

TECHNICZNE ŚRODKI ZABEZPIECZENIA MIENIA

MATERIAŁ POMOCNICZY

opracowany dla potrzeb kursów dla
Kwalifikowanych Pracowników Ochrony
(i jako taki nie stanowiący źródła prawa.)



SOLUTION SM

ul. Amundsena 5B/18
80-288 Gdańsk, Poland

tel: +48 (58) 718 34 59, mobilny: +48 733 50 38 38
e-mail: solution@3net.pl, internet: <http://www.solution.3net.pl>

Opracowanie:

mgr inż. **Marek Szabunio**
Licencja zabezpieczenia technicznego
II stopnia MSWiA nr **0017141**

Autor prosi o niewykonywanie i niepublikowanie nieautoryzowanych kopii opracowania

Gdańsk, wrzesień 2026 r.

SPIS TREŚCI

TECHNICZNE ŚRODKI ZABEZPIECZENIA MIENIA

Podstawa prawna.....	3
Rodzaje Technicznych Środków Zabezpieczenia Mienia.....	3
1. zabezpieczenia i przegrody budowlane.....	3
2. zabezpieczenia mechaniczne.....	3
3. zabezpieczenia elektroniczne.....	3

PODZIAŁ MECHANICZNYCH ZABEZPIECZEŃ MIENIA

SZYBY.....	4
ROLETY.....	4
DRZWI I OKNA.....	5
ZAMKI DRZWIOWE.....	7
SYSTEM KLUCZA.....	8
Przykłady z interwencji do analizy zdarzenia podczas czynności w obiekcie.....	9
SEJFY.....	10
SKARBCE.....	11
Mechaniczne urządzenia zabezpieczające do transportu wartości.....	11

ELEKTRONICZNE URZĄDZENIA ZABEZPIECZAJĄCE

1. Definicja i przeznaczenie.....	12
2. Podział systemów elektronicznych zabezpieczeń technicznych.....	12

SYSTEMY ALARMOWE - budowa i komponenty	12
Podział obiektu na strefy ochrony.....	14
Klasy systemów alarmowych.....	15
Rodzaje czujek alarmowych w podziale na wykrywane zagrożenie.....	15
Monitoring alarmów.....	16
Stacja monitorująca.....	16
Oprogramowanie dla stacji monitorujących i załóg patrolowych.....	17

TELEWIZJA PRZEMYSŁOWA CCTV

Definicja i główne elementy składowe.....	18
Przeznaczenie i zakresy stosowania CCTC.....	19
Przegląd najpopularniejszych kamer stosowanych w monitoringu wizyjnym, codziennej ochronie mienia i osobistej.....	20
Przykład ochrony CCTV obiektu i pól widzenia kamer.....	21
Systemy oprogramowania do kontroli CCTV.....	22
Monitoring wizyjny a bezpieczeństwo danych oraz RODO/GDPR.....	23

KONTROLA DOSTĘPU i SYSTEMY DOMOFONOWE

Opis działania i elementy Systemu Kontroli Dostępu.....	24
Hotelowe systemy zamków na kartę.....	25
Schematy instalacji Kontroli Dostępu i Domofoonowo-Bramofonowej.....	26

SYSTEMY PRZECIWPOŻAROWE

Opis funkcjonalny i składniki systemu.....	27
Rodzaje czujek pożarowych.....	28

SYSTEMY MOBILNE do obserwacji/ochrony tymczasowej

Przykłady zastosowań i funkcjonalności systemów mobilnych.....	29
--	----

TECHNICZNE ŚRODKI ZABEZPIECZENIA MIENIA

ZABEZPIECZENIE TECHNICZNE polega na montażu urządzeń mechanicznych i elektronicznych do ochrony mienia i osób przed zagrożeniami, takimi jak włamanie, pożar, zalanie czy wyciek gazu. Kluczowe elementy to systemy sygnalizacji włamania i napadu (SSWiN), telewizji dozorowej (CCTV), kontroli dostępu (KD) oraz systemy przeciwpożarowe. Systemy te wspierają człowieka w monitorowaniu stanu bezpieczeństwa obiektów i wykrywaniu zdarzeń niepożądanych oraz zapewnianiu bezpieczeństwa.

1. Podstawę prawną stosowania technicznych środków zabezpieczenia mienia (TŚZM) stanowi art.3 ust. 2 ustawy z dnia 22 sierpnia 1997r. o ochronie osób i mienia (Dz. U. z 2020 r. poz. 838).

2. RODZAJE TECHNICZNYCH ŚRODKÓW ZABEZPIECZENIA MIENIA:

- a. **zabezpieczenia i przegrody budowlane** - środki zabezpieczenia mienia utrudniające dostęp osobie niepowołanej do chronionego obiektu, stanowiące jego elementy konstrukcyjne.
- b. **zabezpieczenia mechaniczne** - dodatkowe środki zabezpieczenia utrudniające dostęp osobie niepowołanej do ochranianego mienia.
- c. **zabezpieczenia elektroniczne** - zespół urządzeń wraz ze związaną z nimi instalacją przewodową, światłowodową i radiową.

Podstawowym czynnikiem określenia skuteczności zabezpieczeń, czyli w efekcie bezpieczeństwa chronionego mienia/osób, jest czas pomiędzy naruszeniem systemu ochrony obiektu, a interwencją.

Zabezpieczenia mechaniczne utrudniają i opóźniają działania niepowołane, a zabezpieczenia elektroniczne przyspieszają podjęcie interwencji.

Brak skutecznego opóźnienia działań niepowołanych przez zabezpieczenia mechaniczne może umożliwić sprawcy oddalenie się z łupem szybciej, niż nastąpi interwencja, pomimo prawidłowego zadziałania systemu alarmowego.

Mamy wtedy do czynienia z **przełamaniem systemu ochrony**.

System ochrony, to zespół sumy środków technicznych, organizacyjnych i prawnych, ustanowiony i wdrożony celem uzyskania oczekiwanego poziomu zabezpieczenia.

Warunkiem uzyskania skutecznej i efektywnej ochrony oraz optymalizacji jej kosztów jest wdrożenie właściwego wzajemnego współdziałania systemu zabezpieczeń mechanicznych i elektronicznych, przy zapewnieniu skutecznej interwencji w przypadku zadziałania systemu alarmowego.

PODZIAŁ MECHANICZNYCH ZABEZPIECZEŃ MIENIA:

SZYBY

1. **wzmocnione** po zastosowaniu (oklejeniu) folii o grubości 360-700 mikronów (odporne na uderzenie młotka) oraz szyby:

- hartowane
- hartowane - emaliowane
- wielowarstwowe:
 - klejone
 - klejone - ognioodporne

2. **ochronne, antywłamaniowe** o zwiększonej odporności na włamanie, czyli rozbicie – Norma

PN-EN356 „Szkło ochronne. Badania i klasyfikacja na ręczny atak”.

P1A do P5A - testowane upadkiem kuli 4.11 kg.

P6 do P8B - testowane siekierą

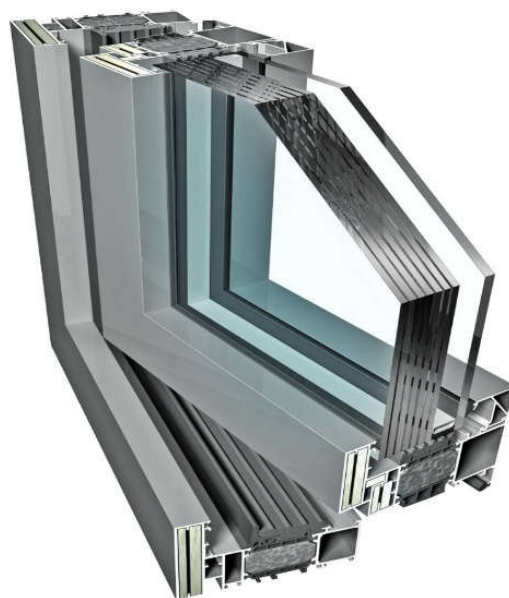


3. **odporne na ostrzał z broni palnej** - kuloodporne – testowane wg europejskiej normy **EN-1063** pod kątem odporności na uderzenia pocisków wystrzelonych z pistoletów, karabinów lub strzelb:

BR1 do BR7 - testowane pod kątem skuteczności przeciwko ostrzałowi z broni palnej (pistoletów, karabinów lub strzelb)

SG1 do SG2 - testowane pod kątem skuteczności przeciwko ostrzałowi ze strzelby.

W tej normie "**S**" oznacza możliwość wystąpienia odprysków szyby po stronie użytkownika, podczas gdy "**NS**" oznacza, iż odpryski nie występują w ogóle.



4. **odporne na działanie fal detonacyjnych** (antywybuchowe) wg normy **PN-EN 13541:2012** – klasyfikują się do czterech kategorii zależnie od ciśnienia fali detonacyjnej i czasu trwania impulsu: **ER1**, **ER2**, **ER3** oraz **ER4** - od podstawowej do najwyższej odporności.

ROLETY

Klasy odporności rolet, określone europejską normą **PN-EN 1627**, dzielą się na sześć kategorii w zależności od odporności na próby włamania:

- **RC1** - ochrona przed przypadkowymi próbami włamania, np. kopaniem, szarpaniem czy podnoszeniem.
- **RC2** - ochrona przed próbami włamań z użyciem prostych narzędzi.
- **RC3** - odporność na użycie narzędzi takich jak łom.
- **RC4** - ochrona przed doświadczonymi włamywaczami z użyciem takich narzędzi jak młotek, siekiera, dłuto czy wiertarka akumulatorowa.
- **RC5** - ochrona przed profesjonalnymi włamywaczami używającymi elektronarzędzi, np. wiertarki, wyrzynarki czy szlifierki kątovej z tarczą do 125mm.
- **RC6** - najwyższa klasa, odporność na użycie cięższych elektronarzędzi, jak wiertarka czy szlifierka z tarczą do 230mm.

DRZWI I OKNA

Klasyfikację **zamknięć i otworów oszklonych** (drzwi, okna) określają normy prawne krajowe i europejskie przeszklenia szyb **PN-EN 356:2000**:

- **klasa P1-P2** - chroni użytkownika przed zranieniem się, utrudnia rozbicie wskutek np. przeciągu, a także stanowi czasową barierę w przypadku włamania bez przygotowania,
- **klasa P3-P4** - utrudnia włamanie,
- **klasa P5-P6** - posiada zwiększoną odporność na włamanie,
- **klasa P7-P8** - jest wysoce odporna na włamania.

