

(PL) Ważne informacje dotycząc bezpieczeństwa i użytkowania produktów z grupy

SYSTEMY ALARMOWE (Systemy Sygnalizacji Włamania i Napadu)

Ostrzeżenia i zalecenia ogólne

Urządzenia z zakresu Systemów Alarmowych takie jak czujki, centrale, zasilacze, moduły rozszerzeń, sygnalizatory są produktami profesjonalnymi. Ich nieprawidłowy lub niezgodny z przeznaczeniem montaż i konfiguracja może uszkodzić urządzenie lub stwarzać zagrożenie dla użytkownika.

Pamiętaj!

System alarmowy wraz z jego poszczególnymi elementami nie stanowi niezawodnej ochrony przed włamaniem czy napadem, jego podstawowym celem jest szybkie wykrycie zagrożenia i przekazanie sygnału alarmowego. Aby zapewnić skuteczność działania, instalację systemu należy zlecić profesjonalistom, którzy posiadają odpowiednie kwalifikacje i doświadczenie. Fachowcy nie tylko zamontują urządzenie, ale również dokładnie wyjaśnią zasady jego obsługi, a także zapewnią regularne przeglądy techniczne i testowanie. Dzięki temu użytkownik będzie mógł korzystać z systemu w sposób bezpieczny i efektywny, minimalizując ryzyko ewentualnych usterek lub nieprawidłowego działania.

Ostrzeżenia ogólne

Potencjalne zagrożenia:

1. Zagrożenia fizyczne:

- **Uszkodzenia mechaniczne:** Niewłaściwa instalacja lub eksploatacja może prowadzić do uszkodzeń mechanicznych komponentów, co może skutkować nieprawidłowym działaniem systemu alarmowego

2. Zagrożenia elektryczne:

- **Przebiecia i zwarcia:** Nieodpowiednia izolacja lub błędy w instalacji mogą prowadzić do przebiecia, zwarcia i porażeń prądem.

3. Zagrożenia cyberbezpieczeństwa:

- **Produkt** musi być zabezpieczony przed nieautoryzowanym dostępem (np. poprzez stosowanie silnych haseł). Brak zabezpieczeń może prowadzić do przejęcia kontroli nad systemem przez osoby trzecie.

Ostrzeżenia:

- **Instalacja i konserwacja:** Produkty powinny być instalowane i konserwowane wyłącznie przez wykwalifikowany personel zgodnie z instrukcjami producenta.
- **Bezpieczeństwo elektryczne:** Przed rozpoczęciem prac instalacyjnych należy upewnić się, że zasilanie jest odłączone, aby uniknąć ryzyka porażenia prądem.
- **Ochrona przed przebieciami:** Zaleca się stosowanie odpowiednich zabezpieczeń przeciwprzebieciowych w celu ochrony sprzętu przed uszkodzeniami.
- **Zabezpieczenia sieciowe:** Należy wdrożyć odpowiednie środki bezpieczeństwa, takie jak firewall, systemy wykrywania intruzów oraz regularne aktualizacje oprogramowania, aby chronić sieć, do której podłączony jest system, przed atakami.

- **Produkty nie są odporne na działanie wody** (chyba że wskazano inaczej w specyfikacji). Nie używać urządzenia w wilgotnym środowisku, w pobliżu cieczy lub w miejscach narażonych na bezpośrednie działanie warunków atmosferycznych

Zalecenia:

1. Bezpieczna instalacja

- Przed rozpoczęciem instalacji upewnij się, że system jest wyłączony z sieci elektrycznej.
- Przeprowadź weryfikację kompatybilności systemu z istniejącą infrastrukturą

2. Testy funkcjonalności

- Po zakończeniu instalacji przeprowadź testy działania, aby upewnić się, że system działa zgodnie z założeniami producenta.
- Regularnie przeprowadzaj przeglądy techniczne i diagnostykę systemu.

3. Projektowanie i instalacja:

- **Zgodność z normami:** Upewnij się, że wszystkie komponenty spełniają obowiązujące normy i standardy bezpieczeństwa.
- **Planowanie infrastruktury:** Dokładnie zaplanuj trasę okablowania, uwzględniając czynniki takie jak zakłócenia elektromagnetyczne i łatwość dostępu do konserwacji.

4. Konserwacja i monitorowanie:

- **Regularne inspekcje:** Przeprowadzaj regularne kontrole stanu fizycznego komponentów oraz monitoruj wydajność systemu w celu wczesnego wykrywania potencjalnych problemów.
- **Aktualizacje oprogramowania:** Regularnie aktualizuj oprogramowanie urządzeń, aby zapewnić ochronę przed nowymi zagrożeniami.

5. Szkolenie personelu:

- **Edukacja w zakresie bezpieczeństwa:** Zapewnij personelowi odpowiednie szkolenia dotyczące najlepszych praktyk w zakresie instalacji, konserwacji oraz bezpieczeństwa sieci.

6. Zarządzanie dostępem:

- **Kontrola dostępu:** Wprowadź mechanizmy kontroli dostępu do infrastruktury sieciowej, aby zapobiec nieautoryzowanemu dostępowi.

7. Dokumentacja:

- **Prowadzenie ewidencji:** Dokumentuj wszystkie prace instalacyjne, konserwacyjne oraz incydenty związane z bezpieczeństwem, aby umożliwić analizę i doskonalenie procedur

W przypadku urządzeń z wymiennymi bateriami należy zachować szczególną ostrożność:

Nie połykaj baterii! Grozi to poważnym poparzeniem chemicznym. Połknięcie baterii guzikowej może w spowodować ciężkie uszkodzenia wewnętrzne, a nawet doprowadzić do śmierci.

Używaj odpowiedniego typu baterii. Wymiana na niewłaściwy typ, szczególnie w przypadku niektórych baterii litowych, może uszkodzić urządzenie lub grozić wybuchem.

Nie wrzucaj baterii do ognia, nie zgniataj i nie przecinaj ich. Takie działania mogą doprowadzić do eksplozji.

Unikaj ekstremalnych temperatur. Przechowywanie baterii w bardzo wysokiej temperaturze może spowodować eksplozję, wyciek łatwopalnej cieczy lub gazu. Ekspozycja na skrajnie niskie ciśnienie powietrza niesie podobne ryzyko.

Dbaj o właściwą utylizację. Zużyte baterie oddawaj do punktów recyklingu, zgodnie z obowiązującymi przepisami. Nie wrzucaj ich do zwykłych koszy na odpady.

Zachowując powyższe zasady, minimalizujesz ryzyko związane z użytkowaniem i utylizacją baterii.

UWAGA!

Jeśli z urządzenia wydobywa się dym, zapachy lub hałas, natychmiast wyłącz zasilanie i odłącz kabel zasilający, a następnie skontaktuj się z instalatorem lub centrum serwisowym.

Pamiętaj!

Jeśli twoje urządzenie będzie łączyło się z Internetem lub inną siecią komputerową dobierz właściwe urządzenia pośredniczące (switch, router, modem) i zadbaj o ich odpowiednią konfigurację. Skorzystaj z wiedzy fachowców aby zapewnić swojej instalacji wysoki poziom cyberbezpieczeństwa

Ochrona środowiska. Selektywna zbiórka odpadów.

