**Spis treści:**

[1 Podstawy opracowania 3](#_Toc322089730)

[2 Wstęp 3](#_Toc322089731)

[2.1 Przedmiot i zakres opracowania 3](#_Toc322089732)

[3 Założenia projektu systemu integracji 3](#_Toc322089733)

[3.1 Wstęp. 3](#_Toc322089734)

[3.2 Zalety wynikające z wdrożenia systemu zintegrowanego 4](#_Toc322089735)

[3.3 Definicje 5](#_Toc322089736)

[3.4 Struktura istniejącego systemu 5](#_Toc322089737)

[4 Opis systemu integrującego 8](#_Toc322089738)

[4.1 Wstęp 8](#_Toc322089739)

[4.2 Charakterystyka poszczególnych modułów oprogramowania Centrów Nadzoru. 9](#_Toc322089740)

[4.2.1 Continuum 9](#_Toc322089741)

[4.2.1 Integral DigitalSENTRY 10](#_Toc322089742)

[5 Integracja podsystemów bezpieczeństwa w ramach Lokalnego Centrum Nadzoru 12](#_Toc322089743)

[5.1 Opis funkcjonalny systemu. 12](#_Toc322089744)

[5.2 Oprogramowanie systemu. 13](#_Toc322089745)

[6 Zestawienie urządzeń i oprogramowania 17](#_Toc322089746)

[Specyfikacja dostaw oprogramowania. 17](#_Toc322089747)

[7 Spis Rysunków 17](#_Toc322089748)

1. Podstawy opracowania
2. Projekt zagospodarowania terenu II i III etapu budowy drogowego przejścia granicznego w Gołdapi,
3. Projekty branżowe 2002,
4. Podkład geodezyjny terenu inwestycji (2001),
5. Wytyczne programowe Urzędu Celnego.
6. Wytyczne i uzgodnienia z użytkownikami drogowego przejścia granicznego w Gołdapi, Służbą Celną, Strażą Graniczną i administracją.
7. Karty katalogowe urządzeń
8. Wstęp
	1. Przedmiot i zakres opracowania

 Przedmiotem opracowania jest projekt Systemu Integrującego dla DPG Gołdap.

W zakres opracowania wchodzi:

1. Opis struktury funkcjonalnej systemu (realizowane zadania)
2. Opis struktury informatycznej systemu,
3. Opisy funkcji oprogramowania systemu
4. Schemat ideowy systemu
5. Plan rozmieszczenia urządzeń zewnętrznych systemu
6. Założenia projektu systemu integracji
	1. Wstęp.

 Celem budowy zintegrowanego ogólnopolskiego systemu bezpieczeństwa dla obiektów administracji celnej jest zwiększenie poziomu bezpieczeństwa podległych obiektów i pracowników służb celnych.

W trakcie przygotowywania projektu systemu posługiwano się zasadą, że wszystkie systemy wchodzące w skład będą standardowo wyposażone w możliwość komunikacji. Pozwoli to na wymianę informacji pomiędzy specjalistycznymi urządzeniami i systemami oraz współpracę w ramach wspólnego dla nich wszystkich systemu zarządzającego. Tego rodzaju rozwiązanie oprócz integracji, a zatem dowolności w automatyzacji współpracy poszczególnych systemów oferuje cały szereg zalet.

Przede wszystkim użytkownik postrzega wszystkie systemy specjalistyczne przez pryzmat jednego uniwersalnego interfejsu.

Połączenie pomiędzy poszczególnymi systemami realizowane jest za pomocą magistrali (sieci) komunikacyjnej oraz wspólnego protokołu transmisji zapewniającego pełną wymienialność informacji pomiędzy różnymi systemami (np. kontrola dostępu, sygnalizacja włamania i napadu i telewizja dozorowa). Centralny system zarządzania i nadzoru przez łącza WAN stanowi uniwersalny interfejs do obsługi wszystkich przedmiotowych instalacji w innych obiektach objętych systemem zabezpieczeń. Jest to podstawowe narzędzie pracy wszystkich osób bezpośrednio odpowiedzialnych za poprawne funkcjonowanie sytemu.

Poza tym system integrujący realizuje cały szereg innych zadań takich jak:

* transmisja, przetwarzanie i archiwizacja danych,
* graficzne przedstawienie różnych instalacji,
* sygnalizacja i obsługa sytuacji alarmowych.

Przy wykorzystaniu protokołu TCP/IP i sieci można teraz monitorować i zarządzać obiektami poprzez łącza WAN. Używając standardowego oprogramowania z poziomu centrów nadzoru można uzyskać dostęp do instalacji w czasie rzeczywistym, generując raporty, analizując alarmy i dane o funkcjonowaniu systemu. System haseł i zabezpieczenia systemowe przy korzystaniu z protokołu TCP/IP gwarantują, że tylko osoby uprawnione, znające hasło będą miały dostęp do danej instalacji.

