

# JTAG-Flash für smart MX 04 L Receiver

## 0. Vorwort

Die neuen smart MX 04 L Receiver basieren auf dem Ali M3329C E1 Chip und haben einen Flash-Chip (EON EN25B16-75, Spansion FL016AIF o.ä.), der ein serielles Programmier-Interface (SPI) besitzt. Wurde eine falsche Firmware geflasht, so dass der Receiver nicht mehr über seine serielle RS-232 Schnittstelle kommuniziert, bleibt als letzte Möglichkeit das Flashen einer passenden Firmware über das vorhandene, interne JTAG-Interface.

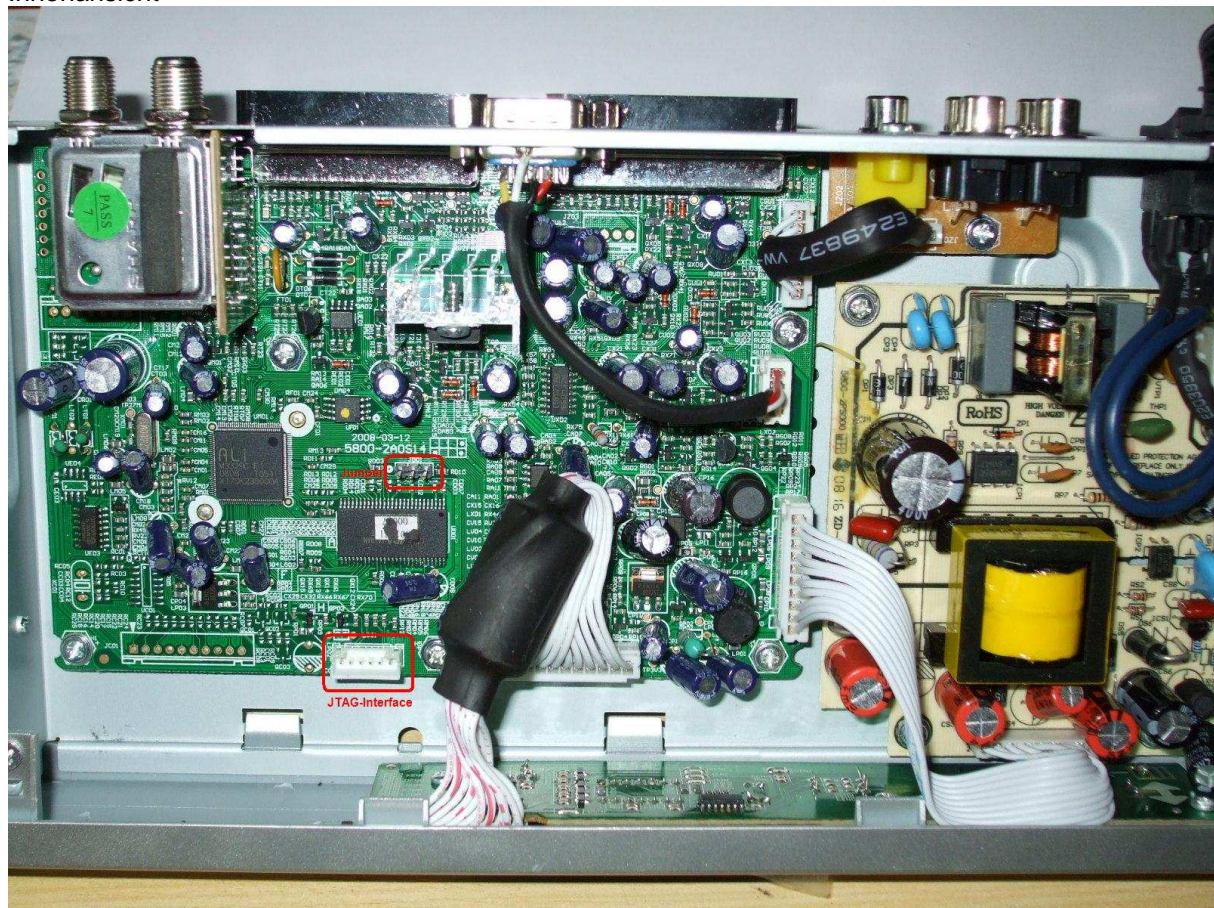
Glücklicher Weise existieren noch einige andere Receiver (z.B. einige Comag SL35 bzw. SL65 Modelle oder die Opticum C Modelle) mit dem selben Ali M3329C E1 Chip, die teilweise auch mit seriellen Flash-Chips bestückt sind, so dass dort schon Erfahrungen mit dem JTAG-Flashen vorhanden sind. Die nachfolgende Beschreibung basiert auf diesen Erfahrungen und berücksichtigt die Besonderheiten des smart MX 04 L Receivers.

Grundvoraussetzung zum JTAG-Flashen ist etwas Elektronik-Erfahrung und ein WindowsXP PC mit einem LPT-Port auf dem Mainboard (LPT-Port PCI-Karten oder PCMCIA/PC-Cards und auch USB/LPT-Adapter sind nicht geeignet).

