Dokumentacja techniczna

COTER-EC

Wersja dokumentu: coter-ec-man-pl
Data ostatniej modyfikacji: 2012-07-30
Obowiązuje od wersji oprogramowania v1.04.x.x

Spis treści

Spis tabel

Indeks ilustracji

1 Wstęp

Urządzenie COTER-EC służy do konwersji sygnałów przenoszonych poprzez sieć Ethernet na sygnały interfejsu szeregowego CAN 2.0B. Urządzenie jest w stanie komunikować się jednocześnie ze 112 urządzeniami podłączonymi do tej samej magistrali. Maksymalna prędkość transmisji magistrali wynosi 1Mbit/s. Konwerter wspiera automatyczną obsługę ramek RTR (Remote Transmit Request).

Urządzenie posiada oprogramowany tryb pracy automatycznego rozszerzenia ramki interfejsu CAN 2.0B na ramki protokołu NX-CAN w celu współpracy z innymi urządzeniami firmy NETRONIX zwłaszcza tych projektowanych z przeznaczeniem do pracy w systemie kontroli dostępu NACS.

Urządzenie posiada:

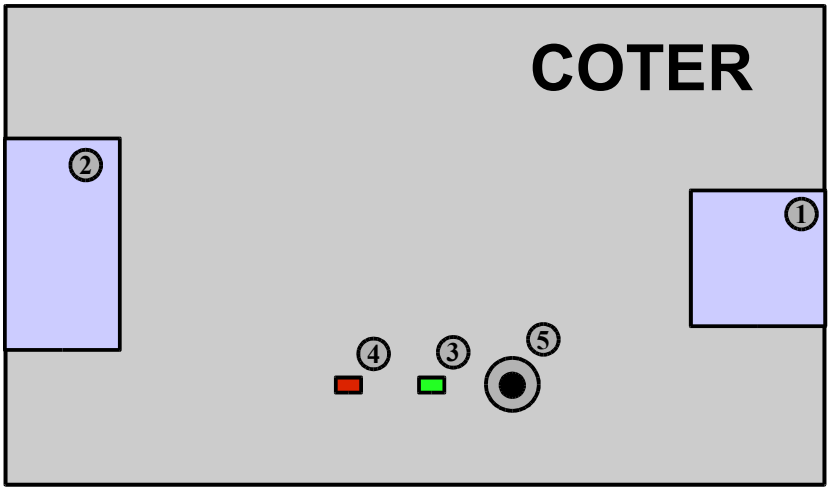
- Interfejs Ethernet 100Mbit/s.
- Interfejs szeregowy CAN 2.0B konfigurowalny do 1Mbps.
- Dioda LED zielona stanu świadcząca o zasilaniu urządzenia.
- Dioda LED czerwona statusu świadcząca o aktywności na interfejsie szeregowym.
- Przycisk powrotu do ustawień fabrycznych.

Urządzenie ma zaimplementowane:

- Serwer WWW umożliwiający konfigurację, zdalny reset oraz podgląd stanu urządzenia.
- Klient DHCP.
- Wsparcie protokołu NBNS.
- Mechanizm odnajdowania urządzeń w sieci z dynamicznym przypisywaniem ustawień sieciowych.
- Serwer konwersji TCP ↔ CAN 2.0B.
- Serwer TFTP do zdalnego przeładowywania firmware'u.
- Listę kontroli dostępu ACL do serwera WWW oraz serwera konwersji TCP ↔ CAN ograniczających dostęp do urządzenia tylko dla wybranych adresów IP.

2 Podłączenie oraz specyfikacja elektryczna

2.1 Elementy obudowy

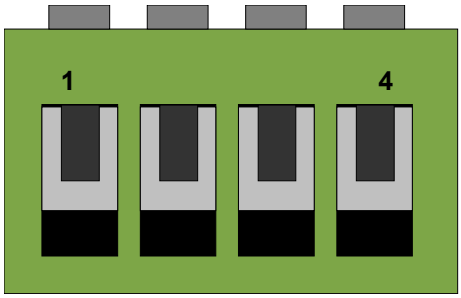


Ilustracja 1: Diagram elementów obudowy.

Tabela 1: Elementy obudowy.

Numer elementu	Nazwa	Opis
1	Gniazdo RJ45	Podłączenie do sieci Ethernet.
2	Gniazdo śrubowe kątowe.	Zasilanie, interfejs CAN.
3	LED - Zielona	Dioda sygnalizująca podłączenie zasilania.
4	LED - Czerwona	Dioda sygnalizująca aktywności na interfejsie szeregowym.
5	Przycisk Reset	Przycisk powrotu do ustawień fabrycznych.

2.2 Sygnały w gnieździe śrubowym urządzenia



Ilustracja 2: Złącze śrubowe widziane od strony frontu.

Tabela 2: Sygnały w gnieździe śrubowym.

Numer pinu	Nazwa	Opis
1	+V	Wejście zasilania
2	GND	Wejście zasilania
3	CAN_L	Linia niskiego potencjału magistrali CAN
4	CAN_H	Linia wysokiego potencjału magistrali CAN

2.3 Specyfikacja elektryczna

Tabela 3: Parametry elektryczne.

Nr	Symbol	Charakterystyka	Wartość			Jednostki	Komentarz
			Min.	Typ.	Maks.		
Parametry zasilania							
1	VPower	Napięcie zasilania	+8.0	-	+25.0	V	
2	IPower	Prąd zasilania	110	130	300	mA	W zależności od obciążenia interfejsu szeregowego oraz napięcia zasilania
Parametry interfejsu CAN							
5	Vcanh(r), Vcanl(r)	CANH, CANL napięcie recesywne linii	2.0	-	3.0	V	
6	Vcanh(d)	CANH dominujące napięcie wyjściowe	2.75	-	4.5	V	
7	Vcanl(d)	CANL dominujące napięcie wyjściowe	0.5	-	2.25	V	
8	Vdiff(r)(o)	Recesywne różnicowe napięcie wyjściowe	-500	-	+50	mV	
9	Vdiff(d)(o)	Dominujące różnicowe napięcie wyjściowe	1.5	-	3.0	V	
10	Vdiff(r)(i)	Recesywne różnicowe napięcie wejściowe	-1.0	-	+0.5	V	
11	Vdiff(d)(i)	Dominujace różnicowe napięcie wejściowe	0.9		5.0	V	
12	Rdiff	Różnicowa rezystancja wejściowa	20	-	100	kΩ	

3 Pierwsze uruchomienie

Urządzenie dostarczane jest z ustawieniami fabrycznymi, w których ustawienia fabryczne interfejsu Ethernet mają następujące wartości.

Tabela 4: Ustawienia fabryczne interfejsu sieciowego.

Nazwa parametru	Opis parametru	Wartość
MAC	Adres fizyczny urządzenia.	00:04:A3:XX:XX:XX(1)
Host Name	Nazwa sieciowa urządzenia.	COTER-EC-V1
DHCP	Klient serwera dynamicznej konfiguracji sieciowej.	Włączony
IP Address	Adres sieciowy.	10.0.0.205(2)
Gateway	Adres bramki sieciowej.	10.0.0.1(2)
Subnet Mask	Maska podsieci.	255.255.255.0(2)
Primary DNS	Adres pierwszego serwera DNS.	10.0.0.1(2)
Secondary DNS	Adres drugiego serwera DNS.	10.0.0.1(2)

Uwaga:

(1) – Unikalna wartość adresu MAC dla każdego z urządzeń i nie może zostać zmieniona podczas procesu konfiguracji.

(2) – Ustawienie ważne gdy serwer DHCP nieaktywny w sieci, lub klient dynamicznej konfiguracji wyłączony.

Procedura nawiązywania połączenia z urządzeniem różni się w zależności od sieci, do której został podłączony.

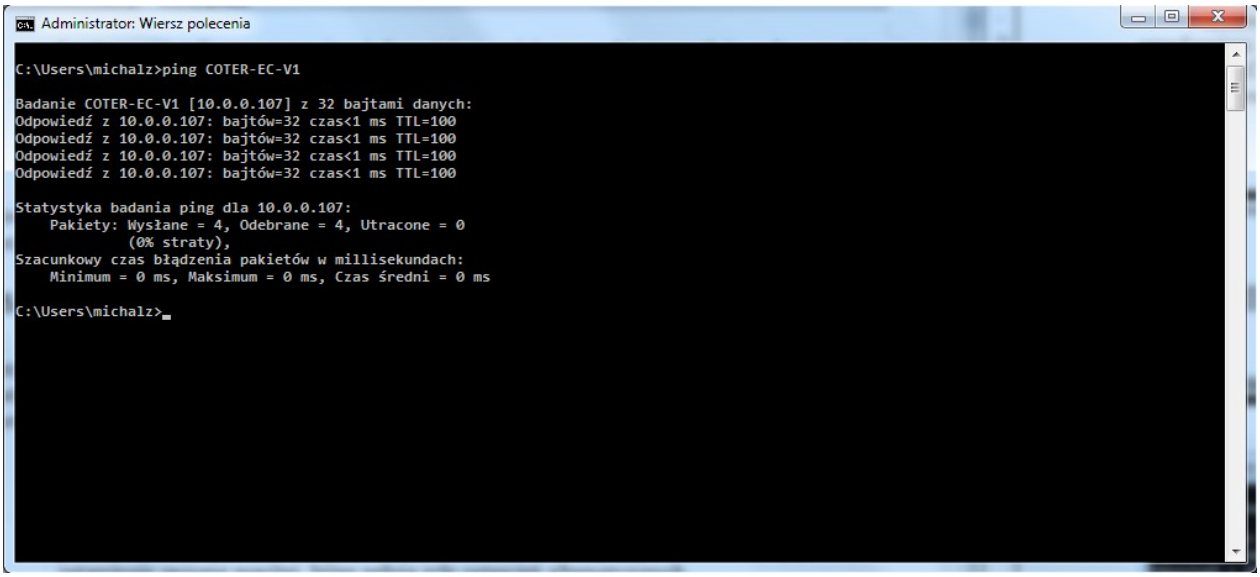
Jeśli urządzenie będzie wpięte do sieci Ethernet, która posiada aktywny serwer DHCP, wówczas należy podjąć dodatkowe kroki pozwalające na zlokalizowanie podłączonego urządzenia w sieci. Jeśli sieć którą dysponujesz nie posiada aktywnego serwera DHCP lub połączenie sieciowe zestawione jest w sposób jeden do jednego z komputerem klasy PC wówczas możesz pominąć kolejny podpunkt „Wyszukiwanie urządzenia w sieci z aktywnym serwerem DHCP" należy jednak zadbać o to by ustawienia sieci były zgodne z ustawieniami urządzenia.

