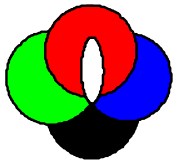

Ogólnopolskie Stowarzyszenie
Inżynierów i Techników
Zabezpieczeń Technicznych
i Zarządzania Bezpieczeństwem
„**POLALARM**”

# POLALARM ST 01/01

# SPECYFIKACJA TECHNICZNA

# Systemy alarmowe

# Część 1: Systemy sygnalizacji włamania i napadu - Wymagania ogólne i zasady stosowania

***Przedruk za zgodą Prezesa Polskiego Komitetu Normalizacyjnego – zezwolenie Nr 16/P/2009. Oryginały norm dostępne są w Wydziale Sprzedaży PKN oraz w autoryzowanych przez PKN punktach dystrybucji.***

***Za zgodność przedruku normy z oryginałem odpowiada autor niniejszej publikacji.***
***Wersja obowiązująca od dnia 1 marca 2010 r.***

## Przedmowa

Niniejsza Specyfikacja Techniczna została opracowana przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM”.

Na podstawie Zezwolenia Nr 16/P/2009 Prezesa Polskiego Komitetu Normalizacyjnego z dn. 14.12.2009 r. w specyfikacji wykorzystano przedruki fragmentów treści norm. Miejsca przytoczenia opatrzono przypisami, za zgodność przedruku z oryginałem odpowiada autor niniejszej publikacji.

Treść projektu Specyfikacji została poddana procedurze akceptacji i zatwierdzona przez Zarząd POLALARM jako ST 01/01 dnia 2009 - 09 - 10.

W sprawach merytorycznych dotyczących treści Specyfikacji można się zwracać do POLALARM, kontakt: www.polalarm.org

## Spis treści

**Załączniki**



**Tablice**

**Wprowadzenie**

Niniejsze wymagania ogólne i zasady stosowania opracowano, aby pomóc projektantom i instalatorom systemów alarmowych sygnalizacji włamania i napadu w klasyfikacji zagrożeń i środowiska pracy systemów oraz w analizie zagrożeń i ryzyka umożliwiając wybór poziomu zabezpieczenia, struktury i klasy systemu oraz klasy wykorzystywanych w nim urządzeń. Zasady stosowania odniesiono do etapów: projektowania systemów, instalowania, uruchomiania, odbioru, obsługi, konserwacji, sprawdzania i użytkowania oraz zapisów.

Do niniejszej Specyfikacji wprowadzono terminy oraz elementy analizy zagrożeń i ryzyka, ułatwia to dobór klasy/stopnia zabezpieczenia systemu alarmowego do kategorii zagrożonych wartości.

Niniejsza Specyfikacja nie dotyczy alarmowych centrów odbiorczych.

**UWAGA:** Wymagania Specyfikacji Technicznej służą utrwaleniu dotychczasowego dorobku krajowego w zakresie projektowania i stosowania systemów alarmowych sygnalizacji włamania i napadu. W Specyfikacji wykorzystano wybrane wymagania dotyczące „dobrej praktyki" w stosowaniu systemów. W klasyfikacji – zachowano podstawowe terminy tj.: „kategoria zagrożonych wartości, klasa systemu alarmowego, klasa urządzenia alarmowego i poziom zabezpieczenia". Wykorzystana w Specyfikacji klasyfikacja systemów od SA1 do SA4 i urządzeń: B, C i S jest klasyfikacją krajową.

## 1 Zakres specyfikacji

Niniejsze wymagania ogólne i zasady stosowania dotyczą systemów alarmowych sygnalizacji włamania i napadu, obejmując: klasyfikację zagrożeń, identyfikację środowiska pracy systemów, analizę ryzyka oraz dobór poziomu zabezpieczenia systemu i klas urządzeń.

Wymagania ogólne i zasady stosowania uporządkowano w 10 rozdziałach, jak następuje:

- **Rozdział 2 – Powołania normatywne**

Podano odniesienie do załącznika A informacyjnego z wykazem norm powołanych.

- **Rozdział 3 – Definicje i skróty**

Przedstawiono 52 terminy i definicje dotyczące wymagań ogólnych i zasad stosowania systemów alarmowych, określono terminy z zakresu analizy ryzyka.

- **Rozdział 4 – Klasyfikacja**

W rozdziale podano zasady klasyfikacji systemów i urządzeń systemów alarmowych sygnalizacji włamania i napadu; w tablicy 2 przedstawiono charakterystykę wybranych podstawowych cech funkcjonalnych systemów klas SA1 – SA4 i zasad ich użytkowania, określono wybrane podstawowe parametry czujek i sygnalizatorów. Opisano klasyfikację środowiskową.

- **Rozdział 5 – Zasady ogólne stosowania systemu**

Przedstawiono zasady oparte na spełnieniu wymagań: producenta urządzeń, użytkownika systemu, projektanta, instalatora, ubezpieczyciela i policji oraz rzeczoznawcy.

- **Rozdział 6 – Projektowanie systemu i wizja lokalna**

W rozdziale podano ogólne zasady projektowania systemu i prowadzenia wizji lokalnej uwzględniając wpływ czynników tj.: zagrożenia, charakterystyka sytuacyjno-budowlana obszaru nadzorowanego, minimalny poziom zabezpieczenia, zawartość projektu wstępnego i zakres wizji lokalnej – inspekcji technicznej.

- **Rozdział 7 – Instalowanie systemu**

W rozdziale zwrócono uwagę na: dobór materiałów instalacyjnych (np. przewodów), zalecane działania instalatora przed rozpoczęciem i podczas instalowania urządzeń i elementów systemu oraz na wprowadzanie rozszerzeń i zmian w systemie.

- **Rozdział 8 – Dokumentacja powykonawcza i deklaracja zgodności**

W rozdziale podano zalecaną zawartość dokumentacji powykonawczej przeznaczonej dla klienta oraz zasadę wydawania deklaracji zgodności

- **Rozdział 9 – Sprawdzenie, uruchomienie i odbiór i użytkowanie systemu**

W rozdziale określono zakres podstawowych procedur związanych z: sprawdzeniem działania systemu, przekazaniem do eksploatacji i wprowadzaniem zmian w warunkach użytkowania obiektu mogących mieć wpływ na pracę systemu. Przedstawiono warunki dotyczące procedur użytkowania systemu, w tym sposobów postępowania z alarmami. Określono zakres przeglądów konserwacyjnych oraz obsługi awaryjnej, uwzględniając dopuszczalny czas reakcji. Podano wymagany zakres zapisów.

- **Rozdział 10 – Audyt**

W rozdziale podano podstawowe zasady przeprowadzania audytów systemów alarmowych, w celu sprawdzenia zastosowanych procedur z zakresu zabezpieczeń organizacyjno-technicznych oraz procesów i procedur z nimi związanych.

W załącznikach **A – F** podano dodatkowe informacje użyteczne przy projektowaniu systemu alarmowych sygnalizacji włamania i napadu. Podano wykaz norm, kryteria oceny systemu transmisji alarmu, zalecaną lokalizację punktów – stref zabezpieczenia, krótki schemat działań w procesie stosowania systemów, zakres informacji projektu wstępnego oraz przykład rejestru zdarzeń.

## 2 Powołania normatywne

Na podstawie Zezwolenia Nr.16/P/2009 Prezesa Polskiego Komitetu Normalizacyjnego do niniejszej specyfikacji wprowadzono wybrane postanowienia zawarte w innych publikacjach, których wykaz podano w załączniku A.

## 3 Definicje i skróty

W niniejszej specyfikacji zastosowano następujące definicje i skróty:

**3.1** **alarm:** ostrzeżenie o istnieniu zagrożenia dla życia, mienia lub środowiska

**3.2** **alarmowe centrum odbiorcze :** centrum z ciągłą obsługą, do którego jest przekazywana informacja dotycząca stanu jednego systemu alarmowego lub większej ich liczby

**3.3** **analiza ryzyka:** systematyczne stosowanie dostępnych informacji do zidentyfikowania zagrożenia i do oszacowania ryzyka dotyczącego osób, populacji, mienia lub środowiska

**3.4** **aplikacja:** w niniejszej specyfikacji jest to elektroniczny system alarmowy np. sygnalizacji włamania/napadu, kontroli dostępu, CCTV, sygnalizacji pożarowej lub system nie-alarmowy np. system klimatyzacji, oświetlenia

**3.5** **audyt:** systematyczna weryfikacja, czy cel w zakresie bezpieczeństwa wyznaczony przez organizację audytowaną został osiągnięty lub czy jej działania są zgodne z akceptowanymi normami, statusem lub praktykami; audyt ocenia także procedury kontrolne celem stwierdzenia, czy przedmiot audytu także w przyszłości będzie odpowiadał uzgodnionym do stosowania wymaganiom

**3.6** **ciągłość działania:** strategiczna i taktyczna zdolność organizacji do planowania odpowiedzi na incydenty i dezorganizację biznesu w celu kontynuacji działań biznesowych na akceptowalnym, wcześniej określonym poziomie

**3.7** **części składowe systemu:** pojedyncze urządzenia, które tworzą system alarmowy, gdy są wspólnie skonfigurowane

**3.8** **dodatkowe podstawowe źródło zasilania:** źródło energii (niezależne od podstawowego źródła zasilania) zdolne do zasilania systemu alarmowego w wydłużonym okresie, bez wpływu na okres gotowości rezerwowego źródła zasilania

**3.9** **dokumentacja:** dokumenty w formie papierowej (bądź innej) zawierające szczegóły dotyczące systemu alarmowego, przygotowana w trakcie projektowania, instalowania, uruchomienia i przekazania systemu

**3.10** **dokumentacja powykonawcza:** dokument, w którym są zapisane szczegóły zainstalowanego systemu alarmowego

**3.11** **elektroniczny system zabezpieczeń**: np. system: alarmowy osobisty, CCTV, kontroli dostępu lub alarmu pożaru, lub nie-alarmowy system elektroniczny/elektryczny, np.: ogrzewania, klimatyzacji, oświetlenia

**3.12** **firma alarmowa:** organizacja zapewniająca obsługę systemu alarmowego

**3.13** **identyfikacja zagrożeń:** proces rozpoznawania potencjalnych zagrożeń i tych, które miały miejsce w przeszłości, oraz definiowanie ich charakterystyk

**3.14** **inspekcja techniczna:** badanie obszaru, który ma być nadzorowany, wykonane po zaakceptowaniu wstępnego projektu w celu weryfikacji wyboru, lokalizacji i miejsca umocowania elementów systemu oraz rozważenie wyboru elementów w danych warunkach środowiskowych, na które są wystawione

**3.15** **instalator:** osoba odpowiedzialna za instalację systemu alarmowego

**3.16** **klient:** osoba lub organizacja odpowiedzialna za odbiór systemu alarmowego

**3.17** **kompatybilność elektromagnetyczna:** zdolność urządzenia do poprawnej pracy w określonym środowisku elektromagnetycznym bez wprowadzania zakłóceń elektromagnetycznych do tego środowiska lub do innego urządzenia przez nie nietolerowanych

**3.18** **monitorowanie:** proces sprawdzania poprawnego działania połączeń wewnętrznych i urządzeń

UWAGA nie należy mylić monitorowania z „monitoringiem" – procesem transmisji alarmów do alarmowego centrum odbiorczego

**3.19** **obszar działania:** ta część budynku/terenu, w której system alarmowy może wykryć zagrożenie

**3.20** **ocena ryzyka:** pełny proces analizowania ryzyka i wyznaczenie dopuszczalności ryzyka

**3.21** **okres gotowości:** okres, w którym rezerwowe źródło zasilania jest zdolne do zasilania systemu alarmowego

**3.22** **operator:** osoba uprawniona (użytkownik) korzystająca z systemu alarmowego w określonym celu osoba uprawniona do obsługi systemu alarmowego