* 1. Zalety wynikające z wdrożenia systemu zintegrowanego

Zalety wynikające z wdrożenia systemu zintegrowanego:

• W pełni wielozadaniowe środowisko pozwalające operatorom na jednoczesne zarządzanie wieloma instalacjami.

• Możliwe globalne sterowanie całym systemem.

• Przejrzyste przedstawienie danych z całej instalacji na ekranach stacji roboczej.

• Czytelna prezentacja informacji w postaci kolorowej grafiki ekranowej.

• Jeden interfejs graficzny dla wszystkich aplikacji: raporty, alarmy, grafika, personalizacja kart.

• Wbudowana biblioteka animacji sterowniczych oraz zestaw narzędzi do tworzenia rysunków dla samodzielnego tworzenia własnych paneli sterowniczych.

• Programowalne dla użytkownika zarządzanie alarmami.

• Alarmy w postaci dźwięku i wizji tworzą efektywny system realizacji powiadamiania.

• Szereg możliwości tworzenia własnych harmonogramów czasowych stosownie do potrzeb konkretnej instalacji.

• Obiektowy system zarządzania systematyzuje dane i upraszcza konfigurowanie systemu.

• Integracja w czasie rzeczywistym systemów zapewniająca bieżący monitoring obszarów zabezpieczanych.

• Szereg wydajnych narzędzi dla komunikacji zdalnej.

• Komunikacja po Ethernet(TCP/IP).

• Możliwość rezygnacji ze służb ochrony 24h w tych obiektach gdzie ona ma miejsce.

• Niższe koszty związane z nadzorem nad obiektami. Jedna osoba pełni nadzór nad wszystkimi obiektami równocześnie, zamiast kilkunastu osób.

• Zdecydowane zmniejszenie ryzyka związanego ze spóźnioną reakcją na zaistniałą sytuację alarmową.

• Zachowanie wszystkich spraw związanych z bezpieczeństwem obiektów wewnątrz jednej instytucji.

• Jedna stacja personalizacji kart systemu kontroli dostępu, w miejsce kilku lokalnych.

• Możliwość pełnej archiwizacji danych.

* 1. Definicje

**OPC** = **OLE** for **P**rocess **C**ontrol; zbiór obiektów do sterowania procesem

OPC to standard stworzony przez [www.opcfoundation.org](http://www.opcfoundation.org) i uznany przez światowych producentów sterowników przemysłowych i oprogramowania. Zawiera definicje interfejsów DCOM pomiędzy aplikacjami Windows i sterownikami przemysłowymi.

**OLE** = Object Linking and Embedding; łączenie i osadzanie obiektów

Technika łączenia obiektów lub aplikacji stosowana w systemach operacyjnych Microsoft Windows. Łączenie odbywa się za pomocą osadzania, na przykład arkusza kalkulacyjnego w edytorze tekstów. Dokonywane w późniejszym czasie zmiany w arkuszy mogą pojawiać się również w dokumencie edytora.

**DCOM = D**istributed **C**omponent **O**bject **M**odel; DCOM jest podstawą do tworzenia środowiska rozproszonego przetwarzania danych. W oparciu o interfejs DCOM komponenty programowe zawarte w aplikacjach klienckich mogą korzystać z funkcji udostępnianych przez komponenty znajdujące się na innych komputerach w sieci lokalnej lub w Internecie. Do transmisji danych między komponentami wykorzystywane są wówczas protokoły TCP/IP oraz HTTP.

* 1. Struktura istniejącego systemu

 W obiektach administracji celnej istnieje i jest obecnie wykorzystywany System Integrujący.

Systemy elektronicznych zabezpieczeń projektowane na drogowym przejściu granicznym w Gołdapi zostaną włączone do systemu istniejącego. Poniżej została przedstawiona obecna struktura systemu i jego krótka charakterystyka.

System integrujący składa się z sieci Centrów Nadzoru i łączy WAN pomiędzy tymi centrami.

W skład struktury Centrum Nadzoru wchodzą następujące centra:

* **Lokalne Centra Nadzoru** (**LCN**) w obiektach Administracji Celnej takich jak: Drogowe Przejścia Graniczne, Kolejowe Przejścia Graniczne;
* **Regionalne Centra Nadzoru** (**RCN**) zlokalizowane w następujących Izbach Celnych (IC):

**- IC Olsztyn,**

**- IC Białystok,**

**- IC Biała Podlaska ,**

**- IC Przemyśl;**

* **Krajowe Centrum Monitoringu** (**KCM**)

Struktura Systemu

.....

.....