3.1 Wyszukiwanie urządzenia w sieci z aktywnym serwerem DHCP

W przypadku sieci, w której do czynienia mamy z dynamicznym przypisywaniem konfiguracji sieciowej urządzeń, nie jesteśmy w stanie przewidzieć jakie ustawienia zostaną nadane, bez definiowania dodatkowych reguł serwera nadającego ustawienia. Istnieją dwie metody weryfikacji adresu IP jaki posiada urządzenie.

3.1.1 Odniesienie do nazwy sieciowej urządzenia

Konwerter udostępnia usługę NetBios Name dzięki, której można nawiązać połączenie z urządzeniem przy pomocy jego nazwy sieciowej. Jeśli nazwa sieciowa jest znana (domyślna wartość to „COTER-EC-V1"), możliwe jest wysłanie pakietu ping z nazwą sieciową urządzenia, w celu odebrania informacji o przypisanym adresie IP.

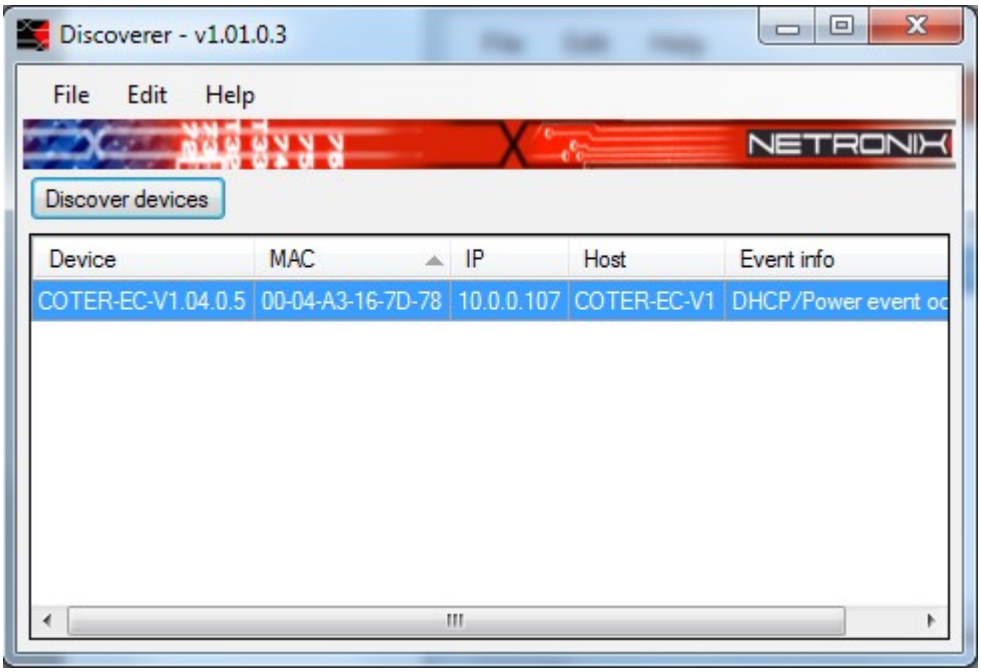


Ilustracja 3: Odpowiedź na zapytanie ping z nazwą hosta.

3.1.2 Odnajdywanie urządzenia przy pomocy programu Discoverer

Urządzenie posiada mechanizm szybkiego odnajdywania w sieci, dzięki czemu będziemy w stanie uzyskać nadany mu dynamicznie adres IP.

Aby móc zlokalizować konwerter należy posłużyć się programem Discoverer firmy NETRONIX. Program jest napisany na platformę .NET 3.5 i w przypadku starszej wersji platformy zgłosi on błąd uruchomienia. Należy więc upewnić się, iż platforma ta została zainstalowana na stanowisku, na którym program ma zostać uruchomiony.



Ilustracja 4: Program Discoverer.

Aby odszukać urządzenia firmy NETRONIX znajdujące się w sieci lokalnej należy lewym klawiszem myszy kliknąć na przycisk „Discover devices" znajdujący się w lewym górnym rogu okna programu. W tabeli okna programu zostaną wyświetlone wszystkie urządzenia sieciowe firmy NETRONIX aktywne w sieci. Na liście wykrytych urządzeń znajdują się takie informacje jak adres IP urządzenia, typ urządzenia adres fizyczny MAC oraz nazwa sieciowa urządzenia.

Jeśli poszukiwane urządzenie nie zgłasza swojej obecności, a urządzenie zostało podłączone poprawnie (dioda sygnalizująca podłączenie zasilania oraz zielona dioda LINK, znajdująca się na gnieździe RJ45 świecą się), może istnieć podejrzenie, że ustawienia sieciowe urządzenia zostały zmodyfikowane i nie pozwalają na poprawną propagację danych w sieci lokalnej.

Mechanizm odnajdywania urządzeń firmy NETRONIX w sieci został bliżej opisany w rozdziale „Mechanizm odnajdywania Discoverer".

3.2 Nawiązanie połączenia

Jeśli urządzenie posiada już znany adres IP można przystąpić do nawiązania połączenia. W tym celu należy otworzyć dowolną przeglądarkę internetową, a następnie w pasku adresu wprowadzić adres IP urządzenia lub jego nazwę sieciową.

W oknie przeglądarki wyświetlona zostanie strona domowa urządzenia, gdzie umieszczone są takie informacje jak wersja firmware'u, data kompilacji oraz informacje na temat monitorowanych urządzeń. W prawym górnym rogu strony domowej znajduję się link do strony logowania, przez którą można się dostać do panelu konfiguracyjnego urządzenia.

4 Mechanizm wyszukiwania Discoverer

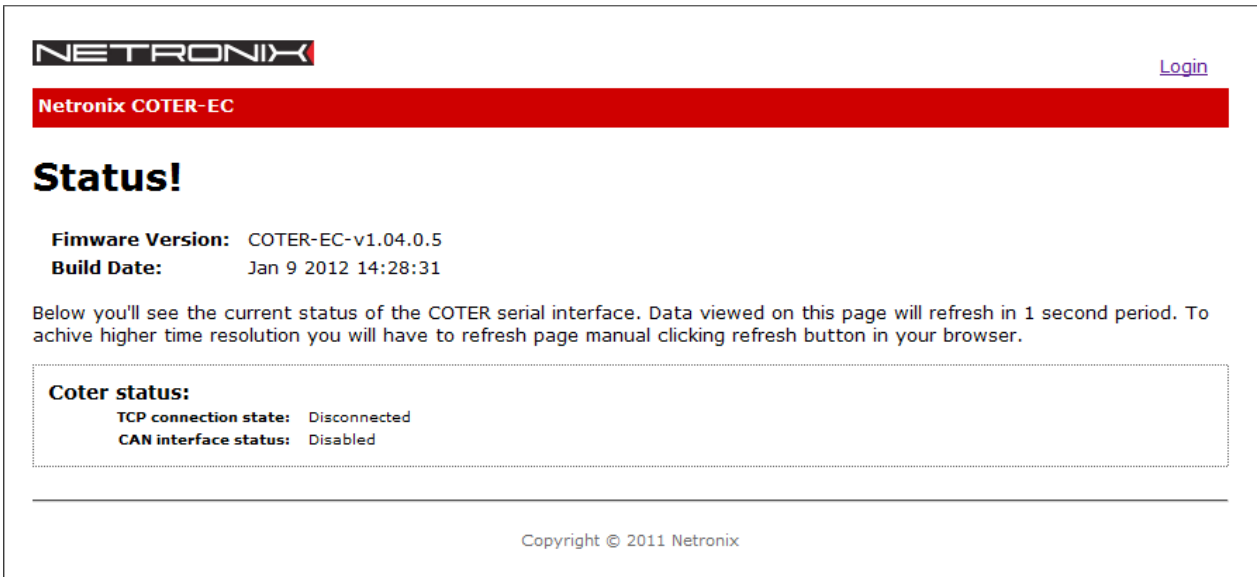
Zasada działania mechanizmu wyszukiwania urządzeń w sieci opiera się na ciągłym nasłuchiwaniu przez urządzenie komunikatów UDP na porcie 30303. W celu uzyskania informacji o urządzeniu wystarczy na wskazany port wysłać komunikat rozgłoszeniowy o treści „Discoverer" na początku pakietu danych. Po odebraniu takiego pakietu, urządzenia wysyłają odpowiedź UDP do nadawcy na port, z którego zapytanie zostało wysłane.

Urządzenie również jest w stanie samoistnie wysyłać rozgłoszeniowe komunikaty na port 30303 w przypadku wystąpienia dwóch zdarzeń:

- Reset urządzenia.
- W przypadku zmiany ustawień sieciowych na skutek odebrania od serwera DHCP nowych parametrów konfiguracyjnych.