**3.23** **podstawowe źródło zasilania:** źródło zasilania wykorzystywane do zasilania systemu alarmowego w normalnych warunkach pracy

**3.24** **podsystem:** część systemu alarmowego zlokalizowana w wyraźnie określonej części nadzorowanego obszaru, zdolna do niezależnego działania

**3.25** **pomocnicze urządzenia sterujące:** wyposażenie używane w celu dodatkowego sterowania (np. klawiatura)

**3.26** **poziom zabezpieczenia:** miara oznaczająca poziom o jaki zredukowano ryzyko przez zastosowanie system alarmowego

**3.27** **poziom zabezpieczenia niższy:** miara oznaczająca poziom o jaki zredukowano ryzyko przez zastosowanie systemu alarmowego, w przypadku ryzyka większego od ryzyka akceptowalnego

**3.28** **poziom zabezpieczenia normalny:** miara oznaczająca poziom o jaki zredukowano ryzyko przez zastosowanie systemu alarmowego, uzyskując ryzyko akceptowalne

**3.29** **poziom zabezpieczenia wyższy:** miara oznaczająca poziom o jaki zredukowano ryzyko przez zastosowanie systemu alarmowego, uzyskując ryzyko jeszcze mniejsze od ryzyka akceptowalnego

**3.30** **rezerwowe źródło zasilania:** źródło zasilania umożliwiające zasilanie systemu w z góry ustalonym czasie, gdy nie jest dostępne podstawowe źródło zasilania

**3.31** **ryzyko akceptowalne:** ryzyko uzyskane po wprowadzeniu zabezpieczeń i ograniczone do poziomu akceptowalnego przez użytkownika

UWAGA wprowadzenie zabezpieczeń powinno redukować ryzyko co najmniej do poziomu akceptowalnego „jak to rozsądnie wykonalne”

UWAGA termin ten może również dotyczyć ryzyka, na które godzi się użytkownik, ignorując ewentualne straty lub przenosząc je na ubezpieczyciela

**3.32** **ryzyko:** kombinacja częstości lub prawdopodobieństwa wystąpienia określonego zdarzenia niebezpiecznego i konsekwencji związanych z tym zdarzeniem

UWAGA na pojęcie ryzyka zawsze składają się dwa elementy; częstość (lub prawdopodobieństwo występowania zagrożenia) i konsekwencja zdarzenia niebezpiecznego

**3.33** **sabotaż:** umyślne zakłócenie działania systemu alarmowego lub jego części

**3.34** **służby reagujące:** wyznaczone służby odpowiedzialne za nadzór nad obiektem w wyniku wystąpienia alarmu i podjęcie odpowiednich działań

**3.35** **stan alarmu:** stan systemu alarmowego lub jego części, który wynika z odpowiedzi systemu na obecność zagrożenia

**3.36** **sterowanie ryzykiem:** proces podejmowania decyzji mających na celu zarządzanie ryzykiem i/lub zmniejszanie ryzyka; zastosowanie i usprawnianie tego procesu, okresowe ponowne wyznaczanie ryzyka, z wykorzystaniem wyników oceny ryzyka jako danych wejściowych

**3.37** **strefa:** wyznaczony/wydzielony obszar, w którym mogą być wykryte nienormalne warunki (np. ruch intruza)

**3.38** **sygnalizacja:** informacja (dźwiękowa, wizualna lub w innej formie) dostarczana do wspomagania działań użytkownika związanych z obsługą systemu alarmowego

**3.39** **sygnalizator:** urządzenie wytwarzające alarm dźwiękowy i lub świetlny w odpowiedzi na wprowadzenie sygnału alarmu

UWAGA Sygnalizator może również zapewniać sygnalizację ostrzegania, pod warunkiem, że informacja ta będzie łatwo odróżnialna od alarmu

**3.40** **system alarmowy sygnalizacji napadu:** system alarmowy zapewniający użytkownikowi środki do celowego wytworzenia stanu alarmu napadu

**3.41** **system alarmowy sygnalizacji włamania i napadu:** łączony system alarmowy sygnalizacji włamania i sygnalizacji napadu

**3.42** **system alarmowy sygnalizacji włamania:** system alarmowy do wykrywania i sygnalizowania obecności, wejścia lub usiłowania wejścia intruza do chronionego obiektu

**3.43** **system alarmowy:** instalacja elektryczna, która odpowiada na ręczne lub automatyczne wykrycie obecności zagrożenia

**3.42** **system transmisji alarmu:** urządzenia i sieć wykorzystywane do przesyłania informacji dotyczącej stanu jednego lub większej liczby systemów alarmowych do jednego lub większej liczby alarmowych centrów odbiorczych

UWAGA systemy transmisji alarmu nie dotyczą bezpośrednich połączeń lokalnych, tj. połączeń wewnętrznych między częściami systemów alarmowych nie wymagające interfejsu przetwarzającego informację z tych systemów na postać dogodną do transmisji

**3.43** **szacowanie i wyznaczanie ryzyka:** całkowity proces identyfikacji ryzyka, jego analizy i oceny – tworzenia miary poziomu analizowanego ryzyka; szacowanie ryzyka składa się z: analizy częstości, analizy konsekwencji i ich połączenia; w wyznaczaniu ryzyka ocenia się dopuszczalność ryzyka i rozpatruje się aspekty kryminalistyczne, prawne, środowiskowe, biznesowe i socjoekonomiczne

**3.44** **szkoda:** uraz fizyczny lub uszczerbek na zdrowiu, uszkodzenie (kradzież) mienia lub degradacja środowiska

**3.45** **zabezpieczenie przeciwsabotażowe:** metody lub środki stosowane do ochrony systemu alarmowego lub jego części przed umyślnym zakłócaniem oraz wykrywanie umyślnego zakłócania systemu alarmowego lub jego części

**3.46** **zagrożenie:** źródło potencjalnej szkody lub okoliczności potencjalnie szkodliwe

**3.47** **zamaskowanie:** stan, w którym jest zablokowane pole widzenia czujki ruchu

**3.48** **zapis systemowy:** historia stanów alarmu i innych zdarzeń w systemie

**3.49** **zarządzanie ryzykiem:** proces podejmowania decyzji mających na celu szacowanie ryzyka, usprawnianie tego procesu, okresowa ponowna ocena ryzyka, systematyczne wprowadzanie procedur do zadań analizowania, wyznaczania i sterowania ryzykiem

**3.50** **zgłoszenie alarmu:** przejście stanu alarmu do sygnalizatorów i/lub systemów transmisji alarmu

**3.51** **zgłoszenie:** przesłanie sygnału stanu alarmu włamania, napadu, sabotażu lub stanu uszkodzenia do sygnalizatorów i/lub systemów transmisji alarmu

**3.52** **znaczące zmniejszenie zasięgu:** zmniejszenie zasięgu czujki ruchu, mierzone w głównych osiach czujki, przekraczające 50 % zasięgu, jak podano we wstępnej koncepcji systemu

# 4 Klasyfikacja

## 4.1 Klasyfikacja zagrożonych wartości

Ze względu na stopień zagrożenia osób i wartość potencjalnych szkód, wyróżnia się wg tabl. 1 cztery **kategorie zagrożonych wartości** od **Z1** do **Z4**, odpowiadające różnym poziomom ryzyka występującego w dozorowanych obiektach.

Podział zagrożonych wartości na kategorie uwzględnia:

a) zdrowie i życie,

b) wartość wymierną mienia i skutki jego utraty,

c) wartość niewymierną przedmiotów i dóbr zabytkowych i muzealnych,

d) wartość informacji niejawnych zawartych w dokumentach i środkach przechowywania informacji objętych tajemnicą.

**Tablica 1 – Kategorie zagrożonych wartości**

| Lp. | Kategoria zagrożonej wartości | Wartości podlegające zabezpieczeniu |
|---|---|---|
| 1 | Z1 | a) mienie małej wartości, które można wymienić lub zastąpić, |
| 2 | Z2 | a) mienie średniej wartości, które można wymienić lub zastąpić,<br>b) dokumenty lub przedmioty o wartości zabytkowej lub muzealnej, występujące w powtarzalnych egzemplarzach lub które można odtworzyć, |
| 3 | Z3 | a) mienie dużej wartości,<br>b) dokumenty lub przedmioty mające wartość zabytkową, niepowtarzalne w kraju,<br>c) dokumenty o dużej wartości, których uszkodzenie, zniszczenie lub kradzież jak również poznanie może prowadzić do dużych szkód,<br>d) dokumenty zawierające tajemnicę służbową, |
| 4 | Z4 | a) życie wielu ludzi,<br>b) życie ludzi związanych z wartościami wymienionymi wyżej w punktach 1,2, 3,<br>c) mienie bardzo dużej wartości,<br>d) przedmioty zabytkowe stanowiące dziedzictwo kultury światowej,<br>e) dokumenty, których kradzież jak również poznanie lub przejrzenie przez osoby niepowołane może zagrażać bezpieczeństwu ludności, osłabieniu obronności albo egzystencji państwa,<br>f) dokumenty zawierające tajemnicę państwową,<br>g) obiekty podlegające szczególnej ochronie oraz ważne obiekty dla bezpieczeństwa i obronności kraju. |

Klasyfikacja zagrożonych wartości jest jednym z elementów zarządzania ciągłością działania rozumianego jako: całościowy proces zarządzania, w którym identyfikowane są potencjalne zagrożenia organizacji (przedsiębiorstwa) i ich wpływy na działania biznesowe, mogące mieć miejsce w przypadku realizacji tych zagrożeń. Proces ten pozwala na określenie warunków ramowych budowania odporności organizacji i zdolności do skutecznej odpowiedzi, która zabezpiecza interesy kluczowych udziałowców organizacji, reputację, markę i jej działalność zarobkową.

Jako ciągłość działania rozumie się strategiczną i taktyczną zdolność organizacji do planowania odpowiedzi na incydenty i na dezorganizację biznesu w celu kontynuacji działań biznesowych na akceptowalnym, wcześniej określonym poziomie.

### 4.2 Szacowanie wartości wymiernej mienia

Do oszacowania wartości wymiernej mienia wg tabl. 1 można wykorzystywać wielokrotność N średniego przeciętnego rocznego wynagrodzenia (dane publikowane w komunikacie przez Prezesa Głównego Urzędu Statystycznego w sprawie przeciętnego miesięcznego wynagrodzenia)[1], oszacowując wartość wymierną jak następuje:

a) $N < 10$ dla mienia małej wartości,

b) $10 < N < 100$ dla mienia średniej wartości,

c) $100 < N < 1000$ dla mienia dużej wartości,

d) $N > 1000$ dla mienia bardzo dużej wartości.

### 4.3 Analiza zagrożeń i ryzyka

Proces projektowania oraz instalowania i uruchamiania systemu alarmowego powinien być poprzedzony analizą zagrożeń ochranianych zasobów. W analizie ryzyka należy zidentyfikować zarówno zagrożenia przypadkowe, jak i celowe oraz określić ich poziom i prawdopodobieństwo wystąpienia.

Przy prowadzeniu analizy zagrożeń i ryzyka należy określić podatności dotyczące chronionych zasobów. Analiza podatności polega na badaniu słabości, które mogą być wykorzystywane w realizacji identyfikowanych zagrożeń. Analiza podatności polega na badaniu ich w obszarach środowiska pracy projektowanego/ocenianego systemu alarmowego i zabezpieczeń (jeśli istnieją). Podatność chronionego zasobu zależy od łatwości, z jaką temu zasobowi może być wyrządzona szkoda.

Koszt zabezpieczeń technicznych (w tym systemów alarmowych) powinien być określany względem strat, które mogą być rezultatem naruszeń bezpieczeństwa oraz względem wymagań prawnych obowiązujących w danej instytucji.

