkie dostosowanie funkcjonalności zintegrowanego systemu zarządzania bezpieczeństwem obiektów do indywidualnych wymagań użytkowników oraz umożliwia podłączenie do niego dowolnych podsystemów i urządzeń różnych producentów.

Oprogramowanie Argus RV może być instalowane na sprzęcie komputerowym pracującym pod systemami operacyjnymi Windows, Windows Server i Linux. Jest też instalowane na serwerach SO-5S i terminalach operatorskich TO-1S certyfikowanego systemu ARGUS RV-C, posiadającego świadectwo dopuszczenia CNBOP-PIB.

Rozproszona, sieciowa architektura oprogramowania typu klient-serwer oraz systemowa współpraca ze specjalizowanymi koncentratorami interfejsów (sterownikami przemysłowymi) i/lub z oprogramowaniem realizującym funkcjonalność koncentratorów wirtualnych, pozwala na tworzenie rozbudowanych systemów sterowania i nadzoru w różnorodnych konfiguracjach. Komunikacja z nadzorowanymi systemami może być realizowana poprzez interfejsy Ethernet TCP/IP, RS-232, RS-485 lub RS-422, przy wykorzystaniu protokołów komunikacyjnych, otwartych standardów OPC albo bibliotek programistycznych (SDK, API) udostępnianych przez producentów, jak również poprzez moduły wejść/wyjść binarnych i analogowych.

#### **ARCHITEKTURA SYSTEMÓW ARGUS RV**

Oprogramowanie Argus RV zbudowane jest funkcjonalnie z dwóch podstawowych aplikacji: serwera oraz aplikacji wizualizacyjnej stacji nadzoru operatorskiego (klienta), pozwalając na bezproblemowe współdziałanie wielu stanowisk nadzoru oraz nadawanie im różnych uprawnień.

Przy zastosowaniu serwera www możliwa jest również obsługa systemu poprzez przeglądarkę internetową. W zależności od potrzeb mogą być stosowane różnorodne konfiguracje systemu: od najprostszej, zbudowanej na jednym komputerze, po najbardziej złożone, składające się z wielu redundantnych koncentratorów, serwerów i stacji operatorskich, tworzących strukturę hierarchiczną.

Wymiana danych pomiędzy elementami takiej struktury realizowana jest systemowo poprzez sieć LAN/WAN dedykowaną dla systemów bezpieczeństwa.

Dla zapewnienia ciągłości pracy systemu w przypadku awarii jego pojedynczego elementu, oprogramowanie Argus RV może być instalowane na klastrze serwerów wysokiej dostępności HA.

Węzły klastra z wirtualnymi macierzami dyskowymi mogą być usytuowane w różnych lokalizacjach geograficznych, co ma szczególne znaczenie w instalacjach ochrony infrastruktury krytycznej.

W konfiguracjach obejmujących centralne zarządzanie bezpieczeństwem wielu oddalonych obiektów z równoczesnym zapewnieniem możliwości lokalnego nadzoru operatorskiego, w przypadku utraty komunikacji z centrum, stosowane są trzy podstawowe sposoby integracji SOT. Każdy z nich wymaga zastosowania na obiekcie lokalnego serwera pracującego z innym rozwiązaniem systemowym oprogramowania:

- tzw. serwera wyspowego ARGUS RV,
- niezależnego serwera ARGUS RV,
- lokalnego serwera z oprogramowaniem ARGUS WEB, które jest autorskim rozwiązaniem firmy TELBUD S.A. wykorzystującym najnowszą technologię sieciową Microsoft NET.

### **Serwer wyspowy ARGUS RV**

Komunikacja z systemami ochrony technicznej realizowana jest równocześnie przez serwer centralny i lokalny serwer wyspowy ARGUS RV na obiekcie. W czasie normalnej pracy oprogramowanie lokalnej stacji operatorskiej jest klientem serwera centralnego, a serwer wyspowy działa w tle, synchronizując na bieżąco bazę danych.

W razie awarii łącza komunikacyjnego obiektu z serwerem centralnym, oprogramowanie lokalnej stacji operatorskiej zostaje przełączone na klienta serwera wyspowego, przy czym zachowana jest pełna funkcjonalność nadzoru z dostępem do zdarzeń archiwalnych.

### **Niezależny serwer ARGUS RV**

W rozwiązaniu, w którym integracja systemów ochrony technicznej realizowana jest przez niezależny lokalny serwer ARGUS RV na obiekcie, serwer centralny otrzymuje dane i przekazuje sterowania za pośrednictwem serwera lokalnego przy wykorzystaniu protokołu TASE 2.

### **Lokalny serwer z oprogramowaniem ARGUS WEB**

W przypadku zastosowania lokalnego serwera ARGUS WEB możliwa jest jego współpraca z oprogramowaniem centralnego serwera ARGUS RV poprzez komunikację po protokole internetowym HTTPS.

