PowerVu secrets

by Colibri
January 16, 2005
The newest document is available
at the PowerVu section on http://colibri.de.ms
colibri_dvb@lycos.com

I have analyzed the firmware (the firmware is not read protected or scrambled) from the PowerVu Business Satellite Receiver D9234 (made by Scientific-Atlanta) and found access codes to enter many secret menus. I have found information about the encryption system also.

The PowerVu scrambled AFN – American Forces Network can received from the Hot Bird satellite at 13.0 °E (Freq. 10.775 GHz and 11.096 GHz / Pol. H / 28 MSym).

No guarantee for the correctness of the information provided in this document.

Important information:
The PowerVu encryption system was not hacked. It is still secure. Nobody can watch channels for free with information provided in this document. Only an authorized Internal Security Element (ISE) is able to decrypt the Control Word (CW). The ISE is like a build in smartcard. It is not possible to read out the program code of the ISE or the secret Multi Session Key (MSK) that is used to decrypt a Control Word.

1. Secret Menus

1.1. Back door Menu

To enter the back door menu do the following:

- press menu to enter the main menu
- in the main menu select “2. Receiver Status”
- in the receiver status menu select “2. User Setup”
- in the user setup menu enter the following key sequence to enter the back door menu: Favorite → 0 → Pause → Channel Up

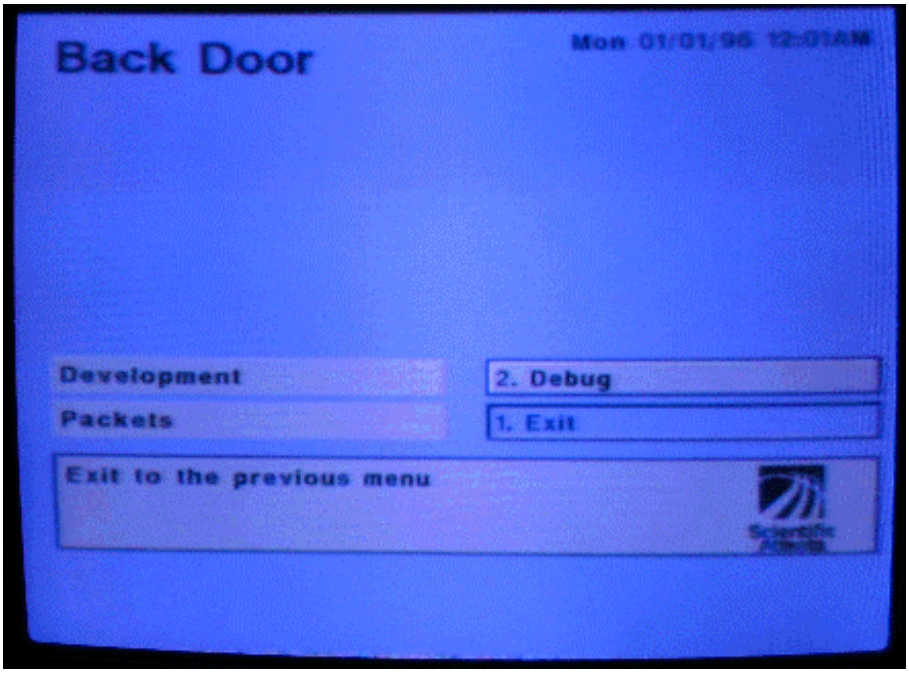

Figure 1 - Back Door Menu

The “Packets” Menu is not implemented.

1.2. Development Menu

To enter the development menu select “Development” in the back door menu.

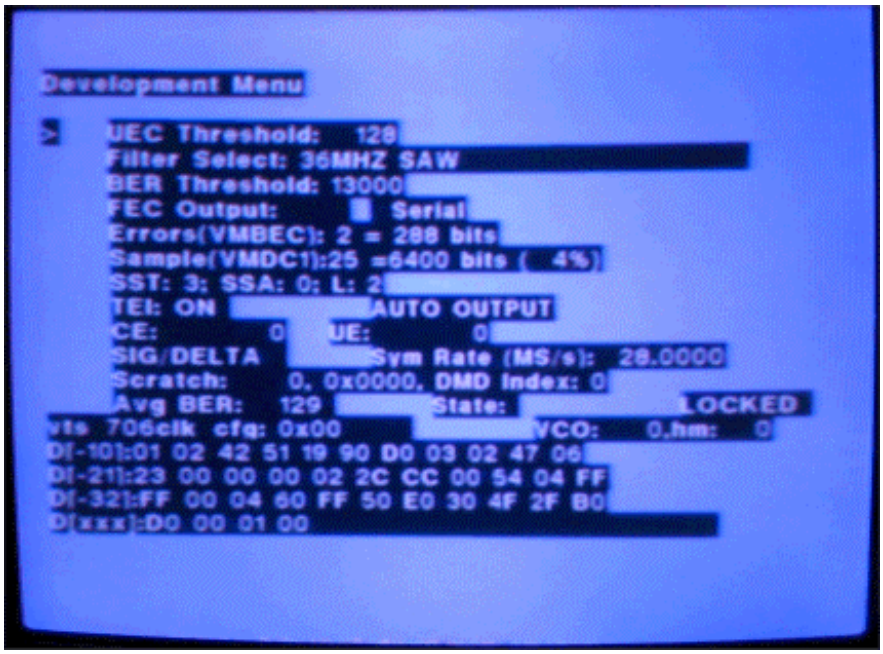

Figure 2 - Development Menu

1.3. Debug Menu

To enter the debug menu select “2. Debug” in the back door menu.

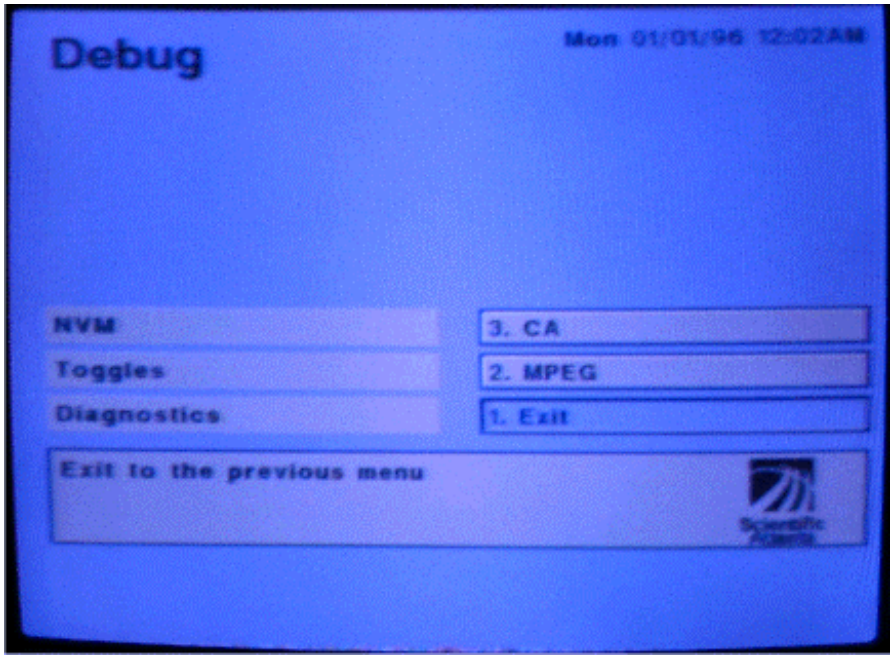

Figure 3 - Debug Menu

1.4. NVM Menu

To enter the NVM menu select “2. Debug” in the back door menu and “NVM” in the Debug Menu.

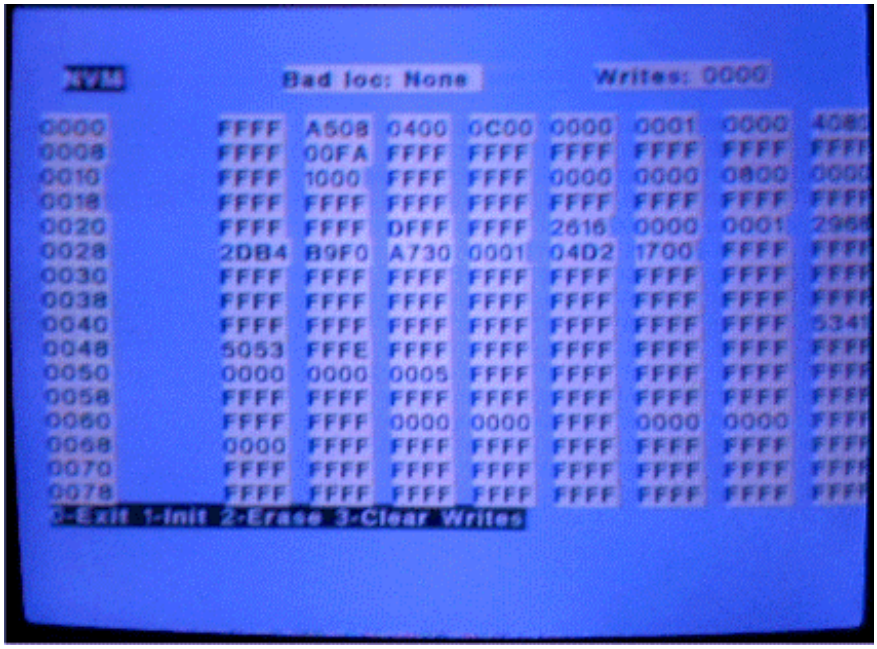

Figure 4 - NVM Menu

1.5. Toggles Menu

To enter the Toggles menu select “2. Debug” in the back door menu and “Toggles” in the Debug Menu.

