



mnb

ul. Widuchowska 19
71-718 Szczecin

tel.: +48 91 439 49 96

faks: +48 91 439 55 99

e-mail: biuro@mnb.pl

http : www.mnb.pl

ISO 9001
AQAP 2110

PROJEKT WYKONAWCZY

DATA : 30.11.2020

NUMER: 806/PT/1070/875

BRANŻA: Zabezpieczenia techniczne

TEMAT: Projekt rozbudowy systemu dozoru SSWiN i CCTV na terenie Zakładu Produkcji Wody w Nieznaniu

ZLECENIODAWCA: Zakład Wodociągów i Kanalizacji Sp. z o.o.
w Szczecinie
ul. Maksymiliana Golisza 10
71-682 Szczecin

AUTOR: **MVB**

OPRACOWAŁ:	mgr inż. Paweł Kozłowski PZT-11771	
OPRACOWAŁ:	mgr inż. Dawid Zeller PZT-17747	
PROJEKTOWAŁ:	mgr inż. Wiktor Gabryliszyn ZAP/0169/P00T/06	
PROJEKTOWAŁ:	mgr inż. Mateusz Przerwa ZAP/0235/PBE/19	

Szczecin, listopad 2020r.

Spis treści

1. Podstawa opracowania	3
2. Przedmiot opracowania	3
3. Zakres opracowania	5
4. Normy i przepisy związane	5
5. Akronimy	7
6. Charakterystyka obiektu	8
7. Ocena obecnego stanu systemów zabezpieczeń technicznych i określenie możliwości ich wykorzystania i dalszej eksploatacji.....	10
7.1. System monitoringu wizyjnego VSS	10
7.2. System sygnalizacji włamania i napadu SSWiN	10
7.3. System kontroli dostępu SKD	11
8. Analiza zagrożeń	13
8.1. Wnioski z analizy zagrożeń	17
9. Opis techniczny, sprzętowy i funkcjonalny instalacji i elementów SZT.	20
9.1. Opis techniczny i funkcjonalny PSIM	31
9.2. Opis techniczny i funkcjonalny systemu VSS	36
9.3. Opis techniczny i funkcjonalny instalacji systemu SSWiN	38
9.4. Opis techniczny i funkcjonalny instalacji systemu ochrony obwodowej	40
9.5. Opis techniczny i funkcjonalny instalacji systemu SKD.	41
9.6. Opis techniczny i funkcjonalny wydzielonej sieci TECH-LAN	42
10. Określenie przebiegu, typu i sposobu układania instalacji teletechnicznej.....	47
11. Określenie przebiegu, typu i sposobu układania instalacji zasilających.....	49
12. Ochrona odgromowa (przebieciowa)	50
13. Ogrodzenie	51
13.1. Pas buforowy – usunięcie drzew i krzewów	52
13.2. Roboty ziemne - budowa ogrodzenia	53
13.3. Opis przyjętych rozwiązań konstrukcyjno-materiałowych ogrodzenie	54
14. Minimalne wymagania funkcjonalno-użytkowe kluczowych urządzeń i oprogramowania.....	55
15. Uwagi końcowe	110
16. Załączniki	111
17. Rysunki	112

1. Podstawa opracowania

Podstawę niniejszego opracowania stanowią:

- Umowa z Zamawiającym;
- Wizja lokalna;
- Dokumenty przekazane przez Zamawiającego;
- Stan faktyczny istniejących instalacji;
- Karty katalogowe urządzeń;
- Aktualne normy i przepisy związane.

2. Przedmiot opracowania

Przedmiotem opracowania jest dokumentacja projektowa pn. „Projekt rozbudowy systemu dozoru SSWiN i CCTV na terenie Zakładu Produkcji Wody Miedwie w Nieznaniu”. W ramach tego opracowania należy wykonać następujące prace:

1. Wykonanie kanalizacji teletechnicznej na potrzeby elektronicznych systemów zabezpieczeń.
2. Posadowienie konstrukcji wsporczych pod kamery.
3. Wykonanie systemu ochrony obwodowej.
4. Modernizacja i wymiana ogrodzenia.
5. Wykonanie wydzielonej sieci bezpieczeństwa TECH-LAN, w tym:
 - a. montaż i konfigurację punktów dystrybucyjnych,
 - b. wykonanie okablowania strukturalnego na bazie kabla światłowodowego jednomodowego,
 - c. instalację tras kablowych i okablowania zasilającego.
6. Wykonanie systemu monitoringu wizyjnego, w tym montaż, programowanie i konfigurację:
 - a. punktów kamerowych,
 - b. rejestratora cyfrowego,
 - c. instalację oprogramowania VSS na jednostkach komputerowych Inwestora,
 - d. instalację tras kablowych i okablowania.
7. Wykonanie systemu kontroli dostępu SKD, w tym:
 - a. montaż, programowanie i konfigurację urządzeń wykonawczych i peryferyjnych,
 - b. konfigurację serwera i oprogramowania systemu SKD,

- c. instalację oprogramowania operatorskiego SKD na jednostkach komputerowych Inwestora,
 - d. instalację tras kablowych i okablowania.
8. Wykonanie systemu sygnalizacji włamania i napadu, w tym:
- a. montaż, programowanie i konfigurację elementów systemowych,
 - b. instalację tras kablowych i okablowania.
9. Wykonanie systemu zarządzania bezpieczeństwem PSIM, w tym:
- a. konfiguracja oprogramowania, interfejsów programowych,
 - b. instalację oprogramowania PSIM na jednostkach operatorskich Inwestora.

Wyżej wymienione instalacje i systemy realizowane są w ramach zadania pn. „Projekt rozbudowy systemu dozoru SSWIN i CCTV oraz wymiany instalacji oświetlenia zewnętrznego na terenie Zakładu Produkcji Wody Miedwie w Nieznaniu”

Instalacja oświetlenia terenu zostanie wykonana w ramach dokumentacji projektowej nr. 850/PT/1070/875 pn. „Projekt wymiany instalacji oświetlenia zewnętrznego na terenie Zakładu Produkcji Wody w Nieznaniu”.

Projekt obejmuje określenie niezbędnego zakresu zabezpieczenia, dobór jego rodzaju oraz określenie standardu technicznego i stopnia zabezpieczenia dla urządzeń systemów zabezpieczeń technicznych obiektów ZPW Miedwie i PW Żelewo.

Przedstawiony w dalszej części projektu sposób ochrony poszczególnych obszarów i obiektów ma na celu podniesienie poziomu bezpieczeństwa ww. obiektów, zapobieganie powstawaniu sytuacji kryzysowych na wczesnym etapie ich rozwoju oraz wypracowanie stosownych rozwiązań, które zminimalizują ich skutki. Zgodnie z wymaganiami Inwestora oraz Zespołu ds. rozbudowy i integracji systemu monitoringu miejskiego Miasta Szczecin projekt zakłada wykonanie systemów zabezpieczeń technicznych obiektów ZPW Miedwie i PW Żelewo przy zachowaniu standardów technicznych i technologii funkcjonującej w obiektach ZWIK. Systemy bezpieczeństwa zostaną wykonane w taki sposób, że będą posiadały możliwość przekierowania strumieni wideo z

kamer CCTV oraz wybranych informacji z systemu SSWiN na stanowiska dyspozytorskie technicznego centrum monitoringu w Szczecinie. Zbudowane w ramach zadania systemy będą przygotowane pod względem technicznym poprzez zastosowanie koniecznych interfejsów oraz licencji umożliwiających transmisję danych do innego systemu. Budowana przez gminę infrastruktura zostanie przygotowana do przyjęcia sygnałów z budowanego systemu licencyjnie i funkcjonalnie na podstawie dokumentacji powykonawczej.

Projekt zakłada rozbudowę funkcjonującej w ZWIK platformy programowej na potrzeby integracji, wizualizacji i zarządzania systemami zabezpieczeń technicznych SZB PSIM o obszar obiektów ZPW Miedwie i PW Żelewo. Projekt zakłada także rozbudowę istniejącego systemu o dodatkową jednostkę operatorską PSIM oraz jednostkę operatorską VSS w budynku Dyrekcji ZWIK.

Projekt obejmuje modernizację części istniejącego ogrodzenia, a także budowę nowego ogrodzenia z bramami i furtkami.

3. Zakres opracowania

Zakres opracowania obejmuje:

- Ogólną ocenę stanu zabezpieczenia ZPW Miedwie i PW Żelewo.
- Analizę zagrożeń.
- Opis techniczny, sprzętowy i funkcjonalny instalacji i elementów Systemu Zabezpieczeń Technicznych.
- Opis funkcjonalny i techniczny systemu integrującego poszczególne elementy SZT.
- Schematy blokowe, ideowe, plany rozmieszczenia urządzeń poszczególnych instalacji projektowanego SZT oraz jego integracji.
- Minimalne wymagania funkcjonalno-użytkowe dla urządzeń kluczowych i oprogramowania.
- Zestawienie materiałowe.

4. Normy i przepisy związane

- Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (tekst jednolity) (Dz.U. z 2014r. poz.1099 z późn. zm.)
- Ustawa z dn. 7.07.1994 Prawo budowlane wraz z późniejszymi zmianami;

- Narodowy Program Ochrony Infrastruktury Krytycznej 2018;
- Norma PN-EN 50131-1:2009 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe” z późn. zm.;
- Norma PN-EN 50131-2-2:2018-01 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 2-2: Czujki sygnalizacji włamania - Pasywne czujki podczerwieni;
- Norma PN-EN 50131-2-3:2010 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 2-3: Wymagania dotyczące czujek mikrofalowych;
- Norma PN-EN 50131-2-4:2009 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 2-4: Wymagania dotyczące dualnych czujek pasywnych podczerwieni i mikrofalowych;
- Norma PN-EN 50131-2-6:2012 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 2-6: Czujki otwarcia stykowe (magnetyczne);
- Norma PN-EN 50131-2-7-1:2013-06 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 2-7-1: Czujki włamania -- Czujki stłuczenia szkła (dźwiękowe);
- Norma PN-EN 50131-4:2019-05 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 4: Sygnalizatory
- Norma PN-EN 50131-6:2017-12 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 6: Zasilacze
- Norma PN-EN 62676-1-1:2014-06 „Systemy dozоровe CCTV stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe, Postanowienia ogólne”;
- Norma PN-EN 62676-4:2015-06 „Systemy dozоровe VSS stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania”;
- Norma PN-EN 60839-11-1:2014-01/AC: „Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i części składowych”;
- Norma PN-HD 60364-4-41:2017-09: „Instalacje niskiego napięcia – Część 4-41: Ochrona dla zapewnienia bezpieczeństwa – Ochrona przed porażeniem elektrycznym

- Norma PN-HD 60364-6:2016-07: „Instalacje elektryczne niskiego napięcia – Część 6: Sprawdzenie”
- Polskie Normy i wytyczne projektowania. Literatura techniczna.
- PN-EN 1990;2004 - Podstawy projektowania konstrukcji
- PN-EN 1991-1-1 - Oddziaływania na konstrukcje
- PN-EN 1991-1-2 - Oddziaływanie użytkowe
- PN-EN 1991-1-3 - Oddziaływanie śniegiem
- PN-EN 1991-1-4 - Oddziaływanie wiatrem
- PN-EN 1997-1 - Projektowanie geotechniczne
- PN-EN 1993-1;2006 - Konstrukcje stalowe
- PN-EN 1992-1-1;2008 - Konstrukcje żelbetowe.

5. Akronimy

GPD	– Główny Punkt Dystrybucyjny
GPZ	– Główny Punkt Zasilający
MEMS	– mikroukład elektromechaniczny (ang. micro-electromechanical system)
PPD	– Pośredni Punkt Dystrybucyjny
PSIM	– system zarządzania bezpieczeństwem SZB (ang. Physical Security Information Management)
SKD	– system kontroli dostępu
SSWIN	– system sygnalizacji włamania i napadu
SZ SSWIN	– stopień zabezpieczenia wg PN-EN 501131-1
SZT	– system zabezpieczenia technicznego
VSS	– system monitoringu wizyjnego (ang. Video Surveillance System). Synonim wg starej nomenklatury – CCTV

Wg nomenklatury aktualnej normy PN-EN 62676-4 system monitoringu wizyjnego określany jest poprzez akronim VSS, który w dalszej części opracowania będzie używany na określenie systemu monitoringu wizyjnego.

6. Charakterystyka obiektu

Zespół obiektów ZPW Miedwie tworzy infrastrukturę wymagającą szczególnej ochrony z punktu widzenia zapewnienia ciągłości dostaw wody dla miasta Szczecina.

ZPW Miedwie, dla którego źródłem wody jest jezioro Miedwie, znajduje się ok. 30 km w kierunku południowo-wschodnim od Szczecina. Jezioro jest zbiornikiem rynnowym, polodowcowym o powierzchni 3816ha, długości 16,6 km, szerokości do 3,2km i głębokości sięgającej aż 43,5m.

Z ZPW Miedwie woda po uzdatnieniu dostarczana jest do Szczecina dwiema magistralami wodociągowymi: tzw. Starą Miedwianką o średnicy 1200 mm i tzw. Nową – 700mm. Trafia do zbiorników ZPW Pomorzany przy ul. Szczawiowej, skąd po powtórnej dezynfekcji, tłoczona jest do lewobrzeżnej sieci wodociągowej miasta. Z magistrali miedwiańskiej, poprzez pompownię w Kijewie, pobierana jest woda do zaopatrzenia prawobrzeżnej części Szczecina.

Ujęcie wody na jeziorze Miedwie zostało oddane do eksploatacji w 1976r i zaopatruje w wodę ok. 330 tys. mieszkańców.

Wodę z jeziora ujmuje się za pomocą czerpni zlokalizowanej 240 m od brzegu jeziora w kierunku wschodnim, 6 metrów ponad dnem jeziora i jednocześnie 17 – 18 m pod powierzchnią zwierciadła wody. Stąd woda grawitacyjnie przepływa dwoma równoległymi rurociągami do pompowni PW Żelewo.

Wody jeziora Miedwie dla potrzeb funkcjonalnych ujęcia są podpiętrzane na jazie zlokalizowanym na rzece Płoni na jej wypływie z jeziora.

Dodatkowo woda płynąc 33-kilometrowym rurociągiem z jez. Miedwie napędza turbinę na terenie ZPW Pomorzany, która produkuje 800MWh energii elektrycznej przyczyniając się do zaoszczędzenia ok. 350 tys. zł rocznie na rachunkach za zużycie prądu dla Spółki.

Oprócz tego na terenie ZPW Miedwie i PW Żelewo funkcjonują farmy fotowoltaiczne przyczyniając się do produkcji energii elektrycznej z odnawialnych źródeł co przyczynia się do utrzymania na stałym poziomie opłat za wodę i odbiór ścieków.



Rys. 6.1 Plan sytuacyjny Zakładu Produkcji Wody Miedwie w Nieznaniu

Na terenie ZPW Miedwie znajdują się następujące obiekty:

- hydrotechniczne:
 - budynek filtrów pośpiesznych z rozdzielniami 15kV oraz 0,4 kV,
 - budynek filtrów węglowych,
 - budynek koagulacji z częścią ozonowni i rozdzielni 0,4kV,
 - budynek osadników,
 - chlorownia,
 - budynek komory zasuw,
 - zbiorniki podziemne przy budynku komory zasuw.
- biurowiec z częścią laboratoryjną
- portiernia
- warsztatowe:
 - budynek warsztatu mechanicznego,
 - budynek warsztatu elektrycznego,
 - i inne pomniejsze.

Na terenie PW Żelewo znajdują się następujące obiekty:

- budynek pompowni stopnia pierwszego P-1,
- stacja transformatorowa,

- budynek hangarowy.

7. Ocena obecnego stanu systemów zabezpieczeń technicznych i określenie możliwości ich wykorzystania i dalszej eksploatacji

7.1. System monitoringu wizyjnego VSS

System monitoringu wizyjnego VSS ZPW Miedwie i PW Żelewo oparty jest o system analogowy w skład którego wchodzi:

- kamery analogowe LTC 0350 - 3 wewnętrznych zainstalowanych w hali koagulacji i w hali filtrów oraz 13 zewnętrznych kamer stacjonarnych zainstalowanych na elewacji budynków laboratorium, chlorowni, rozdzielni WN i NN, koagulacji, kotłowni;
- multiplexer 16 kanałowy LTC 2652/90;
- rejestrator DVR 16 kanałowy 4NSYS
- 3 monitory 17'' LTC 2017/50.

System VSS jest częściowo niesprawny. System w obecnej formie funkcjonuje od wielu lat. Postęp technologiczny jaki miał miejsce w tym czasie powoduje, że system jest przestarzały i rażąco odbiega od dzisiejszych standardów technicznych. System nie jest zgodny z wymogami aktualnych norm dla systemów zabezpieczeń technicznych. Coraz bardziej utrudniony jest dostęp do części zamiennych oraz powtarzające się awarie. System nie jest zintegrowany z innymi systemami zewnętrznymi. Biorąc powyższe pod uwagę istniejący system nie nadaje się do modernizacji, rozbudowy i dalszej eksploatacji.

7.2. System sygnalizacji włamania i napadu SSWiN

Istniejący system SSWiN ZPW Miedwie oparty jest o centralę alarmową DIALOG 128 produkcji Tecnoalarm, rok prod. 2001. Firmware centrali i urządzeń peryferyjnych nie jest już wspierany przez producenta. System funkcjonalnie podzielony jest na 13 stref dozoru w 3 oddzielnych partycjach SSWiN obejmujących następujące obiekty:

- chlorownia
- komora zasuw
- budynek filtrów

- hala filtrów
- koagulacja
- ozonownia
- budynek biurowy
- laboratorium
- magazyn trucizn
- transformatory
- bariery zewnętrzne – brama
- bariery zewnętrzne
- sygnalizacja zagrożeń w strefie chloru

Elementami obsługowymi są szyfratory zainstalowane w pomieszczeniu dyspozytora, chlorowni, budynku filtrów, komory zasuw, ozonowani oraz koagulacji. Elementami detekcyjnymi są czujki pasywnej podczerwieni INFRORED, czujki dualne PIR+MW Dualteco, czujki kontaktronowe ART450, aktywne bariery mikrofalowe EXPLORER oraz czujki różnych producentów, tj. DSC, SATEL, CROW zainstalowane w wyniku prac serwisowych.

W budynku PW Żelewo system SSWIN jest częściowo niesprawny. System SSWIN nie jest zgodny z aktualnymi normami dla systemów zabezpieczeń technicznych. System jest znacznie wyeksploatowany, występują trudności z zakupem części i podzespołów zamiennych w przypadku awarii. System nie jest zintegrowany z innymi zewnętrznymi systemami bezpieczeństwa. System nie nadaje się do modernizacji i dalszej eksploatacji.

7.3. System kontroli dostępu SKD

System kontroli dostępu zainstalowany na wejściu do pomieszczeń laboratorium ZPW Miedwie został oparty na zamku szyfrowym ROGER – bez rejestracji zdarzeń. Jest to instalacja lokalna, autonomiczna.

W pozostałych lokalizacjach, w tym na terenie PW Żelewo nie ma systemu SKD.

Biorąc pod uwagę wszystkie powyższe uwagi, istniejące systemy zabezpieczeń technicznych zainstalowane w ZPW Miedwie nie nadają się do modernizacji i dalszego wykorzystania. Systemy te należy wymienić

na nowe, zgodne z aktualnymi normami i aktualnymi standardami technologicznymi. Przy wymianie należy zachować standard technologiczny istniejących systemów zabezpieczeń funkcjonujących obecnie w ZPW Pomorzany.

8. Analiza zagrożeń

Analiza zagrożeń przedstawiona w niniejszej dokumentacji stanowi dane wejściowe do określenia wymaganego poziomu zabezpieczenia obiektów ZPW Miedwie i PW Żelewo.

Przedstawiona w analizie lista potencjalnych zagrożeń przedstawia się następująco:

Zagrożenia kryminalne – ZK

- ZK-1 kradzież (art. 203 kk oraz art. 119 kw) - zabór mienia
- ZK-2 kradzież z włamaniem (art. 208 kk) - zabór mienia po uprzednim przełamaniu zabezpieczeń budowlanych lub mechanicznych
- ZK-3 kradzież rozbójnicza, rozbój (art. 209 kk oraz art. 210 kk) - tzw. napad
- ZK-4 wymuszenie rozbójnicze, szantaż (art. 211 kk)
- ZK-5 uszkodzenie mienia, dewastacja, wandalizm, podpalenie (art. 212 kk, art. 124 kw oraz art. 415 kc)
- ZK-6 cyberprzestępstwa (art. 267 kk oraz art. 287 kk)

Zagrożenia terrorystyczne - ZT (art. 255a kk)

- ZT-1 terror polityczny
- ZT-2 terror kryminalny
- ZT-3 terror ideologiczny, w tym społeczny (ekoterroryzm, bioterroryzm)
- ZT-4 cyberterroryzm

Zagrożenia środowiskowe – ZS

- ZS-1 powódzie
- ZS-2 podtopienia
- ZS-3 oblodzenia
- ZS-4 huragany, trąby powietrzne
- ZS-5 pożary powodujące umiarkowane szkody
- ZS-6 wyładowania atmosferyczne
- ZS-7 silne pola elektromagnetyczne (urządzenia wyładowcze, komutacyjne, indukcyjne, nadawcze itp.)
- ZS-8 wstrząsy tektoniczne (tąpnięcia, trzęsienia ziemi)
- ZS-9 osunięcia ziemi
- ZS-10inne

Prawdopodobieństwo $[P_i]$ wystąpienia zdarzenia zmienne i zależne od lokalizacji zasobu oraz lokalnych zagrożeń, określone zostało jako iloczyn atrakcyjności $[At_i]$ zasobu i podatności $[Pd_i]$ utraty zasobu wg znormalizowanej następującej skali:

Atrakcyjność:

- | | | | |
|---|---------|---|--------------------|
| 1 | znikoma | - | mało atrakcyjny |
| 2 | niska | - | średnio atrakcyjny |
| 3 | średnia | - | atrakcyjny |
| 4 | wysoka | - | bardzo atrakcyjny |

Podatność:

- | | | | |
|---|---------|---|-----------------------------|
| 1 | znikoma | - | bardzo dobrze zabezpieczony |
| 2 | niska | - | średnio zabezpieczony |
| 3 | średnia | - | słabo zabezpieczony |
| 4 | wysoka | - | niezabezpieczony |

Podatność $[Pd_i]$ z kolei została sklasyfikowana jako iloczyn dostępności do zasobu $[D_i]$ i systemu ochrony zasobu $[SO_i]$ wg znormalizowanej następującej skali:

Dostępność:

- | | | | |
|---|---------|---|--|
| 1 | znikoma | - | Dostępność z zewnątrz bardzo mocno ograniczona. Teren przyległy chroniony. |
| 2 | niska | - | Dostępność z zewnątrz ograniczona. Teren przyległy nie chroniony. |
| 3 | średnia | - | Infrastruktura pozwalająca na pokonanie przeszkód niezauważalnie i w łatwy sposób. |
| 4 | wysoka | - | Swobodny dostęp z zewnątrz. |

System ochrony:

- | | | | |
|---|--------|---|---|
| 1 | wysoki | - | Możliwość odparcia ataku - ochrona fizyczna, rozbudowany system wykrywania zagrożenia |
| 2 | średni | - | Możliwość odparcia ataku - ochrona fizyczna, ograniczony system wykrywania zagrożenia |
| 3 | niski | - | Opóźnione możliwości odparcia ataku, ograniczony |

system wykrywania zagrożenia

4 znikomy - Brak możliwości odparcia ataku, brak możliwości wykrywania zdarzenia.

Poziom ryzyka zaistnienia zdarzenia lub utraty zasobu jest mierzony iloczynem skutku utraty zasobu [S_i] i prawdopodobieństwa zaistnienia takiego incydentu [P_i] i przedstawiony wg znormalizowanej skali:

Ryzyko:

- 1 niskie
- 2 niskie do średniego
- 3 średnie do wysokiego
- 4 wysokie

Skutki utraty zasobów zostały zdeterminowane w następujący sposób:

- 1 znikome z wagą utraty zasobu jako mniej istotny
- 2 niskie z wagą utraty zasobu jako istotny
- 3 średnie z wagą utraty zasobu jako ważny
- 4 poważne z wagą utraty zasobu jako bardzo ważny
- 5 katastrofalne z wagą utraty zasobu jako krytyczny

Skutki utraty danego zasobu mają wpływ na inne elementy bezpieczeństwa i stabilności kraju, takie jak:

- finansowe,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- poziomu bezrobocia.

Biorąc pod uwagę możliwe skutki awarii lub sabotażu obiektów odpowiedzialnych za dostawę wody pitnej, zapewnienie skutecznej ochrony tej infrastruktury jest krytyczne z punktu widzenia bezpieczeństwa regionu. Dlatego też analiza zagrożeń została

opracowana w oparciu o Krajowy Plan Zarządzania Kryzysowego Rządowego Centrum Bezpieczeństwa.

Poziom ryzyka odnosi się do klasyfikacji przedstawionej w dalszej części opracowania, w skali pięciostopniowej. Poszczególnym stopniom przypisano taktykę postępowania z ryzykiem w skali od „A” do „D”.

Pomiar zagrożenia polega na oszacowaniu prawdopodobieństwa wystąpienia zdarzenia, jego wpływu na funkcjonowanie obiektu, ocenę dostępności do obiektu, jak również wdrożony system ochrony przed zagrożeniami.

Nie wykluczono w analizie zagrożeń terrorystycznych, których głównymi źródłami dla Europy są:

- skrajnie fundamentalistyczny terroryzm islamski;
- skrajnie lewicowy i ultraprawicowy ekstremizm;
- ruchy separatystyczne.

Dodatkowym zagrożeniem jest terror społeczny w postaci np. ekoterroryzmu lub bioterroryzmu.

Każdy z wymienionych powyżej rodzajów terroryzmu charakteryzuje się odmienną specyfiką i właściwymi dla siebie trendami. Pojawienie się danego zagrożenia wynika ze specyficznych uwarunkowań historycznych i społeczno-politycznych w poszczególnych państwach. Zagrożenia terrorystyczne mogą być również wynikiem zjawisk o charakterze globalnym, czego przykładem jest terroryzm islamski.

Polska nie jest obecnie pierwszoplanowym celem ataku dla terrorystów, jednakże ze względu na swoją działalność na arenie międzynarodowej, m.in.: uczestnictwo w działaniach w Iraku, Afganistanie, politykę współpracy z USA oraz napięte stosunki dyplomatyczne z Rosją m.in. w kontekście sytuacji Ukrainy, Białorusi i rozbudowy wschodniej flanki NATO nie można w całości zignorować ryzyka ataku terrorystycznego na sektor wodno-kanalizacyjny.

Intruz może przedostać się na teren chronionych obiektów pieszo, samochodem, ciągnikiem, łodzią, kajakiem itp. Nie wykluczono również możliwości przeprowadzenia działań o charakterze przestępczym, sabotażu wewnętrznego przez pracowników ZWIK Szczecin Sp. z o.o.,

zewnętrznych podmiotów serwisujących urządzenia lub pracowników portierni.

