

SPECYFIKACJA SYSTEMU MONITORINGU WIZYJNEGO (VMS)

Poniższa specyfikacja została opracowana na podstawie wymagań dotyczących systemu wizyjnego (CCTV) wraz z serwerem rejestrującym. Dokument uwzględnia zarówno część sprzętową (serwer, komponenty sieciowe, obsługę dysków w macierzy RAID), jak i niezbędne funkcjonalności oprogramowania, wymogi bezpieczeństwa (w tym RODO) oraz sposób zarządzania i rejestracji wideo.

1. Architektura i ogólne założenia systemu

1. Typ architektury

- System w technologii IP, bazujący na koncepcji klient–serwer.
- Komunikacja między modułami systemu (serwer–serwer, serwer–klient) oparta na protokole TCP/IP.
- System ma charakter modułowy i skalowalny – możliwa jest dowolna rozbudowa (np. o kolejne kamery, kolejne serwery rejestrujące).

2. Zastosowanie

- Obsługa zarówno nowo projektowanych kamer IP, jak i istniejących kamer IP w obiekcie.
- Centralne zarządzanie i rejestracja obrazu na jednym (lub kilku) serwerach rejestrujących.

3. Wymagania prawne i bezpieczeństwa (RODO)

- Architektura serwer/klient z przechowywaniem materiałów audio-wideo na dedykowanych serwerach w zabezpieczonej serwerowni.
- Szyfrowane połączenia między serwerem a aplikacjami klienckimi (TLS 1.2 / AES-128).
- Eksport nagrań szyfrowany AES-256, z możliwością nadania hasła chroniącego pliki.
- Funkcja „czterech oczu” – do dostępu do pełnej funkcjonalności (materiał nieanonimizowany) wymagane są hasła od dwóch różnych użytkowników lub odpowiednie uprawnienia jednego użytkownika.
- Rozbudowany system logów, rejestrujący wszelkie operacje (podgląd, eksport, potwierdzenia alarmu, zmiany konfiguracji etc.).

4. Integracja z innymi systemami

- Integracja z systemem alarmowym (sterowanie uzbrojeniem/rozbrojeniem, odbiór sygnałów alarmowych).
- Integracja z systemem kontroli dostępu (przełączanie trybów, otwieranie/zamykanie drzwi, potwierdzanie alarmów).
- Możliwość korzystania z sieciowych modułów wejść/wyjść (I/O) i wywoływania scenariuszy alarmowych w oparciu o różne zdarzenia z innych systemów.

2. Wymagania dotyczące kamer i strumieni wideo

1. Technologia IP

- Wszystkie kamery pracują w sieci IP z protokołem TCP/IP.
- Oprogramowanie systemu VMS musi zapewniać otwartą platformę wspierającą kamery IP różnych producentów.

2. Wielostrumieniowość (multi-streaming)

- Każda kamera musi dostarczać trzy niezależne strumienie:

1. Główny (4 Mpx) – do rejestracji w wysokiej rozdzielczości i wyświetlania w trybie pełnoekranowym.
 2. Pierwszy pomocniczy (D1/VGA) – do wyświetlania w wielopodziałach (niższa rozdzielczość).
 3. Drugi pomocniczy (720p) – do podglądu w średniej rozdzielczości / w mniejszych podziałach.
- System automatycznie dobiera odpowiedni strumień w zależności od liczby kamer na ekranie i rozdzielczości monitora.

3. Dynamiczne przełączanie strumieni

- Monitory 4K:
 - 1 kamera – strumień 5/4 Mpx
 - Podział 4–9 kamer – strumień 720p
 - Powyżej 9 kamer – strumień D1/VGA
- Monitory Full HD:
 - 1 kamera – strumień 4 Mpx
 - Podział do 4 kamer – strumień 720p
 - Powyżej 6 kamer – strumień D1/VGA
- W przypadku przeniesienia obrazu z monitora 4K na monitor Full HD (i odwrotnie), system ma dynamicznie przełączać rozdzielczość wyświetlanego strumienia.

4. Parametry rejestracji

- Konfigurowalna rozdzielczość, kompresja, prędkość zapisu, metoda rejestracji (ciągła, harmonogram, detekcja ruchu, wywołanie alarmowe).
- Możliwość definiowania różnych parametrów dla trybu podglądu na żywo i dla trybu zapisu alarmowego/archiwalnego.
- Wszystkie zmiany konfiguracji muszą być automatycznie logowane (co zmieniono, kiedy i przez którego użytkownika).