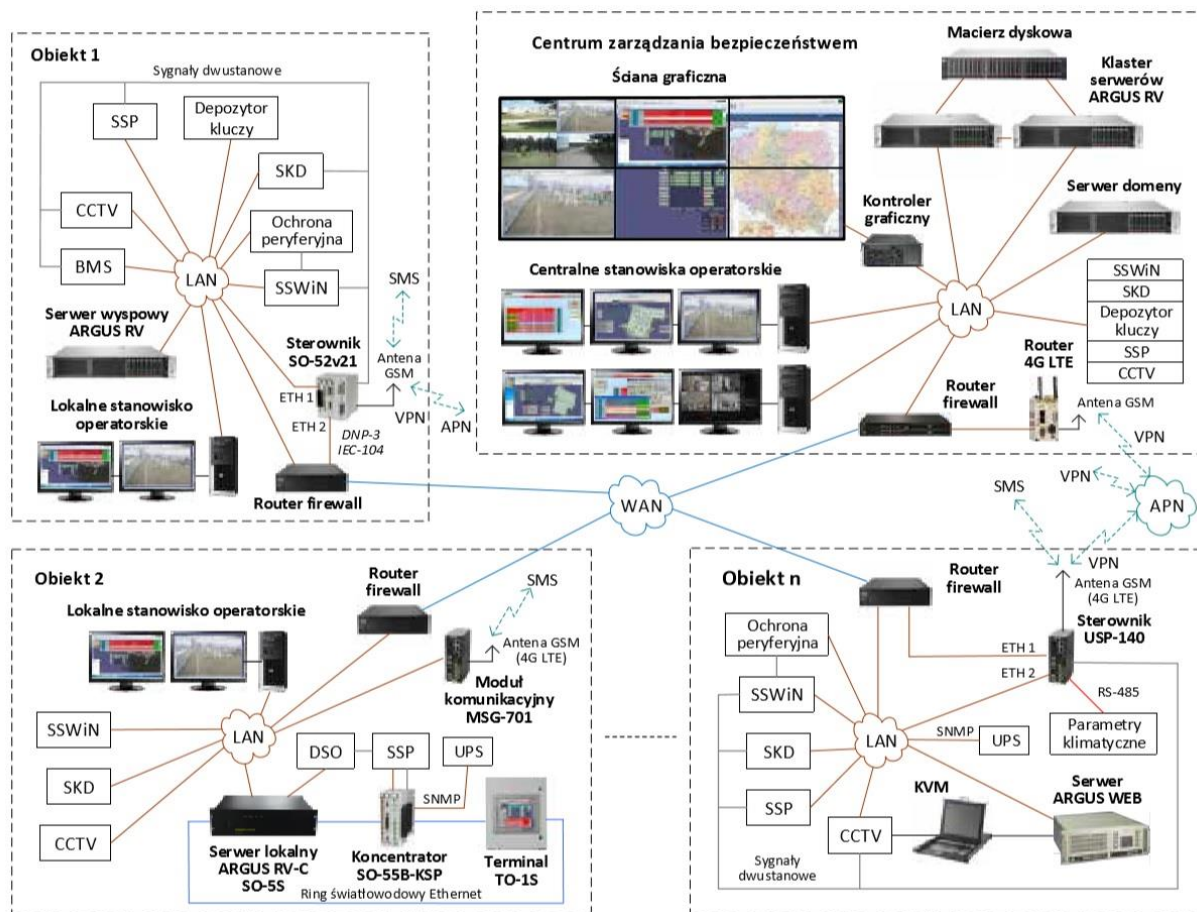
Istnieje też możliwość uruchamiania wybranych modułów systemu ARGUS WEB w oknach aplikacji ARGUS RV. Oprogramowanie driverów komunikacyjnych z urządzeniami systemów ochrony technicznej jest przygotowywane do pracy w obu systemach.

## KOMUNIKACJA SYSTEMOWA Z ROZPROSZONYMI OBIEKTAMI

Komunikacja pomiędzy centrum zarządzania bezpieczeństwem a oddalonymi obiektami realizowana jest najczęściej poprzez prywatną sieć WAN budowaną na traktach światłowodowych, ale mogą być stosowane również dzierżawione łącza telekomunikacyjne.

Na połączeniach lokalnej sieci LAN systemów bezpieczeństwa z siecią WAN instalowane są routery z zaporą firewall. Wykorzystanie koncentratorów systemu ARGUS RV pozwala też na transmisję danych drogą radiową poprzez sieć telefonii komórkowej, z bezpiecznymi kanałami VPN w wydzielonej, prywatnej sieci APN.

*Przykład rozbudowanej konfiguracji systemu ARGUS RV*



## KONCENTRATORY INTERFEJSÓW

Dla rozległych i rozproszonych obiektów podłączenie poszczególnych urządzeń do systemu może być dokonane przez zastosowanie specjalizowanych koncentratorów interfejsów, np. sterowników serii SO-52v21, SO-55B-KSP lub kompaktowych sterowników USP-140 firmy Mikronika, albo koncentratorów UGD-AW001 i UGD-AW002 opracowanych przez Telbud SA na bazie komputerów przemysłowych.

Urządzenia te mogą posiadać wiele portów sieciowych Ethernet oraz portów szeregowych RS-232, RS-485 lub RS-422. Mogą być też wyposażone w dodatkowe moduły wejść/wyjść dwustanowych i analogowych. Poprzez wbudowane lub zewnętrzne modemy GPRS/UMTS/LTE z możliwością zainstalowania dwóch kart SIM niezależnych operatorów telefonii komórkowej realizują również transmisję danych w sieci GSM oraz mogą wysyłać i odbierać wiadomości SMS.

Koncentratory pośredniczą w przekazywaniu sygnałów obiektowych i sterowań pomiędzy nadzorowanymi urządzeniami a jednym lub wieloma serwerami oraz przechowują dane o zdarzeniach w pamięci buforowej niezależnie dla każdego serwera. Urządzenia bazujące na sterownikach Mikroniki pracują pod systemem operacyjnym czasu rzeczywistego Linux i posiadają oprogramowanie systemowe w pełni zintegrowane z oprogramowaniem serwera ARGUS RV po sieci Ethernet.

Komunikacja z serwerami realizowana jest poprzez bezpieczne protokoły DNP3 lub IEC-104, z możliwością szyfrowania przy wykorzystaniu standardu protokołu TLS. Koncentratory oparte na komputerach przemysłowych, które mogą pracować pod systemem operacyjnym Windows lub Linux, komunikują się z serwerem ARGUS RV po protokole Json.