Powyższe przypadki w programie Discoverer objawiają się poprzez dodanie informacji o zdarzeniu, które wywołało wysłanie pakietu.

Zaletą samoistnego wysyłania powiadomień o zaistnieniu zdarzeń jest fakt, iż nie istnieje konieczność ciągłego odpytywania urządzenia, a komunikaty są wysyłane rozgłoszeniowo, dzięki czemu są w stanie dotrzeć do programów nasłuchujących nawet w przypadku błędnie skonfigurowanych ustawień sieciowych.



Ilustracja 5: Strona domowa.

5 Panel konfiguracyjny

W celu dokonania konfiguracji użytkownik musi przejść procedurę weryfikacji. Procedura ta jak i poszczególne panele konfiguracyjne urządzenia zostały opisane w kolejnych podpunktach rozdziału.

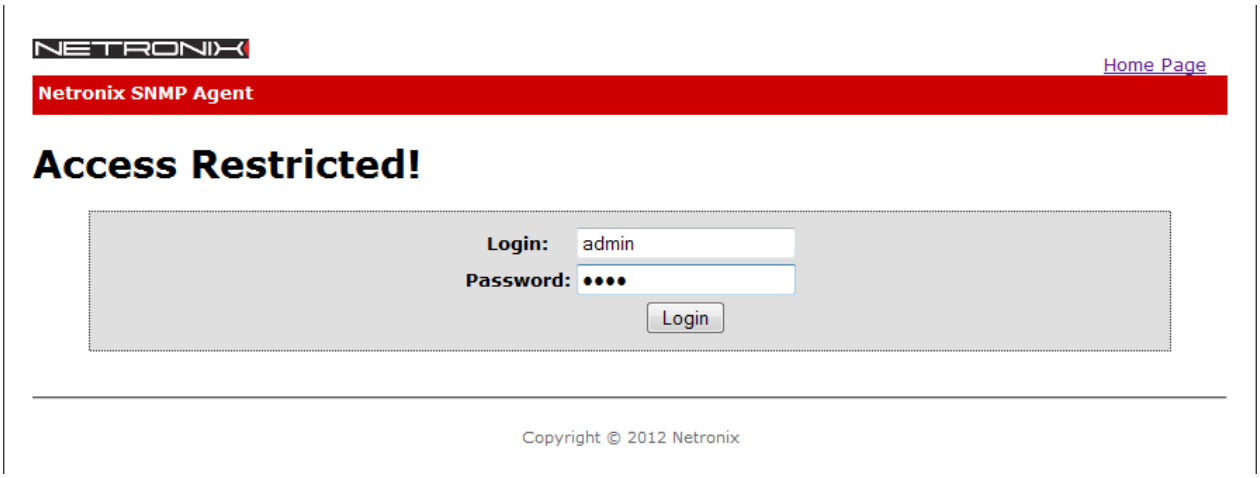
5.1 Logowanie do panelu administracyjnego

W celu dokonania konfiguracji użytkownik musi przejść procedurę weryfikacji. Panel konfiguracyjny zabezpieczony jest hasłem oraz nazwą użytkownika. Aby przejść do strony logowania należy:

- Na stronie domowej WWW urządzenia w prawym górnym rogu kliknąć na link „Login”.
- W polu adresu wpisać nazwę pliku „login.htm”.
- W polu adresu wpisać ścieżkę do dowolnego pliku znajdującego się w katalogu „protect” np: „protect/index.htm”. Serwer w momencie gdy stwierdzi, że przeglądarka, z której następuje próba dostania się do katalogu zastrzeżonego „protect” nie prześle wraz z zapytaniem aktualnego identyfikatora sesji, automatycznie przekieruje przeglądarkę na stronę logowania.

Tabela 5: Ustawienia fabryczne hasła oraz loginu.

Nazwa parametru	Wartość domyślna
Hasło	„1234”
Login	„admin”



Ilustracja 6: Formularz logogowania do panelu konfiguracyjnego.

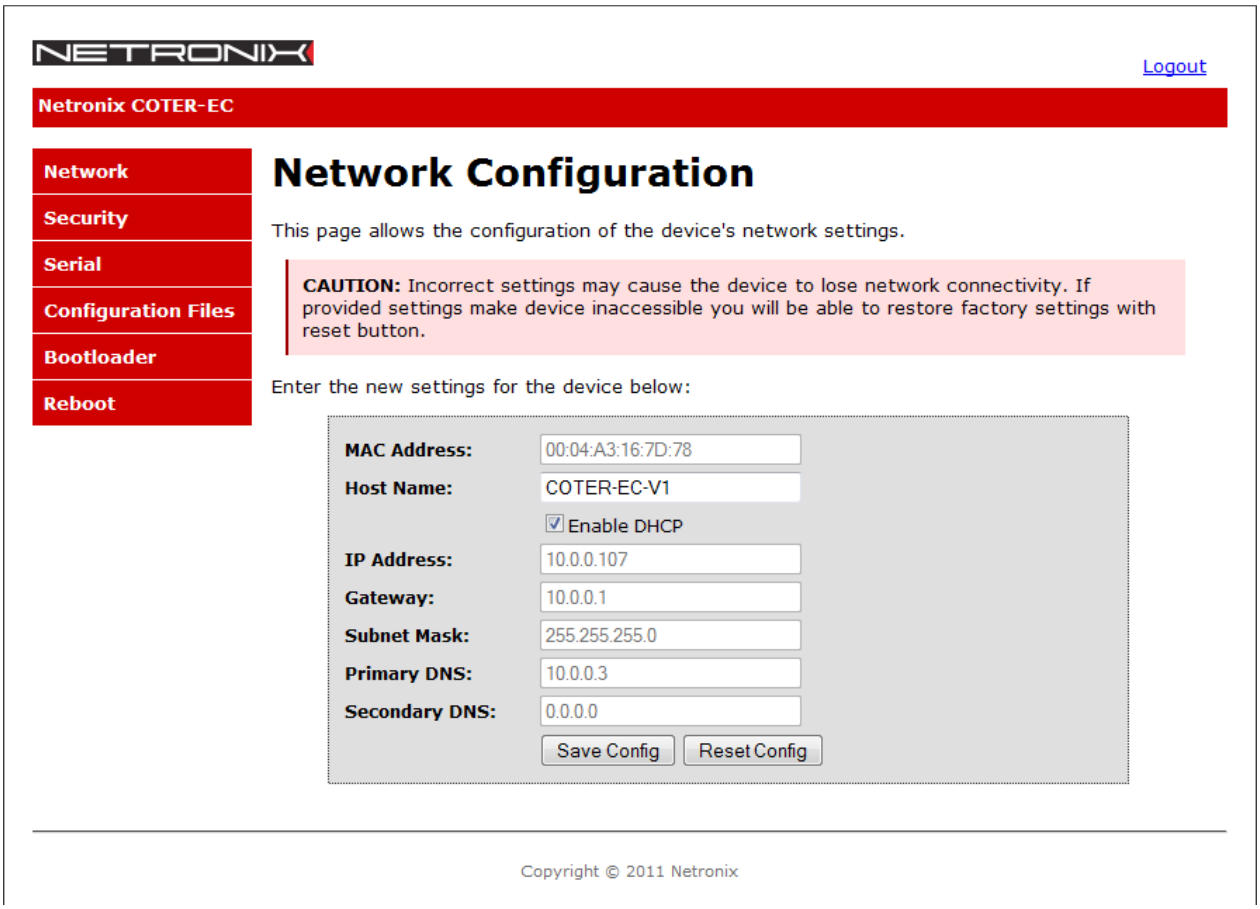
Jeśli użytkownik wprowadzi poprawnie hasło i login w formularzu strony logowania, serwer w odpowiedzi na zapytanie prześle identyfikator sesji oraz przekieruje przeglądarkę na stronę powitalną panelu konfiguracyjnego „protect/index.htm”.

Ilustracja 7: Strona powitalna panelu konfiguracyjnego.

W tym samym momencie zalogowana może być tylko jedna osoba, dlatego też istotne jest aby po zakończeniu pracy z panelem konfiguracyjnym zakończyć sesje przez kliknięcie linku „logout”. Jeśli sesja nie zostanie zamknięta poprawnie serwer zakończy sesję dopiero po minięciu maksymalnego czasu bezczynności. Czas ten może być ustawiany w zakładce „Security” panelu administracyjnego a jego domyślna wartość to 5 minut.

5.2 Konfiguracja ustawień sieciowych

Konfiguracji ustawień sieciowych dokonać można z zakładki „Network” panelu administracyjnego. Przed przystąpieniem do konfiguracji ustawień należy mieć pewność czy po zatwierdzeniu nowych ustawień będziemy w stanie ponownie połączyć się z urządzeniem. Jeśli wprowadzone ustawienia spowodują brak możności nawiązania połączenia, wówczas jeśli nie istnieje inny znany sposób można dokonać powrotu do ustawień fabrycznych jednak spowoduje to usunięcie również pozostałych zmian wprowadzonych w konfiguracji urządzenia.



Ilustracja 8: Panel konfiguracji ustawień sieciowych.

Tabela 6: Ustawienia fabryczne interfejsu sieciowego.