[1] Komunikat Prezesa GUS podaje 3652,40zł jako przeciętne miesięczne wynagrodzenie w grudniu 2010r.

Technika analizy zagrożeń i ryzyka może mieć zastosowanie w całej instytucji, lub tylko w niektórych jej częściach, a także w projektowaniu pojedynczych systemów alarmowych i ich specyficznych elementów lub w planowaniu usług systemu, tam gdzie to jest wykonalne, realne i pomocne.

Zadaniem systemu alarmowego jest redukcja ryzyka do poziomu akceptowalnego. Kierownictwo organizacji (użytkownik) powinno być uświadomione o istnieniu ryzyka szczątkowego w jego pełnym zakresie („wszystkich ryzyk składowych"), w kontekście następstw oraz prawdopodobieństwa zajścia/realizacji określonego zdarzenia/zagrożenia. Decyzja o zaakceptowaniu ryzyka powinna być podejmowana przez te osoby, które są uprawnione do akceptacji konsekwencji ewentualnych skutków realizacji zagrożenia oraz, które są uprawnione do akceptacji wdrożenia dodatkowych zabezpieczeń, jeśli poziom ryzyka szczątkowego jest nie do przyjęcia w organizacji.

### 4.4 Klasyfikacja systemów alarmowych sygnalizacji włamania i napadu

Systemy alarmowe ze względu na zdolność do ochrony dozorowanych obiektów, dzielą się według wymagań niniejszej specyfikacji na cztery klasy od SA1 do SA4 (tabl. 2).

Podział systemów alarmowych na klasy według niniejszej specyfikacji uwzględnia między innymi:

a) właściwości czujek,

b) liczbę wariacji kodów dostępu,

c) sposób zabezpieczenia urządzeń systemu przed sabotażem,

d) cechy sygnalizatorów oraz systemu/systemów transmisji alarmu i ich monitorowania,

e) pojemność i trwałość zapisów w pamięci zdarzeń,

f) sposób monitorowania połączeń wewnętrznych systemu,

g) typy i okresy gotowości zasilania,

h) sposób i częstotliwość kontroli poprawności działania systemu alarmowego.

UWAGA: na wybór klasy systemu alarmowego SA1, SA2, SA3 i SA4 nie ma wpływu fizyczne środowisko pracy systemu (np. temperatura pracy, wilgotność, zakłócenia elektromagnetyczne).

Przy założonym poziomie redukcji ryzyka klasa systemu alarmowego zależy od zdolności sygnalizacyjnych systemu (metod: wykrywania ruchu/działania intruza, zabezpieczenia przed sabotażem, transmisji alarmu itp.). Urządzenia stosowane w systemie muszą być dostosowane do środowiska tzn. być odporne na zakłócenia elektromagnetyczne (kompatybilność elektromagnetyczna) i pracować poprawnie w danych warunkach klimatycznych tzn. mieć odpowiednią klasę środowiskową. Urządzenia muszą też mieć odpowiednią funkcjonalność – decydującą o ich klasie B, C i S, a określoną za pomocą wybranych cech funkcjonalnych (np. tak jak w tab. 2).

## Tablica 2 – Wymagania dotyczące urządzeń alarmowych i funkcjonalności systemu alarmowego

| Klasa systemu | Wymagania |
|---|---|
| **1. Czujki ruchu – badanie testem krokowym i maskowanie** | |
| SA1 | Prędkość wewnątrz granicy zasięgu 0,3m/s; wykrywanie działań blisko czujki – postawa wyprostowana, odległość 2m, prędkość 0,5m/s. |
| SA2 | Prędkość wewnątrz granicy zasięgu 0,3m/s, wysoka prędkość 2m/s; wykrywanie działań blisko czujki – postawa wyprostowana, odległość 2m, prędkość 0,4m/s. |
| SA3 | Prędkość wewnątrz granicy zasięgu 0,2m/s, wysoka prędkość 2,5m/s; wykrywanie działań blisko czujki – postawa czołgająca, odległość 0,5m, prędkość 0,3m/s. |
| SA4 | Prędkość wewnątrz granicy zasięgu 0,1m/s, wysoka prędkość 3m/s; wykrywanie działań blisko czujki – postawa czołgająca, odległość 0,5m, prędkość 0,2m/s,<br>wymagane środki do wykrywania znacznego ograniczenia zasięgu (ponad 50%) spowodowanego np. celowym lub przypadkowym wprowadzeniem przeszkód w obszar działania,<br>wymagane wykrywanie maskowania, generacja sygnału o maskowaniu w ciągu 180s. |
| UWAGA[2]: W czujkach stosowanych w systemach klas SA2 – SA4 nie powinno być możliwe zablokowanie działania czujki za pomocą magnesu; w czujkach do systemów SA2 – magnesem o energii magnetycznej 34kJ/m$^3$, w czujkach do systemów SA3 i SA4 – magnesem o energii magnetycznej 280kJ/m$^3$.<br>UWAGA: Powyższe wymaganie dotyczy również czujek: magnetycznych stykowych, stłuczenia szyby i aktywnych barier podczerwieni, które powinny być odporne na takie oddziaływania, albo powinny generować przy takim oddziaływaniu sygnału włamania lub uszkodzenia. | |
| **2. Czujki magnetyczne stykowe** | |
| SA3 | Pętla sabotażowa. |
| SA4 | Podwójna pętla sabotażowa. |
| **3. Czujki stłuczenia szyby (akustyczne, aktywne, pasywne) i czujki wibracyjne** | |
| SA3 | Wykrywanie zbicia szyby ze szkła zwykłego, hartowanego i laminowanego.<br>Testowanie lokalne przy użyciu testera imitującego dźwięk tłuczenia.<br>Regulacja czułości na wibracje.<br>Sygnalizacja spadku zasilania. |
| SA4 | Wykrywanie zbicia szyby ze szkła zwykłego, hartowanego i laminowanego.<br>Testowanie lokalne przy użyciu testera imitującego dźwięk.<br>Regulacja czułości na wibracje i krytycznej liczby wibracji/impulsów.<br>Dodatkowa czujka magnetyczna stykowa w czujce wibracyjnej.<br>Testowanie zdalne czujek aktywnych.<br>Sygnalizacja spadku zasilania. |
| UWAGA: w załączniku C podano zalecaną lokalizację stref (punktów/stref) zabezpieczenia, w których instaluje się czujki, odpowiednio do klasy systemu.<br><br>UWAGA: powyżej nie określono wymagań dotyczących: czujek magnetycznych stykowych, czujek stłuczenia szyby, wibracyjnych, aktywnych barier podczerwieni i sygnalizatorów przeznaczonych do stosowania w systemach klasy SA1 i SA2 ponieważ urządzenia popularne tych typów są rzadko stosowane, w tych przypadkach zwykle korzysta się z urządzeń profesjonalnych. | |

[2] *Przedruk za zgodą Prezesa Polskiego Komitetu Normalizacyjnego – zezwolenie Nr 16/P/2009. Oryginały norm są dostępne w Wydziale Sprzedaży PKN oraz w autoryzowanych przez PKN punktach dystrybucji.*

| | |
|---|---|
| **4. Aktywne bariery podczerwieni** | |
| SA3 | Kodowanie i synchronizacja wiązek podczerwieni.<br>Regulacja mocy sygnału (zasięgu).<br>Regulacja czasu reakcji/czułości.<br>Ustawianie liczby naruszeń wiązek.<br>Możliwość trwałego wyłączania wiązek.<br>Sygnalizacja naruszenia zamocowania – oderwania i otwarcia. |
| SA4 | Kodowanie i synchronizacja wiązek podczerwieni.<br>Regulacja mocy sygnału (zasięgu).<br>Regulacja czasu reakcji/czułości.<br>Wielopunktowy odbiór nadawanej wiązki.<br>Ustawianie liczby naruszeń wiązek.<br>Możliwość trwałego wyłączania wiązek.<br>Sygnalizacja naruszenia zamocowania – oderwania i otwarcia.<br>Możliwość programowania urządzenia za pomocą komputera z programem konfiguracyjno-diagnostycznym. |
| **5. Sygnalizatory dźwiękowo-świetlne (akustyczno-optyczne)** | |
| SA3 | Sygnalizacja spadku napięcia zasilania i uszkodzenia akumulatora.<br>Sygnalizacja naruszenia zamocowania – oderwania i otwarcia.<br>Wbudowany akumulator. |
| SA4 | Podwójny układ sygnalizacji optycznej.<br>Podwójny przetwornik elektryczno-akustyczny.<br>Wbudowany akumulator.<br>Sygnalizacja spadku zasilania i uszkodzenia akumulatora.<br>Sygnalizacja naruszenia zamocowania – oderwania i otwarcia.<br>Sygnalizacja penetracji – ochrona przed pianą.<br>Możliwość założenia wewnętrznej obudowy metalowej. |
| **6. Kody dostępu do systemu (liczba wariacji)** | |
| SA1 | Klucz logiczny: 1 000 lub klucz fizyczny: 300 |
| SA2 | Klucz logiczny: 10 000 lub klucz fizyczny: 3 000 |
| SA3 | Klucz logiczny: 100 000 lub klucz fizyczny: 15 000 |
| SA4 | Klucz logiczny: 1 000 000 lub klucz fizyczny: 50 000 |
| **7. Zabezpieczenie urządzeń systemu przed sabotażem** | |
| SA1 | Otwarcie w normalny sposób: centrala alarmowa, szyfrator/klawiatura, sygnalizator, zasilacz, system transmisji alarmu. |
| SA2 | Otwarcie w normalny sposób: centrala alarmowa, szyfrator/klawiatura, sygnalizator, zasilacz, system transmisji alarmu, urządzenie sygnalizacji napadu, czujki ruchu i usunięcie z zamocowania czujek bezprzewodowych. |
| SA3 | Otwarcie w normalny sposób: centrala alarmowa, szyfrator/klawiatura, sygnalizator, zasilacz, system transmisji alarmu, urządzenie sygnalizacji napadu, czujki ruchu, puszki połączeniowe (gdy nie ma ochrony transmisji przed zamianą sygnałów lub komunikatów) i usunięcie z zamocowania czujek bezprzewodowych. |
| SA4 | Jak dla SA3 oraz wykrycie zmiany orientacji czujki (gdy jest możliwe ustawianie orientacji). |

| 8. Monitorowanie połączeń wewnętrznych systemu | |
|---|---|
| SA1 | Maksymalny dopuszczalny odstęp czasu komunikatów – 240min. |
| SA2 | Maksymalny dopuszczalny odstęp czasu komunikatów – 120min. |
| SA3 | Maksymalny dopuszczalny odstęp czasu komunikatów – 100s. |
| SA4 | Maksymalny dopuszczalny odstęp czasu komunikatów – 10s. |
| **9. Pamięć zdarzeń w systemie** | |
| SA1 | Nie wymagana |
| SA2 | 250 zdarzeń, 30 dni |
| SA3 | 500 zdarzeń, 30 dni |
| SA4 | 1000 zdarzeń, 30 dni |
| **10. Sygnalizatory i transmisja alarmu** | |
| SA1 | 2 sygnalizatory dźwiękowe lub 1 sygnalizator dźwiękowy z własnym zasilaniem lub tylko system transmisji alarmu ATS1. |
| SA2 | 2 sygnalizatory dźwiękowe i system ATS2 lub 1 sygnalizator dźwiękowy z własnym zasilaniem i system ATS2 lub tylko systemy transmisji alarmu ATS1 i ATS2 lub tylko system ATS3. |
| SA3 | 2 sygnalizatory dźwiękowe i system ATS4 lub 1 sygnalizator dźwiękowy z własnym zasilaniem i system ATS4 lub tylko systemy transmisji alarmu ATS3 i ATS4 lub tylko system ATS5. |
| SA4 | 2 sygnalizatory dźwiękowe i system ATS5 lub 1 sygnalizator dźwiękowy z własnym zasilaniem i system ATS5 lub tylko systemy transmisji alarmu ATS4 i ATS5 lub ATS6. |
| UWAGA: znaczenie symboli ATS1 – ATS6 podano w załączniku B. | |
| **11. Zasilanie w systemie** | |
| SA1 | Minimalny okres gotowości zasilacz rezerwowego z automatycznie doładowywanym akumulatorem – 12h, z niedoładowywaną baterią – 24h. |
| SA2 | Jak dla SA1. |
| SA3 | Minimalny okres gotowości zasilacz rezerwowego z automatycznie doładowywanym akumulatorem – 60h, z niedoładowywaną baterią – 120h. |
| SA4 | Jak dla SA3. |

UWAGA: W systemach klas SA3 i SA4, gdy uszkodzenia podstawowego źródła zasilania są zgłaszane w alarmowym centrum odbiorczym lub w innym centrum oddalonym, czas gotowości zasilacza rezerwowego może być dwukrotnie skrócony.

