



WWW.MULTI-COM.PL

Multi-COM Sp. z o.o., ul. 22-go Lipca 31b, 36-100 Kolbuszowa, POLAND
tel./fax 17 227 50 45, 17 227 00 25, Infolinia: 0 801 67 17 17,
Skype: Multi-COM, www.multi-com.pl, email: biuro@multi-com.pl



Autor

Multi-COM Sp. z o.o.
ul. 22-go Lipca 31b
36-100 Kolbuszowa
NIP: 814-15-61-101
Tel. 172275045/172270025
Skype: Multi-COM
<http://www.multi-com.pl>
e-mail: biuro@multi-com.pl

Licencja na publikację „RIFF Box - JTAG”

Publikacja na licencji **Freeware**, brak możliwości udostępniania i rozpowszechniania bez zgody autora. Publikację legalnie można pobrać jedynie ze strony <http://multi-com.pl> z Działu Download, Umieszczenie publikacji na innym portalu niż wyżej wymieniony bez zgody autora oznacza naruszenie praw autorskich.

Informacje dodatkowe o publikacji

Wszelkie prawa zastrzeżone. Instrukcja tą w postaci pliku danych, mogą Państwo pobierać wyłącznie do własnego użytku. Powielanie, przekazywanie instrukcji lub jej części (fragmentów) w jakiegokolwiek postaci innym osobom jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie instrukcji na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich i może skutkować karą grzywny lub więzienia. Jakiegokolwiek zmiany i modyfikacje bez zgody autora są zabronione.

Wszystkie znaki towarowe zamieszczone na tej stronie są zastrzeżone przez swoich właścicieli. Nazwy produktów, znaki firmowe, symbole handlowe, nazwy handlowe, slogany są własnością odpowiednich firm i są chronione międzynarodowymi przepisami o prawach autorskich, i użyte są tylko w celach informacyjnych. Mimo dołożenia wszelkich starań nie gwarantujemy, że publikowane dane techniczne i opisy nie zawierają braków lub błędów. Autor nie ponosi żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w instrukcji.

RIFF Box – JTAG Revolution

Instrukcja obsługi wersja 1.0

SPIS TREŚCI

1. Wprowadzenie
2. Instalacja sterowników oraz oprogramowania JTAG Manager
3. Rozpoczęcie pracy z urządzeniem RIFF Box
4. Opis sprzętu i pojęć związanych z urządzeniem RIFF Box
5. Opis oprogramowania JTAG Manager
 - Zakładka Resurrection
 - Zakładka JTAG Read/Write
 - Zakładka DCC Read/Write
 - Zakładka Box Service

Wprowadzenie

Riff Box – JTAG Revolution jest sprzętem służącym do profesjonalnej obsługi oraz napraw urządzeń bazujących na popularnych procesorach sterujących (ARM7/9/11, PXA itp.) W odróżnieniu od „zwykłych” urządzeń, które wykorzystują komunikację poprzez wyprowadzenia określonych sygnałów (RX/TX/D+/D-/GND) na zewnątrz (kable FBUS, RS232, USB itp.) Riff Box pracuje z wykorzystaniem niemal bezpośredniego połączenia z procesorem danego urządzenia (np. telefonu). Jest to trudniejsza operacja niż „standardowy” serwis za pomocą kabla, lecz urządzenie RIFF Box jest niezastąpione w przypadku uszkodzenia obszaru bootloadera lub gdy zachodzi konieczność wymiany pamięci Flash i ponownego zaprogramowania obszarów niedostępnych poprzez standardowe magistrale zewnętrzne.

Jest to szczególnie przydatne przy naprawie uszkodzeń bootloadera w popularnych smartfonach firmy HTC (i ich odpowiedników oferowanych pod różnymi markami przez operatorów sieci komórkowych). W przypadku uszkodzenia obszaru startowego (bootloader) urządzenie nie reaguje na standardowe procedury aktualizacyjne, serwisowe itp. Jest „martwe”. Jednak za pomocą urządzenia Riff Box możliwa jest naprawa takich urządzeń z wykorzystaniem bezpośredniego programowania.

W przypadku urządzeń HTC i większości innych urządzeń opartych na popularnych procesorach sterujących i pamięciach flash na ich płytach głównych znajdują się punkty (piny) do bezpośredniej komunikacji z procesorem/pamięcią Flash. Można się do nich przylutować (wymaga bardzo dużej precyzji) lub zakupić w firmie Multi-COM stosowne przystawki idealnie dopasowane do konkretnych urządzeń. Przystawki te **NIE WYMAGAJĄ** lutowania czegokolwiek w telefonie/serwisowanym urządzeniu. Poniżej link do oferty Multi-COM.

http://www.multi-com.pl/index.php/pl_PL,browse,id_gr,312,menu_mode,categories.html

Instalacja sterowników oraz oprogramowania JTAG Manager

Przed korzystaniem z urządzenia RIFF Box należy pobrać ze strony producenta sterowniki oraz oprogramowanie JTAG Manager. W tym celu należy pobrać pliki z poniższych lokalizacji lub poprzez stronę producenta <http://www.riffbox.org/>

Sterowniki urządzenia RIFF Box:

Dla systemów Windows XP, Vista, Windows 7 (wersje 32 bitowe)

http://www.riffbox.org/downloads/RIFF_USB_DRIVER.rar

Dla systemów Windows 7 (wersje 64-bitowe)

http://www.jtagbox.com/downloads/RIFF_64bit_USB_Driver.rar

Sterowniki należy rozpakować do dowolnego katalogu a następnie podłączyć urządzenie RIFF Box do komputera i wskazać miejsce gdzie rozpakowane zostały sterowniki.

SYSTEMY XP/VISTA 64-BITOWE NIE SĄ OBSŁUGIWANE!

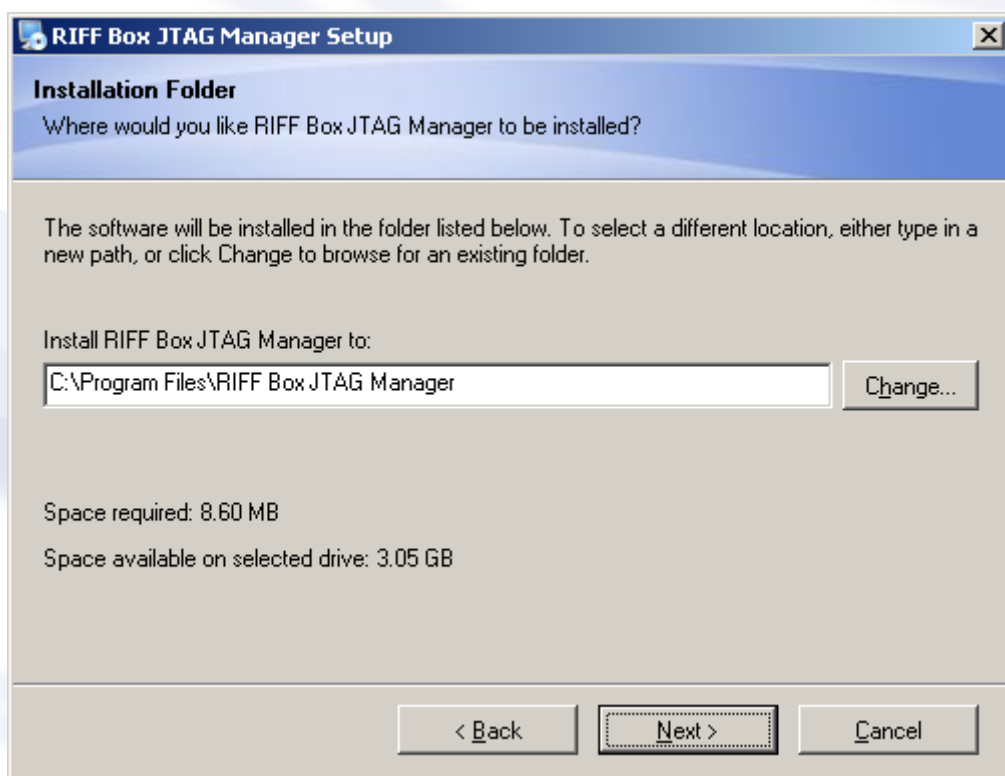
Oprogramowanie JTAG Manager

<http://www.riffbox.org/downloads/RiffSetup.exe>

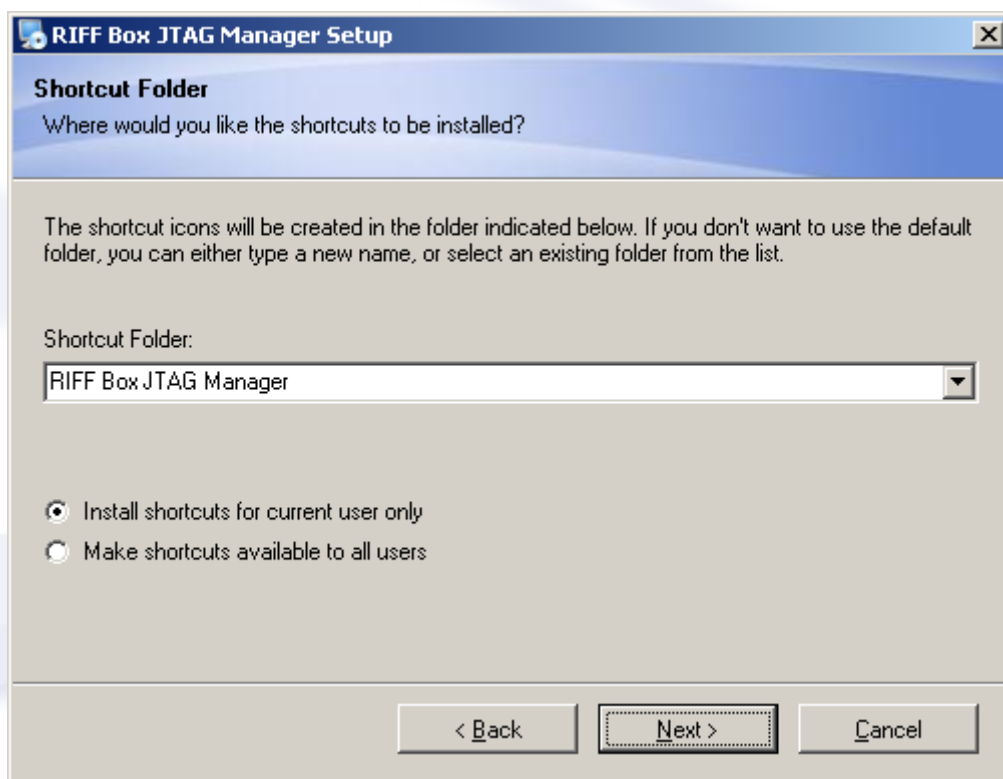
Po pobraniu pliku RiffSetup.exe należy go uruchomić. Pojawi się okienko instalatora