Nazwa parametru	Opis parametru	Wartość
MAC	Adres fizyczny urządzenia.	00:04:A3:XX:XX:XX(1)
Host Name	Nazwa sieciowa urządzenia.	COTER-EC-V1
DHCP	Klient serwera dynamicznej konfiguracji sieciowej.	Włączony
IP Address	Adres sieciowy.	10.0.0.205(2)
Gateway	Adres bramki sieciowej.	10.0.0.1(2)
Subnet Mask	Maska podsieci.	255.255.255.0(2)
Primary DNS	Adres pierwszego serwera DNS.	10.0.0.1(2)

Nazwa parametru	Opis parametru	Wartość
Secondary DNS	Adres drugiego serwera DNS.	10.0.0.1(2)

Uwaga:

(1) – Unikalna wartość adresu MAC dla każdego z urządzeń i nie może zostać zmieniona podczas procesu konfiguracji.

(2) – Ustawienie ważne gdy serwer DHCP nieaktywny w sieci, lub klient dynamicznej konfiguracji wyłączony.

W przypadku gdy serwer DHCP jest włączony, parametry znajdujące się w formularzu będą odpowiadać wartościom na których aktualnie pracuje urządzenie, uzyskanych od serwera. Czyli jeśli urządzenie pracowało do tej pory z aktywnym klientem DHCP oraz otrzymało konfigurację od serwera, ta konfiguracja zostanie przez urządzenie zwrócona do formularza. W przeciwnym wypadku, gdy klient DHCP jest wyłączony urządzenie zwróci parametry sieciowe, które są zapisane w pamięci nieulotnej i służą jako konfiguracja alternatywna w przypadku braku serwera DHCP w sieci.

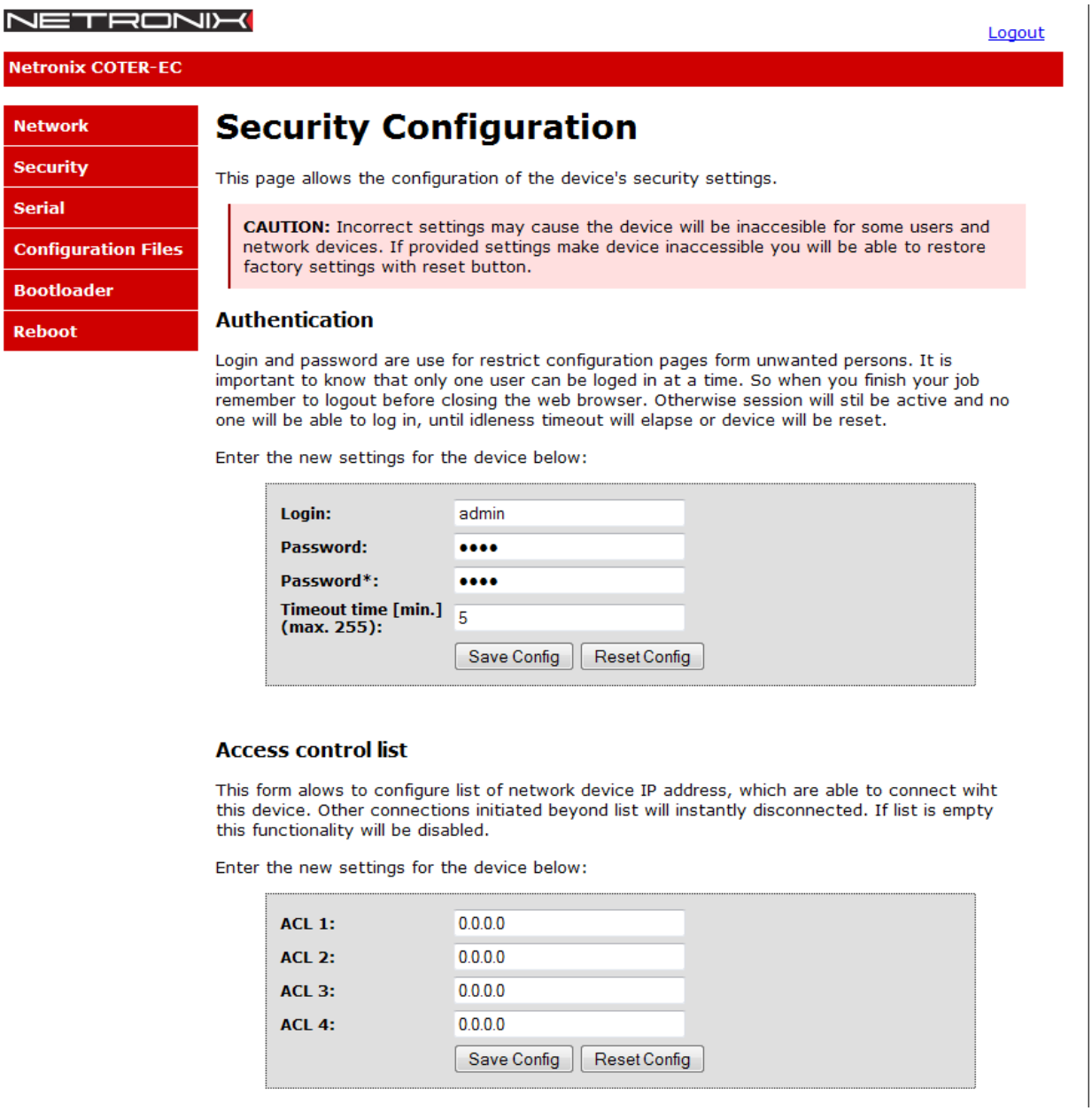
Przycisk „Reset Config" formularza przywraca wartości parametrów sprzed edycji.

Nowe ustawienia sieciowe będą obowiązywać dopiero przy kolejnym uruchomieniu urządzenia, dlatego, tuż po dokonaniu modyfikacji ustawień zalecane jest natychmiastowe wykonanie zdalnego resetu urządzenia.

5.3 Konfiguracja ustawień zabezpieczeń

Urządzenie posiada dwa poziomy zabezpieczeń przed niepowołanym dostępem. Pierwszym z nich jest ograniczenie dostępu do panelu konfiguracji na stronie WWW, poprzez wprowadzenie sesji uwierzytelniającej na podstawie loginu oraz hasła użytkownika. Drugim rodzajem zabezpieczeń jest lista ACL adresów IP, które są akceptowalne przez serwer WWW oraz serwer konwersji TCP ↔ CAN. Połączenia z adresów nie znajdujących się na wspomnianej liście są natychmiastowo odrzucane zaraz po nawiązaniu połączenia. Sprawdzanie adresów z listy ACL można dezaktywować nadając wszystkim adresom IP, znajdującym się na liście ACL wartości zerowe „0.0.0.0". Lista ACL nie ogranicza połączeń z serwerem SNMP, gdyż ten posiada własną listę adresów NMS, które mogą mieć dostęp do danych zgromadzonych w bazie MIB.

Konfiguracja ustawień zabezpieczeń dostępna jest w zakładce „Security" panelu konfiguracyjnego. Nowe parametry należy wprowadzać z rozwagą, aby nie ograniczyć sobie dostępu do panelu konfiguracyjnego. W przypadku takiej sytuacji konieczne może być przywrócenie ustawień fizycznych urządzenia.



Ilustracja 9: Panel konfiguracji ustawień zabezpieczeń.

Górny formularz panelu służy do konfiguracji parametrów sesji uwierzytelniającej użytkownika. Wprowadzenie oraz zapisanie ustawień tego formularza wprowadzi zmiany natychmiastowo bez konieczności resetu urządzenia.

Tabela 7: Ustawienia fabryczne parametrów sesji.

Nazwa parametru	Opis parametru	Wartość domyślna
Login	Nazwa użytkownika.	„admin”(1)
Password	Hasło użytkownika.	„1234”(1)
Password*	Potwierdzenie nowego hasła.	-
Timeout time	Czas bezczynności sesji, po którym sesja zostanie	5 minut

Nazwa parametru	Opis parametru	Wartość domyślna
	automatycznie zamknięta, jeśli w panelu konfiguracyjnym nie są wykonywane żadne czynności.	

Uwaga:
(1) - Maksymalnie 8 znaków.