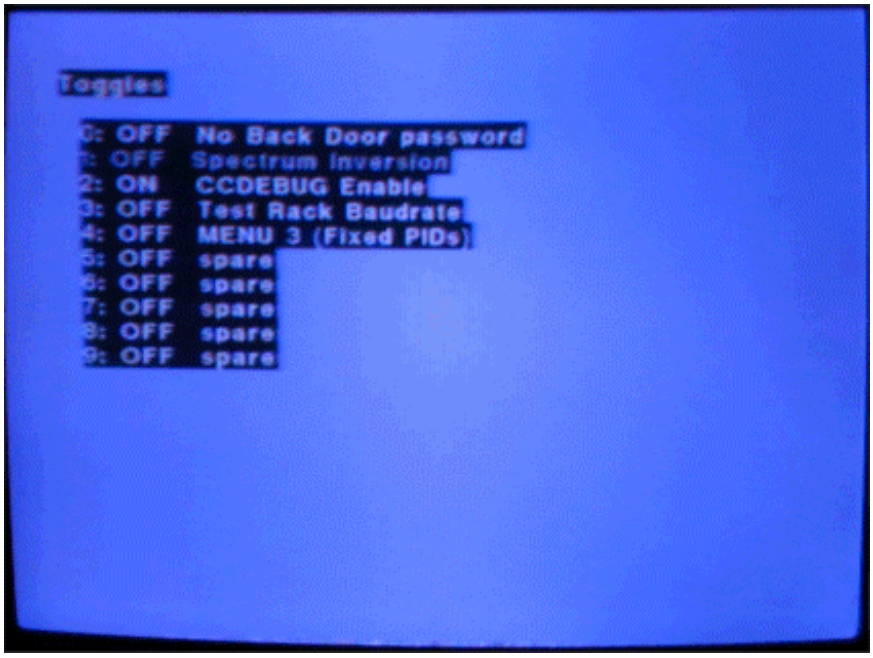

Figure 5 - Toggles Menu

Press the number in front of each line to toggle between the value ON and OFF.

No Back Door password:

- OFF: You must enter the following key sequence to enter the back door menu from the user setup menu: Favorite → 0 → Pause → Channel Up
- ON: You must enter the following key sequence to enter the back door menu from the user setup menu: Favorite → 0

CCDEBUG Enable:

- OFF: Switch the expansion port to the normal mode
- ON: Switch the expansion port to the CCDEBUG mode

Test Rack Baudrate:

- OFF: Set the CCDEBUG baud rate to 115200
- ON: Set the CCDEBUG baud rate to 57600

This menu will only show the spectrum inversion status. Changing is described in 1.19 Download Menu.

1.6. Diagnostics Menu

To enter the Diagnostics menu select “2. Debug” in the back door menu and “Diagnostics” in the Debug Menu.

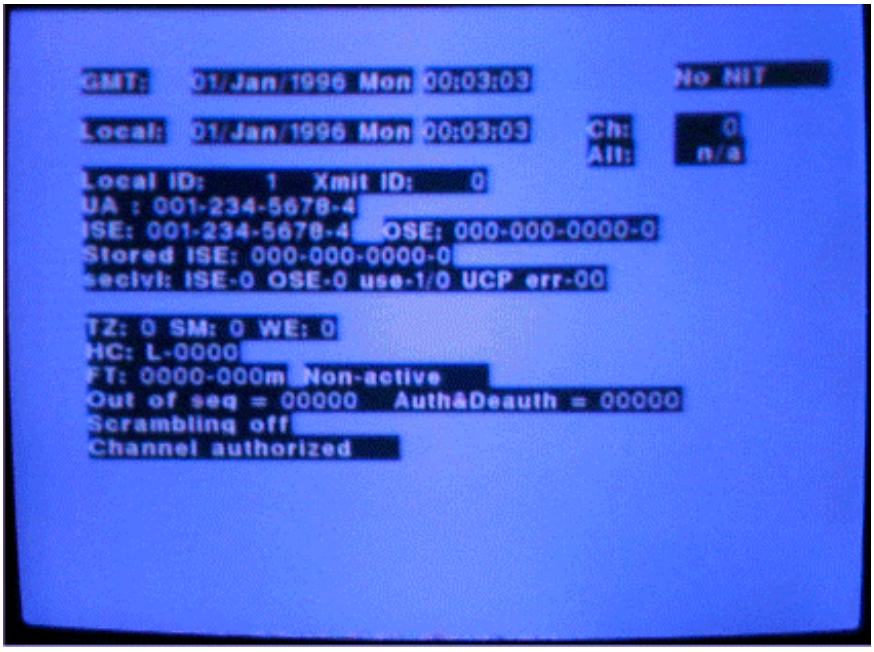

Figure 6 - Diagnostics Menu

1.7. MPEG Menu

To enter the MPEG menu select “2. Debug” in the back door menu and “2. MPEG” in the Debug Menu.

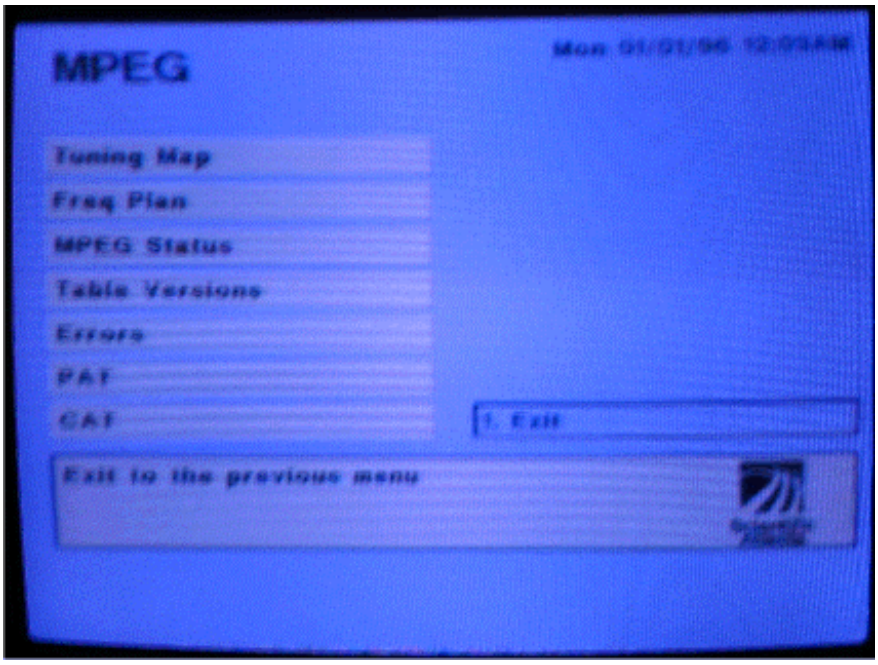

Figure 7 - MPEG Menu

1.8. Tuning Map Menu

To enter the tuning map menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “Tuning Map” in the MPEG menu.

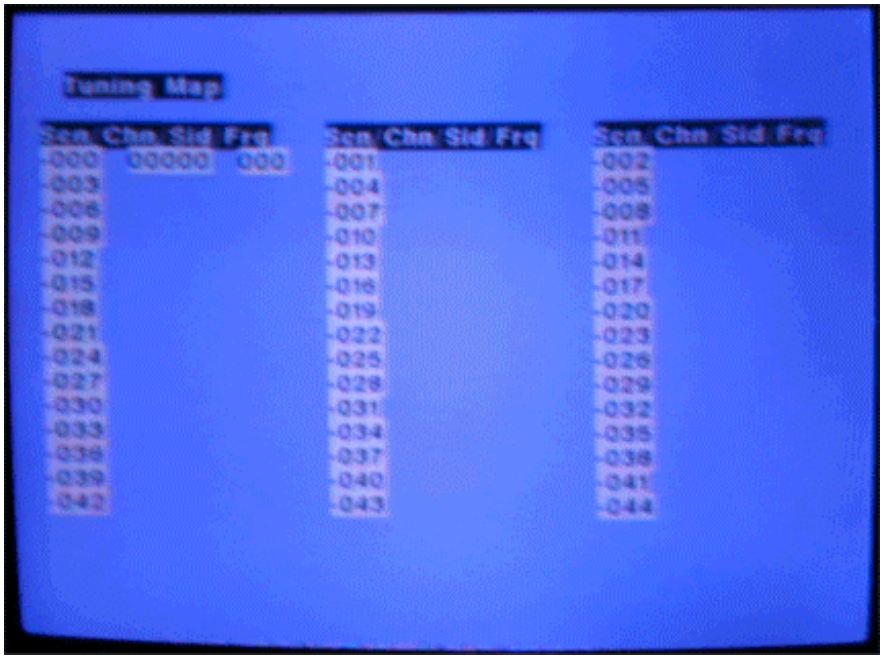

Figure 8 - Tuning Map Menu

1.9. Freq Plan Menu

To enter the tuning map menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “Tuning Map” in the MPEG menu.