Przedostanie się osób nieupoważnionych w pobliże urządzeń technologicznych i ich uszkodzenie może skutkować znaczącą stratą materialną oraz zagrożeniem życia i zdrowia ludności.

Analizę zagrożeń przedstawiono w załączniku nr 1 niniejszej dokumentacji.

8.1. Wnioski z analizy zagrożeń

Obecny stopień zabezpieczenia ZPW Miedwie i PW Żelewo jest niewystarczający.

Konsekwencją wystąpienia najbardziej niekorzystnych scenariuszy przedstawionych w analizie zagrożeń są utracone korzyści na skutek awarii turbin lub infrastruktury technicznej z tytułu sprzedaży wody, a także możliwe katastrofalne skutki masowego zatrucia ludności Szczecina w przypadku ataku terrorystycznego.

Obiekty ZPW Miedwie i PW Żelewo na chwilę obecną są wyposażone w podstawowe zabezpieczenia mechaniczne (zamki, wkładki, ogrodzenie, drzwi), które są podatne na przełamanie w stosunkowo krótkim czasie. Obiekty są zabezpieczone wyeksploatowanymi i niespełniającymi aktualnych standardów technicznych systemami zabezpieczeń. Istniejące systemy zabezpieczeń są wykonane w przestarzałej technologii, bez możliwości ich modernizacji i integracji w ramach projektowanego systemu PSIM. Systemy te nie zapewniają w chwili obecnej wymaganego poziomu zabezpieczenia obiektu. Systemy są wyeksploatowane, częściowo wyłączone z użytkowania. Często nie ma już możliwości zakupu i wymiany uszkodzonych podzespołów. Z powyższych względów należy je obowiązkowo wymienić na nowe. Obiekty ZPW Miedwie i PW Żelewo chronić nowoczesnymi, elektronicznymi systemami zabezpieczeń technicznych.

Do zneutralizowania potencjalnych zagrożeń należy zastosować co najmniej zabezpieczenie obiektów ZPW Miedwie i PW Żelewo z wykorzystaniem:

- Systemu sygnalizacji włamania i napadu,
- Systemu monitoringu wizyjnego,
- Systemu kontroli dostępu,

- Systemu ochrony obwodowej (napłotowego),
- Systemu radarowego (nadzór strefy ujęcia wody),
- Integracji ww. podsystemów w jednym lokalnym centrum zarządzania bezpieczeństwem,

z uwzględnieniem zastosowania działań odpowiednich do poszczególnych taktyk.

Działania z zakresie poszczególnych taktyk są następujące:

Taktyka A

- akceptacja istniejącego stanu i poziomu ryzyka
- sporządzenie notatki na okoliczność wystąpienia zdarzenia

Taktyka B

- wykorzystanie istniejących zabezpieczeń budowlanych
- wykorzystanie istniejących zabezpieczeń mechanicznych
- doposażenie w podstawowe zabezpieczenia mechaniczne (kłódki, kraty, ogrodzenie)

Taktyka C

- działania jak w taktyce B

Oraz dodatkowo:

- zabezpieczenie elektronicznymi systemami zabezpieczeń technicznych w stopniu bezklasowym lub wyższym
- zastosowanie SZT do ochrony obwodowej z zastosowaniem zewn. VSS i SSWIN
- monitorowanie zasobów poprzez:
 - obserwację środowiska zasobów
 - analizę środowiska zasobów
 - okresową analizę zagrożeń
 - okresowe szacowanie ryzyka
 - okresowe kontrolowanie stanu bezpieczeństwa zasobów
 - okresowe sprawdzanie stanu bezpieczeństwa zasobów
 - ograniczenie organizacyjne dostępu do zasobów
 - okresowych przeglądach wewnętrznych regulaminów, procedur i instrukcji

- doraźna, nieplanowana, wrywkowa kontrola przez mobilną grupę interwencyjną SUF0 w zakresie kontroli ruchu materiałowo - osobowego
- wydzielenie stref ochrony i dostępu
- prowadzenie nadzoru nad systemem zamknięć obiektu
- okresowa kontrola stanu zamknięć (zamków, wkładek, kłódek) i ich regularna konserwacja - zabezpieczenie, chronienie i dozorowanie zasobów poprzez:
- dozorowanie stanu zamknięć i zaryglowań zewnętrznych bram, furtek, drzwi wejściowych do budynków, szlabanów - przesyłania sygnałów alarmowych do ACO

Taktyka D

- działania jak w taktyce C

Oraz dodatkowo:

W stopniu ochrony 4:

- zabezpieczenie elektronicznymi systemami zabezpieczeń technicznych w stopniu 2 (grade 2) wg PN-EN 50131-1.

Taktyka D

- działania jak w taktyce C

Oraz dodatkowo:

W stopniu ochrony 5:

- zabezpieczenie elektronicznymi systemami zabezpieczeń technicznych w stopniu 3 (grade 3) wg PN-EN 50131-1.

9. Opis techniczny, sprzętowy i funkcjonalny instalacji i elementów

SZT

Należy zapewnić pełną kompatybilność na poziomie sprzętowym i programowym przy rozbudowie i modernizacji systemu zarządzania bezpieczeństwem i wizualizacji SZB PSIM, systemu monitoringu wizyjnego VSS, systemu kontroli dostępu SKD oraz systemu sygnalizacji włamania i napadu SSWiN z instalacjami obecnie funkcjonującymi w obiektach ZWIK (ZPW Pomorzany) oraz wymaganiami dla gminnych systemów monitoringu wizyjnego CCTV zatwierdzonych decyzją Zespołu ds. rozbudowy i integracji systemu monitoringu miejskiego z dn. 01.03.2019r. System ma możliwość podłączenia do monitoringu wizyjnego miasta Szczecin.

Prowadzone prace nie mogą zakłócić ciągłości pracy istniejących instalacji systemu zarządzania bezpieczeństwem i wizualizacji SZB PSIM, systemu monitoringu wizyjnego VSS, systemu kontroli dostępu SKD oraz systemu sygnalizacji włamania i napadu SSWiN. Wszelkie roboty należy prowadzić w porozumieniu z Zamawiającym i konserwatorem w taki sposób, aby nie naruszyć warunków gwarancji.

Prace konfiguracyjne i instalacyjne w zakresie systemu zarządzania bezpieczeństwem i wizualizacji SZB PSIM, systemu monitoringu wizyjnego VSS, systemu kontroli dostępu SKD oraz systemu sygnalizacji włamania i napadu SSWiN mogą być wykonywane jedynie przez podmioty i osoby posiadające aktualne szkolenie z zakresu konfiguracji, programowania i serwisowania systemów obecnie funkcjonujących w obiektach ZWIK, wydane przez producenta lub dystrybutora systemu.

Z uwagi na konieczność zapewnienia optymalnego poziomu bezpieczeństwa obiektów ZPW Miedwie i ich infrastruktury krytycznej założenia ochrony oparto o Narodowy Plan Ochrony Infrastruktury Krytycznej, opracowany przez Rządowe Centrum Bezpieczeństwa.

Model budowy elektronicznych systemów zabezpieczeń technicznych zakłada wykorzystanie struktury rozproszonej z zachowaniem jednolitej, ustandaryzowanej technologii, pozwalającej na pełną unifikację, kompatybilność i integrację programowo-systemową urządzeń, pełną wymianę i transfer danych z istniejącymi w obiektach ZWIK systemami

zabezpieczeń technicznych oraz centralnym systemem zarządzania bezpieczeństwem SZB PSIM, zlokalizowanym w ZPW Pomorzany. Model zakłada możliwość integracji w przyszłości wszystkich systemów zabezpieczeń w pozostałych obiektach ZWIK w ramach jednego systemu zarządzania w ZPW Pomorzany. W celu zapewnienia nadzoru i kontroli nad obiektami podległymi ZWIK w budynku Dyrekcji ZWIK przewiduje się instalację jednostek operatorskich systemu PSIM oraz VSS.

Obiektami podlegającymi zabezpieczeniu są:

Na terenie ZPW Miedwie:

- budynek filtrów pośpiesznych z rozdzielniami 15kV oraz 0,4 kV,
- budynek filtrów węglowych,
- budynek koagulacji z częścią ozonowni i rozdzielni 0,4kV,
- chlorownia,
- budynek komory zasuw,
- zbiorniki podziemne przy budynku komory zasuw.
- biurowiec z częścią laboratoryjną
- portiernia

Na terenie PW Żelewo:

- budynek pompowni stopnia pierwszego P-1,
- budynek hangarowy.

W celu zapewnienia efektywności systemów zabezpieczenia technicznego ZPW Miedwie i PW Żelewo wydziela się następujące strefy w poszczególnych obiektach:

1. Strefa dozoru zewnętrznego. Strefa poza terenem obiektu znajdująca się bezpośrednio za ogrodzeniem Zakładu (pas o szerokości min. 3m, wolny od roślinności). Nadzór tej strefy przy wykorzystaniu kamer systemu monitoringu wizyjnego w granicach ich pola widzenia, oraz techniki radarowej przy ujęciu wody.
2. Strefa ochrony obwodowej. Ogrodzenie zewnętrzne Zakładu oraz obszar bezpośrednio przy ogrodzeniu od strony wewnętrznej Zakładu a także bramy wjazdowe i furtki. Dla zabezpieczenia tej strefy zakłada się wykorzystanie systemu ochrony napłotowej, czujek zewnętrznych

dopplerowskich oraz kamer systemu VSS. W obszarze bram wjazdowych przewiduje się wykorzystanie systemu kontroli dostępu SKD.

3. Strefa ochrony peryferyjnej. Strefa obejmująca obszar wewnątrz Zakładu znajdujący się pomiędzy strefą ochrony obwodowej a obrysem budynków i wygrodzonych obszarów wewnętrznych. Strefa monitorowana będzie w zakresie głównych ciągów komunikacyjnych i newralgicznych obszarów przy wykorzystaniu kamer monitoringu wizyjnego VSS oraz będzie wsparta systemem sterowanego oświetlenia LED.
4. Strefa ochrony obrysowej. Strefa obejmująca obrys budynków oraz obrys dodatkowych wewnętrznych wygrodzeń wewnątrz Zakładu. Strefa monitorowana punktowo przy pomocy kamer systemu VSS.
5. Strefa ochrony wewnętrznej. Strefa wewnątrz obiektów i budynków. Strefa monitorowana i nadzorowana przy wykorzystaniu systemu sygnalizacji włamania i napadu SSWiN, systemu kontroli dostępu SKD oraz kamer monitoringu wizyjnego VSS. W ramach tej strefy będą dodatkowo wydzielane niezbędne podstrefy alarmowe w budynkach.



Rysunek - Zasada podziału obiektu na strefy dozoru i ochrony na przykładzie PW Żelewo

Generalna zasada zapewnienia ochrony w strefie wewnętrznej to wydzielenie z niej podstref z adekwatnym do zagrożenia sposobem ochrony systemami zabezpieczeń technicznych.

W przypadku obiektów ZPW Miedwie i PW Żelewo podstrefami zazwyczaj będą:

- komunikacja ogólna,
- pomieszczenia technologiczne – rozdzielnie, pomieszczenia transformatorów, akumulatorownie, magazyny kluczowe itp.,
- pomieszczenia składowania danych osobowych, danych wrażliwych i danych będących tajemnicą spółki - archiwa,

- pomieszczenia biurowe przetwarzania danych osobowych, danych wrażliwych i danych będących tajemnicą spółki,
- serwerownie,
- pomieszczenia pośrednich punktów dystrybucyjnych systemów zabezpieczeń technicznych.
- pomieszczenia dyspozytorskie – nastawnie.

Zakres i rodzaj zabezpieczenia powyższych obiektów i terenów należy wykonać w następujący sposób:

1. ZPW Miedwie

1.1. Teren podstawowy - ogrodzenie

W terenie wewnętrznym wydzielone zostaną następujące strefy funkcjonalne:

- linia ogrodzenia obiektu ZPW Miedwie podlegającego szczególnej ochronie,
- brama wjazdowa główna,
- bramy techniczne,
- furtki,

Brama główna ze względu na organizację ruchu pieszego i kołowego zostanie objęta systemem kontroli dostępu SKD z nadzorem przez kamery VSS. Pozostałe bramy i furtki objęte zostaną nadzorem systemu VSS.

Jako ochronę ogrodzenia i terenów bezpośrednio do niego przylegających należy zastosować system napłotowy ochrony obwodowej oparty o czujniki MEMS i kamery systemu monitoringu VSS. Jako uzupełnienie w miejscach szczególnie trudnych z uwagi na ukształtowanie terenu zostaną wykorzystane zewnętrzne czujki dopplerowskie ruchu.

1.2. Teren podstawowy – strefa peryferyjna

W wyniku analizy zagrożeń teren wewnętrzny (strefa peryferyjna - pomiędzy ogrodzeniem Zakładu a budynkami i ogrodzeniami wewnętrznymi) został zakwalifikowany do ochrony wg taktyki C. Główne ciągi komunikacyjne będą nadzorowane przez kamery systemu monitoringu VSS.

1.3. Portiernia

W wyniku analizy zagrożeń budynek portierni został zakwalifikowany do ochrony wg taktyki A.

Budynek jest przeznaczony dla obsługi portierskiej Zakładu oraz do organizacji w razie konieczności posterunku doraźnego ochrony fizycznej.

W pomieszczeniu portierni należy zainstalować:

- jednostkę operatorską systemu SZB PSIM,
- jednostkę operatorską VSS,
- przycisk napadowy,
- manipulator SSWIN.

Z uwagi okresową pracę personelu w budynku portierni pomieszczenie obsługi i ciąg komunikacyjny zabezpieczane zostaną wyłącznie czujkami PIR systemu SSWiN, tworząc strefę w bezklasowym stopniu zabezpieczenia. Drzwi do portierni objęte zostaną kontrolą przejścia.

1.4. Biurowiec

W wyniku analizy zagrożeń budynek biurowca został zakwalifikowany do ochrony wg taktyki C z wydzielonymi strefami do ochrony wg taktyki D w stopniu 4 i 5.

W budynku wydzielone zostaną następujące strefy funkcjonalne:

- komunikacyjna,
- pomieszczeń biurowych,
- pomieszczenie archiwum,
- pomieszczenie rozdzielnic głównej,
- pomieszczenia laboratorium,
- pomieszczenia magazynowe, w tym z miejscem przechowywania trucizn.

Powyższe strefy należy objąć systemem SSWIN w następujących stopniach zabezpieczenia:

- komunikacyjna – system bezklasowy,
- pomieszczeń biurowych – system bezklasowy,

- pomieszczenie archiwum – system w stopniu 2,
- pomieszczenie rozdzielnic głównej – system w stopniu 2,
- pomieszczenia laboratorium – system w stopniu 2,
- pomieszczenia magazynowe, w tym z miejscem przechowywania trucizn – system w stopniu 3.

Wejście do budynku należy objąć kontrolą systemem KD. Dodatkowo kontrolą przejścia należy objąć następujące strefy:

- laboratorium,
- pom. z truciznami,
- pom. z rozdzielnicą główną napięcia.

W pomieszczeniu rozdzielnic głównej należy utworzyć PPD wydzielonej sieci TECH-LAN na potrzeby SZT.

1.5. Budynek filtrów pośpiesznych

W wyniku analizy zagrożeń budynek filtrów pośpiesznych został zakwalifikowany do ochrony wg taktyki C z wydzielonymi strefami do ochrony wg taktyki D w stopniu 4.

W budynku wydzielone zostaną następujące strefy funkcjonalne:

- komunikacyjna,
- pomieszczeń technologicznych hydrotechnicznych:
- pomieszczenie rozdzielni 15kV,
- pomieszczenie rozdzielni 0,4kV,
- pomieszczenia dyspozytorni,
- pomieszczenie serwerowni,
- pomieszczenie kablowni,
- komory transformatorów.

Powyższe strefy objąć systemem SSWIN w następujących stopniach zabezpieczenia:

- komunikacyjna – system bezklasowy,
- pomieszczeń technologicznych hydrotechnicznych – system w stopniu 2,
- pomieszczenie rozdzielni 15kV – system w stopniu 2,

- pomieszczenie rozdzielni 0,4kV – system w stopniu 2,
- pomieszczenie serwerowni – system w stopniu 2,
- pomieszczenie kablowni – system w stopniu 2,
- komory transformatorów – system w stopniu 2.

Wejście do budynku objąć kontrolą przejścia systemu SKD.
Dodatkowo kontrolą przejścia objąć następujące strefy:

- dyspozytornię,
- serwerownię,

W pomieszczeniu serwerowni należy utworzyć punkt GPD wydzielonej sieci TECH-LAN na potrzeby SZT.

1.6. Budynek filtrów węglowych

W wyniku analizy zagrożeń budynek filtrów węglowych został zakwalifikowany do ochrony wg taktyki C z wydzielonymi strefami do ochrony wg taktyki D w stopniu 4.

W budynku wydzielone zostaną następujące strefy funkcjonalne:

- komunikacyjna,
- pomieszczeń technologicznych hydrotechnicznych,
- pomieszczenie transformatorów,
- pomieszczenie rozdzielni RG.
- pomieszczenie sterowni.

Powyższe strefy objąć systemem SSWIN w następujących stopniach zabezpieczenia:

- komunikacyjna – system bezklasowy,
- pomieszczeń technologicznych hydrotechnicznych – system w stopniu 2,
- pomieszczenie transformatorów – system w stopniu 2,
- pomieszczenie rozdzielni RG – system w stopniu 2,
- pomieszczenie sterowni – system w stopniu 2.

Wejście do budynku objąć kontrolą przejścia systemu SKD.
Dodatkowo kontrolą przejścia objąć następujące strefy:

- sterownię.

W pomieszczeniu sterowni należy utworzyć PPD wydzielonej sieci LAN na potrzeby SZT.

1.7. Budynek koagulacji

W wyniku analizy zagrożeń budynek koagulacji został zakwalifikowany do ochrony wg taktyki C z wydzielonymi strefami do ochrony wg taktyki D w stopniu 4.

W budynku wydzielone zostaną następujące strefy funkcjonalne:

- komunikacyjna,
- pomieszczeń technologicznych hydrotechnicznych,
- pomieszczenie magazynu reagentów,
- pomieszczenie rozdzielni 0,4kV,
- pomieszczenie techniczne na I piętrze z szafami sterowniczymi.

Strefy objąć systemem SSWIN w następujących stopniach zabezpieczenia:

- komunikacyjna – system bezklasowy,
- pomieszczeń technologicznych hydrotechnicznych – system w stopniu 2,
- pomieszczenie magazynu reagentów – system w stopniu 2,
- pomieszczenie rozdzielni 0,4kV – system w stopniu 2,
- pomieszczenie techniczne na I piętrze z szafami sterowniczymi – system w stopniu 2.

Wejście do budynku objąć kontrolą przejścia systemu SKD.

W pomieszczeniu technicznym na I piętrze należy utworzyć PPD wydzielonej sieci LAN na potrzeby SZT.

1.8. Budynek chlorowni

W wyniku analizy zagrożeń budynek chlorowni został zakwalifikowany do ochrony wg taktyki D w stopniu 5.

W budynku wydzielona została jedna strefa funkcjonalna obejmująca cały budynek.

Budynek objąć systemem SSWIN w 3 SZ SSWIN.

Weście do budynku objąć kontrolą przejścia systemu SKD.

W budynku należy utworzyć PPD wydzielonej sieci LAN na potrzeby SZT.

1.9. Budynek komory zasuw

W wyniku analizy zagrożeń budynek komory zasuw został zakwalifikowany do ochrony wg taktyki D w stopniu 4.

W budynku wydzielona została jedna strefa funkcjonalna obejmująca cały budynek.

Budynek objąć systemem SSWIN w stopniu 2.

Weście do budynku objąć kontrolą przejścia systemu SKD.

W budynku należy utworzyć PPD wydzielonej sieci LAN na potrzeby SZT.

1.10. Zbiorniki przy komorze zasuw

W wyniku analizy zagrożeń zbiorniki przy komorze zasuw zostały zakwalifikowane do ochrony wg taktyki D w stopniu 4.

Powierzchnię wierzchnią zbiorników należy objąć za pomocą czujek dopplerowskich oraz systemu VSS.

1.11. Budynek warsztatu elektrycznego

W wyniku analizy zagrożeń budynek magazynu elektrycznego został zakwalifikowany do ochrony wg taktyki A.

Ochrona dotychczasowa budynku nie wymaga podwyższenia i opiera się na podstawowym zabezpieczeniu mechanicznym.

1.12. Budynek warsztatu mechanicznego

W wyniku analizy zagrożeń budynek magazynu mechanicznego został zakwalifikowany do ochrony wg taktyki A.

Ochrona dotychczasowa budynku nie wymaga podwyższenia i opiera się na podstawowym zabezpieczeniu mechanicznym.

2. PW Żelewo

2.1. Teren podstawowy - ogrodzenie

W terenie wewnętrznym wydzielone zostaną następujące strefy funkcjonalne:

- linia ogrodzenia obiektu PW Żelewo podlegającego szczególnej ochronie,
- brama wjazdowa główna,
- bramy techniczne,
- furtki,

Wszystkie bramy i furtki objęte zostaną nadzorem systemu VSS.

Jako ochronę ogrodzenia i terenów bezpośrednio do niego przylegających należy zastosować system napłotowy ochrony obwodowej oparty o czujniki MEMS i kamery systemu monitoringu VSS. Jako uzupełnienie w miejscach szczególnie trudnych z uwagi na ukształtowanie terenu zostaną wykorzystane zewnętrzne czujki dopplerowskie ruchu.

2.2. Teren podstawowy – strefa peryferyjna

W wyniku analizy zagrożeń teren wewnętrzny (strefa peryferyjna - pomiędzy ogrodzeniem a budynkami i ogrodzeniami wewnętrznymi) został zakwalifikowany do ochrony wg taktyki C. Główne ciągi komunikacyjne będą nadzorowane przez kamery systemu monitoringu VSS.

2.3. Budynek pompowni stopnia pierwszego P-1

W wyniku analizy zagrożeń budynek pompowni stopnia pierwszego został zakwalifikowany do ochrony wg taktyki D w stopniu 4

W budynku wydzielone zostaną następujące strefy funkcjonalne:

- komunikacyjna,
- pomieszczeń technologicznych hydrotechnicznych:
- pomieszczenie rozdzielni 6kV,
- pomieszczenia dyspozytorni,
- pomieszczenie komory transformatora.

2.4. Budynek hangarowy

W wyniku analizy zagrożeń budynek hangarowy został zakwalifikowany do ochrony wg taktyki A. Ochrona dotychczasowa budynku ze względu na przechowywanie łoża wymaga zabezpieczeniem systemem SSWIN w stopniu bezklasowym i utrzymaniu dotychczasowego zabezpieczenia mechanicznego.

Szczegóły rozmieszczenia poszczególnych elementów systemów zabezpieczeń technicznych w obiektach przedstawiono w części rysunkowej.

9.1. Opis techniczny i funkcjonalny PSIM

Ilość elementów systemów bezpieczeństwa do zamontowania na terenie Zakładu oraz liczba generowanych przez nie informacji wymagać będzie uporządkowania, nadania hierarchii ważności oraz czytelnego przedstawienia wraz z podaniem precyzyjnych instrukcji dla operatora.

Bardzo duża ilość chaotycznych informacji przekazywanych w różnej formie na stanowisko operatora z wielu systemów bezpieczeństwa oraz innych systemów wspomagających może powodować dezorientację, spowolnienie obsługi i ryzyko podjęcia niewłaściwych decyzji w sytuacji kryzysowej.

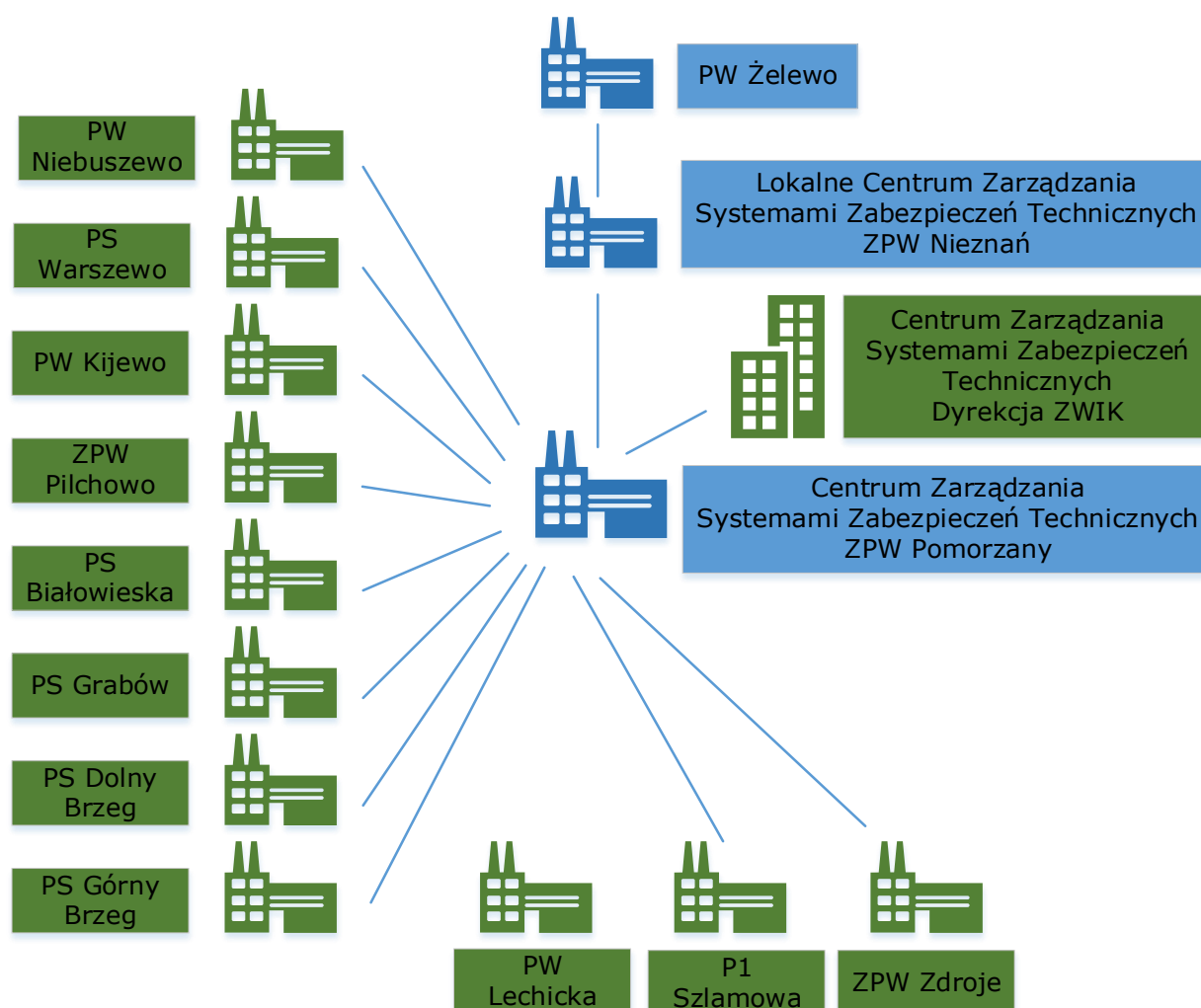
Z tego względu należy bezwzględnie dane te uporządkować, skategoryzować oraz podać w postaci czytelnej, hierarchicznej na stanowisko operatorskie tak, aby umożliwić szybkie i poprawne podjęcie decyzji co do sposobu eliminacji lub minimalizacji skutków danego zdarzenia alarmowego.