3. Serwer rejestrujący – wymagania sprzętowe

1. Obudowa i płyta główna

- Serwer w obudowie rack 1U (lub większej, jeżeli projekt zakłada większe wymagania).
- Obsługa min. 4 dysków w kieszeniach typu „Hot Swap”.

2. Procesor

- Minimum 4 rdzenie / 8 wątków, częstotliwość bazowa 3 GHz.
- Cache: min. 8 MB.
- Wydajność min. 12 000 punktów w PassMark CPU.

3. Pamięć RAM

- Min. 16 GB DDR4, częstotliwość 3200 MHz.
- Obsługa architektury wieloprocessorowej oraz wielowątkowości przez oprogramowanie VMS.

4. Dyski

- Dwa dyski systemowe SSD o pojemności min. 480 GB każdy, skonfigurowane w RAID-1.
- Dwa dyski do przechowywania nagrań (HDD SATA/SAS min. 10 TB każdy), również w RAID-1.
- Montaż dysków w kieszeniach „Hot Swap” umożliwiających wymianę bez wyłączania serwera.

5. Karty sieciowe i interfejsy

- Min. 2 × 10/100/1000 Mbit/s.
- 2 × USB 2.0, 2 × USB 3.0, 1 × VGA (lub inny port graficzny w zależności od konfiguracji).

6. System operacyjny

- System serwerowy (Windows Server lub Linux zgodny z wymaganiami producenta VMS).
- Aplikacja VMS ma się uruchamiać w trybie usługi systemowej, automatycznie po restarcie.

7. Czas przechowywania nagrań

- Minimum 30 dni ciągłego zapisu we wskazanej konfiguracji, z uwzględnieniem macierzy RAID-1.

4. Oprogramowanie VMS i funkcje systemu

1. Klient-serwer

- Centralne przechowywanie wszystkich materiałów audio-wideo, logów, konfiguracji i danych użytkowników na serwerze.
- Aplikacja kliencka umożliwiająca pełną konfigurację systemu (kamery, parametry nagrań, alarmy), podgląd na żywo, odtwarzanie archiwum i eksport.
- Zarządzanie użytkownikami oraz ich uprawnieniami za pomocą profili (zróżnicowane funkcje zależnie od roli operatora).

2. Logowanie operacji i autoryzacja

- Logowanie wszelkich zmian konfiguracji, czynności operatorów (wyświetlenie obrazu, eksport, potwierdzenie alarmu, itp.).
- Logowanie przyporządkowane do konta użytkownika.
- Kontrola dostępu do podglądu obrazu z konkretnych kamer oraz możliwości sterowania, w oparciu o nadane uprawnienia.

3. Funkcje alarmowe i detekcja

- Definiowanie zaawansowanych scenariuszy alarmowych, np. aktywacja zapisu z wielu kamer, wysyłanie powiadomień e-mail/SMS/ OPC / SNMP, czy wywołanie sygnału na modułach I/O.
- Obsługa sprzętowej i/lub programowej detekcji ruchu.
- Tworzenie wirtualnych przycisków do sterowania np. barierami, zamkami drzwi, dodatkowym oświetleniem, itp.

4. Integracja z systemami alarmowymi i kontroli dostępu

- Uprawnieni użytkownicy mogą z poziomu oprogramowania VMS uzbrajać/rozbrajać system alarmowy i zarządzać wejściami drzwiowymi.
- Rejestracja w logach wszystkich akcji operatora związanych z alarmami.

5. Anonimizacja i bezpieczeństwo danych

- System musi umożliwiać anonimizację wybranych obszarów nagrania (rozmywanie postaci lub całego tła) – zarówno w podglądzie na żywo (jeśli wspiera to kamera lub moduł VMS), jak i w eksporcie materiału.
- Dostęp do materiału nieanonimizowanego jedynie po podaniu haseł dwóch użytkowników (funkcja „czterech oczu”) lub w ramach specjalnych uprawnień administracyjnych.

6. Funkcje eksportu wideo

- Eksport materiału audio–wideo z poziomu aplikacji klienckiej – pliki zapisywane na serwerze.
- Możliwość tworzenia sekwencji z jednej lub wielu kamer, z różnymi przedziałami czasowymi.
- Nakładanie kształtów (stref rozmycia albo wyróżnienia) na obraz w celu:
 - Zanonimizowania wybranej osoby/obiektu,
 - Rozmycia całego tła i pozostawienia ostrego obrazu wybranego elementu (lub odwrotnie).
- Możliwość definiowania klatek kluczowych (key frames) celem wyliczenia np. prędkości poruszania się obiektu.
- Podpis cyfrowy lub mechanizm weryfikacji integralności pliku wideo, ostrzegający o ewentualnej ingerencji w nagranie.
- Możliwość dołączania nazwy kamery, daty i godziny jako nakładek w eksporcie.
- Szyfrowanie wyeksportowanego materiału (AES-256) i ochrona hasłem, tak aby odtworzenie go wymagało podania właściwego hasła.