Norma **PN-EN 1627** dzieli **drzwi zewnętrzne** na sześć klas odporności na włamanie, oznaczając je symbolem RC (resistance class):

- **Klasa RC 1** - oznacza niski poziom zaangażowania włamywacza w próby sforsowania drzwi. Przez drzwi należące do tej klasy można włamać się bez szczególnych przygotowań, z użyciem jedynie siły fizycznej lub bardzo prostych narzędzi (można sforsować je poprzez kopnięcie, uderzenie barkiem, podniesienie na zawiasach, wyrwanie, itp.), co trwa zaledwie chwilę.
- **Klasa RC 2** - poziom zaangażowania włamywacza nadal jest niski, a wiedza na temat potencjalnych łupów znikoma. Do sforsowania takich drzwi zwykle dochodzi bez uprzedniego przygotowania. Przestępcy posługują się przeważnie prostymi narzędziami typu: młotek, śrubokręt, obcęgi, klin, itp. Drzwi klasy RC 2 (zgodnie z badaniami) opierają się forsującemu przez zaledwie 3 minuty.



drzwi klasy RC1/RC2 sforsowane akumulatorową „flexą”

- **Klasa RC 3** - włamywacz musi wykazać średni poziom zaangażowania. Musi się również liczyć ze średnim poziomem ryzyka. Dlatego też posiadając wiedzę na temat odporności drzwi, liczy się z czasem i hałasem, który wygeneruje w trakcie podejmowania prób ich sforsowania. Drzwi klasy RC 3 najczęściej wyłamuje się za pomocą stalowego łomu oraz przy użyciu mechanicznej wiertarki i innych prostych narzędzi dodatkowych. Opór trwa tu 5 minut.
- **Klasa RC 4** - sforsowanie drzwi wymaga uprzedniego przygotowania do skoku. Konieczne są narzędzia, które pozwolą włamywaczowi zaatakować przeszkodę (typu wiertarka, piła, przecinak, dłuto, siekiera, duży młotek, czy szlifierka kąтова).

Drzwi tej klasy niszczy się w przekonaniu o osiągnięciu wymiernych korzyści z włamania i przy stosunkowo wysokim poziomie ryzyka. Walka z nimi może trwać 10 minut.

- **Klasa RC 5** – udanego włamania może dokonać tylko doświadczona i dobrze przygotowana osoba. Do sforsowania drzwi potrzebne są elektronarzędzia typu wiertarko-wkrętarka, szlifierka kąтова lub piła mechaniczna, a włamywacz podejmuje w tym przypadku wysokie ryzyko związane z hałasem, generowanym podczas działania. Sforsowanie tych drzwi możliwe jest nie szybciej niż w 15 minut.
- **Klasa RC 6** - drzwi o najwyższym stopniu odporności na włamanie. Do ich pokonania potrzeba przynajmniej 20 minut czasu. Niezbędne są również profesjonalne elektronarzędzia o wysokiej mocy. Takie drzwi jest w stanie sforsować wyłącznie doświadczony i doskonale przygotowany włamywacz. Włamanie do mieszkania z takimi drzwiami jest obarczone wysokim ryzykiem ujawnienia z powodu konieczności wygenerowania długotrwałego, intensywnego hałasu przy próbie ich sforsowania.



drzwi wzmocnione klasy RC3/RC4 po próbie sforsowania maczetą



drzwi wzmocnione klasy RC3/RC4 sforsowane przez wylamanie

ZAMKI DRZWIOWE - norma europejska **EN 12209**, określa podział na klasy bezpieczeństwa zamków i wkładek:

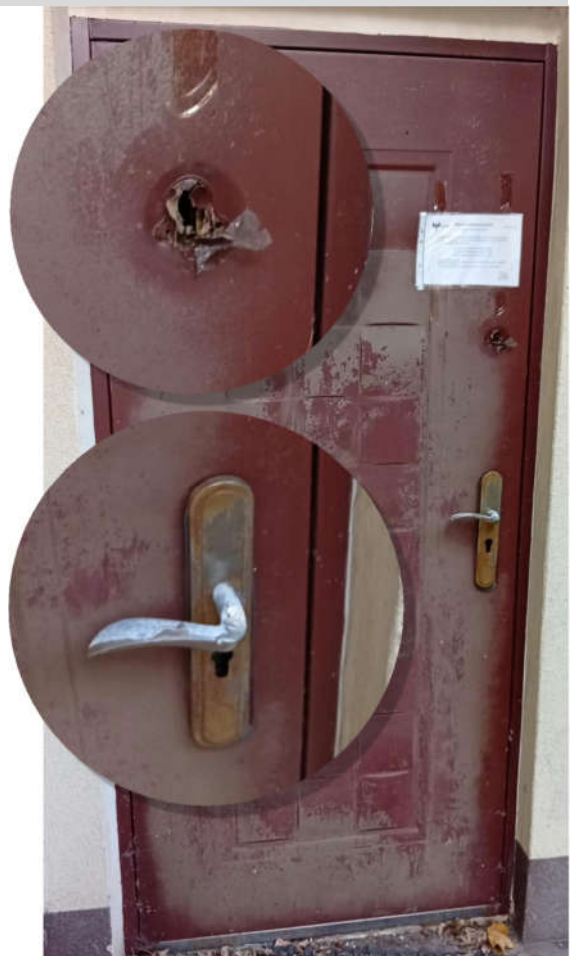
- **Klasa 1 – podstawowe zabezpieczenie** - zamki tej klasy oferują podstawową ochronę przed nieuprawnionym dostępem i są zwykle stosowane w drzwiach wewnętrznych lub miejscach o niskim ryzyku włamania.
- **Klasa 2 i 3 – średnie zabezpieczenie** - zamki te są bardziej odporne na włamanie i często stosowane w drzwiach zewnętrznych mieszkań i domów jednorodzinnych. Zapewniają lepszą ochronę przed narzędziami wykorzystywanymi do łamania lub przecinania.
- **Klasa 4 i 5 – wysokie zabezpieczenie** - zamki tej klasy dedykowane są dla obiektów wymagających wyjątkowo wysokiego poziomu bezpieczeństwa, jak banki czy sklepy jubilerskie. Zapewniają one ochronę przed zaawansowanymi metodami włamania, w tym użyciu specjalistycznych narzędzi.
- **Klasa 6 – maksymalne zabezpieczenie** - najwyższa klasa zabezpieczeń, stosowana w miejscach o krytycznym znaczeniu bezpieczeństwa, gdzie ryzyko ataków jest bardzo wysokie.

Zamki te są projektowane tak, aby oprzeć się nawet najbardziej zaawansowanym próbom sforsowania.

odpowiedni dobór drzwi oraz zamków potrafią powstrzymać nawet intensywne próby ich wyłamania



drzwi RC 4 po intensywnej i długotrwałej próbie wyłamania łomem.



drzwi z zamkami klasy 4/5 zablokowane po wyłamaniu wkładek

A photograph showing a large quantity of electronic components, specifically capacitors, arranged in rows on a wooden surface. The components are organized into two main rows of gold-colored capacitors, each with a blue component attached to its base. Below these rows, there are several small plastic bags containing additional components, and a few loose components are scattered on the surface. The components are arranged in a neat, organized manner, suggesting they are being prepared for assembly or testing.

Podczas projektowania systemu należy uwzględnić i przewidzieć (czasem nadmiarowo) docelową ilość wkładek i ich przeznaczenia funkcjonalnego, gdyż po wykonaniu gotowego systemu przez producenta, zmiany praktycznie

mgr inż. Marek Szabunio
L. 0017141

Gdańsk, dn. 15-09-2023r.

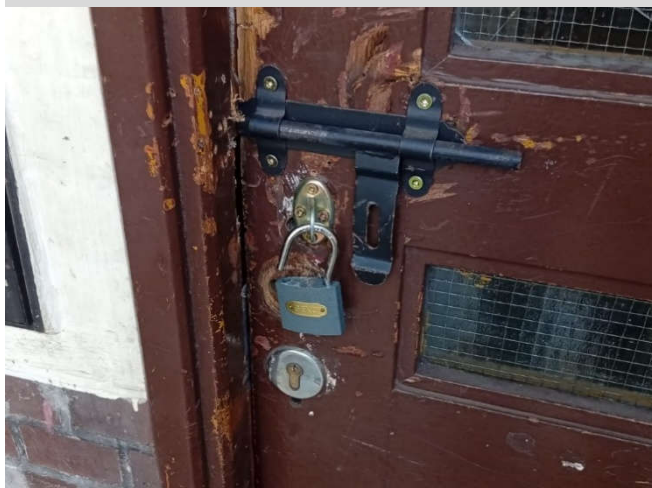
[illegible]

* Wkładki i klucze proszę opisać w sposób jednoznaczny, wybitym numerem klucza na wkładce lub zgodnie z numerem niniejszej Specyfikacji

^{**} System musi umożliwiać ewentualną rozbudowę o kolejne wkładki i klucze funkcyjne w przyszłości.

Z powyższego powodu **zaleca się unikanie oznaczania kluczy** (zwłaszcza funkcyjnych oraz właścicielskich) zawieszkami, czy **brelokami** z rzeczywistym **opisem** ich **przeznaczenia**, czy **logiem firmy**, pozwalającym na jednoznaczną lokalizację i identyfikację przejść chronionych utraconym kluczem.