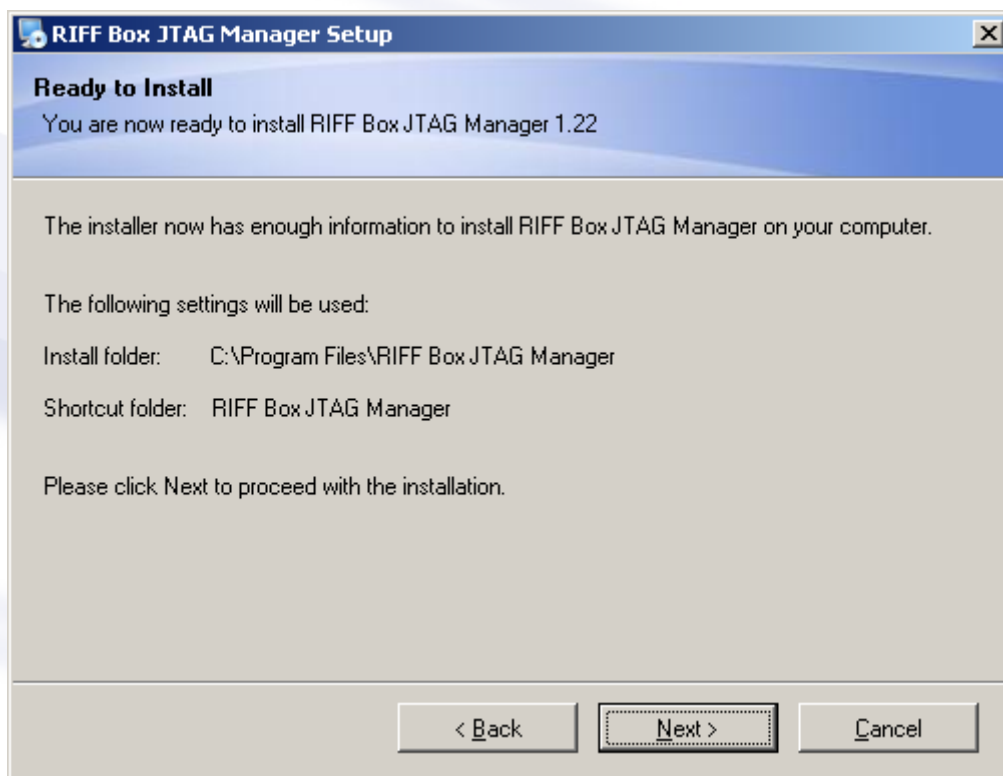
Należy nacisnąć przycisk **Next**



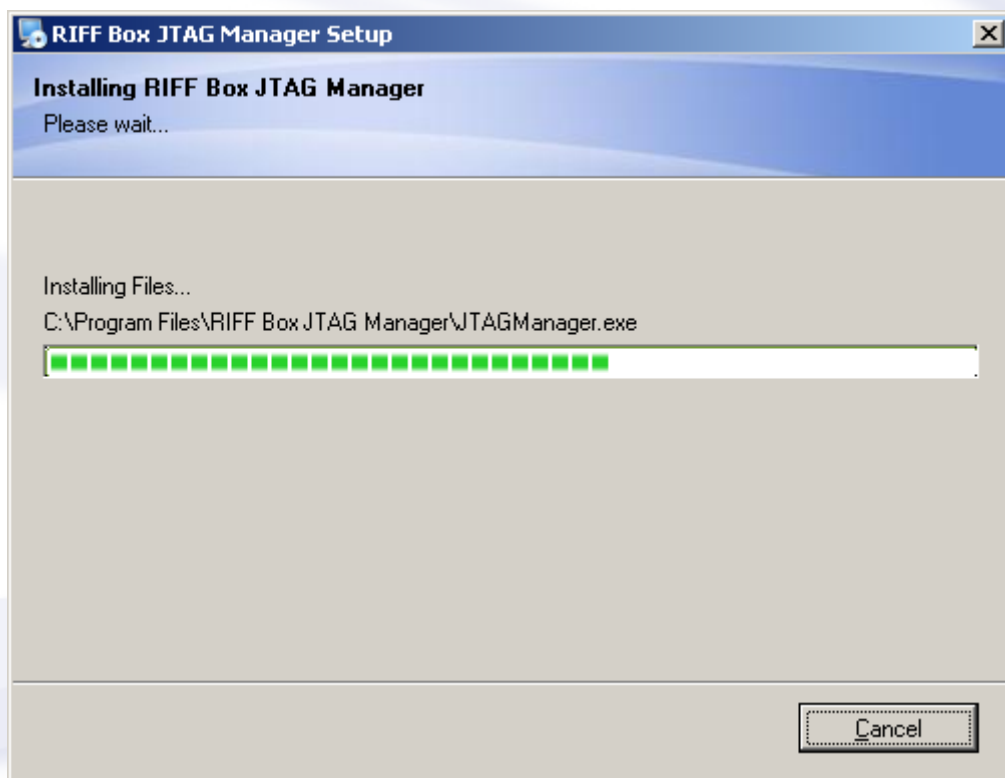
Następnie naciskamy przycisk **Next** (możliwa jest zmiana ścieżki instalacji, lecz zalecane jest pozostawienie domyślnej lokalizacji)



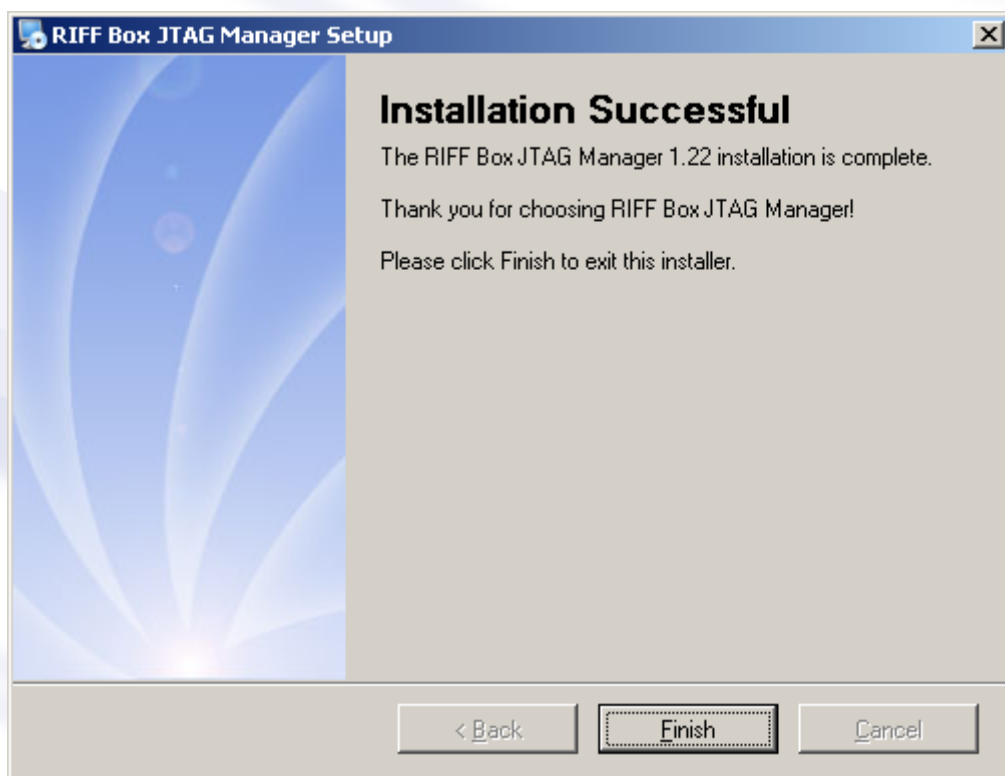
Należy nacisnąć przycisk **Next**



Ponownie naciskamy przycisk Next



Trwa instalacja



Naciskamy przycisk **Finish**. Oprogramowanie JTAG Manager zostało poprawnie zainstalowane.

Rozpoczęcie pracy z urządzeniem RIFF Box

Proszę uważnie zapoznać się z poniższymi uwagami/instrukcjami. Są one niezbędne do poprawnej pracy z urządzeniem RIFF Box i jego interfejsem JTAG.

Interfejs JTAG używa 4 głównych sygnałów. Są to sygnały TCK, TDI, TDO oraz TMS. Dodatkowo często spotykany jest sygnał TRST, RTCK oraz NRST. W przypadku obecności sygnału TRST na schematach urządzenia, które zamierzamy serwisować emisja tego sygnału powinna być wyłączona, gdyż może to spowodować poważne błędy w komunikacji.