Lokalne Centra Nadzoru LCN

Lokalne Centra Nadzoru LCN

Regionalne Centrum

Nadzoru RCN

Regionalne Centrum

Nadzoru RCN

Krajowe Centrum Monitoringu KCM

**Lokalne Centra Nadzoru** (**LCN**) w obiektach granicznych.

Każdy z obiektów Administracji Celnej w którym znajduje się **Lokalne Centrum Nadzoru** (**LCN**) został wyposażony w System Bezpieczeństwa (SB) w skład którego wchodzą w zależności od lokalizacji następujące podsystemy:

* System Kontroli Dostępu - **SKD**;
* System Sygnalizacji Włamania i Napadu- **SSWiN**;
* System Wykrywania Pożaru – **SWP**;
* System Cyfrowej Telewizji Dozorowej – **SCTD**.

Drogowe Przejścia Graniczne będą ponadto wyposażone w System Sterowania ruchem SOC-T - dla samochodów ciężarowych i SOC-O – dla samochodów osobowych.

W obiektach wyposażonych w obydwa systemy (tzn. SB, SKR) używany jest wspólny serwer stanowiący system zintegrowany umożliwiający zarządzanie nim z jednego miejsca (np. ze stacji roboczej administratora).

Lokalne Centra Nadzoru w obiektach Administracji Celnej dzielą się na dwa rodzaje:

* LCN dla drogowych przejść granicznych (systemy samodzielne).

Centra te charakteryzują się pracą całodobową zatem muszą być wyposażone w stacje do zarządzania całą infrastrukturą systemu bezpieczeństwa.

* LCN dla kolejowych przejść granicznych (zarządzane z poziomu RCN).

Centra te charakteryzują się pracą jedno lub dwuzmianową zatem muszą być wyposażone w stację roboczą do rejestracji i transmisji danych do RCN oraz zarządzania infrastrukturą systemu bezpieczeństwa w trakcie pracy zmiany. Po zakończeniu pracy przejścia, nadzór i zarządzanie prowadzone jest z poziomu RCN.

Na granicznych przejściach kolejowych znajdują się systemy bezpieczeństwa zintegrowane w kontrolerze sieciowym CX i Stacji Roboczej Continuum, natomiast serwer jest umiejscowiony w Izbie Celnej w RCN wraz ze stacją administratora. Serwer RCN w Izbie Celnej jest wspólny dla wszystkich tego typu obiektów podległych danej Izbie Celnej.

Systemy bezpieczeństwa i kontroli ruchu posiadają własne, wydzielone bazy danych. Baza danych Systemu Kontroli Dostępu znajduje się w serwerowni Izby Celnej na wydzielonym komputerze. Jest ona wykorzystywana do przechowywania ustawień konfiguracyjnych systemu kontroli dostępu (karty, drzwi, urządzenia). Stacje robocze *Continuum* wykorzystują te informacje do zaprogramowania sterowników CX. Przeprogramowanie potrzebne jest tylko w awaryjnych sytuacjach, kiedy z przyczyn losowych kontrolery utracą ustawienia. Może mieć to miejsce w przypadku rozładowania się akumulatorów buforowych przy dłuższym (kilkugodzinnym) braku zasilania sieciowego. Zmiany w konfiguracji kontroli dostępu można wykonywać bez komunikacji ze sterownikiem, ale wymagane jest późniejsze przeprogramowanie sterowników w celu aktualizacji ustawień.

Baza danych Systemu Kontroli Ruchu znajduje się lokalnie na drogowym przejściu granicznym. Z tą bazą komunikują się wszystkie stacje robocze *SOC-T, (TCS).* Przechowuje ona informacje dotyczące odpraw celnych oraz ustawienia konfiguracyjne systemu. Na komputerze z bazą danych zainstalowane jest oprogramowanie OPC Server, będące interfejsem komunikacyjnym pomiędzy systemem SKR i sterownikami CX. Wykorzystuje się je do sterowania z poziomu aplikacji urządzeniami sygnalizacyjnymi (światła drogowe) i sterującymi ruchem (szlaban) na rogatkach wjazdowych oraz wyjazdowych z przejścia.

W systemie można wydzielić komunikację pomiędzy następującymi urządzeniami (patrz rysunek):

1. stacją roboczą SOC-O (*SWOC)* i serwerem bazy danych SOC-O (SWOC); informacje konfiguracyjne systemu SKR oraz dane dotyczące odpraw celnych,
2. OPC serwerem i sterownikiem CX; sterowanie wyjściami oraz pobieranie informacji o stanie wejść cyfrowych,
3. lokalną stacją roboczą i sterownikiem CX; aktualizacja konfiguracji Systemu Kontroli Dostępu,
4. zdalną stacją roboczą i sterownikiem CX; aktualizacja konfiguracji Systemu Kontroli Dostępu,
5. lokalną stacją roboczą i serwerem bazy danych systemu *Continuum*; aktualizacja konfiguracji Systemu Kontroli Dostępu,
6. zdalną stacją roboczą i serwerem bazy danych systemu *Continuum*; aktualizacja konfiguracji Systemu Kontroli Dostępu.