## 1. Hardware

### 1.1. Der smart MX 04 L

Innenansicht







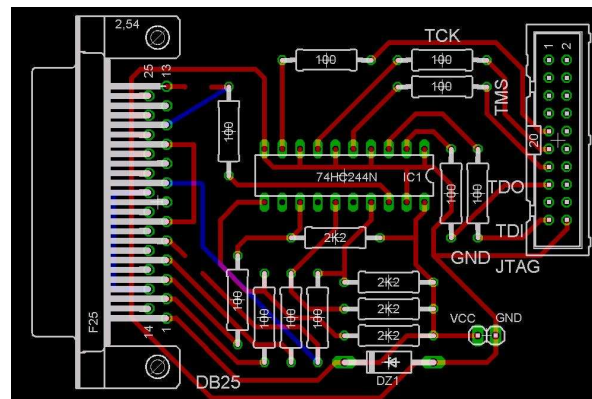
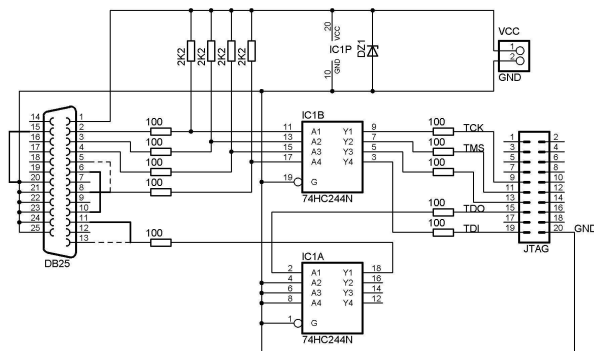
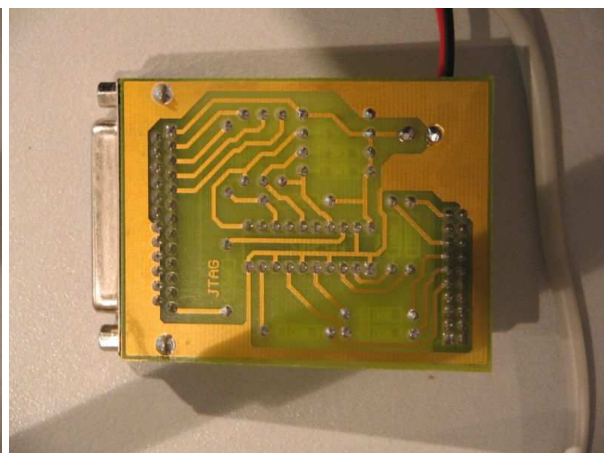
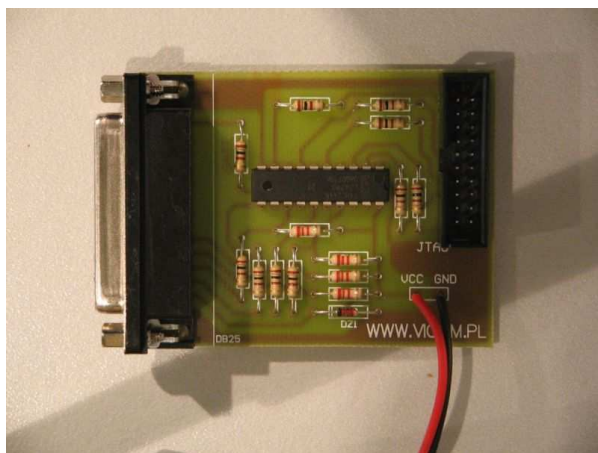
## 1.2. JTAG-Adapter

Auch wenn das JTAG-Interface ein standardisiertes Interface ist, bezieht sich das nur auf die JTAG-Signale (TMS-Target Mode Set, TCK-Target Clock, TDI-Target Data Input und TDO-Target Data Output). Die von verschiedenen Herstellern verwendeten Steckverbinder für ein JTAG-Interface sind teilweise vollkommen unterschiedlich. Genauso gibt es auch vollkommen unterschiedlichste JTAG-Adapter für PCs und die einfachsten davon verwenden den LPT-Port (Line-Printer-Port) des PCs zur Erzeugung der JTAG-Signale. Die vier bekanntesten JTAG-Adapter für den LPT-Port sind: Altera ByteBlaster II, Macraigor /Olimex Wiggler, ST FlashLINK und Xilinx DLC5. Außer zum "Macraigor Wiggler" gibt es beim jeweiligen Hersteller zumindest ein Block-Schaltbild des jeweiligen JTAG-Adapters und auch zum „Olimex Wiggler“. Deren Zuordnung der JTAG-Signale zu den Signalen des LPT-Ports ist dann folgendermaßen:

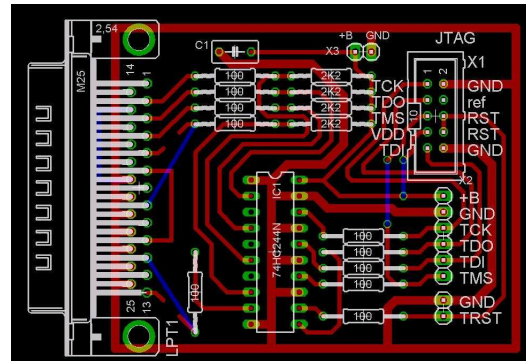
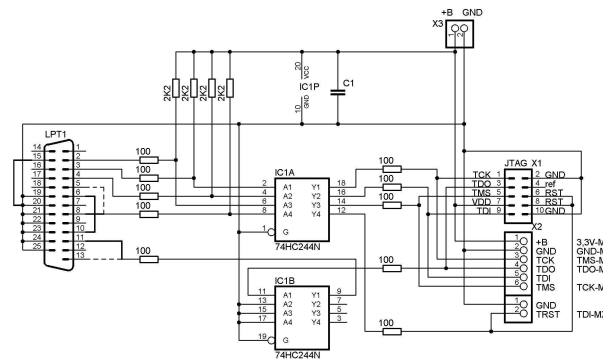
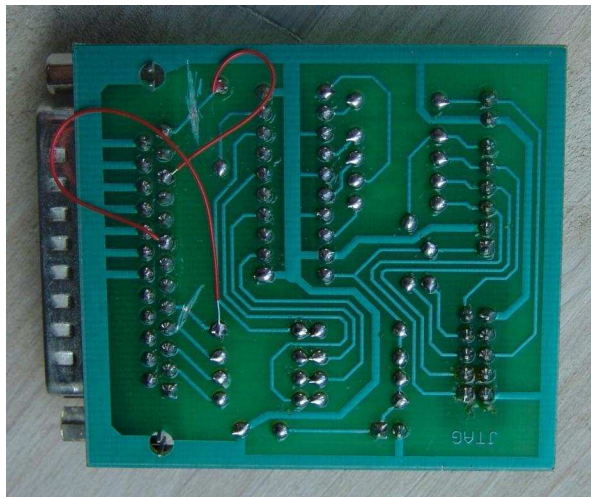
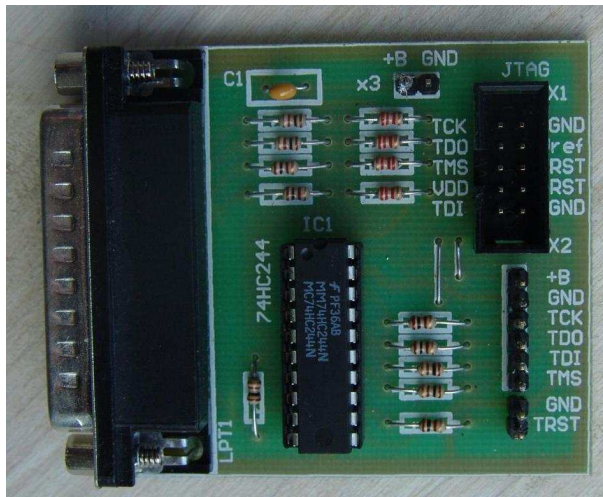
LPT-Port Pin	Signal	Altera ByteBlaster II	Macraigor Wiggler	ST FlashLINK	Xilinx DLC5
1	nSTB				
2	D0	TCK	#nSRST	TCK	TDI
3	D1	TMS	TMS	TMS	TCK
4	D2		TCK	TDI	TMS
5	D3		TDI		(nTRST)
6	D4	(6-10)	nTRST	nTRST	
7	D5			nSRST	
8	D6	TDI	(8-15)		(8-11-12)
9	D7				
10	nACK	(6-10)			
11	BSY	TDO	TDO	VCC	(8-11-12)
12	PE			TDO	(8-11-12)
13	ONL				TDO
14	AF				
15	nERR	GND (#VCC)	(8-15)		VCC
16	nINI				
17	nSEL				
18	GND	GND	GND	GND	GND
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
25	GND	GND	GND	GND	GND



Bisher sind nur Xilinx DLC5 kompatible JTAG-Adapter als fertige Baugruppen von verschiedenen Anbietern gefunden worden, aber das Programm EJTAG\_TinyTool zum JTAG-Flashen der MX 04 L Receiver setzt einen Altera ByteBlaster II kompatiblen JTAG-Adapter voraus. Aus der Zuordnung der Signale am LPT-Port und den JTAG-Signalen beim Xilinx DLC5 und Altera ByteBlaster II JTAG-Adapter ist ersichtlich, dass man mit etwas Überlegung und wenig Aufwand aus einem Xilinx DLC5 JTAG-Adapter auch einen Altera ByteBlaster II JTAG-Adapter machen kann. Das JTAG TDI bzw. TCK Signal des Xilinx DLC5 JTAG-Adapters entspricht dem TCK bzw. TMS JTAG-Signal eines Altera ByteBlaster II JTAG-Adapters. Bei allen preiswerten Xilinx DLC5 JTAG-Adapttern fehlt die Verbindung der LPT-Port Pins 8, 11 und 12 miteinander und auch Pin 15 ist unbeschaltet. Außerdem ist bei allen derartigen JTAG-Adapttern das optionale JTAG-Signal nTRST (Target Reset) wie oben angegeben verschaltet. Dieses nTRST (meist verkürzt als RST bezeichnet) lässt sich durch auftrennen der Verbindung vom LPT-Port Pin 5 und neuverbinden mit LPT-Port Pin 8 als das TDI JTAG-Signal des Altera ByteBlaster II JTAG-Adapters verwenden. Genauso könnte man mit der Verbindung am LPT-Port Pin 13, dem TDO JTAG-Signal des Xilinx DLC5 JTAG-Adapters, verfahren und einfach die Verbindung zum LPT-Port Pin 13 auftrennen und dann eine neue Verbindung zum LPT-Port Pin 11 herstellen so dass damit das TDO JTAG-Signal eines Altera ByteBlaster II JTAG-Adapters zur Verfügung steht. Hier reicht aber statt des Auftrennens der Verbindung zum LPT-Port Pin 13 auch eine einfache zusätzliche Verbindung mit dem LPT-Port Pin 11, da das JTAG-Signal TDO ein Ausgangssignal ist und die bei den JTAG-Adapttern verwendeten Bustreiber-ICs ohne weiteres in der Lage sein sollten, auch zwei LPT-Port Eingänge gleichzeitig anzusteuern. Fehlt nur noch die beim Altera ByteBlaster II JTAG-Adapter vorhandene Verbindung zwischen LPT-Port Pin 6 und Pin 10, sowie die Masseverbindung am LPT-Port Pin 15 und fertig ist ein Altera ByteBlaster II JTAG-Adapter:



