



IFTEREQU

DOKUMENTACJA

UTC Advisor Master

13-12-18

Spis Treści

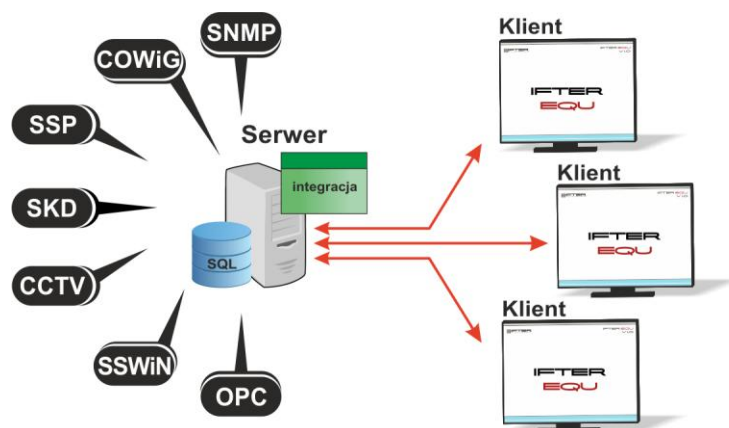
| | | |
|--------|---|----|
| 1. | Oprogramowanie wizualizacyjne IFTER EQU | 1 |
| 2. | Wizualizacja centrali UTC - Advisor Master | 4 |
| 3. | Uzyskanie kodu bezpieczeństwa..... | 5 |
| 4. | Połączenie Komputer – Centrala..... | 6 |
| 5. | Przykładowe ustawienia połączenia z centralą | 6 |
| 5.1. | Ustawienia centrali z poziomu programu TITAN | 6 |
| 5.1.1. | Uruchomienie programu TITAN..... | 6 |
| 5.1.2. | Import systemu do programu TITAN | 6 |
| 5.1.3. | Ustawienia IP oraz portów komunikacyjnych | 8 |
| 5.1.4. | Kod bezpieczeństwa z poziomu programu TITAN..... | 9 |
| 5.2. | Ustawienia modułu ATS1806..... | 9 |
| 5.2.1. | Uruchomienie strony modułu ATS1806..... | 9 |
| 5.2.2. | Ustawienie lub sprawdzenie adresu modułu | 10 |
| 5.2.3. | Ustawienie połączenia z komputerem..... | 11 |
| 5.2.4. | Ustawienie kodu bezpieczeństwa modułu | 12 |
| 5.2.5. | Ustawienia IP modułu ATS1806 | 13 |
| 6. | Ustawienie połączenia w EQU oraz Import pliku konfiguracyjnego do systemu EQU Advisor Master..... | 14 |
| 6.1. | Import systemu z pliku .zip do programu TITAN | 14 |
| 6.2. | Tworzenie integracji UTC – Advisor Master | 16 |
| 6.3. | Ustawienie połączenia w programie EQU | 17 |
| 6.4. | Import konfiguracji..... | 20 |
| 7. | Komponent Użytkownicy – Advisor Master | 23 |
| 7.1. | Umieszczanie komponentu na grafice..... | 23 |
| 7.2. | Wygląd i funkcje komponentu na wizualizacji | 25 |

1. Oprogramowanie wizualizacyjne IFTER EQU

Wizualizacja oparta na programie IFTER EQU pozwala na przedstawienie elementów systemów SSP, SSWiN, KD, CCTV, Automatyki budynkowej oraz urządzeń kontrolno – pomiarowych

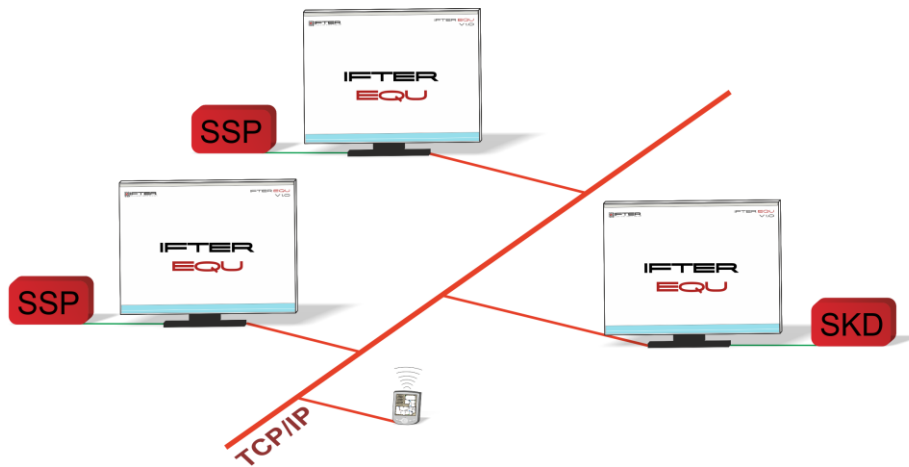
w postaci graficznej i tekstowej. Elementy wizualizacji prezentowane są na planach architektonicznych, geodezyjnych lub ciągach technologicznych.

Architektura oprogramowania pozwala na dostosowanie wizualizacji do wielkości obiektu oraz ułatwia zarządzanie obiektami o rozproszonej lokalizacji. Wykorzystując sieci TCP/IP, możliwe jest stworzenie niezależnie działających stacji roboczych rozmieszczonych w różnych częściach obiektu lub kilku obiektach. Wykorzystanie rozwiązań bazodanowych pozwala na stworzenie sieci stacji monitorujących oraz całych centrów monitorowania, którymi można zarządzać z dowolnego miejsca w sieci.



Rys. 1. Architektura systemu

Dzięki elastyczności oprogramowania, możliwa jest łatwa rozbudowa wizualizacji o kolejne obiekty lub urządzenia monitorowanych systemów. Wygląd wizualizacji może być dowolnie skonfigurowany przez użytkownika, co zapewnia łatwe korzystanie z programu.



Rys. 2. połączenie stacji roboczych

Na jednej stacji roboczej można obsługiwać do ośmiu monitorów oraz dostosować widoczność elementów dla każdego z użytkowników. Uprawnienia do korzystania z funkcji programu przyznawane są oddzielnie dla każdego użytkownika. W celu automatyzacji zadań, użytkownik ma możliwość tworzenia harmonogramów pracy.

Harmonogramy służą zarówno do planowania, sterowania, obsługi alarmów oraz zdarzeń, sterowania stanami pracy integrowanych urządzeń, jak również do ograniczania dostępu użytkowników do systemu. Jeden harmonogram może obsługiwać nieograniczoną liczbę użytkowników i szablonów alarmów. W harmonogramach można skorzystać z opcji „dni specjalne”, które można utworzyć w dowolnej liczbie. Mogą to być dni świąteczne według kalendarza lub dni wybrane przez użytkownika, którym można nadawać nazwy, przedziały czasowe lub wyróżnić kolorem.

Zdarzenia alarmowe oraz zdarzenia z urządzeń zapisywane są w postaci logów w dziennikach. Operator ma możliwość wybrania dla każdego dziennika, z jakich urządzeń zapisywane będą zdarzenia oraz jaki użytkownik może mieć do nich dostęp. Zdarzenia zapisane w dziennikach mogą być wyróżnione kolorem w celu ich łatwiejszej identyfikacji.

Podczas potwierdzania alarmu, system rejestruje czas wystąpienia zdarzenia, czas potwierdzenia alarmu oraz użytkownika potwierdzającego. Dodatkowo komentarz do alarmu, jeśli jest wymagany. W przypadku dodatkowych zadań, które towarzyszą potwierdzeniu alarmów, użytkownik może zdefiniować listę zadań, które operator musi wykonać przed potwierdzeniem alarmu.

W celu ułatwienia monitorowania obiektów użytkownikowi IFTER EQU dostarcza funkcje takie jak:

- wyświetlanie ostrzeżeń o stanach alarmowych z urządzeń w postaci tekstowej oraz graficznej;
- sygnalizowanie stanów alarmowych sygnałem dźwiękowym;
- prezentowanie stanu elementów systemu;
- definiowane procedury postępowania w sytuacjach alarmowych;
- dostarczanie cichych alarmów do centrum monitorowania bez informowania stacji roboczej;
- wyświetlanie lokalizacji zdarzenia alarmowego w chwili jego wystąpienia;
- funkcje integracji, które umożliwiają tworzenie relacji między różnymi urządzeniami;
- prowadzenie użytkownika od planu ogólnego do szczegółowego;
- automatyzacja pracy poprzez wykorzystanie harmonogramów zadań;
- dopasowanie wizualizacji do wymagań użytkownika.

Do głównych cech charakteryzujących ten produkt możemy zaliczyć:

- Wielojęzyczność pozwalającą na dostosowanie systemu do lokalnego języka;
- Bazę danych opartą na SQL firmy Oracle, umożliwiającą wykorzystanie typowej technologii klient-serwer do prezentowania stanu systemów integrowanych, sterowania i konfiguracji na wielu komputerach jednocześnie;
- Możliwość skonfigurowania serwera zarządzającego komunikacją z urządzeniami i komputerami. Serwer może pracować w trybie usługi - nie wymaga wtedy monitora, myszki i klawiatury;
- Dzięki temu że jesteśmy niezależnym producentem oprogramowania, IFTER EQU obsługuje urządzenia wielu konkurencyjnych firm, co pozwala na najlepszy dobór urządzeń do potrzeb obiektu;
- Funkcje integracji, które umożliwiają tworzenie relacji między różnymi urządzeniami;

- Cały wygląd systemu jest swobodnie konfigurowany, co umożliwia idealną prezentację wszystkich systemów integrowanych, wykorzystując do tego niezależne wyświetlanie nawet na czterech monitorach lub korzystając ze wsparcia obsługi paneli dotykowych;
- Na każdym widoku można przedstawić stan dowolnego urządzenia, tak aby jak najlepiej odzwierciedlić funkcjonalność i rozmieszczenie tych urządzeń. Na jednym widoku można przedstawić stan urządzeń systemów bezpieczeństwa i automatyki budynkowej;
- W swobodny sposób możemy również zarządzać dostępem do sterowania urządzeniami, poprzez ograniczenie uprawnień poszczególnych osób lub wymagając wprowadzenia hasła;
- Rozbudowane możliwości alarmowania ułatwiają reagowanie na włamania, sabotaże, ominięcie lub nawet rozbrojenia strefy alarmowej, poprzez wyświetlanie różnych procedur postępowania i komentarzy domyślnych, w zależności od lokalizacji i typu zagrożenia;
- Obsługa automatyki budynkowej jest ułatwiona dzięki wykorzystaniu skryptów, harmonogramów oraz mechanizmów trendów, progów i wzorców.