Wyeksploatowane, zużyte, zepsute urządzenia elektryczne i elektroniczne muszą być gromadzone oddzielnie i poddawane recyklingowi w sposób zgodny z przepisami o ochronie środowiska (europejska dyrektywa w sprawie zużytego sprzętu elektrycznego i elektronicznego). W celu utylizacji starych urządzeń elektrycznych i elektronicznych należy skorzystać z systemu zbiórki tego typu odpadów obowiązującego w danym kraju.

Znak CE umieszczony na urządzeniu oznacza, że urządzenie jest zgodne z obowiązującymi dyrektywami CE i jest bezpieczne.

Ostrzeżenia szczegółowe dotyczące:

Czujki Alarmowe

- przed podłączeniem czujki do centrali lub innych elementów wyłącz zasilanie urządzeń
- w przypadku czujek zasilanych prądem elektrycznym stosuj się do zasad bezpieczeństwa obowiązujących w Twoim kraju
- stosuj tylko zalecane przez producenta zasilacze i kable zasilające
- przed demontażem czujki wyłącz jej zasilanie
- w przypadku montażu sufitowego lub ściennego wykorzystuj tylko stabilne podłoże
- nie montuj czujek na ruchomych elementach lub elementach które mogą wibrować
- korzystaj z załączonych lub dedykowanych przez producenta uchwytów montażowych
- w przypadku montażu w warunkach zewnętrznych upewnij się w karcie katalogowej lub instrukcji czy dana czujka jest przystosowana do pracy na zewnątrz pomieszczeń, jeśli nie jest nie montuj jej.
- wszystkie operacje elektroniczne powinny być ściśle zgodne z lokalnymi przepisami dotyczącymi bezpieczeństwa elektrycznego, ochrony przeciwpożarowej oraz innymi powiązanymi regulacjami.
- nie upuszczaj urządzenia ani nie narażaj go na wstrząsy fizyczne, a także nie wystawiaj go na działanie silnego promieniowania elektromagnetycznego. Unikaj instalowania urządzenia na powierzchniach wibrujących lub w miejscach narażonych na wstrząsy (ignorowanie tego może spowodować uszkodzenie urządzenia).
- upewnij się, że zasilanie zostało odłączone przed podłączeniem, instalacją lub demontażem urządzenia.
- jeśli z urządzenia wydobywa się dym, zapachy lub hałas, natychmiast wyłącz zasilanie i odłącz kabel zasilający, a następnie skontaktuj się z centrum serwisowym.
- nie umieszczaj urządzenia w ekstremalnie gorących (odnieś się do specyfikacji urządzenia w celu uzyskania szczegółowych informacji o temperaturze pracy), zimnych, zakurzonych lub wilgotnych miejscach
- brud, kurz lub pajęczyny mogą zakłócić pracę czujki i obniżyć jej skuteczność.
- urządzenie przeznaczone do użytku wewnętrznego powinno być chronione przed deszczem i wilgocią. Wystawianie urządzenia na bezpośrednie działanie promieni słonecznych, słabą wentylację lub źródła ciepła, takie jak grzejniki czy kaloryfery, jest zabronione (ignorowanie tego może spowodować zagrożenie pożarowe).
- nie kieruj urządzenia na słońce lub wyjątkowo jasne miejsca. Może to powodować zjawisko rozbłysku lub smugi (co nie jest usterką, ale może wpływać na trwałość sensora).
- w przypadku urządzeń zasilanych bateryjnie nieprawidłowe użycie lub wymiana baterii może spowodować ryzyko eksplozji. Wymieniaj baterię wyłącznie na taki sam lub równoważny typ. Zużyte baterie utylizuj zgodnie z instrukcjami producenta baterii.
- nie wystawiaj urządzenia na działanie gazów korozyjnych. Może to spowodować uszkodzenie sprzętu.
- stosowanie standardowych czujek w środowiskach z obecnością gazów palnych lub pyłów wybuchowych może prowadzić do wybuchu.
- błędy w konfiguracji parametrów detekcji (np. zasięgu lub czułości) mogą prowadzić do braku reakcji w sytuacji zagrożenia.

Centrale Alarmowe, Klawiatury, elementy rozszerzeń

- nie umieszczaj urządzenia bezpośrednio na podłożu do instalacji wykorzystaj elementy takie jak dedykowane obudowy
- centralę należy instalować w miejscu trudno dostępnym dla osób nieupoważnionych.
- należy unikać montażu w miejscach narażonych na wilgoć, bezpośrednie działanie promieni słonecznych, wibracje lub skrajne temperatury.
- używaj dedykowanego zasilacza zgodnego z parametrami technicznymi centrali.
- upewnij się, że dostępne jest awaryjne zasilanie, np. akumulator, na wypadek przerw w dostawie prądu.
- centrala powinna być prawidłowo uziemiona, aby zapobiec uszkodzeniom w wyniku przepięć lub wyładowań atmosferycznych.
- montuj centralę z dala od urządzeń generujących silne pole elektromagnetyczne, takich jak transformatory czy duże maszyny elektryczne.
- zabezpiecz centralę hasłem dostępu, a hasło regularnie zmieniaj.
- używaj różnych poziomów uprawnień dla użytkowników w zależności od ich funkcji.
- regularnie aktualizuj firmware centrali, aby zabezpieczyć system przed nowymi zagrożeniami cybernetycznymi
- regularnie sprawdzaj dzienniki zdarzeń w celu wykrycia nietypowych aktywności.
- jeśli centrala jest podłączona do sieci, używaj zapór sieciowych i szyfrowanych połączeń do komunikacji.
- wykonuj okresowe przeglądy techniczne zgodnie z zaleceniami producenta.
- sprawdzaj stan okablowania, połączeń i urządzeń peryferyjnych (np. czujek, sygnalizatorów).
- regularnie przeprowadzaj testy systemu alarmowego, aby upewnić się, że wszystkie funkcje działają poprawnie.
- sprawdzaj i wymieniaj akumulatory awaryjne zgodnie z zaleceniami producenta, aby zapobiec ich rozładowaniu.
- odłącz zasilanie przed podłączeniem, demontażem lub serwisowaniem centrali.
- używaj odpowiednich narzędzi i środków ochrony osobistej, np. rękawic antystatycznych.
- nie podłączaj więcej urządzeń peryferyjnych niż przewiduje specyfikacja centrali.
- zużyte akumulatory i inne elementy utylizuj zgodnie z lokalnymi przepisami ochrony środowiska.
- ogranicz dostęp do systemu do minimum niezbędnego personelu i urządzeń.
- upewnij się, że instalacja i użytkowanie centrali alarmowej są zgodne z lokalnymi przepisami i normami bezpieczeństwa.
- unikaj montażu w miejscach narażonych na wilgoć, silne nasłonecznienie, pył, wibracje czy ekstremalne temperatury.
- chroń manipulator przed przypadkowymi uderzeniami, wstrząsami lub próbami manipulacji przez osoby nieuprawnione.
- używaj przewodów o odpowiedniej długości i przekroju zgodnie z instrukcją producenta
- sprawdź zgodność parametrów zasilania modułu z centralą alarmową i zainstaluj odpowiednie zabezpieczenia, np. bezpieczniki.
- moduły powinny być chronione przed dostępem osób nieuprawnionych, aby zapobiec manipulacji lub sabotażowi.
- jeśli moduł obsługuje aktualizacje firmware'u, należy je regularnie przeprowadzać.