7. Automatyczne aktualizacje (centralny serwer aktualizacji)

- Możliwość pobierania i instalowania poprawek/aktualizacji oprogramowania VMS (zarówno części serwerowej, jak i klienckiej) z centralnego serwera aktualizacyjnego.
- Mechanizm planowania czasu instalacji (np. w godzinach nocnych).
- Funkcja automatycznego „rollbacku” w razie niepowodzenia aktualizacji, a następnie powiadomienie administratora.
- Możliwość grupowania serwerów i stacji roboczych w celu seryjnego wdrażania aktualizacji.

8. Redundancja i serwer awaryjny

- System musi zapewniać automatyczne przełączenie się na serwer zapasowy (awaryjny) w przypadku awarii serwera głównego w czasie nie dłuższym niż 2 minuty.
- Po odzyskaniu sprawności przez serwer główny – automatyczna synchronizacja danych wideo i powrót do normalnej pracy.

9. Funkcje dodatkowe

- Praca w trybie wielomonitorowym (np. wyświetlanie kamer i map na wielu ekranach jednocześnie).
- Sterowanie kamerami PTZ (jeśli są zastosowane) przy użyciu manipulatora 3D, joysticka czy wirtualnych przycisków.
- Obsługa jedno- i dwukierunkowej transmisji audio, włącznie z rejestracją dźwięku (o ile kamery i przepisy prawne na to pozwalają).
- Integracja z ewentualnymi systemami analogowymi przez koderki sieciowe, jeśli nadal istnieją takie kamery w obiekcie.

2. Wymagania dla Wykonawcy

Z uwagi na charakter obiektów przegląd i konserwację oraz serwis może prowadzić wyłącznie uprawniona firma instalatorska, która posiada niezbędną wiedzę i doświadczenie, konieczne do prowadzenia skutecznych prac konserwacyjnych i serwisowych tj.:

- 2.1. posiadająca Koncesję MSWiA w zakresie eksploatacji, konserwacji, napraw mechanicznych i elektronicznych systemów zabezpieczeń technicznych,
- 2.2. musi dysponować minimum 2 pracownikami posiadającymi uprawnienia do pracy przy eksploatacji urządzeń, instalacji i sieci elektroenergetycznych do 1 kV kat. D i E
- 2.3. musi dysponować minimum 2 pracownikami posiadającymi licencje pracowników zabezpieczenia technicznego
- 2.4. musi posiadać doświadczenie w okresie ostatnich 5 lat poparte pozytywnymi rekomendacjami użytkowników tych instalacji, potwierdzające wykonanie minimum 2 zadań związanych z montażem lub konserwacją systemu monitoringu wizyjnego CCTV w obiektach, gdzie obowiązuje:
 - a) ustawa z dnia 14 grudnia 2012 r. o odpadach (Dz.U. z 2022 r. poz. 699 z późn. zm.),
 - b) rozporządzenie Ministra Klimatu i Środowiska z dnia 11 maja 2021 r. w sprawie wymagań dla monitoringu wizyjnego miejsc magazynowania odpadów,
 - c) zalecenia Wojewódzkiego Inspektoratu Ochrony Środowiska.
- 2.5. certyfikat z zakresu konfiguracji i obsługi serwisowej oprogramowania QognifyVMS.

1. Główne założenia systemu

1. Przeznaczenie:

- Zabezpieczenie serwerowni (oraz ewentualnie innych pomieszczeń) przed nieuprawnionym dostępem, włamaniem oraz zagrożeniem pożarowym.
- Kontrola dostępu do serwerowni w oparciu o centralę alarmową zintegrowaną z modułem identyfikacji użytkowników.

2. Struktura okablowania:

- Topologia jednomagistralowa (tzw. BUS), w której wszystkie czujki i manipulatory podłączone są do jednego przewodu łączącego się z centralą.
- Magistrala zapewnia zarówno zasilanie, jak i dwukierunkową transmisję danych.