2. Wizualizacja centrali UTC - Advisor Master

Komunikacja z centralą odbywa się poprzez interfejs RS232 lub sieć Ethernet wykorzystując moduł ATS1801.

Z centrali pobierane są wszystkie typy zdarzeń i następnie rejestrowane w dziennikach zdarzeń i dziennikach alarmów. Zdarzenia zapisane w dziennikach alarmów wymagają od operatora:

- potwierdzenia alarmu, zapisywany jest wtedy czas potwierdzenia,
- wykonania czynności zgodnie ze zdefiniowaną procedurą – opcja,
- skomentowanie alarmu, komentarz może być każdorazowo pisany przez operatora lub może być zdefiniowany dla danego alarmu komentarz domyślny.

Na wizualizacji możemy prezentować stany w postaci ikon lub pól aktywnych:

- linia: brak komunikacji z centralą, brak uzbrojenia, naruszenie, sabotaż rozwarcie, alarm, sabotaż zwarcie, blokada;

- drzwi: brak komunikacji z centralą, stan normalny, drzwi zamknięte, drzwi otwarte, drzwi zablokowane, drzwi odblokowane, drzwi czasowo otwarte, drzwi wyłączone, alarm, przekroczenie czasu otwarcia;
- obszar: brak komunikacji z centralą, alarm, brak gotowości do uzbrojenia, ominięcie, odliczanie – wejście, odliczanie – wyjście, uzbrojenie, rozbrojenie;
- wyjście: brak komunikacji z centralą, stan normalny, aktywacja;
- MZD: brak komunikacji z centralą, stan normalny, awaria, sabotaż.

Z wizualizacji można konfigurować sterowanie poprzez udzielanie uprawnień do:

- obszar: rozbrój, uzbrój, reset;
- linia: odblokuj, zablokuj, reset;
- drzwi: otwórz, zablokuj, odblokuj, wyłącz, włącz, czasowo odblokuj;
- zarządzanie personelem: dodawanie/usuwanie użytkowników, przypisywanie kart, programowanie kart.

3. Uzyskanie kodu bezpieczeństwa

Aby uzyskać kod bezpieczeństwa, należy wykonać następujące kroki w Menu oprogramowania zarządzającego:

1278 *Enter*
19 *Enter*
19 *Enter*

Kod bezpieczeństwa: 0000000000

Następnie zaznacz poniższe opcje:

- Autoryzacja połączenia z komputerem: NIE;
- Włącz zdalny up/download: TAK;
- Up/download, jeśli jakiś ob. Zazb.: TAK;
- Włącz zdalne sterowanie: TAK;
- Zdalne sterowanie, gdy jakiś obszar zazb.: TAK;
- Raportuj alarmy do komputera: TAK;
- Raportuj zdarzenia dostępu do komputera: TAK;
- Adres komputera: Adres – gdy TCP/IP;
- Kod bezpieczeństwa (domyślny: 0000000000) – wpisać do EQU.

4. Połączenie Komputer – Centrala

Komunikacja komputera z centralą odbywa się za pomocą protokołu UDP z wykorzystaniem interfejsu ATS1806. Przed konfiguracją połączenia z EQU należy prawidłowo skonfigurować połączenie ATS1806 z centralą. Urządzenia powinny być w jednej sieci Ethernet oraz powinny się „pingować”. Zapory ogniowe, kontrola kont użytkownika Windows oraz antywirusy powinny być wyłączone na czas nawiązywania pierwszego połączenia. Zabezpieczenie systemu operacyjnego można konfigurować dopiero po zakończeniu prac związanych z połączeniem EQU ze wszystkimi stacjami roboczymi oraz z centralami.

5. Przykładowe ustawienia połączenia z centralą

5.1. Ustawienia centrali z poziomu programu TITAN

5.1.1. Uruchomienie programu TITAN

Do poniższych ustawień centrali możemy wejść z poziomu programu TITAN. Program należy uruchomić i się zalogować. Standardowe dane do logowania:

- login: ADVISOR MASTER,
- hasło: 998765.

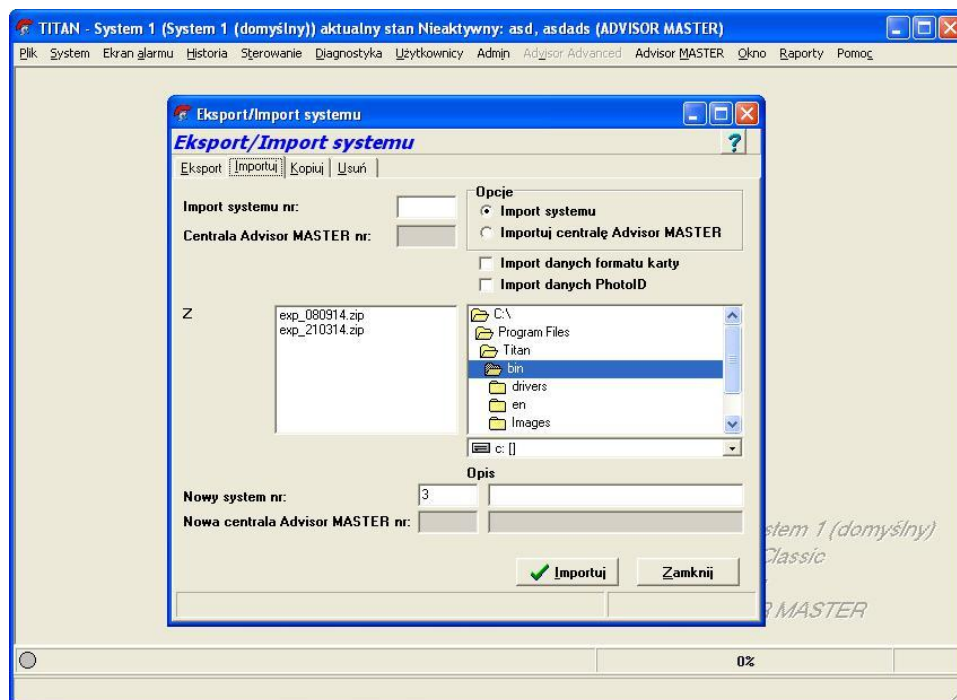
5.1.2. Import systemu do programu TITAN

Jeśli konfigurację centrali mamy jedynie w formie pliku .zip (np. exp_080814.zip), należy najpierw zaimportować odpowiedni system znajdujący się w tym pliku do programu TITAN. Standardowo plik ten znajduje się w katalogu bin z programem TITAN.

(C:\Program Files\Titan\bin). **Pomijamy ten krok, jeśli** odpowiedni system jest już otwarty w programie TITAN i program ten prawidłowo łączy się z centralą.

a) Jeśli system nie jest zaimportowany do programu TITAN, należy go najpierw zaimportować.

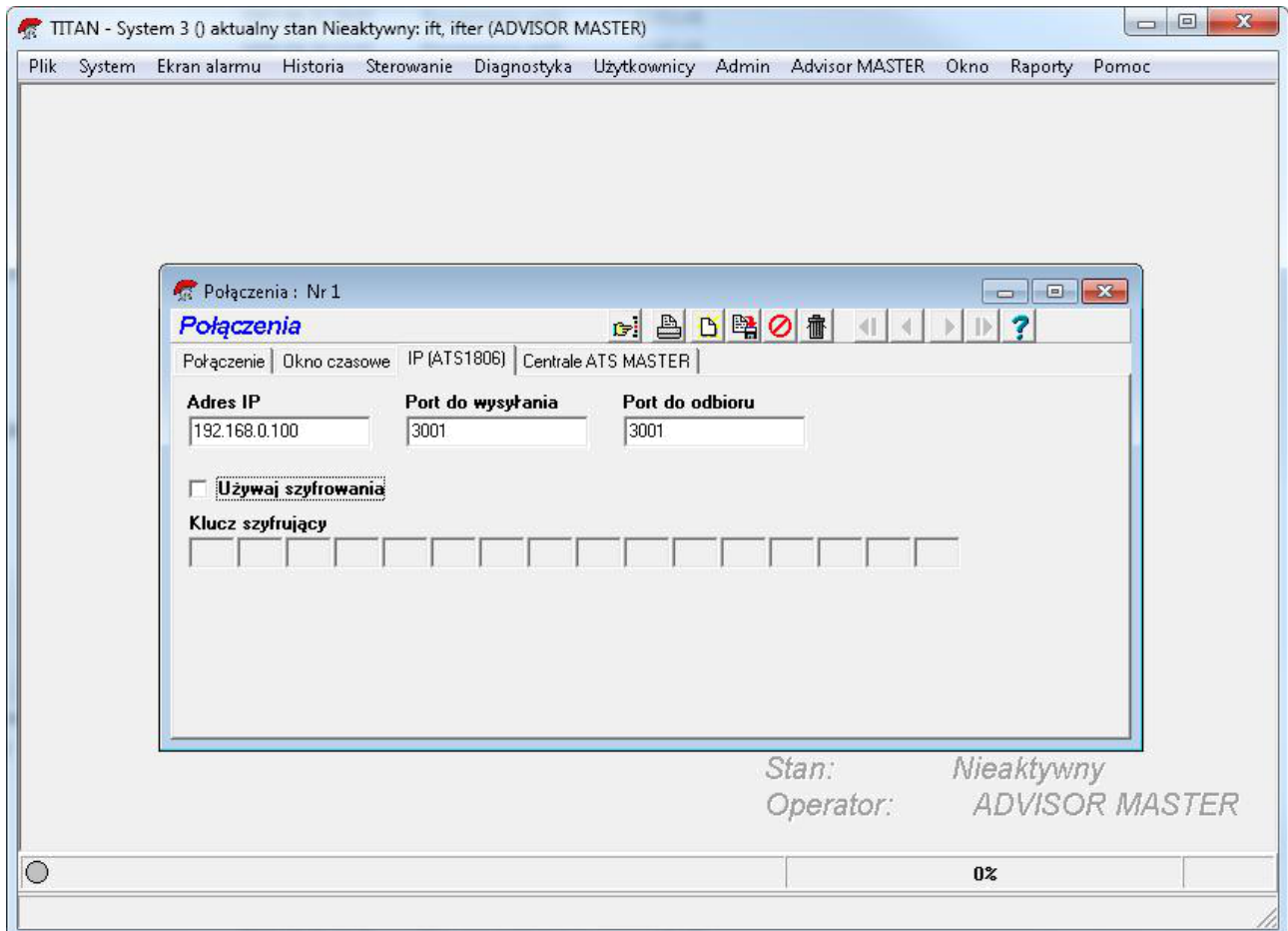
W oknie, które się pojawi, należy wybrać zakładkę **Import**. Następnie należy kliknąć 2 razy w plik z exportem .zip (np. exp_080814.zip). W polu "Import systemu numer:" wartość zmieni się na poprawną. W polu **Nowy system nr** podaj kolejną liczbę. Wartość tą ustawiamy na większą o 1 niż ilość posiadanych systemów (domyślnie powinna być podana już odpowiednia liczba). Następnie należy wskazać folder, gdzie wklejone zostały pliki konfiguracyjne (np. exp_080814.zip). W okienku po lewej stronie zaznaczyć plik konfiguracyjny. Kliknąć **Importuj**.