W przypadku awarii łącza WAN należy liczyć się z zerwaniem komunikacji [**4**] i [**5**]. Spowoduje to brak możliwości przeprogramowania kontrolera CX w przypadku ewentualnej utraty zasilania. Zmiany do konfiguracji można wprowadzać ze stacji zdalnej, ale zaaplikowanie zmian jest możliwe dopiero po przywróceniu komunikacji po sieci WAN.

CX

Serwer MSSQL dla *Continuum*

Stacja robocza

*Continuum*

Serwer bazy danych SOC-O (*SWOC)*

+ OPC Serwer

ruter

ruter

WAN

LAN

LAN

Stacja robocza

*Continuum*

Stacja robocza

*SOC-O (SWOC)*

[**1**]

[**2**]

[**3**]

[**4**]

[**5**]

Izba Celna

Drogowe przejście graniczne

[**6**]

1. Opis systemu integrującego
	1. Wstęp

Oprogramowanie Lokalnego Centrum Nadzoru

* Lokalne Centrum Nadzoru na DPG Gołdapi wyposażone zostanie w specjalistyczne oprogramowanie do planowania awaryjnego i odtwarzania zasobów wykonanego na bazie narzędzi oprogramowania ***Continuum*** firmy **Andover Controls**;
* zastosowane narzędzia programowe umożliwiają pracę w sieci i obsługę z wytypowanych przez Inwestora zdalnych stanowisk roboczych;
* oprogramowanie wyposażone jest w mechanizmy umożliwiające korzystanie ze wspólnej bazy danych, przy zachowaniu istniejącego już środowiska pracy.

**W zakresie dostaw Wykonawcy znajdują się następujące elementy :**

* oprogramowanie systemu integrującego zgodne z wymaganiami systemu CAIFS;
* oprogramowanie stanowiska pracy awaryjnej;
* elementy zabezpieczenia transmisji informacji.
	1. Charakterystyka poszczególnych modułów oprogramowania Centrów Nadzoru.

Continuum

 Oprogramowanie stacji roboczej Continuum jest kolorowym graficznym interfejsem użytkownika, kompatybilnym ze standardem BACnet i opartym na systemie operacyjnym Windows. Oprogramowanie to zapewnia wysoce wydajne narzędzia do programowania, sterowania i monitorowania systemu inteligentnego budynku Continuum poprzez szybką sieć Ethernet .

Stacja robocza Continuum jest centralnym punktem zarządzania budynkiem. Z jednej stacji roboczej Continuum można centralnie zarządzać jednolitym systemem oraz olbrzymią ilością informacji generowaną przez budynek każdego dnia. Jest to bardzo proste. Continuum prezentuje informacje operatorowi używając graficznych stron „menu” oraz paneli graficznych wykorzystujących elementy animacyjne do prezentowania w formie graficznej dynamicznych stanów pracy urządzeń w budynku.

Możliwe jest: wyświetlanie i potwierdzanie alarmów, kontrola ruchu personelu, otwieranie i zamykanie drzwi, zmiana nastaw, sterowanie oświetleniem i innymi urządzeniami, przeglądanie i drukowanie raportów, zmiana harmonogramów czasowych, wyświetlanie zarejestrowanych danych i wykresów, przeglądanie logów wydarzeń - wszystko bez dotykania klawiatury.



Rysunek 1 Cyberstation - stacja robocza CONTINUUM

Stacja robocza Continuum przechowuje dane o całym budynku - alarmy, zużycie energii, stan pracy urządzeń w budynku, rekordy personelu, logi systemowe - w jednej bazie danych Microsoft SQL. SQL jest standardem dla baz danych, co oznacza, że Continuum może wymieniać dane z innymi systemami i sieciami informatycznymi.

Wszystkie informacje są zabezpieczone przed nieautoryzowanym dostępem poprzez złożony, lecz prosty w obsłudze system kluczy konfigurowanych przez użytkownika. Indywidualne klucze zabezpieczają różne części oprogramowania - klasy obiektów, czynności operatora i dostęp do poszczególnych obiektów w systemie. Administrator przypisuje każdemu operatorowi „wirtualny łańcuch kluczy” lub przywilej dostępu do różnych części oprogramowania.

Stacja robocza Continuum składa się z szeregu programów współdziałających ze sobą jednocześnie. Technika OLE zapewnia natychmiastowy dostęp do takich programów jak np.: Microsoft Word® lub Excel® , Netscape Navigator® i Visio® . Dodatkowo liczne edytory aplikacji Continuum i narzędzia wspomagające zapewniają, że uruchomienie systemu jest szybkie i proste.

Oprogramowanie Continuum dla systemu jedno i wielostanowiskowego potrafi sprostać wszystkim wymaganiom konfiguracyjnym dla sieci LAN i WAN. Dostęp do sieci Ethernet może posiadać jednocześnie do 4 milionów węzłów.