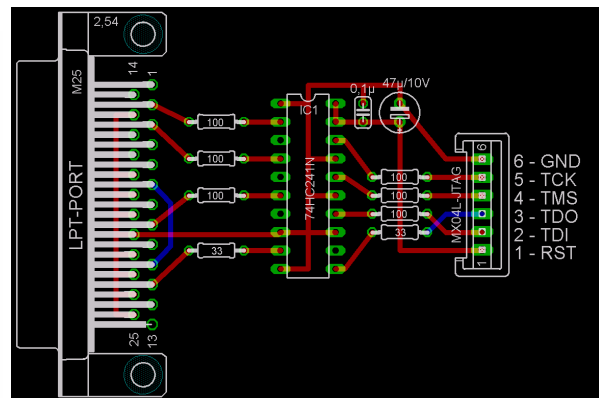
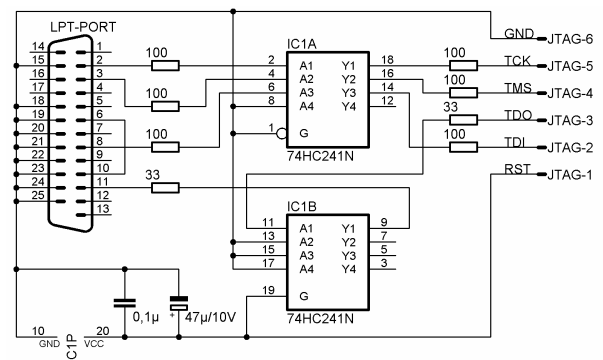




Alle diese JTAG-Adapter benötigen noch eine Betriebsspannung für die integrierte Schaltung (Bustreiber-IC 74HC244) und die kann man in diesem Fall und dieser Anwendung auch direkt vom RST JTAG-Signal des smart MX 04 L „ableiten“, Ansonsten ist auf dem Bild der Receiver-Platine auch der Anschluss des Verbinders-Kabels zum Netzteil gekennzeichnet, der die 3,3V zur Verfügung stellt.

Wichtig ist, dass man die, wie vorher erläuterte und in den Schaltbildern dargestellte, jetzt andere Bedeutung der JTAG-Signale beachtet und die Verbindungen zum JTAG-Interface des Receivers entsprechend herstellt.

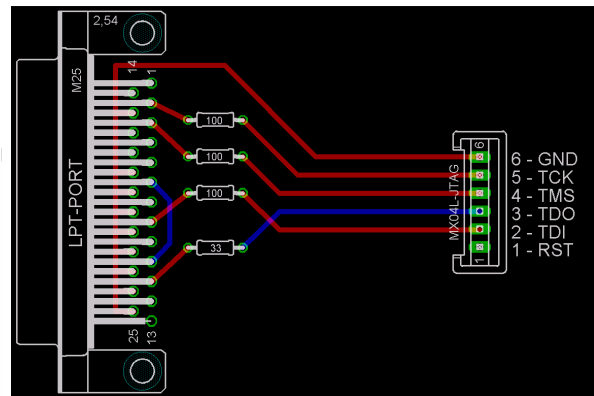
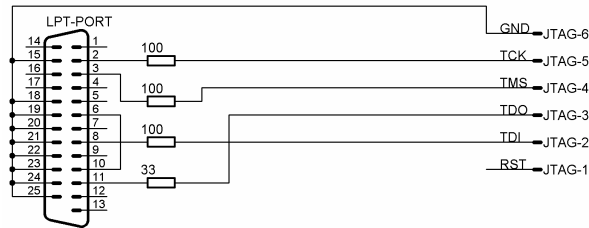
Wer über ausreichende Elektronikkenntnisse verfügt, kann sich für wenig finanziellen Aufwand auch selber einen entsprechenden Altera ByteBluster II kompatiblen JTAG-Adapter zusammenlöten:



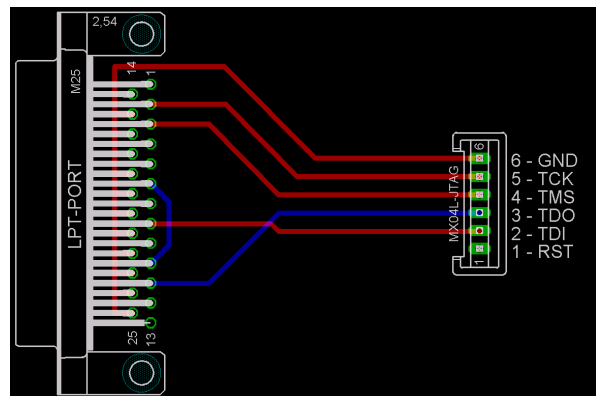
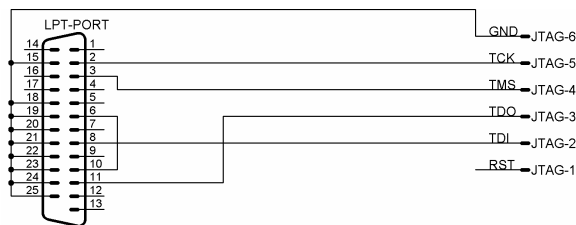
Statt des 74HC241 sind auch andere Bustreiber ICs aus der 74HCxxx bzw. 74HCTxxx Serie geeignet, wenn diese nicht-invertierend arbeiten (z.B. 74HC244, 74HC245 u.ä., andere Anschlussbelegung beachten) und andere IC Serien (z.B. 74xxx oder 74LSxxx) sind ungeeignet. Als Betriebsspannung für die integrierte Schaltung (74HC241 o.ä.) dient der Pegel, der am RST JTAG-Signal des MX 04 L vorhanden ist, so dass keine weitere Verbindung zu einer Spannung im Receiver notwendig ist.