Zintegrowanie wielu niezwiązanych aplikacji i urządzeń zabezpieczających oraz sterowanie nimi przez jeden wszechstronny interfejs użytkownika to podstawowe założenie projektowania systemu wizualizacji i zarządzania SZB PSIM w obiektach ZWIK. Zastosowanie systemu PSIM zapewni wiele korzyści organizacyjnych, w tym zwiększoną kontrolę, ulepszoną świadomość sytuacji i raportowanie zarządzania. Przyczyni się do obniżenia kosztów działalności poprzez większą wydajność ochrony i poprawę bezpieczeństwa Zakładu.

Wszystkie systemy zabezpieczeń technicznych zainstalowane w obiekcie, tj. SSWIN, SKD, VSS, system ochrony obwodowej (system

napłotowy, czujki dopplerowskie, zespół radarowy), będą w pełni monitorowane i zarządzane z poziomu systemu PSIM.

System zarządzania bezpieczeństwem PSIM należy wyposażyć w wymagane interfejsy programowe integrowanych systemów, plany, panele techniczne, punkty, procedury działań zgodnie z polityką bezpieczeństwa obiektu. Należy przewidzieć w przyszłości w ramach jednej platformy sprzętowo-programowej PSIM możliwość integracji, wizualizacji i zarządzania wszystkimi systemami zabezpieczeń technicznych w pozostałych obiektach ZWIK.



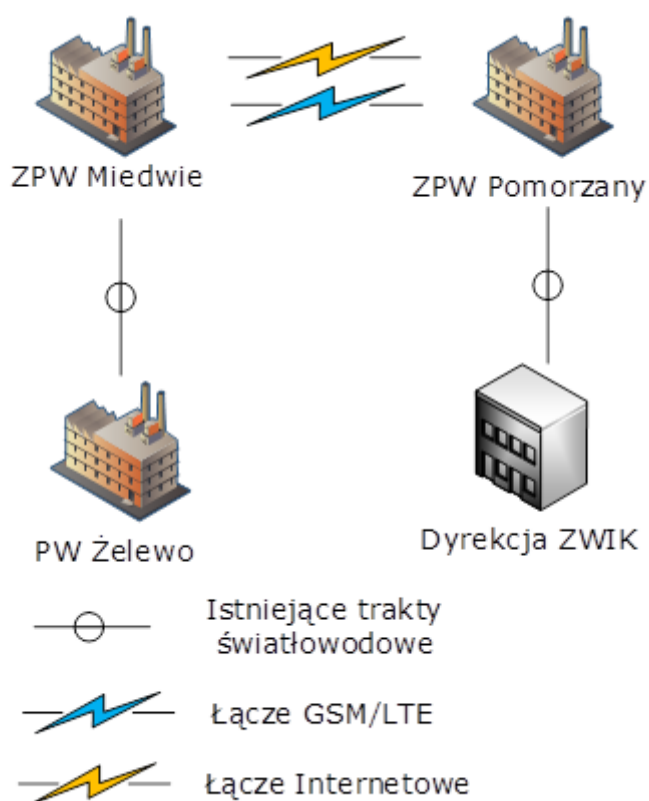
Rysunek – schemat integracji instalacji bezpieczeństwa w obiektach ZWIK

System PSIM strukturalnie składać się będzie z:

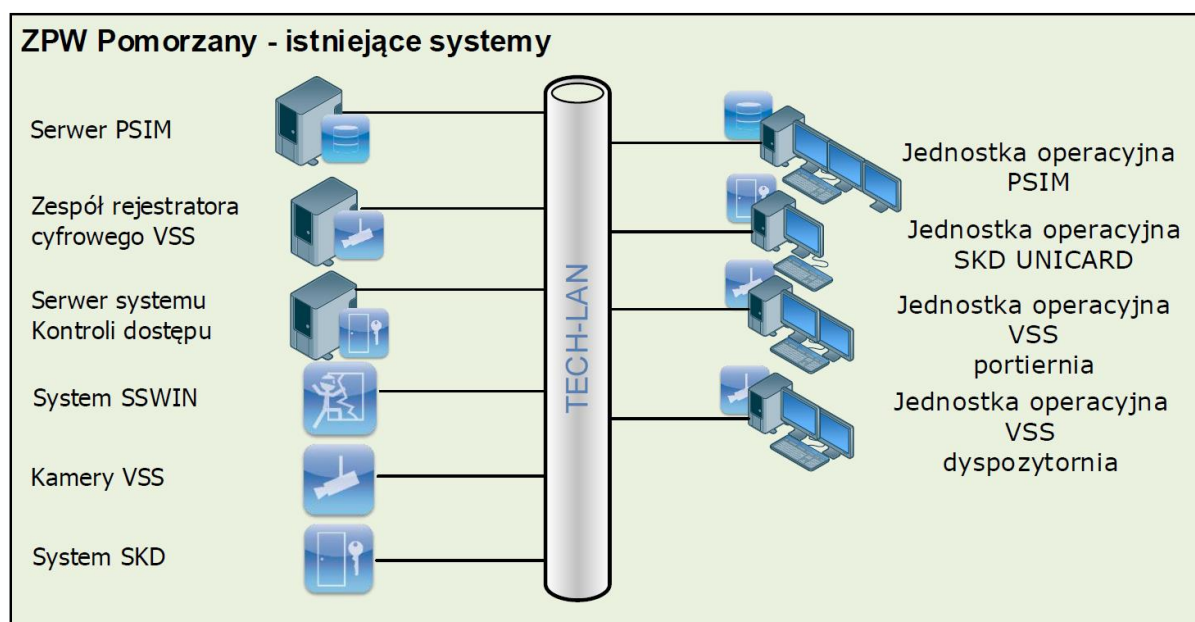
- istniejącej jednostki serwerowej centralnej zainstalowanej w Głównym Punkcie Dystrybucyjnym w ZPW Pomorzany

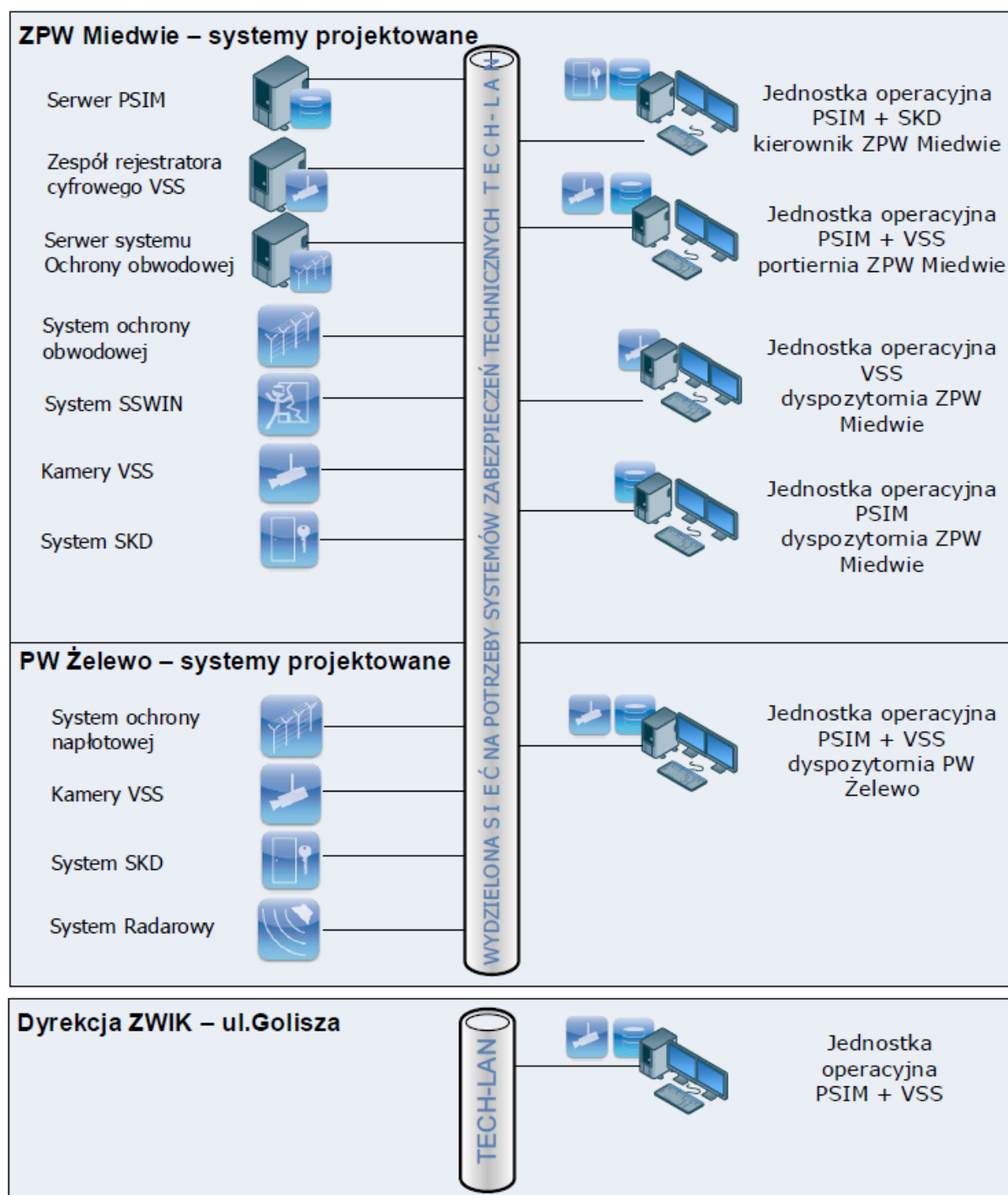
- jednostki serwerowej lokalnej zainstalowanej w Głównym Punkcie Dystrybucyjnym w ZPW Miedwie
- istniejących jednostek operatorskich klienckich w ZPW Pomorzany
- jednostki operatorskiej w budynku Dyrekcji ZWIK
- jednostek operatorskich klienckich:
 - portiernia ZPW Miedwie
 - dyspozytornia ZPW Miedwie
 - dyspozytornia PW Żelewo
- oprogramowania zarządzającego
- niezbędnych licencji oraz interfejsów programowych dla zarządzania i obsługi systemów zabezpieczeń technicznych.

Serwer lokalny PSIM zainstalować w GPD, tj. serwerowni w bud. Filtrów pośpiesznych na terenie ZPW Miedwie. Dzięki wykorzystaniu istniejących łączy światłowodowych pomiędzy ZPW Miedwie oraz PW Żelewo, w PW Żelewo zainstalować jedynie elementy sieciowe oraz wykonawcze poszczególnych systemów zabezpieczeń. Komunikację pomiędzy ZPW Pomorzany a ZPW Miedwie należy wykonać w oparciu o istniejące łącza Internetowe Zamawiającego. Jako awaryjny, alternatywny kanał transmisji należy wykonać połączenie GSM/LTE, przy wykorzystaniu tunelowania VPN oraz routerów brzegowych. Połączenie pomiędzy ZPW Pomorzany a budynkiem Dyrekcji ZWIK zostanie wykonane w oparciu o istniejące łącze światłowodowe i sieć LAN Zamawiającego.



Rysunek – Schemat funkcjonalny połączeń między obiektowych





Rysunek - Schemat funkcjonalny lokalnych PSIM

Integrację systemów zabezpieczeń technicznych należy wykonać w oparciu dedykowaną platformę programową oraz interfejsy programowe w zakresie przesyłania informacji o zdarzeniach alarmowych systemów zabezpieczeń technicznych. System wyposażać w moduł umożliwiający dostęp do stanu nadzorowanych urządzeń, podglądu listy zdarzeń i przeglądania archiwum w systemie za pomocą dedykowanego oprogramowania klienckiego pracującego w środowisku Windows. Ze względów bezpieczeństwa i szyfrowania danych nie dopuszcza się rozwiązań opartych o przeglądarki internetowe.

Czasy systemowe urządzeń zsynchronizować wg serwera czasu rzeczywistego zlokalizowanego w GPD ZPW Miedwie.

9.2. Opis techniczny i funkcjonalny systemu VSS

Długość ogrodzenia terenu Zakładu wynosi dwa kilometry. Zapewnienie nadzoru i kontroli nad tak rozległym obszarem wyłącznie przez pracowników ochrony fizycznej jest nieefektywne i nieekonomiczne. Konieczne jest wsparcie pracowników fizycznych przez elektroniczne systemy zabezpieczeń technicznych. Za wykrycie prób sforsowania ogrodzenia odpowiada system ochrony obwodowej. W celu weryfikacji generowanych przez niego alarmów wykorzystany zostanie system monitoringu wizyjnego VSS. Wykorzystując kamery wysokiej rozdzielczości operator będzie mógł w każdej chwili zweryfikować przyczyny alarmu i podjąć odpowiednie działania zaradcze.

System monitoringu wizyjnego zostanie zintegrowany z systemem ochrony obwodowej (systemy napłotowy i czujki dopplerowskie). Podstawową funkcją integracji jest wysterowanie kamer szybkoobrotowych tak, aby skierowały się w sektor zdarzenia alarmowego. Jednocześnie na jednostce operatora systemu PSIM automatycznie wyświetlone zostaną obrazy z kamer. Realizacja tej funkcjonalności zostanie zrealizowana przy wykorzystaniu dedykowanych interfejsów programowych zespołu rejestratora cyfrowego oraz systemu PSIM.

Dzięki temu rozwiązaniu operator będzie mógł szybciej zweryfikować przyczynę alarmu i podjąć optymalną decyzję odnośnie dalszych działań.

System VSS zostanie zintegrowany w ramach wspólnej platformy zarządzająco-integrującej PSIM w taki sposób, aby na stanowisku operatorskim PSIM otrzymać:

- Prezentację tekstową, wizualizację stanu zespołu rejestratora cyfrowego z zakresu:
 - o alarmów
 - o wyjść sterujących
 - o wejść
 - o kamer
 - o monitorów
 - o odtwarzania
 - o rejestracji
- Sterowanie:
 - o kamerami
 - o wejściami/wyjściami
 - o monitorami
 - o rejestratorem

System VSS należy wykonać w oparciu o sieciowe kamery stałopozycyjne, obrotowe i uchylno-obrotowe.

Kamery dozoru strefy obwodową, peryferyjną i wewnętrzną obiektu - zapewnić rejestrację obrazów z zapisem referencyjnym z gęstością 6 kl/s.

Kamery dozoru strefy wejścia/wjazdu - zapewnić rejestrację obrazów z zapisem referencyjnym z gęstością 12 kl/s.

Rejestrację i zarządzanie obrazami z kamer realizować wykorzystując Zespół Rejestratora Cyfrowego. Zespół wyposażać w możliwość obsługi wymaganej ilości strumieni wideo kamer IP, stacji podglądowych, bazy danych oraz sieciowych interfejsów komunikacyjnych dla wydzielonej sieci TECH-LAN na potrzeby systemów zabezpieczenia technicznego.

Zespół rejestratora cyfrowego zamontować w punkcie GPD ZPW Miedwie umożliwiając m.in. zapis, odtwarzanie, tworzenie kopii, eksport nagrań do popularnych formatów plików video, eksport klatek obrazów do typowego formatu pliku graficznego, retencję obrazów przez

co najmniej 30 dni. Nowy zespół rejestratora cyfrowego zostanie zintegrowany z istniejącym systemem monitoringu wizyjnego VSS w ZPW Pomorzany w taki sposób, aby umożliwić wyświetlanie, rejestrację i dostęp do nagrań archiwalnych z dowolnej kamery w ZPW Miedwie, PW Żelewo oraz ZPW Pomorzany, przy wykorzystaniu każdej z jednostek operatorskich, znajdujących się w tych lokalizacjach, a także z jednostki operatorskiej w budynku Dyrekcji ZWIK. Taka sama funkcjonalność musi być dostępna z poziomu wszystkich jednostek operatorskich systemu PSIM funkcjonujących w ZWIK.

Poszczególne punkty kamerowe rozmieszczono z uwzględnieniem zastosowania normatywnych rozdzielczości obrazu wg PN-EN 62676-4, tj. identyfikacji, rozpoznania, obserwacji lub detekcji.

Bramy i furtki, oraz wejścia należy objąć obserwacją kamerami stałopozycyjnymi z rozdzielczością obrazu 250px/m - identyfikacja, pozostały obszar strefy peryferyjnej należy objąć kamerami szybkoobrotowymi z zoomem umożliwiając obserwację terenu z rozdzielczością 125px/m – rozpoznanie. Obszar strefy zewnętrznej, tj. obszar zewnętrznego pasa buforowego i dalszy poza ogrodzeniem należy monitorować z rozdzielczością min. 25px/m – detekcja, przy czym ze strefy zewnętrznej nie przewiduje się detekcji sygnałów alarmowych, a jedynie monitoring w celach prewencyjnych.

W celu weryfikacji sygnałów generowanych przez system radarowy zaprojektowano kamerę szybkoobrotową, o rozdzielczości HDTV 1080p wyposażoną w zoom 30 krotny oraz zintegrowany oświetlacz podczerwieni IR. Kameralę należy zintegrować z radarem w taki sposób, aby nakierowywała się automatycznie na miejsca, w których wykryty zostanie ruch.

9.3. Opis techniczny i funkcjonalny instalacji systemu SSWIN

System SSWIN ma za zadanie ochronę obiektów zlokalizowanych na terenie ZPW Miedwie i PW Żelewo przed zaistnieniem przestępstw przeciwko mieniu oraz podnieść bezpieczeństwo obsługi w przypadku napadu. SSWiN ma za zadanie wykrycie i powiadomienie użytkownika systemu o naruszeniu bądź próbie naruszenia nadzorowanego obszaru. Celem nadrzędnym systemu jest jak najwcześniejsze wykrycie zagrożenia

i umożliwienie użycia właściwych środków w celu uniknięcia lub minimalizacji strat.

Celem SSWiN jest w szczególności:

- wykrycie intruza znajdującego się w obszarze objętym detekcją w czasie uzbrojenia systemu;
- wygenerowanie sygnałów alarmowych po wykryciu intruza zgodnie z zaprogramowanymi procedurami;
- detekcja osób zbliżających się do obiektów w granicach ich funkcjonowania;
- detekcja wejścia;
- transmitowanie sygnału alarmowego z każdego obiektu do lokalnego centrum zarządzania;
- prewencja;
- wygenerowanie odpowiednich ustalonych sygnałów alarmowych po aktywacji przycisku napadowego przez personel;
- integracja i wizualizacja zdarzeń w systemie PSIM.

System SSWiN ma umożliwiać m.in.:

- utworzenie niezależnie sterowanych stref nadzoru;
- sygnalizację optyczną i dźwiękową zdarzenia;
- automatyczne powiadamianie odpowiednich służb o zaistnieniu incydentów;
- zarządzanie poziomami dostępu do poszczególnych funkcji systemu;
- przeglądanie archiwów zdarzeń;
- integrację z systemem SKD, VSS, PSIM;
- bezprzerwowe podtrzymanie zasilania przez czas zgodny ze stopniem zabezpieczenia;
- szyfrowanie komunikacji co najmniej na poziomie AES 128 bit na połączeniach central SSWiN z platformą systemu integrującego PSIM.

Poszczególne czujki dozoru oraz ich lokalizacje wybrano w taki sposób, aby zapewnić możliwie najkrótszy czas detekcji intruza oraz pewność jego wykrycia. Szczegóły rozmieszczenia, typu oraz lokalizacji czujek przedstawiono w części rysunkowej.

9.4. Opis techniczny i funkcjonalny instalacji systemu ochrony obwodowej

W celu wczesnej detekcji wtargnięcia intruza na teren wewnętrzny Zakładu zostanie zainstalowany zintegrowany system ochrony obwodowej, w skład którego wchodzi:

- System ochrony napłotowej;
- Zewnętrzne dopplerowskie czujki ruchu;
- System monitoringu wizyjnego jako weryfikacja wizualna sygnału alarmowego;
- System zarządzania i wizualizacji PSIM.

Ogrodzenie zewnętrzne zabezpieczyć detektorami MEMS. W szafach punktów dystrybucyjnych PPD kontrolery podłączyć do sieci TECHLAN. Elementy systemu zwizualizować w systemie PSIM należy zintegrować z systemami monitoringu wizyjnego VSS.

Do ochrony obwodowej zastosować system czujników 3D MEMS z przewodową transmisją sygnałów alarmowych i zasilania. Nie dopuszcza się technologii bezprzewodowych z uwagi na ich podatność na zakłócenia toru transmisyjnego.

Czujniki instalować co 5 metrów w linii środkowej prześleń ogrodzenia.

Jako uzupełnienie systemu ochrony obwodowej, w miejscach gdzie konstrukcja ogrodzenia nie umożliwia wykonania systemu ochrony napłotowej (bramy przesuwne), zastosować czujki dopplerowskie.

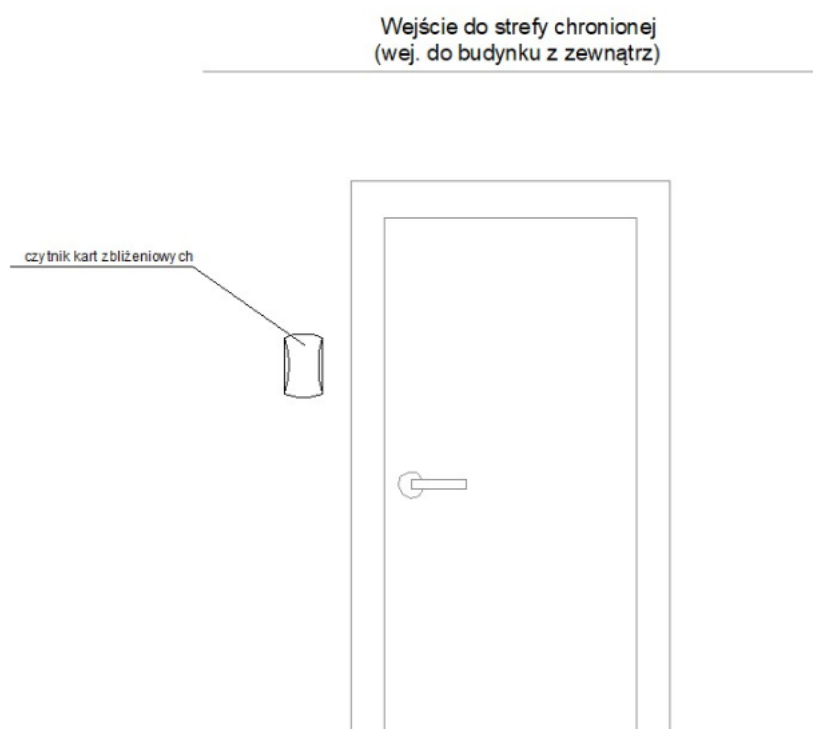
Szczegóły zabezpieczenia obwodowego przedstawiono w części rysunkowej.

Bardzo ważnym obszarem z punktu widzenia zapewnienia bezpieczeństwa obiektu jest ujęcie wody w PW Żelewo. Z uwagi na znaczną odległość ujęcia wody od brzegu, oraz jego lokalizację pod lustrem wody zapewnienie detekcji podejścia jest utrudnione. Z powyższych względów projekt zakłada nadzór tego obszaru przy wykorzystaniu urządzenia radarowego o zasięgu 450 m, zintegrowanego z kamerą szybkoobrotową, wyposażoną w oświetlacz podczerwieni dalekiego zasięgu.

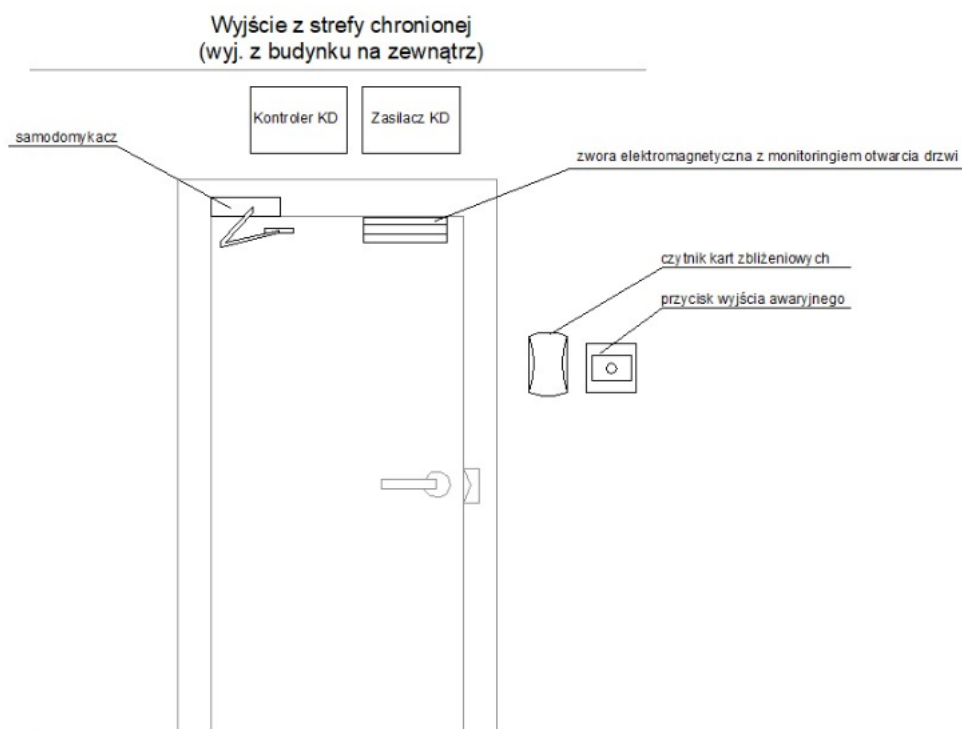
Wszystkie elementy systemu ochrony obwodowej należy zintegrować i zwizualizować w systemie nadrzędnym PSIM.

9.5. Opis techniczny i funkcjonalny instalacji systemu SKD.

W celu zapewnienia kontroli ruchu osobowego w obiekcie oraz wydzielenia stref niedostępnych dla osób nieuprawnionych należy wykonać system kontroli dostępu SKD. System SKD zrealizowany zostanie w oparciu o dwustronną kontrolę przejścia. Wykorzystane zostaną czytniki oraz spersonalizowane karty zbliżeniowe.