Zgłoszenie uszkodzenia zasilacza podstawowego może być opóźnione maksymalnie o 1 h.

Gdy w zasilaczach przewidziano dodatkowe podstawowe źródło zasilania z automatycznym przełączaniem podstawowego źródła zasilania na dodatkowe podstawowe źródło zasilania (np. UPS, agregat), okres gotowości rezerwowego źródła zasilania może być zredukowany do 4 godzin.

W systemach wszystkich stopni wymagane jest wskazanie spadku napięcia rezerwowego źródła zasilania poniżej wymaganego poziomu, przy którym system pracuje poprawnie.

| 12. Przeglądy – kontrola poprawności działania systemu alarmowego | |
|---|---|
| SA1 | W pełnym zakresie w odstępie czasu nie dłuższym niż 12 miesięcy, czujki i tory transmisji alarmu – w odstępie czasu nie dłuższym niż 3 miesiące, podjęcie naprawy w przypadku uszkodzenia w ciągu 24h. |
| SA2 | W pełnym zakresie w odstępie czasu nie dłuższym niż 12 miesięcy, czujki i tory transmisji alarmu – w odstępie czasu nie dłuższym niż 3 miesiące, podjęcie naprawy w przypadku uszkodzenia w ciągu 12h. |
| SA3 | W pełnym zakresie w odstępie czasu nie dłuższym niż 6 miesięcy, czujki i tory transmisji alarmu – w odstępie czasu nie dłuższym niż 3 miesiące, podjęcie naprawy w przypadku uszkodzenia w ciągu 12h. |
| SA4 | W pełnym zakresie w odstępie czasu nie dłuższym niż 3 miesiące, czujki i tory transmisji alarmu – w odstępie czasu nie dłuższym niż 3 miesiące, podjęcie naprawy w przypadku uszkodzenia w ciągu 4h. |

## 4.5 Klasyfikacja urządzeń

Urządzenia systemów alarmowych sygnalizacji włamania i napadu ze względu na zapewniany przez nie stopień zabezpieczenia (zależny od poziomu redukcji ryzyka) są klasyfikowane w określonych klasach B, C i S. Przyporządkowanie urządzenia alarmowego kasy B, C, S do stosowania w określonej klasie systemu SA1 – SA4 następuje na podstawie zgodności ich cech (parametrów i funkcjonalności) z wymaganiami niniejszej specyfikacji, zgodności potwierdzonej w badaniach kwalifikacyjnych i poświadczonej Świadectwem lub Certyfikatem.

Urządzenia klasy wyższej muszą spełniać co najmniej wymagania dotyczące klasy niższej. Wymagania dotyczące stosowania urządzeń klas B, C i S w systemach alarmowych poszczególnych klas: SA1, SA2, SA3 i SA4 podano w tabl. 3.

**Tablica 3 – Klasy urządzeń alarmowych stosowanych w systemach alarmowych sygnalizacji włamania i napadu**

| **Klasa systemu** | **Klasa lub kwalifikacja urządzenia podawana w Świadectwie lub Certyfikacie *)** | |
|---|---|---|
| SA1 | **„B”** - popularna | **„do stosowania w SA1”** |
| SA2 | **„B”** - popularna | **„do stosowania w SA2”** |
| SA3 | **„C”** - profesjonalna | **„do stosowania w SA3”** |
| SA4 | **„S”** – specjalna | **„do stosowania w SA4”** |
| *) Klasa lub kwalifikacja zalecana w przypadku normalnego poziomu zabezpieczenia (tab. 4). | | |

## 4.6 Klasyfikacja poziomu zabezpieczenia

Do oceny skuteczności zabezpieczenia zagrożonej wartości określonej kategorii, (tabl. 1) przez zastosowanie systemu alarmowego sygnalizacji włamania i napadu, ustala się trzy poziomy zabezpieczenia: **normalny, niższy i wyższy**.

W tabl. 4 przyporządkowano klasy (SA1, SA2, SA3, SA4) systemów poziomom zabezpieczenia (niższym, normalnym, wyższym).

**Tablica 4 – Poziomy zabezpieczenia**

| Kategoria zagrożonej wartości | Poziom zabezpieczenia | | |
|---|---|---|---|
| | niższy | normalny | wyższy |
| | uzyskany przez zastosowanie systemu alarmowego klasy wg ST 01 | | |
| Z1 | nieokreślonej | SA1 | SA2 |
| Z2 | SA1 | SA2 | SA3 |
| Z3 | SA2 | SA3 | SA4 |
| Z4 | SA3 | SA4 | SA4*) |

*) wprowadzono nadmiar funkcjonalny środków w systemie alarmowym tj. dodatkowe urządzenia/konfiguracja systemu, nie wymagane na poziomie normalnym, mogą być to np. dołączone do wydzielonej linii dozorowej dodatkowe czujki, bądź maty naciskowe itp.

W przypadku ochrony wartości kategorii Z4 wyższy poziom zabezpieczenia można uzyskać przez wprowadzenie nadmiaru funkcjonalnego w systemie.

System alarmowy uzupełnia w ograniczaniu ryzyka inne środki zabezpieczenia fizycznego chronionego zasobu tj. zabezpieczenia mechaniczno - budowlane. Zaleca się wybór takiej klasy systemu alarmowego, aby ryzyko zostało ograniczone do poziomu akceptowalnego przez użytkownika.

Koszty wprowadzenia systemu alarmowego z uwzględnieniem kosztów jego eksploatacji, serwisu i konserwacji powinny być szacowane w odniesieniu do potencjalnych strat, jakie mogą wyniknąć w przypadku naruszenia bezpieczeństwa chronionego zasobu.

W tablicy 5 przedstawiono orientacyjne relacje między poziomami zabezpieczenia wg. ST 01/01, a systemami klasyfikowanymi zgodnie z wymaganiami normy PN-EN-50131-1.

**Tablica 5 – Poziomy zabezpieczenia**
**(klasyfikacja systemów wg PN-EN 50131-1)**

| Kategoria zagrożonej wartości | Poziom zabezpieczenia | | |
|---|---|---|---|
| | niższy | normalny | wyższy |
| | uzyskany przez zastosowanie systemu alarmowego[3] klasyfikowanego wg PN-EN 10131-1 [1)] | | |
| Z1 | nieokreślonej | stopień 1 | stopień 1 |
| Z2 | stopień 1 | stopień 1 | stopień 2 |
| Z3 | stopień 2 | stopień 2 | stopień 3 |
| Z4 | stopień 3 | stopień 3 | stopień 4 |

**Stopień 1:** **Ryzyko małe**
Spodziewani intruzi lub włamywacze będą mieć małą znajomość I&HAS i będą ograniczeni do korzystania z łatwo dostępnych narzędzi.

**Stopień 2:** **Ryzyko małe do ryzyka średniego**
Spodziewani intruzi lub włamywacze będą mieć ograniczoną znajomość I&HAS i będą korzystać z narzędzi w zakresie podstawowym i z przyrządów ręcznych (np. multimetr).

**Stopień 3:** **Ryzyko średnie do ryzyka wysokiego**
Spodziewani intruzi lub włamywacze będą biegli w I&HAS i będą korzystać z narzędzi w pełnym zakresie i z przenośnych urządzeń elektronicznych.

**Stopień 4:** **Ryzyko wysokie**
Stopień stosowany, gdy zabezpieczenie jest ważniejsze od wszystkich innych czynników. Spodziewani intruzi lub włamywacze będą mieć możliwość lub siły i środki do szczegółowego zaplanowania wtargnięcia lub ruchu intruza i będą mieć pełny zakres urządzeń, łącznie ze środkami zamiany części składowych I&HAS.

UWAGA We wszystkich stopniach termin „intruz" obejmuje różne typy zagrożeń (np. ruch intruza lub zagrożenie przemocą fizyczną mogące mieć wpływ na budowę I&HAS).

I&HAS: System alarmowy do sygnalizacji ruchu intruza i napadu.

## 4.7 Dostosowanie do środowiska

### 4.7.1 Zasady ogólne

System alarmowy sygnalizacji włamania i napadu powinien być tak zaprojektowany i instalowany, aby spełniał określone wymagania w danych warunkach środowiskowych, które mogą występować w chronionych obiektach, uwzględniając narażenia mechaniczne, temperaturę, wilgoć, korozję, gorąco oraz przemysłowe zanieczyszczenia atmosfery.

[3] *Przedruk za zgodą Prezesa Polskiego Komitetu Normalizacyjnego – zezwolenie Nr 16/P/2009. Oryginały norm są dostępne w Wydziale Sprzedaży PKN oraz w autoryzowanych przez PKN punktach dystrybucji.*

Należy rozpatrzyć zarówno warunki środowiskowe istniejące wewnątrz obiektów dozorowanych, wynikające np. z procesów przemysłowych, systemów ogrzewania i wentylacji oraz obecności zwierząt, jak również z warunków na zewnątrz obiektów chronionych, np. skrajnych warunków pogodowych, rodzaju działalności w miejscach sąsiednich oraz z ruchu drogowego w pobliżu (np. drgania podłoża).

Ponieważ system alarmowy może być instalowany wewnątrz lub na zewnętrznej strukturze budynków, gdzie występują różne narażenia, np. zakłócenia elektromagnetyczne, znaczne wahania temperatury, wilgotności, zmiany stanu pogody, atmosfery, możliwości zapylenia i uszkodzeń mechanicznych, w dokumentacji technicznej systemu alarmowego może być wymagana szczegółowa informacja dotycząca tych warunków środowiskowych.

### 4.7.2 Kompatybilność elektromagnetyczna

Elementy składowe systemów alarmowych, które mają być instalowane w budynkach i wokół nich, w środowisku mieszkaniowym, handlowym i lekko uprzemysłowionym powinny spełniać wymagania normy [2] wymienionej w załączniku A. W stosunku do urządzeń wykorzystujących sygnalizację radiową, lub przyłączonych do publicznej sieci telefonicznej mogą mieć zastosowanie dodatkowe wymagania innych norm dotyczących tych mediów.

### 4.7.3 Bezpieczeństwo elektryczne – oznakowanie CE

Oznakowanie CE urządzeń alarmowych potwierdza zgodność tych wyrobów lub procesów ich wytwarzania z zasadniczymi wymaganiami tzn. wymaganiami dyrektyw Nowego Podejścia UE. Nie wszystkie Dyrektywy UE dotyczą urządzeń systemów alarmowych. Dyrektywy mogące dotyczyć tych urządzeń wymieniono w tabeli 6.