W wypadku automatyki budynku niezbędna jest elastyczność w celu dostosowania procedur sterowania do urządzeń zainstalowanych w budynku - a nie dopasowywanie budynku do z góry zadanych możliwości sterowniczych systemu automatyki. Continuum zostało zaprojektowane tak, aby zapewnić elastyczność i różnorodność sekwencji sterowniczych poprzez zastosowanie języka programowania Plain English Andover Controls.



Rysunek 2 Zintegrowane środowisko programistyczne Plain English

Plain English pozwala użytkownikowi Continuum - nawet początkującemu - na zaprogramowanie systemu przez niego samego. Możliwe jest tworzenie własnych procedur programowych, aby zbudować własny, unikalny standard sterowania systemami HVAC, ochroną budynku, alarmami, harmonogramami czasowymi itp.

### Integral DigitalSENTRY

Systemy DS. możemy administrować lokalnie jak i zdalnie za pomocą kilku narzędzi, które udostępnia firma Integral. Za pomocą tego oprogramowania DigitalSentry można połączyć się do wielu systemów DS jednocześnie.

DigitalSENTRY 3.0 posiada nowy kreator konfiguracji, który krok po kroku prowadzi użytkownika poprzez poszczególne etapy. Istnieje możliwość tworzenia bibliotek zawierających pełną konfigurację systemu – gotowe do użycia w każdej chwili. Kreator DSAdmin Wizard jest uzupełnieniem standardowej wersji DSAdmin do konfiguracji systemu.

Oprogramowanie to również ma możliwość łączenia się z wieloma systemami jednocześnie usprawniając konfiguracje dużych systemów CCTV zbudowanych z kilku DS. Enterprise lub DS XPress. Pozwala dodawać oraz konfigurować jednostki VAU, oraz kamery, tworzyć grupy kamer oraz strefy, ustalać harmonogram nagrywania. Dla każdej kamery z osobna można zdefiniować jakość nagrywanego obrazu dostępne są: niska, średnia, wysoka i bardzo wysoka jakość, oraz szybkość nagrywania.

Klient ma również możliwość takiego skonfigurowania urządzenia aby w chwili alarmu wysłał wiadomość e – mail wraz z dołączonym clipem video lub zdjęciem sytuacji alarmowej.

Oprogramowanie DigitalSentry Client nie daje możliwości konfiguracyjnych systemu, za jego pomocą można monitorować obiekt w trybie rzeczywistym, wyszukiwać i przeglądać nagrane wideo. Posiada kilka konfiguracji okna wyświetlającego obraz (z 1 ,4,9 lub16 kamer), łatwo można wyświetlić w oknie obraz z konkretnej kamery wystarczy z zakładki kamery przeciągnąć kamerę która Cię interesuje do okna wyświetlającego.

Także przeglądanie nagranego wideo jest niesłychanie łatwe. Z Opcją Quick Review wystarczy jedno kliknięcie myszą aby zobaczyć widok z wielu kamer jednocześnie. Opcja ta pozwala na oglądnięcie nagrań z ostatnich: 1, 5, 15, 30 lub 60 minut.



Opcja umożliwiająca wyszukiwanie i przeglądanie nagrań wideo niezależnie gdzie one w systemie się znajdują jest oparta na prostym i intuicyjnym interfejsie graficznym. Interfejs zbudowany jest tak iż mamy dostęp do nagrań z całego tygodnia. Wystarczy wybrać odpowiednie kamery oraz oznaczyć na grafie myszką interesujące fragmenty nagrań i odtworzyć. Obraz z wszystkich kamer (do 16) będzie wyświetlany jednocześnie. Wybrane nagrania wideo można łatwo wyeksportować do popularnych formatów graficznych Windows lub do pliku wykonywalnego. Jeżeli dane zostaną wyeksportowane do pliku wykonywalnego można je odtworzyć na dowolnym komputerze klasy PC bez dodatkowego oprogramowania typu mediaplayer.

Kolejnym narzędziem które daje dostęp do systemu DS jest DS. ControlPoint Ma podobną funkcjonalność jak DigitalSENTRY jest także bardzo łatwy i intuicyjny w obsłudze. Nasuwa się więc pytanie po co używać kolejnej aplikacji jeżeli ma taką samą funkcjonalność. Otóż ControlPoint ma jedną bardzo ważną zaletę można go używać także do administracji innych systemów firmy Integral DVX, DVXi, DVXe. Jest to bardzo wygodne narzędzie dla klientów którzy mają w swoich obiektach różne rozwiązania firmy Integral. ControlPoint umożliwia obsługę wielu monitorów co pozwala na łatwiejszą obsługę dużego system CCTV.