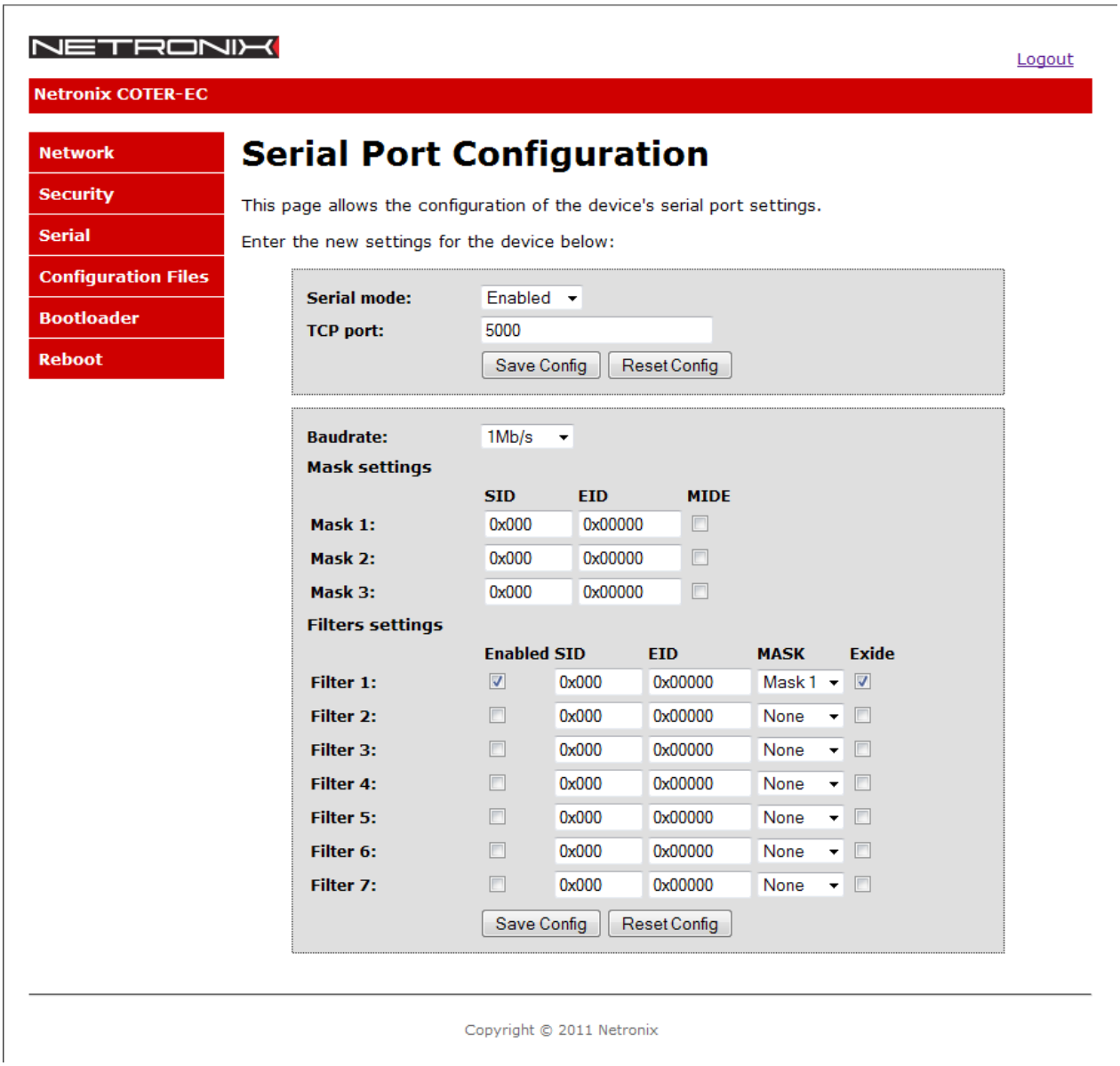
Dolny formularz panelu służy do konfiguracji ustawień listy kontroli dostępu. Zmodyfikowane i zapisane parametry wejdą w życie w momencie kolejnego resetu urządzenia.

Tabela 8: Ustawienia fabryczne parametrów listy dostępu ACL.

Nazwa parametru	Opis parametru	Wartość domyślna
ACL1	Adres IP hosta 1, które może nawiązać połączenie z urządzeniem.	0.0.0.0
ACL2	Adres IP hosta 2, które może nawiązać połączenie z urządzeniem.	0.0.0.0
ACL3	Adres IP hosta 3, które może nawiązać połączenie z urządzeniem.	0.0.0.0
ACL4	Adres IP hosta 4, które może nawiązać połączenie z urządzeniem.	0.0.0.0

5.4 Konfiguracja interfejsu szeregowego

Ustawienia interfejsu szeregowego na stronie konfiguracyjnej są ustawieniami z którymi interfejs szeregowy CAN jest aktywowany w momencie, gdy połączenie z portem konwersji zostanie otwarte. Ustawienia te mogą zostać zmienione w każdym momencie trwania połączenia z konwerterem przy pomocy specjalnych ramek sterujących opisanych w rozdziale dotyczącym protokołu serwera konwersji.



Ilustracja 10: Panel konfiguracji ustawień interfejsu szeregowego.

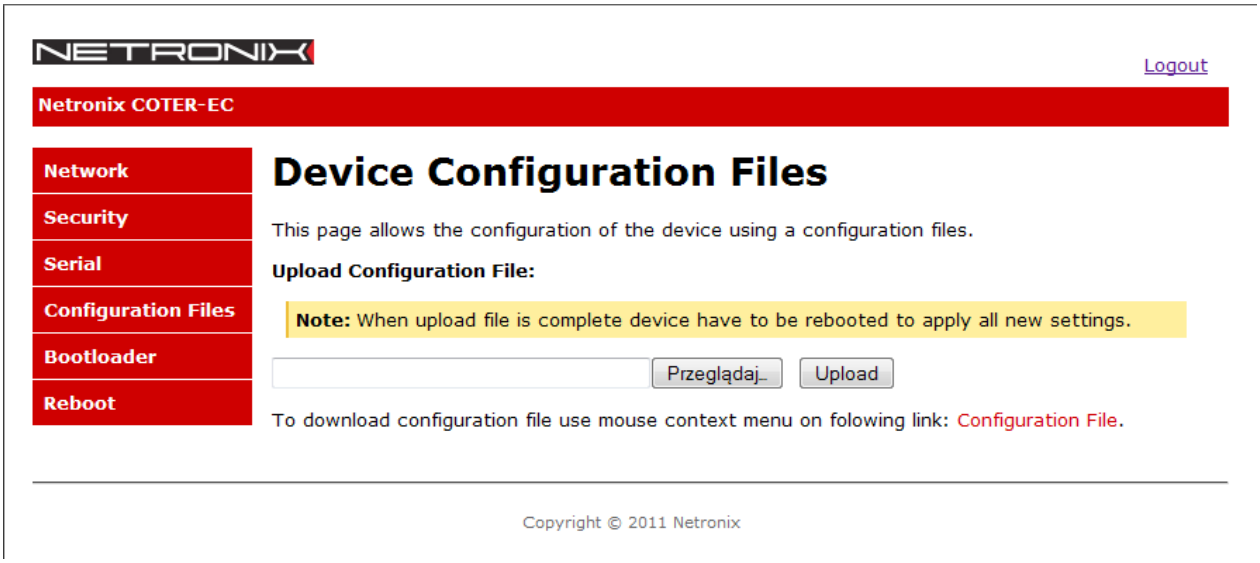
Aby ramka CAN została odebrana przez konwerter należy ustawić odpowiednie filtry, na podstawie których ramki mają być wychwytywane. Ramka CAN wychwytywana jest przez interfejs konwertera w momencie gdy pola bitowe identyfikatora SID/EID są zgodne z polami bitowymi aktywnych filtrów. Przypisanie maski do danego filtru skutkuje załączeniem lub ignorowaniem pola identyfikatora w zależności czy bit na odpowiedniej pozycji maski ma wartość 1 (pole rozpatrywane) lub 0 (pole ignorowane). Ustawienie maski w której wszystkie pola bitowe posiadają wartość 0 powoduje, że wszystkie ramki transmitowane poprzez magistrale CAN będą zgodne ze zdefiniowanym filtrem. Jeśli flaga MIDE jest aktywna rozpatrywane będą wyłącznie ramki rozszerzone gdy EXIDE aktywne lub standardowe gdy EXIDE nieaktywne. W przypadku gdy MIDE nieaktywne flaga EXIDE jest ignorowana a konwerter będzie rozpatrywał ramki o identyfikatorze standardowym jak i rozszerzonym. W

konfiguracji domyślnej konwerter posiada ustawienia początkowe umożliwiające odbiór każdej ramki przesyłanej przez magistrale CAN.

5.5 Plik konfiguracyjny

Konfigurację urządzenia można zapisać do pliku w celu późniejszego użycia do konfiguracji kolejnego urządzenia. W zakładce „Configuration Files" znajduje się formularz dzięki któremu można pobrać jak i zapisać plik z wszystkimi ustawieniami konfiguracyjnymi urządzenia.

Dostęp do pliku konfiguracyjnego możliwy jest z panelu administracyjnego w zakładce „Configuration Files".



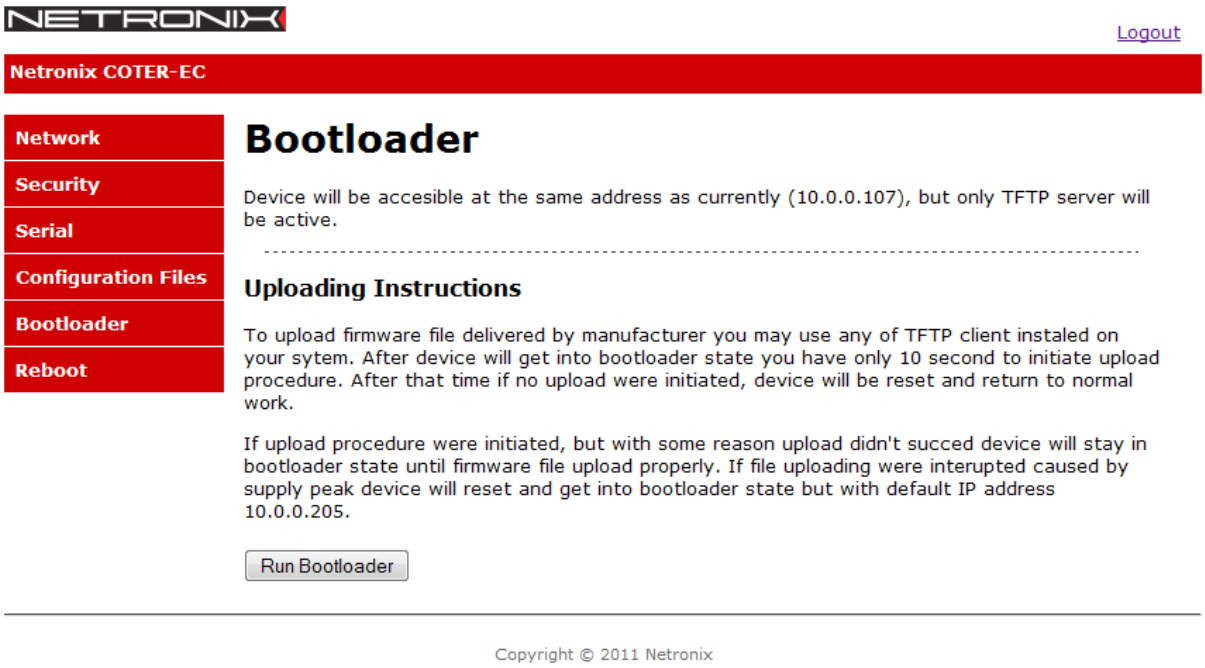
Ilustracja 11: Panel zapisu oraz odczytu pliku konfiguracyjnego.