Sygnał NRST zazwyczaj używany jest w celu sprzętowego (twardego) resetu danego urządzenia. Po użyciu sygnału NRST, urządzenie jest inicjalizowane do znanego stanu początkowego. Sygnał NRST nie jest wymagany do „tradycyjnego” połączenia JTAG, lecz zdecydowana większość modułów naprawczych urządzenia RIFF Box zakłada, że ten sygnał jest obecny. Bez tego sygnału dalsza praca jest możliwa (połączenie z serwisowanym urządzeniem), jednak mogą wystąpić błędy w komunikacji, długie czasy oczekiwania, ponawianie prób transmisji wynikające z niemożności ustalenia, w jakim stanie jest serwisowane urządzenie w danym momencie transmisji.

W przypadku korzystania z modułów naprawczych zakładki Resurrection programu JTAG Manager WYMAGANE jest użycie sygnału NRST!

Sygnał RTCK zwany „zegarem” jest opcjonalnym sygnałem. Użycie tego sygnału umożliwia połączenie i transmisję z maksymalną prędkością, zsynchronizowaną z wewnętrznym zegarem serwisowanego urządzenia. Urządzenie RIFF Box przystosowane jest do pracy z maksymalną częstotliwością sygnału RTCK na poziomie 18.000MHz.

W większości przypadków sygnał RTCK radykalnie zwiększa stabilność połączenia. Co więcej zdarza się, że połączenie z serwisowanym urządzeniem możliwe jest wyłącznie poprzez dopasowanie się do wewnętrznego zegara. Wobec powyższego zalecane jest wykorzystanie sygnału RTCK zawsze tam, gdzie jest to możliwe.

Ważną rzeczą, którą należy wiedzieć jest fakt, iż interfejs JTAG zapewnia jedynie poprawną komunikację z urządzeniem poprzez umożliwienie odczytu/zapisu pamięci lub wykonania kodu przez procesor sterujący. Posiadanie interfejsu JTAG w żaden sposób nie oznacza, że naprawa serwisowanego urządzenia będzie „łatwa i przyjemna” (choć nie dotyczy to w pełni urządzenia RIFF Box o czym dalej w niniejszej instrukcji).

Większość płyt głównych serwisowanych urządzeń jest bardzo skomplikowana; posiada pamięci NAND oraz pamięć RAM, które podłączone są do logiki głównego procesora sterującego. Aby uzyskać do nich dostęp wymagana jest złożona inicjalizacja sprzętu w określonej kolejności. Każda generacja układów wymaga zazwyczaj innej procedury inicjalizacji. Przykładowo użycie tego samego procesora Qualcomm w dwóch różnych płytach głównych nie oznacza pełnej kompatybilności rozwiązań sprzętowych. Oscylatory, alokacja pamięci poprzez użycie konkretnych sygnałów sterujących, zarządzanie zasilaniem oraz inne parametry nie są ściśle powiązane z danym typem procesora sterującego i mogą znacząco się różnić w zależności od kreatywności osoby projektującej serwisowane urządzenie.

W przypadku konieczności serwisowania urządzenia, które nie jest jeszcze wspierane (nie są powszechnie znane metody serwisu) w wielu przypadkach należy ustalić poniższe rzeczy:

- Uzyskać informację, jak wewnętrzne oprogramowanie (firmware) wykonuje inicjalizację sprzętu i z uwagi, że serwisowane urządzenie ma uszkodzony lub wykasowany firmware należy ponownie wpisać poprawne wartości zachowując prawidłową adresację.

- Uzyskać informację, w jaki sposób procesor komunikuje się z zewnętrzną pamięcią (NAND) – nie dotyczy to pamięci NOR, które nie wymagają skomplikowanych czynności związanych z komunikacją.
- Wykonać kod, który będzie w stanie ustanowić komunikację z procesorem i za jego pośrednictwem wysłać dane, które będą zapisane w pamięci flash.
- Uzyskać naturalnie wiedzę, co należy umieścić w pamięci flash i które pozycje (adresy) pamięci flash powinny zostać naprawione, aby całe serwisowane urządzenie zaczęło działać prawidłowo.

Powyższe kroki mogą być bardzo trudne w realizacji, szczególnie dla osób, które nie są wystarczająco obeznane z powyższą problematyką.

Tutaj w sukurs przychodzi urządzenie RIFF Box JTAG – pozwala ono na uwolnienie się od powyższych problemów dzięki unikalnej funkcji „wskrzeszania”

Funkcja „wskrzeszania” zaimplementowana jest jako rozwiązanie “jednoprzyciskowe” – jeśli serwisowane urządzenie wspierane jest przez odpowiedni moduł naprawczy urządzenia RIFF Box, nie musimy wówczas nic wiedzieć na temat rodzaju procesora, pamięci itp. Naprawa płyty głównej wykonywana jest pojedynczym kliknięciem. Jedyne czynności, które należy wykonać to:

- Nie martwić się
- Przeczytać instrukcję „wskrzeszania” jeśli jest dostępna dla danej płyty głównej
- Rozebrać serwisowane urządzenie
- Używając schematów odnaleźć punkty interfejsu JTAG oraz przylutować, bądź użyć zewnętrznych przystawek (polecane przystawki Multi-COM), aby połączyć odpowiednie sygnały urządzenia RIFF Box z punktami płyty głównej serwisowanego urządzenia
- Podłączyć baterię lub przewód USB połączony z komputerem, aby uzyskać niezbędne zasilanie układu

- Wybrać markę i model urządzenia z listy obsługiwanych urządzeń
- Kliknąć przycisk Ressurect („wskrzeszenie”) i poczekać kilkanaście sekund na zakończenie naprawy
- Odłączyć (odlutować) połączenia JTAG, złożyć urządzenie
- Urządzenie działa

Za każdym wyborem konkretnego modelu oraz producenta urządzenia prędkość transmisji poprzez interfejs JTAG urządzenia RIFF Box ustawiana jest na prędkość zalecaną. Można próbować ustawić prędkość wyższą niż zalecana, ale prawidłowe działanie będzie determinowane jakością użytych kabli połączeniowych itp.

Prędkość TCK zależy od połączonego urządzenia i jakości kabla łączącego RIFF Box z punktami JTAG na płycie głównej serwisowanego urządzenia. Użycie długich kabli powoduje generowanie niepożądanych szumów i zakłóceń transmisji oraz wymusza stosowanie niższych wartości prędkości TCK w celu uzyskania stabilnej wymiany danych. Używanie pojedynczych przewodów zamiast płaskiej taśmy powoduje dodatkowe zwiększenie podatności na zakłócenia i szumy, co zmniejsza radykalnie stabilność transmisji. Należy także zwrócić uwagę, iż niektóre serwisowane urządzenia wymagają podłączonej baterii w celu uzyskania poprawnej komunikacji poprzez interfejs JTAG. Dla niektórych urządzeń wystarczy kabel USB podłączony do komputera, aby zapewnić niezbędne zasilanie i poprawne odpowiedzi JTAG. Jest to pole do własnych eksperymentów.

Urządzenie RIFF Box oferuje także możliwość wykonywania skryptów, co jest wielką zaletą dla doświadczonych użytkowników. Dzięki menedżerowi skryptów (Script Manager) wspierane są następujące cechy/urządzenia/rozwiązania:

- Obsługa procesorów ARM7, ARM9, ARM11, Cortex-A8, PXA3xx, PXA270
- Możliwa obsługa wielu urządzeń na łańcuchu JTAG (użyty zostaje numer TAP do właściwej lokalizacji pamięci flash serwisowanych urządzeń/układów

- Dowolny wybór napięć z zakresu ~1,4V do 3,3V
- Możliwość synchronizacji TCK z zegarem urządzenia
- Możliwość zatrzymania pracy procesora (bez zmiany sygnału NRST)
- Możliwość zresetowania procesora (zastosowanie sygnału NRST przed zatrzymaniem)
- Bezpośredni odczyt pamięci (z użyciem 8/16/32bit bajtów/półsłów/słów)
- Bezpośredni zapis pamięci (z użyciem 8/16/32bit bajtów/półsłów/słów)
- Dostęp do rejestrów kontrolnych procesora ARM (koprocessor 15)
- Możliwość programowania pułapek (breakpoints)
- Możliwość uruchamiania kodu
- Wsparcie dla skryptów oraz loaderów DCC (kompatybilnych z trace32)
- Możliwość uruchomienia własnego serwera GDB
- Wykrywanie pinów wejścia/wyjścia (I/O). Jest to UNIKALNA cecha oferowana wyłącznie przez urządzenie RIFF Box

Aby uzyskać więcej informacji na temat składni skryptów oraz szczegółów konkretnych implementacji należy zapoznać się z plikiem „RIFF JTAG Script Manager Specification”

Proszę również zapoznać się z opisem języka Lauternach Trace32 PRACTICE na aby uzyskać dodatkowe informacje na temat skryptów CMM.

W terminologii RIFF Box, określenie „wskrzeszacz” (Resurrector) oznacza samodzielną bibliotekę DLL zawierającą wszystkie niezbędne informacje dotyczące procedury naprawy wybranego urządzenia.