Oprogramowanie aplikacyjne koncentratorów umożliwia również realizację lokalnych algorytmów sterowania i interakcji pomiędzy nadzorowanymi systemami i urządzeniami, bez pośrednictwa serwera.

### Koncentrator SO-52V21



### OPROGRAMOWANIE SERWERA ARGUS RV

Na serwerze uruchamiana jest systemowa baza danych oraz działające wielowątkowo i bezobsługowo w tle procesy systemowe, w tym komunikacji z urządzeniami obiektowymi i koncentratorami interfejsów, rejestracji zdarzeń, rejestracji wartości pomiarowych, sygnalizacji alarmowej, sterowania, obsługi map cyfrowych, itp.

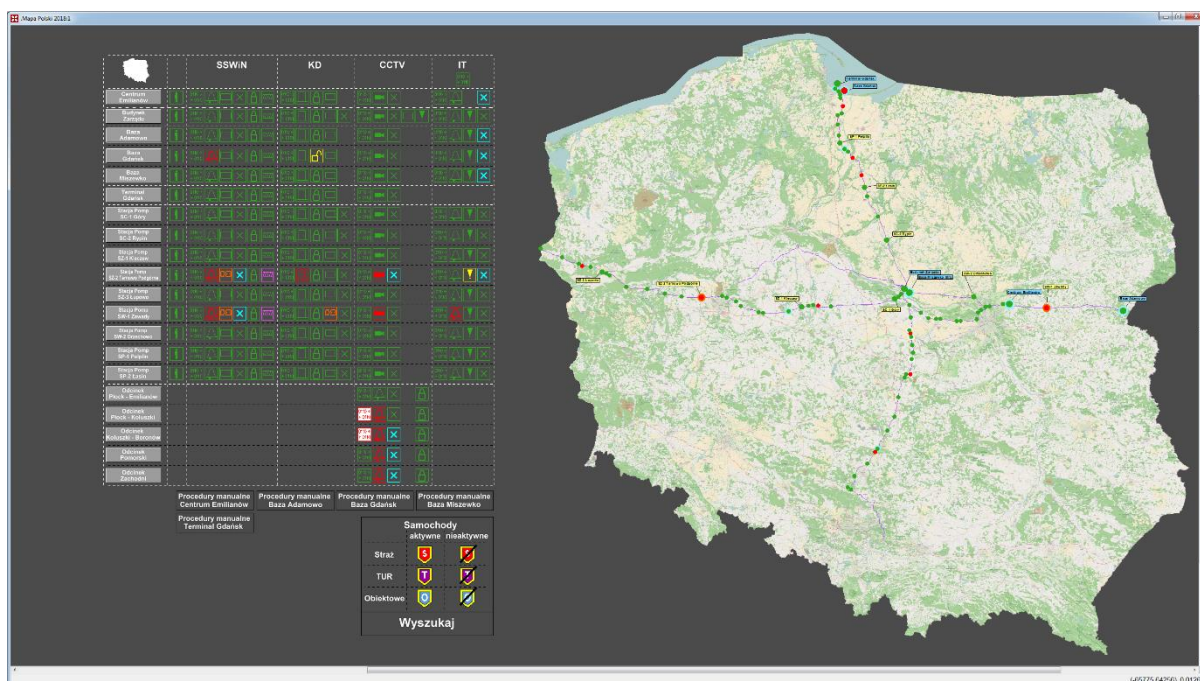
Oprogramowanie realizuje w szczególności następujące podstawowe funkcje:

- zbieranie informacji z nadzorowanych systemów ochrony,
- przetwarzanie informacji i zapis do bazy danych,
- zarządzanie procedurami obsługi zdarzeń alarmowych,
- przekazywanie komend sterujących do nadzorowanych systemów,
- synchronizację danych pomiędzy serwerami struktury hierarchicznej,
- zarządzanie bazą danych – archiwizacja, tworzenie kopii zapasowych, odtwarzanie w przypadku awarii,
- zarządzanie uprawnieniami operatorów oraz komunikacją, bezpieczeństwem i integralnością konfiguracji systemu.

Wszystkie dane pochodzące z różnych źródeł i rejestrowane w bazie danych serwera są natychmiastowo dostępne na jednej lub wielu stacjach nadzoru operatorskiego i przedstawiane są w jednolity sposób. Obsługa operatorska realizowana jest poprzez aplikację wizualizacyjną, która może być instalowana na stacjach roboczych lub dostępna poprzez przeglądarkę internetową. Aplikacja przedstawia zdarzenia w postaci komunikatów dziennika operatorskiego oraz graficznie na mapach.

## APLIKACJA WIZUALIZACYJNA

Aplikacja wykorzystuje pełno-graficzną wektorową platformę prezentacji zdarzeń obiektowych na mapach, z możliwością obsługi map cyfrowych ze współrzędnymi geodezyjnymi lub GPS. Wizualizacja jest możliwa na jednym lub na wielu monitorach, a także na ścianie graficznej.