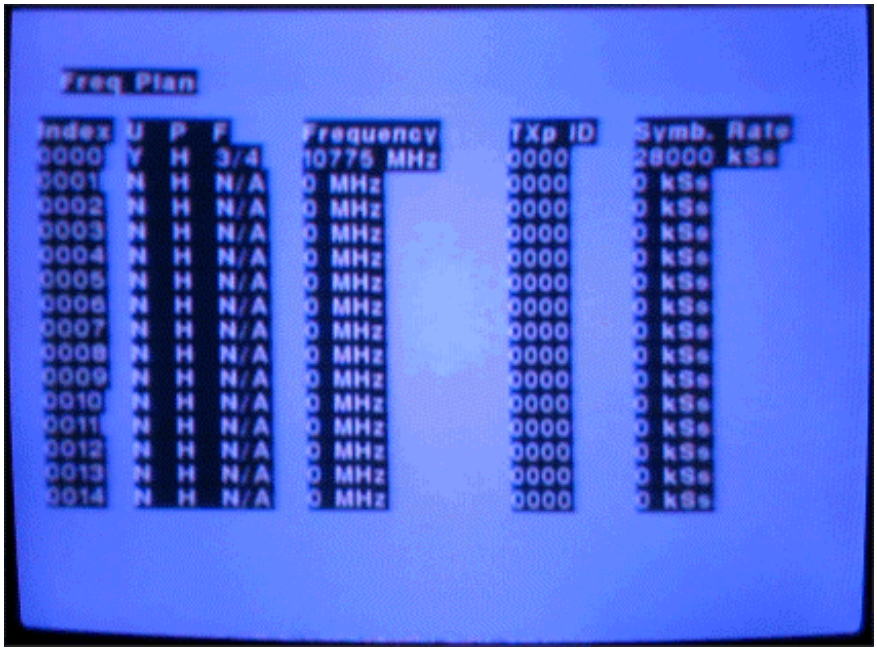

Figure 9 - Freq Plan Menu

1.10. MPEG Status Menu

To enter the MPEG Status menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “MPEG Status” in the MPEG menu.

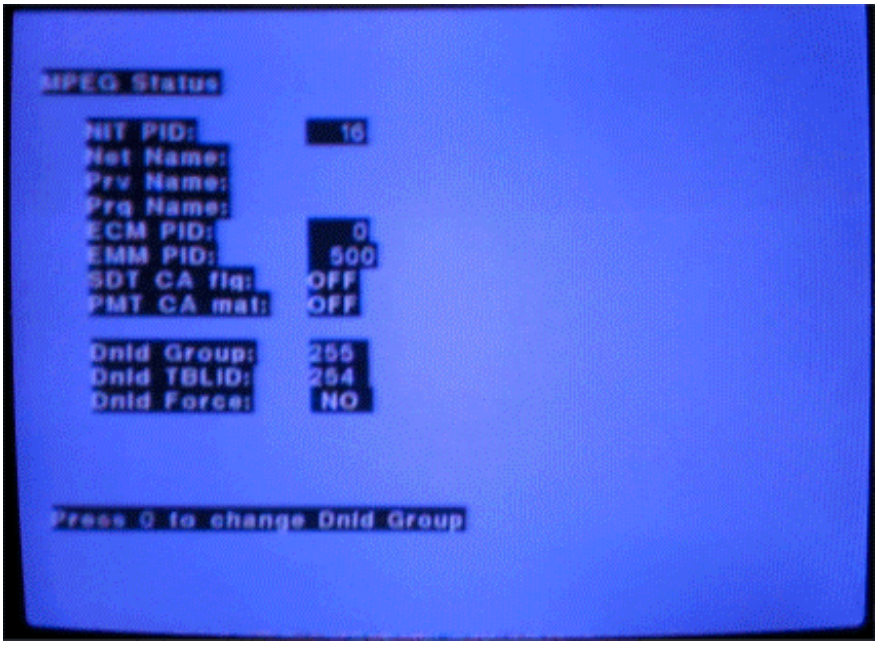

Figure 10 - MPEG Status Menu

1.11. Table Versions Menu

To enter the Table Versions menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “Table Versions” in the MPEG menu.

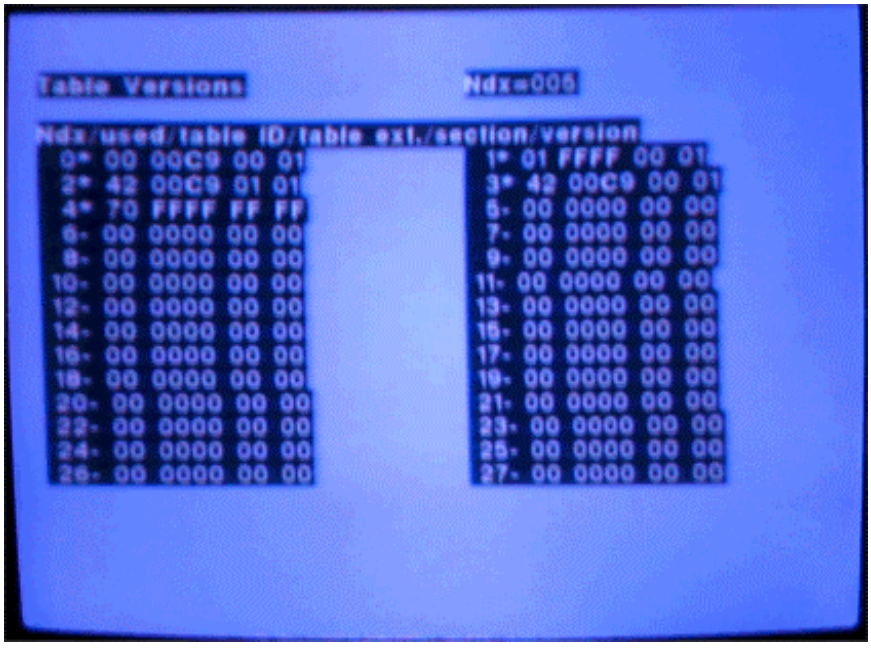

Figure 11 - Table Versions Menu

1.12. Errors Menu

To enter the Errors menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “Errors” in the MPEG menu.

Figure 12 - Errors Menu

1.13. PAT Menu

To enter the PAT menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “PAT” in the MPEG menu.

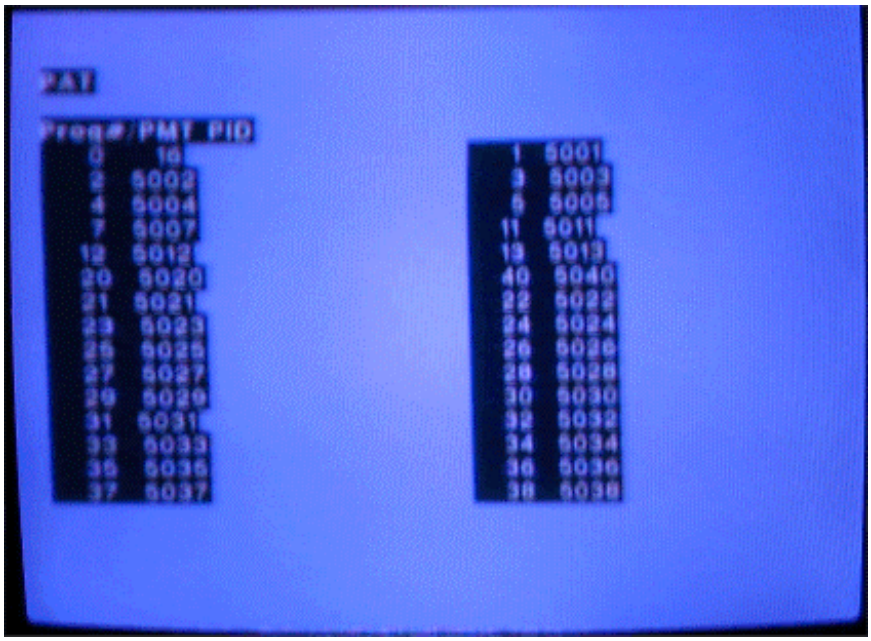

Figure 13 - PAT Menu

1.14. CAT Menu

To enter the CAT menu select “2. Debug” in the back door menu, “2. MPEG” in the Debug Menu and “CAT” in the MPEG menu.

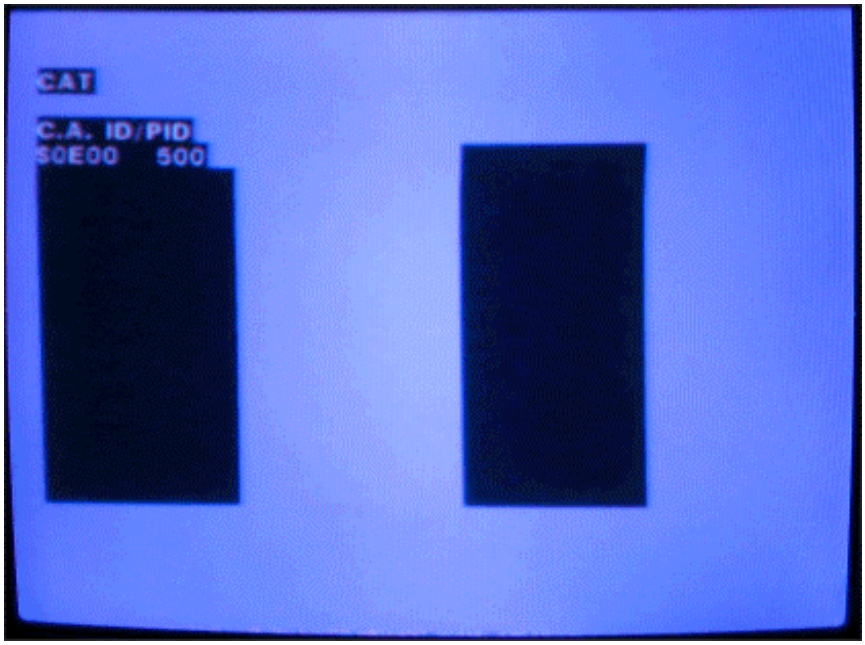

Figure 14 - CAT Menu

1.15. CA Menu

To enter the Diagnostics menu select “2. Debug” in the back door menu and “3. CA” in the Debug Menu.