„Wskrzeszacz” (Resurrector) zawiera:

- Loader DCC zawierający odpowiedni kod, umożliwiający dostęp (odczyt/zapis) do pamięci Flash serwisowanego urządzenia
- Dane inicjalizacji sprzętowej (skrypt uruchamiany przed przesłaniem i wykonaniem loadera DCC w pamięci urządzenia)

- Schemat punktów JTAG urządzenia (jest on opcjonalny i może nie występować). W przypadku, gdy schemat jest dostępny pojawia się przycisk **Interface Pinout** w zakładce Resurrection oprogramowania JTAG Manager
- Krótką instrukcję naprawy ((jest ona opcjonalna i może nie występować). W przypadku, gdy instrukcja jest dostępna pojawia się przycisk **Resurrection Help** w zakładce Resurrection oprogramowania JTAG Manager

Proszę wziąć pod uwagę, że opcja **Interface Pinout** została zaimplementowana dla Twojej wygody. W przypadku, kiedy ta opcja jest dostępna warto zawsze ją sprawdzić. Pozwoli to na wyeliminowanie konieczności szukania w Internecie właściwych schematów połączeń. Czasem także takie informacje nie są dostępne publicznie.

Podobnie jest z funkcją **Resurrection Help** – należy jej używać zawsze, kiedy jest dostępna. Zawiera one dokładne, przetestowane informacje, jakie czynności powinny zostać wykonane do prawidłowego połączenia JTAG i właściwej naprawy („wskrzeszenia – Resurrection) urządzenia. Proszę nie ignorować tych informacji nawet, jeśli jesteś profesjonalistą. Mogą one zawierać pewne ściśle punkty, które należy spełnić (np., że wymagana jest bateria zamiast zasilania zewnętrznego, choć to teoretycznie to samo lub że należy wykonać pewnie „triki” jak np. ukryty przełącznik, który musi być naciśnięty w celu uzyskania poprawnej transmisji, czy przycisk włączenia musi być wciśnięty podczas połączenia czy dokładnie odwrotnie itp.)

Urządzenie RIFF Box używa standardowego 20 –pinowego konektora interfejsu ARM



RJ 45

1	4.2V
2	UART TX
3	UART RX
4	UART TX2
5	MBUS
6	PROBE
7	BSI
8	GND

JTAG

1	VCC
3	TRST
5	TDI
7	TMS
9	TCK
11	RTCK
13	TDO
15	NRST
17	N.C.
19	N.C.

2	N.C.
4	GND
6	GND
8	GND
10	GND
12	GND
14	GND
16	GND
18	GND
20	GND

Napięcie 4,2V (pin 1 złącza RJ45) może zostać użyte jako zasilanie serwisowanego urządzenia zamiast użycia baterii lub w przypadkach gdy użycie baterii jest niewygodne lub utrudnione z uwagi na stan urządzenia (rozłożone, bez obudowy, zatrzasków itp)

Opis sprzętu i pojęć związanych z urządzeniem RIFF Box

Urządzenie RIFF Box pozwala na pracę z pojedynczym urządzeniem lub łańcuchem urządzeń z użyciem numeracji TAP. Poziom napięcie interfejsu JTAG może być ustawiany na różnym poziomie w zależności od rodzaju serwisowanego urządzenia. Przykładowo wiele układów QUALCOMM pracuje na poziomie napięcie 2,6V, zaś układy OMAP zazwyczaj pracują na poziomie 1,5V itp. Interfejs JTAG urządzenia RIFF Box nie jest ustawiony na konkretne napięcie jak to ma miejsce w popularnych, prostych interfejsach JTAG. Napięcie pracy układu jest ustawiane automatycznie w zależności od serwisowanego urządzenia. Sygnał VCC jest także dostępny, lecz może być używany tylko jako wejście ADC (pomiar napięcia) na życzenie użytkownika.

Charakterystyka sprzętowa urządzenia RIFF Box:

- Wewnętrzny regulator napięcia (operuje w zakresie od ~1,4V do 3,6V)
- Możliwość synchronizacji z zegarem układu (wykorzystanie sygnału RTCK o częstotliwości 18MHz) w celu uzyskania maksymalnej prędkości transmisji oraz stabilności połączenia
- Wykorzystanie sygnału TCK (częstotliwość do 18MHz)
- Bezpośredni odczyt/zapis pamięci przy prędkości 100-250 kilobajtów/sekundę
- Odczyt/zapis loaderów DCC przy prędkości 200-300 kilobajtów/sekundę (do 0,8-1,5 megabajta/sekundę przy włączonej kompresji danych)

Charakterystyka oprogramowania JTAG Manager:

- Wykorzystanie pojedynczych bibliotek (DLL) nazywanych "Resurrector" ("wskrzeszacz") w celu zapewnienia niezwykle łatwej naprawy przy użyciu kilku kliknięć

- Wsparcie dla obsługi skryptów dla urządzenia RIFF Box (JTAG)
- Obsługa języka PRACTICE (debugowanie i wykonywanie skryptów *.cmm) co umożliwia komunikację z dowolnym urządzeniem obsługującym transmisję JTAG (w tym przypadku wymagana jest odpowiednia wiedza użytkownika)
- Obsługa odczytu/zapisu napięci poprzez loadery DCC z wieloma funkcjami dodatkowymi takimi jak kompresja danych, wznowianie zatrzymanego odczytu, kontrola procesu transmisji (powtarzanie, ignorowanie błędów, przerywanie bieżących operacji)

W celu uzyskania dalszych informacji proszę zapoznać się z dokumentem „SOFTWARE USERS MANUAL”

Dla wszystkich obsługiwanych procesorów RIFF Box wprowadza dane 0b1 do rejestru IR (zgodnie ze standardem IEEE 1149.1 Test Access Port) gdy procesor znajduje się w stanie CAPTURE. Pozwala to na automatyczne wykrywanie urządzeń na podstawie danych TAP na całym łańcuchu JTAG. Użytkownik nie musi dodatkowo identyfikować układów za pomocą znaczników – wszystko jest ustalane automatycznie. Jedynym parametrem, który musi podać użytkownik jest numer TAP urządzenia, z którym chce się połączyć.

Lista procesorów ARM, obsługiwanych przez urządzenie RIFF Box:

- ARM7
- ARM926
- ARM920T
- ARM1136
- PXA312
- PXA270
- OMAP3xxx
- Cortex-A8

Obsługiwane układy bazujące na powyższych procesorach z funkcjonalnością loaderów RIFF DCC (operowanie na pamięci NAND za pośrednictwem wbudowanego kontrolera NAND danego procesora):

- Bezpośredni dostęp
- OneNAND
- Kontroler Intel Xscale PXA312
- Kontroler QUALCOMM MSM62xx (z wyłączeniem grupy kontrolerów MSM625x)
- Kontroler QUALCOMM MSM625x
- Kontroler SAMSUNG S3C2410
- Kontroler SAMSUNG S3C2440
- Kontroler SAMSUNG S3C6410
- Kontroler Broadcomm BCM21xx
- Kontroler QUALCOMM MSM7225 OneNAND
- Kontroler QUALCOMM MSM7201A
- Kontroler SAMSUNG MSM7291A SDDC

W uproszczeniu, jeśli użytkownik posiada urządzenie z obsługiwany układem posiadającym procesor z listy wspieranych rdzeni ARM może bez problemu ustanowić połączenie i wykonywać operacje odczytu/zapisu za pośrednictwem połączenia JTAG.

W przypadku posiadanie nieobsługiwane urządzenie użytkownik nadal może stworzyć własny skrypt inicjalizujący, a następnie użyć jednego z dostępnych loaderów DCC (zgodnych z typem pamięci RAM oraz NAND). W tym celu należy skorzystać z opcji **Custom Target Settings** oraz przycisku **DCC Loader Settings**. Umożliwia to stworzenie odpowiedniego pliku binarnego z danymi pozwalającymi na przywrócenie działania urządzenia (lub na odczyt danych z działającego urządzenia tego samego typu i ręczny zapis do serwisowanego urządzenia)

Loadery DCC stanowiące część oprogramowania JTAG Manager nie zawierają żadnych procedur inicjalizacyjnych. Zakłada się, że urządzenie jest już zainicjalizowane (pamięć DRAM/SRAM/DDR / skonfigurowane sygnały GPIO itp.) przed załadowaniem i wykonaniem loadera DCC.

Przykładowo użytkownik posiada „martwe” urządzenie bazujące na układzie QUALCOMM MSM6280. Urządzenie posiada pamięć NAND, która jest widoczna dla procesora poprzez wbudowany w układ kontroler pamięci NAND. Generalnie, po resecie układu pamięć DDR nie jest widoczna dla procesora, więc układ musi być uprzednio odpowiednio skonfigurowany, aby uzyskać dostęp do pamięci. Dostępny jest loader DCC MSM6280_01000000.enc. „MSM6280” oznacza dostęp do pamięci poprzez wbudowany kontroler układu MSM6280. Wartość 0x10000000 oznacza, iż loader jest skompilowany w celu wykonania od adresu 0x10000000 w pamięci RAM.

Aby poprawnie skomunikować się z urządzeniem w celu jego naprawy należy:

- Ręcznie utworzyć skrypt inicjalizacyjny (wprowadzenie danych w odpowiednie rejestry urządzenia)
- Upewnić się, że po inicjalizacji sprzętu obszar pamięci RAM w zakresie 0x1000000-0x2000000 jest dostępny
- Użyć przycisku **DCC Loader Settings**, aby wskazać ścieżkę do odpowiedniego pliku loadera, adres pamięci RAM skryptu inicjalizacyjnego, częstotliwość sygnału TCK itp.
- Skorzystać z opcji odczytu/zapisu/kasowanie pamięci w celu zapisania odpowiednich danych w pamięci „martwego” urządzenia.

A co należy robić, gdy serwisowane urządzenie spełnia wszystkie kryteria loadera, lecz nie ma dostępnej pamięci RAM dokładnie od adresu 0x1000000, zaś dostępna jest inna adresacja?