To, czy dana Dyrektywa dotyczy danego urządzenia alarmowego wynika z jego budowy i spełnianych funkcji, z tego czy:

- jest zasilane napięciem 230V AC czy 12V DC?
- można je uznać za wyrób budowlany? czy np. przez to musi spełniać wymagania ochrony przeciwpożarowej dotyczące obiektów budowlanych tak jak urządzenia systemów sygnalizacji pożarowej i urządzenia systemów kontroli dostępu,
- urządzenie ma być odporne na zaburzenia (zakłócenia) elektromagnetyczne i czy je emituje?
- ma być instalowane w przestrzeniach zagrożonych wybuchem (przestrzeni, w której może wystąpić gazowa atmosfera wybuchowa, tzn. mieszanina substancji palnych w postaci gazu, pary lub mgły z powietrzem w warunkach atmosferycznych, której po zapaleniu spalanie rozprzestrzenia się na całą nie spaloną mieszaninę)?
- jest urządzeniem radiowym albo telekomunikacyjnym końcowym?

**Tablica 6. – Dyrektywy Nowego Podejścia, które mogą dotyczyć urządzeń alarmowych**

| Dyrektywa | Numer (pierwsza wersja i zmiany) |
|---|---|
| Sprzęt elektryczny niskiego napięcia (potocznie „Dyrektywa niskonapięciowa”) | LVD 73/23/EEC (obecnie 2006/95/EC) |
| Wyroby budowlane | CPD 89/106/EEC |
| Kompatybilność elektromagnetyczna | EMC 89/336/EEC (obecnie 2004/108/EC) |
| Urządzenia i systemy ochronne przeznaczone do użytku w przestrzeniach zagrożonych wybuchem | ATEX 94/9/EC |
| Urządzenia radiowe i telekomunikacyjne urządzenia końcowe | RTE 99/5/EC |

Dyrektywa niskonapięciowa nie dotyczy urządzeń zasilanych napięciem niższym od 50V AC lub 75V DC, zatem w zasadzie objęte nią są tylko zasilacze urządzeń alarmowych korzystające z napięcia 230V AC albo inne urządzenia zasilane z 230V AC (kamery, monitory CCTV).

Natomiast wszystkie elektroniczne urządzenia systemów alarmowych muszą spełniać Dyrektywę „Kompatybilność elektromagnetyczna”, która stawia **zasadnicze wymagania** dotyczące kompatybilności elektromagnetycznej (odporności na zakłócenia i poziomu emisji zakłóceń).

### Klasy środowiskowe urządzeń systemów alarmowych

Części składowe systemu alarmowego powinny być odpowiednie do stosowania w jednej z czterech klas środowiskowych[4] I, II, III i IV, określonych w PN-EN 50130-5. Klasy charakteryzują się rosnącą ostrością narażania dlatego wyrób klasy środowiskowej IV może np. być eksploatowany w środowisku klasy III.

Klasa środowiskowa I – środowisko wewnętrzne

Wpływy środowiskowe normalnie doznawane w pomieszczeniach zamkniętych, gdzie temperatura jest utrzymywana w najwęższych granicach (np. w nieruchomościach mieszkalnych i komercyjnych).

UWAGA Przewidywana temperatura może się zmieniać między +5ºC i +40ºC, w warunkach średniej wilgotności względnej w przybliżeniu 75%, bez wystąpienia zjawiska kondensacji.

Klasa środowiskowa II – środowisko wewnętrzne ogólne

Wpływy środowiskowe normalnie doznawane w pomieszczeniach zamkniętych, gdzie temperatura nie jest dobrze utrzymywana (np. w korytarzach, holach lub klatkach schodowych i tam gdzie może wystąpić kondensacja pary na szybach również w nieogrzewanych składach i magazynach, ogrzewanych z przerwami).

[4] *Przedruk za zgodą Prezesa Polskiego Komitetu Normalizacyjnego – zezwolenie Nr 16/P/2009. Oryginały norm są dostępne w Wydziale Sprzedaży PKN oraz w autoryzowanych przez PKN punktach dystrybucji.*

UWAGA Przewidywana temperatura może się zmieniać między -10ºC i +40ºC, w warunkach średniej wilgotności względnej w przybliżeniu 75%, bez wystąpienia zjawiska kondensacji.

Klasa środowiskowa III - środowisko zewnętrzne osłonięte przed ekstremalnymi warunkami środowiskowymi

Wpływy środowiskowe normalnie doznawane na zewnątrz pomieszczeń, gdzie elementy składowe systemu nie są całkowicie wystawione na działanie czynników atmosferycznych.

UWAGA Przewidywana temperatura może się zmieniać między -25ºC i +50ºC, w warunkach średniej wilgotności względnej w przybliżeniu 75%, bez wystąpienia zjawiska kondensacji. Można przewidywać że w ciągu 30 dni w roku wilgotność względna może się zmieniać między 85% i 95%, bez wystąpienia zjawiska kondensacji.

Klasa środowiskowa IV - środowisko zewnętrzne ogólne

Wpływy środowiskowe normalnie doznawane na zewnątrz pomieszczeń, gdzie elementy składowe I&HAS są całkowicie wystawione na działanie czynników atmosferycznych.

UWAGA Przewidywana temperatura może się zmieniać między -25ºC i +60ºC, w warunkach średniej wilgotności względnej w przybliżeniu 75%, bez wystąpienia zjawiska kondensacji. Można przewidywać że w ciągu 30 dni w roku wilgotność względna może się zmieniać między 85% i 95%, bez wystąpienia zjawiska kondensacji.

Szczelność obudów urządzeń systemu alarmowego na wnikanie pyłów i wody oraz na dostęp do ich części wewnętrznych określa się wykorzystując kod IP (według PN-EN 60529:2003 Stopnie ochrony zapewniane przez obudowy (kod IP)).

W normie [1] przyjęto, że szczelność na pył obudów tych urządzeń powinna być IP5X lub IP6X.

Urządzenia systemu alarmowego zgodnie z [1] powinny być odporne na uderzenia mechaniczne na ich powierzchnię (obudowę), których można się spodziewać w warunkach pracy.

Urządzenia klas środowiskowych I – III powinny mieć obudowy klasy IK04 (energia 3 uderzenia 0,5J), urządzenia klasy IV – obudowę IK06 (uderzenia1,0J) (według PN-EN 62262:2003 Stopnie ochrony przed zewnętrznymi uderzeniami mechanicznymi zapewnianej przez obudowy urządzeń elektrycznych - kod IK).

## 5 Zasady ogólne stosowania systemu

System alarmowy sygnalizacji włamania i napadu powinien być zainstalowany, obsługiwany i konserwowany zgodnie z zaleceniami projektanta oraz producentów wykorzystywanych urządzeń, w dostosowaniu do warunków środowiskowych użytkowania.

Elementy innych systemów mogą być łączone z lub włączane do systemu, jeżeli nie będzie to miało negatywnego wpływu na jego działanie.

Powinny być uwzględnione wymagania dotyczące bezpieczeństwa instalacji elektrycznej.

Powinny być podjęte przez projektantów, instalatorów i użytkowników środki zapobiegające fałszywym alarmom.

Powinna być wyraźnie określona i uzgodniona pomiędzy odpowiednimi stronami odpowiedzialność za realizację każdej fazy procesu realizacji systemu: projektowania, instalowania, uruchomienia i przekazania.

Osoba odpowiedzialna za ocenę zagrożeń oraz projektowanie, instalowanie, konserwacje i naprawy systemu powinna posiadać odpowiednie kwalifikacje potwierdzone obowiązującymi dokumentami (np. licencja pracownika zabezpieczenia technicznego itp.).

Wybrane informacje związane z projektowaniem, instalacją, obsługą i konserwacją systemu mogą być traktowane jako tajemnica służbowa. Projekt systemu powinien być tworzony w porozumieniu z klientem bądź specyfikatorem systemu (lub ich reprezentantem) oraz wszelkimi powiązanymi stronami.

PRZYKŁAD: ubezpieczyciele, policja.

Kiedy to jest konieczne należy zasięgnąć porady rzeczoznawcy.

Projektant systemu powinien uwzględnić wszelkie wymagania niezbędne do uzyskania zatwierdzenia projektu przez odpowiednie instytucje. Należy określić wszystkie takie wymagania we wczesnej fazie projektowania i wyboru elementów systemu.

Wybór elementów systemu powinien zapewniać ich pełną kompatybilność (współpracę). W przypadku wystąpienia wątpliwości należy przeprowadzić odpowiednie konsultacje z producentem/dostawcą, laboratorium lub odpowiednią instytucją.

## 6 Projektowanie systemu i wizja lokalna

W fazie projektowania systemu powinna być określona jego klasa zabezpieczenia jako całości, odpowiedniej klasy zabezpieczenia wybranych elementów i ich klasy środowiskowe oraz przygotowany wstępny projekt systemu.

W trakcie wizji lokalnej należy określić:

- czynniki zagrożeń (atrakcyjność dla włamywacza, wartość wymierną i niewymierną mienia jak w tabl. 1, łatwość dostępu, historie kradzieży w obiekcie i jego pobliżu, jeżeli takie miały miejsce; zagrożenia uszkodzeniem – wandalizmem, podpaleniem itp.),
- strukturę obiektu (konstrukcja, typy otwory, zajętość przez osoby, lokalizacja, istniejące zabezpieczenia mechaniczne i systemy alarmowe, przepisy lokalne, rodzaj terenu miejski/wiejski),
- minimalne poziomy zabezpieczeń (patrz załącznik C).

Wstępny projekt systemu powinien być przekazany inwestorowi i zawierać następujące informacje:

- dane klienta,
- dane nadzorowanego obiektu,
- stopień zabezpieczenia i klasę systemu/systemów alarmowego,
- klasę środowiskową elementów systemu,
- zestawienie urządzeń,
- opis konfiguracji systemu i lokalizacji urządzeń,
- dane dotyczące sygnalizacji i transmisji alarmu,
- wymagania dotyczące obowiązujących przepisów lokalnych,
- wykaz norm powołanych,
- świadectwa i certyfikaty urządzeń i materiałów wykorzystywanych do budowy systemu alarmowego,
- sposób reakcji i interwencji na alarmy,
- plan konserwacji i serwisu (napraw).

Kolejna wizja lokalna powinna obejmować czynność weryfikujące założenia wstępnego projektu systemu dotyczące:

- obsługi systemu,
- wyboru elementów,
- połączeń – lokalizacji tras kablowych,
- poprawek w projekcie wstępnym.

Wszelkie zmiany wynikające z wizji lokalnej powinny być uzgodnione z klientem (w obiektach złożonych może być wymagane kilka wizji lokalnych).

# 7 Instalowanie systemu

## 7.1 Okablowanie

Parametry przewodów elektrycznych (przekrój - rezystancja) powinny być takie, aby przy przepływie maksymalnego prądu napięcie między określonymi zaciskami urządzeń lub elementów nie było mniejsze niż jego określona wartość robocza, (np. w przypadku sygnalizatorów instalowanych w znacznej odległości od centrali).

Połączenia przewodów elektrycznych powinny mieć odpowiednią wytrzymałość mechaniczną i elektryczną oraz powinny być od siebie odizolowane elektrycznie. Do połączeń przewodów należy wykorzystywać listwy zaciskowe pokryte materiałem izolacyjnym lub puszki połączeniowe o szczelności obudowy dostosowanej do warunków środowiskowych.

Mogą być użyte inne elementy łączące (np. wtyczka i gniazdo lub specjalne złącza firmowe) pod warunkiem, że w warunkach gdzie występują połączenia przewodów z tymi elementami, spełniają powyższe wymagania.

Połączenia giętkie powinny być takie, aby przewody i izolacja były odporne na zmęczenie lub naprężenia występujące w konkretnym zastosowaniu.

Okablowanie powinno być odpowiednio zamocowane i rozprowadzone, albo zabezpieczone w celu uniknięcia uszkodzeń mechanicznych (sabotażu) i klimatycznych w środowisku, w którym jest stosowane.