Stany integrowanych systemów przedstawiane są w kilku podstawowych rodzajach okien:

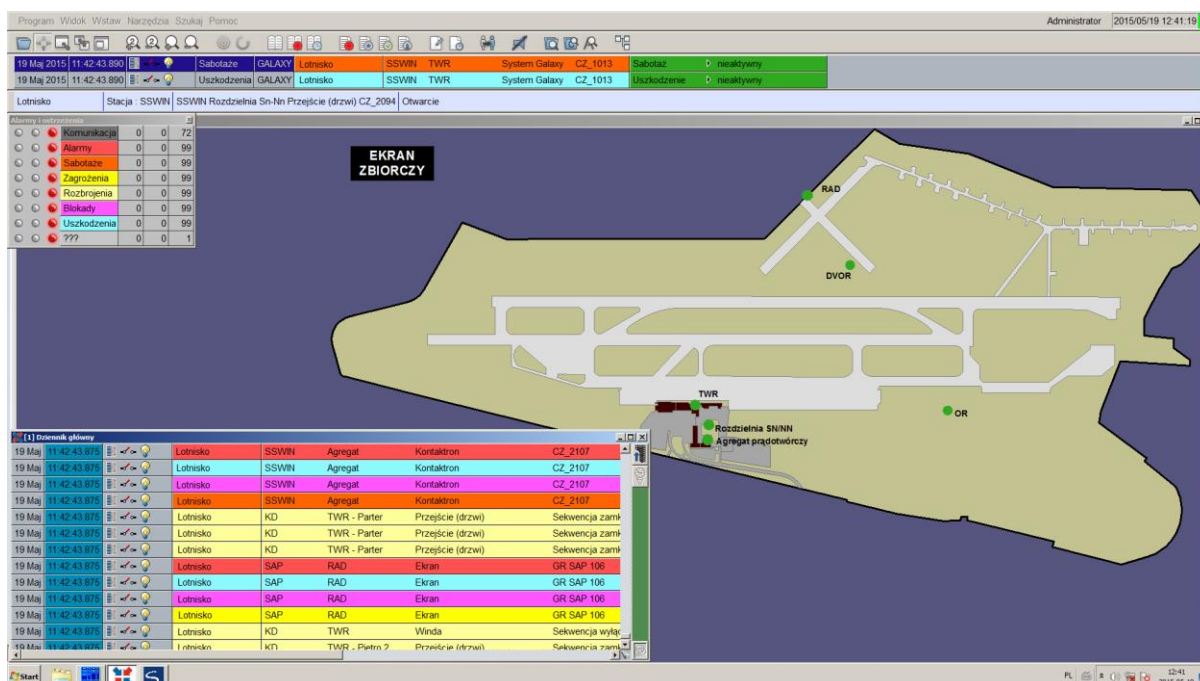
- na mapach lub ekranach synoptycznych obiektów, z predefiniowanymi ikonami obrazującymi aktualny stan wszystkich elementów nadzorowanych instalacji i urządzeń,
- w dzienniku operatorskim przedstawiającym chronologicznie, z cechą czasu rzeczywistego, komunikaty o wszystkich zdarzeniach, które zostały zarejestrowane przez system,



- na wykresach obrazujących zmiany i trendy wartości pomiarowych i sygnalizacyjnych w wybranym czasie.

### Wizualizacja na mapach.

Mapy i ekrany synoptyczne przygotowywane są w układzie hierarchicznym – od ogólnej mapy z lokalizacją wszystkich monitorowanych obiektów i zbiorczą sygnalizacją pozwalającą na natychmiastową ocenę stanu bezpieczeństwa na całym nadzorowanym obszarze, poprzez ekrany sygnalizacji zdarzeń i statusu systemów ochrony technicznej na poszczególnych obiektach, do szczegółowych map (podkładów budynków, kondygnacji) z lokalizacją i sygnalizacją stanu każdego z elementów tych systemów.

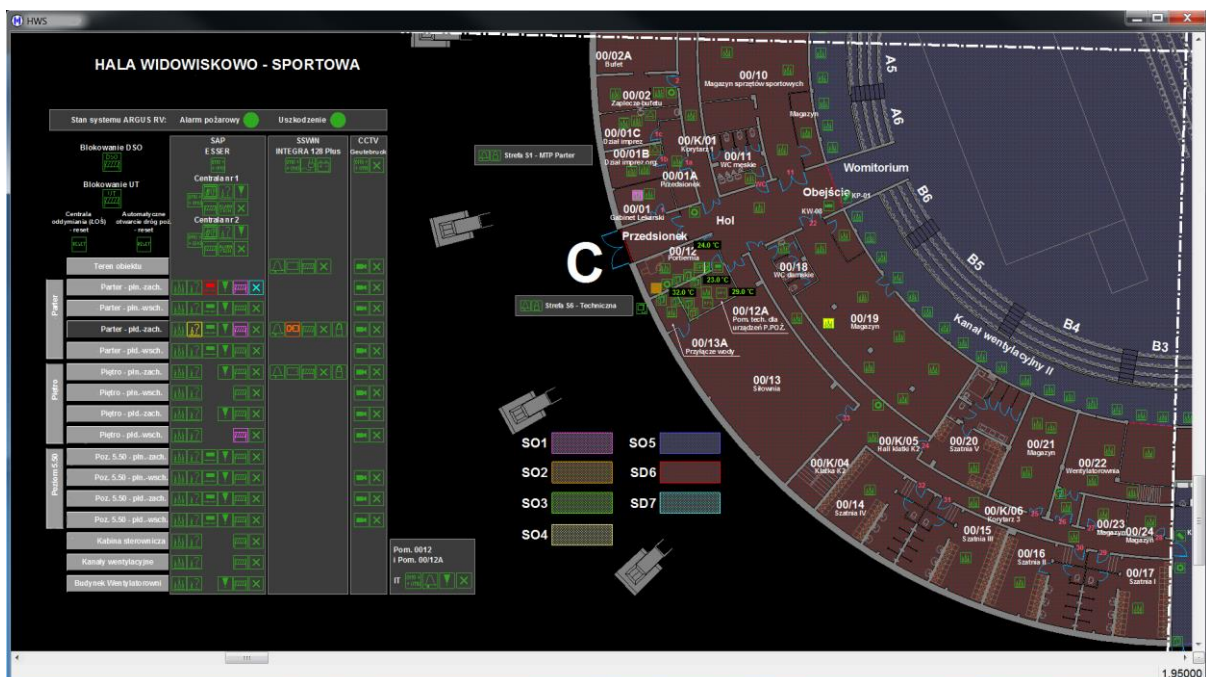


Operator ma możliwość obserwacji map w dowolnej skali, zmienianej płynnie kółkiem myszy, z automatycznym przełączaniem pomiędzy kolejnymi warstwami map z różnym stopniem szczegółowości (decluttering). Jednolity system kolorów pozwala na natychmiastowe rozróżnienie poszczególnych stanów monitorowanych elementów: stanu normalnego, alarmów, ostrzeżeń, sabotaży, awarii, braku komunikacji, itp.