Man kann die Schaltung auch ganz ohne Bustreiber-IC aufbauen und wenn die Verbindung vom LPT-Port im PC zum JTAG-Interface im MX 04 L sehr kurz ist (maximal ca. 15cm) funktioniert das mit etwas Glück auch:



Ganz Mutige lassen auch noch die strombegrenzenden Widerstände weg, so dass dann eine direkte Verbindung zwischen LPT-Port im PC und dem JTAG-Interface im Receiver besteht:



## 2. Software

### 2.1. Der Treiber GIVEIO.SYS

Damit ein JTAG-Flash-Programm den direkten Zugriff auf den LPT-Port eines WindowsXP PCs erhalten kann, wird der spezielle **GIVEIO.SYS** Treiber benötigt. Dieser muss unter WindowsXP in das Verzeichnis `c:\windows\system32\drivers\` kopiert werden, mit dem Programm **LoadDrv.exe** erst installiert (Install) und dann gestartet (Start) werden. Dabei ist der angegebene Pfad zu dem Treiber unbedingt mit dem Treibernamen zu ergänzen.



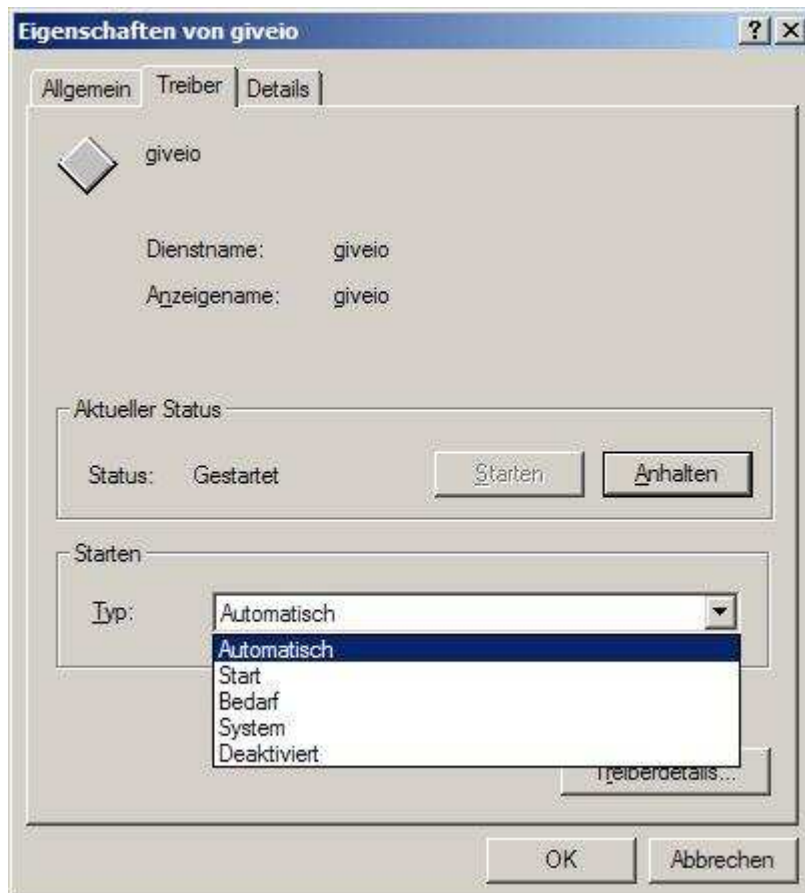
Mit dem Programm **LoadDrv.exe** lässt sich der Treiber GIVEIO.SYS auch wieder stoppen (Stop) und aus dem WindowsXP System entfernen (Remove). Auch wenn der Treiber GIVEIO.SYS im WindowsXP System installiert ist, wird er bei einem Neustart des Systems nicht automatisch gestartet.



Man kann den Start des Treibers aber auch automatisieren, dazu öffnet man einmal den Geräte-Manager von WindowsXP und dort wählt man unter Ansicht die Einstellung „Ausgeblendete Geräte anzeigen“, so dass der giveio-Treiber bei den Nicht-PnP-Treibern sichtbar wird.



Bei den Eigenschaften des GIVEIO-Treibers kann man dann den Start-Typ auf „Automatisch“ einstellen, so dass GIVEIO.SYS bei jedem Start von WindowsXP automatisch gestartet wird und man nicht erst das Programm LoadDrv.exe bemühen muss.