Rozmieszczenie elementów systemu KD w obszarze zabezpieczanego typowego przejścia. Widok od strony niechronionej.



Rozmieszczenie elementów systemu KD w obszarze zabezpieczanego typowego przejścia. Widok od strony chronionej.

Należy zainstalować modułowy system kontroli dostępu jako rozbudowę istniejącego systemu SKD zainstalowanego obecnie na ZPW Pomorzany. System ma zapewniać możliwość nadzoru i nadawania uprawnień użytkowników z poziomu administratora w ZPW Pomorzany. System musi wykorzystywać te same karty dostępowe, oraz obsługiwać tę samą bazę danych, które funkcjonują w ZPW Pomorzany.

Systemem SKD należy zintegrować i zwizualizować w systemie PSIM.

Szczegółowe rozmieszczenie elementów przedstawiono w części rysunkowej.

9.6. Opis techniczny i funkcjonalny wydzielonej sieci TECH-LAN

Na potrzeby elektronicznych systemów zabezpieczeń technicznych należy wybudować dedykowaną, wydzieloną sieć teletechniczna TECH-LAN.

Sieć TECH-LAN należy wykonać w topologii ringów. Jako medium transmisyjne wykorzystać kable światłowodowe wielowłóknowe, jednomodowe. Dzięki zastosowaniu komunikacji dwustronnej oraz protokołu RSTP, sieć będzie odporna na awarię urządzeń aktywnych sieci lub przerwy okablowania magistralnego.

Obiekty ZPW Pomorzany, oraz Dyrekcji ZWIK przyłączyć do sieci TECH-LAN ZPW Miedwie przy wykorzystaniu odpowiednio istniejących łączy Internetowych oraz łączy GSM/LTE, zgodnie z rysunkiem *Schemat funkcjonalny połączeń między obiektowych*.

Sieć zostanie skonfigurowana w oparciu o wirtualne sieci VA, z separacją dla poszczególnych systemów. Dodatkowo sieć management zostanie wydzielona logicznie.

Wymagane jest wykorzystanie zarządzanych przełączników sieciowych w celu optymalizacji i nadzoru parametrów sieci. W celu zwiększenia poziomu bezpieczeństwa urządzenia sieciowe zostaną poddane procesowi hardeningu (wyłączanie zbędnych usług, portów, zmiana domyślnych portów dostępu, haseł dostępowych itp.).

Stacje klienckie wyposażać w wysokiej klasy system antywirusowy ze zintegrowanym firewall, skonfigurowanym do dostępu tylko do niezbędnych usług serwerowych. Reszta ruchu sieciowego zablokować ze względu na bezpieczeństwo systemu. System serwerowy także podać procesowi hardeningu tak, aby aktywne pozostały jedynie niezbędne usługi.

Punkty dystrybucyjne wewnętrzne i zewnętrzne należy wykonać w postaci szaf telekomunikacyjnych typu rack lub przemysłowych w zależności od miejsca montażu, zgodnie z częścią rysunkową dokumentacji.

Szafy zewnętrzne montować na postumentach betonowych. Drzwi szaf PPD zabezpieczyć magnetycznymi czujnikami otwarcia w celu umożliwienia monitorowania stanu otwarcia drzwi.

Pośredni punkt dystrybucyjny (PPD) stanowi punkt węzłowy komunikacji, zarządzania i dystrybucji zasilania dla instalacji systemów zabezpieczeń technicznych.

Punkty PPD na potrzeby nadzoru poszczególnych obszarów ochrony powiązać logicznie w strukturze sieci TECHLAN w punktach wskazanych w części rysunkowej, tworząc połączenia w ringach światłowodowych.

Lokalizacje PPD wynikają z:

- optymalnego położenia względem kamer i pozostałych urządzeń systemów zabezpieczeń technicznych,
- zabezpieczenia przed dostępem osób nieupoważnionych,

- minimalizację wpływu warunków atmosferycznych i zakłóceń elektromagnetycznych,
- dostępności zasilania,
- optymalizacji struktury kablowej oraz połączeń sieciowych,
- ilości urządzeń aktywnych i pasywnych sieci.

Główny punkt dystrybucyjny GPD oraz PPD12 wewnętrzne należy wykonać jako stojące szafy rack 19" 42U 800x1000.

Szafy wyposażać w m.in.:

- część elektryczną 230 Vac:
 - rozłącznik główny izolacyjny
 - rozłącznik bezpiecznikowy
 - wkładka bezpiecznikowa,
 - ogranicznik przepięć,
 - lampka kontrolna obecności fazy,
 - wyłącznik nadprądowy,
 - moduły RDC z członem nadprądowym,
 - gniazdo z uziemieniem dla celów serwisowych,
 - przekaźnik,
 - gniazdo przekaźnika,
 - listwy zaciskowe,
 - zasilacz UPS
- część ochrony przeciwprzepięciowej torów sygnałowych UTP:
 - panel przeciwprzepięciowy,
- część teletechniczna:
 - zarządzalne przełączniki sieciowe w ilości zależnej od urządzeń obsługiwanych,
 - mikroprocesorowy kontroler punktu dystrybucyjnego z dedykowanym oprogramowaniem integrującym z systemem wizualizacji i zarządzania bezpieczeństwem PSIM: zintegrowane czujniki temperatury, wilgotności, nadzór obecności napięcia, otwarcia drzwi PPD, czujnika wstrząsowego. Programowalny wyświetlacz cyfrowy obrazujący stan techniczny nadzorowanego PPD oraz punktów kamerowych. Komunikacja: Ethernet.
- część zabezpieczenia przed nieuprawnionym dostępem:

- o wkładki patentowe,
 - o czujniki otwarcia drzwi,
- część organizacyjno – montażowa:
 - o panel krosowy,
 - o przełącznice światłowodowe,
 - o panel wentylacyjny.

Punkty dystrybucyjne w terenie zewnętrznym zostaną wykonane jako stojące na fundamencie prefabrykowanym, o wymiarach zależnych od ilości niezbędnego wyposażenia, zamykane na klucz.

Szafy PPD zewnętrzne wyposażać w m.in.:

- część elektryczną 230 Vac:
 - o rozłącznik główny izolacyjny
 - o rozłącznik bezpiecznikowy
 - o wkładka bezpiecznikowa,
 - o ogranicznik przepięć,
 - o lampka kontrolna obecności fazy,
 - o wyłącznik nadprądowy,
 - o moduły RDC z członem nadprądowym,
 - o gniazdo z bolcem dla celów serwisowych,
 - o przełącznik faz,
 - o przekaźnik,
 - o gniazdo przekaźnika,
 - o listwy zaciskowe,
- część zasilania napięcia stałego 48 VDC:
 - o zasilacz buforowy,
 - o przetwornica napięcia 48 VDC na 12 VDC,
 - o akumulatory 12 VDC,
- część ochrony przeciwprzepięciowej torów sygnałowych UTP:
 - o panel przeciwprzepięciowy,
- część teletechniczna:
 - o zarządzalne przemysłowe przełączniki sieciowe w ilości zależnej od urządzeń obsługiwanych,
 - o mikroprocesorowy kontroler punktu dystrybucyjnego z dedykowanym oprogramowaniem integrującym z systemem

wizualizacji i zarządzania bezpieczeństwem PSIM: zintegrowane czujniki temperatury, wilgotności, nadzór obecności napięcia, otwarcia drzwi PPD, czujnika wstrząsowego. Programowalny wyświetlacz cyfrowy obrazujący stan techniczny nadzorowanego PPD oraz punktów kamerowych. Komunikacja: Ethernet.

- część zabezpieczenia przed nieuprawnioną manipulacją:
 - o czujka magnetyczno – wibracyjna,
 - o wkładki patentowe,
 - o obudowy wkładki patentowej,
- część organizacyjno – montażowa:
 - o panel krosowy,
 - o przełącznice światłowodowe,
 - o odpowiednio od zastosowania: elementy grzejne, wentylacyjne.

Szafy należy uziemić. Rezystancja obwodu uziemienia szafy nie może przekroczyć 10Ω .

10. Określenie przebiegu, typu i sposobu układania instalacji teletechnicznej

Zakłada się wykorzystanie w maksymalnym stopniu istniejącej infrastruktury tras kablowych oraz kanalizacji teletechnicznej.

Istniejące okablowanie instalacji oświetlenia zgodnie z projektem nr. 806/PT/1070/875 pn. „Projekt rozbudowy systemu dozoru SSWiN i CCTV na terenie Zakładu Produkcji Wody Miedwie w Nieznaniu”, w miejscach kolidującymi z budowanymi trasami kablowymi należy zdemontować.

W miejscach wskazanych w części rysunkowej wybudować nową kanalizację teletechniczną. W pasach drogowych zastosować elementy odpowiednio wzmocnione. Kable światłowodowe układać w kanalizacji wtórnej przy wykorzystaniu rur osłonowych typu RHDPE 25/2 mm.

Okablowanie sygnałowe z punktów dystrybucyjnych do zewnętrznych kamer poza główną kanalizacją kablową prowadzić w rurach osłonowych RHDPE 32/2 mm. Na odcinakach ze studni kablowej do słupów i konstrukcji wsporczych urządzeń kable również prowadzić w rurze HDPE 32mm.

W celu prawidłowego ułożenia rur w gruncie należy zastosować się do poniższych wytycznych:

- na dnie wykopu ułożyć podsypkę z piasku o grubości nie mniejszej niż 10 cm;
- odległość między boczną częścią rury a ścianą wykopu powinna wynosić co najmniej 10 cm i stanowić powinna miejsce dla obsybki bocznej z piasku. Wysokość obsybki bocznej powinna stanowić łączną średnicę zewn. rury wraz dystansem między nimi;
- obsypkę wierzchnią z piasku ułożyć nie mniejszą niż 10 cm;
- pozostałą część wykopu zasypać do powierzchni gruntu z materiału dostępnego na miejscu, przy czym materiał ten nie powinien zawierać więcej niż 10% materiału frakcji 100-150mm. Zasyпка nie powinna być mniejsza niż 50 cm;
- zagęścić grunt do stopnia 85-90% wg zmodyfikowanej próby Proctora. W przypadku zagęszczania gruntu znajdującego nad rurą przy wykorzystaniu płyty wibracyjnej minimalna grubość warstwy ochronnej powinna wynosić 25 cm;

- zapewnić odległość między ułożeniem rur w pionie min. 2 cm z zastosowaniem uchwytych dystansowych. Dystanse układać w przypadku rur gładkościennych co 2 m, a rur karbowanych co 1,5 m;
- rury układać ze spadkiem co najmniej 0,1% w kierunku zaciągania kabla.

W budynkach instalacja układać w metalowych korytach podwieszanych, a także w rurach i listwach elektroinstalacyjnych PCV.

11. Określenie przebiegu, typu i sposobu układania instalacji

zasilających

Wybudować wydzieloną instalację zasilania na potrzeby elektronicznych systemów zabezpieczeń technicznych oraz instalacji oświetleniowej. Okablowanie pomiędzy rozdzielnicami zasilającymi a oprawami zostanie realizowane zgodnie z projektem nr 850/PT/1070/875 pn. „Projekt wymiany instalacji oświetlenia zewnętrznego na terenie Zakładu Produkcji Wody w Nieznaniu” w ramach odrębnego zadania. Kable WLZ układać pomiędzy istniejącymi obiektowymi rozdzielnicami zgodnie z częścią rysunkową.

Ochronę podstawową przed porażeniem prądem elektrycznym zrealizować przez zastosowanie izolowania części czynnych oraz stosowanie obudów o stopniu ochrony co najmniej IP4X. Ochronę dodatkową (przed dotykiem pośrednim) realizować za pomocą samoczynnego wyłączenia napięcia przy zastosowaniu wyłączników instalacyjnych. Wszystkie obwody oraz linia zasilająca powinny być powykonawczo sprawdzone pod względem skuteczności samoczynnego wyłączenia.

Ochrona przeciwporażeniowa polega na połączeniu części przewodzących dostępnych z uziemionym przewodem ochronnym PE lub ochronno-neutralnym PEN i powodującym w warunkach zakłóceń odłączenie zasilania. Punkty PPD należy podłączyć do istniejących instalacji uziemiania lub wykonać uziomy, których rezystancja nie może przekraczać 10Ω .

Należy zapewnić awaryjne podtrzymanie zasilania przez czas odpowiednio:

- SSWIN – 12 lub 30 godz. w zależności od stopnia zabezpieczenia 2 lub 3 wg PN-EN 50131-1;
- SKD – 2 godziny
- VSS – 2 godziny
- PSIM – 2 godziny

12. Ochrona odgromowa (przepięciowa)

Urządzenia systemów zabezpieczenia technicznego pracujące na zewnątrz np. kamery VSS, urządzenia zewnętrzne systemu SSWiN montować w strefie zabezpieczonych przez zwody piorunowe ochrony odgromowej budynku lub innej konstrukcji metalowej obiektu stanowiącą taką ochronę. Zespół radarowy należy zabezpieczyć wykorzystując dodatkowy zwód pionowy montowany na istniejącym słupie.

Urządzenia wyposażone w obudowy przewodzące należy uziemić.

Zabezpieczenia przeciwprzepięciowe zastosować zarówno na obwodach zasilających jak i sygnałowych jedynie od strony urządzeń aktywnych sieci TECHLAN w punktach dystrybucyjnych. Nie przewiduje się zabezpieczeń przeciwprzepięciowych przy kamerach, czujkach SSWiN, sygnalizatorach zewnętrznych.

Instalację elektryczną na potrzeby zasilania urządzeń SZT zabezpieczyć przeciwprzepięciowo na obwodach zasilania ochronnikami typu 1+2.

13. Ogrodzenie

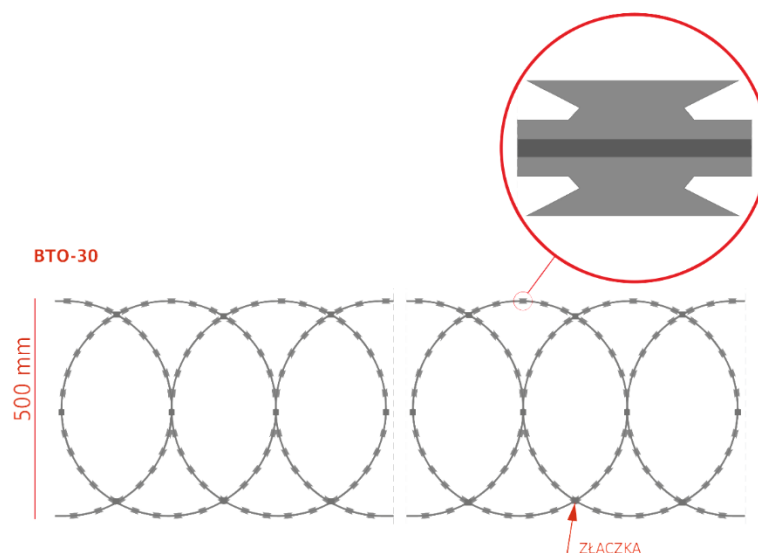
Istniejące ogrodzenie wykonane jest w różnej technologii: z siatki, przęseł panelowych i prefabrykatów betonowych.

Wysokość ogrodzenia jest poniżej 2m. W istniejącym ogrodzeniu brak jakiegokolwiek zabezpieczenia przed wejściem osób postronnych na teren zakładu. W ogrodzeniu występują liczne ubytki oraz możliwości wejścia niepostrzeżenie na teren chroniony. Ogrodzenie częściowo porośnięte pnączami, krzewami i drzewami.

Ogrodzenie z wyjątkami wskazanymi w części rysunkowej dokumentacji nie nadaje się do objęcia elektronicznym systemem napłotowym.

Biorąc powyższe pod uwagę, istniejące ogrodzenie wokół terenu ZPW Miedwie i PW Żelewo nie spełnia wymogów bezpieczeństwa i ochrony terenu Zakładu. Dlatego też należy dokonać jego modernizacji i wymiany na nowe. Zakres zmian przedstawiono w części rysunkowej.

W miejscach, gdzie przewidziano wymianę ogrodzenia i budowę nowego projektuje się ogrodzenie panelowe, kratowe o wysokości całkowitej 257 cm. Szerokość panelu 250 cm. Panel ogrodzeniowy kratowy – zgrzewany z surowego drutu, następnie cynkowany ogniowo lub galwanicznie i z powłoką poliestrową, z prętów stalowych poziomych podwójnych i pionowych pojedynczych. Średnica drutu poziomego (podwójny) – 2x6 mm; średnica drutu pionowego 5 mm. Wymiar oczek prostych 5x200 mm. Zakończenie od góry drutami pionowymi o długości 30 mm. Panel zakończony zasiekami płaskimi z drutu ostrzowego (kręgi umieszczone równolegle do osi ogrodzenia), zamocowanym na wysięgnikach słupków typu „I” na trzech rzędach drutu prostego ostrzowego. Zasiek o średnicy kręgu 500 mm z drutu ostrzowego (drut ze stali nierdzewnej) o gęstości min. 3,5-4 zwojów na metr bieżący ogrodzenia. Panele ogrodzenia łączone ze sobą za pomocą elementów spinających przenoszących drgania i montowane do słupków od czoła słupa.



Rysunek – Charakterystyka drutu ostrzowego

Panel posadowiony na podmurówce prefabrykowanej żelbetowej – $L=2,44\text{m}$, $h=0,3\text{m}$, $e=0,05\text{m}$.

Ogrodzenie należy zabezpieczyć antykorozyjnie za pomocą ocynku i powłoki poliestrowej.

Projektowane słupki – przekrój $60 \times 40 \times 1,5$ z odkosem stalowym typu „I” dla wsparcia zasieku ze zwojów drutu ostrzowego.

Fragmenty ogrodzenia wraz z bramami i furtkami od strony drogi gminnej w ZPW Miedwie oraz PW Żelewo pozostawić istniejące. Natomiast należy je uzupełnić o odkosy typu „I” z drutem ostrzowym.

Na terenie PW Żelewo należy dodatkowo uziemić ogrodzenie na odcinku 50m pod linią napowietrzną wysokiego napięcia. Uziemienie ogrodzenia należy wykonać za pomocą bednarki ocynkowanej FeZn $30 \times 4\text{mm}$. Rezystancja obwodu uziemienia nie może przekroczyć 10Ω .

Szczegóły przedstawiono w części rysunkowej.

13.1. Pas buforowy – usunięcie drzew i krzewów

Zauważalna obecność środków systemu bezpieczeństwa fizycznego (ogrodzenie i jego zwieńczenie, oświetlenie) zniechęca potencjalnych intruzów przed dokonaniem czynów prawnie zabronionych. Jednocześnie Narodowy Plan Ochrony Infrastruktury Krytycznej 2018 Rządowego Centrum Bezpieczeństwa nakłada obowiązek utrzymania zewnętrznego 3 metrowego

i wewnętrznego 5 metrowego pasa terenu tzw. pasa buforowego wolnego od zadrzewienia, aby mieć możliwość obserwacji i monitorowania ogrodzenia oraz wszystkich wejść i wyjść ze stref ochrony, a także sygnalizować naruszenie strefy, włamania i jak najszybsze wykrycie intruza i przeciwdziałania na szkodę obiektu. Usunięcie istniejącego zadrzewienia na obszarze pasa buforowego jest kluczową sprawą w zakresie zapewnienia bezpieczeństwa oraz zapobieganiu aktom terroryzmu, sabotażu oraz wandalizmu. Zakres wycinki przedstawiono w części rysunkowej.

13.2. Roboty ziemne - budowa ogrodzenia

- Pod budowę ogrodzenia należy zdjąć warstwę gruntów nasypowych o miąższości 0,5 m.
- Wykopy pod fundamenty bram oraz słupów ogrodzenia powinny być wykonane w ten sposób, aby nie naruszyć naturalnej struktury gruntu poniżej spodu fundamentów.
- Przy wykonywaniu wykopów fundamentowych za pomocą maszyn należy na dnie wykopu zostawić w gruntach sypkich warstwę gruntu o gr. 0,2 - 0,3 m, w gruntach spoistych – o gr. 0,5 m poniżej przewidywanego poziomu posadowienia, ze względu na możliwość rozluźnienia gruntu przez maszyny. Dalsze roboty ziemne należy wykonywać ręcznie.
- Wyrównanie, względnie podnoszenie poziomu dna wykopu przez podsypywanie gruntem miejscowym jest niedopuszczalne.
- Dno wykopów należy chronić przed zalaniem wodami powierzchniowymi i gruntowymi.
- Przy istnieniu na dnie wykopu w poziomie posadowienia gruntów spoistych, a szczególnie gruntów pylastych oraz gruntów łatwo rozmakających, należy bezpośrednio po wykonaniu wykopów pokryć dno wykopu warstwą chudego betonu o gr. 10 cm.
- Podczas wykonywania wykopów w warunkach zimowych należy ochronić podłoże gruntowe od przemarzania.
- Przed nastaniem mrozów fundamenty powinny być zasypane do odpowiedniej wysokości gruntem lub ochronione w inny sposób tak, aby nie nastąpiło zjawisko spęcznienia gruntów pod fundamentami.

13.3. Opis przyjętych rozwiązań konstrukcyjno-materiałowych ogrodzenie

- Wysokość ogrodzenia - 257 cm. Szerokość panela 2500 mm.
- Panel ogrodzeniowy kratowy – zgrzewany z prętów stalowych.
- Podmurówki żelbetowe typowe. Podmurówkę posadowić z wykorzystaniem uchwytów metalowych przy słupkach
- Stopy fundamentowe żelbetowe wylewane z betonu B25 (C20/25) zbrojone stal AIIIIN RB 500 i stal St0S-b, na podkładzie z chudego betonu (C10/12) .
- Dopuszczone wylewanie na mokro fundamenty pod słupki ogrodzeniowe – beton towarowy B20 półsuchy.
- Otulina zbrojenia – na całości gr. 4 cm.
- Izolacja powłokowa – dyspersyjna masa asfaltowo-kauczukowa

14. Minimalne wymagania funkcjonalno-użytkowe kluczowych urządzeń i oprogramowania

System zarządzania i wizualizacji PSIM

Wymagania systemu PSIM

System zarządzania i wizualizacji PSIM powinien być otwartym, modułowym konfigurowalnym systemem klasy *PSIM (Physical Security Information Management)*, który ma zastosowanie jako neutralna platforma służąca do integracji i zarządzania heterogenicznymi technologiami bezpieczeństwa, zarządzania budynkami i obiektami oraz urządzeniami zastosowanymi w poszczególnych instalacjach. System powinien charakteryzować się koncepcją otwartego interfejsu i dużą liczbą dostępnych standardowych modułów interfejsów, które pozwolą na podłączenie wielu systemów bezpieczeństwa i techniki budowlanej, tworząc jedno homogeniczne środowisko pracy, zapewniające centralizację i pełen nadzór nad realizowanymi procesami zarządzania bezpieczeństwem. System musi zapewnić skalowalność i modułowość, które pozwolą na swobodne i nieograniczone w czasie dostosowanie systemu zarządzania do struktury obiektowej, funkcjonalnej i organizacyjnej. Rozwiązanie musi umożliwić użytkownikowi końcowemu zarządzanie zdarzeniami, które zostaną wykryte przez różne systemy, tworząc jednolity plan sytuacyjny dla całego obiektu lub zespołu obiektów.

Aplikacja PSIM powinna być definiowana jako oprogramowanie PSIM+, co oznacza, że rozwiązanie wykracza poza ramy standardowych wizualizacji, oferując możliwość zaawansowanej integracji wszystkich technologii systemów bezpieczeństwa, systemów przemysłowych, aplikacji dziedzinowych, automatyki budynkowej czy komunikacji.

System zarządzania i wizualizacji musi odbierać wszystkie incydenty z różnych systemów bezpieczeństwa, automatyki i komunikacji. Inteligentna wizualizacja zdarzeń powinna umożliwić użytkownikowi łatwe rozpoznanie sytuacji na obiekcie oraz wypracowania decyzji zarządczych. System musi zawierać między innymi: dynamiczne scenariusze, plany sytuacyjne, automatyczne działania, dzięki którym operator będzie naprowadzany do najbardziej odpowiedniej metody

rozwiązania problemu zgodnie z ustalonymi wytycznymi zarządzania kryzysowego.

System PSIM musi zapewnić możliwość rozbudowy w przyszłości o kolejne obiekty ZWiK, dlatego system musi mieć możliwość konfiguracji w różnych wariantach. Jednocześnie system musi mieć możliwość połączenia wszystkich lokalizacji i zarządzania nimi z Centrum Zarządzania Systemami Zabezpieczeń Technicznych znajdującym się w ZPW Pomorzany oraz Dyrekcji ZWiK.

Struktura rozwiązania PSIM

System PSIM powinien oferować wysokiej klasy rozwiązanie spełniające wymagania nowoczesnego zarządzania bezpieczeństwem. System powinien integrować i łączyć systemy bezpieczeństwa i zarządzania budynkiem różnych producentów w jednym jednolitym, przyjaznym dla użytkownika interfejsie i służyć jako scentralizowana jednostka dowodzenia i kontroli.

System PSIM musi mieć możliwość wdrożenia jako system jedno lub wielostanowiskowy, stand-alone bądź jako rozproszona instalacja, która powinna się składać z wielu serwerów lokalnych i nadrzędnym centrum zarządzania:

- ✓ PSIM jako pojedynczej stacji roboczej (autonomicznej).
- ✓ System PSIM z zastosowaniem serwera z Hot-Standby (redundancji), serwerami lokalizacji (serwery w poszczególnych lokalizacjach), serwerem interfejsów i klientami końcowymi z różnymi interfejsami.

Każda stacja w sieci musi mieć unikalną nazwę, która będzie konfigurowana lokalnie w ustawieniach stacji. Każda stacja musi posiadać swój unikalny numer, który jest skonfigurowany w tabeli stacji roboczych i przypisany do odpowiednich nazw. Numer ten będzie wykorzystywany wewnętrznie w systemie m.in. do identyfikacji danych lokalnych stacji. Dodatkowo każda stacja musi pełnić rolę (serwer aktywny, serwer rezerwowany itp.) przejmując określone funkcje wynikające z rodzaju i roli w systemie w danym momencie.

Stacje w sieci muszą komunikować się ze sobą za pośrednictwem połączeń TCP / IP, gdzie wszystkie interakcje i dostęp do danych w

systemie muszą być realizowane tylko za pośrednictwem tych połączeń IP.

Synchronizacja zegara i szyfrowanie komunikacji

Jednym z ważnych wymogów działania sieci jest synchronizacja czasu między stacjami roboczymi. Jedna stacja robocza, na przykład serwer, powinna być skonfigurowana / zainstalowana jako serwer czasu Windows®. Wszystkie inne stacje robocze powinny synchronizować czas za pośrednictwem tej stacji roboczej. Alternatywnie czas może być synchronizowany przez PSIM, przy czym logowanie użytkownika w systemie Windows® będzie wymagało niezbędnych uprawnień.