Dla każdej ikony reprezentującej nadzorowane urządzenie na mapie operator ma możliwość wywołania menu kontekstowego, z którego uzyskuje dostęp do szeregu funkcji, w tym między innymi:

- informacji o typie urządzenia,
- wyświetlenia historii zdarzeń związanych z urządzeniem,
- sterowania urządzeniem, jeżeli takie działanie jest dostępne dla danego elementu,
- wyświetlenia obrazu z kamery CCTV skojarzonej z tym urządzeniem.

Pojawienie się jakiegokolwiek zdarzenia alarmowego może, w zależności od skonfigurowania systemu, spowodować automatyczne wyświetlenie obrazu z odpowiedniej kamery skierowanej na miejsce wystąpienia zdarzenia, co pozwala operatorowi na natychmiastową weryfikację zdarzeń np. w wypadku naruszenia strefy ochrony obiektu.



## Dziennik zdarzeń.

Dziennik operatorski rejestruje zarówno wszystkie zdarzenia obiektowe, jak również działania operatorów oraz stany samego systemu ARGUS RV. Komunikatów zarejestrowanych w dzienniku nie można usunąć.

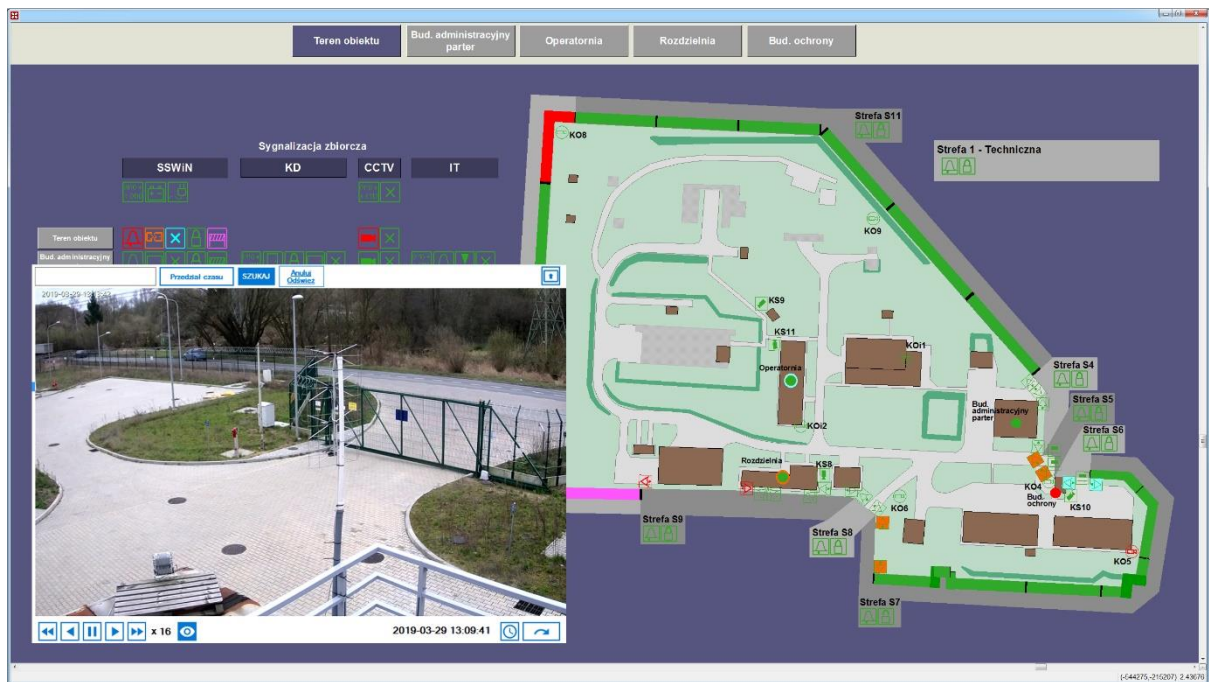
Komunikaty prezentowane w oknie dziennika podają między innymi następujące informacje:

- datę i czas wystąpienia zdarzenia,
- lokalizację zdarzenia,
- typ i rodzaj elementu sygnalizującego zdarzenie,
- opis zdarzenia,
- oznaczenie typu komunikatu i komunikatów powiązanych,
- sygnalizację statusu komunikatu (np. konieczność potwierdzenia odbioru zdarzenia przez operatora).

Kolorystyka poszczególnych komunikatów odpowiada kolorystyce stanów ikon na mapach synoptycznych. Z poziomu dziennika operator może w prosty sposób kwitować odbiór komunikatów alarmowych oraz natychmiastowo uaktywniać odpowiednie mapy synoptyczne z automatycznym wyszukiwaniem ikon odpowiadających elementom sygnalizującym zdarzenie, dopisywać swoje uwagi do poszczególnych komunikatów, jak również uaktywniać procedury obsługi zdarzeń.

## Filtry zdarzeń w dzienniku.

Rozbudowany, wielokryterialny system filtrów pozwala na szybkie uzyskanie dostępu do komunikatów dotyczących wybranych obiektów i elementów, jak również na tworzenie tzw. dzienników potomnych. Komunikaty wyszukane poprzez zastosowanie określonych kryteriów filtrowania wyświetlane są w oddzielnych oknach, w związku z czym aktualny dziennik zdarzeń może być zawsze widoczny dla operatora.