- okresowe testy systemu są niezbędne, aby upewnić się, że wszystkie komponenty działają zgodnie z założeniami.
- instalacja powinna być zgodna z obowiązującymi normami i przepisami dotyczącymi systemów alarmowych.

Sygnalizatory

- sygnalizator powinien być zamontowany w miejscu niedostępnym dla osób niepowołanych, np. na wysokości uniemożliwiającej łatwe manipulowanie urządzeniem.
- unikać miejsc narażonych na bezpośrednie działanie wody, wilgoci, lub intensywnych źródeł ciepła (chyba, że urządzenie jest przeznaczone do montażu na zewnątrz).
- sygnalizator powinien mieć funkcję detekcji sabotażu (np. czujnik otwarcia obudowy, oderwania od ściany) oraz być zamontowany w sposób utrudniający jego usunięcie lub uszkodzenie.
- należy zabezpieczyć urządzenie przed przypadkowym uszkodzeniem, np. uderzeniami czy upadkiem przedmiotów.
- sygnalizator musi być zasilany zgodnie z zaleceniami producenta. Niewłaściwe napięcie może doprowadzić do uszkodzenia urządzenia lub wywołania fałszywych alarmów.
- należy regularnie sprawdzać, czy sygnalizator emituje właściwy poziom hałasu i światła (zgodny z normami).
- urządzenie musi być solidnie zamocowane, aby wytrzymać silne wiatry, wibracje czy próby manipulacji.
- instalacja sygnalizatorów powinna być wykonana przez przeszkolony personel zgodnie z dokumentacją techniczną producenta.
- testy funkcjonalne sygnalizatorów powinny być przeprowadzane w ramach diagnostyki całego systemu alarmowego.
- należy zachować instrukcje obsługi i dokumentację techniczną, aby umożliwić szybkie rozwiązywanie problemów i przeprowadzanie konserwacji.

Urządzenia radiowe

- w przypadku bezprzewodowych central alarmowych unikaj instalacji urządzenia na powierzchniach metalowych.
- w przypadku bezprzewodowych central alarmowych nie wolno owijać urządzenia metalem.
- w przypadku bezprzewodowych central alarmowych unikaj przeszkód w odległości 50 cm wokół urządzenia, z wyjątkiem powierzchni montażowej.
- w przypadku bezprzewodowych central alarmowych retransmitery sygnału (Repeater) należy zainstalować pomiędzy panelem sterującym a urządzeniami peryferyjnymi.
- zaleca się sprawdzić siłę sygnału przed instalacją zaleca się montaż urządzenia w miejscu, w którym poziom sygnału będzie zbliżony do 100% (Nie zakrywaj czujnika rękami podczas sprawdzania siły sygnału).
- bezprzewodowe urządzenia alarmowe mogą być podatne na zakłócenia ze strony innych urządzeń pracujących w tej samej częstotliwości. Należy zadbać o odpowiednie kanały pracy oraz unikanie obszarów o dużym natężeniu fal radiowych.

- urządzenia powinny mieć wbudowane mechanizmy wykrywania prób zakłócania sygnału (np. funkcja "antyjamming").
- należy upewnić się, że wszystkie urządzenia znajdują się w zasięgu centrali alarmowej i że sygnał radiowy nie jest blokowany przez ściany, metalowe elementy czy urządzenia elektroniczne.
- dane przesyłane między urządzeniami powinny być odpowiednio szyfrowane, aby zapobiec przechwyceniu lub manipulacji przez osoby niepowołane.
- wszystkie urządzenia radiowe muszą być montowane zgodnie z zaleceniami producenta, uwzględniając optymalne rozmieszczenie dla sygnału.
- system należy testować okresowo, aby upewnić się, że urządzenia bezprzewodowe komunikują się poprawnie z centralą.
- urządzenia radiowe są zwykle zasilane bateriami, które należy regularnie wymieniać. Upewnij się, że centralka informuje o niskim poziomie baterii w urządzeniach.
- systemy radiowe wymagają regularnych przeglądów oraz testów działania, aby zapewnić ich niezawodność.

Zasilacze i akumulatory

- zasilacze mogą się przegrzewać podczas długotrwałego użytkowania. Upewnij się, że otwory wentylacyjne nie są zablokowane.
- używaj zasilaczy zgodnych z wymaganiami urządzenia docelowego (napięcie, natężenie, moc), aby zapobiec przeciążeniu.
- podłączanie urządzeń o wyższej mocy niż obsługiwana przez zasilacz może prowadzić do uszkodzenia urządzenia lub pożaru.
- podłączenie zasilacza do sieci o napięciu wykraczającym poza jego specyfikację może skutkować porażeniem prądem lub uszkodzeniem.
- nie używaj zasilacza z uszkodzonym kablem lub obudową. Może to prowadzić do porażenia prądem lub zwarcia.
- przetadowanie lub zwarcie akumulatora może prowadzić do wybuchu lub pożaru.
- uszkodzone akumulatory mogą wydzielać szkodliwe substancje chemiczne, powodujące podrażnienia skóry, oczu i dróg oddechowych.
- przechowywanie lub używanie akumulatorów w ekstremalnych temperaturach (zbyt wysokich lub zbyt niskich) może spowodować ich uszkodzenie.
- użycie nieodpowiedniej ładowarki lub parametrów ładowania może prowadzić do przetadowania, uszkodzenia ogniw lub pożaru.
- istnieje ryzyko porażenia prądem elektrycznym wynikające z kontaktu z odłoniętymi przewodami, uszkodzoną izolacją lub nieprawidłowym uziemieniem.
- zasilacze bez odpowiednich filtrów mogą zakłócać pracę innych urządzeń elektronicznych
- niewłaściwie dobrany zasilacz może uszkodzić urządzenia podłączone do niego
- używaj tylko zasilaczy certyfikowanych zgodnych z normami bezpieczeństwa (np. CE, UL)
- regularnie sprawdzaj stan kabli, wtyczek i obudowy pod kątem uszkodzeń.
- zapewnij odpowiednią wentylację wokół zasilacza, aby zapobiec przegrzaniu.
- nie podłączaj urządzeń o mocy większej niż dopuszczalna dla zasilacza.
- nie upuszczaj akumulatorów ani nie używaj ich, jeśli są widocznie uszkodzone.
- używaj akumulatorów tylko w temperaturze określonej przez producenta.

- akumulatory zużyte lub uszkodzone należy utylizować w wyznaczonych punktach zgodnie z lokalnymi przepisami.