Cała komunikacja pomiędzy poszczególnymi stacjami roboczymi (Serwer / Klienci) musi być realizowana w sposób szyfrowany (AES 256). System musi umożliwiać również szyfrowanie samej bazy danych systemu.

Podstawowe rozwiązania sprzętowe systemu PSIM

Podstawowe typy urządzeń wymagane w infrastrukturze systemu PSIM+:

- ✓ Serwer (również serwer/y rezerwow/e)

Serwer powinien być definiowany w systemie jako podstawowe miejsce zapisu danych i zasad dostępu do nich. W zależności od tego, który serwer jest aktualnie aktywnym serwerem – przy scenariuszu z serwerami redundantnymi, połączenia interfejsów i priorytety połączeń IP mogą być opcjonalnie skonfigurowane inaczej dla każdego z serwerów. Koncepcja powinna być realizowana w oparciu o rozproszone przechowywanie danych na serwerach i klientach w systemie PSIM. Serwery rezerwowe (2 lub 3) powinny być konfigurowane tak samo, jak serwer aktywny. W przypadku niedostępności aktywnego serwera, jeden z serwerów rezerwowych przejmie rolę serwera aktywnego. Jeśli chodzi o podział ról, serwery powinny synchronizować się ze sobą i automatycznie rozwiązuje wszelkie konflikty.

Wszystkie dane główne i uruchomieniowe dotyczą czasu trwania połączenia, konsekwentnie przechowywane na serwerach równolegle i synchronizowane. Wszystkie serwery muszą zawsze zawierać aktualny stan systemu. Przełączanie aktywnego serwera

powinno odbywać się ręcznie lub automatycznie. Ponieważ chodzi tylko o zmianę roli, przełącznik powinien zostać wykonany bezpośrednio podczas operacji na serwerze. W razie potrzeby nastąpi również restart interfejsów, których dotyczy przełącznik - w sposób przejrzysty dla użytkownika.

Bieżący stan serwera powinien być zwizualizowany w interfejsie użytkownika (UI) za pośrednictwem stanów i zdarzeń punktów danych. Ponadto polecenia i zdarzenia dla poprzedniego trybu podwójnego (z jednym serwerem i jednym trybem gotowości) powinny być dodatkowo obsługiwane, dzięki czemu nie będzie wymagana adaptacja w istniejących systemach.

✓ Serwer lokalizacji

Serwer lokalizacji powinien pełnić funkcję serwera interfejsu, ale dodatkowo powinien oferować funkcje routingu i logowania, tzn. inni klienci mogą się do niego logować. W przypadku zastosowania serwera lokalizacji musi istnieć możliwość zdefiniowania zasad komunikacji oraz zakresu wymiany danych z serwerem głównym.

System powinien posiadać funkcję segmentacji danych dużych systemów sieciowych, które w razie potrzeby będzie można rozdzielić na częściowe ilości (zwane segmentami).

Segmentacja powinna służyć realizacji zbioru logicznych mniejszych systemów częściowych w ramach dużego systemu sieciowego.

Dostęp do danych obcego segmentu musi być zabezpieczony w sposób niezawodny, nie tylko na podstawie uprawnień, ale także ze względu na to, że dane nie są nawet przekazywane do stacji spoza segmentu. Każdy zestaw danych i każdy plik musi być przypisany tylko do dokładnie jednego segmentu. Kwoty częściowe zdefiniowane przez segmenty muszą być rozłączne, chyba że zestaw danych nie zostanie przypisany do żadnego segmentu, wtedy musi być dostępny we wszystkich segmentach.

W definicji stacji roboczej powinno się ustalić, które segmenty danych będą tam dostępne. Jeśli dla stacji nie zostanie wskazany segment, wszystkie dane będą tam dostępne.

✓ Serwer interfejsów

Serwer interfejsów musi posiadać funkcjonalność klienta, ale dodatkowo powinien oferować możliwość obsługi interfejsów. Oznacza, to iż w przypadku małych instalacji nie jest wymagane stosowanie serwera, a w przypadku dużych, sieciowych instalacji serwer interfejsów, powinien umożliwiać optymalizację ruchu i przesyłu danych pomiędzy poszczególnymi lokalizacjami, jak i umożliwiać efektywnie przyłączać małe lokalizacje do rozbudowanej struktury bezpieczeństwa.

✓ Wyświetlanie wideo

System PSIM powinien umożliwiać zainstalowanie klienta o funkcjonalności programu wyświetlania wideo, który musi być osobną stacją roboczą PSIM i jest przeznaczony do wyświetlania wideo. Każda stacja robocza powinna umożliwiać definiowanie do czterech okien wideo, a każde okno można podzielić na różne obszary wyświetlania wideo.

✓ Stacje robocze (klienci)

Klient pełni funkcje stanowiska ogólnego, tj. powinien służyć przede wszystkim do obsługi systemu po zalogowaniu się na danego użytkownika, do którego przypisane będą role i prawa dostępu.

Opcjonalnie, powinna być możliwość podłączenie określonych interfejsów z funkcjami specjalnymi, takimi jak np. SMS, e-mail, sterowanie wideo, zarządzanie LDAP, itp.

Interfejsy systemowe

Systemy różnych producentów, typów i rozmiarów powinny być podłączone do systemu PSIM poprzez interfejsy. Interfejsy powinny być specjalnie opracowane zgodnie z indywidualnymi opisami protokołów

przez producenta lub można zastosować standardowe interfejsy, takie jak OPC czy Modbus.

Wiele dzisiejszych interfejsów wykorzystuje TCP / IP jako podstawę do komunikacji, inne, zwykle starsze, wykorzystują połączenia szeregowe, takie jak RS232 lub RS485.

Technicznie wyróżnia je zdolność do wysyłania tylko danych (zdarzeń) lub odbierania danych i obsługi funkcji kontrolnych, takich jak wyłączanie, otwieranie aplikacji itp. Niektóre systemy zapewniają również możliwość zapytań lub definiowania złożone dane, takie jak dane konfiguracyjne.

System PISM powinien obsługiwać oba typy interfejsów i koncentrować się na optymalizacji wydajności zapewnianej przez odpowiedni interfejs.

System PSIM musi umożliwiać integrację z systemami zewnętrznymi za pomocą interfejsów systemowych. Oprócz wsparcia i obsługi otwartych, uniwersalnych protokołów (np. OPC, ModBus, BacNet), system PSIM powinien zapewniać ponad 400 interfejsów natywnych oraz narzędzia do generowania nowych interfejsów, niebędących wspieranych przez standardową funkcjonalność.

System PSIM+ powinien posiadać wydajną strukturę sprzętową, która pozwoli na budowanie najbardziej złożonych i rozbudowanych instalacji sieciowych, zapewniających dostęp do ściśle określonych i wymaganych danych na każdym z poziomów zarządzania.

W celu osiągnięcia najwyższych standardów bezpieczeństwa system PSIM musi umożliwiać zastosowanie nawet 3 serwerów w układzie redundantnym oraz pełne szyfrowanie komunikacji, z wykorzystaniem protokołu AES 256.

Interfejs użytkownika

Interfejs użytkownika systemu PSIM musi w pełni dostosować się do wymagań projektu i użytkownika. Interfejs musi składać się przynajmniej z:

- ✓ Okna głównego, które w zależności od konfiguracji okna musi wyświetlać nazwę projektu w ramie okna.
- ✓ Menu i pasek narzędzi znajdującego się w górnej części do wywoływania funkcji systemu.
- ✓ Obszar eksploratora po lewej stronie służącego jako centralny panel sterowania.
- ✓ Dolnej sekcji, która będzie zawierać listę aktualnie zarządzanych zdarzeń
- ✓ Paska stanu, który wyświetli informacje o stanie systemu.

W systemie PSIM+ interfejs użytkownika (układ, tło, elementy wyświetlacza itp.), dostępne funkcje i uprawnienia muszą zależeć od utworzonego profilu, który definiuje prawa użytkowników w systemie.

Profile użytkowników i wsparcie dla LDAP

W systemie zasadniczo powinno rozróżniać się typy profili, profile użytkownika, stacji roboczej, funkcji i uprawnień. Poprzez profile powinna być możliwość definiowania wyglądu i funkcji interfejsów użytkownika dla użytkowników, grup użytkowników i stacji roboczych. System powinien umożliwiać definiowanie uprawnień użytkownika do pracy w systemie w profilu użytkownika. System powinien umożliwiać przypisanie każdemu użytkownikowi więcej niż jeden profil, aby zapewnić mu niezbędne uprawnienia i funkcje do wykonywania jego obowiązków.

System musi umożliwiać użytkownikom wybór spośród przypisanych im profili podczas logowania do systemu. Wybór powinien być wstępnie przydzielony z domyślnym profilem użytkownika lub stacji roboczej. Wygląd i funkcje programu oraz interfejsu użytkownika muszą zależeć od wybranego profilu, podobnie jak uprawnienia. Jeśli użytkownik nie będzie miał przypisanego profilu, po zalogowaniu się powinien korzystać z predefiniowanego standardowego interfejsu ze wszystkimi uprawnieniami (administratora).

Użytkownik powinien mieć możliwość zdefiniowania globalnie lub dla każdej stacji roboczej i skonfigurowany tak, aby logował się automatycznie przy uruchomieniu programu przy wykorzystaniu funkcji

LDAP (Login with Active Directory) do katalogu aktywnego (wymagany serwer Windows®).

Prawa użytkowników

Prawa użytkowników systemu PSIM muszą być zarządzane centralnie i jednolicie. Rdzeniem koncepcji praw powinny być w dużej mierze swobodnie definiowane Aktywności / Prawa indywidualne, za pomocą których będzie można tworzyć Reguły. System powinien umożliwiać przypisywanie reguł do zestawów reguł, profili, użytkowników lub stacji roboczych. W rezultacie do każdego profilu - bezpośrednio lub pośrednio poprzez zestawy reguł - będzie można przypisać określoną liczbę reguł. W ten sam sposób system musi umożliwić przypisywanie pewnej liczby reguł do każdej stacji roboczej - bezpośrednio lub pośrednio poprzez zestawy reguł. Przydział między profilami, stacjami roboczymi, zestawami reguł i regułami musi być określany w trzech kolumnach po lewej stronie okna dialogowego, gdzie ikony powinny wskazywać, czy przypisania są wykonywane za pośrednictwem stacji roboczych, profili (typ profilu) czy zestawów reguł.

Reguły

Reguły w systemie PSIM muszą określać, co dany użytkownik może robić w systemie i powinna być możliwość ich przypisywania do każdego profilu lub stacji roboczej. Reguły muszą wynikać z definicji czynności - pozwalają lub zabraniają informacji, a także muszą posiadać priorytet. Reguły powinny również kompilować w zestawy reguł.

Reguły muszą składać się z: czynności lub pojedynczego prawa lub grupy czynności / pojedynczych praw określonych w Czynności / Pojedyncze prawa; zezwolenie lub zakaz; priorytet (od 0 do 10). W przypadku działań w programie, które są podporządkowane systemowi reguł systemu PSIM - na przykład uprawnień kontrolnych dla punktów danych – powinna być przeszukiwana lista przypisanych reguł począwszy od najwyższego priorytetu. Zakazy z tym samym priorytetem co uprawnienia muszą mieć wewnętrznie wyższy priorytet niż uprawnienia (o tym samym priorytecie). Jeśli zostanie znaleziona pasująca reguła, mechanizm musi się zatrzymać, a akcja jest dozwolona lub zabroniona

zgodnie z dokładną definicją reguły. Jeśli nie zostanie znalezione dopasowanie, akcja będzie zabroniona.

Na przykład, jeśli kontrolowanie punktów danych (wszystkie) jest dozwolone z priorytetem 0; punkty danych w lokalizacji A są zabronione z priorytetem 0; punkty danych z interfejsu 1 są dozwolone z priorytetem 1; w rezultacie jeden powinien kontrolować punkty danych z interfejsu 1, ale nie powinien kontrolować punktów danych, które są przypisane do lokalizacji A lub jednej z jej podrzędnych lokalizacji z dowolnego innego interfejsu. Identyczne wpisy powinny pojawiać się wielokrotnie na liście reguł, na przykład gdy kilka zestawów reguł jest przypisanych do profilu, a reguły zawarte w zestawach reguł nakładają się.

Układ interfejsu użytkownika

Interfejs użytkownika musi być ogólnie dostępny w pełnym obszarze wyświetlania stacji roboczej, a w przypadku alertów powinien tu również wyświetlić odpowiednie zdarzenia.

Menu i pasek narzędzi okna głównego muszą zawierać ogólne funkcje, które generalnie będzie można zawsze wykonać, niezależnie od typu otwieranych lub wyświetlanych elementów.

Wygląd okna głównego i / lub całego interfejsu użytkownika powinien być w większości konfigurowalny w sposób otwarty, dzięki czemu można samodzielnie określić, co i gdzie ma być wyświetlane.

Dodatkowo, poprzez odpowiednie ustawienia w profilach użytkownika i stacji roboczej system powinien umożliwiać określenie, jak będzie skonfigurowany interfejs użytkownika. Użytkownik powinien zdecydować czy menu lub pasek narzędzi ma być w ogóle wyświetlany. System powinien umożliwić łatwe ustalenie definicji menu, pasków narzędzi i klawiszy skrótów dla użytkowników lub stacji roboczych. System powinien umożliwić zmianę ustawień dostępu do systemu i indywidualne prawa użytkownika poprzez profile użytkowników.

Co istotne, system musi umożliwiać dowolną edycję zawartości obszaru wyświetlania, w tym edycję grafiki, tekstów, układów itp.

Przywoływanie tych elementów powinno odbywać się za pomocą dodatkowych zakładek lub pasków, a także dodatkowych wyskakujących

okienek lub okienek. Układy powinny pozwalać na elastyczną konfigurację obszaru wyświetlania zgodnie z własnymi preferencjami.

Jeśli dla stacji roboczej zostanie zdefiniowanych kilka okien (praca na wielu monitorach), te dodatkowe obszary wyświetlania powinny zostać również, niezależnie, odpowiednio skonfigurowane.

Ekspłorator danych

System musi umożliwić poruszanie się po dużych, rozbudowanych, strukturach danych powiązanych i zarządzanych z poziomu systemu. W systemie muszą być dostępne hierarchiczne reprezentacje danych, mechanizmy przeciągnij i upuść, przejrzyste prezentacje stany systemu, opcje bezpośredniego sterowania i inne liczne narzędzia ułatwiające obsługę.

Oknie eksploratora punkty danych powinny być wyświetlane z ich bieżącymi stanami. Punkty danych powinny być uporządkowane hierarchicznie, ale powinna być możliwość zmiany ustawień w ustawieniach filtru. Punkty danych powinny być przypisane do odpowiednich kategorii punktów danych na najwyższym poziomie hierarchii. Kategorie punktów danych powinny być wyświetlane w tym miejscu tylko wtedy, gdy zostały zdefiniowane i przypisane punkty danych odpowiadające odpowiedniej kategorii punktów danych. W przeciwnym razie te elementy zostaną wygaszone. Ogólna widoczność punktów danych w eksploratorze może być ograniczona przez prawa. Ponadto, aby wybrać punkty danych do wyświetlenia, muszą być zdefiniowane filtry za pomocą okna dialogowego filtrów do wyboru punktów danych do wyświetlenia. Bieżące stany punktów danych powinny być oznaczone symbolem stanu znajdującym się za punktem danych. Oprócz symbolu tekst stanu może być również wyświetlany po symbolu.

Jeśli operator nakieruje kursor nad punkt danych lub czujnik, powinny zostać wyświetlone dodatkowe informacje o tym w postaci małego okna informacyjnego (Etykieta) w pobliżu pozycji kursora. Treść odpowiedzi powinna być zdefiniowana dla interfejsu w systemie. Domyślnie powinna być wyświetlona nazwa punktu danych (jeśli dotyczy z numerem czujnika), typ czujnika, lokalizacja i opis, o ile te treści są zdefiniowane. Jeśli czujniki są przypisane do punktu danych,

powinny znajdować się poniżej punktu danych, do którego są przypisane. Punkty danych powinny być edytowane za pomocą widoku formularza. Zmiany w kategorii lub nazwie punktu danych są muszą być natychmiast wprowadzane w oknie eksploratora po ich zapisaniu.

Dla wygody operatora, dwukrotne kliknięcie punktu danych powinno spowodować otwarcie widoku testowego punktu danych w jego bieżącym stanie. Jeśli widok testowy będzie aktywny, kliknięcie w punkt danych powinno spowodować zmianę sposobu wyświetlania.

To, który z eksploratorów będzie dostępny dla danego użytkownika, musi określać definicja przypisanej listy menu.

Elastyczność interfejsu użytkownika

Informacje prezentowane w obszarach wyświetlania powinny być przetwarzane przez użytkownika na różne sposoby, przy czym użytkownik musi mieć odpowiednie uprawnienia, a pulpit (obszary / zawartość) musi być skonfigurowany tak, aby zezwalał na realizację tychże poleceń przypisanych do użytkownika.

Elementy z obszaru wyświetlania powinny umożliwiać zmianę w swobodnie przesuwane okna lub ponowa integrację pulpitem. System powinien umożliwiać podzielenie istniejących obszarów i wypełnienie ich dodatkową treścią lub usunięcie poszczególnych obszarów wyświetlacza. Obszar aktywny powinien być zaznaczony kliknięciem myszy i oznaczony kolorową ramką (domyślnie: np. ciemnożółta). System powinien umożliwiać przenoszenie obszarów za pomocą przeciągania i upuszczania w interfejsie użytkownika. Odbywa się to poprzez kliknięcie tytułu obszaru i przeciągnięcie go w wybrane miejsce. W miejscu docelowym obszar powinien być podświetlony kolorem, gdzie można wstawić ten przeciągnięty obszar. System powinien umożliwiać określenie powierzchni docelowej, przesuwając mysz w inne miejsce. Jeśli mysz zostanie umieszczona po prawej, lewej stronie, u góry lub u dołu obszaru docelowego, obszar docelowy powinien zostać odpowiednio podzielony, a przeniesiony obszar powinien zostać wstawiony jako podział. Jeśli mysz zostanie umieszczona pośrodku, przesunięty obszar powinien zostać wstawiony jako dodatkowa zakładka lub pasek do obszaru docelowego.

Edytor grafik

System PSIM powinien zawierać wybudowany edytor grafik. Oznacza to, iż operator posiadający określone uprawnienia będzie mógł samodzielnie przygotowywać grafiki systemowe, jak i na bieżąco dokonywać ich aktualizacji przy wykorzystaniu wbudowanych narzędzi.

Funkcje edytora graficznego w systemie PSIM muszą być zorientowane obiektowo i oparte na grafice wektorowej. Każdy kształt geometryczny musi reprezentować obiekt, który można edytować i któremu będzie można przypisać określone właściwości (na przykład kolor, szerokość linii itp.). System musi umożliwiać gromadzenie obiektów w grupy. Grupa powinna zachowywać się wtedy jak jeden obiekt, a wszystkie elementy w tej grupie muszą być razem. Każdy punkt powinien przypisać maksymalnie pięć grafik, które będzie można wyświetlić w przypadku wystąpienia zdarzenia. Grafikę będzie można również definiować niezależnie od zdarzeń i przedstawiać informacje, takie jak bieżące stany punktów danych (na przykład jako grafika tła). Nazywa się to grafiką stanu.

Warstwy grafik

Edytor grafiki umożliwia zdefiniowanie kilku indywidualnych poziomów grafiki, które można edytować niezależnie od siebie. Te poziomy nazywane są warstwami. Funkcje takie jak Okienko, Ramka i Szybki kadr pozwalają na użycie części grafiki w innych grafikach. W ten sposób, na przykład, poszczególne sekcje rzutu budynku powinno móc wykorzystać w innych grafikach i wstawić tam jako dodatkowe obiekty. Oprócz kształtów geometrycznych istnieją również inne obiekty, takie jak importowane grafiki, symbole, przyciski, wyświetlacze wideo itp. Za pomocą przycisków użytkownik powinien mieć możliwość zaprojektowania grafiki w sposób interaktywny. Użytkownik powinien mieć możliwość wstawiania przycisków w celu wyświetlania dodatkowej grafiki, kontroli punktów danych, wyświetlania tekstów itp. Umożliwi to łatwe wyświetlanie zarówno przeglądu, jak i szczegółowej reprezentacji budynku. Każda grafika powinna mieć przypisaną dowolną liczbę dodatkowych grafik.

System musi obsługiwać następujące formaty wektorowe i graficzne:

- ✓ WMF Windows Metafile
- ✓ EMF Windows Enhanced Metafile
- ✓ DXF Drawing Interchange Format (AutoCAD)
- ✓ DWG AutoCAD Format pliku
- ✓ DGN Format pliku MicroStation
- ✓ SLD Slajd (AutoCAD)

System musi obsługiwać następujące formaty grafiki bitmapowej:

- ✓ BMP Windows Bitmap
- ✓ JPG Format wymiany plików
- ✓ PNG Portable Network Graphic
- ✓ GIF Graphic Interchange Format (bez animacji)
- ✓ TIFF Tagged Image File

Animacje

Celem schematów animacji jest określenie kolorów i działania animowanych obiektów i przycisków w grafice. Każdy schemat animacji powinien mieć do 10 różnych pozycji kolorów. Oprócz koloru powinna być możliwość określenia, czy wyświetlacz ma migać okresowo przy każdym wpisie. Schematy animacji muszą być używane do definiowania różnych stanów punktów danych. Następnie powinny być one używane do wyświetlania odpowiednich symboli w grafice. Miganie powinno dotyczyć tylko grafiki wyświetlanej w tzw. Trybie stanu. Znaczenie lub wykorzystanie wybranego koloru ma zależeć od późniejszego zastosowania schematu animacji:

- ✓ Stany punktów danych - w przypadku animacji stanów punktów danych wpisy mają definiować kolor odpowiednich stanów.
- ✓ Wartości punktów danych - w przypadku animacji analogowych punktów danych (wartości) pozycje 0–4 mają definiować kolor zakresów wartości.
- ✓ Przyciski - w przypadku kolorowania przycisków pozycje 0-5 mają określać kolor przycisków.

Edytor symboli

Jednocześnie system powinien umożliwiać możliwość edycji wszystkich wykorzystywanych w systemie symboli, grafik, etc. co znacząco podniesie bezpieczeństwo systemu, jak i zapewni pełną niezależność od integratora wykonującego uruchomienie systemu.

W systemie PSIM symbole będą używane do reprezentowania różnych stanów (typów stanów) punktów danych w eksploratorze. Jeśli punkt danych wykazuje jednocześnie różne stany, na przykład uzbrojenie i alarm, oba symbole powinny być wyświetlane w eksploratorze obok siebie po nazwie. Symbole w grafice przypisane do punktu danych powinny reprezentować tylko jeden stan. Powinien być używany symbol stanu z najwyższym priorytetem animacji.

Tagi

System PSIM musi zapewnić dowolne definiowanie elementów znakujących (etykiet), które będą mogły być użyte do różnych obiektów systemowych.

Tagi będą wykorzystywane do dodatkowej klasyfikacji odpowiednich obiektów, aby móc je wybrać, np. za pomocą filtrów. Tagi powinny być dowolnie definiowane przez użytkownika, grupowane i hierarchicznie zorganizowane. Tagi będą służyć do strukturyzacji obiektów w sposób zdefiniowany przez użytkownika i grupowaniach w „konkretne” nakładające się podzbiory.

Aplikacja mobilna

Aplikacja mobilna PSIM dostępna na systemy Android i IOS powinna zapewniać w sposób przejrzysty, kompaktowy dostęp do stanów i zdarzeń systemu PSIM, w tym do przetwarzania zdarzeń i funkcji sterowania.

System powinien zapewniać wyzwalanie zdarzeń, w tym załączników (notatki / zdjęcia / filmy itp.) za pomocą smartfona i przesyłanie ich do centrum sterowania. Dodatkowo aplikacja powinna umożliwiać przesyłanie współrzędnych geograficznych wydarzenia do centrum sterowania, dzięki czemu będzie możliwa dokładna lokalizacja.

Cała komunikacja pomiędzy aplikacją mobilną a serwerem powinna być szyfrowana, co zagwarantuje najwyższy poziom bezpieczeństwa.

Wymagania minimalne aplikacji mobilnej to:

- ✓ Pełne drzewo punktów danych z wyświetlaniem stanów.
- ✓ Wykonywanie poleceń sterujących systemem.
- ✓ Wyświetlacz graficzny z animacją, przełącznikiem graficznym i kontrolą punktu danych.
- ✓ Wyświetlanie lokalizacji, w tym obsługa grafiki lokalizacyjnej. Tworzenie / odbiór / akceptacja / resetowanie / zakończenie wydarzeń.
- ✓ Informacje o nowych zdarzeniach, nawet jeśli urządzenie mobilne jest w trybie czuwania.

Obsługa zdarzeń

Jednym z kluczowych elementów pracy z systemem PSIM jest obsługa zdarzeń. Ogólnie, wiadomości powinny być tworzone przez zdarzenia zarejestrowane przez połączone systemy. Moduł interfejsu musi odbierać zdarzenie, powinien interpretować informacje, a następnie wysyłać odpowiednie informacje o zdarzeniu lub stanie do systemu PSIM, gdzie są one wyświetlane.

Lista zdarzeń

W dolnej części głównego okna systemu PSIM powinna znajdować się lista zdarzeń, prezentująca zdarzenia wpływające do systemu. Lista powinna zawierać różne, definiowalne przez filtr obszary, z bieżącymi zdarzeniami oczekującymi.

Lista zdarzeń powinna zawierać własne dwa paski narzędzi, które będą używane do obsługi zdarzeń. Każde zdarzenie ma podlegać akceptacji (przypisaniu), automatycznie bądź ręcznie, do danego operatora. Posiadając określoną funkcję, dany operator powinien móc decydować o przydzieleniu poszczególnego zadania innemu operatorowi.

Zdarzenia powinny być grupowane po poszczególnych typach w postaci dedykowanych zakładek tak, aby zapewnić operatorowi jak najwyższą ergonomię pracy, zwłaszcza w ramach dużych instalacji, gdzie spływa wiele zdarzeń z różnych obszarów dziania.

Dodatkowo do każdego typu zdarzenia oraz etapu jego realizacji powinien być przypisany czas konieczny na rozpoczęcie i realizację danego etapu. W przypadku braku działania, system powinien automatycznie eskalować zdarzenie wyżej w strukturze.

Wysokość listy zdarzeń powinna być edytowalna w dowolnym momencie, przeciągając ją myszą w ramach predefiniowanych limitów. Powinny być określone ustawienia wyświetlania, wyglądu i właściwości listy zdarzeń podczas projekcji.

Podczas definiowania systemu należy określić, które teksty i grafiki mają być wyświetlane wraz ze zdarzeniami dla każdego obiektu podczas jego projekcji (na przykład dla punktów danych: dokumenty kart indeksowych). Inną funkcją powinien być raport zdarzeń, który będzie gromadzić wszystkie informacje dotyczące zdarzeń (w tym dzienniki zdarzeń) w jednolitym dokumencie PDF.