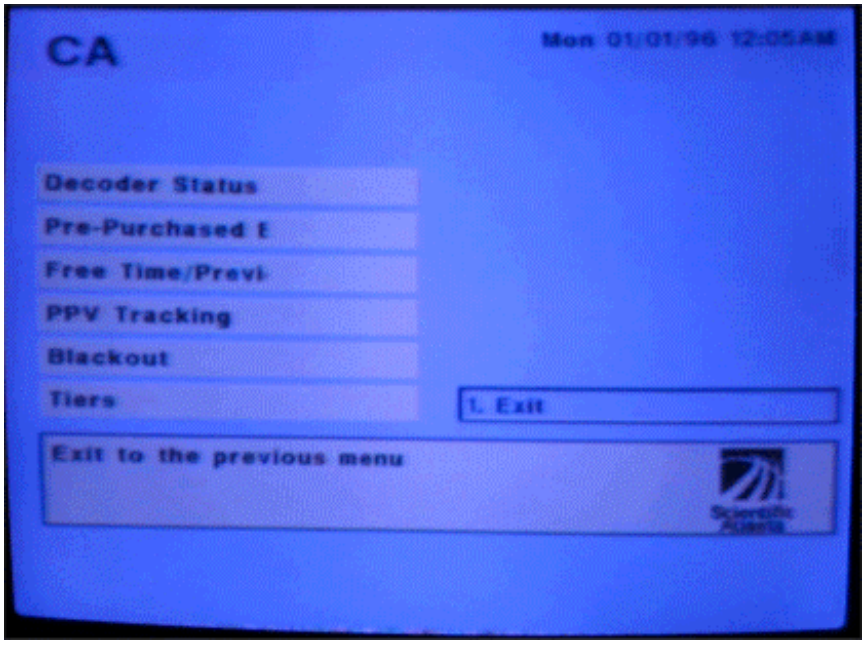

Figure 15 - CA Menu

The menus “Decoder Status”, “Pre-Purchased Events”, “Free Time/Preview” and “PPV Tracking” are not implemented.

1.16. Blackout Menu

To enter the Blackout menu select “2. Debug” in the back door menu, “3. CA” in the Debug Menu and “Blackout” in the CA menu.

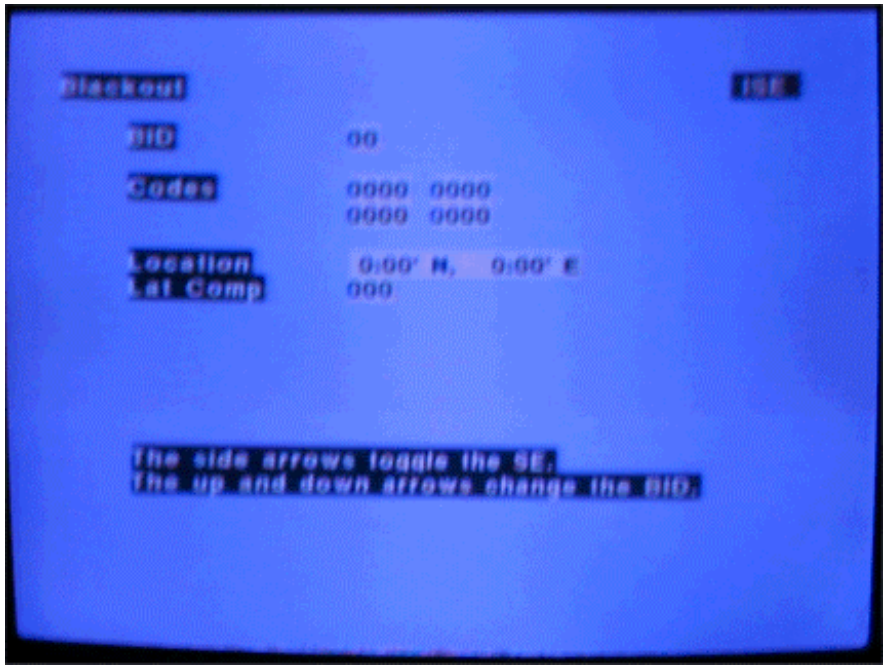

Figure 16 - Blackout Menu

1.17. Tiers Menu

To enter the Tiers menu select “2. Debug” in the back door menu, “3. CA” in the Debug Menu and “Tiers” in the CA menu.

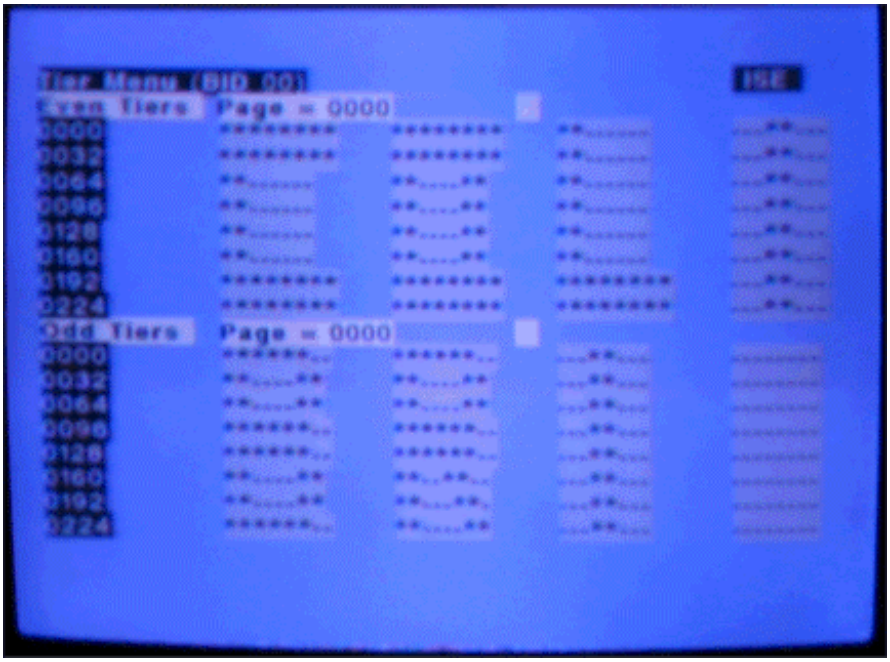

Figure 17 - Tiers Menu

1.18. Fixed PIDs Menu

Press menu to enter the main menu. Press the following key sequence to enter the fixed PIDs Menu:
Info → Info → 4 → 0

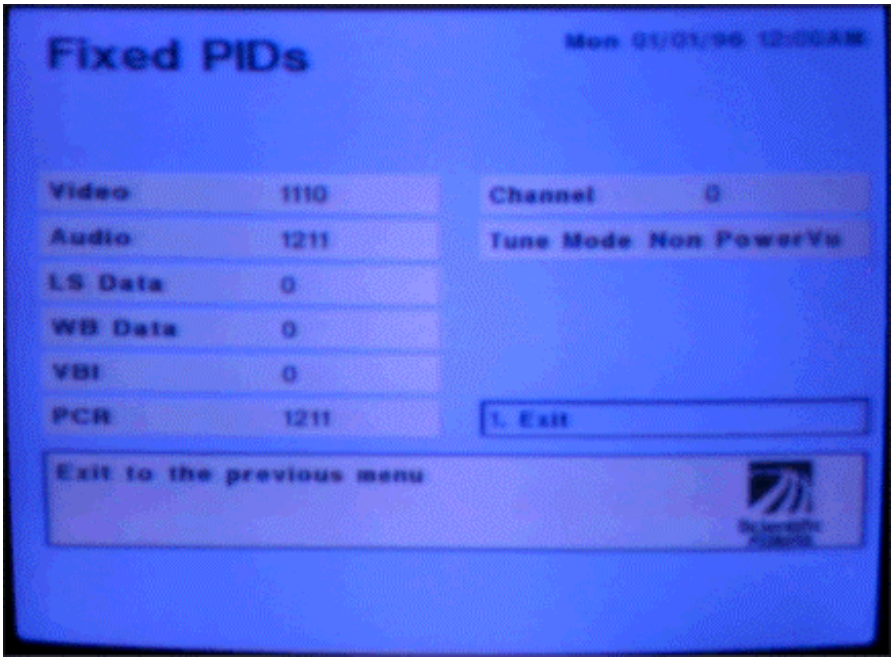

Figure 18 - Fixed PIDs Menu

1.19. Download Menu

To activate the download menu you have two possibilities:

- Disconnect the power cable → press and hold the up and down key on the front panel → connect the power cable → release the up and down key when the download menu is shown
- Press the menu button to enter the main menu → press the up and down key on the front panel at the same time 3 times → press the select key

In the download decoder status menu you can initialise the NVM (this will also unblock all menus and set the pin to the default value “1234”) if you press the down and select key on the front panel at the same time 2 times.