Moduły komunikacyjne

- moduły mogą doświadczać zakłóceń sygnału w obszarach o słabym zasięgu sieci komórkowej, co może ograniczyć ich funkcjonalność.
- antena GSM musi być prawidłowo zamontowana i umieszczona w odpowiednim miejscu, aby uniknąć utraty sygnału.
- moduły GSM mogą być podatne na celowe zakłócenia sygnału (jamming), które uniemożliwią przesyłanie danych.
- użycie karty SIM z niewystarczającym planem danych lub niewłaściwej dla danego operatora może prowadzić do przerw w komunikacji.
- moduły IP mogą przestać działać w przypadku awarii lokalnej sieci internetowej lub problemów z dostawcą usług.
- moduły IP mogą być celem cyberataków, takich jak przejęcie kontroli nad modułem czy modyfikacja danych przesyłanych w sieci.
- błędne ustawienia sieciowe (np. niewłaściwy adres IP, niewłaściwe DNS) mogą uniemożliwić poprawne działanie modułu.
- moduł IP może przestać działać w przypadku przeciążenia lokalnej sieci lub routera.
- w przypadku braku zasięgu sieci GSM, alarmy i powiadomienia mogą nie zostać przesłane.
- nieodpowiedni plan taryfowy dla karty SIM może generować wysokie koszty, szczególnie w przypadku przesyłania danych w roamingu.
- utrata połączenia internetowego uniemożliwi przesyłanie sygnałów alarmowych do stacji monitorowania lub użytkownika.
- luki w zabezpieczeniach mogą umożliwić ataki na system alarmowy.
- rozważ połączenie GSM jako rezerwowe w systemach, gdzie podstawową komunikację zapewnia moduł IP.
- regularnie aktualizuj firmware modułu i stosuj silne hasła dostępne.
- ogranicz dostęp do modułów komunikacyjnych tylko do autoryzowanych użytkowników

(EN) Important Information on Safety and Use of Products in the Group

ALARM SYSTEMS (Intruder & Hold Up Alarm Systems)

Warnings and General Recommendations

Devices in the Alarm Systems category, such as detectors, control panels, power supplies, expansion modules, and signalers, are professional products. Incorrect or improper installation and configuration may damage the device or pose a threat to the user.

Remember!

An alarm system and its individual components do not provide infallible protection against burglary or robbery. Its primary purpose is to detect threats quickly and transmit an alarm signal. For effective operation, the system installation should be entrusted to professionals with appropriate qualifications and experience. Experts will not only install the device but also thoroughly explain its operation and ensure regular maintenance and testing. This allows users to use the system safely and efficiently, minimizing the risk of malfunctions or improper functioning.

General Warnings

Potential Hazards:

1. Physical Hazards:

- **Mechanical damage:** Improper installation or operation may lead to mechanical damage to components, resulting in system malfunction.

2. Electrical Hazards:

- **Surges and short circuits:** Inadequate insulation or installation errors may cause surges, short circuits, or electric shock.

3. Cybersecurity Risks:

- The product must be secured against unauthorized access (e.g., using strong passwords). A lack of proper security measures may result in the system being compromised by third parties.

Warnings:

- **Installation and Maintenance:** Products should only be installed and maintained by qualified personnel in accordance with the manufacturer's instructions.
- **Electrical Safety:** Ensure the power supply is disconnected before starting installation to avoid the risk of electric shock.
- **Surge Protection:** It is recommended to use appropriate surge protection to safeguard equipment from damage.
- **Network Security:** Implement security measures, such as firewalls, intrusion detection systems, and regular software updates, to protect the network connected to the system from attacks.

- **Environmental Resistance:** Unless specified otherwise, products are not waterproof. Do not use the device in damp environments, near liquids, or in areas exposed to weather conditions.
-

Recommendations

1. Safe Installation:

- Ensure the system is disconnected from the electrical network before installation.
- Verify system compatibility with the existing infrastructure.

2. Functionality Tests:

- After installation, conduct functionality tests to ensure the system operates according to the manufacturer's specifications.
- Perform regular technical inspections and diagnostics.

3. Design and Installation:

- **Compliance with Standards:** Ensure all components meet applicable safety and regulatory standards.
- **Infrastructure Planning:** Plan cable routing carefully, considering factors such as electromagnetic interference and maintenance access.

4. Maintenance and Monitoring:

- Conduct regular inspections of the physical condition of components and monitor system performance to detect potential problems early.
- Regularly update device software to protect against new threats.

5. Staff Training:

- Provide personnel with appropriate training on best practices for installation, maintenance, and network security.

6. Access Management:

- Implement access control mechanisms to secure network infrastructure and prevent unauthorized access.

7. Documentation:

- Document all installation, maintenance work, and security-related incidents to enable analysis and procedure improvement.
-

Special Care for Devices with Replaceable Batteries:

- **Do not swallow batteries!** Button batteries can cause severe chemical burns if ingested, leading to serious internal injuries or death.

- Use only the correct battery type. Replacing with an incorrect type, especially certain lithium batteries, may damage the device or pose an explosion risk.
- Do not throw batteries into fire, crush, or cut them, as this can cause explosions.
- Avoid extreme temperatures. Storing batteries in very high temperatures can cause explosions, leakage of flammable liquids, or gases.
- Dispose of used batteries properly at recycling points according to applicable regulations.

WARNING:

If the device emits smoke, odors, or unusual noise, immediately disconnect the power and contact the installer or service center.

Cybersecurity Recommendations:

If your device connects to the Internet or another network, select appropriate intermediary devices (e.g., switches, routers, modems) and configure them securely. Use expert knowledge to ensure your installation maintains a high level of cybersecurity.

Environmental Protection - Selective Waste Collection:

Used, worn-out, or damaged electrical and electronic devices must be collected separately and recycled in accordance with environmental protection regulations (European directive on waste electrical and electronic equipment). Use the designated collection systems for such waste in your country.

The CE mark on the device indicates compliance with applicable CE directives and safety standards.

Detailed Warnings for:**Alarm Detectors**

- Disconnect the power supply before connecting the detector to the control panel or other components.
- For detectors powered by electricity, follow the safety regulations applicable in your country.
- Use only power supplies and cables recommended by the manufacturer.
- Disconnect the power supply before disassembling the detector.
- For ceiling or wall mounting, use only stable surfaces.
- Do not install detectors on moving elements or components that may vibrate.
- Use mounting brackets provided or recommended by the manufacturer.
- For outdoor installations, verify in the product's specification or manual that the detector is suitable for outdoor use. If it is not, do not install it outdoors.