3. Główne elementy zestawu:

- Centrala alarmowa z wbudowanym komunikatorem sieciowym (LAN) i możliwością obsługi dodatkowego modułu GSM/LTE.
- Komunikator LTE (4G) – opcjonalny moduł do przesyłania alarmów i powiadomień za pośrednictwem sieci komórkowych.
- Czujka ruchu PIR (przewodowa, wpięta w magistralę BUS).
- Czujka dymu i temperatury (przewodowa, magistralowa).
- Niezależny czujnik temperatury do ciągłego monitorowania warunków panujących w serwerowni.
- Zintegrowana funkcja kontroli dostępu (np. kod PIN lub karty/breloki zbliżeniowe).

2. Centrala alarmowa

1. Zasilanie i rezerwa:

- Główne: 230 V AC $\pm 10\%$, wbudowany zasilacz 12 V DC do zasilania urządzeń na magistrali.
- Akumulator wewnętrzny (12 V / 2,6 – kilku godzinny czas podtrzymania).

2. Komunikacja sieciowa (LAN):

- Port Ethernet (10/100 Mbps) do zdalnej konfiguracji i monitoringu przez internet.
- Dostępna aplikacja lub panel WWW służące do nadzorowania stanu systemu, przeglądania historii zdarzeń i zarządzania użytkownikami.

3. Obsługa modułu GSM/LTE:

- Działanie w zakresie częstotliwości 4G (zwykle 800/900/1800/2100/2600 MHz).
- Wysyłanie powiadomień (SMS, e-maile, komunikaty PUSH lub połączenia głosowe) w razie wystąpienia alarmu.
- Funkcja automatycznego przełączania się na łączność komórkową przy awarii internetu stacjonarnego (failover).

4. Funkcje alarmowe i partycje:

- Obsługa wielu stref (partycji), co pozwala na niezależne uzbrajanie/rozbrajanie serwerowni i pozostałych obszarów.
- Programowalne reakcje linii wejściowych (natychmiastowe, opóźnione, 24-godzinne).

5. Kontrola dostępu:

- Możliwość rejestrowania użytkowników, nadawania im kodów PIN lub definiowania identyfikatorów zbliżeniowych (karty/breloki RFID).
- Zapis w pamięci centrali wszystkich zdarzeń wejść/wyjść wraz z datą i godziną.

3. Komunikator LTE

1. Przeznaczenie:

- Zapewnienie kanału komunikacyjnego do wysyłania powiadomień w sieciach komórkowych (4G), co pozwala na niezależność od łącza internetowego LAN.
- Współpraca z centralą w zakresie przekazywania alarmów, sterowania zdalnego i autoryzacji użytkowników.

2. Parametry techniczne:

- Obsługa transmisji LTE/3G/2G w powszechnie używanych zakresach częstotliwości.
- Możliwość podłączenia zewnętrznej anteny dla lepszego zasięgu.
- Powiadomienia SMS, ewentualnie połączenia telefoniczne (głosowe) i data push.

4. Czujka ruchu PIR (przewodowa, BUS)

1. Zasada działania:

- Wykrywanie zmian promieniowania podczerwonego w strefie detekcji.
- Zakres detekcji: ok. 10–12 m przy kącie pokrycia do 110° (w zależności od wersji).

2. Parametry elektryczne:

- Zasilanie z magistrali: 12 V DC ($\pm 15\%$).

3. Funkcje dodatkowe:

- Opcja kompensacji temperatury, zapewniająca stabilne działanie w pomieszczeniach klimatyzowanych lub ogrzewanych.
- Stopień ochrony obudowy: najczęściej IP30 (montaż wewnątrz obiektu).

4. Zastosowanie w serwerowni:

- Czujka monitoruje obecność osób po uzbrojeniu alarmu, chroniąc przed nieautoryzowanym wejściem w godzinach, gdy nikt nie powinien przebywać w pomieszczeniu.

5. Czujka dymu i temperatury (przewodowa, BUS)

1. Detekcja optyczna dymu:

- Wbudowany układ optyczny rozpoznający cząsteczki dymu we wczesnej fazie pożaru.
- Czułość zgodna z normami dotyczącymi detektorów ppoż. (np. EN 54-7).

2. Pomiar temperatury (termiczny):

- Progowe wykrywanie wzrostu temperatury do określonego poziomu (np. 60–65°C).
- Możliwość generowania alarmu niezależnie od obecności dymu.

3. Parametry instalacyjne:

- Zasilanie: 12 V DC z magistrali BUS, pobór prądu od 5–15 mA.
- Sygnalizator akustyczny wewnątrz czujki (zazwyczaj 80–85 dB).
- Montaż na suficie serwerowni – w miejscu, gdzie przepływ powietrza umożliwia wczesne wykrycie zadymienia.