Są dwie możliwości:

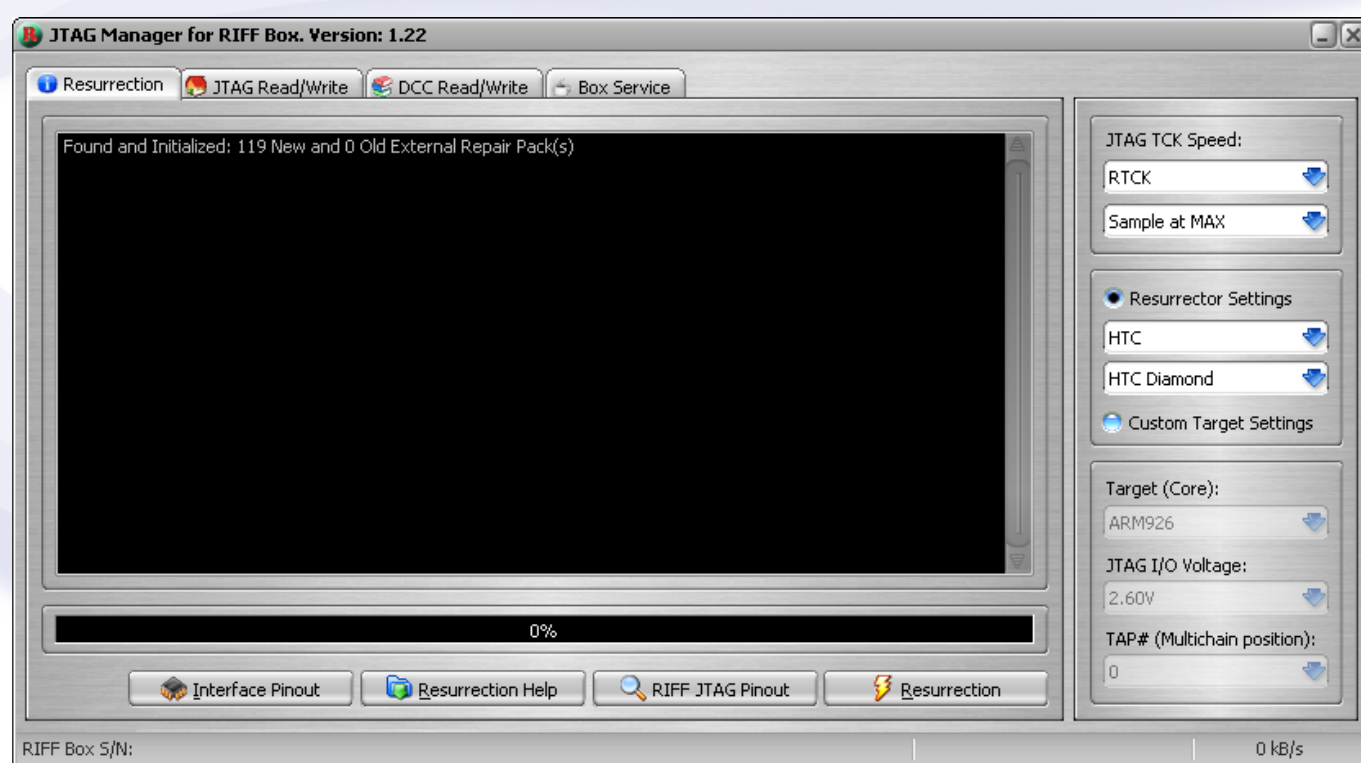
- Należy skonfigurować moduł MMU procesora (jest on dostępny w architekturze ARM od wersji ARMv4) w taki sposób, że procesor ma dostęp do wirtualnej pamięci od adresu 0x1000000 (dodanie skryptu konfiguracji/inicjalizacji sprzętu koprocatora CP15 dla modułu MMU, translacji do fizycznej pamięci RAM, ustawienie bazowych rejestrów itp.)
- W przypadku niepowodzenia należy się skontaktować z autorami urządzenia RIFF Box w celu uzyskania loaderów DCC pracujących przy pożądanej adresacji pamięci RAM

← Multi-COM

Opis oprogramowania JTAG Manager

Do wygodnej obsługi urządzenia RIFF Box służy oprogramowanie JTAG Manager. Dzięki stosownym modułom „wskrzeszaczy”, naprawa uszkodzonych urządzeń jest niezwykle prosta. Podczas uruchamiania oprogramowanie JTAG Manager przeszukuje katalog RESURRECTOR w poszukiwaniu modułów DLL i po znalezieniu ich umieszcza na liście obsługiwanych urządzeń. Z punktu widzenia użytkownika wyświetlana jest lista producentów/modeli, z której należy wybrać konkretny typ serwisowanego urządzenia. Po zainstalowaniu odpowiednich sterowników urządzenia RIFF Box, należy uruchomić oprogramowanie JTAG Manager.

Zakładka Resurrection



Po prawej stronie znajduje się panel ustawień zawierający następujące pozycje (są one wspólne dla wszystkich zakładek)

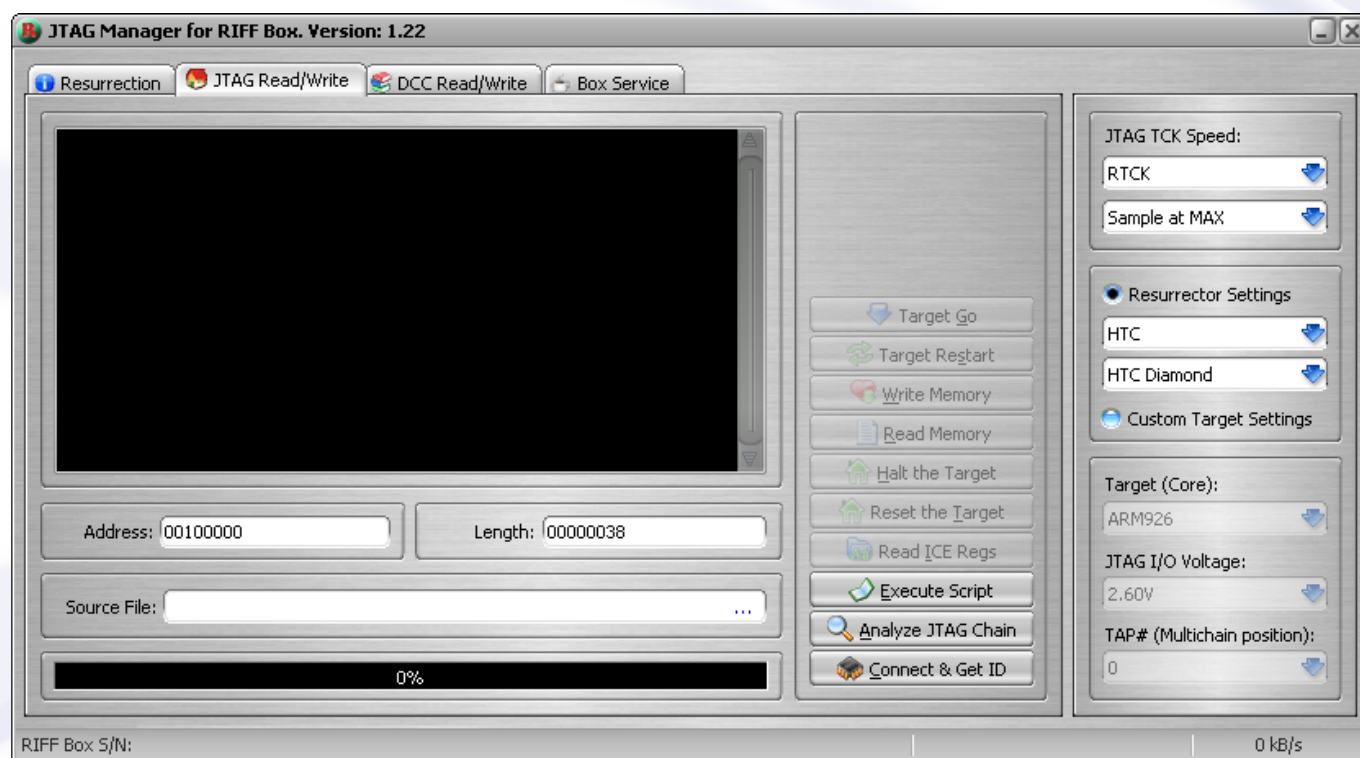
JTAG TCK Speed – opcja umożliwiająca wybór prędkość i rodzaj taktowania serwisowanego urządzenia. ZALECA się używanie sygnału RTCK w celu zapewnienia stabilnej transmisji. Należy zwrócić uwagę, że wybrana prędkość/rodzaj sygnału ustawiane są po załadowaniu oraz wykonaniu loadera DCC korespondującego z układami serwisowanego urządzenia. W przypadku zakładki **Resurrection**, wszystko ustawiane jest automatycznie.

Resurrecter Settings – opcja umożliwiająca wybór producenta i konkretnego modelu serwisowanego urządzenia.