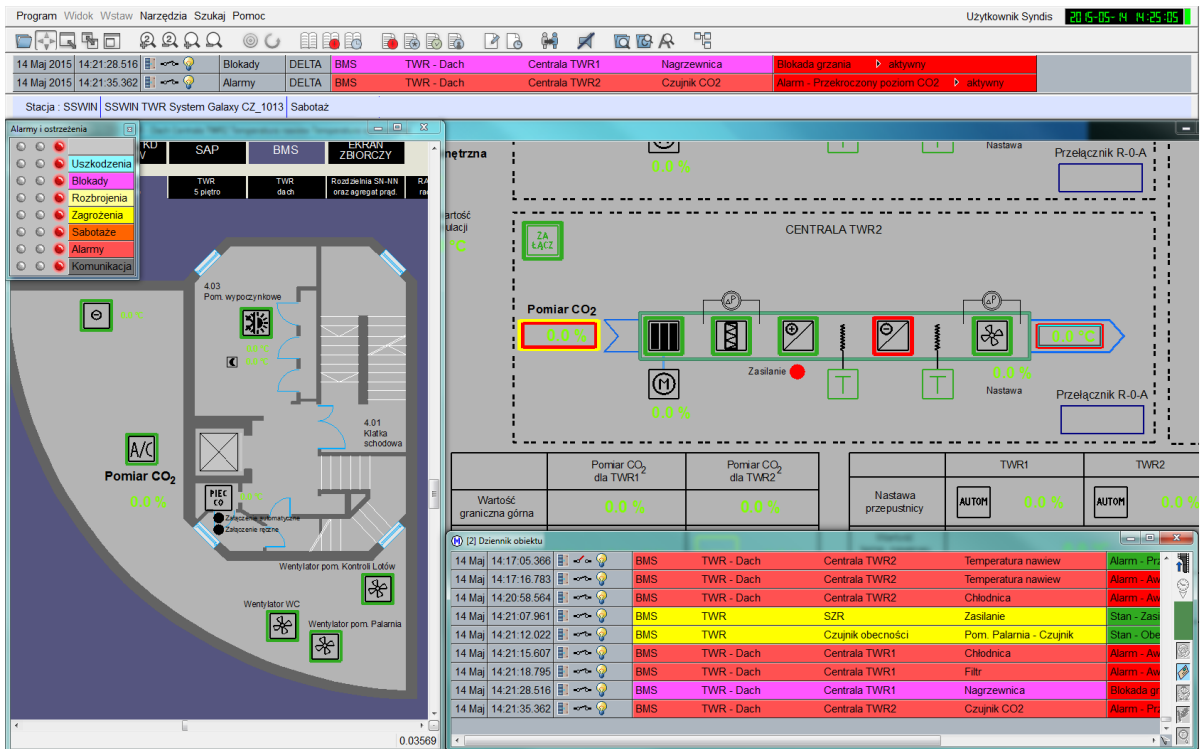


## Listy pomocnicze.

Oprócz dziennika zdarzeń w systemie dostępnych jest również szereg list pomocniczych, ułatwiających operatorom obsługę, jak np. lista alarmowa zawierająca wszystkie komunikaty nie skwitowane przez operatora, lista ostrzegawcza informująca o wszystkich aktywnych alarmach i ostrzeżeniach, lista stanów prezentująca aktualny stan wszystkich nadzorowanych elementów, czy też lista odstępstw od stanu normalnego.

## OBŚLUGA ZDARZEŃ

W systemie obsługiwane są trzy podstawowe rodzaje zdarzeń: alarmy, ostrzeżenia i informacje. Zdarzenia podzielone są na grupy funkcjonalne zgodne z przydzielonymi kategoriami sygnałów, takimi jak alarmy zabezpieczeń technicznych, sabotaże, uszkodzenia, blokady, zaniki komunikacji, powiadomienia, itp.



Rozróżnienie poszczególnych rodzajów i grup zdarzeń dokonywane jest kolorystyką ikon i symboli na mapach oraz komunikatów w dzienniku zdarzeń. Kolor zielony zarezerwowany jest standardowo dla stanu normalnego. Wystąpienie nowego zdarzenia, w zależności od jego rodzaju i konfiguracji systemu, może powodować:

- wygenerowanie sygnału dźwiękowego,
- zmianę kolorystyki i wyglądu ikony elementu na mapie,
- zapisanie komunikatu w dzienniku zdarzeń,
- pojawienie się komunikatu w liście alarmowej (do momentu skwitowania),
- pojawienie się komunikatu na pasku alarmowym (widoczne dwa ostatnie komunikaty),

- uruchomienie sygnalizacji czerwonym światłem migowym w oknie alarmy i ostrzeżenia (zbiorcza sygnalizacja alarmów),
- zainicjowanie procedury obsługi zdarzenia.

Po otrzymaniu komunikatu alarmowego i jego zidentyfikowaniu operator powinien potwierdzić (skwitować) odbiór alarmu. W następnej kolejności może zlokalizować na mapie element sygnalizujący zdarzenie oraz zweryfikować alarm obserwując obraz z odpowiedniej kamery CCTV.

### **Procedury postępowania.**

Poza standardową wizualizacją i archiwizacją zdarzeń oprogramowanie Argus RV jest wyposażone w mechanizmy wspomagania operatora w zakresie funkcji obsługi procedur bezpieczeństwa stosownie do zaistniałych zagrożeń i alarmów, jak również wsparcia zarządzania informacją o zasobach służb ochrony.