Alarmowanie o nowych zdarzeniach

Kiedy wygenerowany zostanie komunikat o nowym zdarzeniu, to powinien on być automatycznie przypisywany do stacji roboczej i wyświetlany tam bezpośrednio, chyba że będzie tam obecnie obsługiwane inne zdarzenie o wyższym priorytecie lub będą ustanowione inne procesy systemowe. Nowe wydarzenie powinno migać na liście wydarzeń. Odebranie zdarzenia musi wyzwać również sygnał dźwiękowy na stanowisku pracy. Projektowane polecenia są wykonywane przez system automatycznie. Pierwszym krokiem w procesie obsługi po otrzymaniu zdarzenia powinna być akceptacja zdarzenia lub pobranie / pobranie (z innej stacji roboczej). Po wykonaniu tej czynności zdarzenie powinno przestać migać, alarm dźwiękowy musi się wyłączyć.

Po odebraniu przez system informacji o zakończeniu zdarzenia z urządzenia, czas zakończenia zdarzenia powinien być zapisywany na liście zdarzeń. Po wykonaniu wszystkich kroków prawidłowo i żadne dalsze działania nie będą konieczne, użytkownik powinien móc zamknąć wydarzenie. Po zamknięciu wydarzenia powinno być ono przeniesione do archiwum wydarzeń. Po przeniesieniu wydarzenia do archiwum system musi uniemożliwić wprowadzanie dalszych zmian w wydarzeniu, które znajduje

się w archiwum. Jednak w dowolnym momencie powinno umożliwić wyświetlenie wydarzenia w archiwum wydarzeń.

Ręczne wprowadzenie zdarzeń

System PSIM powinien umożliwić tworzenie zdarzeń ręcznie za pomocą modułu funkcyjnego Alarm użytkownika lub Symulacja zdarzenia, a także innych procesów wewnętrznych.

Zdarzania muszą być automatycznie wyświetlane na wybranej stacji roboczej. Dodatkowo użytkownicy powinni być powiadamiani o otrzymaniu zdarzenia za pomocą sygnału dźwiękowego.

Grupowanie zdarzeń

System PSIM powinien umożliwić grupowanie i przetwarzanie zdarzeń razem. Grupowanie powinno być wykonane ręcznie przez operatora, jak również automatycznie za pomocą poleceń skryptowych. W tym przypadku, każda grupa powinna być reprezentowana przez jedno zdarzenie nadrzędne. Domyślnie zdarzenia podrzędne nie powinny być wyświetlane na liście zdarzeń. Lista nadrzędna musi mieć szczególne znaczenie podczas pracy z grupami. Ta lista musi zawierać wszystkie wydarzenia z wybranej grupy. Przetwarzając zdarzenie nadrzędne grupy (zaakceptuj, zakończ itp.), cała grupa powinna zostać odpowiednio przetworzona. Przepływy pracy zdarzeń podrzędnych powinny być przetwarzane jako opcja. System musi umożliwić rozgrupowanie grupy w dowolnym momencie. Ręczne sterowanie grupą powinno być zrealizowane za pomocą menu kontekstowego. System powinien zapewnić możliwość dodawania i usuwania pojedynczych wydarzeń.

Za obsługę zdarzenia w danym momencie powinna odpowiadać tylko jedna stacja robocza. I tylko na aktualnie wyznaczonym stanowisku roboczym możliwe jest wypełnianie formularzy w dokumentacji tekstowej związanej z wydarzeniem. W przypadku wszystkich innych stacji roboczych - nawet jeśli mają one odpowiednie prawa do przeglądania zdarzenia - odpowiednie interaktywne elementy tekstowe muszą być chronione przed zapisem (tylko do odczytu).

Kalendarz i automatyczne generowanie zdarzeń

W systemie PSIM kalendarz musi być częścią funkcji czasu i musi służyć do informowania systemu, które dni są dniami roboczymi. Dane kalendarza będą służyć do rozróżniania dni tygodnia i dni wolnych od pracy oraz w celu wykonywania tzw. automatycznych działań.

Aby uprościć pracę użytkownika, niektóre polecenia systemowe powinny być zdefiniować tak, aby były wykonywane automatycznie, np. raz w określonym czasie lub w regularnych odstępach czasu. Operacje przełączania, takie jak uzbrojenie / rozbrojenie, powinny być wstępnie zaprogramowane lub określone raporty mogą być generowane automatycznie.

Dodatkowo, powinna być możliwość określenia, czy przed wykonaniem dowolnego zaplanowanego polecenia wymagane jest potwierdzenie użytkownika. Jeśli będzie wymagane potwierdzenie, użytkownicy powinni mieć możliwość wykonania, opóźnienia lub anulowania akcji za pomocą okna dialogowego Wykonanie.

Przepływ zadań

W ramach systemu PSIM miejsce lub sposób wyświetlania przepływu pracy musi zależeć nie tylko od samego tekstu, ale także od odpowiedniego zdarzenia, stacji roboczej, użytkownika i typu wyświetlania (na przykład układów) itp.

W interaktywnych polach przepływu pracy użytkownicy powinni móc wprowadzać informacje. Poprzez interaktywne przyciski w przepływie pracy użytkownicy powinni mieć możliwość przełączania się do innych przepływów pracy lub pobierać dodatkowe funkcje.

Przepływy pracy mogą i powinny być przetwarzane, a każdy step powinien być monitorowany i zapisywany przez system. Poszczególne zdarzenia wraz z pełną historią, służą jako dziennik i powinny być automatycznie zapisywane po zamknięciu wydarzenia i przeniesieniu do archiwum.

W ramach definiowania przepływu pracy pola wejściowe użytkownik powinien mieć możliwość zdefiniowania jako pola wymagane. Oznacza to, że użytkownik powinien wprowadzić określone informacje, zanim dane wydarzenie, etap realizacji zdarzenia, będzie mogło zostać zamknięte.

Poprzez odpowiednie elementy wejściowe (na przykład pola wyboru), poszczególne sekcje tekstu powinny być przyciemniane lub zmniejszane. Pozwala to na tworzenie i używanie dynamicznych przepływów pracy dla zdarzeń. Dzięki dynamicznemu przepływowi pracy użytkownicy powinni móc podejmować niezbędne decyzje dotyczące konkretnego zdarzenia i, w zależności od tych decyzji, zobaczyć obraz przebiegu procesu. Ponadto elementy wejściowe, jeśli będą aktywowane, będą mogły wprowadzić ustawienia wstępne lub informacje zdefiniowane przez użytkownika do dziennika systemu. Ta informacja powinna być widoczna w dzienniku zdarzeń przypisanym do zdarzenia.

Logowanie realizowanych działań w systemie

Każdy przepływ pracy posiada tzw. dziennik zdarzeń, który jest tworzony za pośrednictwem dziennika systemowego. Wszystkie wpisy w dzienniku systemowym muszą otrzymać automatycznie odpowiednie odniesienie, jeśli kontekst zdarzenia był w tym czasie aktywny. W ramach przetwarzania przepływu pracy do dziennika systemowego powinny być wprowadzane jawne wpisy dziennika zdarzeń. Zawartość dziennika systemowego musi posiadać funkcję filtracji - w szczególności w ramach wyświetlania zdarzeń, tak aby wyświetlane były tylko wpisy odpowiadające zdarzeniu - dziennik zdarzeń.

Załączniki do zdarzeń

Do każdego przepływu pracy powinno być możliwe dodawanie załączników do wydarzeń - nazywane również po prostu załącznikami - to pliki lub notatki, które powinny być dodane do wydarzenia z systemie PSIM jako załącznik. Oprócz notatek, zdjęć, raportów, obrazów stanu i sekwencji wideo, powinno być możliwe dodawanie plików zewnętrznych i zaopatrywanie ich w notatki. W celu przeglądania załączniki, w zależności od typu pliku, powinny być otwierane albo wewnętrznie w określonym obszarze wyświetlania (w przypadku obsługiwanych bezpośrednio standardowych typów plików, takich jak bitmapa i PDF), albo zewnętrznie za pośrednictwem połączonej aplikacji systemu Windows® (we wszystkich innych przypadkach).

Prioryteryzacja zdarzeń

System PSIM musi umożliwiać nadawania priorytetów, które m.in. określają, które zdarzenie jest wyświetlane jako pierwsze, jeśli w tym samym czasie zostanie odebranych więcej niż jedno zdarzenie. Im wyższa wskazana wartość, tym wyższy priorytet zdarzenia. Dodatkowo, jeśli otrzymane zostanie zdarzenie, które ma wyższy priorytet niż to, które jest aktualnie obsługiwane, program powinien natychmiast otworzyć zdarzenie o wyższym priorytecie.

Podczas konfigurowania interfejsów lub definiowania punktów danych musi być możliwość określenia priorytetów różnych stanów zdarzeń. Podczas definiowania priorytetów powinno móc posługiwać się zakresem od -1 do 999.

Ręczne uruchamianie zdarzeń

System PSIM musi zapewnić ręczne zainicjowanie alarmu dla danego punktu danych. W ten sposób również zdarzenia specjalne, takie jak powiadomienie o alarmie przez telefon, odnotowywanie działań i procesów dla systemów nieobjętych interfejsem systemowym, np. nadzór nad wyposażeniem (nadzór nad gaśnicami).

Funkcjonalność ta ma umożliwiać zintegrowane z normalnymi procesami obsługi zdarzeń, tak aby można było wykorzystać wszystkie zasoby systemowe. W tym celu powinny być ustalone punkty danych z wymaganymi tekstami i dokumentami graficznymi. Alternatywnie, alarm użytkownika powinien być utworzony dla każdego punktu danych za pomocą menu kontekstowego eksploratora.

Operacje kontrolne

System PSIM musi umożliwić definiowanie okresów (pojedynczych lub cyklicznych), w których poszczególne punkty danych lub czujniki zostaną umieszczone w określonym stanie docelowym. Na początku lub na końcu tak zdefiniowanego okresu komendy sterujące muszą zostać wysłane do poszczególnych punktów danych, w pełni automatycznie lub po potwierdzeniu. Stan punktów danych musi być wtedy monitorowany. Jeżeli po określonym czasie tolerancji pozostaną stany odbiegające, np. w

przypadku nieudanych poleceń sterujących powinno zostać to zasygnalizowane użytkownikowi.

Oprócz planowania i automatyzacji czasów kontroli, moduł operacji kontrolnych musi przejąć ich administrację i dokumentację. Konfiguracja czasów sterowania powinna być zorganizowana w taki sposób, że operacje sterujące powinny być zlecane i monitorowane tylko przez określoną grupę użytkowników, tylko po potwierdzeniu przez upoważnioną osobę.

Ponadto spontanicznymi blokadami i ponownymi włączeniami powinien zarządzać za pomocą operacji sterującej, np. w celu zapewnienia ponownego włączenia. W przypadku każdej operacji kontrolnej powinny być zapisane dodatkowe dane, takie jak temat i informacje. Informacje te powinny być dostępne do przeglądania w kontrolowanym punkcie danych i wyświetlane również w przypadku zdarzeń, które będą wyżyłowane bezpośrednio przez polecenie sterujące (np. Zablockowanie). Poza tym nie może być związku między operacjami kontrolnymi a zdarzeniami. Wymaganie reakcji oraz stany błędu podczas operacji sterowania nie mogą być sygnalizowane zdarzeniami, ale musi istnieć niezależny mechanizm monitorowania zdefiniowany przez odpowiednie uprawnienia.

Operacje kontrolne muszą być archiwizowane wraz z przechowywanymi informacjami i faktycznymi czasami wykonania. Zarządzanie pojedynczymi operacjami kontrolnymi musi być zdecentralizowane, definiowalne w systemie. Konfiguracja, modyfikacja i wykonywanie operacji sterujących w poszczególnych częściach systemu więc powinna być możliwa również niezależnie od połączenia z serwerem.

Archiwum zdarzeń

Po zakończeniu obsługi zdarzenia (zamknięciu) to zdarzenie wraz ze wszystkimi informacjami dotyczącymi przetwarzania musi być zapisywane w Archiwum zdarzeń. To, czy zapis do archiwum następuje automatycznie, musi być wykonane ręcznie, czy też zdarzenie zostanie odrzucone bez zapisywania, musi zależeć od ustawień systemu i jest to parametr aplikacji.

Wraz ze zdarzeniem odpowiednie teksty zawierające wszystkie wpisy użytkowników są zapisywane w obiektach interaktywnych. W ten sposób wpisy w polach wprowadzania, status pól wyboru itp. Muszą być zapisywane w archiwum. Ponieważ archiwizowany będzie cały tekst, zmiany w szablonach tekstowych nie mogą mieć żadnego wpływu na zarchiwizowane zdarzenia.

Archiwum musi umożliwiać pobranie zdarzenia i wyświetlać je dokładnie w taki sam sposób, w jaki były wyświetlane w momencie zapisywania do archiwum.

Szczególnym przypadkiem archiwum wydarzeń jest Historia zdarzeń. Historię zdarzeń powinna być otwarta albo za pomocą przycisku, który można umieścić na przykład na pasku narzędzi listy zdarzeń, albo za pośrednictwem menu kontekstowego punktów danych i lokalizacji w eksploratorze oraz symboli graficznych, które są połączone z punktami danych. W przypadku Historii zdarzeń, powinno być możliwe użycie predefiniowanego filtra, który powinien móc zostać skonfigurowany w ustawieniach obsługi zdarzeń.

Panel docelowy używany do wyświetlania historii zdarzeń powinien być konfigurowalny w ustawieniach zawartości.

Logi systemowe

System PSIM powinien zawierać funkcję dokumentowania procesów w sposób identyfikowalny i kompleksowy oraz powinien umożliwiać szczegółowe przeszukiwanie przechowywanych danych.

W tym celu system powinien przechowywać szeroki zakres danych w protokołach i archiwach. Pozwala to z jednej strony na dokumentację i rekonstrukcję procesów systemowych oraz obsługę ich przez użytkowników, a z drugiej na szybkie rozpoznanie i usunięcie podatności i potencjalnych źródeł błędów w systemie.

Wszystkie w pełni obsłużone zdarzenia muszą być przechowywane w archiwum wraz z różnymi informacjami dotyczącymi przetwarzania. Dostęp do archiwum powinien być dostępny się za pomocą różnych filtrów, a zdarzenia można w dowolnym momencie ponownie wyświetlić z archiwum.

Wszystkie działania użytkownika muszą być przechowywane w dzienniku systemowym, dzięki czemu będzie można je szczegółowo

odtworzyć, gdy zajdzie taka potrzeba. Dziennik interfejsu musi przechowywać wszystkie dane, które są wysyłane lub odbierane przez interfejsy do / z instalacji zewnętrznych. Typ i zakres dziennika dla każdego interfejsu zależy od używanego modułu interfejsu.

Stany punktów danych i historia zmian stanów muszą być przechowywane w oddzielnym dzienniku stanu. Dostęp do wszystkich dzienników powinien być dostępny za pomocą różnych filtrów.

System PSIM powinien umożliwić eksport archiwum zdarzeń i dzienniki jako plik CSV (zobacz Eksport i import CSV).

Ponadto informacje z archiwum i dzienników powinno móc się zestawiać w niestandardowych raportach i drukować.

Zarządzanie video w systemie PSIM

System PISM musi umożliwiać wyświetlanie obrazu video na monitorach, w tym w pełnej korelacji z występującymi zdarzeniami.

W przypadku danych wideo podstawową opcją w systemie powinien być moduł „menadżer wideo”. Dane wideo powinny być również wyświetlane w postaci grafiki lub przy użyciu zewnętrznego wyświetlacza z wykorzystaniem modułu „wyświetlanie wideo”. „Menadżer wideo” powinien służyć do sterowania modułem „wyświetlanie wideo”. „Menadżer wideo” musi obsługiwać ładowanie kamer metodą „przeciągnij i upuść” lub za pomocą ręcznych / automatycznych poleceń dotyczących punktów danych.

W systemie PSIM kamery muszą być używane jako ogólny punkt dostępu do danych wideo. Przy odbieraniu strumienia wideo, nie ma znaczenia, czy stacja robocza będzie miała połączenie bezpośrednio z kamerą, czy z centralnym serwerem wideo. W celu uzyskania dostępu do danych archiwalnych, wymagane jest przechowywanie danych wideo na dedykowanym rejestratorze lub serwerze.

Zasada działania „menadżera wideo”

„Menadżer wideo” musi umożliwiać scentralizowany dostęp do różnych systemów wideo w systemie PSIM. Oprócz wyświetlania cyfrowych filmów wideo, funkcje „menadżera wideo” muszą obejmować również sterowanie wideo, dostęp do zarchiwizowanych danych systemu wideo, a także sterowania odpowiednimi kamerami PTZ.

„Menadżer wideo” musi posiadać własny pasek narzędzi, który powinien być wyświetlany w górnej krawędzi okna. Dane wideo muszą być wyświetlane w środkowej części okna. Kliknięcie prawym przyciskiem myszy na jednym z elementów wyświetlania powinien utworzyć menu kontekstowe z dostępnymi poleceniami. Funkcje sterowania kamerami PTZ powinny się po prawej stronie, a dolna sekcja powinna zawierać elementy do sterowania archiwum wideo lub wyświetlania danych dziennika. Dane dziennika to fragment dziennika systemowego. Ponadto powinno być możliwe tworzenie zakładek za pomocą menu kontekstowych w Menedżerze filmów oraz zapisywanie lub odtwarzanie sekwencji jako klipów. Dalsze zarządzanie tymi danymi odbywa się za pośrednictwem archiwum wideo.

Archiwum nagrań video

Celem archiwum wideo jest centralne zarządzanie informacjami i danymi wideo. Oprócz zakładek, przechowywane muszą być tutaj strumienie wideo zapisane jako klipy w systemie.

Zakładki mają reprezentować logiczny widok użytkownika i tylko tutaj można zapisać odpowiednie informacje, takie jak opisy i powiązane zdarzenie.

Klipy muszą reprezentować poziom fizyczny i służą jedynie do zarządzania zapisanymi plikami wideo.

Zarówno klipy, jak i zakładki muszą mieć przypisany punkt danych kamery, a także informacje związane z czasem, przez które będą ze sobą pośrednio połączone i będą do siebie przypisane.

Na przykład w przypadku zakładki wyświetlane będą dostępne źródła (strumienie wideo i klipy), a dla klipu muszą być dostępne odpowiednie zakładki. W szczególności klipy powinny być filtrowane na podstawie informacji z powiązanych zakładek. Użytkownik musi mieć możliwość znalezienia i uporządkowania sekwencji wideo i zawartych w nich informacji za pomocą zakładek, niezależnie od miejsca ich przechowywania.

Zakładki i klipy powinny być tworzone przez „menadżer wideo”, jeśli jest to wymagane, również automatycznie za pomocą polecenia w skryptach (np. po odebraniu zdarzenia). Po utworzeniu zakładki z

sekwencją czasową należy wskazać, czy powiązana sekwencja wideo ma również zostać zapisana jako klip.

W zakresie wyświetlania wydarzeń powiązane zakładki muszą być wyraźnie wyświetlane w nowym układzie zawartości archiwum wideo. Nadal powinno być obsługiwane bezpośrednio dodawanie sekwencji wideo jako załączników do wydarzeń.

Strumieniowanie

W systemie PSIM cyfrowe strumienie wideo powinny być wyświetlane bezpośrednio za pomocą tak zwanych monitorów. Te monitory to obszary do wyświetlania wideo w module „menadżera wideo”, w grafice systemowej lub w module „wyświetlanie wideo”, którymi użytkownik powinien móc zarządzać za pośrednictwem punktów danych monitora. Punkty danych monitora nie muszą być przypisane do interfejsu zewnętrznego i powinny być zdefiniowane jako wewnętrzne punkty danych. Monitor wewnętrzny powinno móc przypisać do obszaru wyświetlania wideo za pośrednictwem menu kontekstowego.

Automatyczne wyświetlanie obrazu skorelowane ze zdarzeniami

System PSIM, poza standardową funkcjonalnością tzw. monitora alarmowego, musi umożliwić konsolidację monitorów wewnętrznych w tak zwane banki wideo.

W ramach banków wideo, kamery powinny być ładowane automatycznie w zależności od zdarzenia. Jeśli zostało zdefiniowanych kilka banków wideo, istnieją dwie opcje dotyczące kolejności przydzielania. Obie kamery są ładowane zgodnie z ostatnio wybranym zdarzeniem lub według rankingu priorytetów każdego odpowiedniego zdarzenia.

Jednostka operatorska PSIM

Wymagane parametry techniczne:

- Procesor: minimum Intel Core i3-9100; 3,6 GHz turbo boost do 4,2 Ghz; pamięć podręczna 6144 KB.
- Dysk twardy: minimum 128 GB SSD SATA III.
- Pamięć operacyjna RAM:
 - Wielkość pamięci: 4096 MB,

- Rodzaj pamięci: DDR4,
 - Ilość banków pamięci: 2,
 - Ilość wolnych banków pamięci: 2,
 - Max. wielkość pamięci: 16384 MB,
 - Taktowanie: min. 2400 MHz.
- Multimedia:
 - Karta graficzna: zintegrowana,
 - Głośniki: TAK.
- Komunikacja:
 - Karta sieciowa LAN: 10/100/1000 Mbps,
 - Karta bezprzewodowa: TAK,
 - Bluetooth: TAK.
- Napęd optyczny: DVD±RW.
- Porty wejścia/wyjścia:
 - Słuchawkowe: TAK,
 - Mikrofonowe: TAK,
 - Wejście zasilania (AC-in): TAK,
 - USB: 2x USB 3.0, 4x USB 2.0,
 - VGA: TAK,
 - HDMI: TAK,
 - Gniazdo RJ45: TAK,
 - Czytnik kart pamięci: TAK.
- System operacyjny:
 - Windows 10 Professional (64 bit).
- Moc zasilacza: 240 W.

Klawiatura + mysz.

System monitoringu wizyjnego VSS

Najważniejsze urządzenia zarządzające systemem monitoringu wizyjnego (rejestratory lub grupy rejestratorów, oprogramowanie zarządzające i integrujące rejestratory, stacje podglądowe, krosownice wizyjne, macierze dyskowe) powinny spełniać następujące wymagania techniczno- użytkowe:

- System powinien zapewniać pełną integralność z istniejącym w ZPW Pomorzany zespołem rejestratora cyfrowego. System musi zapewniać

możliwość nadawania i zarządzania uprawnieniami użytkowników zarówno z poziomu stacji operatorskich VSS w ZPW Pomorzany, Dyrekcji ZWIK oraz ZPW Miedwie. System musi umożliwiać dostęp do obrazów na żywo, do nagrań archiwalnych z poziomu każdej stacji operatorskiej do każdego z rejestratorów cyfrowych w powyższych lokalizacjach.

- Użyty sprzęt i materiały powinny być komponentami standardowymi dostępnymi w stałej ofercie danego producenta.
- Wszystkie systemy powinny być przetestowane i wdrożone w istniejących instalacjach.
- Gwarancja producenta nie powinna być krótsza niż 36 miesięcy od daty dostawy.
- Producent urządzenia lub jego reprezentant powinien udostępniać linię telefoniczną dla wsparcia technicznego, dostępną przez wszystkie dni robocze w godzinach pracy tych firm.
- Producent zagwarantować powinien minimum 8 lat wsparcia serwisowego urządzeń od momentu ich zakupu.
- System powinien pozwalać na rozszerzenie funkcjonalności poprzez uaktualnienie oprogramowania bez potrzeby zmian w strukturze sprzętowej.
- Do zapisu obrazu z kamer wykorzystany powinien być cyfrowy rejestrator sieciowy. Powinien on umożliwiać wykorzystanie zaawansowanej technologicznie kompresji typu MPEG4 i H.264 zoptymalizowanej i zaadoptowanej do wykorzystania w profesjonalnych systemach nadzoru CCTV, dostępnej dla każdego obsługiwanego kanału oraz JPEG – użytkownik powinien mieć możliwość wyboru rodzaju kompresji w zależności od zastosowanych kamer, ich funkcji w systemie itp.
- Algorytm kompresji i dekompresji (w przypadku MPEG-4 i H.264) powinien umożliwiać niezależne definiowanie parametrów pracy dla każdego kanału (wejścia) wideo, z uwzględnieniem ustawienia długości struktury GOP lub częstości występowania klatek bazowych; zagwarantuje to dopasowanie do charakterystyki obserwowanej sceny i umożliwi dokładne definiowanie parametrów przepływności strumienia danych.

- System powinien obsługiwać połączenie sieciowe z obsługą protokołu TCP/IP i prędkością połączenia 1 GBit/sekundę. W przypadku wykorzystywania kamer sieciowych, każdy z serwerów rejestrujących posiadać powinien minimum podwójną kartę Ethernetową (pierwsza dla sygnałów przychodzących z kamer, druga dla strumieni wysyłanych do stacji podglądowych). Przy zastosowaniu macierzy iSCSI rejestrator powinien być wyposażony w trzy karty sieciowe.
- Zamawiający wymaga aby zaimplementowane były minimum: 10 protokołów do sterowania kamerami obrotowymi, 300 typów kamer IP lub serwerów sieciowych, 100 typów kamer MPixelowych, a także powinny być wspierane (dla podglądu i zapisu) standardy ONVIF i RTSP.
- System powinien umożliwiać lokalny podgląd na żywo, odtwarzanie i nagrywanie wszystkich podłączonych kamer. Funkcja podglądu bez ograniczeń musi być dostępna również poprzez połączenie sieciowe z rejestratorem. Podgląd obrazów z kamer w żaden sposób nie może wpływać na prowadzoną rejestrację. Dla wybranych użytkowników istnieć musi możliwość zdefiniowania niezależnych ograniczeń co do podglądu na żywo i/lub odtwarzania pojedynczych kamer/grup kamer. Jednocześnie musi istnieć możliwość zdefiniowania maksymalnego wieku nagrań, jaki przysługuje użytkownikowi dla podglądu zarejestrowanego materiału (np. użytkownik może otworzyć wyłącznie materiał nie starszy niż 1 godzina)
- Prędkość przetwarzania obrazów z podłączonych kamer sieciowych powinna być zależna wyłącznie od możliwości i parametrów samej kamery i nie powinna być w żaden sposób ograniczona przez rejestrator.
- System powinien umożliwiać tworzenie wielopoziomowego systemu zabezpieczeń dostępu w oparciu o hasła. System powinien umożliwiając tworzenie kont pojedynczych użytkowników oraz grup użytkowników z przypisanymi uprawnieniami dostępu. Prawa dostępu powinny co najmniej umożliwić rozróżnienie grup administracyjnych (z dostępem do opcji konfiguracji systemu) oraz grup użytkowych (dostęp do poszczególnych rejestratorów i

kamer, podgląd "na żywo" oraz dostęp do archiwum, definiowanie akcji takich jak przetwarzanie i wyświetlanie stanów alarmowych, tworzenie kopii zapasowych, drukowanie, eksport sekwencji obrazów).