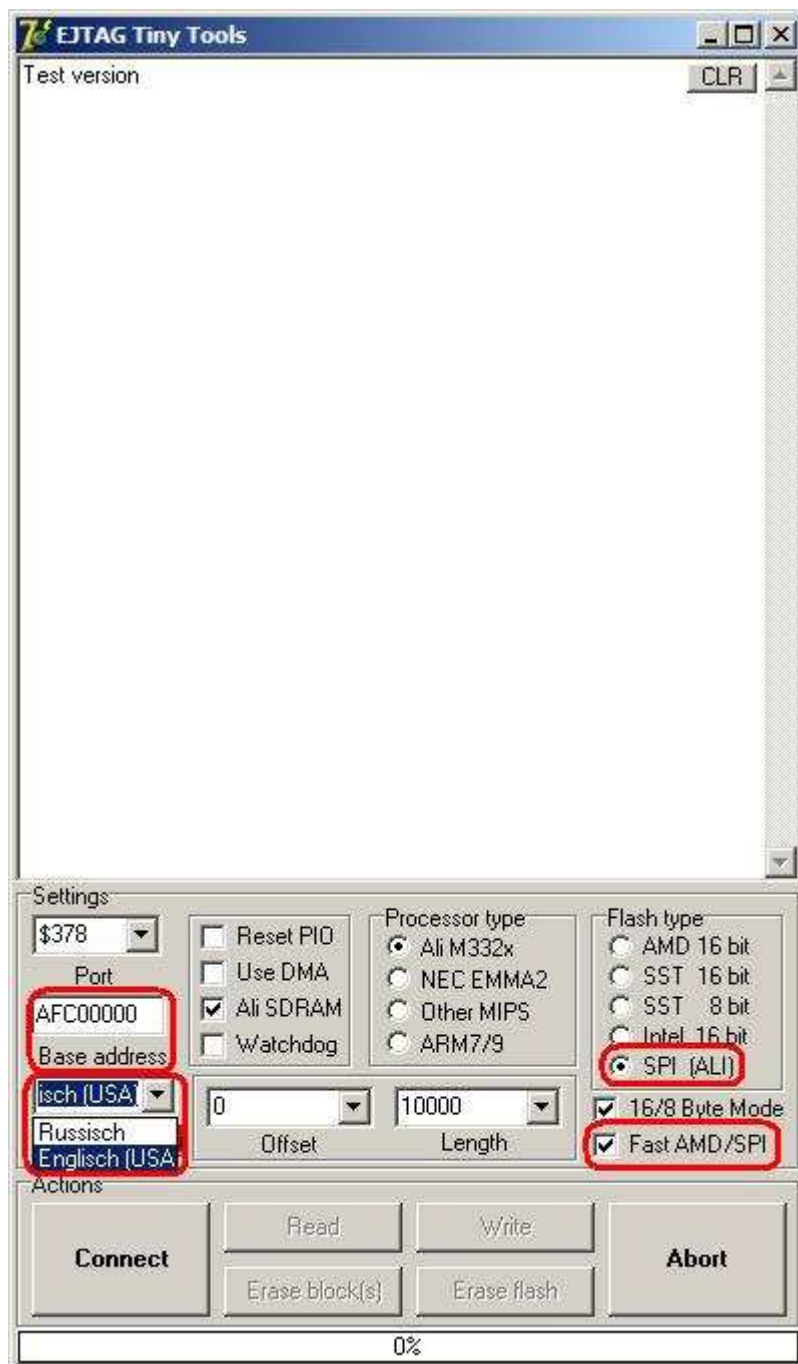




## 2.2 Das JTAG-Flash-Programm EJTAG\_TinyTool

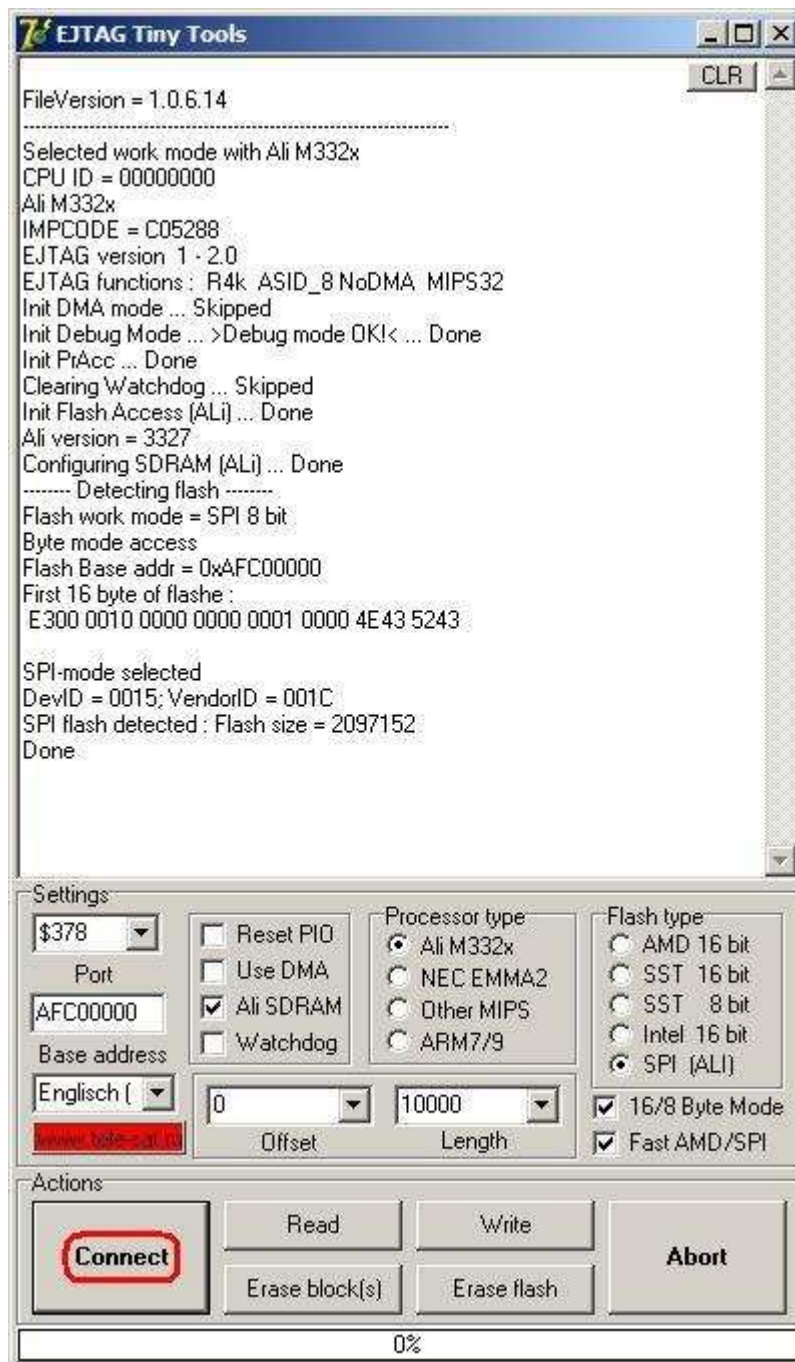
Zum eigentlichen JTAG-Flashen des smart MX 04 L Receivers verwendet man das sehr einfach zu bedienende, aber mit vielen Funktionen versehene Programm EJTAG\_TT in Verbindung mit einem Altera ByteBlaster II kompatiblen JTAG-Adapter. Man schließt den JTAG-Adapter an den Receiver wie unter 1.1 dargestellt entsprechend an, **setzt den Debug-Jumper** und verbindet den JTAG-Adapter mit dem LPT-Port des PC. Startet man jetzt EJTAG\_TT, sollte bzw. muss man

- die Sprache von Russisch auf **English umstellen**,
- die Base adress auf **AFC00000 einstellen**,
- den Flash type **SPI (ALI)** auswählen,
- das Häkchen bei **Fast AMD/SPI** setzen.