- Ensure all electrical operations comply with local regulations for electrical safety, fire protection, and other relevant standards.
- Avoid dropping the device or subjecting it to physical shocks, and do not expose it to strong electromagnetic radiation. Do not install the device on vibrating surfaces or in areas prone to shocks (ignoring this may damage the device).
- Confirm that the power supply is disconnected before connecting, installing, or removing the device.
- If the device emits smoke, odors, or noise, immediately disconnect the power supply and contact the service center.
- Do not place the device in extremely hot, cold, dusty, or damp locations (refer to the product specification for operational temperature details).
- Dirt, dust, or cobwebs can disrupt detector operation and reduce its efficiency.
- Indoor-use devices should be protected from rain and moisture. Do not expose them to direct sunlight, poor ventilation, or heat sources like radiators (ignoring this may cause a fire hazard).
- Avoid directing the device at the sun or excessively bright areas. This can cause glare or streaks (not a defect, but it may affect sensor durability).
- For battery-powered devices, improper use or replacement of the battery can result in an explosion risk. Replace batteries only with the same or equivalent type. Dispose of used batteries following the manufacturer's instructions.
- Do not expose the device to corrosive gases as this may damage the equipment.
- Using standard detectors in environments with flammable gases or explosive dust can lead to explosions.
- Errors in configuring detection parameters (e.g., range or sensitivity) can lead to a failure to respond in an emergency.

Alarm Control Panels, Keypads, and Expansion Components

- Do not place the device directly on the surface; use dedicated enclosures or other mounting elements.
- Install the control panel in a location inaccessible to unauthorized individuals.
- Avoid installing in areas exposed to moisture, direct sunlight, vibrations, or extreme temperatures.
- Use a dedicated power supply compatible with the technical specifications of the control panel.
- Ensure backup power, such as a battery, is available in case of power outages.
- Properly ground the control panel to prevent damage from surges or lightning strikes.

- Install the control panel away from devices generating strong electromagnetic fields, such as transformers or heavy electrical machinery.
- Protect the control panel with a password, and change the password regularly.
- Assign different permission levels to users based on their roles.
- Regularly update the firmware of the control panel to protect against new cybersecurity threats.
- Regularly check event logs for unusual activities.
- If the control panel is connected to a network, use firewalls and encrypted communication.
- Conduct periodic technical inspections per the manufacturer's recommendations.
- Check the condition of wiring, connections, and peripheral devices (e.g., detectors, signalers).
- Regularly test the alarm system to ensure all functions operate correctly.
- Check and replace backup batteries per the manufacturer's guidelines to prevent depletion.
- Disconnect the power supply before connecting, disassembling, or servicing the control panel.
- Use appropriate tools and personal protective equipment, such as anti-static gloves.
- Do not connect more peripheral devices than specified by the control panel.
- Dispose of used batteries and other components per local environmental regulations.
- Restrict system access to essential personnel and devices only.
- Ensure the installation and use of the alarm control panel comply with local laws and safety standards.
- Avoid installing in areas exposed to moisture, excessive sunlight, dust, vibrations, or extreme temperatures.
- Protect keypads from accidental impacts, shocks, or tampering by unauthorized individuals.
- Use wires of appropriate length and cross-section as specified in the manufacturer's instructions.
- Verify the power supply parameters for compatibility with the control panel and install suitable protective measures, such as fuses.
- Protect modules from unauthorized access to prevent tampering or sabotage.
- If the module supports firmware updates, perform them regularly.
- Periodic system tests are necessary to ensure all components work as intended.
- Installation should comply with applicable standards and regulations for alarm systems.

Signalers

- Install the signaler in a location inaccessible to unauthorized individuals, e.g., at a height that prevents easy tampering.
- Avoid locations exposed to water, moisture, or intense heat unless the device is specifically designed for outdoor installation.
- Signalers should have sabotage detection features (e.g., cover tamper sensors or removal detection) and be mounted securely to prevent removal or damage.
- Protect the device from accidental damage, such as impacts or falling objects.
- Ensure the signaler is powered per the manufacturer's recommendations. Incorrect voltage may damage the device or cause false alarms.
- Regularly verify that the signaler emits the correct noise and light levels (per standards).
- The device must be securely fixed to withstand strong winds, vibrations, or tampering attempts.
- Signalers should be installed by trained personnel following the manufacturer's technical documentation.
- Perform functional tests of signalers as part of diagnostics for the entire alarm system.
- Retain user manuals and technical documentation to facilitate quick problem resolution and maintenance.

Wireless Devices

- For wireless alarm panels, avoid installing devices on metallic surfaces.
- Do not wrap the device in metal materials.
- Keep a 50 cm radius around the device free of obstacles, except for the mounting surface.
- Install repeaters between the control panel and peripheral devices if necessary.
- Verify the signal strength before installation and place the device where signal strength approaches 100%. (Do not cover the detector with your hands while checking the signal strength.)
- Wireless alarm devices may experience interference from other devices operating at the same frequency. Ensure appropriate channel allocation and avoid areas with high radio wave density.
- Devices should include mechanisms to detect signal jamming (e.g., "anti-jamming" functionality).
- Ensure all devices are within the range of the alarm control panel and that the radio signal is not obstructed by walls, metal elements, or electronic devices.

- Transmitted data should be encrypted to prevent interception or tampering by unauthorized individuals.
 - Install wireless devices according to the manufacturer's recommendations, considering optimal signal placement.
 - Periodically test the system to confirm proper communication between wireless devices and the control panel.
 - Wireless devices are often battery-powered; replace batteries regularly. Ensure the control panel alerts for low battery levels in devices.
 - Wireless systems require regular inspections and functional tests to ensure reliability.
-

Power Supplies and Batteries

- Power supplies may overheat during prolonged use. Ensure ventilation openings are not blocked.
- Use power supplies that meet the device's requirements (voltage, current, power) to avoid overloading.
- Connecting devices with higher power consumption than the power supply supports may damage the device or cause a fire.
- Connecting the power supply to a voltage source outside its specifications may result in electric shock or damage.
- Do not use a power supply with damaged cables or casings, as this may cause electric shock or short circuits.
- Overcharging or short-circuiting a battery can result in an explosion or fire.
- Damaged batteries may release harmful chemicals, causing skin, eye, and respiratory irritation.
- Storing or using batteries in extreme temperatures (too high or too low) may damage them.
- Using an improper charger or charging parameters may lead to overcharging, cell damage, or fire.
- There is a risk of electric shock from exposed wires, damaged insulation, or improper grounding.
- Power supplies without proper filters may interfere with other electronic devices.
- Incorrectly selected power supplies may damage connected devices.
- Use only certified power supplies compliant with safety standards (e.g., CE, UL).
- Regularly inspect cables, plugs, and casings for damage.
- Ensure adequate ventilation around the power supply to prevent overheating.
- Do not connect devices exceeding the power supply's maximum output.