6 Zmiana firmware'u

Urządzenie posiada możliwość zdalnego przeładowywania firmware'u przy pomocy klienta TFTP. W celu przeładowania frimware'u należy w panelu administracyjnym przejść do zakładki „Bootloader". Przycisnąć przycisk „Run Bootloader", znajdujący się na samym dole panelu. Od tego momentu urządzenie porzuci dalsze wykonywanie normalnego programu i na kolejne 10 sekund przejdzie w tryb pracy bootloadera. Jeśli przez 10 sekund ładowanie nowego firmware'u nie zostanie zainicjowane urządzenie wyjdzie z tego trybu i powróci do trybu normalnej pracy. Gdy bootloader jest uruchamiany aplikacja przekazuje mu adresy sieciowe, na których pracowała do tej pory. Zachowanie te jest istotne w przypadku dynamicznego przypisywania adresów IP w sieci.

Do wysłania nowego firmware'u można wykorzystać dowolnego klienta TFTP dostępnego z linii komend większości systemów. W przypadku Windows 2000/XP przykład takiego wywołania to:
`TFTP 10.0.0.205 put coter.nhex`. Jeśli procedura przeładowywania firmware'u zostanie zainicjowana urządzenie pozostanie w stanie bootloadera, aż do pomyślnego zapisania nowego programu. Po zakończeniu zapisu urządzenie wychodzi z booloadera i przechodzi do wykonywania nowego programu.

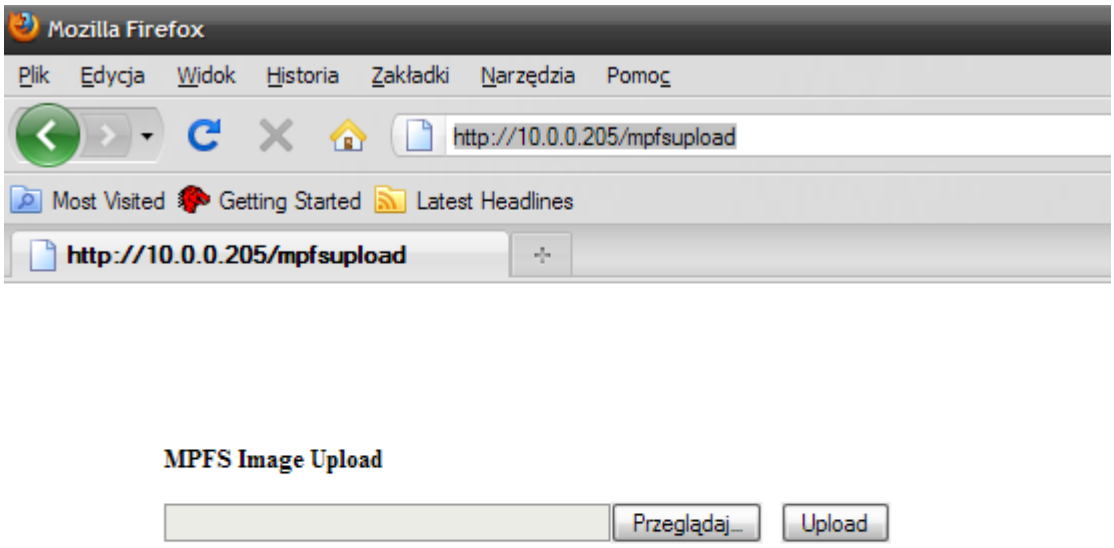
Gdy połączenie zostanie z niewiadomych przyczyn przerwane a zapis nie będzie zakończony, można ponownie podjąć próbę zapisu nowego programu. W przypadku, gdy przyczyną przerwy w transmisji pliku jest zanik napięcia, lub po nieudanym zapisie użytkownik postanowi zresetować urządzenie, konwerter ponownie przejdzie w tryb pracy bootloadera, lecz jego ustawienia sieciowe pozostaną zmienione na fabryczne, czyli IP 10.0.0.205 oraz adres MAC 00:04:A3:00:00:00. W przypadku urządzeń z unikalnym adresem MAC również nastąpi zmiana ze względu na odrębność aplikacji bootloader'a od aplikacji docelowej. Bootlader nie posiada dostępu do pamięci, gdzie przechowywany jest unikalny adres MAC więc może zaistnieć konieczność zresetowania tablicy ARP systemu, gdy nastąpi taka okoliczność.



Ilustracja 12: Panel aktywujący bootloader.

7 System plików

Konwerter posiada wbudowany system plików, w którym przechowywane są takie dane jak, struktura bazy MIB, pliki strony WWW oraz inne pliki skryptowe konieczne do poprawnego sterowania urządzeniem. Pliki te przechowywane są na zewnętrznej pamięci EEPROM, dlatego też nie mogą być jednocześnie przeładowywane podczas wgrywania nowego firmware'u. Aby przeładować system plików na nowy należy w pasku adresu przeglądarki wpisać adres urządzenia oraz „mpfsupload" np.: http://10.0.0.205/mpfsupload. W oknie przeglądarki zostanie wyświetlony formularz przy pomocy, którego można dokonać zapisu obrazu nowego systemu plików.



Ilustracja 13: Formularz zapisu systemu plików.

Należy podkreślić, że nie każda zmiana firmware'u musi wiązać się z koniecznością zmiany systemu plików. Jest to wymagane wyłącznie, gdy skrypty CGI wykonywane podczas wyświetlania stron różnią się od tych, które zostały użyte w poprzedniej wersji. System plików posiada sygnaturę, która świadczy o konieczności dokonania zapisu zgodnego obrazu plików dla aktualnej wersji firmware'u. Jeśli sygnatura aplikacji nie jest zgodna z wersją obrazu wówczas objawiać się to będzie komunikatami „File not Found" w przypadku próby otwarcia strony WWW.

8 Przywracanie ustawień fabrycznych

W przypadku, gdy dostarczone urządzenie posiada zmodyfikowane ustawienia oraz istnieje problem z nawiązaniem połączenia, użytkownik może przywrócić znane ustawienia fabryczne. Aby tego dokonać należy przy pomocy szpilki wcisnąć przycisk Reset ukryty pod obudową urządzenia i przytrzymać przez około 5 sekund. Urządzenie zasygnalizuje rozpoczęcie procedury czyszczenia aktualnych ustawień poprzez zaświecenie się diody statusu (czerwona). W tym momencie można już zwolnić przycisk. Urządzenie dokona zapisu ustawień fabrycznych a następnie zostanie zresetowane.

9 Opis protokołu sterującego serwerem konwersji

Opisywany w niniejszym rozdziale protokół komunikacyjny umożliwia sterowanie parametrami transmisji interfejsu CAN, jak również służy do wysyłania oraz odbierania danych przesyłanych na magistrali.

9.1 Budowa ramki

IAC	CMD	LEN	ID	DATA (+ OP_CODE)

Tabela 9: Budowa ramki sterującej.

Pole	Liczba bajtów	Znaczenie	Zakres zmienności
IAC	1	Początek komendy sterującej.	255
CMD	1	Kod komendy sterującej. Bit MSB jeśli aktywny świadczy o ramce odpowiedzi.	0 – 126 – Kody komend. 128 – 254 – Kody odpowiedzi.
LEN	1	Długość pola danych.	0 - 91
ID	2	Losowo wygenerowany identyfikator ramki. Wartość 0 zarezerwowana dla ramek wygenerowanych przez konwerter nie będących odpowiedzią na zapytanie.	0 – 2^16-1
DATA	0 - 90	Parametry komendy. W przypadku gdy ramka jest odpowiedzią ostatni bajt danych jest kodem wykonania komendy zwracanym przez serwer.	Zakres zmienności bajtu.

Tabela 10: Opis pól ramki sterującej.

Kod IAC (255) zawarty w ramce jest kodem rozpoczynającym interpretacje ramki jako komenda sterująca. W przypadku gdy w ramce np. w polu danych istnieje konieczność przesłania wartości 255 wartość ta musi być powielona w następnym transmitowanym bajcie ramki. Powielenia wartości 255 w polu danych nie powodują zwiększenia się wartości pola LEN. Pojedyncze wystąpienia wartości 255 w strumieniu danych transmitowanych do konwertera poprzez port TCP/IP traktowane będzie jako rozpoczęcie nowej komendy sterującej.
W przypadku ramki odpowiedzi na wysłaną komendę serwer konwertera zwróci ramkę z identyfikatorem ramki (ID) identycznym z tym zawartym w wysyłanym zapytaniu oraz zgodnym kodem komendy (CMD). W polu kodu komendy zostanie ustawiona flaga odpowiedzi czyli wartość pola będzie powiększona 128 w stosunku do wartości kodu zapytania. Do danych zapytania zostanie dodany dodatkowy bajt statusu wykonania operacji czyli wartość w polu długości danych (LEN) będzie powiększona o 1. W przypadku gdy serwer wysyła ramkę nie będącą odpowiedzią na zapytanie lecz informacją wygenerowaną przez zdarzenie np. odczytu ramki z interfejsu CAN, identyfikator ramki (ID) przyjmuje wartość 0 oraz flaga odpowiedzi w polu komendy (CMD) jest aktywna.