Wenn man den smart MX 04 L jetzt einschaltet, sollte man im Display des Receivers „6:6“ oder „-:-“ angezeigt bekommen und der Receiver befindet sich im Debug-Mode. Falls der Receiver normal startet, hat man den Debug-Jumper vergessen oder falsch gesteckt.

Jetzt kann man bei EJTAG\_TT auf „Connect“ klicken und sollte folgende Ausgabe bei EJTAG\_TT erhalten:

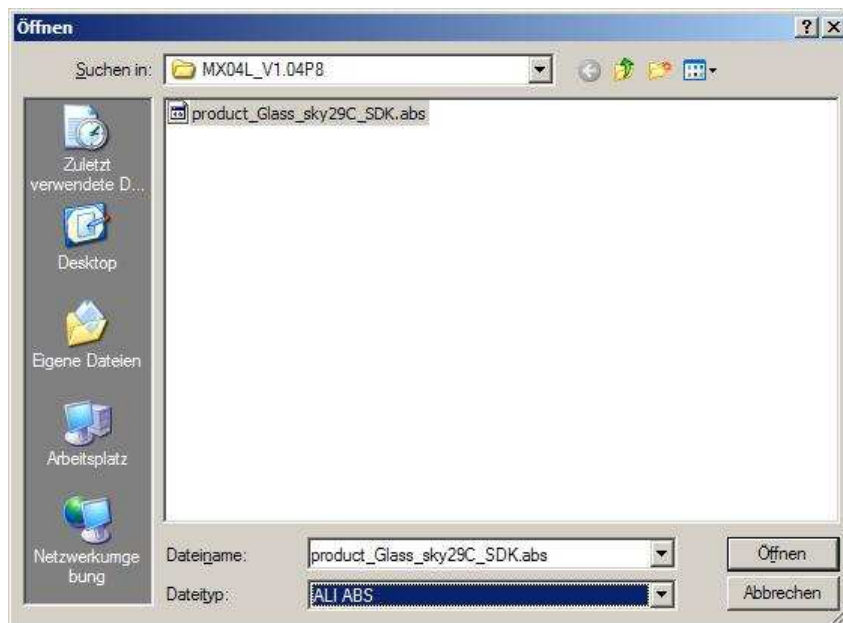


Wenn der Flash-Chip im Receiver richtig erkannt wurde, werden die Buttons für „Read“ (Lesen), „Write“ (Schreiben), „Erase block(s)“ (Löschen Blöcke) und „Erase flash“ (Löschen des gesamten Flash-Chips) aktiviert.