You can toggle the spectrum inversion as follows:
In the download decoder status menu press the left key to enter the download setup menu.
In the download setup menu press the down and select key on the front panel at the same time.

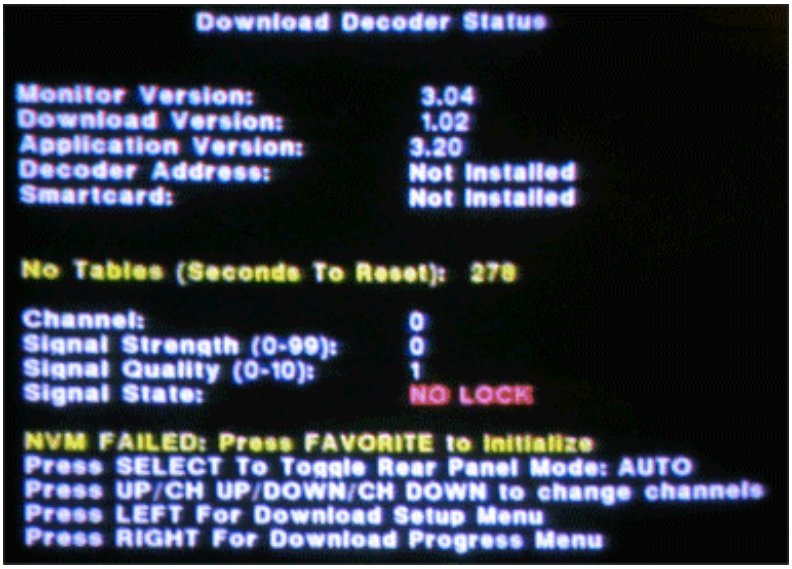

Figure 19 - Download Decoder Status Menu

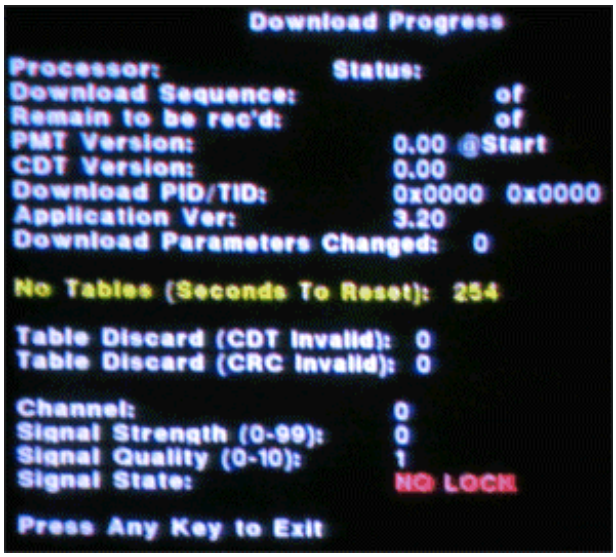

Figure 20 - Download Progress Menu

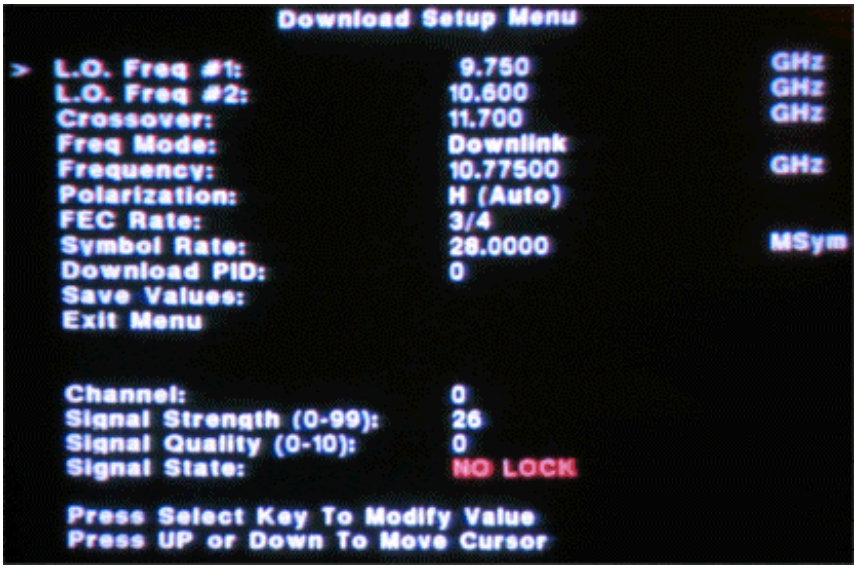

Figure 21 - Download Setup Menu

2. Expansion Port

To connect the expansion port to the serial port of a PC use one of the following cables (don't use a standard 1:1 cable):

IRD - 25 pin expansion port		PC - **25** pin serial com port
pin 12 (remote Rx)	<----------	pin 2 (TxD)
pin 13 (remote Tx)	---------->	pin 3 (RxD)
pin 7 (GND)	----------	pin 7 (GND)

IRD 25 pin expansion port		PC - **9** pin serial com port
pin 12 (remote Rx)	<----------	pin 3 (TxD)
pin 13 (remote Tx)	---------->	pin 2 (RxD)
pin 7 (GND)	----------	pin 5 (GND)

The expansion port can be switched between two modes, the "normal" and the "ccdebug" mode. To change the mode do the following:

- press menu to enter the main menu
- in the main menu select "2. Receiver Status"
- in the receiver status menu select "2. User Setup"
- in the user setup menu enter the following key sequence to enter the back door menu: Favorite → 0 → Pause → Channel Up
- in the back door menu select "2. Debug"
- in the debug menu select "Toggles"
- press "2" to switch the CCDEBUG mode on or off (default is off)

2.1. Normal mode

The commands for the normal mode are not secret. The description can be found in "Appendix C Serial Remote Control Command Set" of the original manual.

The baud rate for this mode can be changed in the user setup menu.
Possible values are 300, 600, 1200, 2400, 4800 or 9600 (the default).

2.2. CCDEBUG mode

The baud rate for this mode can be changed in the toggle menu (press "3" to change it).
If "Test Rack Baudrate" is set to OFF the baud rate is 115200 (the default)
If "Test Rack Baudrate" is set to ON the baud rate is 57600

During a cold start (when the power cable is plugged in) you will receive a text like this on your terminal:

```
Start

Config: 0x00001080 (Max Config: 00003C80)
MV 00000004.00000003
DL Avail
IOP Com. O.K. 00000004
Check CRC ...
CRC O.K.
Launch App
```

```
**************
*  Ver 2.05  *
**************
Compiled by: FURLANO
Date & time: Nov  3 1997, 15:34:29

All printing enabled. Press space bar to toggle on/off.
Time stamping enabled. Press 't' to turn on/off.
Press 'o' to toggle printing of MPEG Xport error messages.
```

Command help:

Command	Description
A	cmd_ydo_plus
B	cmd_yds_plus
Q	cmd_ydo_minus
R	cmd_yds_minus
W	cmd_xdo_plus
S	cmd_xds_plus
V	cmd_xds_minus
Z	cmd_xdo_minus
d	dec_volume()
D	Start Download App.
e	cmd_psi_debug
f or F	Display PID filters
G	Set debug EPG time/disable TDT
h	Display ??? packet header
i	inc_volume()
L	Adjust tuner freq
m	Display MPEG info
o	Display Xport error messages
p	PCR display
P	Toggle PES/non-PES AV
r or s	Toggle RF/SWIF input
t	Toggle system time display
T	Enter system time
u	Toggle tuning mode (DVB/MPEG/FIXED)
v	Get Boot Versions
X or x	Exit to ROM monitor
z	Modify parameters of PCR feedback loop
[or]	Change debug screens
<Space>	Toggle all printing
< or >	Video mode: NTSC/PAL
+	inc_timer()
-	dec_timer()
|	Change modem country
/	Send modem table data
=	Initiate phone home
#	Change LED's
@	Change to SRC
%	nvm_erase()
*	nvm_initialize()
{	cmd_secure_uart_char_wr
}	secure_uart_char_rd()
)	cmd_secure_uart_ctrl_regs_rd
^	VCR communications testing
,	Pan scan value
.	Pan scan value
;	Vid. debug
2	Toggle line 21 test mode
7	Frame skip
8	Frame repeat
9	Mute OFF
0	Mute ON
a	Read STi3520A VID_DCF
b	Status: menu, channel
?	Command help

As shown above you can change debug screens ('[' for previous screen, ']' for next one). The following screens are available:

0	Default
1	Unused???
2	Subtitle Task Error Messages
3	Video Service & Control Task

4	Video Service & Control Task
5	PID Manager Task
6	Control Words
7	TXVER Task
8	Stream Control Task
9	PSI Task
10	RXDCPPKT Task
11	PSIcom
12	Channel Change
13	Channel Change Deluxe
14	Picture Header Info
15	Time Stamps
16	STi3520A Audio Task
17	I/O Processor Task
18	EPG Task
19	Front End Task
20	NVM Messages
21	MPEG Transport Error Messages
22	Line 21/Closed Captioning
23	Video bit buffer levels

For example if you switch to the debug screen “6. Control Words” on an authorized IRD then you will get an continue output of all (video, audio, ...) decrypted (plain) control words for this channel (odd and even CWs). This plain CWs are DES keys that are used to scramble (DES-ECB mode) the channel.