Przykładowe zdjęcia z interwencji do analizy zdarzenia i podjęcia adekwatnych decyzji i środków bezpieczeństwa podczas czynności w obiekcie:



zerwana kłodka z dystansu maskująca włamanie, zasuwa otwarta – sprawcy mogą nadal być wewnątrz obiektu



zerwana kłodka, zasuwa zamknięta – obiekt bezpieczny, choć sprawcy zapewne planują powrót



drzwi otwarte przez zniszczenie zamka, w napadzie szalu zmasakrowane siekierą – sprawca nadal może przebywać wewnątrz obiektu



obiekt powłamaniony prowizorycznie zabezpieczony przez załogę patrolową podczas interwencji

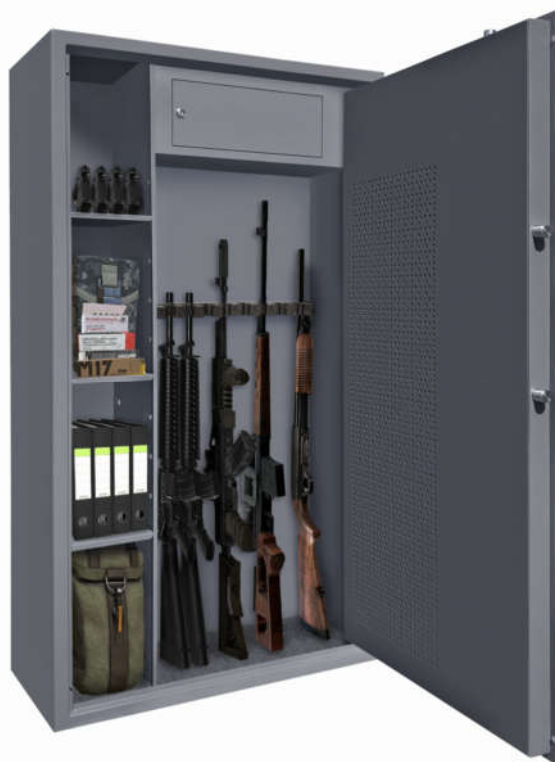


SEJFY

znane również jako kasy pancerne, to zamykane, wytrzymałe metalowe szafy lub skrzynie do bezpiecznego przechowywania wartościowych przedmiotów, takich jak pieniądze, obligacje, biżuteria, dokumenty, nośniki danych oraz broń i inne niebezpieczne przedmioty lub substancje - (słowo „sejf” pochodzi od angielskiego „safe”, czyli bezpieczny).



Klasy bezpieczeństwa sejfów określają poziom ochrony przed włamaniem, zgodny z normami europejskimi, takimi jak **PN-EN 14450** (klasy S1, S2) oraz **PN-EN 1143-1** (klasy od 0 do XIII):



Klasy S1 i S2 (wg PN-EN 14450):

- zapewniają podstawową ochronę przed włamaniem, odpowiednią dla przechowywania broni palnej i mniejszych wartościowych przedmiotów.
- są to zwykle sejfy o konstrukcji jednościennej.
- posiadacze broni palnej muszą posiadać sejf co najmniej klasy S1.

Klasy od 0 do XIII (wg PN-EN 1143-1):

- oferują znacznie wyższy poziom odporności na włamanie niż S1 i S2.
- każda kolejna klasa oznacza wyższą wytrzymałość na próby włamania.
- do przechowywania dokumentów, gotówki i cennych przedmiotów oraz biżuterii.

Warto sprawdzić, czy sejf posiada dodatkowe certyfikaty dotyczące ochrony przed ogniem, takie jak normy **EN 15659** (ochrona papieru) lub **EN 1047-1** (ochrona nośników elektronicznych).



SKARBCE

Skarbiec to pomieszczenie specjalne, przeznaczone do długookresowego przechowywania gotówki w bankach i innych instytucjach finansowych, skonstruowane ze specjalistycznych elementów lanych monolitycznych lub modułowych.



Nowoczesne skarbce wykonane są z żelbetu zbrojonego stalą i wyposażone w skomplikowane mechanizmy blokujące oraz systemy zabezpieczeń.

W przeciwieństwie do sejfów, należących do zabezpieczeń mechanicznych, skarbce są integralną częścią struktury budynku, w którym są zbudowane (oraz jego fundamentów), należy więc uznać je za zaawansowane zabezpieczenia budowlane.

Zgodnie z normą **PN-EN 1143-1+A1:2009**, dzielą się na klasy **V, VI, IX, XI**.

MECHANICZNE URZĄDZENIA ZABEZPIECZAJĄCE TRANSPORT WARTOŚCI:

- samochody do przewozu wartości
- pojemniki do przewozu wartości
- teczki do przewozu wartości wyposażone wariantowo w:
 - systemy odstraszańco-sygnalizujące
 - generatory dymu - dla wskazania drogi ucieczki
 - barwienie banknotów - aby były bezużyteczne
 - porażające - generator wysokiego napięcia
 - lokalizator GPS w celu śledzenia drogi przewozu wartości

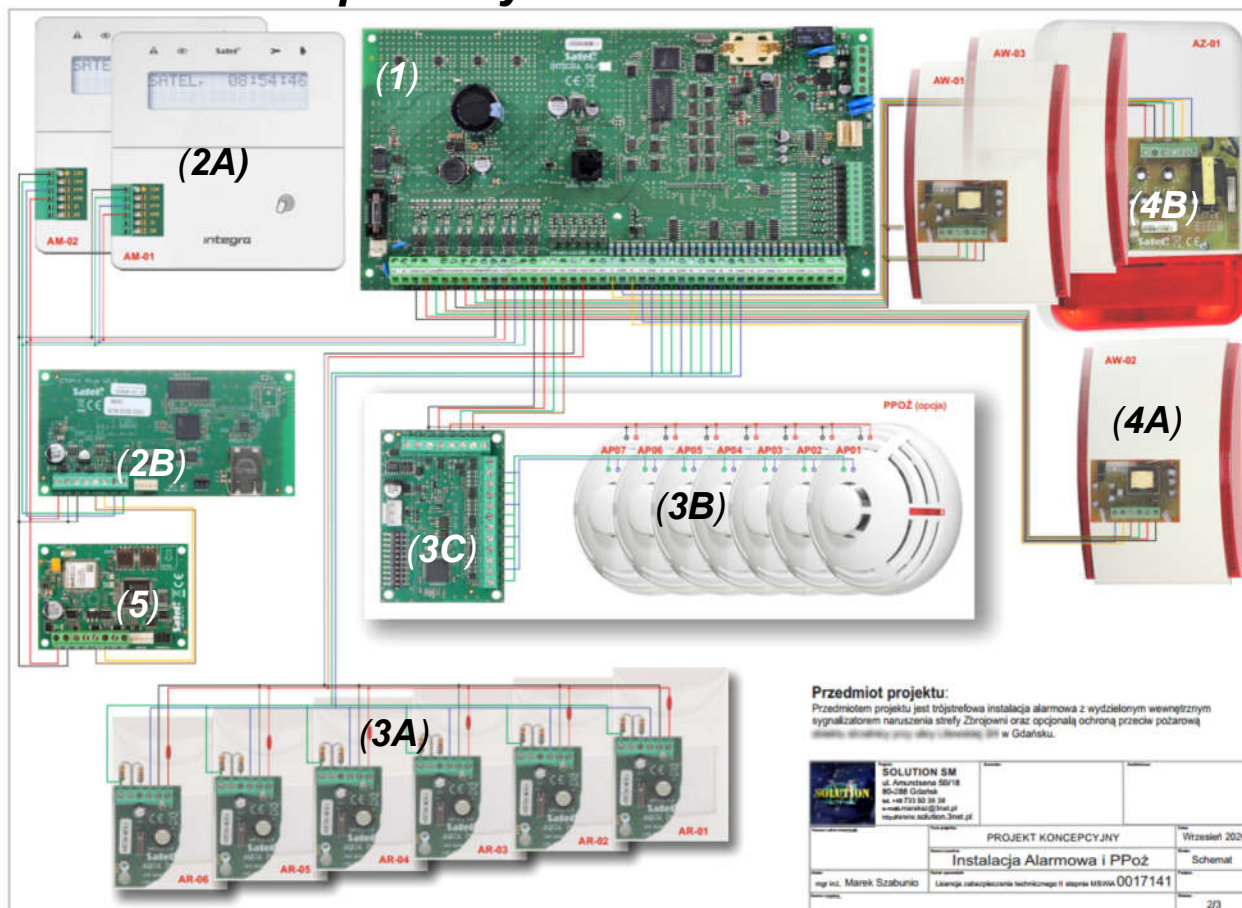




ELEKTRONICZNE URZĄDZENIA ZABEZPIELAJĄCE

1. Elektroniczne systemy zabezpieczające to zespoły urządzeń i związanych z nimi instalacji przewodowych, światłowodowych lub innych, służące do ochrony mienia i osób przed zagrożeniami, wspierając człowieka w bieżącym monitorowaniu i wykrywaniu niepożądanych zdarzeń oraz zapewnianiu bezpieczeństwa.
2. Podział systemów elektronicznych zabezpieczeń technicznych:
 - **systemy alarmowe (SSWiN)** - wykrywają zagrożenia, takie jak próby włamania lub napadu, za pomocą czujników (np. ruchu, zbitcia szyby) oraz uruchamiają sygnalizatory dźwiękowe lub świetlne.
 - **systemy telewizji dozorowej (CCTV)** - wykorzystują kamery do monitorowania oraz nagrywania zdarzeń, często z wykorzystaniem zaawansowanej analityki obrazu przez AI i integracji z innymi systemami bezpieczeństwa.
 - **systemy kontroli dostępu (KD)** - umożliwiają dostęp do wybranych obszarów wyłącznie osobom uprawnionym, np. za pomocą kart lub breloków zbliżeniowych, kodów dostępu lub biometrii.
 - **systemy przeciwpożarowe (PPOŻ)** - obejmują systemy wykrywania pożaru (czujniki dymu, temperatury, gazów) oraz systemy gaśnicze (np. zraszacze) i oddymiania, które pomagają w ewakuacji oraz ograniczaniu strat.
 - **systemy wykrywania gazów** - detektory wykrywają niebezpieczne stężenia gazów (np. czadu) w pomieszczeniach, uruchamiając alarm oraz systemy wentylacyjne.
 - **systemy zarządzania budynkiem (BMS) i inteligentne systemy bezpieczeństwa (PSIM)** - integrują różne systemy bezpieczeństwa (alarmy, kontrolę dostępu, klimatyzację, instalację ppoż oraz sterowanie windami i bramami garażowymi) w jednym miejscu, co ułatwia zarządzanie i reagowanie na zdarzenia.