### 7.2 Działania wstępne poza miejscem zainstalowania systemu

Urządzenia i elementy systemu mogą być sprawdzone w zakładzie producenta/instalatora, jeśli tak zostało uzgodnione. Opakowanie powinno chronić urządzenia i elementy przed uszkodzeniem podczas transportu i przechowywania oraz powinno być tak oznakowane, aby mogły być zidentyfikowane poszczególne elementy. Urządzeń i elementów nie należy dostarczać wcześniej niż będzie możliwe ich zainstalowanie, chyba że zostaną zapewnione odpowiednie warunki składowania (w pomieszczeniu zamkniętym), włącznie z zapewnieniem ochrony składowania.

### 7.3 Zalecenia dotyczące instalowania urządzeń i elementów systemu

Urządzeń i elementów systemu alarmowego nie należy instalować w pobliżu źródeł ciepła, np. grzejników, urządzeń klimatyzacyjnych, jeżeli mogłoby to wpłynąć ujemnie na ich działanie. Prace, które będą wykonywane w miejscu zainstalowania urządzeń i elementów systemu alarmowego powinny obejmować:

- wstępne przygotowanie miejsca pracy;
- rozprowadzenie kabli i przewodów;
- rozmieszczenie urządzeń sterujących i sygnalizacyjnych (central alarmowych, klawiatur, sygnalizatorów dźwiękowych i świetlnych (dźwiękowo-świetlnych), czujek oraz przycisków napadowych (ostrzegaczy) oraz urządzeń transmisji alarmu;
- łączenie urządzeń i elementów;
- sprawdzenie systemu, badanie końcowe i odbiór.

### 7.4 Rozszerzenia i zmiany

Jeżeli ma nastąpić rozszerzenie instalacji systemu alarmowego, to istniejące urządzenia i elementy należy starannie sprawdzić w celu upewnienia się, czy będą funkcjonować w sposób zadawalający w połączeniu z urządzeniami dodatkowymi oraz, czy zasilacze będą mogły zasilić urządzenia dodatkowe.

Jeżeli działania sygnalizatorów dźwiękowych/świetlnych i/lub transmisja sygnałów alarmu zostały przerwane w trakcie wprowadzania zmian w istniejącej instalacji, to należy je sprawdzić ponownie, po upoważnieniu należy również sprawdzić system/systemy transmisji alarmu.

# 8 Dokumentacja powykonawcza i deklaracja zgodności

## 8.1 Dokumentacja powykonawcza

Dokumentacja powykonawcza dostarczona klientowi powinna zawierać:

- dane firmy instalacyjnej, bądź konserwatora systemu;
- nazwę i dane alarmowego centrum odbiorczego odpowiedzialnego za reakcję na komunikaty z systemu;
- dane organizacji (np. agencji ochrony) odpowiedzialnej za kontrolę nadzorowanego obszaru w przypadku alarmu;
- projekt wykonawczy systemu z naniesionymi zmianami;
- instrukcję obsługi systemu, szczegółową na tyle, by zminimalizować możliwość niewłaściwego użytkowania (np. powstawania fałszywych alarmów). Instrukcja powinna mieć dwie części:
  - dotyczącą: włączania/wyłączania, weryfikacji stanu alarmu, kasowania, blokowania i testowania,
  - opisującą pozostałe funkcje systemu;
- instrukcję konserwacji i napraw z danymi kontaktowymi osoby odpowiedzialnej za konserwację/naprawy;
- protokół z przeszkolenia obsługi przekazywanego systemu z zapisem miejsca, daty oraz danych osób szkolących i przeszkolonych;
- protokół odbioru;
- deklarację zgodności.

## 8.2 Deklaracja zgodności

Firma instalacyjna powinna dostarczyć klientowi deklarację zgodności stwierdzającą wykonanie systemu w deklarowanej klasie zgodnie z dokumentacją powykonawczą.

W przypadku gdy instalowane urządzenia alarmowe lub ich części są wyrobami podlegającymi obowiązkowej ocenie zgodności (np. zasilacze), firma instalacyjna powinna dostarczyć certyfikat albo deklarację ich zgodności z zasadniczymi wymaganiami (oznakowanie CE). Certyfikat taki wydaje notyfikowana jednostka certyfikująca, a deklaracja jest oświadczeniem producenta lub jego upoważnionego przedstawiciela.

# 9 Sprawdzenie, uruchomienie, odbiór i użytkowanie systemu

## 9.1 Zasady ogólne

Zaleca się aby po sprawdzeniu działania systemu alarmowego w obecności jego użytkownika i/lub właściciela był sporządzony protokół odbioru.

Po zatwierdzeniu protokołu odbioru odpowiedzialnym za użytkowanie systemu alarmowego staje się jego nabywca/użytkownik.

Właściciel lub użytkownik obiektu dozorowanego powinien wyznaczyć osobę odpowiedzialną (administratora) za nadzór nad systemem alarmowym. Osoba odpowiedzialna powinna mieć przekazane informacje dotyczące odpowiedniego poziomu/poziomów dostępu do systemu.

Osobie tej należy przyznać uprawnienia do wykonywania prac niezbędnych do utrzymania systemu alarmowego w stanie sprawności, dokonywania odpowiednich zapisów oraz obsługi.

Użytkownicy instalacji powinni być przeszkoleni w zakresie użytkowania systemu alarmowego.

Należy ustalić procedury postępowania z alarmami, ostrzeżeniami o uszkodzeniu, wyłączeniu części lub całego systemu alarmowego ze stanu działania. Procedury te powinny być zatwierdzone przez odpowiednie władze przed ich wprowadzeniem.

Powinna być zapewniona współpraca z osobami odpowiedzialnymi za konserwację budynku, jego remonty itp., aby było pewne, że ich praca nie spowoduje uszkodzeń lub nie zakłóci w inny sposób działania systemu alarmowego.

Użytkownik powinien zapewnić wolną przestrzeń roboczą wokół każdej czujki alarmowej i wszystkie przyciski/ostrzegacze alarmowe pozostawić odsłonięte.

Jeżeli nastąpi zmiana wystroju lub najemcy dozorowanego obiektu, to użytkownik odpowiednio wcześnie powinien rozważyć konieczność przeprowadzenia niezbędnych zmian w systemie alarmowym.

## 9.2 Działanie w przypadku alarmu

Należy ustalić procedury postępowania z alarmami, ostrzeżeniami o uszkodzeniu, wyłączeniu części lub całego systemu alarmowego ze stanu działania. Procedury te powinny być zatwierdzone przez odpowiednie władze przed ich wprowadzeniem.

Działanie to powinno być określone z góry i ustalone w ścisłym porozumieniu z organizacjami, które posiadają doświadczenie lub władzę w tych dziedzinach oraz są kompetentne do określenia wszystkich czynników, które należy wziąć pod uwagę przy podejmowaniu decyzji o tym, jakie działanie należy przedsięwziąć w przypadku alarmu i jakie urządzenia sygnalizacyjne są wymagane do jego podtrzymania.

Odpowiedni personel powinien być poinstruowany o właściwym inicjowaniu stanu alarmowania i wszelkich działaniach, które należy podjąć w przypadku zaistnienia alarmu.

Przy projektowaniu systemu alarmowego należy wziąć pod uwagę fakt, że skuteczność działań w przypadku zaistnienia alarmu będzie zależeć od stanu urządzeń sygnalizacyjnych systemu oraz czasu potrzebnego na przybycie pomocy.

## 9.3 Przeglądy i konserwacja

Konserwacja okresowa powinna być przeprowadzana nie rzadziej niż w okresach zgodnych z wymaganiami dotyczącymi danego systemu alarmowego (patrz tablica 2). Podczas każdej konserwacji okresowej należy wykonać następujące sprawdzenia i wszelkie niezbędne poprawki:

a) sprawdzenie instalacji, właściwego rozmieszczenia i zamocowania całego wyposażenia i urządzeń na podstawie dokumentacji technicznej,

b) sprawdzenie poprawności działania wszystkich czujek alarmowych, łącznie z urządzeniami uruchamianymi ręcznie,

c) sprawdzenie zgodności z wymaganiami wszystkich połączeń giętkich,

d) sprawdzenie czy zasilacze główne i rezerwowe pracują i są sprawne,

e) sprawdzenie centrali alarmowej i jej obsługi zgodnie z procedurą zakładu instalacji alarmowych,

f) sprawdzenie poprawności działania każdego urządzenia transmisji alarmu przy współpracy z odpowiedzialną władzą albo z odpowiednim alarmowym centrum odbiorczym,

g) sprawdzenie poprawności działania każdego dźwiękowego, świetlnego, dźwiękowo/świetlnego sygnalizatora alarmowego,

h) sprawdzenie czy system alarmowy jest całkowicie w stanie gotowości.

## 9.4 Obsługa awaryjna

Jeżeli zakład instalacji alarmowych zapewnia obsługę awaryjną, to właściciel obiektu/użytkownik powinien mieć adres (mailowy) i numer telefonu do centrum serwisowego lub inną możliwość komunikowania. W czasie, w którym wymagane jest, aby system alarmowy był czynny, należy zapewnić możliwość obsługi awaryjnej.

UWAGA: Zaleca się takie zlokalizowanie i zorganizowanie obsługi awaryjnej, aby (z wyjątkiem nienormalnych okoliczności) przedstawiciel zakładu instalacji alarmowych znalazł się w dozorowanym obiekcie w ciągu okresu czasu od powiadomienia o uszkodzeniu, podanego w umowie o konserwację systemu.

Jeśli jest możliwe, to użytkownik powinien być informowany przy zgłaszaniu uszkodzenia o możliwym opóźnieniu.

## 9.5 Książka eksploatacji systemu alarmowego

Każdy system alarmowy powinien mieć swój system rejestrowania.

*Rejestrowanie wyposażenia*

Należy wpisać do rejestru nazwę i adres użytkownika oraz rozmieszczenie i typy wszystkich czujek i innych urządzeń. W konserwacji powinien być stosowany kod lub system skrótów; należy przy tym zachować poufność.

*Rejestr zdarzeń*

Każdy system alarmowy powinien mieć rejestr zdarzeń (patrz zał. F), zawierający datę każdej wizyty, wykryte uszkodzenia oraz przedsięwzięte działania. Ponadto należy w nim rejestrować każdy wywołany alarm wraz ze szczegółami o podjętym działaniu oraz, jeśli to możliwe, przyczynę alarmu.

*Zapis konserwacji*

Należy sporządzić oddzielny zapis każdego wyłączenia systemu na czas konserwacji, która powinna obejmować działania podane w punkcie 9.3. Należy też zapisać działania podjęte w celu uzupełnienia czynności, których nie wykonano w trakcie tej konserwacji z braku możliwości i datę ich realizacji.

*Rejestr obsługi awaryjnej*

Powinien być wykonany zapis daty i czasu odbioru każdego wezwania awaryjnego wraz z datą i czasem trwania niezbędnego działania.

*Zapis okresowego wyłączenia*

Okres każdego wyłączenia systemu alarmowego w całości lub jakiejkolwiek jego części powinien być zapisany. W zapisie powinna być zaznaczona każda niedziałająca w jakimkolwiek okresie czujka lub inne niedziałające wyposażenie. Powinien być podany powód ich wyłączenia oraz data ponownego włączenia. Każde wyłączenia powinno być dokonane po pisemnym upoważnieniu przez użytkownika lub jego przedstawiciela.