During a CCDEBUG session you can press <Control-C> to enter the BRKSIG menu:

```
BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: E

00  00  CLR     01  00  CLR     02  00  CLR     03  02  CLR
04  00  CLR     05  00  CLR     06  00  CLR     07  00  CLR
08  00  CLR     09  00  CLR     10  00  CLR     11  00  CLR
12  00  CLR     13  00  CLR     14  00  CLR     15  04  CLR
16  00  CLR     17  00  CLR     18  00  CLR     19  00  CLR
20  00  CLR     21  00  CLR     22  00  CLR     23  00  CLR
24  00  CLR     25  00  CLR     26  00  CLR     27  00  CLR
28  00  CLR     29  00  CLR     30  00  CLR     31  00  CLR
32  00  CLR     33  00  CLR     34  17  CLR     35  00  CLR
BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: P
PID   NAME    STAT  WHO  SP    P1    P2     RET   TCNT  SPTOP  SPMAX  PC
 01 BRKSIG   READY 00 0C8A7C 0C8A7C 000000 0001  184EA 0C8890 0C89E8 1016C
 02 VIDSERV  EVTBK 03 0C8C98 0C8C98 000000 0003  2FAA 0C8AD0 0C8C98 1016C
 03 ISETASK  RCABK 00 0C9094 0C9094 0C90F8 0005  01AA 0C8D10 0C9008 1016C
 04 TBL2ISE  EVTBK 15 0C92D0 0C92D0 000000 0001  0013 0C9150 0C92D0 1016C
 05 FRONT    DELAY 01 0C9568 0C9568 000000 0000  77D8 0C9390 0C9548 1016C
 06 VIDCTRL  DELAY 01 0C97A0 0C97A0 000000 0001  1BD4 0C95D0 0C972C 1016C
 07 AUDCTRL  DELAY 05 0C9BF8 0C9BF8 000000 0000  0595 0C9810 0C9BF8 1016C
 08 STRMCTL  RCABK 00 0C9DF0 0C9DF0 0C9E38 000B  0060 0C9C50 0C9DF0 1016C
 09 RXDCPPKT RCABK 00 0CA1F4 0CA1F4 0CA278 0001  01EA 0C9E90 0CA178 1016C
 10 PSITASK  DELAY 01 0CB4E0 0CB4E0 000000 0001  25E7 0CAA10 0CB4B0 1016C
 11 TBLEVAL  RCABK 00 0CCB5C 0CCB5C 0CCB60 0001  2B7D 0CC510 0CCAD8 1016C
 12 EPG      DELAY 01 0CA96C 0CA96C 000000 0000  8D19 0CA2D0 0CA910 1016C
 13 SUBTITLE DELAY 01 0CB718 0CB718 000000 0000  0986 0CB550 0CB718 1016C
 14 IOP TASK DELAY 01 0CB928 0CB928 000000 0000  8A5F 0CB790 0CB900 1016C
 15 TEST1    DELAY 50 0CBB7C 0CBB7C 000000 0000  00FC 0CB9D0 0CBB64 1016C
 16 VIDWDOG  DELAY 05 0CBDE0 0CBDE0 000000 0000  0208 0CBC10 0CBDE0 1016C
 17 SRC      EVTBK 34 0CC02C 0CC02C 000000 0001  0081 0CBE50 0CBFE8 1016C
 18 CCDEBUG  READY 01 0CC248 0CC248 000000 0070  1160 0CC090 0CC15C 1016C
 19 AVSQUE   READY 01 0CC4A8 0CC4A8 000000 0001  1267 0CC2D0 0CC474 1016C
Hit any key to continue, x to exit.
PID   NAME    STAT  WHO  SP    P1    P2     RET   TCNT  SPTOP  SPMAX  PC
 20 SELFTEST READY 02 0CCE48 0CCE48 000000 0000  16EA 0CCBD0 0CCD28 1016C
 21 DVBCLEAN READY 02 0CD43C 0CD43C 000000 0000  0937 0CD250 0CD41C 1016C
 22 CHANNEL  DELAY 02 0CD1E8 0CD1E8 000000 0000  0A8B 0CCF10 0CD158 1016C
 23 NULL     READY 00 0CD590 000000 000000 3D98C  74015 0CD490 0CD590 2A678

BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
```

```
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: M
Start addr :0
End addr:   80
Press 'x' to stop
00000000: EA000021 EA000012 EA000018 EA000010
00000010: EA00000F EA00000E EA000006 E82D40FF
00000020: E59F100C E1A0E00F E591F000 E9BD40FF
00000030: E25EF004 0000207C E82D5FFF E59F100C
00000040: E1A0E00F E591F000 E9BD5FFF E25EF004
00000050: 00002078 E82D5FFF E59F100C E1A0E00F
00000060: E591F000 E9BD5FFF E1B0F00E 00002084
00000070: E82D5FFF E59F100C E1A0E00F E591F000


BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: C
Kcall Counters:

# of Entries through TRAP          = 009192
# of Entries through KENTRY        = 000822
# of INT RTEs  (already in kernel)  = 000028
# of INT RTEs  (NR)                 = 000013

# of INT RTEs  (multiple INTs)      = 000000
# of INT Exits through kernel (RR)  = 000781
# of Exits through run_process (RR) = 009973
# of Exits through run_process (NR) = 000002

BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: W
PID   NAME   BANK
 01 BRKSIG    00001800
 02 VIDSERV   00001800
 03 ISETASK   00001800
 04 TBL2ISE   00001800
 05 FRONT     00001800
 06 VIDCTRL   00001800
 07 AUDCTRL   00001800
 08 STRMCTL   00001800
 09 RXDCPPKT  00001800
 10 PSITASK   00001800
 11 TBLEVAL   00001800
 12 EPG       00001C00
 13 SUBTITLE  00001800
 14 IOP TASK  00001800
 15 TEST1     00001800
 16 VIDWDOG   00001800
 17 SRC       00001C00
 18 CCDEBUG   00001800
 19 AVSQUE    00001800
Hit any key to continue, x to exit.
PID   NAME   BANK
 20 SELFTEST  00001800
 21 DVBCLEAN  00001800
 22 CHANNEL   00001800
 23 NULL      00001800
 24 ê  00000000

BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: Z
Average Timing
  Task      Total(mSec)  Pct.     # calls    Last(mSec)   Avg.(mSec)
  KERNEL        6068.6  42.36       9973          0.0          0.6
  BRKSIG        1106.2   7.72       1376          0.0          0.8
  VIDSERV        135.5   0.94        547          0.3          0.2
  ISETASK          4.7   0.03         17          0.0          0.2
  TBL2ISE          0.2   0.00          3          0.0          0.0
  FRONT          340.8   2.37       1156          0.4          0.2
  VIDCTRL         79.1   0.55        406          0.0          0.1
  AUDCTRL         15.8   0.11        181          0.1          0.0
  STRMCTL          1.0   0.00          3          0.0          0.3
```

```
  RXDCPPKT          5.4   0.03          38          0.0         0.1
  PSITASK         107.8   0.75         416          0.2         0.2
  TBLEVAL         123.7   0.86        1105          0.0         0.1
  EPG             401.3   2.80        1538          0.0         0.2
Hit r to reset average, x to exit,
any other key to continue.
  Task      Total(mSec)  Pct.     # calls    Last(mSec)   Avg.(mSec)
  SUBTITLE         27.0   0.18         355          0.0         0.0
  IOP TASK        393.5   2.74         356          0.7         1.1
  TEST1             2.8   0.01          34          0.0         0.0
  VIDWDOG           5.7   0.03          72          0.1         0.0
  SRC               1.4   0.00          14          0.0         0.1
  CCDEBUG          49.4   0.34          40          0.0         1.2
  AVSQUE           52.3   0.36         355          0.1         0.1
  SELFTEST         65.1   0.45         553          0.1         0.1
  DVBCLEAN         26.2   0.18         352          0.0         0.0
  CHANNEL          29.9   0.20         364          0.0         0.0
  NULL           5279.5  36.86         692          0.5         7.6
  Total         14322.9 100.00
Hit r to reset average, x to exit,
any other key to continue.

BRKSIG   is starting to execute.
E)vents,P)cb,S)tep,T)race,B)reak_on_pid,M)emory,R)eset,L)og
1)set_event,0)clear_event,H)alt,U)nhalt,I)history,C)ounters,
D)ma_history,Y)nterrupt_history,A)VS buffers,W)Bank,Z)Timing,X)it: X
```

3. XPeRT MONITOR

To get access to the XPeRT MONITOR you must connect the expansion port to your computer via a special cable (the cable is described in 2 Expansion Port). Start a terminal program (e.g. the in Windows included HyperTerminal). You must use “none” as handshake setting. The default baud rate is 115200 (if this will not work use 57600 or 9600 instead). If “Offline” is displayed in the status line, type a key (e.g. space bar) to change it to established. Disconnect the power cable of your D9234, then connect it again and press the key ‘x’ before “Check CRC ...” is shown. On IRDs with an old boot version (e.g. 3.04) the information “press ‘x’ to start monitor” is shown, on newer boot versions (e.g. 4.03) the information how to enter the monitor is hidden, but entering the monitor will still work.