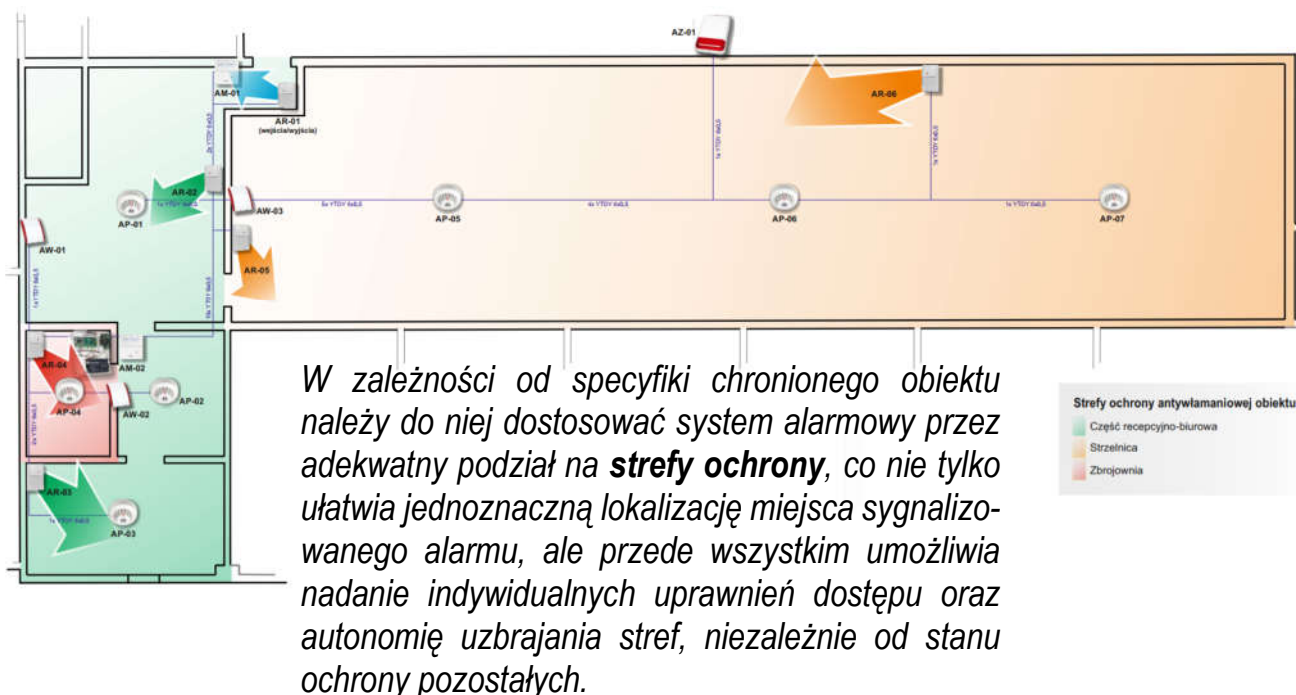
Budowa i komponenty SYSTEMU ALARMOWEGO:



1. płyta główna centrali alarmowej (1) – integrująca wszystkie podzespoły systemu i sterująca całą procesem ochrony oraz uprawnieniami dostępu w zaprogramowanych strefach.
2. manipulatory (2A) i interfejsy komunikacyjne (2B) – umożliwiające lokalne oraz zdalne sterowanie stanem centrali alarmowej i jej programowanie.
3. czujki ruchu PIR (3A), pożarowe (3B) i czujniki otwarcia (kontaktrony), podłączone do płyty głównej (bezpośrednio lub za pomocą dodatkowych modułów rozszerzeń 3C) wykrywają i przekazują centrali sygnały o zagrożeniach.
4. sygnalizatory akustyczno-optyczne (4) służą do lokalnej sygnalizacji wykrytego zagrożenia w chronionym obiekcie i jego bezpośrednim otoczeniu.
5. moduły komunikacyjne i powiadomiania służą do przekazywania sygnału o zagrożeniu na zewnątrz – poprzez transmisję GSM (5) oraz internetem (2B) do Centrów Monitoringu lub zdalnych pomieszczeń ochrony obiektu.

Rolą systemu alarmowego jest powiadomianie o zaistniałym zagrożeniu lokalnie (poprzez sygnalizatory akustyczne) oraz w miejscu, w którym może być uruchomiona interwencja (poprzez moduły komunikacyjne).

Podział obiektu na strefy ochrony:



Rysunek powyżej przedstawia instalację alarmową przykładowej strzelnicy, podzielonej na 3 strefy ochrony: część recepcyjno-biurową, tory strzeleckie oraz magazyn broni. Dostęp do części „zielonej” ma każdy uprawniony do wejścia do obiektu, poprzez identyfikację na manipulatorze wejściowym, natomiast dostęp do strefy „żółtej” wymaga uprzedniego rozbrojenia strefy przez osobę uprawnioną, a otwarcie drzwi strefy „czerwonej” jest możliwe wyłącznie po każdorazowym jej rozbrojeniu autoryzacją uprawnień dostępu na manipulatorze. Strefy „żółta” i „czerwona” mogą być uzbrojone, niezależnie od stanu strefy „zielonej”, natomiast czujniki ppoż w całym obiekcie działają zawsze, niezależnie od stanu poszczególnych stref.

Czujnik ruchu na wejściu do obiektu („błękitny”) ma status „wejścia/wyjścia”, czyli zapewnia określony czas (zwykle 20-30s) na autoryzację/rozbrojenie strefy „zielonej” przy wejściu do obiektu oraz na opuszczenie go i zamknięcie drzwi wejściowych po uzbrojeniu systemu. Pozostałe czujniki nie mają zwłoki czasowej i w stanie uzbrojenia alarmują natychmiast po wykryciu ruchu. Manipulator strefy „czerwonej” jest na zewnątrz przed drzwiami strefy, więc zwłoka czasowa byłaby bezzasadna, wręcz niebezpieczna w przypadku np. pozostawienia klucza w zamku drzwi. Strefa „czerwona” ma własny sygnalizator akustyczno-optyczny, pozostałe sygnalizatory wewnętrzne służą ostrzeganiu personelu i gości przed ewentualnymi zagrożeniami ppoż.

Klasy systemów alarmowych, znane jako „stopnie zabezpieczenia” (ang. Grade), określają poziom ryzyka, przed którym system ma chronić, zgodnie z normą **PN-EN 50131-1** :

- **Grade 1** - instalacja o niskim stopniu ryzyka - stosuje się kiedy ryzyko włamania jest znikome. Najczęściej wyposaża się w nie mieszkania i domy jednorodzinne. W przypadku tej klasy domniemany intruz nie będzie posiadał wiedzy o systemach alarmowych, a przy pokonywaniu systemu będzie używał podstawowych narzędzi.

- **Grade 2** - instalacja o niskim lub średnim stopniu ryzyka - wykorzystuje się miejscach o średnim stopniu ryzyka. Zakładamy, że potencjalny intruz ma podstawową wiedzę na temat systemów alarmowych. Rozwiązanie to oferowane jest, gdy istnieją podejrzenia, że włamywacz może korzystać z szerokiej gamy narzędzi ogólnodostępnych.
- **Grade 3** - instalacja o średnim lub wysokim stopniu ryzyka - znajduje zastosowanie w miejscach, gdzie potencjalny intruz posiada ponadprzeciętną wiedzę na temat systemów alarmowych oraz ma dostęp do specjalistycznych narzędzi służących do rozbrojenia systemu. Najczęściej stosuje się go w obiektach o średnim i wysokim ryzyku, takich jak instytucje publiczne.
- **Grade 4** - instalacja o wysokim stopniu ryzyka - zakłada, że potencjalny intruz posiada obszerną wiedzę o systemach alarmowych oraz zna specjalistyczne narzędzia, zatem zakłada się, że będzie w stanie dokładnie zaplanować napad na obiekt, zaczynając od dezaktywacji urządzeń informujących, a kończąc na dezaktywacji samej centrali alarmowej. Stopień ten jest konieczny do zabezpieczenia obiektów takich jak: banki, muzea, galerie, czy inne miejsca wyposażone w cenne przedmioty bądź dokumenty.

Rodzaje czujek alarmowych w podziale na wykrywane zagrożenie:

- **czujki ruchu** (PIR, mikrofalowe, dualne), wykrywające obecność intruza;
- **czujki dymu i gazu** (w tym czujki czadu/tlenku węgla), które reagują na zagrożenie pożarowe lub wyciek gazu;
- **czujki otwarcia i zbitcia szyby** (magnetyczne, wstrząsowe), monitorujące dostęp do obiektu lub jego integralność;
- **czujki zalania**, chroniące zbiory muzealne, dokumentację oraz sprzęt elektroniczny przed zniszczeniem bądź uszkodzeniem.

CZUJKI RUCHU:

- **PIR** (pasywne czujniki podczerwieni) - wykrywają zmiany temperatury, np. ciepło ciała w polu widzenia czujki.
- **Mikrofalowe** - emitują i odbierają fale elektromagnetyczne, alarmując, gdy odbite fale zakłóci poruszający się obiekt.
- **Dualne** - łączą technologię podczerwieni i mikrofalową, wymagając spełnienia dwóch warunków do aktywacji alarmu, co znacząco redukuje liczbę fałszywych alarmów.



CZUJKI POŻAROWE I GAZU:

- **Czujki dymu** - wykrywają cząsteczki dymu we wczesnych etapach pożaru, emitując sygnał akustyczny.
- **Czujki gazu** - monitorują stężenie niebezpiecznych gazów, takich jak gaz ziemny, który może prowadzić do wybuchu.
- **Czujki czadu** - reagują na stężenie śmiertelnie niebezpiecznego tlenku węgla.



CZUJKI OTWARCIA I WIBRACJI:

- **Czujki magnetyczne** - składają się z dwóch magnesów; rozłączenie czujki sygnalizuje otwarcie drzwi lub okna.
- **Czujki wstrząsowe** - wykrywają wibracje podłoża i są stosowane do wykrywania próby zbitcia szyby.



Lokalne alarmowe systemy obiektowe, wykrywające zagrożenia i zdarzenia niepożądane w obszarach swoich stref ochrony, informują o ich zaistnieniu sygnalizatorami optyczno-akustycznymi wewnątrz i na zewnątrz obiektu, ostrzegając personel, ewentualny dozór i wręcz przechodniów o sytuacji zagrożenia w obiekcie, a odpowiednio zaprogramowane potrafią również informować właścicieli, osoby upoważnione lub/i profesjonalne agencje ochrony.



MONITORING ALARMÓW - to zbieranie za pomocą łączy teletransmisyjnych, radiowych i internetowych oraz specjalistycznego oprogramowania informacji o stanie oddalonych, niezależnych od siebie obiektowych systemów alarmowych przez alarmowe centrum odbiorcze zwane **Stacją/Centrum Monitoringu** w celu podjęcia stosownych działań interwencyjnych (przez załogi patrolowe) w przypadku odebrania sygnału alarmu z chronionego obiektu.

STACJA MONITORINGU – to centrum teletransmisyjne, zbierające i analizujące sygnały z ochraniających obiektów (na dowolnie rozległym obszarze), celem podjęcia reakcji, adekwatnej do otrzymanej informacji o zagrożeniu i wysłania najbliższej grupy patrolowej, bądź powiadomienia straży pożarnej i innych służb w lokalizacji danego obiektu.