- b) Aby włączyć zaimportowany system należy wejść w zakładkę **System** → **Wybierz**
- c) Wybieramy zaimportowany system → **OK**. Dopiero teraz możemy poruszać się po zaimportowanym systemie.

5.1.3. Ustawienia IP oraz portów komunikacyjnych

Aby wejść do poniższego okna należy otworzyć zakładkę **Admin** → **Połączenia** → **IP (ATS1806)**.



Przykładowe ustawienie w przypadku, gdy łączymy się z tylko jedną centralą:

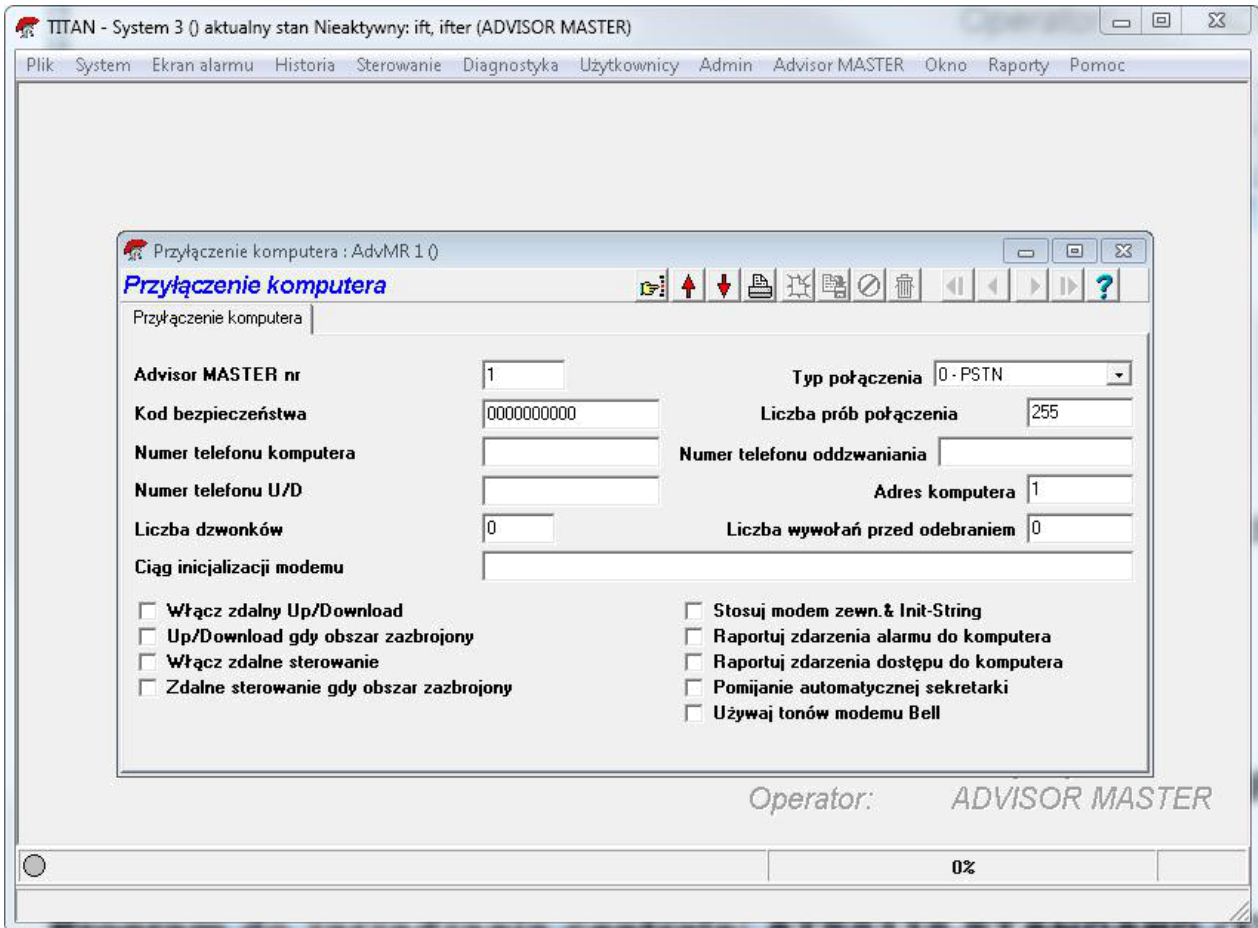
- Adres IP centrali: 192.168.0.161,
- Port wysłania: 3001,
- Port odbioru: 3001.

Powyższe dane będą nam potrzebne do ustawienia komunikacji w EQU.

Gdy mamy wiele central IP oraz Porty wysłania i odbioru powinny być dla nich różne.

5.1.4. Kod bezpieczeństwa z poziomu programu TITAN

Aby wejść do poniższego okna należy otworzyć zakładkę **Advisor MASTER** → **Komunikacja** → **Przyłączenie komputera**.



Kod bezpieczeństwa będzie nam potrzebny do ustawienia komunikacji w EQU.

5.2. Ustawienia modułu ATS1806

5.2.1. Uruchomienie strony modułu ATS1806

Przy pierwszym uruchomieniu ATS1806 należy:

- Założyć jumper J8 na ATS1806. Spowoduje to ustawienie domyślnego adresu IP interfejsu na 192.168.0.100,
- Włączyć zasilanie centrali i ATS1806,
- Począkać 20 sekund,
- Włączyć komputer do sieci TCP/IP i ustawić jego adres IP w tej samej podsieci (np. 192.168.0.101 i maska 255.255.255.0),

- Uruchomić przeglądarkę internetową i wpisać domyślny adres interfejsu (*http://192.168.0.100*),
- Pojawi się strona startowa interfejsu ATS1806,
- Zalogować się (Log-in) domyślnym użytkownikiem *ADVISOR MASTER* z hasłem *998765*.

5.2.2. Ustawienie lub sprawdzenie adresu modułu

Należy wybrać zakładkę **Panel Physical Address**. Wyświetli nam się numer modułu.



The screenshot displays the GE Security web interface. On the left is a navigation menu with categories: User Authentication (Home, Login, Logout, Change user details), Network Setup (Static address parameters, Central station parameters, Network Receiver, Email/TFTP parameters, Network Probing), Panel Setup (SecureStream: Event ACK interval, SecureStream: Heartbeat interval, Panel physical address, Panel security password, Twofish Encryption key), Firewall Setup (Show all rules, Add a new rule, Delete a rule), and Utilities (Auto enroll, Restart communications, Local event log, Printer event log, CPU load, System uptime, Flash ROM version, Reboot CPU, Upload ROM image). The right side shows the 'Setup the Panel Physical Address (Computer Address)' page with a text input field labeled 'Panel address:' containing the value '1', and 'Submit' and 'Reset' buttons.

Adres modułu będzie nam potrzebny do ustawienia komunikacji w **EQU**.

5.2.3. Ustawienie połączenia z komputerem

Aby wejść do poniższego okna, należy za pomocą przeglądarki internetowej zalogować się na stronie modułu **ATS1806**, a następnie wybrać zakładkę **Central station parameters**. Wyświetli nam się numer modułu.



| |
|----------------------------------|
| User Authentication |
| Home |
| Login |
| Logout |
| Change user details |
| Network Setup |
| Static address parameters |
| Central station parameters |
| Network Receiver |
| Email/FTP parameters |
| Network Probing |
| Panel Setup |
| SecureStream: Event ACK interval |
| SecureStream: Heartbeat interval |
| Panel physical address |
| Panel security password |
| Twofish Encryption key |
| Firewall Setup |
| Show all rules |
| Add a new rule |
| Delete a rule |
| Utilities |
| Auto enroll |
| Restart communications |
| Local event log |
| Printer event log |
| CPU load |
| System uptime |
| Flash ROM version |
| Reboot CPU |
| Upload ROM image |



Setup the Central Station Network Parameters

Alarm Reporting Central Stations

| Station | IP Address | Protocol | Port | Event Type | Encryption |
|---------|------------|----------|------|------------|------------|
| 1 | 0 0 0 0 | TCP | 0 | None | None |
| 2 | 0 0 0 0 | TCP | 0 | None | None |
| 3 | 0 0 0 0 | TCP | 0 | None | None |

Management Central Stations

| Station | IP Address | Protocol | Port | Event Type | Encryption |
|---------|---------------|----------|------|------------|------------|
| 4 | 192 168 0 101 | UDP | 3001 | Computer | None |
| 5 | 0 0 0 0 | TCP | 0 | None | None |
| 6 | 0 0 0 0 | TCP | 0 | None | None |
| 7 | 0 0 0 0 | TCP | 0 | None | None |
| 8 | 0 0 0 0 | TCP | 0 | None | None |
| 9 | 0 0 0 0 | TCP | 0 | None | None |
| 10 | 0 0 0 0 | TCP | 0 | None | None |
| 11 | 0 0 0 0 | TCP | 0 | None | None |
| 12 | 0 0 0 0 | TCP | 0 | None | None |
| 13 | 0 0 0 0 | TCP | 0 | None | None |
| 14 | 0 0 0 0 | TCP | 0 | None | None |
| 15 | 0 0 0 0 | TCP | 0 | None | None |

Submit Reset all

Ważne, aby w jednej z linijek tabeli **Management Central Stations** tym miejscu wybrać ustawienia:

- Protocol: UDP
- Event Type: Computer
- Encryption: NONE
- IP Address: Adres IP komputera
- Port: numer portu odbioru

Powyższe ustawienia (IP oraz numer portu odbioru) powinny być zgodne z ustawieniami w komputerze i na centrali.