Custom Target Settings – opcja dla zaawansowanych użytkowników umożliwiająca wybór rodzaju procesora, napięcia oraz numeru pozycji TAP w łańcuchu JTAG

Niemal każdy pakiet naprawczy zawiera dodatkowe schematy oraz instrukcje w celu poprawnego serwisowania podłączonego urządzenia. W przypadku dostępności przycisku **Interface Pinout**, należy z niego skorzystać, aby wyświetlić schemat punktów połączeniowych interfejsu JTAG w serwisowanym urządzeniu. Tuż obok znajduje się zwykle przycisk **Resurrection Help** zawierający szczegółowe instrukcje dotyczące naprawy wybranego z listy urządzenia. Niezależnie od stopnia zaawansowania użytkownika należy się zapoznać z w/w instrukcjami – niekiedy należy użyć różnych trików (sposób włączenia, zasilania itp.) w celu przeprowadzenia poprawnej naprawy. Przycisk **Resurrection** rozpoczyna proces naprawy (oczywiście po przylutowaniu punktów JTAG lub zastosowaniu przystawek, zasileniu układu oraz podłączeniu do urządzenia RIFF Box). W przypadku poprawnego połączenia należy odczekać kilka/kilkanaście sekund w celu zakończenia procesu naprawy. W przypadku urządzeń HTC może pojawić się dodatkowe pytanie o naprawę uszkodzonego obszaru IMEI Security. Po zakończeniu procesu naprawy serwisowane urządzenie powinno już ustanawiać komunikację za pośrednictwem standardowych metod (kable USB/RS232 itp.)

Zakładka JTAG Read/Write



Opcje zawarte w zakładce **JTAG Read/Write** służą do bezpośredniej komunikacji JTAG z serwisowanym urządzeniem (zgodnie z wyborem ustawień w panelu z prawej strony lub bibliotek DLL). Są to opcje dla zaawansowanych użytkowników. W przypadku obecności stosownych bibliotek naprawczych nie ma potrzeby stosowania opcji z tej zakładki.

Przed użyciem jakiegokolwiek opcji należy kliknąć przycisk **Connect & Get ID**. Wynikiem tego będzie ustawienie parametrów połączenia (numer TAP, częstotliwości TCK, napięcie itp.) oraz sprawdzenie poprawności połączenia (odczytanie ID układów serwisowanego urządzenia). W przypadku wybrania opcji **Resurrector Settings** wszystkie ustawienia komunikacji zostaną pobrane z pakietu naprawczego danego urządzenia, zaś w przypadku opcji **Custom Target Service** zgodnie z wyborem w panelu.

W przypadku prawidłowego połączenia zostanie wyświetlone ID urządzenia. W przypadku podłączenia nieznanego urządzenia zaleca się użycie przycisku **Analyze JTAG Chain** w celu wykrycia ile urządzeń jest podłączonych do magistrali JTAG.

Od tej pory można używać opcji zatrzymania pracy układu (**Halt Target**) lub jego zresetowania (**Reset Target**). W pierwszym przypadku urządzenia zostaje zatrzymane, zaś w drugim przypadku przed zatrzymaniem urządzenia zostaje do niego wysłany sygnał **NRST**. W celu wysłania tylko sygnału **NRST** (bez zatrzymania układu) należy podczas wybierania przycisku **Reset Target** przytrzymać klawisz **Control**.

Opcje **Write Memory**, **Read Memory** oraz **Target Go** (odczyt pamięci, zapis pamięci oraz wznowienie pracy układu) działają tylko, gdy serwisowane urządzenie jest zatrzymane. W przypadku braku spełnienia tego wymogu wystąpi błąd. Pola **Fields Address** oraz **Lenght** są używane wspólnie przez opcje **Read Memory/Write Memory**. Dodatkowo opcja **Write Memory** używa pola **Source File** zawierającego ścieżkę do pliku z danymi, które mają być zapisane w pamięci. Obecna wersja oprogramowania obsługuje tylko odczyt/zapis w formie 32-bitowych słów (**WORDS**) – w takiej formie jak szyny obsługiwanych procesorów

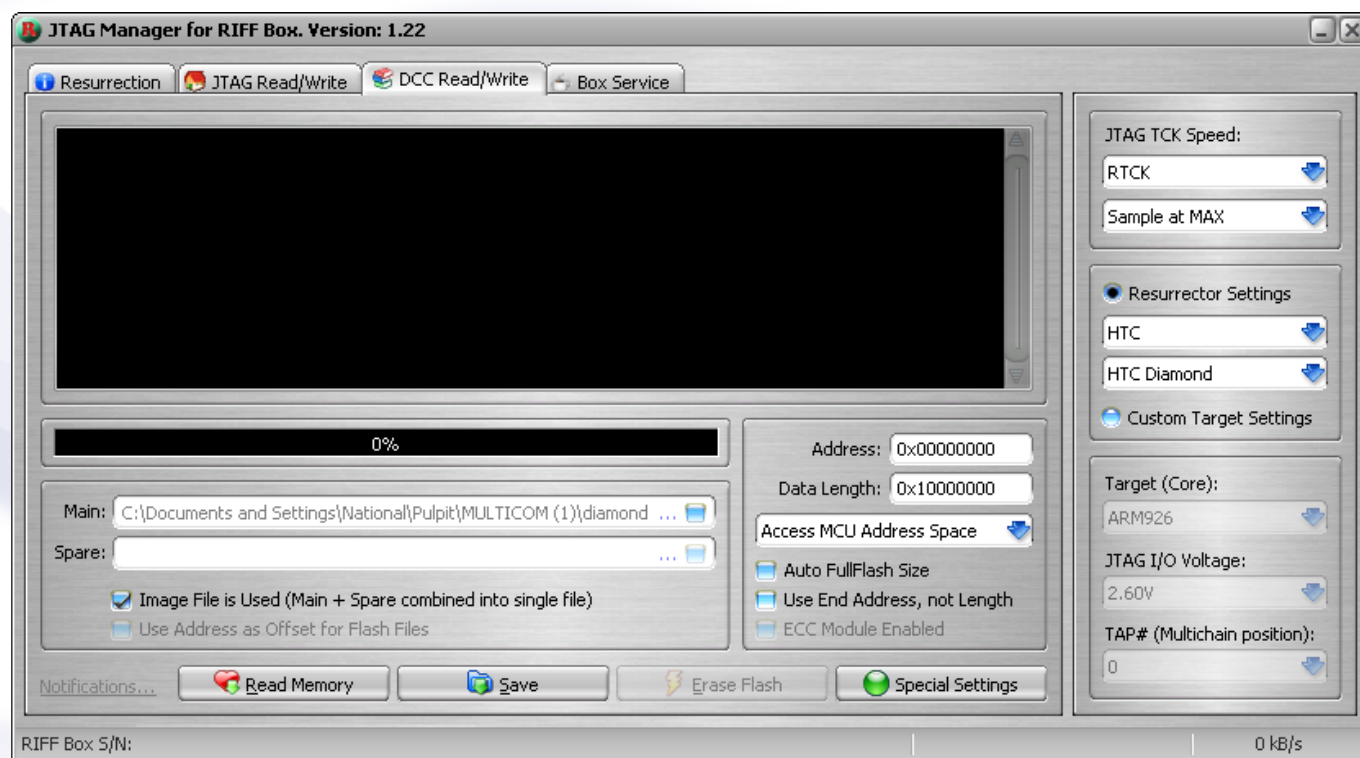
Opcja **Target Go** umożliwia uruchomienie pracy układu. Start następuje od adresu podanego w polu **Address**. Należy zwrócić uwagę, że tryb pracy procesora nie zmienia się – bit **T** rejestru **CPSR** pozostaje bez zmian podczas użycia opcji **Target Go**

Dostępne są także opcje **Read ICE Regs** oraz **Execute Script**. Pierwsza służy do odczytywania rejestrów procesora serwisowanego układu, natomiast druga pozwala na wykonanie własnych skryptów (tylko dla zaawansowanych użytkowników)

Najczęstsze błędy mogące wystąpić przy użytkowaniu opcji zakładki JTAG Read/Write

- Układ nie może być zatrzymany, operacje zatrzymania są niestabilne, odczyt/zapis skutkuje błędnymi danymi – przyczyną może być niepoprawne połączenie z punktami JTAG, zbyt wysoka częstotliwość TCK. **Należy ZAWSZE używać sygnału RTCK, jeśli jest to możliwe!**
- Wszystko wygląda poprawnie, jednak podczas odczytu lub zapisu komunikacja zostaje przerwana – przyczyną może być fizyczne uszkodzenie układu pamięci, próba odczytu/zapisu chronionego obszaru MMU lub brak/błąd inicjalizacji sprzętowej serwisowanego układu.

Zakładka DCC/Read Write



Podobnie jak w przypadku zakładki JTAG Read/Write opcje zakładki DCC Read/Write są przeznaczone dla zaawansowanych użytkowników. W przypadku obecności stosownych bibliotek naprawczych nie ma potrzeby stosowania opcji z tej zakładki.

Opcje zawarte w zakładce **DCC Read/Write** umożliwiają odczyt/zapis pamięci serwisowanego układu za pomocą specjalnych loaderów DCC z użyciem stosownych połączeń obsługiwanych przez większość procesorów. W celu poprawnego skorzystania z tych opcji musi być dostępny pakiet naprawczy dla konkretnego urządzenia (z pakietu pobierane są loadery DCC). Wstępna inicjalizacja (ustawienie parametrów połączenia, sygnały TCK, TAP, inicjalizacja sprzętowa, wczytanie i uruchomienie loadera) wykonywana jest dokładnie tak w przypadku korzystania z przycisku **Resurrection** w zakładce **Resurrection**.

Za pomocą opcji **Read Memory** (odczyt pamięci) możliwe jest odczytanie dowolnego zakresu pamięci RAM oraz pamięci Flash serwisowanego układu. Sposób adresacji RAM lub Flash wybierany jest z rozwijalnej listy po prawej stronie.

W przypadku bezpośredniej adresacji RAM dostępna jest cała przestrzeń 4Gbit (oczywiście zależna od faktycznej pojemności układów serwisowanego urządzenia. W przypadku wyboru adresacji pamięci Flash (NAND) loader wykonuje niezbędne sekwencje inicjujące procesora oraz innych urządzeń peryferyjnych, aby uzyskać dostęp do pamięci (transmisja „poprzez” procesor)..