Stacje monitoringu używają specjalistycznego oprogramowania, dedykowanego do bieżącej obsługi sygnałów zdarzeń napływających z chronionych obiektów i komunikacji z załogami patroli interwencyjnych, przydzielonych do ich weryfikacji oraz ewentualnego podjęcia działań prewencyjnych na miejscu w obiekcie.

TELEWIZJA PRZEMYSŁOWA CCTV:

Telewizja przemysłowa CCTV (ang. Closed Circuit TV) to działający w zamkniętej sieci (niepublicznej) system nadzoru wizyjnego oparty na kamerach i rejestratorach obrazu, dostępny w ramach struktury zabezpieczeń dla określonych urządzeń (stacjonarnych i mobilnych) oraz uprawnionych użytkowników.

Główne elementy systemu CCTV:

- **kamery** – rejestrują obraz (analogowe, IP, obrotowe PTZ, termowizyjne).



kamera analogowa



kamera IP

- **rejestratory (DVR/NVR)** – zapisują nagrania z kamer i umożliwiają ich analizę oraz umożliwiają zdalny dostęp osobom uprawnionym (internet).

analogowe i hybrydy 5w1 4x, 8x i 16 kanałowe.



IP klasyczne i z wbudowanym routingiem PoE



- **monitory i manipulatory** – służą do podglądu obrazu na żywo.
- **okablowanie / sieć** – przewody koncentryczne, skrętka UTP, światłowody lub sieć IP.
- **oprogramowanie** – umożliwia zdalny podgląd, analizę obrazu oraz powiadomienia alarmowe.

Zastosowania CCTV:

- **ochrona obiektów** (sklepy, biura, magazyny, lotniska, banki).
- **monitorowanie przestrzeni publicznej** (ulice, place, transport publiczny).
- **kontrola procesów przemysłowych** (produkcja, logistyka).
- **bezpieczeństwo w budynkach prywatnych** (domy, osiedla).
- **materiał dowodowy w sprawach karnych i wypadkach.**

Cele i zakres stosowania CCTV:

- **wizualna weryfikacja przyczyny alarmu** - monitoring wizyjny
- **nadzór bieżący** - stosowany wszędzie tam, gdzie jest konieczne zapewnienie natychmiastowego reagowania na dynamicznie zmieniającą się sytuację (sklepy, skrzyżowania, dworce w godzinach szczytu)
- **nadzór ciągły** (bezpośredni) - umożliwia zdalną kontrolę, umożliwiając sterowanie różnymi procesami technologicznymi i urządzeniami, jak również umożliwia interaktywny nadzór nad zespołami ludzkimi, klientami supermarketów, widzami na koncertach i czy stadionach, zwłaszcza w sytuacjach zagrożenia, gdy trzeba ich bezpiecznie ewakuować.
- **wideodetekcja** – tryb pracy kamer, w którym reagują one na ruch (zmianę obrazu) w zadanym obszarze pola widzenia, zapisując wykryte zmiany na dysku rejestratora i generując powiadomienie dla operatora.
- **wideoidentyfikacja:**
 - rozpoznawanie numerów rejestracyjnych pojazdów
 - rozpoznawanie twarzy (Face Recognition System)
 - termowizyjna analiza zagrożeń (np. podczas Covid 19)
- **dokumentacja zdarzeń**, umożliwiająca odtworzenie ich przebiegu oraz ewentualną orientację w poczynaniach przestępcy od wtargnięcia, aż do jego bieżącego położenia w obiekcie.

Rodzaje kamer monitoringu CCTV:

- **ze względu na rodzaj przetwarzania i transmisji obrazu:**
 - **kamery IP**, działające w strukturze sieci LAN i WiFi obiektu
 - **kamery analogowe**, wymagające odrębnego okablowania AV
 - kamery z zapisem własnym – nasobne, fotopułapki, rejestratory pokładowe w pojazdach i inne (np. w paralizatorach TASER)
 - **kamery internetowe** z zapisem w chmurze.
- **ze względu na budowę i funkcjonalność:**
 - **kamery tubowe** w obudowach ochronnych
 - **kamery tubowe** kompaktowe
 - **kamery kopułowe**
 - **kamery obrotowe**

- **ze względu wymaganą jakość obrazu w warunkach pracy obiektu:**
 - **kamery o stałej ogniskowej** (dobieranej w fazie projektowania)
 - **kamery zmienno-ogniskowe z MotoZOOM i automatyczną ostrością**
 - **kamery z filtrami kompensacji światła (WDR)**
 - **kamery termowizyjne i inne specjalistyczne**

Przegląd najpopularniejszych kamer stosowanych w monitoringu wizyjnym, w codziennej ochronie mienia i osobistej:



kamery tubowe



kamery obrotowe 360°



kamery kopułkowe



kamery panoramiczne 180°



kamery internetowe



kamery osobiste nosobne

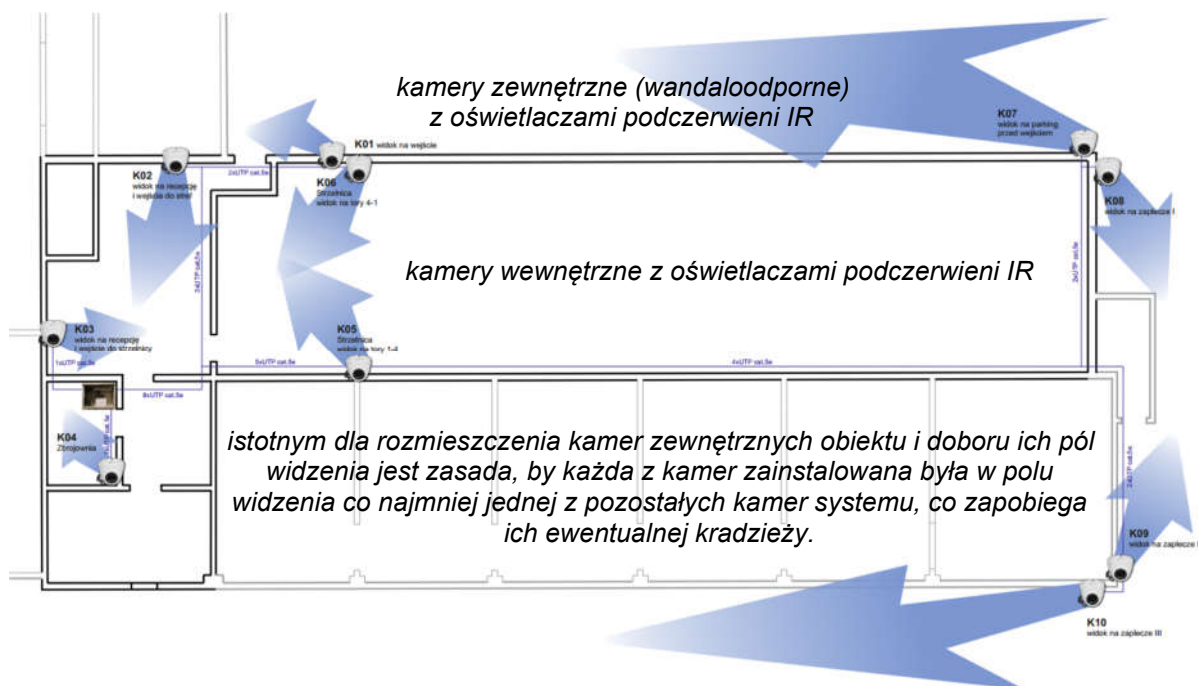


fotopułapki

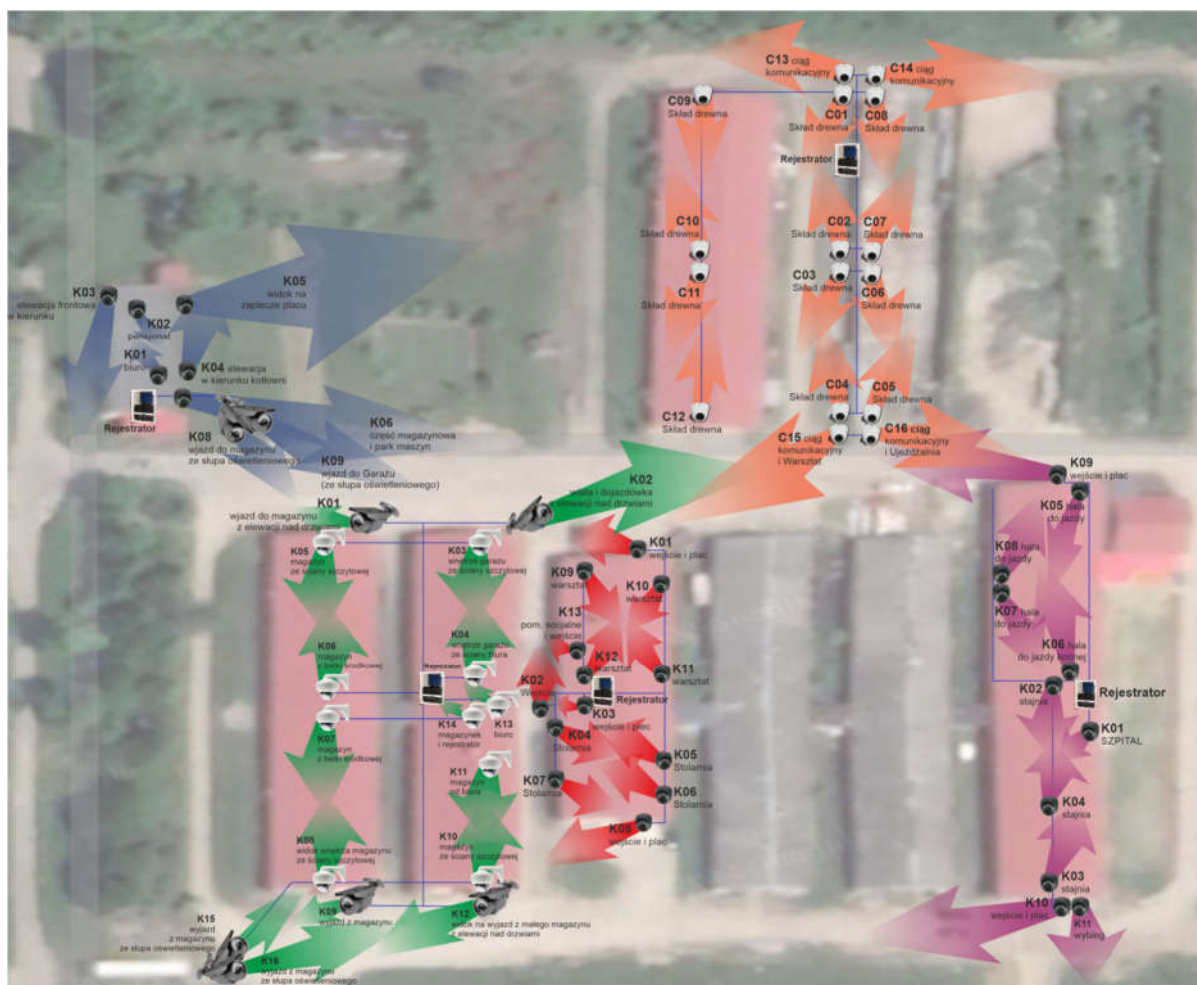


rejestratory pokładowe

Przykłady ochrony CCTV obiektów i pól widzenia kamer:



W przypadku rozległych, wielorejestrowych systemów monitoringu CCTV istotnym jest, by na użytek operatorów Centrum Monitoringu stworzyć model topograficzny pól widzenia poszczególnych kamer.