## 10 Audyt – przegląd techniczno-eksploatacyjny systemu

Zaleca się w organizacji korzystającej z systemów alarmowych przeprowadzanie audytów w zaplanowanych odstępach czasu, w celu określenia, czy zastosowane zabezpieczenia organizacyjno-techniczne oraz procesy i procedury z nimi związane są:

a) zgodne z dokumentacją powykonawczą;
b) zgodne z wymaganiami niniejszej specyfikacji technicznej i normami powołanymi, odpowiednimi ustawami i przepisami, uwzględniając nowe ustawy i przepisy;
c) zgodne ze zidentyfikowanymi zagrożeniami i poziomami ryzyka, uwzględniając nowe zagrożenia i ryzyka;
d) efektywnie wdrożone i eksploatowane, a systemy odpowiednio konserwowane i serwisowane;
e) zgodne z oczekiwaniami użytkownika.

Program audytu powinien zostać zaplanowany w określonych obszarach, jak również uwzględniać wyniki poprzednich audytów. Powinny być zdefiniowane kryteria stosowane w procesie audytu, zakres, częstotliwość i metody. Wybór audytorów i przeprowadzenie audytu powinny zapewnić obiektywność i bezstronność procesu. Audytorzy nie powinni prowadzić audytów dotyczących ich własnej pracy.

Wymagania i odpowiedzialność za planowanie i przeprowadzanie audytów w organizacji oraz za raportowanie ich wyników i utrzymywanie zapisów powinny być zdefiniowane w udokumentowanej procedurze.

Audytorzy powinni posiadać udokumentowane uprawnienia środowisk branżowych, potwierdzające wiedzę, doświadczenie oraz umiejętności.

**Załącznik A (informacyjny)**

**Wykaz norm użytecznych do projektowania i instalowania systemów alarmowych sygnalizacji włamania i napadu**

W załączniku przedstawiono wykaz norm powołanych w Specyfikacji. Normy te wprowadzono do Polskich Norm metodą tłumaczenia i uznaniową w języku angielskim (U). Normy są identyczne z odpowiednimi Normami Europejskimi opracowywanymi w Komitecie Technicznym CENELEC TC 79 Systemy Alarmowe.

| Lp. | Numer | Tytuł normy | Miejsce przytoczenia Uwagi |
|---|---|---|---|
| **1** | PN-EN 50130-5:2002 | Systemy alarmowe - Część 5**:** Próby środowiskowe | p. 4.7.4 |
| **2** | PN-EN 50130-4:2002/ A1:1998/A2:2002 | Systemy alarmowe - Część 4: Kompatybilność elektromagnetyczna - Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów alarmowych pożarowych, włamaniowych i osobistych | Zharmonizowana z Dyrektywą EMC 89/336/EEC<br><br>p.4.7.2 |
| **3** | PN-EN 50131-1:2009 | Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe | p.4.4. tab.2 |
| **4** | PN-EN 50131-1/IS1:2009(U) | Systemy alarmowe - Systemy sygnalizacji włamania i napadu – Interpretacje 1 | Tłumaczenie w przygotowaniu |
| **5** | PN-EN 50131-2-2:2009 | Systemy alarmowe - Systemy sygnalizacji włamania - Część 2-2: Wymagania dotyczące czujek pasywnych podczerwieni | p.4.4. tab.2 |
| **6** | PN-EN 50131-2-3:2008(U) | Systemy alarmowe - Systemy sygnalizacji włamania - Część 2-3: Wymagania dotyczące czujek mikrofalowych | Tłumaczenie w przygotowaniu |
| **7** | PN-EN 50131-2-4:2009 | Systemy alarmowe - Systemy sygnalizacji włamania - Część 2-4: Wymagania dotyczące czujek dualnych pasywnych podczerwieni i mikrofalowych | Tłumaczenie w przygotowaniu |
| **8** | PN-EN 50131-2-5:2008(U) | Systemy alarmowe - Systemy sygnalizacji włamania - Część 2-5: Wymagania dotyczące czujek dualnych pasywnych podczerwieni i ultradźwiękowych | Tłumaczenie w przygotowaniu |
| **9** | PN-EN 50131-2-6:2008(U) | Systemy alarmowe - Systemy sygnalizacji włamania - Część 2-6: Wymagania dotyczące czujek stykowych otwarcia (magnetycznych) | Tłumaczenie w przygotowaniu |
| **10** | PN-EN 50131-3:2009(U) | Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 3: Centrale alarmowe | |
| **11** | PN-CLC/TR 5015:2008(U) | Wykaz interpretacji dotyczących opublikowanych norm „Systemy alarmowe” | p.4.4. tab.2 |

| | | | |
|---|---|---|---|
| **12** | PN-EN 50131-6:2009 | Systemy alarmowe - Systemy sygnalizacji włamania – Część 6: Zasilanie | p.4.4. tab.2 |
| **13** | PN-CLC/TS 50131-7:2008(U) | Systemy alarmowe - Systemy sygnalizacji włamania - Część7: Zasady stosowania | Tłumaczenie w przygotowaniu |
| **14** | PN-EN 50131-5-3:2005(U) | Systemy alarmowe - Systemy sygnalizacji włamania - Część 5-3: Wymagania dotyczące urządzeń stosowanych do połączeń wewnętrznych wykorzystujących techniki radiowe. | |
| **15** | PN-EN 50131-5-3:2005/ A1:2008(U) | Systemy alarmowe - Systemy sygnalizacji włamania - Część 5-3: Wymagania dotyczące urządzeń stosowanych do połączeń wewnętrznych wykorzystujących techniki radiowe. | |
| **16** | PN-EN 50136-1-1:2007/ A1:2001 | Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 1-1: Wymagania ogólne dotyczące systemów transmisji alarmu | Zał. B |
| **17** | PN-EN 50136-1-1:2007/ A2:2008 | Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 1-1: Wymagania ogólne dotyczące systemów transmisji alarmu | Zał. B |
| **18** | PN-EN 50136-1-5:2008 | Systemy alarmowe - Systemy i urządzenia transmisji alarmu – Część 1-5: Wymagania dotyczące sieci z komutacją pakietów PSN | |
| **19** | PN-EN 50136-2-1:2007 | Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 2-1: Wymagania ogólne dotyczące urządzeń transmisji alarmu | |

## Załącznik B (normatywny)

## Kryteria oceny działania systemu transmisji alarmu[5]

W tablicy B.1 podano wymagania dotyczące 6 opcji systemów transmisji alarmu (ATS), wykorzystywanych zgodnie z wymaganiami tablicy 2 (punkt. 4.4).

### Tablica B. 1 – Wymagania dotyczące działania systemu transmisji alarmu

| Kryteria działania | Klasyfikacja czasu transmisji | Czas transmisji wartość maksymalna | Klasyfikacja czasu raportowania | Zabezpieczenie przed zamianą | Zabezpieczenie informacji |
|---|---|---|---|---|---|
| ATS 1 | D1 | M1 | T2 | S0 | I0 |
| ATS 2 | D2 | M2 | T2 | S0 | I0 |
| ATS 3 | D2 | M2 | T2 | S1 | I1 |
| ATS 4 | D2 | M2 | T3 | S1 | I2 |
| ATS 5 | D3 | M3 | T4 | S2 | I3 |
| ATS 6 | D4 | M4 | T6 | S2 | I3 |

Klasyfikacja zabezpieczenia zapewnianego przez system transmisji alarmu jest określona zbiorem pięciu parametrów:

D czas transmisji – klasyfikacja,

T czas raportowania,

M czas transmisji – wartości maksymalne,

S zabezpieczenie przed zamianą;

I zabezpieczenie informacji.

Wartości liczbowe tych parametrów określono w EN 50136-1-1 i w podanych niżej tablicach oraz w treści „Zabezpieczenie sygnalizacji”.

### Tablica B. 2 – Klasyfikacja czasu transmisji

| Klasa | D0<br>s | D1<br>s | D2<br>s | D3<br>s | D4<br>S |
|---|---|---|---|---|---|
| Średnia arytmetyczna ze wszystkich transmisji | - | 120 | 60 | 20 | 10 |
| Powyżej 95 % wszystkich transmisji | 240 | 240 | 80 | 30 | 15 |

### Tablica B. 3 – Czas transmisji – wartości maksymalne

| Klasa | M0<br>s | M1<br>s | M2<br>s | M3<br>s | M4<br>S |
|---|---|---|---|---|---|
| Maksymalny dopuszczalny czas transmisji | - | 480 | 120 | 60 | 20 |

### Tablica B. 4 – Klasyfikacja czasu raportowania

| Klasa/okres | Czas raportowania | | | | | |
|---|---|---|---|---|---|---|
| Klasa | T1<br>d | T2<br>h | T3<br>min | T4<br>s | T5<br>s | T6<br>s |
| Maksymalny okres | 32 | 25 | 300 | 180 | 90 | 20 |

[5] *Przedruk za zgodą Prezesa Polskiego Komitetu Normalizacyjnego – zezwolenie Nr 16/P/2009. Oryginały norm są dostępne w Wydziale Sprzedaży PKN oraz w autoryzowanych przez PKN punktach dystrybucji.*

**Zabezpieczenie sygnalizacji**

W systemie transmisji alarmu należy przewidzieć środki do zabezpieczenia lub wykrywania celowych prób zakłócania transmisji komunikatu alarmowego lub zakłócania innej informacji transmitowanej między systemem alarmowym i związanym z nim alarmowym centrum odbiorczym, przez blokowanie zamiany, jednym z podanych niżej sposobów.

**Zabezpieczenie przed zamianą:** Ochronę urządzenia nadawczo-odbiorczego systemu alarmowego przed nieuprawnioną zamianą przez podobne urządzenie włączone w łącze transmisyjne systemu transmisji alarmu, uzyskuje się jedną z następujących dróg:

**S0** brak środków;

**S1** środki do wykrycia zamiany urządzenia nadawczo-odbiorczego w dozorowanym obiekcie, polegające na wprowadzeniu identyfikatorów lub adresów do wszystkich komunikatów transmitowanych przez łącze transmisyjne alarmu;

**S2** środki do wykrycia zamiany urządzenia nadawczo-odbiorczego w dozorowanym obiekcie, polegające na:

a) szyfrowaniu lub adresowaniu wszystkich komunikatów transmitowanych przez łącze transmisyjne alarmu,

b) uwierzytelnieniu urządzenia nadawczo-odbiorczego w dozorowanym obiekcie, przez wprowadzenie w każdym dołączonym urządzeniu, różnych i ukrytych kodów lub

c) zastosowaniu innych środków określonych przez producenta.

Uwierzytelnienie wymaga zwykle zastosowania wystarczającej liczby kluczy umożliwiających działanie każdego urządzenia nadawczo-odbiorczego oznaczonego innym kodem. Liczba wszystkich różnych adresów w S2 nie powinna być mniejsza niż 250.

**Bezpieczeństwo informacji:** Ochrona informacji transmitowanej przez system transmisji alarmu powinna być utrzymywana dzięki zastosowaniu następujących środków:

**I0** brak środków,

**I1** środki zabezpieczające przed nieuprawnionym odczytem transmitowanej informacji,

UWAGA Mogą być one uzupełniane przez szyfrowanie.

**I2** środki zabezpieczające przed nieuprawnioną modyfikacją transmitowanej informacji,

UWAGA Mogą być one uzupełniane przez szyfrowanie lub przez zastosowanie kryptograficznej metody uwierzytelnienia.

**I3** środki zabezpieczające przed nieuprawnionym odczytem i modyfikacją transmitowanej informacji.

Zastosowane algorytmy kryptograficzne powinny być takie, aby w synchronicznych systemach transmisji alarmu sekwencja danych składająca się ze 100 dowolnych kolejnych bitów nie powtarzała się w ciągu kolejnych 10 000 000 bitów, a w systemach asynchronicznych sekwencja danych składająca się ze 100 dowolnych kolejnych bajtów nie powtarzała się w ciągu kolejnych 1 000 000 bajtów.