- Do not drop batteries or use them if visibly damaged.
 - Use batteries only within the temperature range specified by the manufacturer.
 - Dispose of used or damaged batteries at designated points in accordance with local regulations.
-

Communication Modules

- Modules may experience signal interference in areas with weak cellular network coverage, limiting functionality.
- Ensure the GSM antenna is properly mounted and placed to avoid signal loss.
- GSM modules may be vulnerable to deliberate signal interference (jamming), preventing data transmission.
- Using a SIM card with insufficient data plans or incompatible with the operator may disrupt communication.
- IP modules may cease functioning in the event of local internet network failure or service provider issues.
- IP modules may be targeted by cyberattacks, such as module control takeover or data tampering.
- Incorrect network settings (e.g., wrong IP address, DNS) may hinder proper module operation.
- IP modules may fail in the event of network or router overload.
- In areas without GSM network coverage, alarms and notifications may not be transmitted.
- Inappropriate SIM card plans may incur high costs, especially for data transmission in roaming.
- Loss of internet connection will prevent alarm signals from being sent to monitoring stations or users.
- Security vulnerabilities may expose the alarm system to attacks.
- Consider GSM connectivity as a backup in systems where the primary communication is provided by an IP module.
- Regularly update module firmware and use strong passwords.
- Limit communication module access to authorized users only.

(LT) Svarbi informacija apie saugumą ir produktų iš grupės

ALARMŲ SISTEMOS naudojimą

Įspėjimai ir bendrosios rekomendacijos

Signalizacijos sistemų įrenginiai, tokie kaip jutikliai, valdymo pultai, maitinimo šaltiniai, plėtimo moduliai ir signalizatoriai, yra profesionalūs produktai. Netinkamas ar ne pagal paskirtį atliktas montavimas ir konfigūravimas gali sugadinti įrenginį arba kelti pavojų naudotojui.

Atminkite!

Signalizacijos sistema ir jos komponentai nesuteikia patikimos apsaugos nuo įsilaužimų ar apiplėšimų. Pagrindinis sistemos tikslas – greitai aptikti grėsmę ir perduoti pavojaus signalą. Norint užtikrinti veiksmingą sistemos veikimą, jos įrengimą turėtų atlikti specialistai, turintys tinkamą kvalifikaciją ir patirtį. Specialistai ne tik įrengs sistemą, bet ir išsamiai paaiškins jos veikimą bei užtikrins reguliarią techninę priežiūrą ir testavimą. Tai leis naudotojui naudotis sistema saugiai ir efektyviai, sumažinant galimų gedimų ar netinkamo veikimo riziką.

Bendrieji įspėjimai

Potencialios grėsmės:

1. Fizinės grėsmės:

- **Mechaniniai pažeidimai:** Netinkamas įrengimas ar eksploatavimas gali sukelti mechaninius komponentų pažeidimus, dėl kurių sistema gali veikti netinkamai.

2. Elektros grėsmės:

- **Įtampos šuoliai ir trumpieji jungimai:** Netinkama izoliacija ar klaidos įrengimo metu gali sukelti elektros smūgius, įtampos šuolius ar trumpuosius jungimus.

3. Kibernetinio saugumo grėsmės:

- Įrenginys turi būti apsaugotas nuo neautorizuotos prieigos (pvz., naudojant stiprius slaptažodžius). Nepakankamas saugumas gali leisti trečiosioms šalims perimti sistemos valdymą.

Įspėjimai:

- **Montavimas ir priežiūra:** Produktus turi montuoti ir prižiūrėti tik kvalifikuoti specialistai pagal gamintojo nurodymus.
- **Elektros sauga:** Prieš montavimą įsitikinkite, kad maitinimas atjungtas, kad išvengtumėte elektros smūgio.
- **Apsauga nuo įtampos šuolių:** Rekomenduojama naudoti tinkamas apsaugas nuo įtampos šuolių, kad būtų apsaugota įranga.
- **Tinklo saugumas:** Naudokite ugniasienes, įsilaužimų aptikimo sistemas ir reguliariai atnaujinkite programinę įrangą, kad apsaugotumėte tinklą nuo atakų.
- **Atsparumas aplinkos veiksniams:** Produktai, nebent kitaip nurodyta specifikacijoje, nėra atsparūs vandeniui. Nenaudokite įrenginių drėgnose vietose, šalia skysčių ar ten, kur jie gali būti veikiami atmosferos sąlygų.

Rekomendacijos

1. Saugus montavimas:

- Įsitikinkite, kad sistema atjungta nuo elektros tinklo prieš montavimą.
- Patikrinkite, ar sistema suderinama su esama infrastruktūra.

2. Funkcionalumo testai:

- Po montavimo atlikite veikimo testus, kad įsitikintumėte, jog sistema veikia pagal gamintojo specifikacijas.
- Reguliariai atlikite techninę priežiūrą ir diagnostiką.

3. Projektavimas ir montavimas:

- **Atitiktis standartams:** Užtikrinkite, kad visi komponentai atitiktų galiojančius saugos standartus.
- **Infrastruktūros planavimas:** Atidžiai suplanuokite kabelių maršrutus, atsižvelgdami į elektromagnetinius trikdžius ir priežiūros patogumą.

4. Priežiūra ir stebėjimas:

- Reguliariai tikrinkite komponentų fizinę būklę ir stebėkite sistemos našumą, kad laiku pastebėtumėte galimas problemas.
- Reguliariai atnaujinkite įrenginių programinę įrangą, kad apsaugotumėte nuo naujų grėsmių.

5. Darbuotojų mokymai:

- Užtikrinkite, kad darbuotojai gautų tinkamus mokymus apie geriausias praktikas, susijusias su įrengimu, priežiūra ir tinklo saugumu.

6. Prieigos valdymas:

- Naudokite prieigos kontrolės mechanizmus tinklų infrastruktūrai apsaugoti nuo neautorizuotos prieigos.

7. Dokumentacija:

- Dokumentuokite visus montavimo, priežiūros darbus ir saugumo incidentus, kad būtų galima analizuoti ir tobulinti procedūras.

Įspėjimai dėl baterijų naudojimo

- **NIEKADA neprarykite baterijų!** Tai gali sukelti stiprų cheminį nudegimą, vidinius sužalojimus ar net mirtį.
- Naudokite tik tinkamas baterijų rūšis. Netinkama baterija, ypač tam tikros ličio baterijos, gali sugadinti įrenginį arba sukelti sprogimą.

- Niekada nemeskite baterijų į ugnį, nespauskite ir nepjaustykite jų. Tai gali sukelti sprogimą.
 - Venkite ekstremalių temperatūrų. Labai aukšta temperatūra gali sukelti sprogimą ar skysčio/gazų nutekėjimą.
 - Tinkamai utilizuokite naudotas baterijas pagal galiojančius teisės aktus.
-

DĖMESIO!

Jei įrenginys skleidžia dūmus, kvapą ar triukšmą, nedelsdami išjunkite maitinimą, atjunkite laidą ir kreipkitės į montuotoją ar aptarnavimo centrą.

Aplinkos apsauga - atliekų rūšiavimas

Senos, nusidėvėjusios ar sugadintos elektros ir elektronikos įrangos atliekos turi būti surinktos atskirai ir perdirbtos pagal galiojančius aplinkos apsaugos teisės aktus (Europos elektros ir elektronikos įrangos atliekų direktyva). Naudokite tam skirtą surinkimo sistemą savo šalyje.

CE ženklas ant įrenginio nurodo, kad įrenginys atitinka taikomas CE direktyvas ir yra saugus naudoti.