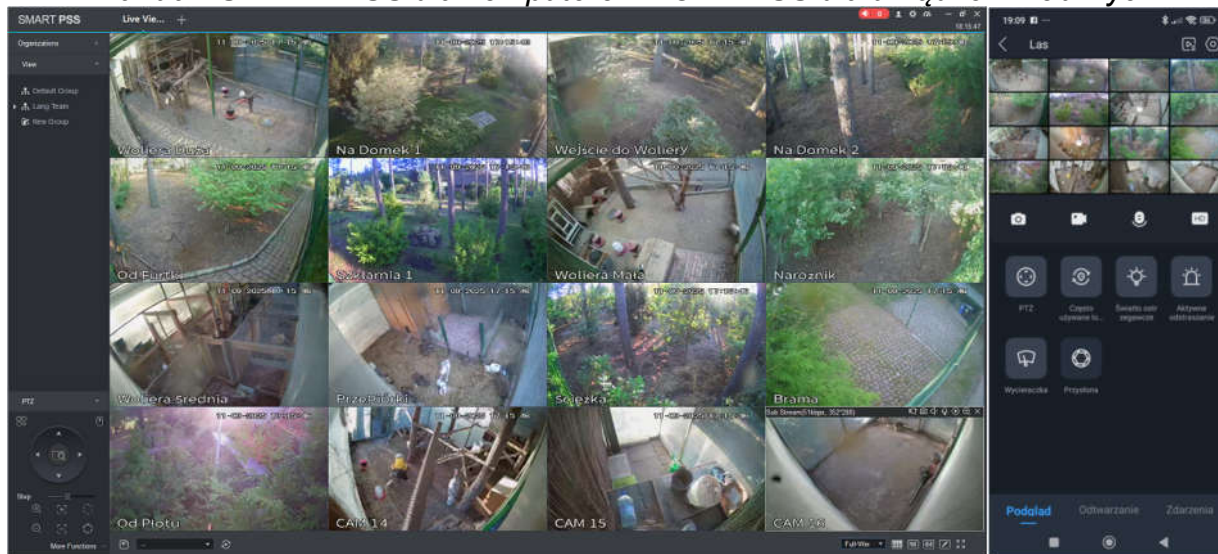


Systemy oprogramowania do kontroli CCTV:

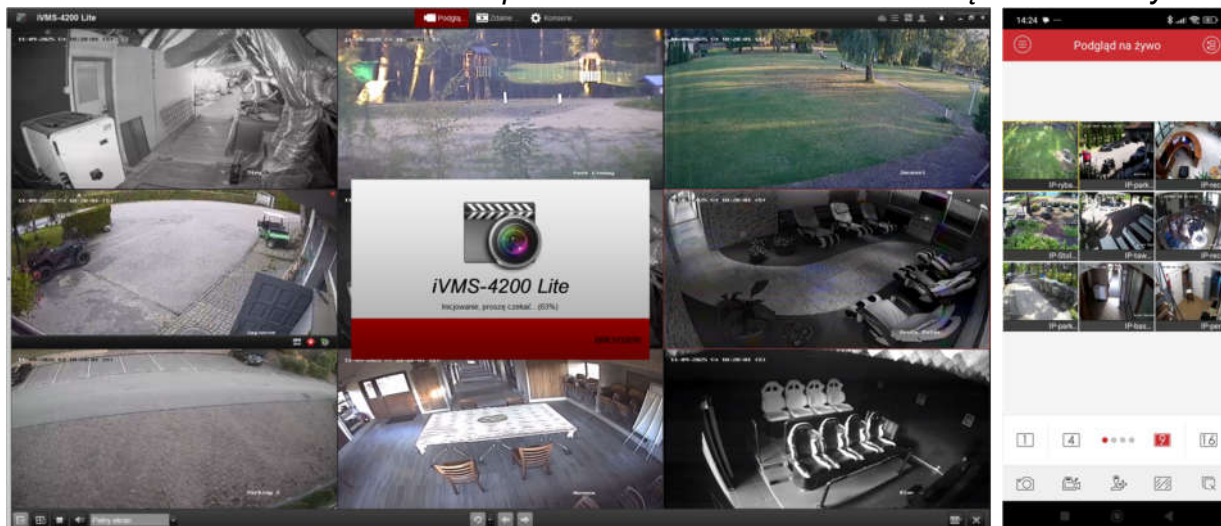
Na polskim rynku dostawców kompletnych systemów monitoringu wizyjnego CCTV wiodą producenci **Dahua** i **Hikvision**, oferujący pełną gamę komponentów i wsparcie serwisowe, od kamer wszystkich typów, przez rejestratory, aż po dedykowane im oprogramowanie do monitorowania, przetwarzania i analizy obrazu z kamer systemu oraz zapisanych archiwów rejestratorów.

Oprogramowanie to dostępne jest bezpłatnie dla komputerów PC, zarówno pracujących z systemami Microsoft Windows jak i dla komputerów Apple z systemem macOS oraz dla urządzeń mobilnych z systemami Android i iOS (iPhone).

Dahua - SMART PSS dla komputerów PC i DMSS dla urządzeń mobilnych



Hikvision – iVMS-4200 dla komputerów PC i iVMS-4500 dla urządzeń mobilnych

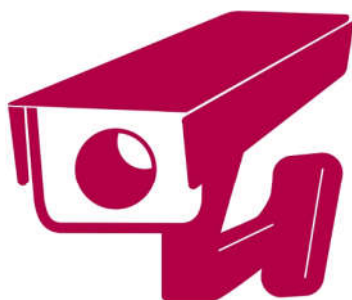


Analogiczne aplikacje oferują w pakiecie ze swoimi produktami wszyscy wiodący producenci systemów monitoringu. Niestety są one kompatybilne wyłącznie z rejestratorami własnej produkcji i niemożliwym jest ich użycie z produktami konkurencji, dlatego wybór producenta instalowanego rejestratora należy poprzedzić wyborem optymalnej dla swoich oczekiwań i potrzeb aplikacji, zarówno dla urządzeń stacjonarnych, jak i mobilnych.

Monitoring wizyjny a ochrona danych osobowych

RODO, obecnie EU GDPR pozwala na stosowanie monitoringu wizyjnego, po spełnieniu przez administratorów szeregu obowiązków, m.in. określenia celu przetwarzania (ochrona mienia i/lub bezpieczeństwo), zachowania zasady minimalizacji danych (utrwalanie tylko niezbędnego obrazu, unikanie rejestracji dźwięku, chyba że jest to uzasadnione), ustalenia okresu przechowywania nagrań, a także zapewnienia transparentności (obowiązek informacyjny poprzez umieszczenie wyraźnych **tabliczek informujących o monitoringu** obiektu).

UWAGA! OBIEKT MONITOROWANY



Więcej informacji:

- 1) na stanowisku recepcji/obsługi klienta,
- 2) na stronie internetowej [...],
- 3) poprzez kod QR.

ADMINISTRATOR DANYCH

Administratorem Pani/Pana danych osobowych przetwarzanych w związku z prowadzonym monitoringiem wizyjnym jest z siedzibą w (...) przy ul.

W przypadku pytań związanych z prowadzonym monitoringiem zapraszamy do kontaktu z inspektorem ochrony danych pod adresem:

CEL PRZETWARZANIA

Pani/Pana dane osobowe będą przetwarzane w celu zapewnienia bezpieczeństwa pracowników oraz współpracowników Administratora, ochrony jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Administratora na szkodę, co stanowi prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f) RODO).

POSTANOWIENIA SPECJALNE I PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Zakresem monitoringu wizyjnego objęty jest obszar wokół siedziby Administratora, ciągi komunikacyjne budynku oraz kluczowe pomieszczenia. Administrator przechowuje nagrania przez trzy (3) miesiące od dnia nagrania.

Jako osobie, której dane dotyczą przysługuje Pani/Panu szereg uprawnień, w tym m.in. prawo dostępu do Pani/Pana danych osobowych lub ich usunięcia. Więcej informacji na temat procesu przetwarzania danych osobowych oraz przysługujących Pani/Panu praw dostępnych jest w sposób określony po lewej stronie.

Zapis obrazu rejestratorów podlega ochronie prawnej i może być udostępniony jedynie w formie nakazu sądowego lub formalnego wniosku policji z podpisem komendanta placówki.

Niedopuszczalnym są jakiegokolwiek „wycieki” nagrań do mediów, czy internetu, bo kończy się to surowymi karami finansowymi i procesami cywilnymi dla podmiotu monitorującego oraz dyscyplinarnymi dla osób za nie odpowiedzialnych.

Dla zapewnienia bezpieczeństwa danych monitoringu, a także jego operatorów rejestratory obrazu kamer powinny być instalowane w miejscach bezpiecznych (serwerownie lub inne zamykane pomieszczenia dedykowane bądź szafy), niedostępnych dla osób postronnych, zwłaszcza ewentualnych napastników.