5.2.4. Ustawienie kodu bezpieczeństwa modułu

Należy wybrać zakładkę **Panel Security password**. Wyświetli nam się poniższa tabelka:



GE Security

Setup the Panel Security Password

User Authentication

- Home
- Login
- Logout
- Change user details

Network Setup

- Static address parameters
- Central station parameters
- Network Receiver
- Email/TFTP parameters
- Network Probing

Panel Setup

- SecureStream: Event ACK interval
- SecureStream: Heartbeat interval
- Panel physical address
- Panel security password**
- Twofish Encryption key

Firewall Setup

- Show all rules
- Add a new rule
- Delete a rule

Utilities

- Auto enroll
- Restart communications
- Local event log
- Printer event log
- CPU load
- System uptime
- Flash ROM version
- Reboot CPU
- Upload ROM image

Security password: 00 00 00 00 00

Submit Reset

Powinien być tu ustawiony kod dostępu taki jak dla centrali.

5.2.5. Ustawienia IP modułu ATS1806

Należy wybrać zakładkę **Static address parameters**. Wyświetli nam się poniższa tabelka:



| |
|--|
| User Authentication |
| Home |
| Login |
| Logout |
| Change user details |
| Network Setup |
| Static address parameters |
| Central station parameters |
| Network Receiver |
| Email/TFTP parameters |
| Network Probing |
| Panel Setup |
| SecureStream: Event ACK interval |
| SecureStream: Heartbeat interval |
| Panel physical address |
| Panel security password |
| Twofish Encryption key |
| Firewall Setup |
| Show all rules |
| Add a new rule |
| Delete a rule |
| Utilities |
| Auto enroll |
| Restart communications |
| Local event log |
| Printer event log |
| CPU load |
| System uptime |
| Flash ROM version |
| Reboot CPU |
| Upload ROM image |

| | | | | |
|------------------------|-----|-----|-----|-----|
| Enter IP address: | 192 | 168 | 0 | 100 |
| Enter netmask: | 255 | 255 | 255 | 0 |
| Enter gateway address: | 192 | 168 | 0 | 1 |

W tym miejscu ustawiamy docelowy adres IP interfejsu oraz maskę sieci i bramkę (jeżeli potrzebna).

Uwaga: Ważne, aby adres IP modułu był dokładnie tym samym adresem, który jest ustawiony dla centrali w programie TITAN.

Po zapisaniu zmian i zdjęciu jumpera J8, należy na chwilę wyłączyć zasilanie i uruchomić interfejs z nowymi ustawieniami sieci.

Uwaga: stosownie do wykonanych zmian, należy też uaktualnić ustawienia sieci dla komputera PC!

6. Ustawienie połączenia w EQU oraz Import pliku konfiguracyjnego do systemu EQU Advisor Master

6.1.Import systemu z pliku .zip do programu TITAN

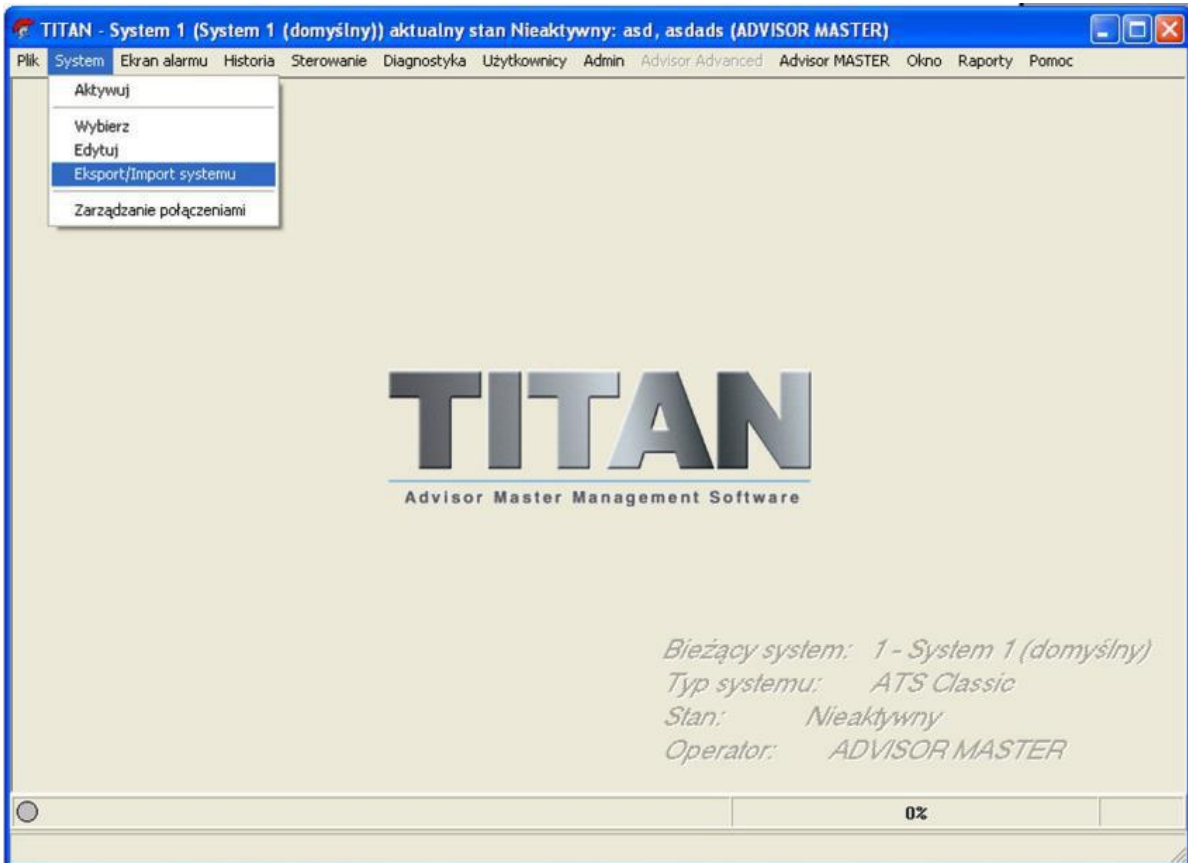
Program do zarządzania centralą: ATS8118-STANDARD (Titan)

Plik konfiguracyjny: plik wyeksportowany z centrali o rozszerzeniu .zip

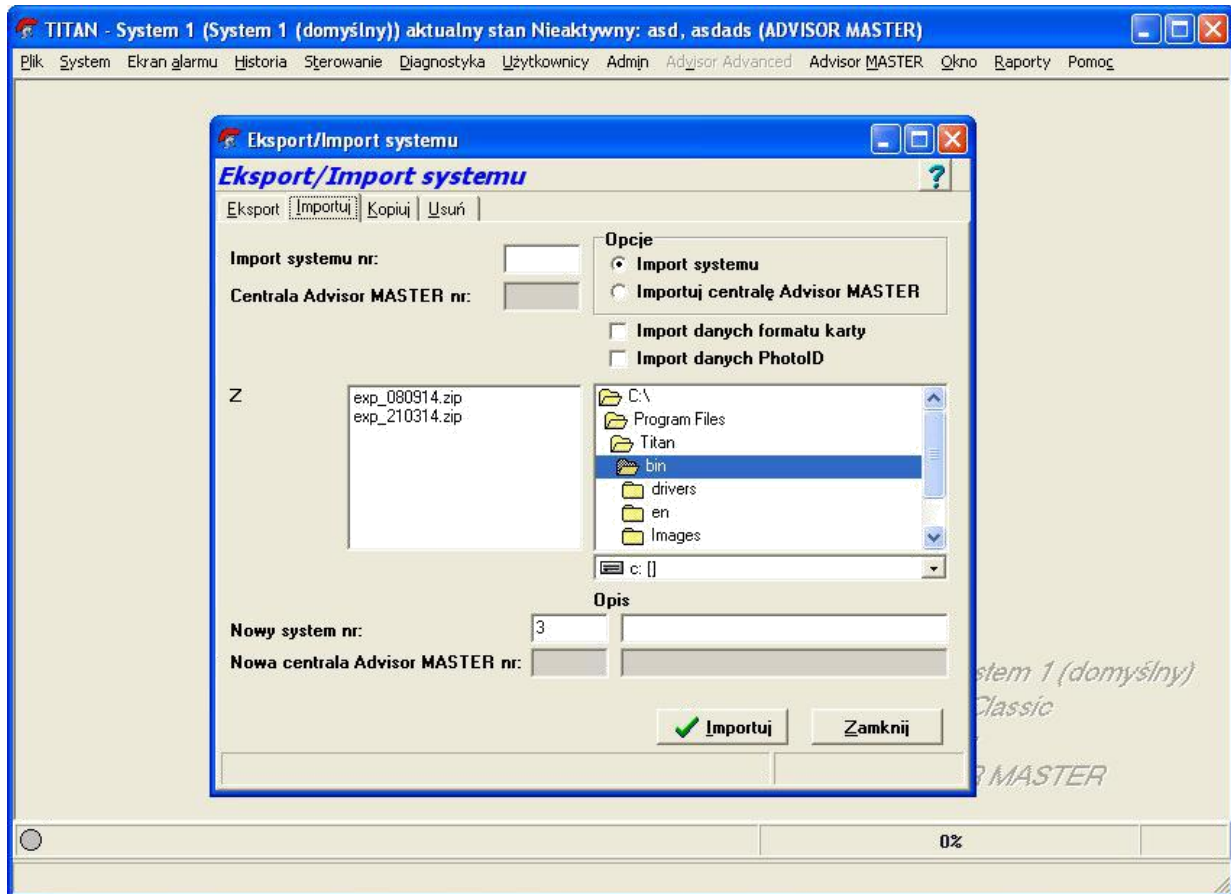
- a) Wkleić spakowany folder (.zip) z plikami konfiguracyjnymi z centrali do katalogu C:\Program Files\Titan.
- b) Wyłączyć EQU na wszystkich stacjach roboczych, jeśli jest włączone. (TITAN oraz EQU nie mogą być uruchomione w tym samym czasie)
- c) Uruchomić program Titan i zalogować się, gdzie Użytkownik to **ADVISOR MASTER**, a hasło: **998765**.



- d) Wybrać pozycję System, a następnie Eksport/Import systemu.




e) Jeśli system, z którego mamy pobrać konfigurację nie jest zaimportowany do programu TITAN należy go najpierw zaimportować. W oknie, które się pojawi wybrać zakładkę Import. Następnie należy kliknąć 2 razy w plik z exportem .zip (np. exp_080814.zip). W polu "Import systemu numer:" wartość zmieni się na poprawną. W polu **Nowy system nr** podać kolejną liczbę, czyli wartość tą ustawiamy na większą o 1 niż ilość posiadanych systemów (domyślnie powinna być podana już odpowiednia liczba). Następnie należy wskazać folder, gdzie wklejone zostały pliki konfiguracyjne (np. exp_080814.zip). W okienku po lewej stronie zaznaczyć plik konfiguracyjny. Kliknąć **Importuj**.



f) Aby włączyć zaimportowany system należy wejść w zakładkę System → Wybierz → Wybieramy zaimportowany system → OK. Dopiero teraz możemy poruszać się po zaimportowanym systemie.


g) Możemy zamknąć program TITAN.