- System powinien udostępniać otwarte i udokumentowane interfejsy komunikacyjne. Producent systemu na żądanie powinien bezpłatnie udostępniać zestaw narzędzi programistycznych (z ang. Software Development Kit, SDK) umożliwiający stworzenie oprogramowania integrującego z innymi systemami.
- System powinien być skalowany i rozszerzalny aby umożliwić prostą rozbudowę w razie takiej potrzeby.
- System powinien wspierać podłączenie zewnętrznych macierzy dyskowych RAID (poziom 5). Możliwe powinno być też automatyczne tworzenie kopii zapasowych całości lub wybranej części materiału. System powinien zarządzać zapisanymi kopiami nagrań udostępniając co najmniej opcje: dzielenie dużych plików na części przy ich tworzeniu, szyfrowanie tworzonych plików (hasło), limitowanie pasma zajmowanego przez proces backupu, autousuwanie najstarszych nagrań po zdefiniowanym czasie lub przekroczeniu wielkości zdefiniowanej przestrzeni dyskowej.
- System umożliwiać powinien tworzenie kopii fragmentów lub całości zarejestrowanego materiału. Konfiguracja tworzenia kopii zapasowych powinna pozwolić użytkownikowi wskazywać różne katalogi dla przechowywania kopii zapasowych na nośnikach magazynujących połączonych lokalnie lub poprzez sieć, dla różnych zdarzeń dotyczących tworzenia kopii zapasowych.
- Tworzenie kopii zapasowych powinno być możliwe regularnie, we wcześniej określonych godzinach lub dniach jak również wywoływać je powinien dowolny alarm lub zdarzenie systemowe.
- Powinna istnieć możliwość rozróżniania między kopiami zapasowymi nagrań ciągłych oraz alarmów lub zdarzeń, przy dodatkowym rozróżnianiu poziomu alarmu lub zdarzenia.
- Zbiór parametrów opisujących tworzenie kopii zapasowej zależnie od przyczyn wywołujących tą kopię (opisanych w punkcie powyżej) umożliwia co najmniej zdefiniowanie docelowego katalogu, czasu

archiwizacji oraz zachowania związanego z nadpisywaniem starych plików kopii zapasowych.

- Prędkość rejestracji, rozdzielczość i jakość powinna być ustalana przez użytkownika niezależnie od parametrów strumieni do podglądu "na żywo". Konfiguracja powinna umożliwiać zmianę parametrów rejestracji „w locie” (bez konieczności zmiany parametrów kamery/kodera z aplikacji konfiguracyjnej – wcześniej predefiniowane parametry dla rejestracji) dla każdej kamery niezależnie, w różnych trybach pracy: nagrywanie ciągłe, nagrywanie zgodnie z harmonogramem czasowym oraz nagrywanie pre-alarmowe i alarmowe różne dla różnych typów zdarzeń alarmowych.
- Dostępna przestrzeń dyskowa zespołu rejestratorów powinna być zorganizowana logicznie w formie odrębnych segmentów (pierścieni, z ang. ring). Pozwoli to na prowadzenie zapisu z różnymi parametrami odnośnie czasu i priorytetu przechowywania zapisu z poszczególnych kamer i zdarzeń. System powinien udostępniać co najmniej 5 pierścieni zapisu i 5 poziomów (priorytetów) zapisu. Zapis na pierścieniach powinien odbywać się poprzez automatyczne nadpisywanie i zastępowanie najstarszych nagrań.
- System powinien umożliwiać stworzenie bazy danych na wielu dyskach twardych / macierzach dyskowych. Baza danych powinna posiadać strukturę umożliwiającą prawidłową pracę i dostęp do danych na wszystkich sprawnych zasobach dyskowych w przypadku awarii dowolnego z nich. Rozbudowa bazy danych (zwiększenie pojemności) nie prowadzi do utraty zgromadzonych zapisów.
- Dla wydłużenia czasu archiwizacji materiału video, system (w przypadku współpracy z urządzeniami o specjalizowanej kompresji zaadoptowanej do systemów CCTV) powinien umożliwiać zmianę ilości klatek już zarejestrowanego materiału – rozrzedzanie zapisu. Oznacza to, że po wcześniej zaprogramowanym przez użytkownika czasie, system automatycznie usunie zdefiniowaną przez użytkownika część zarejestrowanego materiału.
- Przykładowo: przy normalnej rejestracji prędkość zapisu wynosiła 25kl/sek. Po tygodniu należy zachować tylko 5 klatek/s (spośród

zapisanych wcześniej w ciągu każdej sekundy 25 klatek należy odpowiednio wykasować 20 klatek zarejestrowanego materiału).

- System powinien obsługiwać dynamiczną transmisję strumieniową, w celu optymalizacji obciążenia sieci, obniżenia wymagań dla dekompresji obrazu i zwiększenia wydajności wyświetlania na stacjach podglądowych. W tym celu rozdzielczość transmitowanych "na żywo" obrazów powinna automatycznie dostosowywać się do rozmiaru (rozdzielczości) okien podglądu, w których wyświetlane są obrazy z poszczególnych kamer na stacji podglądowej. Dopasowanie to zależne powinno być od typu zastosowanej kamery, jednak system przy współpracy z wybranymi kamerami umożliwiać powinien automatyczne dopasowanie minimum do rozdzielczości: QCIF, QVGA, VGA, SVGA, WXGA, 720p, 1080p, 3MPix, 5MPix.
- Użytkownik powinien mieć możliwość ustawiania takich parametrów, jak rozmiar, kolor, kolor tła oraz czcionka, przy pomocy których informacje te są wyświetlane.
- System powinien umożliwiać generowanie zdarzeń oraz tworzenie harmonogramów czasowych w oparciu o zegar astronomiczny zaprogramowany na podstawie lokalizacji geograficznej (dynamiczne obliczanie wschodów i zachodów słońca).
- Zarządzanie zdarzeniami i alarmami powinno pozwalać na efektywną adaptację reakcji systemu na stany alarmowe oraz inne zdarzenia, zgodnie z wymaganiami użytkownika. Reakcje systemu powinny uwzględniać:
 - Zdefiniowane przez użytkownika dowolnego czasu trwania sekwencji wideo przed i po wystąpieniu alarmu;
 - Parametry rejestracji (jakość i prędkość) niezależne (indywidualne) dla wszystkich kamer;
 - Automatyczne wyświetlanie obrazów alarmowych zdefiniowanych przez użytkownika (na żywo i/lub w trybie odtwarzania) na predefiniowanych stacjach roboczych;
 - Zmiana stanu jednego lub kilku styków wyjściowych przekaźników;
 - Wysyłanie informacji o alarmach lub zdarzeniach do zalogowanych użytkowników;

- Obsługa interfejsów do systemów innych producentów;
- Ustawienie jednej lub wielu kamery PTZ w zaprogramowanej pozycji;
- Rozpoczęcie tworzenia automatycznych kopii zapasowych predefiniowanych sekwencji w razie wystąpienia alarmu, bądź innego zdarzenia;
- Generowanie alarmów powinno następować co najmniej na skutek następujących zdarzeń: wewnętrzna analiza obrazu, zewnętrzne wejścia alarmowe oraz interfejsy z systemów innych producentów (szeregowe lub łącze TCP/IP).
- System udostępniać powinien harmonogramy czasowe do kontroli przetwarzanych zdarzeń oraz parametrów rejestracji. Pozwala to na całkowicie bezobsługowe działanie systemu, np. włączenie funkcji detekcji (wykrywania) ruchu w określonym przedziale czasowym, lub sprawdzanie stanu styków wejściowych w określonych przedziałach czasowych. System udostępnia co najmniej 80 definiowanych przez użytkownika przedziałów czasowych.

Cechy techniczne rejestratora cyfrowego

Parametry techniczne:

- Procesor Intel QuadCore XEON 3 GHz lub lepszy.
- Wyjścia wideo: 1x DVI-D, 2x Display Port.
- Wejścia sterujące: 16 wewnętrznych bezpotencjałowych styków wejściowych, z kontrolą sabotażu (przełączalne).
- Wyjścia przekaźnikowe: 8 wewnętrznych wyjść przekaźnikowych, 24 VDC, 1 A.
- Porty RS-232: 1x interfejs szeregowy RS-232.
- USB: 4x USB 2.0, 5x USB 3.0.
- Ethernet: 2x interfejs Ethernet 10/100/1000 Base-TX.
- Pamięć wewnętrzna: 1x 128 GB SSD na system operacyjny i bazę danych SQL. 16x 3,5 calowy dysk twardy HDD (SATA 3).
- Maksymalna baza danych: 450 TB.
- Pamięć RAM: 4x4 GB DDR4 ECC SDRAM.

Jednostka operatorska VSS

Wymagane parametry techniczne:

- Procesor: minimum Intel Core i3-9100; 3,6 GHz turbo boost do 4,2 Ghz; pamięć podręczna 6144 KB.
- Dysk twardy: minimum 128 GB SSD SATA III.
- Pamięć operacyjna RAM:
 - Wielkość pamięci: 4096 MB,
 - Rodzaj pamięci: DDR4,
 - Ilość banków pamięci: 2,
 - Ilość wolnych banków pamięci: 2,
 - Max. wielkość pamięci: 16384 MB,
 - Taktowanie: min. 2400 MHz.
- Multimedia:
 - Karta graficzna: zintegrowana,
 - Głośniki: TAK.
- Komunikacja:
 - Karta sieciowa LAN: 10/100/1000 Mbps,
 - Karta bezprzewodowa: TAK,
 - Bluetooth: TAK.
- Napęd optyczny: DVD±RW.
- Porty wejścia/wyjścia:
 - Słuchawkowe: TAK,
 - Mikrofonowe: TAK,
 - Wejście zasilania (AC-in): TAK,
 - USB: 2x USB 3.0, 4x USB 2.0,
 - VGA: TAK,
 - HDMI: TAK,
 - Gniazdo RJ45: TAK,
 - Czytnik kart pamięci: TAK.
- System operacyjny:
 - Windows 10 Professional (64 bit).
- Moc zasilacza: 240 W.
- Klawiatura + mysz.

Wielofunkcyjna klawiatura operatora

Wymagane parametry techniczne:

- 5-calowy ekran dotykowy 800x400 pikseli.
- Interfejsy: LAN/Ethernet 10/100 RJ-45 PoE.
- Zasilanie: LAN (PoE), USB.
- Liczba programowalnych klawiszy: 16.
- Liczba programowalnych klawiszy: 4.
- Joystick 3-osiowy ze zintegrowaną funkcją zoom/focus

Kamera stałopozycyjna kopułkowa – TYP 1

Parametry techniczne:

- Rozdzielczość 2 MP (1920 x 1080).
- Przetwornik CMOS 1/3" RGB z progresywnym skanowaniem.
- Czułość w kolorze: 0,16 luksa (F1,4, 1/30s), Obraz monochromatyczny: 0 luksów (przy włączonej diodzie LED IR).
- Obiektyw 3 do 10 mm (zoom optyczny 3,3x).
- Minimalny zakres widoczności przy użyciu podczerwieni: 30 m.
- Dzień/noc (filtr podczerwieni), WDR (120 dB).
- Czas migawki 1/66500 – 1 s.
- Gniazdo kart microSD / microSDHC / microSDXC.
- Obsługa kodeków H.264, MJPEG.
- Funkcje Pan/Tilt/Zoom: cyfrowy obrót, pochylenie, PTZ, położenie zaprogramowane.
- Oświetlenie IR: oświetlacz podczerwieni z diodami LED IR 850, skuteczny zasięg widzenia co najmniej 30 m.

Kamera stałopozycyjna – TYP 2

Parametry techniczne:

- Rozdzielczość 2 MP (1920 x 1080).
- Przetwornik CMOS 1/2,8" RGB z progresywnym skanowaniem.
- Czułość w kolorze: 0,05 luksów (50 IRE F1.2), Obraz monochromatyczny: 0,01 luksów (50 IRE F1.2).
- Obiektyw 2,8 do 8 (zoom optyczny 2,85x).
- Dzień/noc (filtr podczerwieni), WDR (120 dB).
- Czas migawki 1/34500 – 2 s.
- Gniazdo kart microSD / microSDHC / microSDXC.

- Obsługa kodeków H.264, H.265, MJPEG.
- Funkcje Pan/Tilt/Zoom: cyfrowy obrót, pochylenie, PTZ.

Kamera obrotowa – TYP 3

Parametry techniczne:

- Rozdzielczość 2 MP (1920 x 1080).
- Przetwornik CMOS 1/2,8" RGB z progresywnym skanowaniem.
- Czułość w kolorze: 0,15 luksów (30 IRE F1.6), Obraz monochromatyczny: 0,01 luksów (30 IRE F1.6).
- Obiektyw 4,3 do 129 (zoom optyczny 30x).
- Dzień/noc (filtr podczerwieni), WDR (120 dB).
- Czas migawki 1/60000 – 2 s.
- Gniazd kart microSD / microSDHC / microSDXC.
- Obsługa kodeków H.264, MJPEG.
- Funkcje Pan/Tilt/Zoom:
 - Pa: 360° , 0,05-700°/s,
 - Tilt: +20° do -90°; 0,05° - 500°/s,
 - Zoom: 30x optyczny, 12x cyfrowy, całkowity zoom 360x.

Kamera obrotowa z oświetlaczem IR – TYP 4

Parametry techniczne:

- Rozdzielczość 2 MP (1920 x 1080).
- Przetwornik CMOS 1/1,9" RGB z progresywnym skanowaniem.
- Czułość w kolorze: 0,07 luksów (30 IRE F1.6), Obraz monochromatyczny: 0 luksów (30 IRE F1.6).
- Obiektyw 6,7 do 201 (zoom optyczny 30x).
- Dzień/noc (filtr podczerwieni), WDR (120 dB).
- Czas migawki 1/30000 – 1/6 s.
- Gniazd kart microSD / microSDHC / microSDXC.
- Obsługa kodeków H.264, MJPEG.
- Funkcje Pan/Tilt/Zoom:
 - Pa: 360° , 0,05-150°,
 - Tilt: -90° do +90°; 0,05° - 150°/s,
 - Zoom: 30x optyczny, 12x cyfrowy, całkowity zoom 360x.

Sieć TECH-LAN

Przełącznik sieciowy – TYP 1

Parametry techniczne:

- Klasa przełącznika: zarządzalny.
- Standardy: IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.3ad 802.1d, 802.1w, 802.1s, 802.1Q, 802.1X, 802.1p, ITU-T G.8032, Y.1344 ERPS.
- Protokoły: IGMPv1 / v2, SNMP v1 / v2c / v3, TFTP, SNTP, SMTP, RMON, HTTP, HTTPS, Telnet, Syslog, opcja DHCP 66/67/82, SSH / SSL, Modbus / TCP, LLDP, IPv4 / IPv6.
- Ramki Jumbo: 9.6K.
- Konfiguracja: Konsola Web, Telnet, CLI.
- Konfiguracja kopii zapasowej: 1xPort USB 2.0.
- Konsola szeregową: 1x RS232 złącze RJ45, 115.2 Kbps, 8,N,1.
- Porty światłowodowe 2x 100/1000 SFP Slot.
- Ochrona: Linia energetyczna EFT: 2,000 VDC; ESD Ethernet: 6,000 VDC.
- Porty Gigabit: 8
- Porty SFP: 2.
- Porty PoE: 8.

Przełącznik sieciowy – TYP 2

Parametry techniczne:

- Porty Gigabit: 24.
- Porty SFP: 4.
- Porty PoE: 24.
- PoE+ (802.3at): 24.
- Budżet PoE: 384 W.
- Tablica MAC: 8K.
- Ilość VLAN: 256.
- VLAN routing: TAK.
- Dynamic VLAN: TAK.
- MLD Snooping: TAK
- Statyczne trasy: 32.
- Tablica ARP: 1024 w trybie switch, 100 w trybie router.
- IEEE: TAK.

- Zasilacz: Wewnętrzny 100-240 VAC, 50-60 Hz.
- Temperatura pracy: 0 do 50°C.

System Kontroli Dostępu

System powinien:

- System powinien mieć możliwość pełnej integracji z systemem SKD funkcjonującym obecnie w ZWIK w obiekcie ZPW Pomorzany. Nadawanie i zarządzanie uprawnieniami użytkowników musi odbywać się z poziomu istniejących jednostek operatorskich ZWIK, jak i nowo projektowanej w ZPW Miedwie.
- Nowo projektowane kontrolery KD muszą być nadzorowane przez istniejący serwer systemu KD oraz wymieniać dane z istniejącą bazą danych w ZPW Pomorzany.
- System wraz z oprogramowaniem powinien być swobodnie rozbudowywalne, zapewniając skalowalność i modułowość w przypadku etapowej realizacji.
- Oprogramowanie nie powinno posiadać limitu kart identyfikacyjnych w systemie,
- Zarządzać poszczególnymi punktami KD monitorując ich stan w trybie on-line,
- Powinno zarządzać uprawnieniami operatorów oprogramowania z możliwością podziału dostępu do poszczególnych części programów dla grup pracowników
- Powinno mieć możliwość tworzenia raportów ze wszystkich zdarzeń w systemie z możliwością ich filtrowania wg: czasu, zadanego przedziału czasu, nr kar, użytkowników, wybranego punktu kontroli dostępu, numerze strefy,
- Powinno w formie graficznej zobrazować użycie karty w formie zdjęcia użytkownika, który jest przypisany do danej karty identyfikacyjnej,
- Powinno posiadać moduł gości, który pozwoli na ewidencjonowanie ruchu gości po terenie Zakładu, Moduł powinien posiadać możliwość wpisania do bazy danych następujących danych: imię, nazwisko, nr dokumentu, PESEL, nr rejestracyjny pojazdu, firma, marka pojazdu, cel wizyty, informacje dodatkowe, nr przydzielonej karty identyfikacyjnej. W celu zautomatyzowania procesu wprowadzania gości do systemu, powinien zostać zainstalowany czytnik dowodów osobistych. Moduł do obsługi gości powinien

wyświetlić informację czy pracownik, do którego przyszedł Gość, jest obecny na zakładzie. Moduł powinien także posiadać informację o ilości Gości przebywających na Zakładzie,

- Możliwość przeglądania zarejestrowanych zdarzeń, tzw. Logi systemowe,
- System powinien umożliwić wieloprofilowość, tzn. przypisanie jednej osoby do kilku profili uprawnień,
- Zapewnić możliwość rejestracji pracy całego systemu, wywoływania pewnych akcji po wystąpieniu określonych zdarzeń, np. wyświetlenie komunikatu na ekranie programu, uruchomienia sygnału dźwiękowego w przypadku próby sforsowania drzwi, wysterowania dodatkowego modułu przekaźnikowego na komputerze klienckim,
- Posiadać możliwość filtrowania odczytów (rejestracji zdarzeń), przeglądanie ścieżek przejścia pracowników, stany osobowe stref,
- System powinien mieć możliwość graficznej ilustracji rozkładu czytników w budynku,
- Powinien sygnalizować forsowanie drzwi – sprzętowo i w oprogramowaniu, w tym możliwość współpracy z zewnętrznym systemem dozorowym,
- Odczytywać rejestracje w sposób ciągły zapewniający stały dostęp do aktualnych zdarzeń w kontrolowanym systemie. System po rozpoczęciu komunikacji okresowej ma przeprowadzać pobieranie danych zgromadzonych na urządzeniach do momentu opróżnienia lokalnych buforów danych na każdym z urządzeń. W czasie pobierania rejestracji oraz wysyłania uprawnień system cały czas powinien normalnie działać (otwierać drzwi uprawnionym osobom).
- Umożliwić kontrolę pracy systemu, nadawania uprawnień poszczególnym użytkownikom, modyfikację reguł dostępu do określonych pomieszczeń, sporządzanie raportów.
- Możliwość stałego zablokowania lub odblokowania drzwi przez operatora w dowolnym przedziale czasu.
- Funkcje rejestracji czasu pracy i kontroli dostępu,
- Aplikacja ma mieć możliwość określenia dodatkowych parametrów opisujących grupy pracowników.

Jednostka operatorska SKD

Wymagane parametry techniczne:

- Procesor: minimum Intel Core i3-9100; 3,6 GHz turbo boost do 4,2 Ghz; pamięć podręczna 6144 KB.
- Dysk twardy: minimum 128 GB SSD SATA III.
- Pamięć operacyjna RAM:
 - Wielkość pamięci: 4096 MB,
 - Rodzaj pamięci: DDR4,
 - Ilość banków pamięci: 2,
 - Ilość wolnych banków pamięci: 2,
 - Max. wielkość pamięci: 16384 MB,
 - Taktowanie: min. 2400 MHz.
- Multimedia:
 - Karta graficzna: zintegrowana,
 - Głośniki: TAK.
- Komunikacja:
 - Karta sieciowa LAN: 10/100/1000 Mbps,
 - Karta bezprzewodowa: TAK,
 - Bluetooth: TAK.
- Napęd optyczny: DVD±RW.
- Porty wejścia/wyjścia:
 - Słuchawkowe: TAK,
 - Mikrofonowe: TAK,
 - Wejście zasilania (AC-in): TAK,
 - USB: 2x USB 3.0, 4x USB 2.0,
 - VGA: TAK,
 - HDMI: TAK,
 - Gniazdo RJ45: TAK,
 - Czytnik kart pamięci: TAK.
- System operacyjny:
 - Windows 10 Professional (64 bit).
- Moc zasilacza: 240 W.
- Klawiatura + mysz.

Sterownik kontroli dostępu KD

Parametry techniczne:

Parametry techniczne:

- Kontroler musi posiadać obudowę metalową,
- Kontroler musi pracować w standardzie Aba Track II/Wiegand,
- Kontroler musi obsługiwać jednocześnie cztery czytniki kart magnetycznych lub zbliżeniowych,
- Kontroler musi obsługiwać jednocześnie dwa kompletne punkty kontroli dostępu wyposażone w czytniki, rygle, kontaktrony, przyciski otwarcia drzwi oraz sygnalizację akustyczno-optyczną,
- Kontroler ma być zasilany napięciem 12 – 14V DC,
- Maksymalny pobór prądu kontrolera nie powinien przekraczać 350 mA,
- Kontroler ma posiadać pamięć wewnętrzną RAM o wielkości minimum 2MB,
- Kontroler ma posiadać pamięć wewnętrzną Flash o wielkości minimum 8 GB,
- Kontroler powinien być wyposażony w płytę główną dwuprocesorową opartą na technologiach AVR i ARM9,
- Kontroler ma posiadać wejście Ethernet przeznaczone do instalacji oraz komunikacji z oprogramowaniem zarządzającym kontrolerem,
- Kontroler ma posiadać wejście RS-232/RS-485 przeznaczone do konfiguracji,
- Kontroler ma posiadać wejście RS-232 do podłączenia urządzeń peryferyjnych,
- Kontroler musi posiadać interfejs CAN do podłączenia modułów wejść/wyjść.

Moduł rozszerzeń kontroli dostępu KD

Parametry techniczne:

- Moduł rozszerzeń musi posiadać obudowę metalową,
- Moduł rozszerzeń musi pracować w standardzie Aba Track II/Wiegand,

- Moduł rozszerzeń musi obsługiwać jednocześnie cztery czytniki kart magnetycznych lub zbliżeniowych,
- Moduł rozszerzeń musi obsługiwać jednocześnie dwa kompletne punkty kontroli dostępu wyposażone w czytniki, rygle, kontaktrony, przyciski otwarcia drzwi oraz sygnalizację akustyczno-optyczną,
- Moduł rozszerzeń ma być zasilany napięciem 12 – 14V DC,
- Maksymalny pobór prądu modułu rozszerzeń nie powinien przekraczać 350 mA,
- Moduł rozszerzeń powinien być wyposażony w płytę główną dwuprocesorową opartą na technologiach AVR i ARM9,
- Moduł rozszerzeń ma posiadać wejście RS-232 do podłączenia urządzeń peryferyjnych.

Czytnik kart zbliżeniowych

Parametry techniczne:

- Napięcie zasilania: 9-14V DC,
- Maksymalny pobór prądu: 140 mA dla zasilania 12V,
- Zasięg odczytu: do 7 cm, w zależności od typu transpondera,
- Częstotliwość pracy: 13,56 MHz,
- Sygnalizacja: dioda LED sygnalizator akustyczny,
- Czujnik antysabotażowy: mechaniczny, styk typu NC, obciążalność max. 100mA,
- Interfejs komunikacyjny: standardowy ABA Track II,
- Stopień ochrony obudowy: IP 65 wg EN 60529,
- Temperatura pracy: od -25°C do +75°C,
- Wilgotność względna otoczenia: max 90% (dopuszczalna kondensacja),
- Waga: ok. 320g,
- Wymiary: 105 x 52 x 25 mm.

Czytnik personalizacji kart

Parametry techniczne:

- Standard interfejsu: USB 2.0, zgodność z USB 1.1, wtyk typu A/
- Prędkość transmisji: 12 Mbps.
- Częstotliwość pracy dla kart bezstykowych: 125 kHz, 13,56 MHz.

- API: PC/SC (zgodność z interfejsem i sterownikami CCID).
- Obsługiwane formaty kart bezstykowych – 13,56 MHz: iCLASS SE,
- Temperatura pracy: 0 do +70°C.
- Wilgotność: 10-90% wilgotność względa.
- Stopień ochrony: IP54.

Przycisk wyjścia awaryjnego

Parametry techniczne:

- Obciążalność styków: 2 A/230 VDC.
- Rodzaj styku: NO/NC.
- Obudowa: ABS.
- Resetowanie: dedykowany kluczyk.
- Stopień ochrony: IP24.
- Temperatura pracy: -30 do +70°C.

Zasilacz buforowy impulsowy

Parametry techniczne:

- Zasilanie: 230 VAC.
- Wyjście zasilania:
 - 3 A/13.8 VDC – dla ogólnego zastosowania,
 - 1.4 A/13.8 VDC – GRADE 1÷2,
 - 0.56 A/13.8 VDC – GRADE 3,
- Zgodność z normami: Norma alarmowa EN50131, stopień 1÷3.
- Prąd ładowania akumulatora: 0.2 A/0.6 A/1.5 A.
- Sprawność: 70%.
- Zabezpieczenia: SCP, OLP, OVP, UVP, OHP, tamper – otwarcie obudowy, tamper – oderwanie od ściany.
- Wyjścia techniczne:: EPS – awaria sieci AC, PSU – awaria zasilacza, APS – awaria akumulatora.
- Port komunikacyjny „SERIAL” z zaimplementowanym protokołem MODBUS RTU.
- Wejścia techniczne: EXT IN – awaria zewnętrzna.
- Sygnalizacja: wyświetlacz LED, BUZZER.
- Stopień szczelności: IP20.