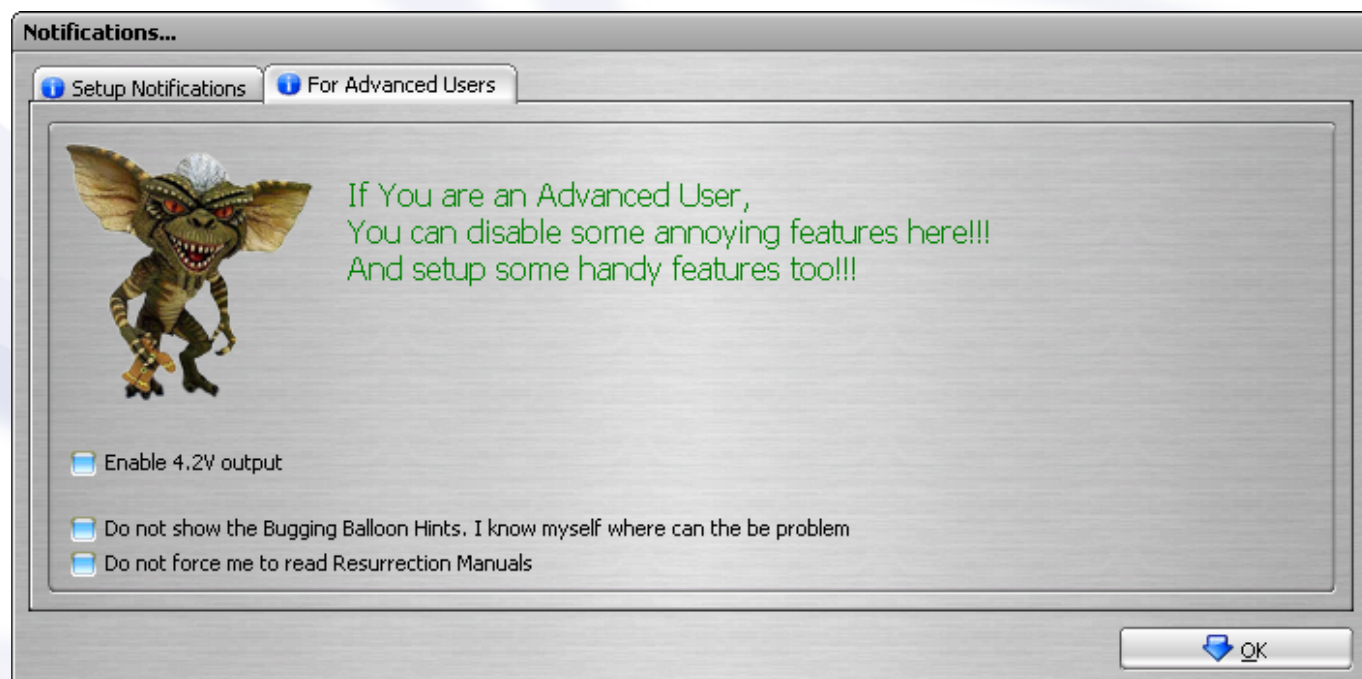
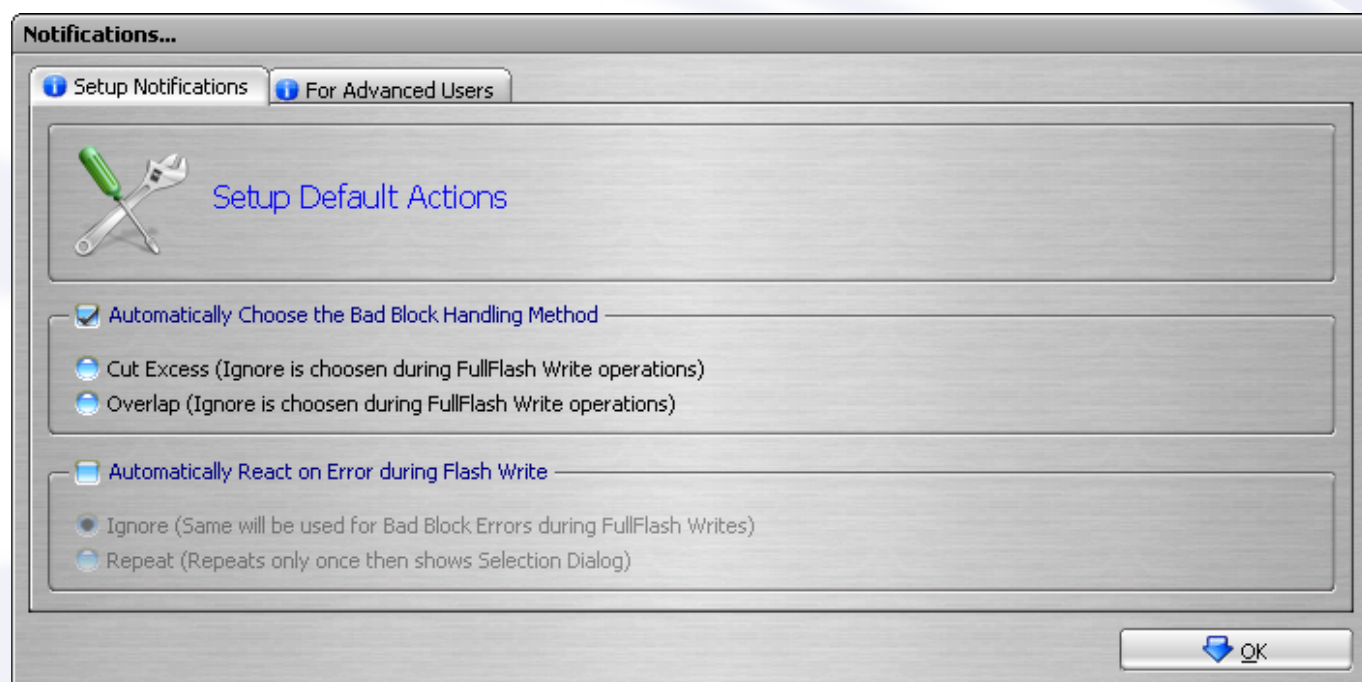
Opcja **Write Flash** służy do zapisu danych do pamięci. W tym trybie niedozwolona jest adresacja bezpośrednia. Opcja **ECC Enable** włącza lub wyłącza kontrolę korekcji błędów udostępnianą przez wiele układów posiadających kontroler pamięci NAND. W przypadku jej włączenia dane nadmiarowe (redundancja) zapisywane są wyłącznie w nieużywanych obszarach (nie zajmowanych przez dane ECC). Dane ECC zazwyczaj są generowane bezpośrednio przez kontroler pamięci. Przykładowo jeśli kontroler ECC umieści dane ECC w 6,7,8 bajcie strefy zapasowej (spare) to oryginalne 6,7,8 bajty są zastępowane przez wyliczone dane. W przypadku braku zaznaczenia opcji **ECC Enable**, kontroler ECC zostaje wyłączony i obszar zapasowy (spare) jest nadpisywany przez dane z pliku Spare. Podczas odczytu pamięci NAND kontroler ECC zostaje automatycznie wyłączony, z uwagi na zastosowanie opcji **ECC Enable** wyłącznie do procesu zapisu pamięci.

Pola **Main** oraz **Spare** służą do wskazania ścieżki do odpowiednich plików z danymi, które mają być umieszczone w pamięci NAND. W związku z organizacją pamięci NAND występują 2 obszary: dane główne oraz dane nadmiarowe (spare). Dane główne zorganizowane są w postaci stron (najczęściej z rozmiarem 0x200 lub 0x800 bajtów), zaś dane nadmiarowe to dodatkowe 0x10 bajtów na każdą stronę o wielkości 0x200 bajtów (w przypadku strony o wielkości 0x800 bajtów jest to 0x40 bajtów).

Osobne zaznaczenie odpowiednich pól daje 3 różne możliwości ustawienia procesu zapisu:

- **Zaznaczenie tylko głównego pliku z danymi (MAIN)** – w tym przypadku obszar nadmiarowy nie jest wykorzystywany. Poprzednie dane nadmiarowe pozostają nienaruszone (na etapie kasowania są odczytane i zapisane ponownie). W przypadku użycia opcji ECC Enable dane nadmiarowe zostają zastąpione wartościami wyliczonymi przez układ ECC kontrolera pamięci
- **Zaznaczenie tylko pliku z danymi nadmiarowymi** – w tym przypadku zostaje zapisany tylko obszar nadmiarowy. Dane MAIN zostają zachowane (na etapie kasowania są odczytane i zapisane ponownie). Zależnie od wyboru opcji ECC Enable (włączona lub wyłączona) dane ECC są zapisane zgodnie z wybranym plikiem lub rekalkulowane przez układ ECC kontrolera pamięci.
- **Zaznaczenie obu plików (MAIN i SPARE)** – w tym przypadku cały obszar NAND zostaje zapisany danymi z odpowiednich plików. Rodzaj zapisu obszaru ECC uzależniony jest od wyboru opcji ECC (włączona lub wyłączona) tak jak w opcji powyżej.

Na dole okienka po lewej stronie dostępna jest także mało widoczna opcja Notifications



Automatically Choose the Bad Block Handling Method

- Cut Excess (Ignore is chosen during FullFlash Write operations)
- Overlap (Ignore is chosen during FullFlash Write operations)

Automatically React on Error During Flash Write

- Ignore (Same will be used for Bad Block Errors during FullFlash Writes) – ignorowanie błędów podczas zapisu
- Repeat (Repeats only once then shows Selection Dialog) – pojedyncza próba ponowienia a następnie wyświetlenie okna dialogowego z dalszym wyborem akcji.