Dla każdego zdarzenia (incydentu) może zostać zdefiniowana procedura postępowania z listą czynności do wykonania przez operatora i zadań realizowanych automatycznie przez system. W chwili wystąpienia zdarzenia lista ta jest udostępniana w oddzielnym oknie, a realizacja poszczególnych zadań jest nadzorowana i rejestrowana z cechą czasu rzeczywistego do chwili zakończenia obsługi incydentu.

Poprzez połączenie z bazą danych służb odpowiedzialnych za bezpieczeństwo obiektu oraz przez integrację z systemami łączności tych służb i z systemem GPS, istnieje możliwość wskazywania na mapach cyfrowych aktualnej lokalizacji pojazdów i personelu ochrony oraz wysyłania komunikatów i poleceń podjęcia działań w celu weryfikacji i neutralizacji występujących zagrożeń i alarmów, jak również kontrolowania wykonania tych działań.

## STEROWANIE

Oprogramowanie Argus RV pozwala na sterowanie elementami nadzorowanych systemów. Sterowanie może być realizowane ręcznie przez operatora z poziomu aplikacji wizualizacyjnej lub automatycznie z aplikacji serwera.

### **Sterowanie ręczne.**

Sterowanie ręczne dokonywane jest poprzez wybór opcji sterowania z menu kontekstowego skojarzonego z ikoną reprezentującą nadzorowany element na mapie lub z poziomu procedury obsługi zdarzenia. Wykonanie sterowania musi być poprzedzone potwierdzeniem operatora, przy czym może wymagać wpisania dodatkowego kodu cyfrowego. Pozwala to na dwustopniowe rozbrajanie stref SSWiN zgodnie z wymaganiami Normy Obronnej NO-04-A004:2016, które polega na wprowadzeniu cyfrowego kodu na dwóch niezależnych od siebie urządzeniach, np. na stacji operatorskiej systemu integrującego i na fizycznej klawiaturze dostępu do strefy.

Po wysłaniu polecenia sterowania system oczekuje na zmianę stanu sterowanego elementu, po czym operator otrzymuje komunikat o poprawnym wykonaniu sterowania, a ikona elementu na mapie zmienia kolor i ewentualnie kształt. Jeżeli w zadany czas nie nastąpiła zmiana stanu elementu, generowany jest komunikat o niepowodzeniu sterowania.

Każdorazowe polecenie sterowania oraz potwierdzenie jego wykonania bądź przekroczenie czasu na jego realizację, dokumentowane jest odpowiednimi komunikatami w dzienniku zdarzeń.

W zależności od konfiguracji systemu, aplikacja serwera może wysyłać polecenia bezpośrednio do nadzorowanego urządzenia po protokole komunikacyjnym lub przekazać realizację sterowania do odpowiedniego koncentratora interfejsów.

### **Sterowanie automatyczne.**

System może automatycznie wysyłać polecenia sterowania w reakcji na zdarzenia obiektowe (np. alarm pożarowy) lub zgodnie z zadany harmonogramem czasowym. Sterowania te mogą być realizowane bezpośrednio przez serwer ARGUS RV lub samodzielnie przez koncentrator. Aplikacja oprogramowania serwera i koncentratora może generować również zaprogramowaną sekwencję sterowań. Odpowiednie komunikaty zapisywane są do dziennika zdarzeń jak przy sterowaniu ręcznym.

## UPRAWNIENIA UŻYTKOWNIKÓW

Funkcje oprogramowania Argus RV dostępne są po uprzednim zalogowaniu się operatora (podaniu unikatowego identyfikatora i hasła).

Dostępność poszczególnych funkcji uwarunkowana jest posiadaniem uprawnień nadawanych przez administratora systemu. W celu ograniczenia możliwości manipulacji przez osoby nieuprawnione system posiada wbudowane funkcje wymuszania okresowej zmiany hasła z zachowaniem reguł tworzenia haseł.

Domyślnie skonfigurowane są dwa konta: operatora i administratora. Działania poszczególnych użytkowników rejestrowane są w dzienniku zdarzeń, dzięki czemu zapewniona jest pełna rozliczalność obsługi systemu.

Dodatkowym elementem tej rozliczalności jest unikatowy mechanizm przekazywania zmiany pomiędzy operatorami, z rejestracją i wizualizacją stanu systemu w momencie przekazania.

Oprogramowanie posiada możliwość skonfigurowania nadrzędnych stanowisk operatorskich, których obsługa może nadzorować pracę innych operatorów lokalnych. Brak reakcji operatora lokalnego na występujące zdarzenia, w szczególności brak kwitowania alarmów lub obsługi procedur bezpieczeństwa, uruchamia odpowiednią sygnalizację na stanowisku nadrzędnym. Operator tego stanowiska ma możliwość przejęcia uprawnień operatora lokalnego do obsługi zdarzeń.

## BEZPIECZEŃSTWO CYFROWE

W systemie ARGUS RV zaimplementowano wiele zaawansowanych mechanizmów bezpieczeństwa cyfrowego, które obejmują w szczególności szyfrowanie, hardening, uwierzytelnianie operacji krytycznych, wielowarstwową strukturę zabezpieczeń oraz walidację certyfikatów.

Do komunikacji z integrowanymi systemami po sieci Ethernet powinna być wykorzystywana wyłącznie wydzielona sieć LAN, dedykowana dla systemów zabezpieczeń technicznych. Zaleca się szyfrowanie kanałów komunikacyjnych co najmniej algorytmem AES-128 lub wykorzystanie szyfrowanych protokołów SSL.