Išsamūs įspėjimai dėl:

Signalizacijos jutiklių

- Prieš prijungdami jutiklį prie valdymo pulto ar kitų komponentų, atjunkite įrenginio maitinimą.
- Jei jutikliai maitinami elektra, laikykitės jūsų šalyje galiojančių elektros saugos taisyklių.
- Naudokite tik gamintojo rekomenduojamus maitinimo šaltinius ir kabelius.
- Prieš išmontuodami jutiklį, atjunkite jo maitinimą.
- Lubų ar sienų montavimui naudokite tik stabilius paviršius.
- Nemontuokite jutiklių ant judančių ar vibruojančių elementų.
- Naudokite pridėtus arba gamintojo rekomenduotus tvirtinimo laikiklius.
- Montuojant lauke, patikrinkite produkto specifikaciją ar instrukciją, ar jutiklis tinkamas naudoti lauko sąlygomis. Jei ne, nemontuokite jo lauke.
- Visi elektriniai darbai turi griežtai atitikti vietos elektros saugos, priešgaisrinės apsaugos ir kitų susijusių taisyklių reikalavimus.
- Neleiskite įrenginiui nukristi ar patirti fizinių smūgių, taip pat neeksponuokite jo stipriai elektromagnetinei spinduliuotei. Venkite montuoti ant vibruojančių paviršių ar vietose, kur yra smūgių pavojus (tai gali sugadinti įrenginį).
- Įsitikinkite, kad maitinimas atjungtas prieš prijungiant, montuojant ar išmontuojant įrenginį.

- Jei iš įrenginio sklinda dūmai, kvapai ar triukšmas, nedelsdami išjunkite maitinimą, atjunkite laidą ir kreipkitės į aptarnavimo centrą.
- Nemontuokite įrenginio itin karštose, šaltose, dulkėtose ar drėgnose vietose (detalesnę informaciją apie darbinę temperatūrą rasite produkto specifikacijoje).
- Purvas, dulkės ar voratinkliai gali trukdyti jutiklio veikimui ir sumažinti jo efektyvumą.
- Patalpose naudojami įrenginiai turi būti apsaugoti nuo lietaus ir drėgmės. Negalima jų eksponuoti tiesioginiams saulės spinduliams, prastai ventiliuojamose vietose ar šalia šilumos šaltinių, tokių kaip radiatoriai (tai gali sukelti gaisro pavojų).
- Nenukreipkite įrenginio į saulę ar itin ryškias vietas. Tai gali sukelti šviesos blyksnius ar juostas (tai nėra gedimas, tačiau gali turėti įtakos jutiklio ilgaamžiškumui).
- Baterijomis maitinamų įrenginių netinkamas naudojimas ar baterijų keitimas gali sukelti sprogimo pavojų. Naudokite tik to paties arba lygiaverčio tipo baterijas. Naudotas baterijas utilizuokite pagal gamintojo instrukcijas.
- Neeksponuokite įrenginio koroziniams dujoms, nes tai gali sugadinti įrenginį.
- Naudojant standartinius jutiklius aplinkoje, kur yra degių dujų ar sproglių dulkių, gali įvykti sproginimas.
- Neteisingai nustatyti aptikimo parametrai (pvz., diapazonas ar jautrumas) gali lemti, kad jutiklis nereaguos į grėsmę.

Signalizacijos valdymo pultai, klaviatūros ir plėtimo moduliai

- Nemontuokite įrenginio tiesiai ant paviršiaus – naudokite specialius korpusus.
- Valdymo pultas turi būti montuojamas sunkiai pasiekiamoje vietoje, neautorizuotiems asmenims.
- Venkite montavimo vietose, kur yra drėgmės, tiesioginių saulės spindulių, vibracijų ar ekstremalių temperatūrų.
- Naudokite specialiai tam skirtą maitinimo šaltinį, atitinkantį valdymo pulto techninius reikalavimus.
- Užtikrinkite atsarginį maitinimą, pvz., akumuliatorių, nutrūkus elektros tiekimui.
- Valdymo pultas turi būti tinkamai įžemintas, kad būtų apsaugota nuo viršįtampių ar žaibo.
- Montuokite valdymo pultą toliau nuo įrenginių, generuojančių stiprius elektromagnetinius laukus, tokių kaip transformatoriai ar didelės elektrinės mašinos.
- Apsaugokite valdymo pultą slaptažodžiu ir reguliariai jį keiskite.
- Naudokite skirtingus prieigos lygius, atsižvelgiant į naudotojų funkcijas.
- Reguliariai atnaujinkite valdymo pulto programinę įrangą, kad apsaugotumėte sistemą nuo naujų kibernetinių grėsmių.

- Nuolat tikrinkite įvykių žurnalus, kad pastebėtumėte neįprastą veiklą.
- Jei valdymo pultas prijungtas prie tinklo, naudokite ugniasienes ir šifruotus ryšius.
- Vykdykite periodinius techninius patikrinimus pagal gamintojo rekomendacijas.
- Tikrinkite laidų, jungčių ir periferinių įrenginių (pvz., jutiklių, signalizatorių) būklę.
- Reguliariai vykdykite signalizacijos sistemos testus, kad įsitikintumėte, jog visos funkcijos veikia tinkamai.
- Tikrinkite ir keiskite atsarginius akumuliatorius pagal gamintojo rekomendacijas, kad išvengtumėte jų išsikrovimo.
- Prieš prijungdami, išardydami ar taisydami valdymo pultą, atjunkite maitinimą.
- Naudokite tinkamus įrankius ir asmenines apsaugos priemones, pvz., antistatinės pirštines.
- Neprijunkite daugiau periferinių įrenginių, nei numatyta specifikacijoje.
- Naudotus akumuliatorius ir kitas dalis utilizuokite pagal vietos aplinkos apsaugos taisykles.
- Ribokite prieigą prie sistemos tik būtiniausiems darbuotojams ir įrenginiams.
- Užtikrinkite, kad signalizacijos valdymo pulto įrengimas ir naudojimas atitinka vietos taisykles ir saugumo standartus.

Signalizatoriai

- Signalizatorius turi būti sumontuotas vietoje, kuri būtų nepasiekiamą neautorizuotiems asmenims, pvz., pakankamai aukštai, kad būtų sunku manipuliuoti įrenginiu.
- Venkite montuoti vietose, kur gali būti tiesioginė drėgmė, vanduo ar stipri šiluma (nebent signalizatorius pritaikytas naudoti lauke).
- Signalizatorius turi turėti apsaugos nuo sabotažo funkciją (pvz., dangtelio atidarymo jutiklį arba tvirtinimo nuo sienos detektorių) ir būti sumontuotas taip, kad jį būtų sunku pašalinti ar sugadinti.
- Įsitikinkite, kad įrenginys apsaugotas nuo atsitiktinių pažeidimų, pvz., smūgių ar krentančių daiktų.
- Signalizatorius turi būti maitinamas pagal gamintojo specifikacijas. Netinkamas maitinimas gali sugadinti įrenginį arba sukelti melagingus signalus.
- Reguliariai tikrinkite, ar signalizatorius skleidžia reikiamą garso ir šviesos lygį (pagal standartus).
- Įrenginys turi būti tvirtai pritvirtintas, kad galėtų atlaikyti stiprius vėjus, vibracijas ar bandymus manipuliuoti.
- Signalizatorių montavimą turėtų atlikti apmokytas personalas, laikantis gamintojo techninės dokumentacijos.