System Włamania i Napadu

Centrala alarmowa systemu SWiN

Parametry techniczne:

- Linie na płycie głównej 16 (2EOL, 3EOL lub 4EOL).
- Ilość linii maksymalnie: 520, (2EOL, 3EOL lub 4EOL).
- Wyjścia przekaźnikowe na płycie: 1.
- Wyjścia 400 mA na płycie: 7.
- Wyjścia 10 ma na płycie: 6.
- Magistrale RS485 (max. 1 km): 4.
- Klawiatura: 32.
- Moduły DCM z interfejsem Wieganda: 32.
- Użytkownicy: 1000.
- Rejestr zdarzeń standardowy: 1500.
- Rejestr kontroli dostępu: 1000.
- Rejestr zdarzeń – A033 – 400 000.
- Połączenia logiczne: 256.
- Port RS232 56 kb/s – 1.
- Moduł Telekom PSTN – wbudowany w płytę.

Moduł rozszerzeń z zasilaczem – centrala SSWiN

Parametry techniczne:

- Napięcie wejściowe: 230 VAC, 50 Hz.
- Napięcie wyjściowe: 13,8 V – wyjścia Aux1 oraz Aux2.
- Prąd wyjściowy 2,75 A.
- Prąd wyjściowy (max) Aux1: 0,75.
- Prąd wyjściowy (max) Aux2: 0,75.
- Maksymalny prąd wyjściowy EN50131 @30 h/80% - 0,9 A – 2x17 Ah.
- Prąd ładowania akumulatora (max): 1,4 A.
- Czas ładowania akumulatora do 80%: 24h przy 2x17 Ah.
- Poziom tętnień <100 mV.
- Maks. wydajność wyjścia: 1,2 A.
- Rodzaje koncentratora: przewodowy, magistrala RS485.
- Ilość linii dozorowych (2,3,4 EOL): 8.
- Ilość wyjść programowalnych OC: 4.

- Programowalna polaryzacja wyjść OC: TAK – POZ/ENG.
- Switch adresowy: TAK – 16 pozycyjny.
- Zgodność z: EN50131-3:2009, EN50131-6:2008, PD6662:2010: GRADE 3.

Moduł rozszerzeń – centrala SSWiN

Parametry techniczne:

- Rodzaj koncentratora: przewodowy, magistrala RS485.
- Ilość linii dozorowych: 8 (2EOL, 3EOL lub 4EOL).
- Ilość wyjść 400 mA OC: 4.
- Programowalna polaryzacja wyjść OC: TAK – POZ/ENG.
- Zabezpieczenie antysabotażowe: TAK.
- Switch adresowy: TAK.
- Zgodność z: PD6662:2004/2010, EN50131-1:2006 GRADE 3, Environmental Class II.

Moduł komunikacyjny – centrala SSWiN

Parametry techniczne:

- Interfejs: TCP/IP.
- Protokoły TCP, UDP.
- Szybkość komunikacji: 10 Mb/s.
- Gniazda: RJ45.
- Heartbeat: TAK.
- Detekcja sieci: TAK.
- Enkrypcja przesyłanych danych: 128 bit.
- Konfigurowalny port IP: TAK.
- Połączenie z centralą alarmową: magistrala RS485.
- Sygnalizacja komunik. z centralą: dioda LED.
- Napięcie zasilania: 12-15 VDC.

Klawiatura LCD systemu SWiN

Parametry techniczne:

- Wyświetlacz: LDC, 2x16 znaków.
- Komunikacja: magistrala przewodowa RS485.
- Zabezpieczenie antysabotażowe: TAK.

- Napięcie zasilania: 12 VDC.
- Zgodność z EN50131: GRADE 3.

Konwerter RS232/Ethernet – moduł centrali SSWiN

Parametry techniczne:

- Liczba portów: 1.
- Prędkość 10/100 Mbps.
- Ochrona: izolacja magnetyczna 1,5 kV.
- Port szeregowy:
 - Porty szeregowy: 1x RS-232,
 - Złącze: DB9 męskie,
 - Zabezpieczenie przeciwprzepięciowe: 15 kV dla wszystkich sygnałów.
- Parametry portu szeregowego:
 - Bity danych: 5, 6, 7, 8,
 - Bity stopu: 1, 1.5, 2,
 - Parzystość: None, Even, Odd, Space, Mark,
 - Kontrola przepływu: RTS/CTS, DTR/DSR (tylko RS-232), XON/XOFF,
 - Prędkość transmisji: od 110 bps do 230.4 kbps,
 - Sygnały: TxD, RxD, RTS, CTS, DTR, DSR, DCN, GND
- Protokoły: ICMP, IP, TCP, UDP, DHCP, BOOTP, Telnet, DNS, SNMP, HTTP, SMTP.
- STEROWNIKI: Windows Real COM (system Windows), Linux Real TTY driver, Fixed TTY driver (SCO Unix, SCO OpenServer, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD, AIX 5.x, HP-UX 11i, Mac 10.3).
- Napięcie zasilania: 12-48 VDC.

Czujka PIR – TYP 1

Parametry techniczne:

- Zakres detekcji: 12 m.
- Ochrona przed czołganiem: TAK.
- Czułość: Normalna/Wysoka.
- Pole widzenia: 86°, 9 kurtyn.

- Wysokość montażu: 1.8 do 3.0 m.
- Zasilanie: 9-15 VDC.
- Wyjście przekaźnikowe alarmowe: NC.
- Wyjście przekaźnikowe sabotażowe: NC.
- Wejście sterujące: wejście Walk test.
- Pamięć alarmów: NIE.
- Przetwarzanie sygnały: V2E.
- Temperatura pracy: -10 do +55°C.
- Zgodność z EN50131: GRADE 2.

Czujka PIR – TYP 2

Parametry techniczne:

- Zakres detekcji: 12 m.
- Ochrona przed czołganiem: TAK.
- Czułość: Normalna/Wysoka.
- Pole widzenia: 86°, 9 kurtyn.
- Wysokość montażu: 1.8 do 3.0 m.
- Zasilanie: 9-15 VDC.
- Wyjście przekaźnikowe alarmowe: NC.
- Wyjście przekaźnikowe sabotażowe: NC.
- Wejście sterujące: wejście Walk test.
- Pamięć alarmów: TAK.
- Przetwarzanie sygnały: V2E.
- Temperatura pracy: -10 do +55°C.
- Zgodność z EN50131: GRADE 3.

Czujka wibracyjna

Parametry techniczne:

- Zasięg detekcji: 5m.
- Analiza sygnału: cyfrowa.
- Czułość: regulowana.
- Zabezpieczenia antysabotażowe: TAK.
- Wyjście alarmowe: NO/NC.
- Napięcie zasilania: 8-16 VDC.
- Temperatura pracy: -40 do +70°C.

- Wilgotność pracy: 0-95%.
- Zgodność z EN50131: GRADE 3.

Czujka stłuczenia szyby

Parametry techniczne:

- Zasięg detekcji: max. 9 m.
- Kąt widzenia: 165°.
- Max. Wymiary chronionej szyby: 600x600 mm.
- Ochrona szyb ze szkła: zwykłe (4 mm), laminowane P2, P4 (4 mm + 4 mm).
- Funkcja aktywnego antymaskingu: TAK.
- Zaawansowana obróbka sygnału: TAK.
- Cyfrowa kompensacja akustyki: DRC.
- Zabezpieczenia antysabotażowe: TAK.
- Stopień ochrony: IP31.
- Napięcie zasilania: 7-30 VDC.
- Wyjście alarmowe: NC, 50 mA/50 VDC.
- Wyjście tamper: NC, 50 mA/50 VDC.
- Temperatura pracy: +5 do +40°C.
- Zgodność z EN50131: GRADE 3.

Przycisk napadowy

Parametry techniczne:

- Przycisk: podwójny, ręczny.
- Obudowa: stal nierdzewna.
- Styki: NO/NC.
- Obciążalność: 3 A/125 VAC.
- Resetowanie: kluczykiem.
- Wbudowane rezystory parametryczne.
- Mikroprzełącznik alarmowy z tamperem.
- Klasa zabezpieczenia: GRADE 3.

Kontaktron bramowy

Parametry techniczne:

- Montaż: nawierzchniowy.

- Obudowa: metalowa o wysokiej odporności mechanicznej.
- Szczelina: 50 mm.
- Szczelina na drzwiach drewnianych: 36 mm.
- Szczelina na drzwiach stalowych: 30 mm.
- Wejście alarmowe: typ A, NC.
- Pętla sabotażowa: TAK.
- Dopuszczalne obciążenie: DC szczytowo 200 V/500 mA/10 VA.
- Odporność na uderzenia: 100g/11 ms/0,5 Hz.
- Stopień ochrony: IP67.
- Temperatura pracy: -40 do +70°C.
- Zgodność EN50131: GRADE 3.

Kontaktron – TYP 1

Parametry techniczne:

- Montaż: powierzchniowy.
- Funkcja przełącznika: NC.
- Dane styków kontaktu: 48 VDC/500 mA/10 VA.
- Szczelina na drzwiach drewnianych: 31 mm.
- Szczelina na drzwiach stalowych: 16 mm.
- Zabezpieczenie sabotażowe: TAK.
- Temperatura pracy: -40 do +70°C.
- Stopień ochrony: IP43.
- Zgodność EN50131: GRADE 2.

Kontaktron – TYP 2

Parametry techniczne:

- Montaż: powierzchniowy.
- Funkcja przełącznika: NC.
- Normalna operacja: 12 VDC.
- Dane styków kontaktu: 48 VDC/500 mA/10 VA.
- Szczelina na drzwiach drewnianych: 27 mm.
- Szczelina na drzwiach stalowych: 10 mm.
- Temperatura pracy: -40 do +70°C.
- Stopień ochrony: IP43.
- Zgodność EN50131: GRADE 3.

Sygnalizator optyczno-akustyczny zewnętrzny SSWiN

Parametry techniczne:

- Sygnalizacja: akustyczna i optyczna.
- Natężenia dźwięku: 115 dB.
- Źródło dźwięku: przetwornik piezoelektryczny.
- Zabezpieczenie antysabotażowe: otwarcie obudowy, oderwanie.
- Kolor i źródło światła: biały, LED.
- Zgodność z EN50131: GRADE 3.

Zespół Radarowy

Parametry techniczne:

- Sensor: MIMO z cyfrową wiązką.
- Częstotliwość: C-Band.
- Zakres detekcji: człowiek – 400 m, pojazd – 600 m, dron – 100 m.
- Szybkość skanowania: 2 scany na sekundę.
- Pokrycie w poziomie: 100°.
- Pokrycie w pionie: 30°.
- Dokładność detekcji: <1.0 m.
- Pozycja horyzontalna: 1°.
- Szybkość obiektów: 0.3 – 25 m/s.
- Możliwość integracji z kamerami obrotowymi i szybkoobrotowymi.
- Możliwość integracji z systemami VMS i PSIM – protokół ModBus TCP/IP.
- Zasilanie: 48 VDC.
- Temperatura pracy: -40 do +85°C.

Mikroprocesorowy kontroler parametrów pracy punktu dystrybucyjnego

Urządzenie powinno umożliwiać:

- Alarmowanie o przekroczeniu predefiniowanych progów temperatury i wilgotności.
- Zabezpieczenie dostępu 4 cyfrowym hasłem z możliwością przypisywania haseł jednorazowych.

- Brak wprowadzonego hasła dostępu w określonym czasie lub 3-krotne wpisanie błędnego hasła skutkuje alarmem dźwiękowym.
- Możliwość programowej konfiguracji sposobu wizualizacji i sygnalizacji dźwiękowej alarmów i awarii.
- Możliwość zdalnego rozbrojenia urządzenia.
- Zarządzanie zmianą haseł kontrolera z poziomu systemu zarządzania bezpieczeństwem.
- Automatyczne uzbrojenie urządzenia przy zamknięciu drzwi oraz po upływie zadanego czasu bezczynności.
- Szyfrowana transmisja danych (algorytm AES) wraz z autoryzacją dostępu.
- Synchronizacja z serwerem czasu.
- Funkcja zdalnej aktualizacji oprogramowania.
- Możliwość wysterowania dowolnych urządzeń wyjściowych (wentylator, grzałka).
- Alarmowanie na podstawie zmiany stanu wejść cyfrowych.
- Możliwość tworzenia zależności logicznych pomiędzy wejściami a wyjściami cyfrowymi.
- Wygaszenie ekranu na podstawie wejścia cyfrowego.
- Kontrola parametrów środowiskowych (termostat).
- Możliwość zdalnej konfiguracji parametrów sieci LAN.
- Automatyczne wyszukiwanie urządzeń w sieci LAN.
- Dedykowane oprogramowanie do konfiguracji urządzenia.
- Monitorowanie kontrolowanych parametrów, zdarzeń i alarmów, prezentacja ich na wyświetlaczu oraz przekazanie ich do zintegrowanych systemów, w tym:
 - otwarcia drzwi szafy/obudowy – obsługa czujników otwarcia,
 - wartości aktualnej temperatury i wilgotności powietrza – czujniki zintegrowane wewnętrzne i opcjonalne zewnętrzne,
 - nieuprawnionego dostępu do kontrolowanego punktu,
 - braku zasilania szafy,
 - stanu połączenia z siecią LAN,
 - stanu zdalnego połączenia z urządzeniem.
- Integracja z rejestratorem cyfrowym oraz systemem PSIM, w odpowiedniej konfiguracji powinna umożliwiać:

- wywoływanie zdefiniowanych zdarzeń na podstawie alarmu z urządzenia,
- monitorowanie parametrów urządzenia i wyświetlanie na kanale mediów,
- ustawienie presetu kamery na miejsce zdarzenia przy wywołanym alarmie,
- tworzenie wykresów z wykonanych pomiarów i wyświetlanie na kanale mediów,
- sterowanie wirtualnymi wejściami/wyjściami powiązanych z wejściami w urządzeniu,
- wyświetlenie na urządzeniu statusu kamer.
- Parametry techniczne:
 - Dodatkowo możliwość integracji z innymi systemami poprzez dedykowany szyfrowany protokół TCP/IP,
 - Wyświetlacz kolorowy min. 3,5" o rozdzielczości min. 320x240.
 - Buzzer wysokotonowy,
 - Obsługa protokołu 1-wire: dla dodatkowych, zewnętrznych czujników np. temperatury,
 - 4 wejścia cyfrowe,
 - 2 wyjścia przekaźnikowe niskonapięciowe,
 - Złącze Ethernet 10/100 Base-T ,
 - Pamięć operacyjna flash min. 2MB,
 - Pamięć EPROM min. 2048B,
 - Czujnik temperatury i wilgotności,
 - Temperatura pracy od -40 do +70 st.C,
 - Zasilanie PoE 35-60 VDC lub 5 VDC lub 12 VDC,
 - Mocowanie na szynie DIN.

System ochrony napłotowej (ochrona obwodowa)

System ochrony napłotowej powinien składać się z sensorów z trójosiowymi sensorami MEMS (sensory mikro elektro-mechaniczne), pogrupowanymi po siedem sensorów. Grupy powinny składać się z jednego sensora głównego i sześciu pomocniczych. System powinien umożliwiać instalacje 20 czujników głównych oraz 120 czujników pomocniczych rozstawionych do 5m od siebie, w ramach jednego

kontrolera. Każdy z sensorów pomocniczych powinien działać indywidualnie i generować własny sygnał wysyłany niezależnie do sensora głównego, który powinien przekazywać je do kontrolera. Kontroler systemu powinien zbierać informacje na temat stanu sensorów głównych i pomocniczych, dzięki czemu możliwe powinno być analizowanie docierających z nich informacji w odniesieniu do innych sensorów. Kontroler dzięki aproksymacji powinien wykrywać i rejestrować miejsce zdarzenia z dokładnością do jednego metra. Wszystkie grupy powinny łączyć się z kontrolerem za pomocą dwóch niezależnych magistral oraz za pomocą wydzielonej sieci bezpieczeństwa TECHLAN w tzw. redundancji połączeń. Czujniki na obu magistralach, niezależnie od przynależności do grupy czy magistrali powinny umożliwiać podział logiczny na 80 dowolnej długości stref w obrębie jednego kontrolera. Dzięki możliwości analizowania parametrów pojedynczego sensora, system powinien być adaptowany do różnych rodzajów ogrodzenia nawet, jeżeli występują one w obrębie jednego kontrolera. Możliwe powinno być dopasowanie parametrów pracy indywidualnie dla każdej strefy, a także dla każdego sensora. Wysokie prawdopodobieństwo wykrycia oraz niski poziom fałszywych alarmów powinien być wynikiem precyzyjnego pomiaru, przez każdy sensor drgań występujących w trzech płaszczyznach i ich analizy przez sterownik. Analiza odbywać się powinna przy zastosowaniu algorytmu logiki rozmytej (fuzzy logic).

System odbierając sygnały generowane przez ogrodzenie powinien potrafić rozróżnić próbę włamania od uszkodzenia lub wspinania się na ogrodzenie, co pozwolić powinno na eliminowanie fałszywych alarmów. Czujniki rozmieszczone na ogrodzeniu powinny wykrywać wibracje spowodowane przez próbę włamania i konwertować je na postać cyfrową, które powinny być następnie analizowane wstępnie przez czujnik główny dla danej grupy czujników. Informacje powinny być następnie wysyłane za pośrednictwem magistrali szeregowej RS485 do kontrolera, który między innymi powinien przechowywać wszystkie dane związane z włamaniami z odpowiadającą im datą i godziną. System powinien być wtedy w stanie przesłać dane alarmowe w czasie

rzeczywistym do innych systemów kontroli, aby np. aktywować przekaźniki do sygnalizacji alarmowej lub też umożliwić podgląd naruszanego odcinka ogrodzenia za pomocą systemu monitoringu wizyjnego. Nie dopuszcza się rozwiązań bezprzewodowych komunikacji pomiędzy elementami systemu.

Cechy systemu ochrony napłotowej:

- Wykrywanie przecięć, wspinania się na ogrodzenie, podnoszenie lub przemieszczanie segmentu ogrodzenia,
- Wykorzystanie technologii MEMS,
- Analiza sygnału przy pomocy algorytmu logiki rozmytej,
- Możliwość instalacji systemu na różnego typu ogrodzeniach w obrębie jednego kontrolera,
- Natywny adres IP,
- Redundancja przesyłu informacji do kontrolera w wyniku przerwania linii magistrali,
- Detekcja położenia sensora precyzyjna lokalizacja intruza,
- Temperatura pracy min. z zakresu od -40 do 70°C, wilgotność min. z zakresu od 0-100%.

Elementy systemu ochrony obwodowej należy zwizualizować na planach w systemie nadrzędnym PSIM – wykorzystując oprogramowanie zarządzające ochroną napłotową oraz dedykowane interfejsy programowo-sprzętowe systemu PSIM.

Czujka dopplerowska (ochrony obwodowa)

- Zasięg min. 12 lub 24m w zależności od konfiguracji.
- Wykorzystanie efektu Dopplera z modulacją dwóch częstotliwości.
- Min. 4 kanały modulacji.
- Zapas mocy dla kompensacji warunków propagacji min. ≥ 16 dB.
- Cyfrowa analiza sygnału przy użyciu algorytmu "FUZZY LOGIC".
- Dynamiczny cyfrowy antymasking.
- Liniowa polaryzacja wiązki mikrofalowej.
- Funkcja SRTD (Short Range Target Discrimination) tj. odróżnienie ruchu blisko czujnika spowodowany przez małe zwierzęta, ptaki.

- Funkcja LRTD (Long Range Target Discrimination) tj. niewrażliwość na zbyt odległe obiekty.
- Prędkość wykrywania obiektu min. z zakresu od 30 mm/2 do 15 m/s.
- Możliwość komunikacji przez sieć IP i zasilania w technologii PoE.
- Dedykowane oprogramowanie do regulacji i serwisowania urządzeń.
- Obudowa wykonana z poliwęglanu o wysokiej wytrzymałości.

15. Uwagi końcowe

Wszystkie prace budowlane prowadzić zgodnie:

- z zasadami sztuki budowlanej
- z warunkami technicznymi wykonania i odbioru robót budowlano – montażowych
- z zachowaniem przepisów BHP i p.poż.
- zgodnie z przywołanymi Polskimi Normami
- pod nadzorem osób uprawnionych.

16. Załączniki

- Z01 – Analiza ryzyka
- Z02 – Zestawienie kanalizacji na terenie ZPW Miedwie
- Z03 – Zestawienie kanalizacji na terenie PW Żelewo
- Z04 – Zestawienie studni kablowych
- Z05 – Zestawienie konstrukcji wsporczych
- Z06 – Lista kablowa połączeń elektrycznych – zasilających 230, 400VAC
- Z06 – Lista kablowa magistral SSWiN
- Z08 – Lista kablowa połączeń światłowodowych
- Z09 – Bilans bazy danych rejestratora cyfrowego
- Z10.1 – Bilans prądowy zasilacza SKD dla jednego przejścia dwustronnie kontrolowanego
- Z10.2 – Bilans prądowy zasilacza SKD dla dwóch przejść dwustronnie kontrolowanych
- Z11 – Bilans prądowy SSWIN – centrala
- Z12.1 – Bilans prądowy SSWIN – zasilacz (grade 2)
- Z12.2 – Bilans prądowy SSWIN – zasilacz (grade 3)
- Z13.1 – Bilans mocy GPD
- Z13.2 – Bilans mocy PPD02
- Z13.3 – Bilans mocy PPD03
- Z13.4 – Bilans mocy PPD04
- Z13.5 – Bilans mocy PPD05
- Z13.6 – Bilans mocy PPD06
- Z13.7 – Bilans mocy PPD07
- Z13.8 – Bilans mocy PPD08
- Z13.9 – Bilans mocy PPD09
- Z13.10 – Bilans mocy PPD10
- Z13.11 – Bilans mocy PPD11
- Z13.12 – Bilans mocy PPD12
- Z13.13 – Bilans mocy PPD13
- Z13.14 – Bilans mocy PPD14
- Z13.15 – Bilans mocy PPD15
- Z14 – Dobór kabli zasilających i zabezpieczeń elektrycznych
- Z15 – Zestawienie urządzeń SSWIN
- Z16 – Zestawienie punktów kamerowych

17. Rysunki

- R01 – Schemat ideowy integracja SZT w ZWIK Szczecin Sp. z o.o.
- R02 – Schemat blokowy połączeń SZT
- R03 – Schemat blokowy SSWiN
- R04 – Schemat blokowy SKD
- R05 – Schemat blokowy systemu ochrony napłotowej
- R06 – Zewn. instal. elektr. i teletechn. - kanalizacja na terenie ZPW Miedwie – arkusz A
- R06 – Zewn. instal. elektr. i teletechn. - kanalizacja na terenie ZPW Miedwie – arkusz B
- R07 – Przebieg ogrodzenia i pasów buforowych na terenie ZPW Miedwie – arkusz A
- R07 – Przebieg ogrodzenia i pasów buforowych na terenie ZPW Miedwie – arkusz B
- R08 – System ochrony napłotowej na terenie ZPW Miedwie – arkusz A
- R08 – System ochrony napłotowej na terenie ZPW Miedwie – arkusz B
- R09 – System monitoringu wizyjnego na terenie ZPW Miedwie – arkusz A
- R09 – System monitoringu wizyjnego na terenie ZPW Miedwie – arkusz B
- R10 – Zewnętrzne instalacje elektryczne – kable zasilające na terenie ZPW Miedwie – arkusz A
- R10 – Zewnętrzne instalacje elektryczne – kable zasilające na terenie ZPW Miedwie – arkusz B
- R11 – Zewn. instalacje teletechniczne – kable światłowodowe na terenie ZPW Miedwie – arkusz A
- R11 – Zewn. instalacje teletechniczne – kable światłowodowe na terenie ZPW Miedwie – arkusz B
- R12 – Drzewa i krzewy do wycinki na terenie ZPW Miedwie
- R13 – Zewn. instal. elektr. i teletechn. - kanalizacja na terenie PW Żelewo
- R14 – Przebieg ogrodzenia i pasów buforowych na terenie PW Żelewo
- R15 – System ochrony napłotowej na terenie PW Żelewo
- R16 – System monitoringu wizyjnego na terenie PW Żelewo
- R17 – Zewnętrzne instalacje elektryczne – kable zasilające na terenie PW Żelewo

- R18 – Zewn. instalacje teletechniczne – kable światłowodowe na terenie PW Żelewo
- R19 – Drzewa i krzewy do wycinki na terenie PW Żelewo
- R20.1 – Rozmieszczenie urządzeń SZT – Biurowiec p. Piwnica
- R20.2 – Rozmieszczenie urządzeń SZT – Biurowiec p. Parter
- R20.3 – Rozmieszczenie urządzeń SZT – Biurowiec p. I piętro
- R21.1 – Rozmieszczenie urządzeń SZT – Budynek Filtrów Pospiesznych p. Piwnica
- R21.2 – Rozmieszczenie urządzeń SZT – Budynek Filtrów Pospiesznych p. Parter
- R21.3 – Rozmieszczenie urządzeń SZT – Budynek Filtrów Pospiesznych p. I piętro
- R22.1 – Rozmieszczenie urządzeń SZT – Budynek Filtrów Węglowych p. przyziemienie 1
- R22.2 – Rozmieszczenie urządzeń SZT – Budynek Filtrów Węglowych p. przyziemienie 2
- R23 – Rozmieszczenie urządzeń SZT – Chlorownia
- R24.1 – Rozmieszczenie urządzeń SZT - Budynek koagulacji p. parter
- R24.2 – Rozmieszczenie urządzeń SZT - Budynek koagulacji p. I piętro
- R25 – Rozmieszczenie urządzeń SZT - Komora Zasuw p. -43,41
- R26 – Rozmieszczenie urządzeń SZT – Portiernia
- R27 – Rozmieszczenie urządzeń SZT – Pompownia Żelewo p. parter
- R28 – Widok i schemat elektryczny rozdzielnic napięcia RN WE
- R29 – Widok i schemat elektryczny rozdzielnic napięcia RN WM
- R30 – Widok i schemat elektryczny rozdzielnic napięcia RN P1
- R31 – Widok, schemat elektryczny i logiczny głównego punktu dystryb. GPD
- R32 – Widok, schemat elektryczny i logiczny pośredniego punktu dystryb. PPD02
- R33 – Widok, schemat elektryczny i logiczny pośredniego punktu dystryb. PPD03
- R34 – Widok, schemat elektryczny i logiczny pośredniego punktu dystryb. PPD04
- R35 – Widok, schemat elektryczny i logiczny pośredniego punktu dystryb. PPD05

- R36 – Widok, schemat elektryczny i logiczny pośredniego punktu dystryb. PPD06
- R37 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD07
- R38 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD08
- R39 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD09
- R40 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD10
- R41 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD11
- R42 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD12
- R43 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD13
- R44 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD14
- R45 – Widok, schematy elektryczny i logiczny pośredniego punktu dystryb. PPD15
- R46 – Szczegóły techniczny ogrodzenia – panel ogrodzeniowy
- R47 – Szczegóły techniczny ogrodzenia – bramy i furtki
- R48 – Szczegóły techniczny fundamentów i podmurówki ogrodzenia