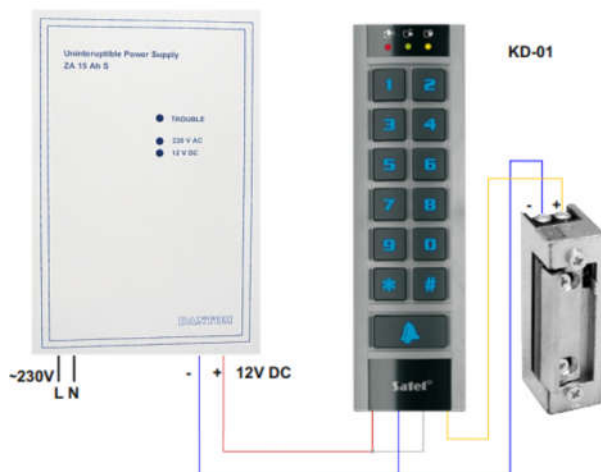
KONTROLA DOSTĘPU I SYSTEMY DOMOFONOWE

Kontrola dostępu (ang. access control) to zestaw zabezpieczeń i procedur kontrolnych w zakresie uprawnień do uzyskania dostępu do określonych zasobów, obszarów, informacji lub usług, a **system kontroli dostępu**, jako jej materializacja, to element zabezpieczenia technicznego stosowany głównie w zakładach przemysłowych, obiektach infrastruktury krytycznej i biurach, choć coraz częściej jego elementy używane są także do zapewnienia bezpieczeństwa w mniejszych budynkach i na prywatnych posesjach, zwłaszcza w postaci bramofonowo-domofonowej.

Systemy kontroli dostępu mogą być również zintegrowane z innymi systemami, jak monitoring wizyjny (CCTV), rejestracja czasu pracy (RCP), czy systemy alarmowe.

Podstawowe elementy systemu Kontroli Dostępu:

- **kontrolery przejścia**, identyfikujące uprawnienia osób wchodzących:
 - **klawiatury dotykowe** do manualnego wprowadzenia kodu dostępu,
 - **czytniki zbliżeniowe** kart i breloków dostępowych,
 - **skanery biometryczne** linii papilarnych lub rozpoznawania twarzy,
- **elektrozaczepy** zwalniające blokady przejścia,
- ewentualnie **oprogramowanie Rejestracji Czasu Pracy** lub zbliżone.

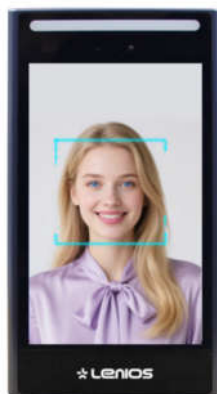


Schemat prostej instalacji systemu kontroli dostępu zarządzającego otwarciem drzwi przejścia o zadanym poziomie uprawnień dostępowych na bazie dualnego kontrolera przejścia (klawiatura + czytnik zbliżeniowy) produkcji Satel.

Przegląd biometrycznych kontrolerów dostępu i skanerów identyfikacji tożsamości:



identyfikacja linii papilarnych



rozpoznawanie twarzy



identyfikacja tęczówki oka

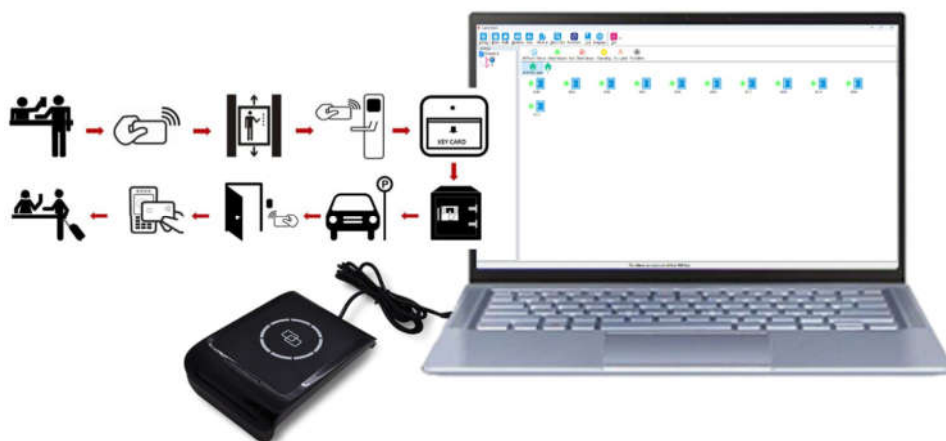
HOTELOWE SYSTEMY ZAMKÓW NA KARTĘ



Systemy elektronicznych zamków hotelowych, tanie w eksploatacji, wygodne i nowoczesne, bazują na zamkach z czytnikami lokalnie programowalnych kart magnetycznych wielokrotnego użytku, konfigurowanych przez recepcję indywidualnie dla każdego z gości na czas jego pobytu.

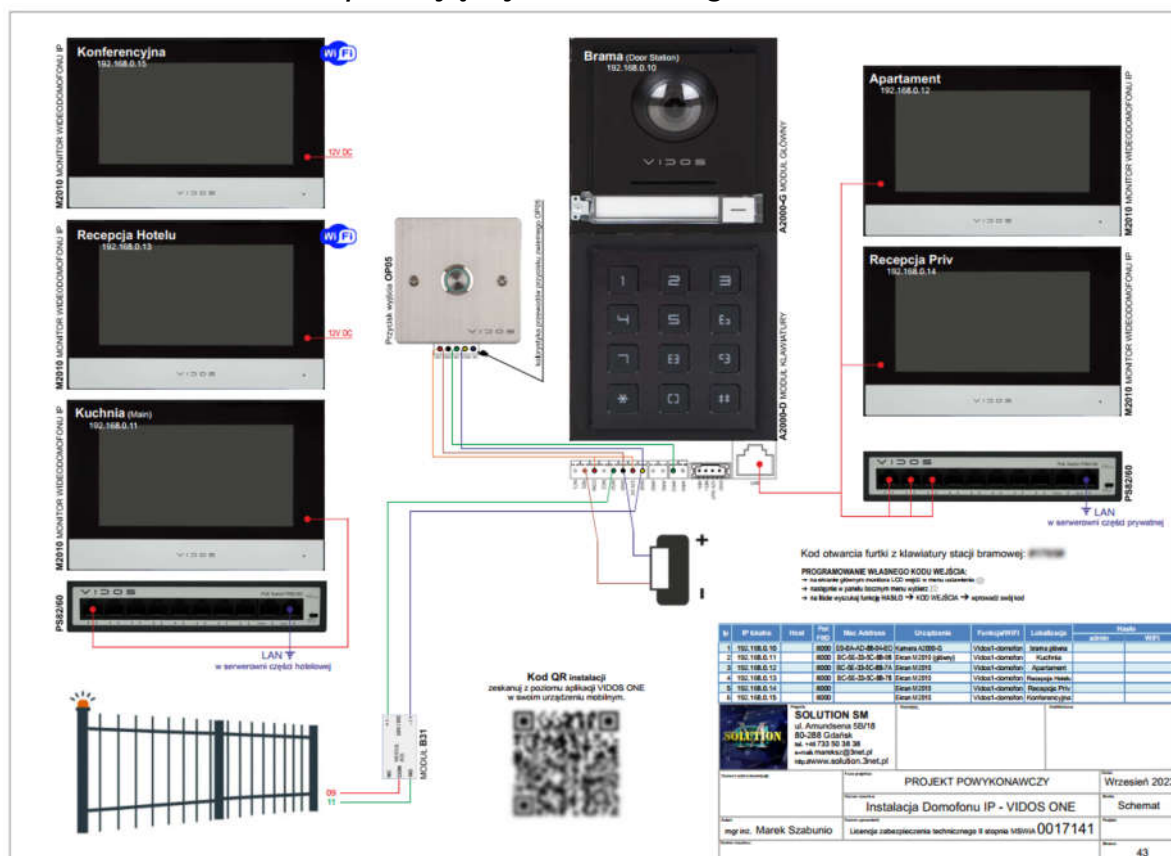
Karty te otwierają zamek drzwiowy pokoju, choć mogą również zapewniać dostęp do innych przejść hotelu (typu wyjście na parking, basen, siłownię oraz inne przejścia dostępne w ramach oferty pakietu pobytowego).

Karty magnetyczne są tańsze i trudniejsze do skopiowania w porównaniu do kluczy mechanicznych, dodatkowo w przypadku pokoiów kilkuosobowych można ich kopię wydać indywidualnie każdemu z gości, a w razie zgubienia lub kradzieży wystarczy na poczekaniu wygenerować i wydać ich duplikat z funkcją „zastąp starą kartę”, co jest nieporównanie tańsze i prostsze od konieczności kosztownej wymiany wkładki drzwiowej po zgubieniu lub utracie klucza mechanicznego.



Karty magnetyczne są wielokrotnego użytku, ich „ważność” generuje się każdorazowo (nadpisując poprzedni zapis) za pomocą programatora kart aplikacją w komputerze recepcji indywidualnie dla danego pokoju na czas pobytu gościa, a po upływie terminu uprawnienia karty samoczynnie tracą ważność, zatem nawet w przypadku, gdyby wyjeżdżający gość jej nie zwrócił, nie będzie to stanowić jakiegokolwiek zagrożenia dla kolejnych gości hotelu.

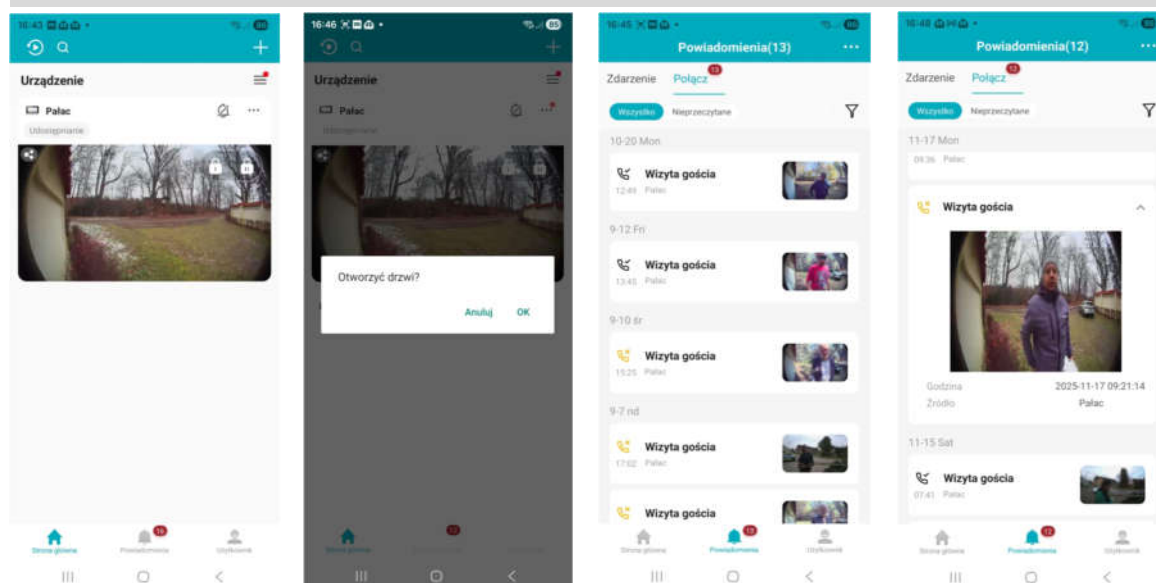
Schemat zaawansowanej instalacji bramofonowo-domofonowej Vidos ONE, pracującej w technologii IP sieci LAN i WiFi



System umożliwia lokalną i zdalną (przez internet za pomocą aplikacji mobilnej) kontrolę otwarcia furtki oraz bramy, z możliwością uprzedniej rozmowy weryfikującej z osobą dzwoniącą oraz zapewnia komunikację wewnętrzną pomiędzy terminalami monitorowymi (intercom)

Dodatkowo podłączenie systemu Vidos ONE do lokalnej struktury LAN obiektu umożliwia integrację kamery bramofonu z rejestratorem CCTV, dzięki czemu możliwym jest zapis jej obrazu na równi z obrazami pozostałych kamer systemu CCTV.