- Funkciniai signalizatorių testai turi būti atliekami kaip visos signalizacijos sistemos diagnostikos dalis.
 - Išsaugokite vartotojo vadovą ir techninę dokumentaciją, kad būtų galima greitai spręsti problemas ir atlikti techninę priežiūrą.
-

Radijo įrenginiai

- Naudojant belaidžius signalizacijos valdymo pultus, venkite montuoti įrenginius ant metalinių paviršių.
 - Belaidžiai signalizacijos valdymo pultai neturi būti apvynioti metalu.
 - Belaidžiams valdymo pultams venkite kliūčių 50 cm spinduliu aplink įrenginį, išskyrus montavimo paviršių.
 - Signalų retransliatorius (repeater) turi būti įrengtas tarp valdymo pulto ir periferinių įrenginių.
 - Prieš montuodami patikrinkite signalo stiprumą, įrenginį montuokite vietoje, kur signalo lygis siekia apie 100 %. Atliekant signalo stiprumo testą, nelaikykite jutiklio rankose.
 - Belaidžiai signalizacijos įrenginiai gali būti jautrūs trikdžiams iš kitų įrenginių, veikiančių toje pačioje dažnių juostoje. Užtikrinkite tinkamus darbo kanalus ir venkite vietų su dideliu radijo bangų intensyvumu.
 - Įrenginiai turi turėti įmontuotus signalo trikdymo aptikimo mechanizmus (pvz., „anti-jamming“ funkciją).
 - Užtikrinkite, kad visi įrenginiai būtų valdymo pulto veikimo zonoje ir kad radijo signalas nebūtų blokuojamas sienų, metalinių konstrukcijų ar elektroninių įrenginių.
 - Duomenys, perduodami tarp įrenginių, turi būti tinkamai šifruoti, kad būtų išvengta perėmimo ar manipuliavimo trečiųjų asmenų.
 - Visi radijo įrenginiai turi būti montuojami pagal gamintojo rekomendacijas, atsižvelgiant į optimalią signalo sklaidos vietą.
 - Sistemą reikia periodiškai testuoti, kad būtų užtikrinta, jog belaidžiai įrenginiai tinkamai bendrauja su valdymo pultu.
 - Radijo įrenginiai dažniausiai yra maitinami baterijomis, kurias reikia reguliariai keisti. Užtikrinkite, kad valdymo pultas informuotų apie žemą baterijos lygį.
 - Belaidės sistemos reikalauja reguliarios priežiūros ir veikimo testų, kad užtikrintumėte jų patikimumą.
-

Maitinimo šaltiniai ir akumuliatoriai

- Maitinimo šaltiniai gali perkaisti ilgo naudojimo metu. Užtikrinkite, kad ventiliacijos angos nebūtų užblokuotos.

- Naudokite maitinimo šaltinius, atitinkančius įrenginio techninius reikalavimus (įtampą, srovę, galią), kad išvengtumėte perkrovos.
- Prijungus įrenginius, kurių galia viršija maitinimo šaltinio ribas, gali būti sugadinti įrenginiai arba kilti gaisro pavojus.
- Prijungus maitinimo šaltinį prie tinklo, kurio įtampa viršija jo specifikaciją, gali būti sukeltas elektros smūgis arba sugadintas įrenginys.
- Nenaudokite pažeistų kabelių ar maitinimo šaltinių korpusų. Tai gali sukelti elektros smūgį arba trumpąjį jungimą.
- Perkrauti arba trumpinti akumuliatoriai gali sukelti sprogamą ar gaisrą.
- Pažeisti akumuliatoriai gali išskirti kenksmingas chemines medžiagas, kurios gali dirginti odą, akis ir kvėpavimo takus.
- Akumuliatorius laikykite ir naudokite tik gamintojo nurodytose temperatūrose (ne per aukštose ar per žemose).
- Netinkamas įkroviklio naudojimas arba parametrai gali perkrauti akumuliatorių, sugadinti jo elementus ar sukelti gaisrą.
- Rizika patirti elektros smūgį kyla dėl atvirų laidų, pažeistos izoliacijos arba netinkamo įžeminimo.
- Naudokite tik sertifikuotus maitinimo šaltinius, atitinkančius saugos standartus (pvz., CE, UL).
- Reguliariai tikrinkite kabelių, jungčių ir korpuso būklę dėl pažeidimų.
- Užtikrinkite pakankamą vėdinimą aplink maitinimo šaltinį, kad išvengtumėte perkaitimo.
- Nenaudokite akumuliatorių, jei jie yra pažeisti arba nukritę.
- Akumuliatorius utilizuokite tik nurodytose surinkimo vietose, laikydamiesi vietos teisės aktų.

Ryšio moduliai

- Moduliai gali patirti signalo trikdžius vietose, kuriose yra silpnas mobiliojo tinklo ryšys, o tai gali riboti jų funkcionalumą.
- GSM antena turi būti tinkamai sumontuota ir įrengta tinkamoje vietoje, kad būtų išvengta signalo praradimo.
- GSM moduliai gali būti jautrūs tyčiniam signalo trikdymui („jamming“), kuris gali sutrikdyti duomenų perdavimą.
- Naudojant SIM kortelę su netinkamu duomenų planu arba nepritaikytą konkrečiam operatoriui, ryšys gali būti nutrūkęs.
- IP moduliai gali nustoti veikti dėl vietinio interneto tinklo sutrikimų arba paslaugų teikėjo problemų.
- IP moduliai gali tapti kibernetinių atakų taikiniu, pvz., perimant modulio kontrolę ar keičiant perduodamus duomenis.

- Netinkamai nustatyti tinklo parametrai (pvz., neteisingas IP adresas ar DNS) gali sutrikdyti modulio veikimą.
- IP moduliai gali nustoti veikti dėl vietinio tinklo arba maršrutizatoriaus perkrovos.
- Esant GSM tinklo ryšio praradimui, signalai ir pranešimai gali nebūti perduoti.
- Netinkamas SIM kortelės tarifas gali sukelti dideles išlaidas, ypač perduodant duomenis tarptinkliniu ryšiu.
- Interneto ryšio praradimas neleis perduoti pavojaus signalų stebėjimo stočiai arba vartotojui.
- Saugumo spragos gali leisti atlikti kibernetines atakas prieš signalizacijos sistemą.
- Apsvarstykite GSM ryšio naudojimą kaip atsarginį sprendimą sistemose, kuriose pagrindinė komunikacija vyksta per IP modulį.
- Reguliariai atnaujinkite modulio programinę įrangą ir naudokite stiprius prisijungimo slaptažodžius.
- Ribokite ryšio modulio prieigą tik autorizuotiems vartotojams ir naudokite