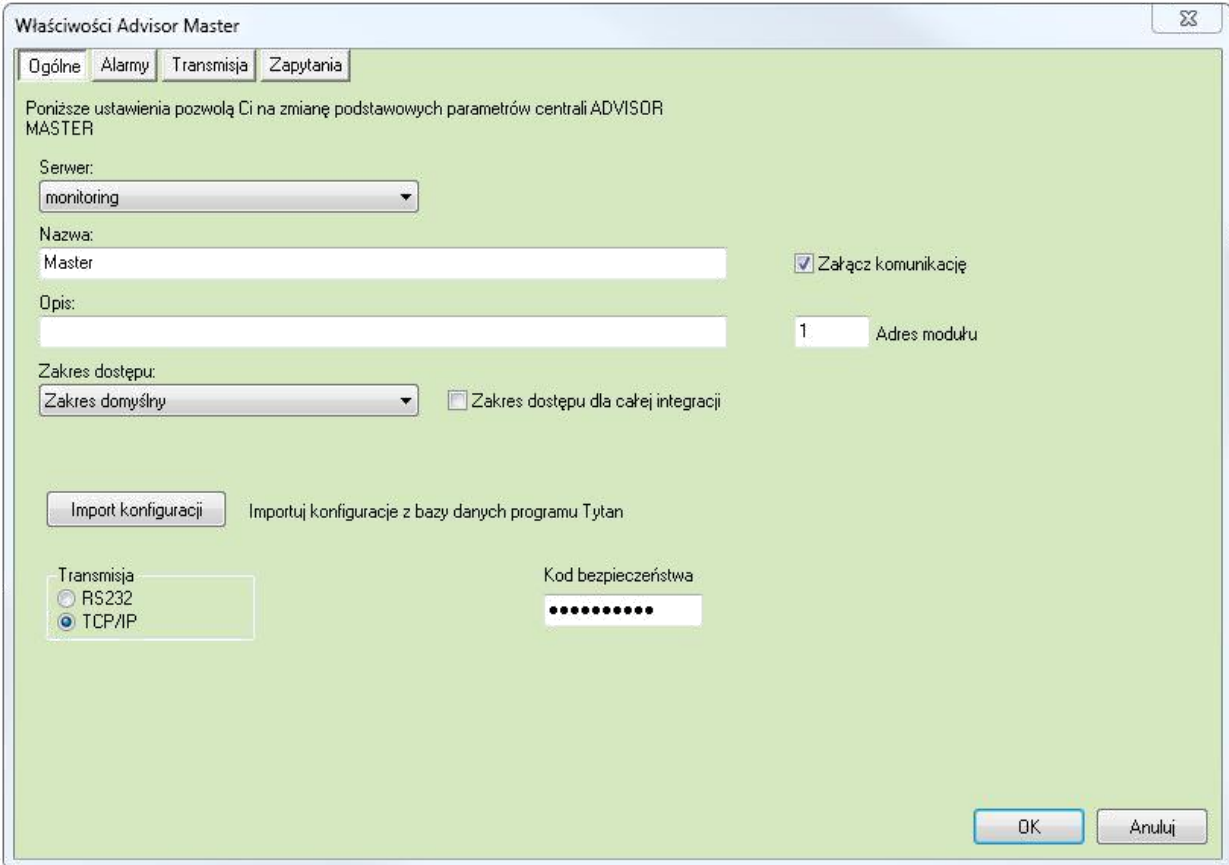
6.2. Tworzenie integracji UTC – Advisor Master

- Aby uruchomić EQU program Titan musi być zamknięty.
- Uruchamiamy EQU na prawach administratora.
- Logujemy się do programu za pomocą operatora Ifter.
- Po uruchomieniu EQU dodajemy integrację UTC – Advisor Master. W tym celu klikamy kolejno: Start → Eksplorator → Integracja → Dodaj 
- Otworzy nam się okno, w którym wybieramy integrację UTC – Advisor Master po czym klikamy Dalej >
- W kolejnym oknie wybieramy Serwer integracji, a następnie Dalej >
- Wpisujemy kod bezpieczeństwa i klikamy Dalej >, a następnie Zakończ
- Utworzy nam się nowa integracja Master

6.3. Ustawienie połączenia w programie EQU

Aby w EQU prawidłowo skonfigurować połączenie z integracją UTC – Advisor Master należy:

- a) Wejść do właściwości integracji **Master** (**Start** → **Eksplorator** → **Integracja** →  **właściwości**)
- b) W otwartym oknie ustawić **Adres modułu** taki jaki jest ustawiony na stronie modułu **ATS1806** w zakładce **Panel Physical address**.



Właściwości Advisor Master

Ogólne Alarmy Transmisja Zapytania

Poniższe ustawienia pozwolą Ci na zmianę podstawowych parametrów centrali ADVISOR MASTER

Serwer:
monitoring

Nazwa:
Master

Opis:

Zakres dostępu:
Zakres domyślny

Załącz komunikację

1 Adres modułu

Zakres dostępu dla całej integracji

Import konfiguracji Importuj konfiguracje z bazy danych programu Tytan

Transmisja
 RS232
 TCP/IP

Kod bezpieczeństwa
●●●●●●●●

OK Anuluj

- c) W polu Transmisja wybieramy **TCP/IP**
- d) Następnie otwieramy zakładkę **Transmisja**

Właściwości Advisor Master

Ogólne Alarmy **Transmisja** Zapytania

Poniższe ustawienia pozwolą Ci na zmianę parametrów konfiguracji TCP/IP wykorzystywanego do transmisji danych pomiędzy IFTER EQU, a centralą alarmową Master.

192 168 0 100 Adres IP

3001 Port wysyłania

3001 Port odbioru

OK Anuluj

e) W tym miejscu ustawiamy **Adres IP** centrali oraz **porty wysyłania i odbioru**, tak jak jest to ustawione w programie **TITAN** oraz module komunikacyjnym (**Admin** → **Połączenia** →

Właściwości Advisor Master

Ogólne Alarmy **Transmisja** Zapytania

Poniżej należy wybrać o stan jakich elementów program ma odpytywać centrale.

Obszary Wyjścia MZD
 Linie Drzwi

Poniżej należy ustawić maksymalny czas przesyłania pakietu przez centrale. Im dłuższy czas tym centrala wolniej się komunikuje ale transmisja jest stabilniejsza. Jeżeli będą się pojawiać błędy transmisji należy czas wydłużyć.


Szybko Ustawiono: 100 Wolno

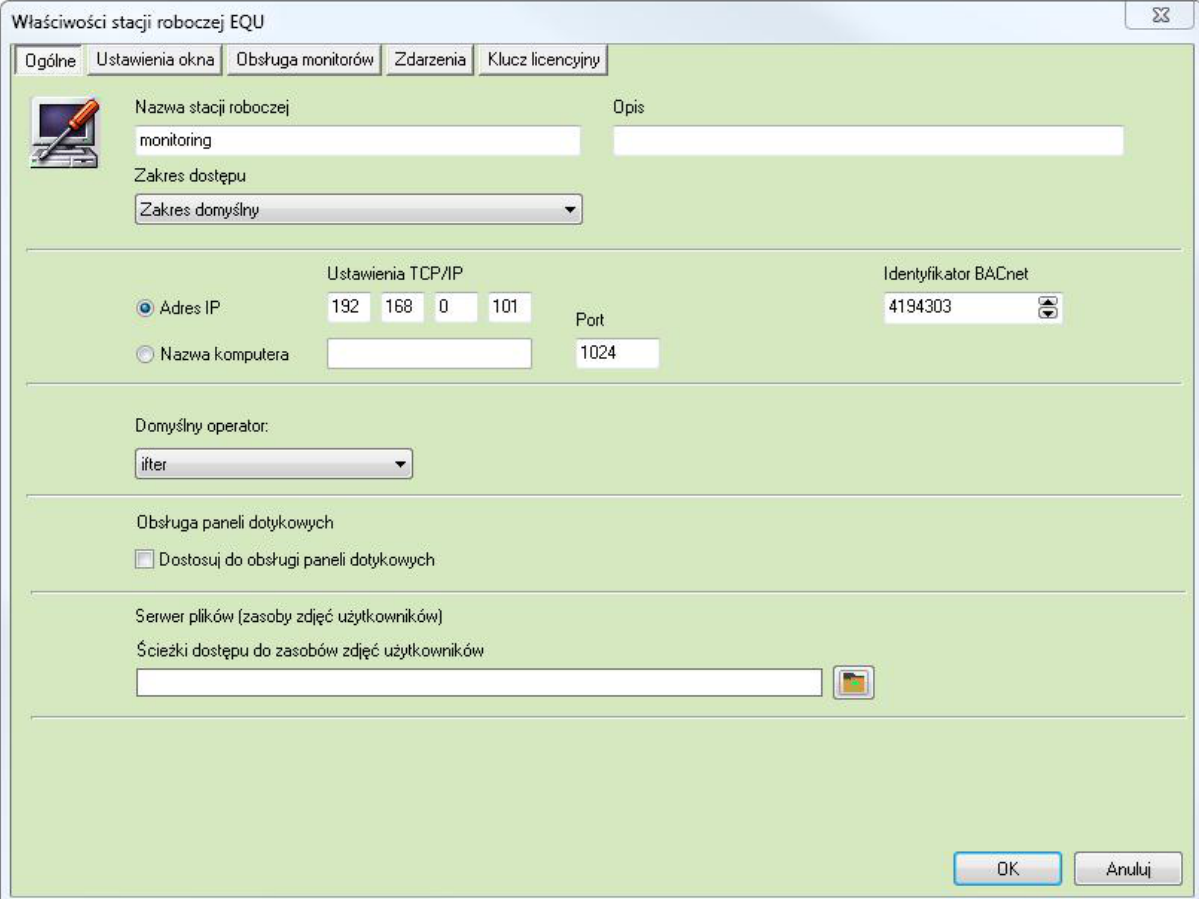
1 20

Liczba błędów transmisji:
0

OK Anuluj

IP (ATS1806)). Następnie przechodzimy na zakładkę **Zapytania** i wybrać o stan jakich elementów program ma odpytywać centralę.

- f) Naciskamy **OK**, aby zatwierdzić zmiany.
- g) W drzewku EQU rozwijamy gałązkę **Sieć IFTER EQU**, po czym wybieramy stację roboczą z którą wybraliśmy jako serwer integracji we właściwościach integracji, a następnie wchodzimy do jej  **właściwości**.
- h) W otwartym oknie w polu **Adres IP** wpisujemy adres IP komputera, z którym będzie się łączyła centrala. Ten adres musi się też zgadzać z ustawieniem na stronie modułu **ATS1806** w zakładce **Central Station parameters** oraz **fizycznym adresem komputera z zainstalowaną aplikacją**.