**Załącznik C (informacyjny)**

**Punkty zabezpieczenia**

W tablicy C podano propozycję dotyczącą lokalizacji stref (punktów) zabezpieczenia. Przedstawiono w zależności od klasy systemu alarmowego SA1 – SA4, odpowiednio do lokalizacji punktów/stref zabezpieczenia, zalecane środki zabezpieczenia (sygnalizacji włamania) przed otwarciem, penetracją i wejściem/ruchem intruza.

**Tablica C – Punkty zabezpieczenia**

| Rozważany punkt/strefa do zabezpieczenia | Klasa systemu alarmowego sygnalizacji włamania | | | |
|---|---|---|---|---|
| | SA1 | SA2 | SA3 | SA4 |
| Drzwi zewnętrzne | O | O | O+P | O+P |
| Okna | N | O | O+P | O+P |
| Inne otwory | N | O | O+P | O+P |
| Ściany | N | N | N | P |
| Sufity i dachy | N | N | N | P |
| Podłogi | N | N | N | P |
| Pomieszczenie | T | T | T | T |
| Przedmiot (wysokie ryzyko) | N | N | S | S |

O = otwarcie (np. sygnalizacja otwarcia przez zastosowanie czujek stykowych otwarcia/magnetycznych)

N = nie wymaga się zabezpieczenia

P = penetracja (np. zabezpieczenie struktury obiektu w celu wykrycia włamania/wejścia intruza lub ich próby; sygnalizacja penetracji np. przez zastosowanie czujek: stykowych, wibracyjnych)

T = pułapka (np. zabezpieczenie wybranego obszaru - przestrzeni, gdzie istnieje wysokie prawdopodobieństwo detekcji – wykrycia intruza; zastosowanie: czujek wykrywających ruch intruza, mat naciskowych)

S = obiekt wymagający specjalnej uwagi (np. zabezpieczenie urządzenia, szafy, kasety, sejfu, eksponatu muzealnego)

## Załącznik D (informacyjny)

### Schemat działań

Niżej podano schemat działań, w którym przedstawiono kolejno podstawowe procesy składające się na proces realizacji systemu alarmowego. Procesy wyszczególniono oddzielnie, jednak w praktyce niektóre z nich mogą być przeprowadzane równocześnie. Zaznaczono kursywą dokumenty powstałe w wyniku każdego z procesów.

**Projektowanie systemu**

- proces: wizja lokalna, analiza zagrożeń,
- proces: wizja lokalna, inne czynniki,
- dokument: *projekt wstępny systemu*.

**Planowanie instalacji**

- proces: inspekcja techniczna – potwierdzenie spełnienia wymagań projektu wstępnego,
- dokument: *poprawiony projekt wstępny systemu*,
- dokument: *plan instalacji – projekt wykonawczy*.

**Instalowanie systemu**

- proces: instalowanie systemu,
- proces: kontrola, testowanie i uruchomienie systemu,
- dokument: *dokumentacja powykonawcza.*

## Załącznik E (informacyjny)

### Niezbędne informacje zawarte w projekcie wstępnym

Wstępny projekt systemu powinien być przedstawiony klientowi albo wykonującemu specyfikacje techniczną. Projekt wstępny powinien zawierać niezbędne informacje gwarantujące klientowi lub specyfikatorowi spełnienie przez system wymagań dotyczących danego zastosowania.

### E. 1 Dane klienta

Nazwisko, adres, nazwa firmy oraz wszelkie inne informacje potrzebne do jednoznacznej identyfikacji klienta.

### E. 2 Dane nadzorowanego obiektu

Nazwa i adres nadzorowanego obiektu (np. rodzaj zabudowy, liczba kondygnacji). Przeznaczenie obiektu ( sklep, fabryka, dom).

### E.3 Poziom zabezpieczenia

Klasa planowanego systemu, klasa każdego podsystemu.

### E.4 Klasa środowiskowa

Klasa środowiskowa każdego elementu systemu.

### E.5 Zestawienie urządzeń

Zestawienie wszystkich urządzeń z podaniem ich typów i lokalizacji (w formie słownej lub schematu blokowego) oraz przewidywanego obszaru działania czujek ruchu.

### E.6 Konfiguracja systemu

Szczegóły dotyczące głównych funkcji systemu (specyfikacja funkcjonalna), wraz z włączaniem/ wyłączaniem i częściowym włączaniem (uzbrajaniem).

### E.7 Sygnalizowanie

Szczegóły dotyczące planowanych urządzeń sygnalizacyjnych, rodzaj i rozmieszczenie sygnalizatorów, urządzeń transmisji alarmu, nazwa alarmowego centrum odbiorczego, lub innego systemu oddalonego, do którego będą transmitowane sygnały.

### E.8 Legislacja

Szczegóły dotyczące wymagań nakładanych na elementy systemu lub na system wynikające z lokalnych lub państwowych przepisów prawnych (np. dopuszczalny poziom hałasu).

### E.9 Normy

Wymagania dotyczące zgodności elementów systemu lub systemu z Normą Krajową lub Europejską.

### E.10 Inne przepisy

Wymagania dotyczące zgodności elementów systemu lub systemu z wszelkimi innymi przepisami, np. publikowanymi przez firmy lub inspektoraty ubezpieczeniowe.

### E.11 Certyfikaty

Szczegóły dotyczące wymagań certyfikatów dla elementów systemu i systemu.

### E.12 Interwencja

Planowana reakcja na aktywacje alarmu i/lub awarie, np. policja, klucznik, organizacja interwencyjna, firma serwisowa.

### E.13 Konserwacja

Zalecany plan konserwacji systemu lub jego elementów włącznie ze szczegółami dotyczącymi częstotliwości każdej wizyty konserwacyjnej oraz listą czynności do wykonania w czasie każdej wizyty. W czasie serwisowania system powinien być przejrzany i przetestowany oraz wyregulowany w celu zapewnienia właściwej pracy. przykłady czynników, które należy wziąć pod uwagę przy konserwacji opisano w punkcie 9.3.

### E.14 Naprawa

Szczegóły dotyczące proponowanego serwisu, łącznie z danymi kontaktowymi (patrz punkt 9.4).

**Załącznik F (informacyjny)**

**Rejestr zdarzeń (przykład)**

**Dane podstawowe:**

Nazwa i adres ……..……

……..……

Osoba odpowiedzialna .....…….. data ……..

…….. data ……..

…….. data ……..

System zainstalowany przez …….. data ……..

Konserwowany przez …….. data ……..

Sprawdzany przez …….. data ……..

…….. data ……..

…….. data ……..

Numer telefonu/email ……. należy powiadomić, jeśli wymagany jest serwis

**Dane dotyczące zdarzenia:**

| Data | Godzina | Zdarzenie | Wymagane działanie | Data ukończenia | Podpis |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Zużyte elementy:

……

……

Do wymiany:

……

……

POLSKI KOMITET NORMALIZACYJNY

# PRODUKTY I USŁUGI PKN

... z myślą o naszych klientach!

## SPRZEDAŻ NORM I PRODUKTÓW NORMALIZACYJNYCH

- **W SKLEPIE INTERNETOWYM NA www.pkn.pl**
  **DOSTĘPNE FORMY:**
  - **plik do pobrania**
    **dostawa:** przez internet
    **płatność:** karta/przelew
  - **plik na płycie CD**
    **dostawa:** odbiór osobisty/poczta/kurier
    **płatność:** gotówka/karta/ przelew
  - **wydruk na papierze**
    **dostawa:** odbiór osobisty/poczta/kurier
    **płatność:** gotówka/karta/przelew
- **NA www.pkn.pl POPRZEZ FORMULARZ ZAMÓWIENIA**
  **DOSTĘPNE FORMY:**
  - **plik wysyłany pocztą elektroniczną**
    **dostawa:** po zaksięgowaniu wpłaty na koncie PKN
  - **plik na płycie CD**
    **dostawa:** odbiór osobisty/poczta/kurier
    **płatność:** gotówka/karta/przelew
  - **wydruk na papierze**
    **dostawa:** odbiór osobisty/poczta/kurier
    **płatność:** gotówka/karta/przelew
- **W SIEDZIBIE PKN**
  w Warszawie, ul. Świętokrzyska 14, tel. 22 556 77 77
  w Łodzi, ul. Narutowicza 75, tel. 42 678 54 60
  w Katowicach, ul. Dąbrowskiego 22, tel. 32 251 89 04, faks 32 209 91 29
  **DOSTĘPNE FORMY:**
  - **plik na płycie CD**
    **dostawa:** odbiór osobisty/poczta/kurier
    **płatność:** gotówka/karta/przelew
  - **wydruk na papierze**
    **dostawa:** odbiór osobisty/poczta/kurier,
    **płatność:** gotówka/karta/przelew

## PRENUMERATA NORM I DOKUMENTÓW NORMALIZACYJNYCH

- **ZAMÓWIENIE MOŻNA ZŁOŻYĆ W SKLEPIE INTERNETOWYM, KORZYSTAJĄC Z FORMULARZA ZAMÓWIENIA DOSTĘPNEGO NA www.pkn.pl LUB W SIEDZIBIE PKN:**
  w Warszawie, ul. Świętokrzyska 14, tel. 22 556 77 74, 22 556 77 29
  w Łodzi, ul. Narutowicza 75, tel. 42 678 54 60

## PRENUMERATA MIESIĘCZNIKA „WIADOMOŚCI PKN. NORMALIZACJA"

- **PRENUMERATĘ MOŻNA ZAMÓWIĆ W SKLEPIE INTERNETOWYM, KORZYSTAJĄC Z FORMULARZA ZAMÓWIENIA DOSTĘPNEGO NA www.pkn.pl LUB W SIEDZIBIE PKN:**
  w Warszawie, ul. Świętokrzyska 14, tel. 22 556 77 74, 22 556 77 29
  w Łodzi, ul. Narutowicza 75, tel. 42 678 54 60
  w Katowicach, ul. Dąbrowskiego 22, tel. 32 251 89 04, faks 32 209 91 29

## SPRZEDAŻ ZAGRANICZNYCH NORM I WYDAWNICTW NORMALIZACYJNYCH

- **ZAMÓWIENIA MOŻNA SKŁADAĆ W SIEDZIBIE PKN:**
  w Warszawie, ul. Świętokrzyska 14, **osobiście** lub **e-mailem**, na adres: grazyna.luniewska@pkn.pl
  w Katowicach, ul. Dąbrowskiego 22, **dzwoniąc** pod nr telefonu 32 251 89 04
  lub **wysyłając faks** pod nr 32 209 91 29
  **UWAGA! PKN W KATOWICACH REALIZUJE TYLKO ZAMÓWIENIA NA NIEMIECKIE NORMY I WYDAWNICTWA NORMALIZACYJNE.**

## INFORMACJA NORMALIZACYJNA

- **UDZIELANA POD NR TELEFONU: 22 556 77 55 (WARSZAWA), 42 678 54 60 (ŁÓDŹ), 32 251 89 04 lub 32 359 79 61 (KATOWICE). Opłata za przygotowanie specjalistycznej informacji - wg cennika PKN dostępnego na www.pkn.pl**
  Zakres usługi obejmuje m. in. opracowywanie wykazów norm na zamówiony temat, informację o wprowadzeniu norm międzynarodowych i europejskich do norm krajowych oraz informację dotyczącą sprawdzenia aktualności norm

## CZYTELNIA NORM

- **W SIEDZIBIE PKN**
  w Warszawie, ul. Świętokrzyska 14, tel. 22 556 76 50, czynna w godzinach $9^{00}$-$16^{00}$
  w Łodzi, ul. Narutowicza 75, tel. 42 678 54 60, czynna w godzinach $8^{30}$-$15^{30}$
  w Katowicach, ul. Dąbrowskiego 22, tel. 32 251 89 04, czynna w godzinach $9^{00}$-$15^{00}$
  **Czytelnia czynna w dni robocze.**