Boot version 3.04

```
Start

Config: 0x00000080 (Max Config: 00003C80)
MV 00000003.00000004
Downloader present
Waiting (press 'x' to start monitor)
Check CRC ...
CRC O.K.
Starting The Application
```

Boot version 4.03

```
Start

Config: 0x00001080 (Max Config: 00003C80)
MV 00000004.00000003
DL Avail
IOP Com. O.K. 00000003
Check CRC ...
CRC O.K.
Launch App
```

Type a „?“ at the command prompt „>“ and you will get a command summary

```
>?

     XPeRT MONITOR Vers. 00000004.00000003

                        Command Summary
```

```
B<baud rate> - Set Baud Rate: baud rate = <9600|57600|115200>
C[Flash Area] - Erase Flash default = app, 1 = Boot Area
D - Download request
N - Switch the verify flag to ON or OFF
Q<b|s><SPACE><address><CR|SPACE> - Read 8<b> or 16<s> bit data from <address>
W<b|s><SPACE><address><SPACE><data><CR|SPACE> - Write 8<b> or 16<s> bit data
                                More - Press any key
c - Check CRC32 of the application
d<start_address><CR|SPACE><end_address> - Dump memory
e - Run Application
g<address> - Execute code starting from the given address
h or ? - Get help
k[start address] - Load into Flash an IHF file from the serial port
l[start address] - Load into RAM an IHF file from the serial port
r<address> - Read a word from a selected address
w<address><SPACE><data> - Write a word to a selected address
y<bank> - Enable Bank, Bank = 00, 01, 10 - 17, 20, 21
z - Display the bank configuration
# - Null command, waits for CR

All commands are terminated with CR or SPACE (with more messages)
>
```

4. Disable menu lockout and recover a lost pin

It is possible the change the standard pin “1234” and protect access to the menus.
If you forgot the pin then the receiver is may be unusable.

To disable the menu lockout do the following:

- connect the serial port of a PC to the expansion port as described in “2 Expansion Port”
- the expansion port must be in normal mode (CCDEBUG mode will not work)
- open a terminal session (e.g. with the windows “Hyper Terminal”)
- if you don’t know the baud rate that is configured in the user setup menu the you must try all possible values (300, 600, 1200, 2400, 4800 or 9600 the default)
- enter the command “`SA1LOCK=0`” to disable the menu lockout (if the command was successful the receiver will respond with “`LOCK=0`”)

To recover a lost pin do the following:

- press menu to enter the main menu
- in the main menu select “2. Receiver Status”
- in the receiver status menu select “2. User Setup”
- in the user setup menu enter the following key sequence to enter the back door menu: Favorite → 0 → Pause → Channel Up
- in the back door menu select “2. Debug”
- in the debug menu select “NVM”
- write down the hexadecimal pin value at address 2C
- convert the hexadecimal value to decimal (e.g. via the windows calculator)
- this decimal value is the current pin (if the value is less then 4 digit long then fill them up with leading zeros)

Here are examples:
If the hexadecimal value is “04D2” then the pin is “1234” (the default pin).
If the hexadecimal value is “0055” then the pin is “0085”.

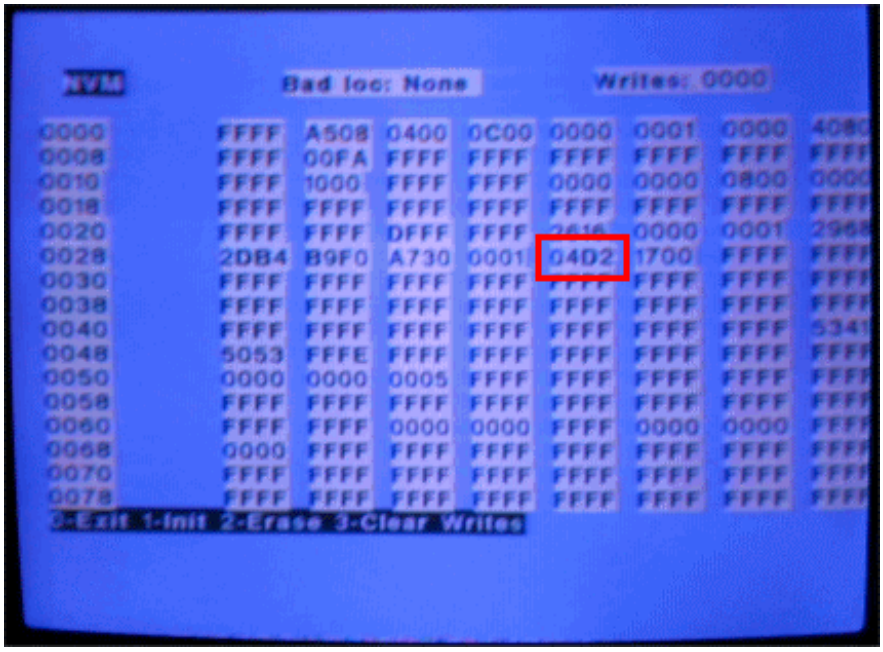

Figure 22 - NVM Menu with marked PIN

Alternatively you can reset all setting to factory default. This will also unblock all menus and set the pin to the default value “1234”. The procedure is described in the in the chapter 1.19 Download Menu.

5. Unstable picture or menu text

It is possible that you can’t read the menus because the menu text scrolls very fast vertically. The reason for this is that you have different video modes set between your receiver and the TV. To change the video mode (NTSC => PAL-B => PAL-M => PAL-N) on the receiver press the up and the select key on the front panel at the same time for 2 times. Repeat this until the picture is stable.

6. PowerVu Conditional Access system

Before you continue please read the basics about the PowerVu Conditional Access (CA) system first:
Go to http://www.sciatl.com/products/customers/whitepapers.htm and select
“Content Origination and Distribution Part II - Secure Broadcasts with Originator Encoder”

An other interesting site is: http://www.growl.de/d9234

6.1. Internal Security Element (ISE)

Here is a picture of the ISE Chip:

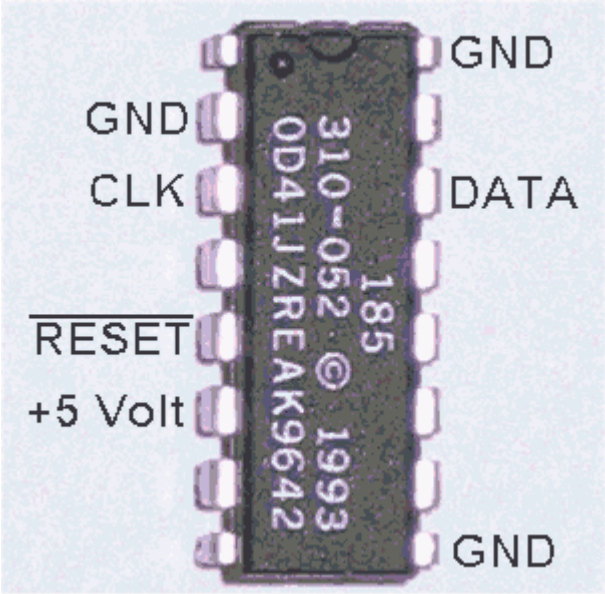

Figure 23 - ISE Chip

The back site of the chip is labeled with „PHILIPPINES“.

The IRD have a slot for the Outboard Security Element (OSE), a smartcard, also.

The baud rate of the serial data pin of the ISE depends from the frequency on the clk input pin. The baud rate is calculated as follows:
baud rate = clk / 32 decimal
The IRD have an oscillator with 8 MHz. This frequency is divided by two by a circuit before it feeds the clk pin of the ISE with 4 MHz. The resulting baud rate is 125000 Bit/sec.
If you want to log the traffic by an serial com port from an PC this will not work, because a PC does only support standard baud rates like 115200 Bit/sec.
But if you change the oscillator to 7.3728 MHz then the baud rate will be 115200 Bit/sec.
If you connect an RS232 converter between the ISE data pin and the RxD pin of the serial com port of a PC the you can log the ISE traffic.
After the change the IRD will continue work as expected, because this oscillator provides not only the ISE, it provides also the UART of the IRD that is used for the ISE communication.

The ISE has a special usage of the parity bit (it don’t uses the typical settings 8N1, 8O1 or 8E1). The first byte (the length byte) of a command or answer block is transmitted with the parity bit set (8M1 = 8 data bits / Mark parity / 1 stop bit). The remaining bytes of a command or answer block are transmitted with the parity bit cleared (8S1 = 8 data bits / Space parity / 1 stop bit).

The command block is structured as follows:

Length byte	Command byte	Optional data bytes	Checksum
Parity set	Parity cleared	Parity cleared	Parity cleared
The length byte includes the command byte and the optional data bytes. The length byte itself and the checksum byte are not included.			if you add all bytes of the command block (length byte, command byte, optional data bytes and the checksum byte itself) the last byte of the result must be 0.

The answer block is structured as follows:

Length byte	Optional data bytes	Checksum
Parity set	Parity cleared	Parity cleared
The length byte includes the optional data bytes. The length byte itself and the checksum byte are not included. ISE will signal an error with length byte = FF (no data or checksum follows).		if you add all bytes of the answer block (length byte, optional data bytes and the checksum byte itself) the last byte of the result must be 0.