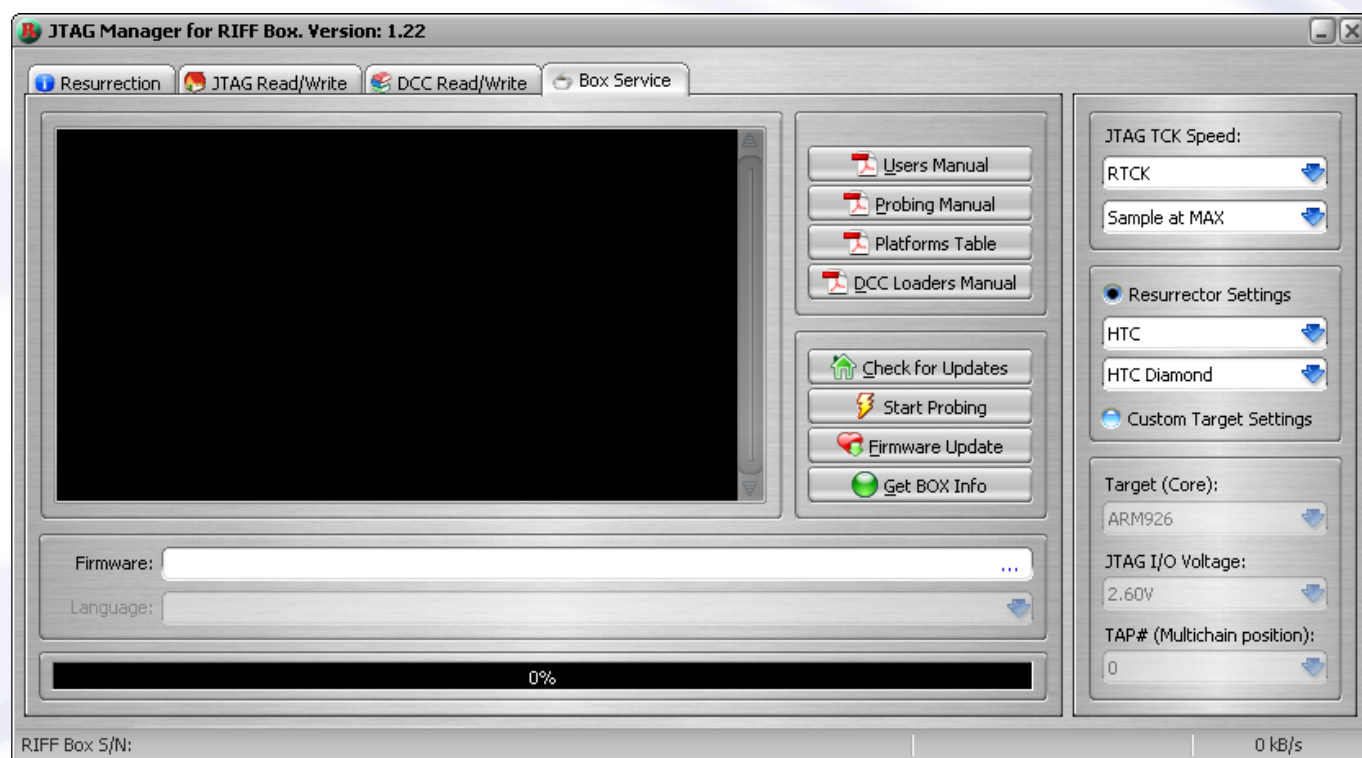
Enable 4,2V output – włączenie napięcia 4,2V na wyjściu urządzenia RIFF Box

Do not show the Bugging Balloon hints. I know myself where can be the problem – wyłączenie pokazywania potencjalnych przyczyn błędu komunikacji/naprawy

Do not force me to read Resurrection Manuals – wyłączenie opcji konieczności czytania instrukcji przed użyciem opcji Resurrection (przydatne przy większej ilości sztuk danego urządzenia). Najczęstsze błędy mogące wystąpić przy użytkowaniu opcji zakładki **DCC Read/Write**

- Wybrano poprawnego producenta i model urządzenia, lecz stale pojawiają się błędy o niemożności ustanowienia komunikacji – przyczyną może być niepoprawne połączenie z punktami JTAG, zbyt wysoka częstotliwość TCK. **Należy ZAWSZE używać sygnału RTCK, jeśli jest to możliwe!**
- Pojawiają się częste lub stałe komunikaty o błędach CRC. Występują one często lub wyłącznie podczas odczytu pamięci, podczas gdy zapis funkcjonuje bez problemu – przyczyną może być różnica pomiędzy prędkościami wymuszonymi przez firmware urządzenia RIFF Box w module naprawczym; należy wówczas zmniejszyć lub zwiększyć doświadczalnie częstotliwość taktowania. Inną przyczyną może być zbyt wysoka częstotliwość TCK. W przypadku gdy częstotliwość sygnału TCK ustalana jest poprzez sygnał RTCK należy wówczas ustawić ręcznie (w sposób doświadczalny) częstotliwość TCK.

Zakładka Box Service



Zakładka **Box Service** służy do obsługi urządzenia RIFF Box oraz do aktualizacji oprogramowania JTAG Manager. Zawiera także moduł próbkowania sygnałów JTAG.

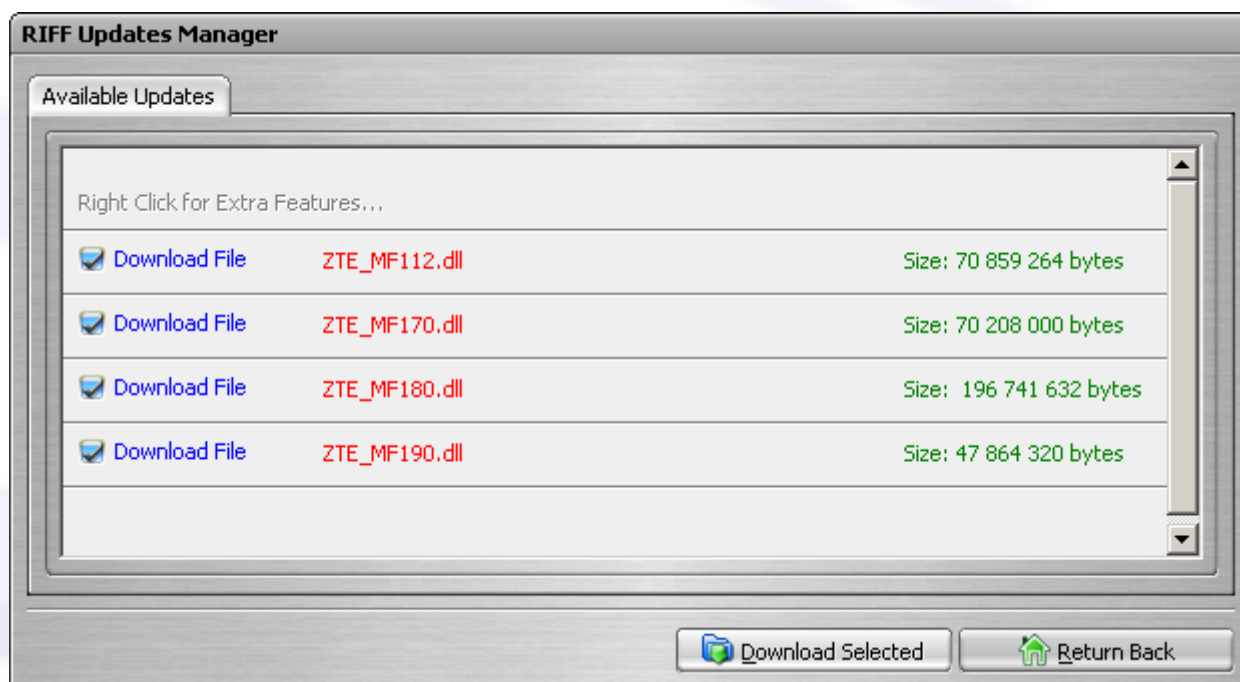
Users Manual – przycisk umożliwiający wyświetlenie instrukcji obsługi urządzenia RIFF Box i/ lub oprogramowania JTAG Manager (język angielski)

Probing Manual – przycisk umożliwiający wyświetlenie instrukcji obsługi próbkowania punktów JTAG (język angielski)

Platforms Table – przycisk umożliwiający wyświetlenie tabeli z rozpisaną adresacją pamięci, typem procesora itp. dla obsługiwanych przez RIFF Box urządzeń (język angielski)

DCC Loader Manual - przycisk umożliwiający wyświetlenie instrukcji modyfikowania i tworzenia nowych loaderów DCC (język angielski)

Check for Updates – opcja pozwalająca na połączenie się z serwerem aktualizacji urządzenia RIFF Box i wyświetlenia, (jeśli są dostępne) modułów do pobrania:



Po poprawnym połączeniu z serwerem zostaną domyślnie zaznaczone wszystkie brakujące pakiety – można oczywiście odznaczyć niepotrzebne. Przycisk **Download Selected** pobiera wybrane pakiety, zaś przycisk **Return Back** pozwala na powrót do zakładki **Box Service**.

Start Probing – przycisk umożliwiający uruchomienie modułu próbkowania sygnałów JTAG

Firmware Update – przycisk pozwalający na aktualizację wewnętrznego oprogramowania urządzenia RIFF Box (firmware). Po pobraniu nowej wersji firmware, należy wskazać ścieżkę do odpowiedniego pliku w polu **Firmware** i następnie nacisnąć przycisk **Firmware Update**.

Get Box Info – przycisk pozwalający na odczytanie wersji firmware i numeru seryjnego urządzenia RIFF Box