Właściwości stacji roboczej EQU

Ogólne Ustawienia okna Obsługa monitorów Zdarzenia Klucz licencyjny

Nazwa stacji roboczej: monitoring Opis:

Zakres dostępu: Zakres domyślny

Ustawienia TCP/IP

Adres IP: 192 168 0 101 Port: 1024

Nazwa komputera:

Identyfikator BACnet: 4194303

Domyślny operator: ifter

Obsługa paneli dotykowych

Dostosuj do obsługi paneli dotykowych

Serwer plików (zasoby zdjęć użytkowników)

Ścieżki dostępu do zasobów zdjęć użytkowników:


OK Anuluj

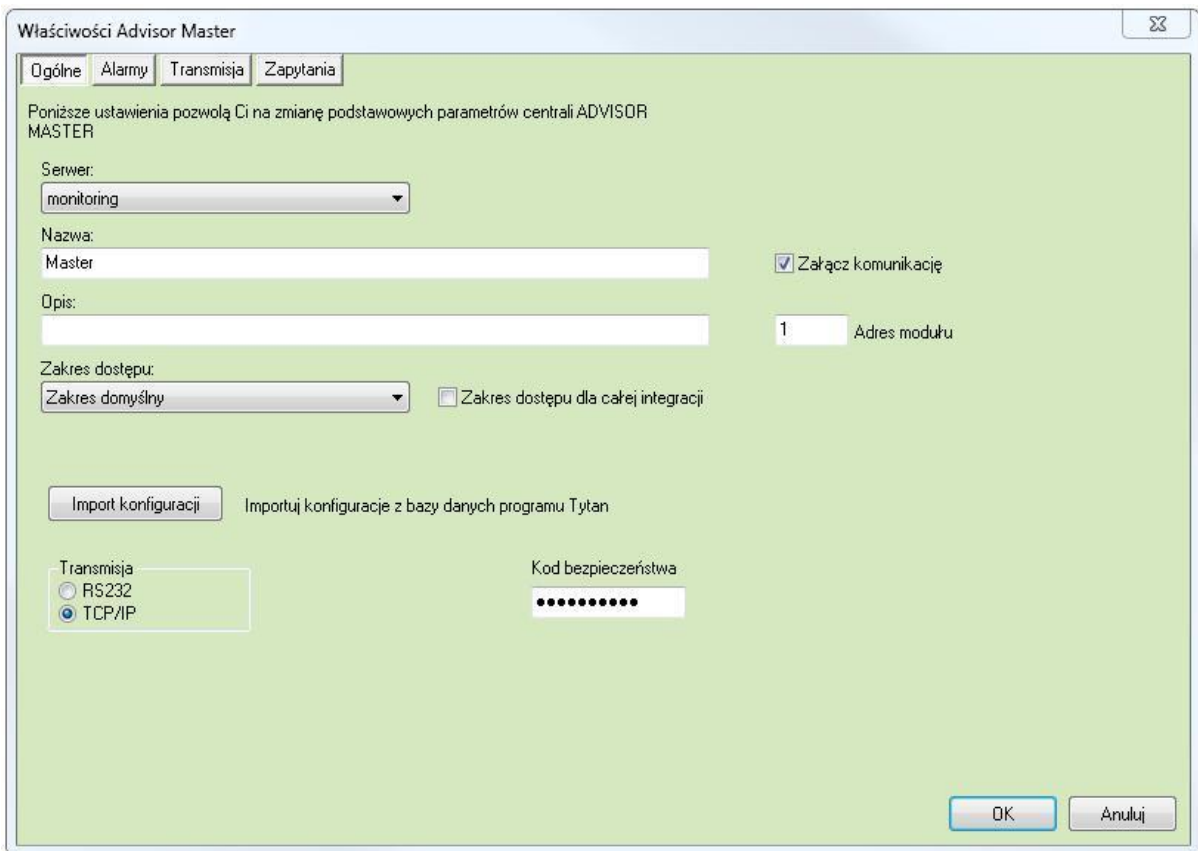
Zatwierdzamy zmiany przyciskiem OK.

- i) Wyłączamy, a następnie włączamy **EQU**, aby rozpocząć komunikację.

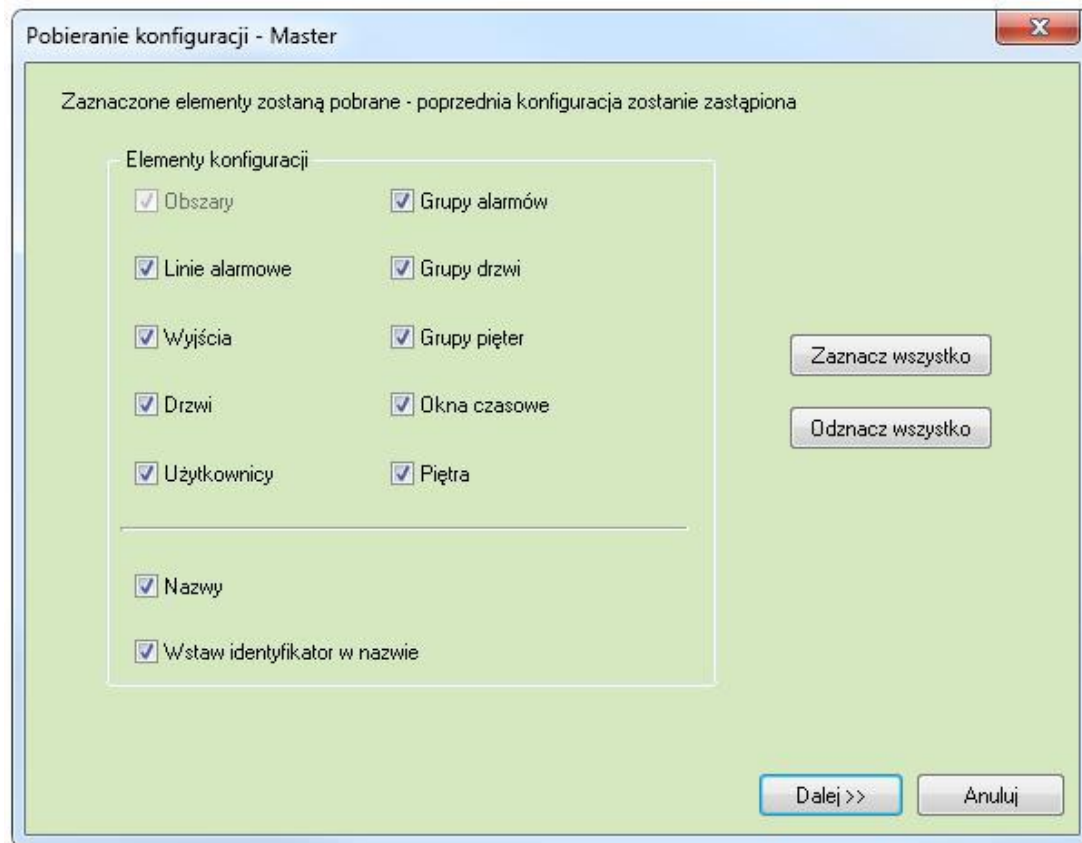
6.4.Import konfiguracji

Uwaga: Przed importem konfiguracji należy prawidłowo ustawić połączenie we właściwościach integracji w EQU wg punktu nr 3.

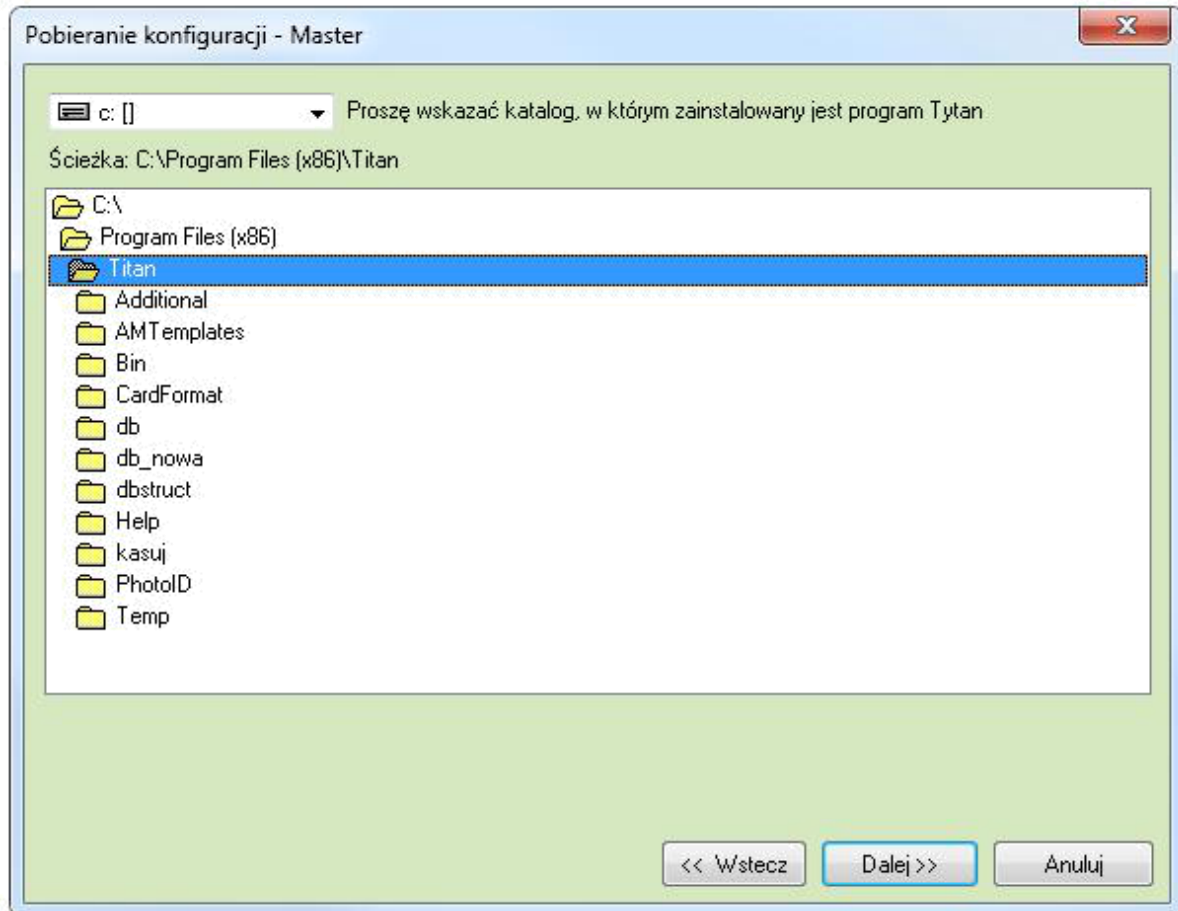
- a) Po wyłączeniu programu TITAN i uruchomieniu **EQU** na prawach administratora i dodaniu do systemu integracji **UTC – Advisor Master**, należy w drzewku EQU;
- b) wybrać gałązkę **Master**, a następnie otworzyć  **właściwości** tej integracji , po czym otworzy nam się poniższe okno:



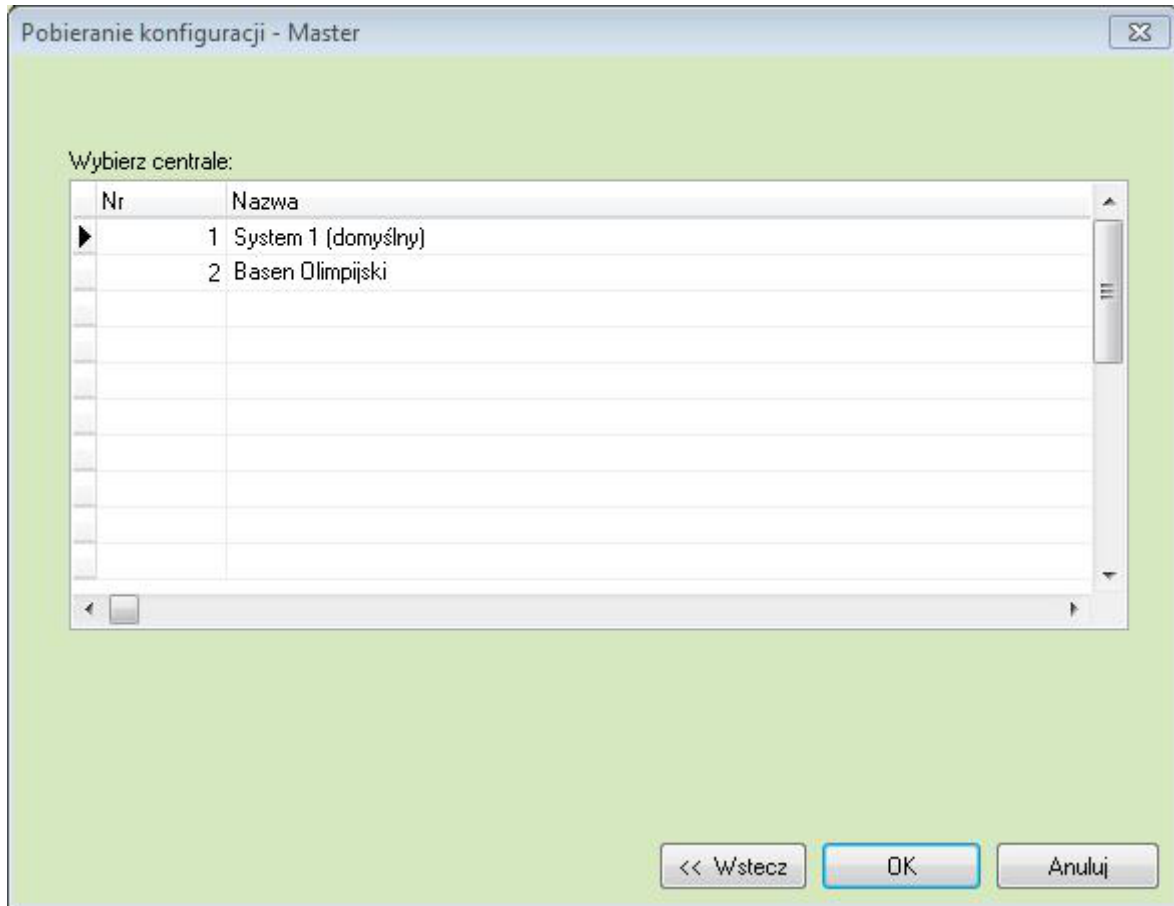
- c) Należy kliknąć przycisk **Import konfiguracji**. W oknie, które się wyświetli, zaznaczyć wszystko i kliknąć przycisk **Dalej**,



- d) Wskazać katalog z programem Titan i kliknąć przycisk **Dalej** (Uwaga: katalog ten musi być kompletny),



e) Z listy należy zaznaczyć system, z którego zaimportowana zostanie konfiguracja centrali,



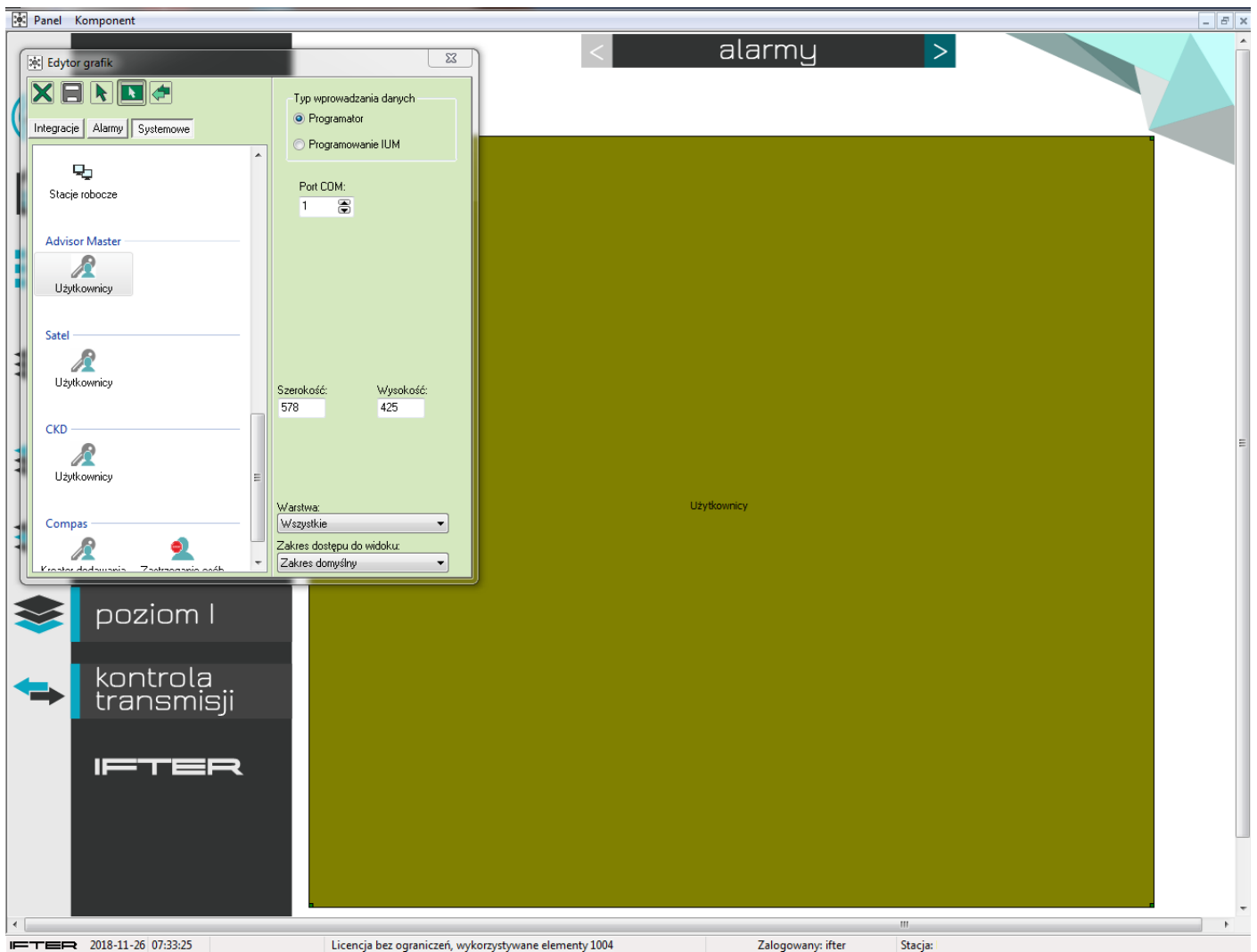
- f) Kliknąć **OK**, aby zaimportować konfigurację.
- g) Sprawdzamy, czy zaimportowały się wszystkie potrzebne elementy integracji.
- h) Wyłączamy, a następnie włączamy **EQU**, aby rozpocząć komunikację.


7. Komponent Użytkownicy – Advisor Master

7.1. Umieszczanie komponentu na grafice

Aby umieścić komponent Użytkownicy na grafice:

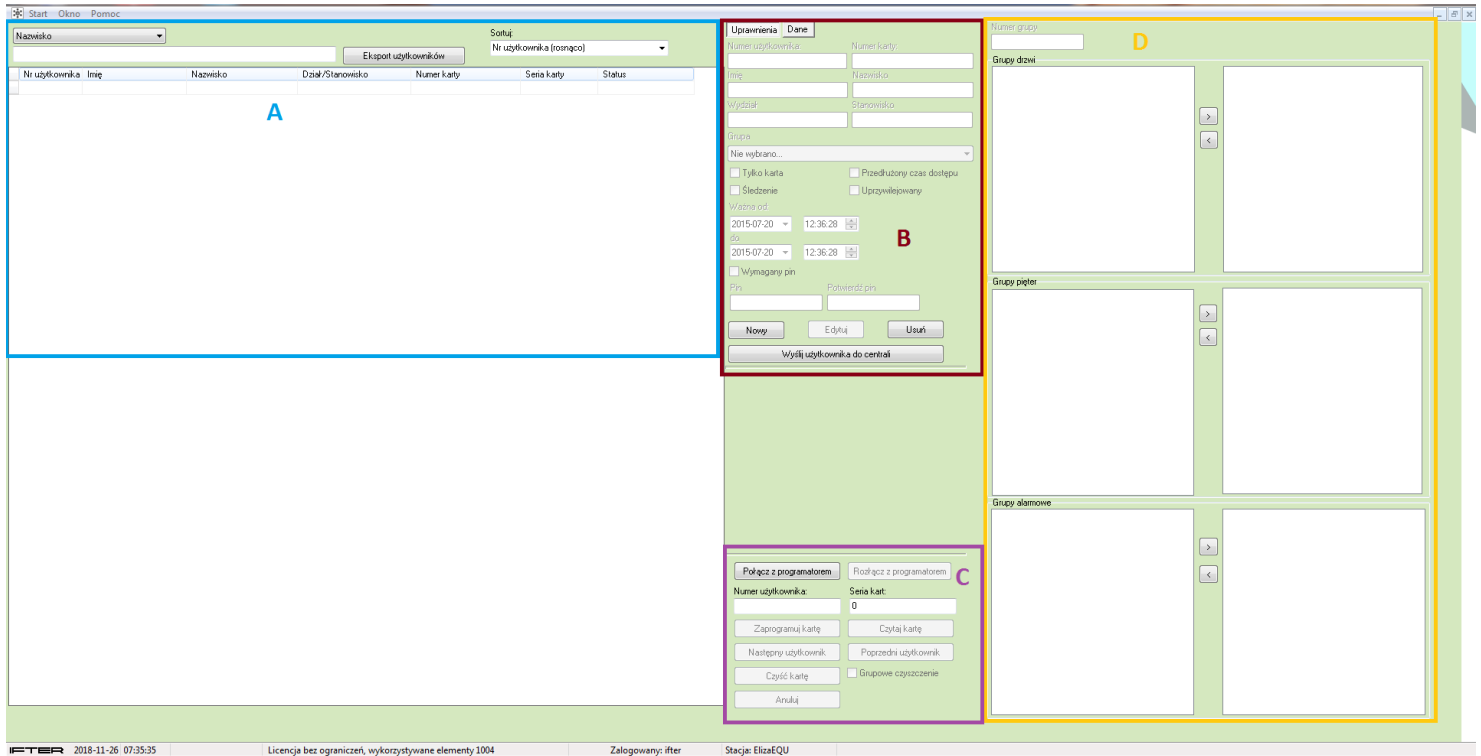
- a) należy po wejściu w **Edytor grafik** przejść w zakładkę **Systemowe**,
- b) zakładce tej spośród komponentów wybieramy **Advisor Master- Użytkownicy** i ustalamy:
 - Tryb wprowadzania danych,
 - Port COM, jeśli wybraliśmy typ **Programator**,
 - Centralę alarmową i Urządzenie, jeśli wybraliśmy typ **Programowanie IUM**,
 - Rozmiar komponentu na grafice,
 - Warstwę,
 - Zakres dostępu widoku.
- c) Umieszczamy komponent klikając lewym przyciskiem myszy na daną grafikę. Komponent po odtworzeniu grafiki będzie dopasowany automatycznie do wielkości okna.



d) Po umieszczeniu komponentu zapisujemy zmiany przyciskiem  **Zapisz.**

7.2. Wygląd i funkcje komponentu na wizualizacji

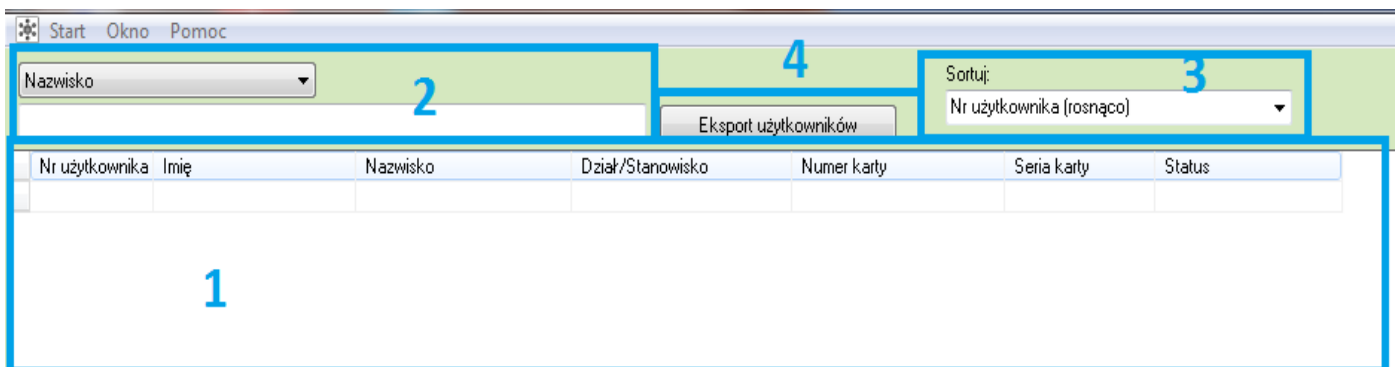
Komponent Użytkownicy umożliwia wyświetlanie panelu kontroli dostępu oraz uprawnień wybranych użytkowników w integracji Advisor Master. Pozwala na zarządzanie uprawnieniami Użytkowników i kart w centrali włamaniowej.



Panel komponentu Użytkownicy

A)

Po włączeniu danej grafiki wizualizacji widzimy nowe okno. Po lewej stronie znajduje się pole z listą osób przypisanych do integracji Advisor Master [1]. Nad listą znajduje się pole do wyszukiwania danych osób [2]. Osoby mogą być wyszukiwane według Numeru użytkownika, Nazwiska, Działu/Stnowiska lub Numeru karty. Możemy również dokonać sortowania



wyników [3], a także eksportować Użytkowników z listy do zewnętrznego pliku [4]. Eksportowana lista zostanie zapisana w formacie .CSV .

B)

Zakładka Uprawnienia

W środkowej części okna widnieją dane Użytkownika wraz jego uprawnieniami [1]:

- Numer użytkownika,
- Numer karty,
- Imię,
- Nazwisko,
- Wydział,
- Stanowisko,
- **Grupa** – grupa użytkowników.

Poniżej znajdują się okienka [2], które umożliwiają ograniczanie lub udzielanie uprawnień kartom Użytkowników:

Śledzenie - wszystkie funkcje alarmów i dostępu wykonywane przez użytkownika będą powodować wysłanie komunikatu związanego ze śledzeniem użytkownika do systemu TITAN.

Tylko karta Użytkownik NIE będzie uprawniony do korzystania z kodu PIN. Umożliwia to używanie pola kodu PIN do programowania kart w formatach, które zazwyczaj nie są zgodne centralą Advisor MASTER, w przypadku korzystania ze specjalnego czytnika.

Uprzywilejowany - Kod/karta użytkownika będzie zastępować wszystkie ograniczenia „Antipassback”.

Dostęp poszerzony - Użytkownik będzie uprawniony do rozszerzenia przedziałów czasowych odblokowania drzwi np. dłuższy czas otwarcia drzwi w przypadku osób niepełnosprawnych.

Możemy zmieniać datę ważności karty z dokładnością co do godziny w polu [3].

Wymagany PIN [4]– zaznaczamy, czy przejścia będą obsługiwane dodatkowo za pomocą obowiązkowego kodu PIN. Wpisujemy kod składający się z co najmniej 4 znaków, po czym potwierdzamy go wpisując go ponownie.

Opcje zarządzania Użytkownikami [5]:

Nowy – umożliwia dodanie nowego Użytkownika- wybranie tej opcji aktywuje pola z danymi Użytkownika, dając możliwość ich edycji;

Edytuj – po wybraniu Użytkownika z listy po lewej strony, mamy możliwość edycji danej osoby;

Usuń – opcja umożliwia usunięcie zaznaczonego na liście Użytkownika;

Wyślij użytkownika do centrali – wysyła dodanego lub edytowanego Użytkownika do urządzenia. Jest to bardzo ważne, aby po zakończeniu edycji wysłać użytkownika do centrali, ponieważ samo dodanie go do listy nie oznacza, że znajdzie się w urządzeniu.

Zakładka Dane

W tej zakładce mamy możliwość dodania lub usunięcia zdjęcia z Danych użytkownika [1]. Znajduje się tu również okienko umożliwiające podgląd dodanego zdjęcia [2]. Zaznaczamy płeć użytkownika [3], wpisujemy numer ewidencyjny [4] oraz dodajemy dodatkowe informacje [5]. Przycisk OK potwierdza wprowadzone dane, Anuluj- anuluje je.

C)

W zależności od określonego wcześniej typu programowania, pole programatora może się różnić wyglądem i funkcjami

Typ wprowadzania danych - Programator

Połącz z programatorem – łączy kartę z wcześniej określonym programatorem;

Rozłącz z programatorem – rozłącza kartę z programatorem;

Numer użytkownika – numer danego użytkownika;

Seria kart – seria kart użytkownika;

Zaprogramuj kartę – umożliwi zaprogramowanie karty;

Czytaj kartę – umożliwi odczytanie karty;

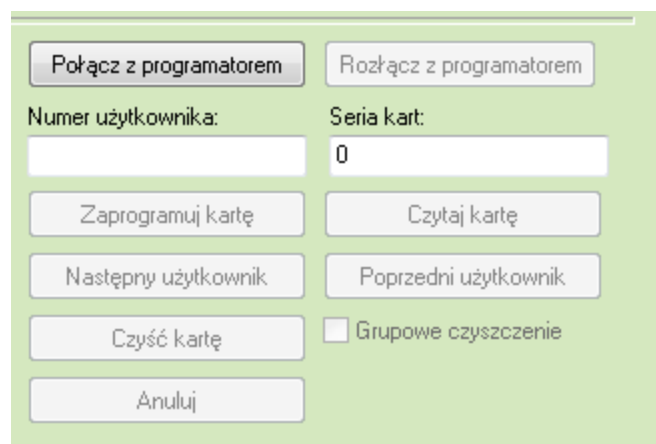
Następny użytkownik – wybiera kolejnego użytkownika z listy;

Poprzedni użytkownik – wybiera poprzedniego użytkownika z listy;

Czyść kartę – usuwa dane z karty;

Anuluj – anuluje proces;

Grupowe czyszczenie – usuwa dane z karty wszystkich Użytkowników.



Typ wprowadzania danych – Programowanie IUM

Zczytany numer karty – wyświetla numer karty, który został sczytany przez programator;

Przypisz numer karty użytkownikowi - przypisuje numer karty użytkownikowi.



D)

Po prawej stronie okna znajdują się pola umożliwiające zarządzanie dostępem do poszczególnych obszarów oraz alarmów:

- grupy drzwi;
- grupy pięter;
- grupy alarmowe.

Grupy te możemy dodawać i edytować wchodząc w drzewko EQU w zakładkę Integracja → Master. W tym miejscu możemy również sprawdzić jaki numer mają dane grupy. Po tym numerze możemy wyszukiwać je w polu **Numer grupy**[1]

Listy po lewej stronie [2] zawierają grupy dostępne do wyboru a listy po prawej [3] zawierają grupy wybrane, do których dostęp został przydzielony.

Pośrodku znajdują się strzałki [4], służące do przenoszenia grup z jednego okna do drugiego.