Komenda	Kod komendy	Kod odpowiedzi
Echo	0x00	0x80
Wersja firmware'u	0x01	0x81
Wyślij dane	0x03	0x83
Odebrane dane	0x04	0x84
Ustaw prędkość transmisji	0x05	0x85
Ustaw filtr	0x06	0x86
Ustaw maskę	0x07	0x87
Ustaw tryb pracy	0x08	0x88

Tabela 11: Kody komend.

Kod operacji	Opis
0x00	Operacja została poprawnie wykonana
0x01	Nieznana komenda
0x02	Błąd składni komendy
0x03	Błąd parametrów komendy
0x04	Bufor transmisji pełny

Tabela 12: Kody operacji.

9.2 Opis komend

9.2.1 Komenda „Echo”

Komenda ta służy wyłącznie do weryfikacji poprawności transmisji z serwerem. Na wysłane zapytanie z kodem komendy „Echo” konwerter odpowie ramką z danymi umieszczonymi w zapytaniu dodając kod wykonania komendy.

IAC	CMD	LEN	ID	DATA
0xFF	0x00	0x05	0x1234	0xAA 0xBB 0xCC 0xDD 0xEE

Tabela 13: Przykładowa ramka komendy "echo".

IAC	CMD	LEN	ID	DATA
0xFF	0x80	0x06	0x1234	0xAA 0xBB 0xCC 0xDD 0xEE + kod operacji

Tabela 14: Odpowiedź konwertera na przykładową ramkę komendy "echo".

9.2.2 Wersja oprogramowania

Komenda ta służy do weryfikacji wersji firmware'u konwertera.

IAC	CMD	LEN	ID	DATA
0xFF	0x01	0x00	0x1234	-

Tabela 15: Przykładowa ramka komendy sprawdzenia wersji oprogramowania.

IAC	CMD	LEN	ID	DATA
0xFF	0x81	0x13	0x1234	„COTER-EC-v1.04.0.5” + kod operacji

Tabela 16: Odpowiedź konwertera na przykładową ramkę zapytanie o wersje oprogramowania.

9.2.3 Transmisja ramki na magistrale CAN

W celu wysłania danych na magistralę CAN należy posłużyć się specjalnym formatem danych opisującym wszystkie niezbędne dane do wysłania pakietu na magistralę.

Numer bajtu	Znaczenie
1	Flagi specyficzne dla pakietów interfejsu CAN2.0B. Bit <0 – LSB> EXIDE – Flaga świadcząca o transmisji na magistralę pakietu o rozszerzonym identyfikatorze ramki. Bit <1> RTR – Flaga wymuszająca wysłanie na magistralę ramki z załączoną flagą Remote Transmission Request. Gdy flaga ustawiona dane zamieszczone w ramce pakietu są ignorowane zgodnie ze standardem CAN2.0B. Bit <4..7>(2) - Numer filtru do którego odebrana ramka została przypasowana.
2	Liczba bajtów danych transmitowanych w pakiecie.
3 – 6(1)	Bity <28..18> Standardowy identyfikator pakietu CAN. Bity <17..0> Rozszerzony identyfikator ramki CAN.
7 – 15	Bajty danych.

Tabela 17: Dane do transmisji na magistralę CAN w trybie normalnej pracy.

Uwaga:
(1) – Bity bardziej znaczące transmitowane w pierwszej kolejności.
(2) – Ustawiany przez konwerter w momencie odbioru ramki z interfejsu CAN. W przypadku transmisji na magistralę szeregową bity te są ignorowane.

Numer bajtu	Znaczenie
1	Bajt ignorowany
2	Liczba bajtów danych transmitowanych w pakiecie.
3 – 6(1)(2)	Bit <28> Zawsze zerowy. Bit <27> Flaga komendy. Bity <26..18> Kod komendy NXCAN. Bity <17..0> Identyfikator urządzenia NXCAN.
7 – 96	Bajty danych.

Tabela 18: Dane do transmisji na magistralę CAN w trybie pracy ze wsparciem protokołu NXCAN.

Uwaga:
(1) – Bity bardziej znaczące transmitowane w pierwszej kolejności.

(2) – W celu bliższego zapoznania się z protokołem NXCAN należy zapoznać się z dokumentacją protokołu dostępną na stronie firmy Netronix.

IAC	CMD	LEN	ID	DATA
0xFF	0x03	0x0E	0x1234	0x01 08 12 34 56 78 01 02 03 04 05 06 07 08

Tabela 19: Przykładowa ramka komendy wysłania ramki na magistrale CAN.

IAC	CMD	LEN	ID	DATA
0xFF	0x83	0x0F	0x1234	0x01 08 12 34 56 78 01 02 03 04 05 06 07 08 + kod operacji

Tabela 20: Odpowiedź konwertera z potwierdzeniem umieszczenia ramki w buforze nadawczym magistrali CAN.

9.2.4 Odbiór ramki z magistrali CAN

Komenda ta służy wyłącznie do odbierania danych odebranych przez konwerter z magistrali CAN. Podobnie jak w przypadku transmisji ramki na magistralę CAN dane odebrane z magistrali zwracane są przez konwerter w odpowiednim formacie (patrz wyżej).

IAC	CMD	LEN	ID	DATA
0xFF	0x84	0x13	0x00000	Bajty ramki CAN lub NXCAN + kod operacji

Tabela 21: Ramka informującą o odebraniu przez konwerter ramki danych z magistrali CAN.

9.2.5 Ustalanie prędkości transmisji magistrali CAN

Komenda służy do ustalania prędkości transmisji magistrali szeregowej CAN.

IAC	CMD	LEN	ID	DATA
0xFF	0x05	0x01	0x1234	BAUDRATE

Tabela 22: Przykładowa ramka komendy ustawiającej prędkość transmisji.

IAC	CMD	LEN	ID	DATA
0xFF	0x85	0x2	0x1234	BAUDRATE + kod operacji

Tabela 23: Odpowiedź konwertera na przykładową ramkę komendy ustawiającej prędkość transmisji.

Prędkość transmisji	Parametr BAUDRATE
1 Mbps	0
500 kbps	1
250 kbps	2
125 kbps	3
100 kbps	4
50 kbps	5
20 kbps	6

Tabela 24: Obsługiwane prędkości transmisji CAN.

9.2.6 Ustawienia filtrów

Komenda służy do konfiguracji filtru interfejsu CAN.

IAC	CMD	LEN	ID	DATA
0xFF	0x06	0x0F	0x1234	FILTER_NUM(0 – 6) FILTER_CONFIG_DATA

Tabela 25: Przykładowa ramka komendy ustawiającej filtr odbieranych ramek.

IAC	CMD	LEN	ID	DATA
0xFF	0x86	0x10	0x1234	FILTER_NUM(0 – 6) FILTER_CONFIG_DATA + kod operacji

Tabela 26: Odpowiedź konwertera na przykładową ramkę komendy ustawiającej filtr odbieranych ramek.

Numer bajtu	Znaczenie
1 – 4	Bity <28..18> Standardowy identyfikator pakietu CAN. Bity <17..0> Rozszerzony identyfikator ramki CAN.
5 – 12	Dane do automatycznego wysłania na magistralę CAN gdy ustawiona flaga RTR.
13	Liczba bajtów do wysłania w odpowiedzi na ramkę z flagą RTR.
14	Bit <1..0> Numer przypisanej maski do filtra: 0 – przypisano maskę 1 1 – przypisano maskę 2 2 – przypisano maskę 3 3 – brak przypisanej maski Bit <2> Enabled – Flaga aktywująca filtr. Bit <4> EXIDE(1) – Flaga filtrująca wyłącznie ramki rozszerzone. Bit <5> RTR – Flaga wymuszająca wyzwolenie automatycznej odpowiedzi na ramki z aktywnym RTR, które pasują do konfigurowanego filtru.

Tabela 27: Dane konfiguracyjne filtru.

Uwaga:

(1) – W przypadku gdy flaga MIDE przypisanego filtru jest nieaktywna flaga jest ignorowana co skutkuje odbieraniem ramek zarówno standardowych jak i rozszerzonych..

9.2.7 Ustawienia masek

Komenda służy do konfiguracji maski interfejsu CAN.

IAC	CMD	LEN	ID	DATA
0xFF	0x07	0x06	0x1234	MASK_NUM(0 – 2) MASK_CONFIG_DATA

Tabela 28: Ramka komendy ustawiającej maskę.

IAC	CMD	LEN	ID	DATA
0xFF	0x87	0x07	0x1234	MASK_NUM(0 – 2) MASK_CONFIG_DATA + kod operacji

Tabela 29: Odpowiedź konwertera na ramkę komendy ustawiającej maskę.

Numer bajtu	Znaczenie
1 – 4	Bity <28..18> Standardowy identyfikator pakietu CAN. Bity <17..0> Rozszerzony identyfikator ramki CAN.
5	Bit <0> MIDE – Flaga aktywująca znaczenie flagi EXIDE przypisanego filtru. Jeśli flaga wyłączona odbierane są ramki standardowe jak i rozszerzone. W przypadku gdy aktywna konwerter odbiera wyłącznie ramki adekwatne do zaznaczenia flagi EXIDE przypisanego filtru.

Tabela 30: Dane konfiguracyjne maski.