1. Integracja podsystemów bezpieczeństwa w ramach Lokalnego Centrum Nadzoru
	1. Opis funkcjonalny systemu.

Zintegrowany system kompleksowego zabezpieczenia technicznego składa się z:

1. Podsystemów lokalnych zabezpieczenia technicznego objętych oddzielnymi opracowaniami:

* systemu wykrywania pożaru SWP
* systemu sygnalizacji włamania i napadu SSWiN
* systemu kontroli dostępu SKD
* systemu telewizji dozorowej SCTD
1. systemu integrującego w/w instalacje (Continuum - Andover Controls) będącego przedmiotem bieżącego opracowania.

W zintegrowanym systemie zabezpieczeń technicznych rozróżnia się 2 rodzaje sprzężeń pomiędzy podsystemami zabezpieczeń:

1. integracja sprzętowa podsystemów (poprzez wejścia/wyjścia dwustanowe) – lokalnie poza systemem integrującym,
* połączenie sprzętowe systemu SWP z systemem SKD (strefowe odblokowywanie nadzorowanych przejść w razie zaistnienia alarmu pożarowego),
* podłączenia pojedynczych, a istotnych z punktu widzenia ochrony obiektu sygnałów do wejść alarmowych systemu SSWiN w celu ich rejestracji i prezentacji w układzie systemu SSWiN,
* integracja sprzętowa systemu SSWiN i SCTD poprzez wejścia/wyjścia dwustanowe poza systemem integrującym,
1. rozbudowa pkt. (1) z wykorzystaniem nadrzędnego systemu komputerowego (systemu integrującego) poprzez podłączenie podsystemów zabezpieczeń technicznych za pomocą łącz komunikacji szeregowej RS232/485 i/lub poprzez wejścia/wyjścia dwustanowe do jednego stanowiska zarządzającego.

W/w połączenia umożliwiają sterowanie podłączonych systemów jak również akwizycję danych na temat ich stanu (dane o dużej szczegółowości). Odpowiednio wykonane oprogramowanie aplikacyjne na sterownikach i stanowisku operatorskim systemu integrującego umożliwia obsługę podsystemów zabezpieczeń technicznych w obiekcie w oparciu o jednolity interfejs graficzno-tekstowy. Funkcje systemu integrującego mogą być dowolnie zmieniane na drodze programowej. System ten na podstawie danych otrzymywanych z poszczególnych podsystemów umożliwia automatyczne sterowanie np. systemem SCTD, SSWiN, monitorowanie systemów SSP, SKD jak również podłączenie. Wykonanie systemu nadrzędnego w oparciu o komunikację szeregową minimalizuje okablowanie i ilość modułów wykonawczych (moduły alarmowe, przekaźnikowe) oraz umożliwia przekazywanie praktycznie nieograniczonej liczby sygnałów. W systemie tym gromadzą się informacje ze wszystkich podsystemów zabezpieczeń elektronicznych.

Sterowniki CX komunikują się z podsystemami lokalnymi łączami szeregowymi RS232 za pośrednictwem modułów komunikacyjnych oraz za pomocą modułów wejść/wyjść dwustanowych typu DM20. System będzie współpracować z nadrzędnym stanowiskiem centralnego monitoringu poprzez łącza komunikacyjne pracujące w oparciu o protokół TCP/IP.

Sposób podłączenia podsystemów zabezpieczenia technicznego do systemu integrującego:

* System Sygnalizacji Włamania i Napadu (centrala GALAXY) - komunikacja RS232 pomiędzy portem COM1 sterownika CPU2, a modułem komunikacyjnego E054 centrali GALAXY za pośrednictwem modułu interfejsowego INT3 i modułu izolacji RS232/RS232 IS3,
* System Wykrywania Pożaru - komunikacja RS232 pomiędzy portem COM1 sterownika CPU1, a modułem komunikacyjnym centrali pożarowej za pośrednictwem modułu izolacji RS232/RS232 IS1,
* System Kontroli Dostępu – Komunikacja systemowa poprzez magistralę ACCLON,
* System SCTD (Rejestrator cyfrowy) - komunikacja poprzez oprogramowanie rejestratora.
	1. Oprogramowanie systemu.

System integrujący swoje funkcje użytkowe realizuje za pomocą oprogramowania aplikacyjnego przygotowanego w środowisku systemu Continuum Cyberstation oraz oprogramowania aplikacyjnego pracującego na sterownikach CX. Oprogramowanie to zapewnia szybką lokalizację źródła zagrożenia niezależnie od systemu w którym zdarzenie zostało wygenerowane.