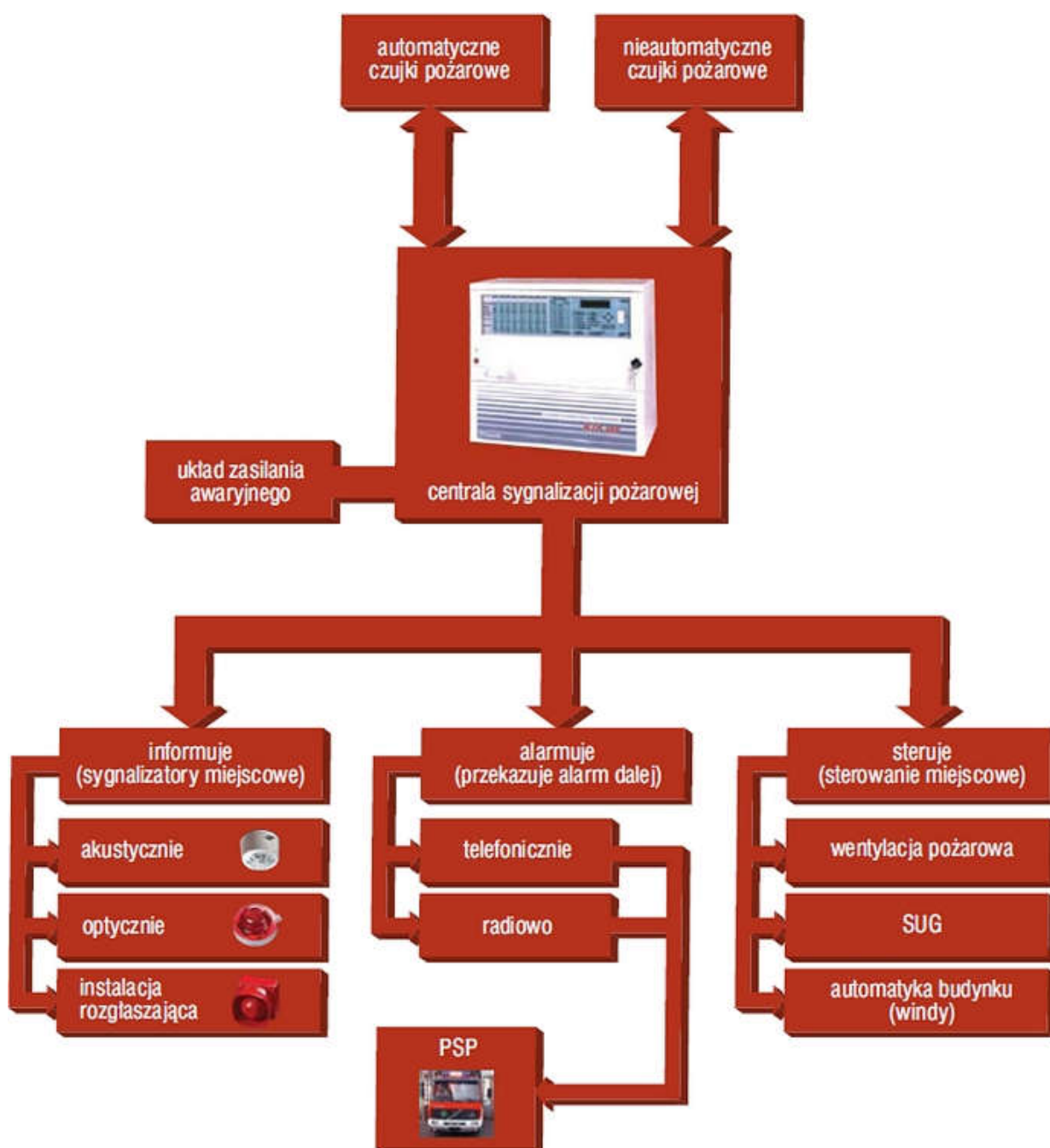
Możliwości komunikacji z opisaną stacją bramową i dzwoniącymi gośćmi za pomocy aplikacji mobilnej



SYSTEMY PRZECIWPOŻAROWE

Zadaniem **systemu sygnalizacji pożarowej** jest sygnalizowanie zagrożeń pożarowych po odebraniu przez centralę informacji od zainstalowanych czujek lub ręcznych ostrzegaczy pożarowych oraz wskazanie miejsca zagrożonego. Po otrzymaniu sygnału alarmu centrala może uruchomić sygnalizatory akustyczne lub akustyczno-optyczne (o ile są zainstalowane w systemie) oraz przesłać sygnał alarmu do stacji monitoringu lub do właściwych służb np. PSP. Za pośrednictwem przekaźników znajdujących się wewnątrz, centrala może uruchomić zewnętrzne, zabezpieczające urządzenia przeciwpożarowe oraz kontrolować ich stan.

System przeciwpożarowy najczęściej steruje gaśniczym systemem zraszaczy, układami automatyki przewietrzenia (sterowanie otwarciem klap dymowych), sprowadzania wind na najniższe kondygnacje oraz wyłączeniem zasilania układów wentylacji i klimatyzacji.



System przeciwpożarowy składa się z:

- centrali - "mózgu" całego systemu odpowiedzialnej za monitorowanie sygnałów z wejść (czujników ppoż) oraz odpowiednie sterowanie wyjściami w przypadku wystąpienia pożaru,
- zasilania głównego i awaryjnego,
- urządzeń inicjujących przekazywanie informacji o wystąpieniu pożaru do centrali alarmowej
 - uruchamiane ręcznie np. ręczne ostrzegacze pożarowe (ROP)
 - uruchamiane automatycznie: czujki dymu, ognia, tlenku węgla, itp.
- urządzeń powiadamiających, czyli sygnalizatorów akustyczno - optycznych, dźwiękowych systemów ostrzegawczych (DSO), radiolinii itp., odpowiedzialnych za powiadamianie odpowiednich osób oraz służb
- opcjonalnie system może być wyposażony w komponenty ograniczające niszczycielskie działanie dymu i ognia w postaci zraszaczy, urządzeń gaszących, klap odymiających.

Rodzaje czujek pożarowych:

- **czujki dymu:**
 - **jonizacyjne (izotopowe)** wykorzystujące izotop do jonizacji powietrza w komorze czujnika.
 - **fotoelektryczne (optyczne)** działające na zasadzie wykrywania rozpraszania lub pochłaniania światła przez cząsteczki dymu. Występują w formie punktowej lub liniowej, sprawdzając się w dużych pomieszczeniach jak hale czy zabytkowe obiekty.
- **czujki ciepła:**
 - **punktowe**, reagujące na przekroczenie ustalonej, wysokiej temperatury powietrza lub na gwałtowny wzrost temperatury.
 - **liniowe**, monitorujące temperaturę na dużej przestrzeni, często wykorzystując światłowody lub przewodniki o zmiennej rezystancji. Są stosowane w tunelach, metrze i innych obszarach o dużej powierzchni.
- **czujki płomienia**, wykrywające płomień na podstawie emitowanego przez niego promieniowania, zazwyczaj podczerwonego (IR) lub ultrafioletowego (UV).
- **czujki gazu**, reagujące na obecność specyficznych gazów pożarowych lub tlenku węgla (CO).
- **czujki wielodetektorowe** (multisensoryczne), łączące w sobie kilka technologii detekcji, np. optyczno-termiczne lub optyczno-termiczne z detektorem CO, zwiększając tym samym niezawodność systemu.



SYSTEMY MOBILNE do obserwacji/ochrony tymczasowej

Dotychczas omówione systemy zabezpieczeń elektronicznych dotyczyły ochrony obiektów stacjonarnych, o stałej strukturze zasilania, okablowania i przyłączy teletransmisyjnych (internet), coraz częściej zachodzi jednak potrzeba objęcia czasową ochroną obiektów „nieuzbrojonych”, przykładowo pustostanów, placów budów, czy coraz częściej mieszkań i domów bez stałej instalacji monitoringu (np. na czas wyjazdu wakacyjnego właścicieli).



Monitorowanie wtargnięć do obiektów bez zasilania (pustostany) przy użyciu mobilnego nadajnika **NANO-05**, karty GSM i akumulatora.

System powiadamia o ruchu/włamaniu SMSem do Centrum Monitorowania, gdzie podejmowana jest decyzja o wysłaniu Grupy Interwencyjnej.

Akumulator pozwala na nieprzerwaną pracę do 3-4 tygodni, po czym system poinformuje o konieczności jego rychłej wymiany.

Tymczasowy monitoring wizyjny w obiektach bez własnej infrastruktury kablowej (mieszkania, domy jednorodzinne - na czas przykładowo wyjazdu wakacyjnego, czy długiej podróży służbowej).

System bazuje na rozkładanym okablowaniu, własnym routingu (opcjonalnie z własnym internetem na kartę), rejestratorze oraz kamerach na statywach, jest prosty i szybki w montażu, a po zakończeniu ochrony jego demontaż trwa szybciej, niż rozpakowanie walizek klienta.



Mobilne Wieże Monitorujące

Samodzielne systemy do monitorowania placów budów i innych dużych obiektów tymczasowych, wyposażone we własne zasilanie akumulatorowe, wspomagane ogniwami fotowoltaicznymi oraz spalinowymi generatorami prądu.