Zdalna komunikacja z systemem po łączach radiowych powinna być realizowana wyłącznie poprzez bezpieczne kanały VPN. Rozwiązania „Cyber security” w koncentratorach są oparte na rekomendacjach ENISA, NIST, BDEW, BlueCrypt, a implementacja bezpieczeństwa jest zgodna z PN-EN 62351, IEEE P1686, PN-ISO/IEC 27001, BDEW White Paper „Requirement for Secure Control and Telecommunication Systems”. Do zapewnienia bezpieczeństwa serwerów i stacji roboczych wykorzystywane są mechanizmy ochrony dostępne w systemach operacyjnych Windows.

## **BADANIA I CERTYFIKACJA**

W 2014 r. został wdrożony Komputerowy System Nadzoru i Sterowania ARGUS RV dedykowany dla sterowania i wizualizacji systemów ochrony przeciwpożarowej, który przeszedł pozytywnie badania w laboratorium CNBOP-PIB i uzyskał aprobatę techniczną, certyfikat zgodności i świadectwo dopuszczenia.

Od sierpnia 2018 r. system ten dostępny jest pod nazwą Argus RV-C.

W 2019 r. w systemie wprowadzono zmiany, które są potwierdzone aktualnymi dokumentami certyfikacyjnymi:

- Krajową oceną techniczną CNBOP-PIB-KOT-2018/0057 wydanie 2,
- Krajowym certyfikatem stałości własności użytkowych Nr 063-UWB-0110 wydanie 2,
- Świadectwem dopuszczenia NR 3328/2018.

W 2016 r. system ARGUS RV otrzymał Świadectwo kwalifikacyjne TECHOM (Nr 02/16) urządzenia alarmowego klasy „S”.

## APLIKACJE REFERENCYJNE

Platforma ARGUS RV została wdrożona do integracji i zarządzania systemami zabezpieczeń technicznych dla wielu obiektów na terenie całego kraju.

Duża część z nich to rozległe i rozproszone obiekty z infrastrukturą krytyczną, dla których zastosowano rozbudowaną, hierarchiczną strukturę systemu z nadzorem lokalnym oraz zdalnym w centrach zarządzania bezpieczeństwem.

Oprogramowanie Argus RV znalazło też zastosowanie w systemie monitoringu urządzeń radionawigacyjnych, radiolokacyjnych i radiokomunikacyjnych Polskiej Agencji Żeglugi Powietrznej z centrum nadzoru w Warszawie, obejmującym obecnie nadzór ponad 130 obiektów odpowiedzialnych za bezpieczeństwo lotów.

Osobną grupę zastosowań stanowią aplikacje oprogramowania ARGUS RV w zintegrowanych systemach technicznej ochrony jednostek wojskowych, zgodne z wymaganiami Normy Obronnej NO-04-A004:2016.

## ZESTAWIENIE PODSTAWOWYCH CECH OPROGRAMOWANIA ARGUS RV

- Zgodność ze standardem PSIM (Physical Security Information Management)
- Sieciowa architektura oprogramowania systemu typu klient-serwer
- Możliwość tworzenia rozproszonych, hierarchicznych i redundantnych struktur wieloserwerowych
- Działanie na systemach operacyjnych Windows Server 2016, Windows 7, Windows 2010 i Linux
- Współpraca z bazą danych Oracle oraz MySQL
- Praca w czasie rzeczywistym z rozdzielczością czasową do 1 ms
- Funkcjonalność SCADA dla automatyki przemysłowej i BMS
- Wsparcie dla obsługi procedur bezpieczeństwa oraz zarządzania informacją o zasobach służb ochrony
- Rejestracja wszystkich zdarzeń w dzienniku operatorskim
- Rejestracja wartości pomiarowych oraz ich prezentacja na wykresach
- Wykorzystanie sekwencji sterowniczych do sterowania grupami elementów
- Możliwość definiowania sygnałów przy wykorzystaniu formuł logicznych

- Graficzny interfejs użytkownika wspierający pracę z wieloma monitorami oraz ze ścianą graficzną
- Wektorowa prezentacja stanu wszystkich nadzorowanych elementów na mapach
- Możliwość płynnej zmiany skali map z automatycznym przełączaniem pomiędzy różnymi warstwami szczegółowości (decluttering)
- Wyszukiwanie elementów na mapie z poziomu dziennika zdarzeń
- Obsługa map cyfrowych z GPS - możliwość śledzenia lokalizacji osób i pojazdów
- Możliwość zintegrowania z systemami łączności przewodowej i radiowej służb ochrony
- Wyświetlanie obrazów z wybranych kamer CCTV
- Pełna integracja z systemami CCTV i VMS różnych producentów
- Zaawansowane mechanizmy konfigurowania raportów
- Zaawansowane funkcje zarządzania uprawnieniami użytkowników
- Możliwość nadzoru pracy operatorów lokalnych oraz dynamicznego przejmowania uprawnień przez operatorów nadrzędnych
- Możliwość wykorzystania sprzętowych koncentratorów interfejsów i danych ze zintegrowanym systemowo oprogramowaniem i wbudowanymi modemami Możliwość realizacji nadzoru nad działaniem sieci teleinformatycznej i innych urządzeń z protokołem SNMP
- Komunikacja systemowa po protokołach DNP3 i IEC-104 z możliwością szyfrowania
- Testowanie w zakresie cyber-bezpieczeństwa
- Możliwość konfigurowania aplikacji przez użytkownika
- Skalowalność i elastyczność konfiguracji
- Możliwość szybkiego dostosowania do indywidualnych potrzeb użytkowników
- Możliwość zintegrowania z sieciowym oprogramowaniem ARGUS WEB oraz z modułami oprogramowania ARGUS CCTV i ARGUS KD
- Certyfikacja i świadectwo dopuszczenia CNBOP-PIB w ramach systemu ARGUS RV-C
- Zgodność z Normą Obronną NO-04-A004:2016