***Wykonawca zrealizuje oprogramowanie zarządzające systemami zabezpieczeń technicznych poprzez:***

* wykonanie modyfikacji standardowych driverów komunikacyjnych (PlainEnglish driver) do urządzeń zgodnie potrzebami wynikającymi z konfiguracji integrowanych systemów zabezpieczeń,
* wprowadzenie grafik obrazujących rzuty poszczególnych kondygnacji wraz z naniesionymi aktywnymi symbolami graficznymi elementów podłączonych podsystemów tj. czujek pożarowych, przycisków ROP, czujek włamaniowych, przycisków napadowych, manipulatorów szyfrowych, drzwi, czytników, kamer, kontrolerów, czujników krańcowych itd. – stan poszczególnych elementów (stref, urządzeń, pomieszczeń itd.) rozróżniany jest poprzez kolor, kształt, animację,
* wykonanie oprogramowania wiążącego dane otrzymywane z driverów komunikacyjnych z poszczególnymi elementami aktywnymi naniesionymi na grafiki,
* wykonanie oprogramowania wiążącego dane wysyłane ze środowiska operatorskiego poprzez drivery komunikacyjne do podłączonych do systemu urządzeń (np. sterowanie kamerami, uzbrajanie/rozbrajanie stref itd.),
* zdefiniowanie alarmów, wykonanie oprogramowania sterującego środowiskiem graficznym użytkownika w razie zaistnienia alarmu zagrożeniowego,
* wykonanie oprogramowania sterującego elementami (bramy, szlaban, sygnalizator) na podstawie wytycznych zawartych w projekcie systemu kontroli dostępu.

***Współpraca systemu SCTD z systemem integrującym:***

* system SCTD będzie sterowany i monitorowany przez system integrujący

SCTD-sterowanie w normalnym trybie pracy:

* poszczególne kamery zostaną naniesione na grafiki obrazujące rzuty poszczególnych kondygnacji i terenu,
* użytkownik będzie sterować wyświetlaniem obrazów z kamer poprzez kliknięcie myszką na piktogramie kamery naniesionej na rzuty pięter,

SCTD-sterowanie w razie alarmu zagrożeniowego:

* automatycznie sterowanie SCTD w powiązaniu z systemem SKD (wyświetlenie obrazu z najbliższej kamery przy zaistnieniu alarmu FORSOWANIE DRZWI),
* podstawowe funkcje sterowania i zmiany trybów pracy systemu SCTD na skutek alarmów zagrożeniowych generowanych w systemie SSWIN,
* automatycznie sterowanie SCTD w powiązaniu z systemem SWP (wyświetlenie wszystkich kamer ze strefy w której zaistniał alarm pożarowy).

***Współpraca systemu SSWiN z systemem integrującym:***

* system SSWiN będzie monitorowany i zarządzany przez system integrujący,
* poszczególne elementy systemu: czujki, czujniki krańcowe, urządzenia nadzorowane przez system SSWiN zostaną naniesione na grafiki obrazujące rzuty poszczególnych kondygnacji,
* wykonany zostanie panel synoptyczny obrazujący zbiorcze zestawienie stanu stref .

***Współpraca systemu SKD z systemem integrującym:***

* system SKD będzie monitorowany przez system integrujący i sterowany w zakresie obsługi elementów,
* poszczególne elementy systemu: drzwi, czytniki, szlabany zostaną naniesione na grafiki obrazujące rzuty poszczególnych kondygnacji,
* na podstawie sygnałów z systemu SKD istnieć będzie możliwość wysterowania alarmowego systemu SCTD (funkcja konfigurowalna przez użytkownika),
* stan poszczególnych elementów generujących alarmy techniczne tj. moduły drzwiowe, kontrolery SKD zostanie zobrazowany na zbiorczym panelu synoptycznym.

***Współpraca systemu SWP z systemem integrującym:***

* system SWP będzie monitorowany przez system integrujący,
* poszczególne elementy systemu: czujki pożarowe, przyciski ROP zostaną naniesione na grafiki obrazujące rzuty poszczególnych kondygnacji obiektu,
* na podstawie sygnałów z systemu SWP istnieć będzie możliwość wysterowania alarmowego systemu SCTD (funkcja konfigurowalna przez użytkownika),
* stan poszczególnych elementów generujących alarmy techniczne tj. centrala, pętle zobrazowany zostanie na zbiorczym panelu synoptycznym,
* przewidziano współpracę systemu przeciwpożarowego z systemem kontroli dostępu polegającą na automatycznym otwarciu drzwi znajdujących się na głównych ciągach komunikacyjnych w momencie wykrycia pożaru.

UWAGA:

Podstawowe funkcje sterowania urządzeń systemu SWP (tj. sterowanie pożarowe wentylacją, oddymianiem, systemem kontroli dostępu) realizowane są poprzez bezpośrednie sprzężenie przekaźnikowych wyjść alarmowych centrali SWP i wejść sterowania pożarowego w/w systemów poza systemem integrującym (bezpośrednie przerwanie obwodów zasilających rygle elektromagnetyczne przez przekażniki centrali SWP). Automatyczne otwarcie drzwi następuje po wystąpieniu alarmu pożarowego II stopnia.