4. Przeznaczenie w serwerowni:

- Ochrona sprzętu i infrastruktury IT przed zagrożeniem pożarowym.
- Szybkie ostrzeganie o dymie lub nadmiernym wzroście temperatury, co daje czas na reakcję (gaszenie, wyłączenie urządzeń itp.).

6. Niezależny czujnik temperatury (przewodowy, BUS)

1. Zakres pomiaru:

- Typowo: -10°C do $+70^{\circ}\text{C}$, z rozdzielczością $0,1^{\circ}\text{C}$

2. Funkcje alarmowe:

- Definiowane progi alarmu (np. 28°C , 30°C , 35°C) – wywołanie powiadomienia przy przekroczeniu zadanych wartości.
- Możliwość zapisu historii pomiarów w pamięci centrali, do późniejszej analizy.

3. Zastosowanie w serwerowni:

- Ciągłe monitorowanie temperatury w celu kontroli warunków pracy serwerów (awarie klimatyzacji, przegrzewanie sprzętu).
- Powiadomienie administratorów o krytycznych wzrostach temperatury, co pozwala na natychmiastową interwencję.

7. Kontrola dostępu (zintegrowana z centralą)

1. Metody uwierzytelniania:

- Kody PIN wprowadzane na klawiaturze/manipulatorze.
- Identyfikatory zbliżeniowe (karty, breloki RFID).

2. Funkcjonalność:

- Przydzielanie uprawnień dostępu wybranym użytkownikom do strefy serwerowni.
- Możliwość definiowania harmonogramów (np. dostęp w godzinach pracy, w dni robocze).
- Rejestrowanie zdarzeń wejść/wyjść (kto, kiedy, do której strefy).

3. Drzwi serwerowni:

- Wykorzystanie elektrozaczepu, zwory elektromagnetycznej lub innego elektronicznego zamka sterowanego z centrali.
- Opcjonalny czujnik stanu drzwi, sygnalizujący, czy zostały prawidłowo zamknięte.

8. Montaż i konfiguracja

1. Topologia okablowania:

- Pojedyncza magistrała BUS (4-żyłowa lub inna zgodna z zaleceniami) łącząca centralę z urządzeniami peryferyjnymi (czujki, manipulator, moduły dostępu).

2. Instalacja w serwerowni:

- Czujkę dymu i temperatury montuje się na suficie, w miejscu zapewniającym wczesne wykrycie zadymienia.
- Niezależny czujnik temperatury – na wysokości optymalnej do pomiaru (unikanie bezpośrednich źródeł ciepła/chłodu).

- Czujkę ruchu PIR – na ścianie, ok. 2,2 m nad podłogą, tak aby obejmowała obszar wejścia i wnętrze pomieszczenia.

3. Konfiguracja systemu:

- Za pomocą oprogramowania producenta lub panelu WWW (przy wykorzystaniu komunikatora LAN).
- Definiowanie stref i harmonogramów (np. serwerownia zawsze uzbrojona poza wyznaczonymi porami obsługi).
- Ustawianie progów alarmowych dla temperatury, personalizacja powiadomień, przydzielanie uprawnień użytkownikom.

9. Rozbudowa:

- System można rozbudować o dodatkowe czujki (zalania, zbita szyby) czy kolejne moduły dostępu w innych częściach obiektu, jeśli wymaga tego rozwój infrastruktury.

10. Podsumowanie

Wymagany system alarmowy wraz z kontrolą dostępu jest w pełni dopasowany do specyfiki serwerowni. Wykorzystuje on:

- Centralę z wbudowanym komunikatorem sieciowym, gotową do współpracy z dodatkowym modulem LTE,
- Czujkę ruchu PIR do detekcji intruzów,
- Czujkę dymu i temperatury do wczesnego wykrywania pożaru,
- Niezależny czujnik temperatury zapewniający ciągłe monitorowanie warunków wewnątrz pomieszczenia,
- Zintegrowaną kontrolę dostępu (z kodami PIN lub identyfikatorami zbliżeniowymi), która chroni dostęp do serwerowni.

Dzięki temu instalacja chroni zarówno przed nieautoryzowanym wejściem, jak i potencjalnymi awariami środowiskowymi (pożar, przegrzanie). Jednocześnie zapewnia wygodny zdalny nadzór (LAN / GSM/LTE) oraz elastyczność w zakresie konfiguracji uprawnień i sposobu powiadamiania.