9.2.8 Ustawienie trybu pracy konwertera

Konwerter posiada dwa tryby pracy w których może dokonywać konwersji sygnałów otrzymywanych / wysyłanych na magistralę CAN. W zależności od zastosowania konwerter może zostać ustawiony w tryb normalnej pracy, w której ramki transmitowane na magistrali CAN2.0B nie są w żaden sposób interpretowane przez konwerter. W przypadku trybu pracy ze wsparciem protokołu NXCAN pakiety transmitowane podlegają dodatkowej analizie i interpretacji. Protokół NXCAN jest metodą transmisji opracowaną przez firmę Netronix w celu umożliwienia transmisji większej ilości danych przy zastosowaniu standardowych ramek CAN2.0B niż zezwala na to standardowy pakiet danych, który jest ograniczony tylko do 8 bajtów. Protokół ten wykorzystywany jest w komunikacji z urządzeniami firmy Netronix z interfejsem CAN a jego opis został zamieszczony w odrębnym dokumencie zamieszczonym na stronie producenta. Dzięki dodatkowemu trybowi pracy znajomość protokołu NXCAN nie jest konieczna do komunikacji z urządzeniami przy pomocy tego protokołu. W przypadku pracy z protokołem NXCAN należy pamiętać by filtry oraz maski ustawione w parametrach interfejsu zezwoliły na odbiór wszystkich transmitowanych ramek.

IAC	CMD	LEN	ID	DATA
0xFF	0x07	0x01	0x1234	NXCAN_ENABLED

Tabela 31: Ramka komendy ustawiająca tryb pracy serwera konwersji.

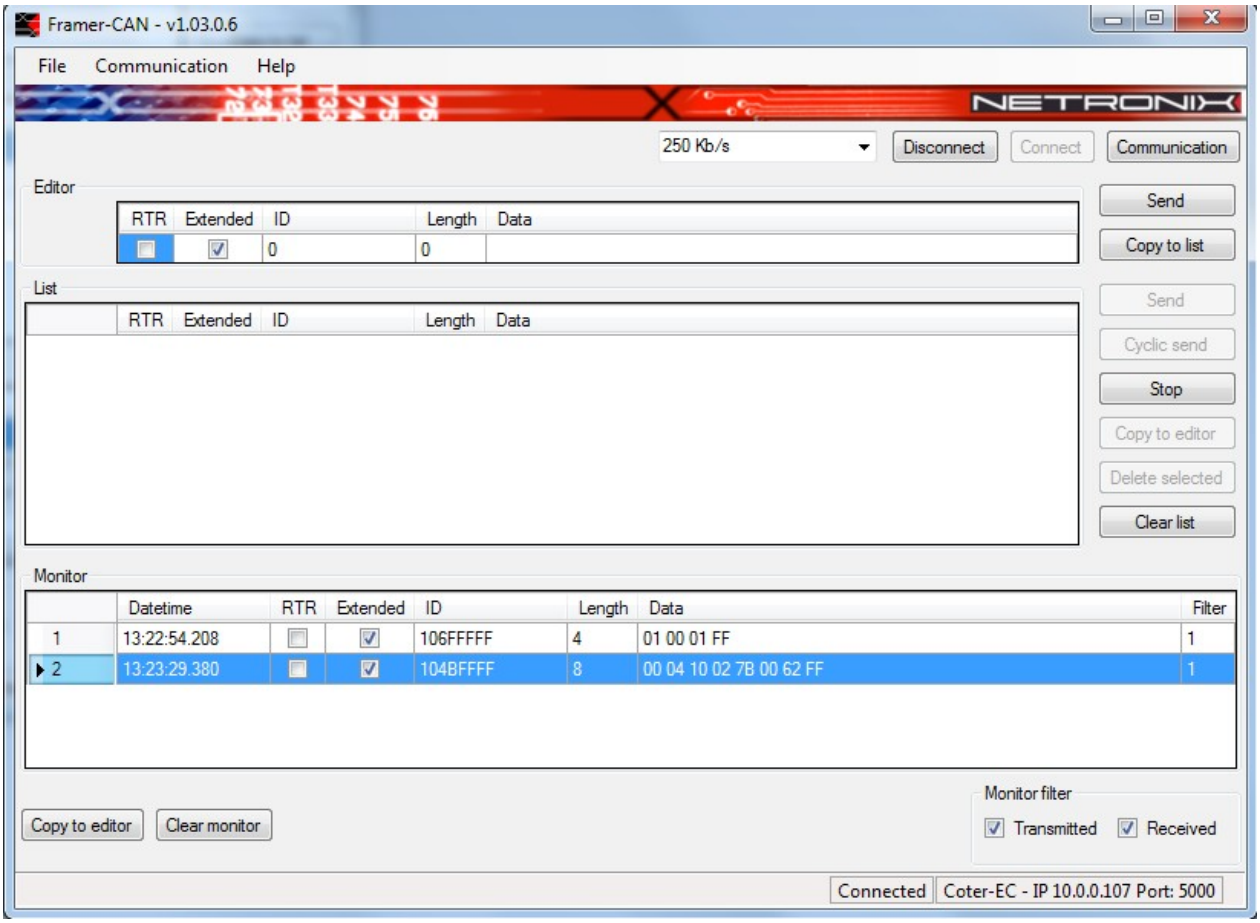
IAC	CMD	LEN	ID	DATA
0xFF	0x87	0x02	0x1234	NXCAN_ENABLED + kod operacji

Tabela 32: Odpowiedź konwertera na ramkę zapytanie o wersje oprogramowania.

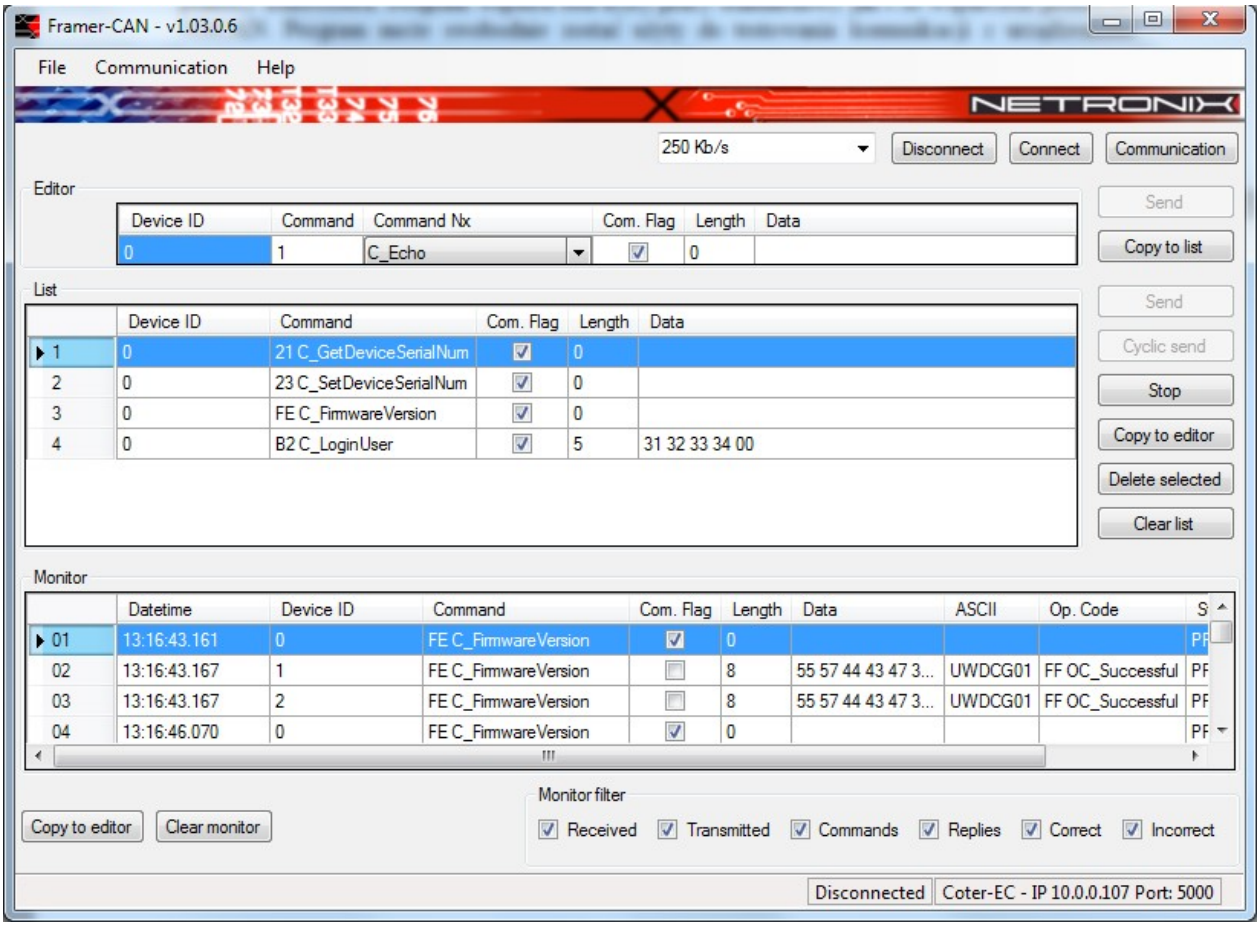
10 Program Framer-CAN

Program jest aplikacją diagnostyczną służącą do transmisji danych z lub na magistralę CAN przy pomocy konwertera. Program wspiera oba tryby pracy standardowy jak i ze wsparciem protokołu NXCAN. Program może swobodnie zostać użyty do testowania komunikacji z urządzeniami wykorzystującymi tradycyjne ramki CAN2.0B oraz rozszerzoną metodę transmisji opisaną przez firmę Netronix.

Program dostępny jest bezpłatnie na stronie firmy Netronix.



Ilustracja 14: Praca programu Framer-CAN w trybie komunikacji standardowej.



Ilustracja 15: Praca programu Framer-CAN w trybie komunikacji ze wsparciem protokołu NXCAN.