***Wytyczne ogólne dotyczące funkcji administracyjnych systemu integrującego:***

* archiwizacja wszystkich zdarzeń alarmowych umożliwiając ich późniejszą obróbkę: przeglądanie, drukowanie, generację raportów (z każdym zdarzeniem przechowywana jest miejsce, data, godzina przyjścia alarmu oraz dane osoby potwierdzającej zdarzenie),
* możliwość przyszłościowego przekazywania informacji do zewnętrznego systemu monitoringu,
* dokumentacja podsystemów lokalnych w bazie danych: poprzez przeniesienie części dokumentacji w/w systemów do systemu integrującego (np. poprzez kliknięcie na symbolu graficznym czujki, kontrolera itd. operator uzyskuje dokładne informacje o typie elementu, miejscu jego zainstalowania, stanie itd. – dowolnie zdefiniowane),
* wprowadzenie systemu haseł zabezpieczających oraz zdefiniowanie zakresu uprawnień do posługiwania się systemem dla poszczególnych operatorów – skonsultować z inwestorem w fazie realizacji,

***Wytyczne odnośnie definicji alarmów i reakcji systemu na zdarzenia alarmowe:***

 W systemie integrującym należy rozróżnić 2 typy alarmów:

* alarmy zagrożeniowe,
* alarmy techniczne.

Dla alarmów zagrożeniowych zdefiniowano priorytety umożliwiające systemowi integracji prezentację dla operatora zdarzeń i alarmów o najwyższym priorytecie.

Przyjęto następujący priorytet zdarzeń w ramach podsystemów zabezpieczenia technicznego:

* SYSTEM SYGNALIZACJI POŻAROWEJ >
* SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU >
* SYSTEM KONTROLI DOSTĘPU >
* ALARMY TECHNICZNE ZE WSZYSTKICH PODSYSTEMÓW (np. brak zasilania 220/12V, brak komunikacji itd.).

Przyjęto następujący priorytet zdarzeń w obrębie każdego z podsystemów zabezpieczenia technicznego:

SYSTEM SWP

* Pożar

SYSTEM SSWiN

* Włamanie/Napad >
* Sabotaż (czujki, manipulatora szyfrowego)

SYSTEM SKD

* Forsowanie drzwi >
* Nieprawidłowa karta

W razie zaistnienia alarmu zagrożeniowego system integracji automatycznie wyświetla grafikę z aktywnym elementem oraz wysteruje system SCTD dla alarmu o najwyższym priorytecie. Po obsłużeniu alarmu o najwyższym priorytecie system automatycznie prezentuje kolejny alarm o najwyższym priorytecie.

Przy alarmach technicznych oraz zdarzeniach alarmowych różnych od: „Pożar”, „Włamanie/Napad”, „Sabotaż”, „Otwarcie pod przymusem”, „Błędny kod”, „Forsowanie drzwi”, „Nieprawidłowa karta” pozostawiono mechanizm ręcznego wybierania alarmu do obsługi oraz ręcznego wyboru panela graficznego.

Opis przykładowej reakcji zintegrowanego systemu zabezpieczeń na zdarzenie alarmowe – naciśnięcie przycisku napadowego systemu SSWiN:

* cicha sygnalizacja zdarzenia w pomieszczeniu ochrony, wyświetlenie informacji na klawiaturze systemowej, rejestracja zdarzenia w systemie lokalnym,
* przekazanie informacji do RCN, KCM, zewnętrznej stacji monitoringu i dialerowych systemów powiadamia,
* automatyczne wysterowanie systemu SCTD na kamery najbliższe zdarzeniu alarmowemu,
* automatyczne wyświetlenie grafiki ze wskazaniem pobudzonego elementu na komputerze operatora,
* archiwizacja alarmu i sposobu jego obsługi w bazie danych systemu integracji.
1. Zestawienie urządzeń i oprogramowania

**W zakresie dostaw Wykonawcy znajdowały się następujące elementy :**

* oprogramowanie systemu integrującego zgodne z wymaganiami dokumentacji systemu CAIFS;
* elementy do rozbudowy routerów.

## Specyfikacja dostaw oprogramowania.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis** | **Ilość** |
| 1 | Alarm Video Network Monitoring | 1 |
| 2 | Oprogramowanie do podglądu obrazów z rejestratorów  | 1 |
| 3 | Interfejs do systemu SSWiN Galaxy | 1 |
| 4 | Interfejs do systemu SAP Esser | 1 |

1. Spis Rysunków

|  |  |
| --- | --- |
| R01 | Schemat sieci integracji systemów bezpieczeństwa IC Olsztyn. |
| R02 | Schemat integracji systemów bezpieczeństwa na obszarze obiektu granicznego. |
|  |  |
|  |  |
|  |  |
|  |  |