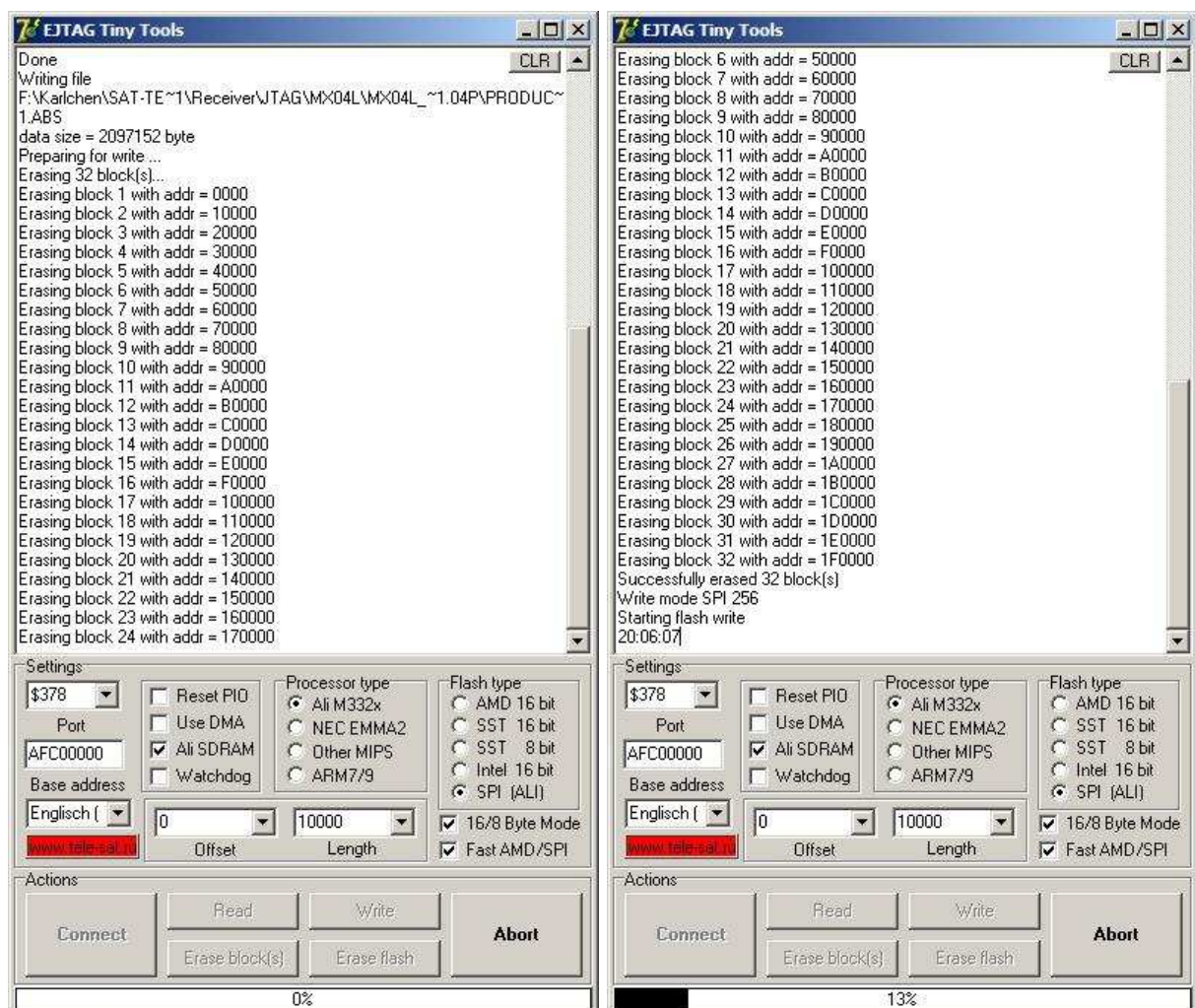




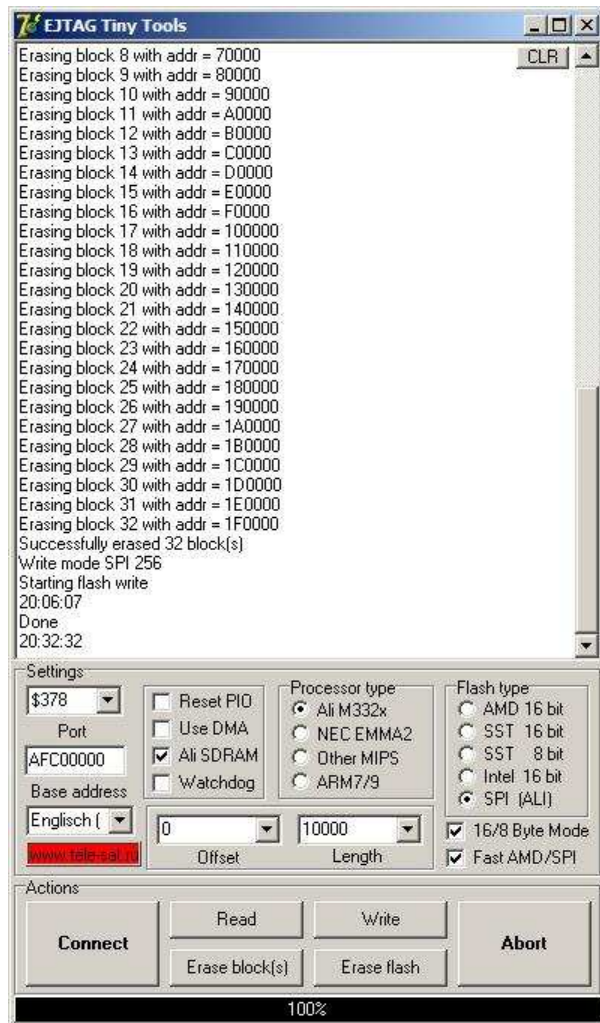
Klickt man auf „Write“ für Schreiben, öffnet sich ein Datei-Auswahl Fenster und dort kann man dann die passende Firmware-Datei auswählen (eventuell den Dateityp passend wählen, so dass man die gewünschte Datei auch angezeigt bekommt) und setzt dann mit „Öffnen“ fort.



Nach der Auswahl der Firmware-Datei **beginnt sofort das Löschen** des Flash-Chips und der Flash-Vorgang dauert ca. 30 Minuten:



Während des Flash-Vorganges zeigt das Display des MX 04 L „66:66“ oder „---:--“, und die rote LED leuchtet. Mit Geduld muss man bis zum Ende des Flash-Vorganges warten.



Jetzt kann man den Receiver ausschalten, den JTAG-Adapter entfernen, den Debug-Jumper wieder entfernen und dann das Programm EJTAG\_TT beenden.

Wenn alles gut gegangen ist, sollte der smart MX 04 L nach dem Einschalten wieder normal mit der neuen und hoffentlich passenden Firmware starten.

In manchen Fällen und insbesondere bei einem einfachen JTAG-Adapter ohne Bustreiber-IC, also nur mit ein paar Widerständen oder auch ganz ohne, ist der Flash-Vorgang vom Timing her zu schnell, so dass kein erfolgreiches Flashen möglich ist und der Receiver nicht richtig startet. In diesen Fällen hilft es, das Häkchen bei „Fast AMD/SPI“ zu entfernen und den Flash-Vorgang noch mal zu wiederholen. Das dauert dann aber ca. 2 Stunden und nicht nur ca. 30 Minuten. Hilft das auch nicht, nach dem „Connect“ und vor dem Flashen („Write“) einmal durch klicken auf den Button „Erase flash“ den Flash-Chip vollständig löschen lassen und danach einfach noch mal auf „Connect“ klicken, dann sollten als die ersten 16 Bytes im Flash-Chip lauter FFFF angezeigt werden und hoffentlich ein nachfolgender Flash-Vorgang (eventuell ohne „Fast AMD/SPI“) erfolgreich verlaufen.

Ich wünsche allen, die dieser Anleitung folgen, viel Erfolg.

Rimini at Nachtfalke-Forum