6.1.1. Command overview

Length without the length byte and the checksum byte	Command	Description
15	00	Get base CW
20	01	Get CW seeds for Video, Audio 1 & 2, High Speed Data (HSD), Utility and VBI
1C	03	Send EMM
01	04	Double decrypts the EMM
01	05	NOP (no operation)
01	08	Get CW seeds for Audio 3 & 4
06	0A	Sends the OSE serial to the ISE
01	20	Get Serial, Version, AlgoNr and ISE-Type
02	21	Get even Tiers
02	22	Get odd Tiers
02	25	Get Blackouts
03	26	Get tiers page number
05	2C	Send Serial and get security level

The following tables are constructed as follows:

1st line: Byte position or byte range of the command or answer array (starting with 0)
The value in brackets shows the length of the range

2nd line: Bit position or bit range of the byte (bit pos 7 = MSB / bit pos 0 = LSB).
if this field is empty then the meaning is 7..0 (the entire byte)

3rd line: A typical value of a field

4th line: Description

6.1.2. Command 00

A part of the ECM is send to the ISE. The answer includes the base CW.

Command:

0	1	2..11 (10)	12..15 (4)	16
15	0		0	
Length	Command	Part of ECM		Checksum

Answer:

0	1	1	2..8 (7)	9
	7	6..0		
8				
Length	1 = no MSK present to calc the base CW		base CW	Checksum

6.1.3. Command 01

A part of the ECM is send to the ISE. The answer includes CW seeds for Video, Audio 1 & 2, High Speed Data (HSD), Utility and VBI.

Command:

0	1	2..20 (1F)	21
20	1		
Length	Command	Part of ECM	Checksum

Answer:

0	1	1	1	1	1	1
	7	6	5	4	3	2
20						
Length	1 = send command 08 to retrieve CW seeds for Audio 3 & 4		1 = Video CW seed field is valid	1 = Audio 1 CW seed field is valid	1 = HSD CW seed field is valid	1 = Audio 2 CW seed field is valid

1	1	2..5 (4)	6..8 (3)	9..C (4)	D..F (3)	10..11 (2)
1	0					
1 = Utility CW seed field is valid	1 = VBI CW seed field is valid	Video CW seed	Audio 1 CW seed	HSD CW seed	Audio 2 CW seed	Utility CW seed

12..13 (2)	14..1A (7)	1B..1C (2)	1D..20 (4)	21
VBI CW seed		Error number		Checksum

I have found the following error table in the IRD firmware. It is possible that not all error numbers are relevant to command 01. Perhaps a few error numbers are used IRD internally only.

Error number table:

Error number	Description
0000	No error
F01E	No Authorization Key
F01F	Program is Authorized
F020	Program is NOT Authorized
F021	Program is Blacked Out
F024	Replace Smartcard
F025	This is a PPV Program Press 1 Buy Program Press 2 Free Preview.
F028	Insufficient Credit to Buy This Program
F03D	Not Authorized. Call Your DTH Operator to Order This Program
F03E	Not Authorized. Press SELECT for Free Preview, or Call Your DTH Operator to Order This Program.
F051	Not Authorized. Press SELECT to Buy This Program.
F052	Not Authorized. Press SELECT to Buy or Preview This Program.
F055	Buy Program? Press SELECT to Confirm.
F056	Insufficient Credit to Buy This Program
F057	Ippv Tracking Buffer Full
F058	No More Free Previews Available
F082	DCP General Message
F096	Please Upgrade Your Smartcard
F09B	DVB Scrambling Not Supported
F0C8	ISE NVM Failure
F0CA	Waiting For Signal
F0CB	No Signal
F0CC	Parental Rating Failure
F0CD	Searching
F0CE	Monitor Mismatch

6.1.4. Command 03

A part of the EMM is send to the ISE.

Command:

0	1	2..1C (1B)	1D
1C	3		
Length	Command	Part of EMM	Checksum

Answer:

0	1	1	1	2
	7	6	5..0	
1				
Length	0 = Command 04 (EMM double decryption) is necessary	1 = ADP check error (e.g. the EMM was corrupt, manipulated or not for this ISE serial number)		Checksum

6.1.5. Command 04

EMM double decryption
This command is send to the ISE dependent of the command 03 answer

Command:

0	1	2
1	4	
Length	Command	Checksum

Answer:

0	1	1	1	2
	7	6	5..0	
1				
Length		1 = ADP pending error		Checksum

6.1.6. Command 05

NOP (No OPeration) command
This command is regular send to the ISE. It checks if the communication to the ISE is ok.

Command:

0	1	2
1	5	FA
Length	Command	Checksum

Answer:

0	1
0	0
Length	Checksum

6.1.7. Command 08

This command is send to the ISE dependent of the command 01 answer. The answer includes CW seeds for Audio 3 & 4.

Command:

0	1	2
1	8	F7
Length	Command	Checksum

Answer:

0	1	1	1	2..3 (2)	4..6 (3)	7..9 (3)	A
	7	6	5..0				
9							
Length	1 = Audio 3 CW seed field is valid	1 = Audio 4 CW seed field is valid			Audio 3 CW seed	Audio 4 CW seed	Checksum

6.1.8. Command 0A

This command sends the serial number of the Outboard Security Element (OSE), the smartcard, to the ISE.

Command:

0	1	2	3..6 (4)	7
6	A			
Length	Command		OSE Serial	Checksum

Answer:

0	1
0	0
Length	Checksum

6.1.9. Command 20

This command is used to get information about the ISE/OSE (e.g. version, algorithm number or type).

Command:

0	1	2
1	20	DF
Length	Command	Checksum

Answer:

0	1..4 (4)	5	6	6	7	8	8
			7..4	3..0		7	6..5
8		2	2	1	5	0	0
Length	Serial number of the ISE	Algorithm number		Major version	Minor version	1 = send command 2C with OSE serial number to ISE	Type 0=UCP 1=CPL 2=WCP 3=SCP

8	8	9
4	3..0	
1	4	
1 = Command 26 is supported The tiers menu will show the correct page number. 0 = Command 26 is not supported. The tiers menu will show “Page = ----”		Checksum

6.1.10. Command 21

This command will return the even tiers.
Tiers can be viewed via the secret tiers menu also (1.17 Tiers Menu).

Command:

0	1	2	3
2	21		
Length	Command	Tiers BID (valid values are 0..3)	Checksum

Answer:

0	1..20 (20)	21..22 (2)	23
22			
Length	Even tiers	if this two bytes are not equal then only the first C bytes from the previous field “Even tiers” are shown in the tiers menu. The last 13 bytes are overwritten by 0. The tiers menu will also show a “X” instead of an space right of the “Page = ...” field.	Checksum

The tiers array from the answer is 20 bytes long (= 100 bits to represent 100 tiers). If the bit is 1 then the tier is activated. If the bit is 0 then the tier is deactivated.
Byte 0 bit 7 is tier number 0
Byte 1F bit 0 is tier number FF

Examles:

```
80 00 00 ... => only tier number 0 is activated

03 00 00 ... => Tiers number 6 and 7 are activated

00 02 00 ... => only tier number D is activated

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 01   => only tier number FF is activated

FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF   => all tiers from 0 till FF are activated
```

6.1.11. Command 22

This command will return the odd tiers.
Tiers can be viewed via the secret tiers menu also (1.17 Tiers Menu).

Command:

0	1	2	3
2	22		
Length	Command	Tiers BID (valid values are 0..3)	Checksum

Answer:

0	1..20 (20)	21..22 (2)	23
22			

Length	Odd tiers	if this two bytes are not equal then only the first C bytes from the previous field “Odd tiers” are shown in the tiers menu. The last 13 bytes are overwritten by 0. The tiers menu will also show a “X” instead of an space right of the “Page = ...” field.	Checksum

6.1.12. Command 25

This command will return blackout information.
Blackout information can be viewed via the secret blackout menu also (1.16 Blackout Menu).

Command:

0	1	2	3
2	25		
Length	Command	BID (valid values are 0..3)	Checksum

Answer:

0	1..2 (2)	3..4 (2)	5..6 (2)	7..8 (2)
D				
Length	Code1	Code2	Code3	Code4

9..A (2)	B..C (2)	D	E
Location if positive then north else south hours = value / 60 minutes = value modulo 60	Location if positive then east else west hours = value / 60 minutes = value modulo 60	Lat Comp	Checksum

6.1.13. Command 26

Get tiers page number. The page number will be shown in the tiers menu.

Command:

0	1	2	3	4
3	26		0	
Length	Command	BID (valid values are 0..3)		Checksum

Answer:

0	1	2	3
2	0	0	
Length	Even tiers page number	Odd tiers page number	Checksum

6.1.14. Command 2C

Send Serial and get security level.

Command:

0	1	2..5 (4)	6
5	2C		
Length	Command	serial number of the other SE OSE serial number if sent to ISE ISE serial number if sent to OSE	Checksum

Answer:

0	1..4 (4)	5	6
5			
Length		Security level	Checksum

6.2. ECMs

ECM packets can received via the PIDs described in 6.4 Plain control word calculation.

ECM packet:

0	1	1	2	3	3	4
	7..4	3..0		7..4	3..0	
80 or 81	3	03D		3	037	
Table ID		Section length			Length	

5	6..7 (2)	8	9	A	B	C..1B (10)	1C
20	0E00	0	0	0		A0 00 ...	0
Tag	0E00 = CAID of Scientific Atlanta			Security level	Continuous counter	Encrypted base CW will be send via command 00 to the xSE If bit 6 of the first byte is 0 it will be send to the ISE (the default). If it is 1then it will be send to the OSE (the smatcard).	

1D..2B (1F)	2C..2F (4)
Encrypted CW seeds for Video, Audio 1 & 2, High Speed Data (HSD), Utility and VBI. Will be send via command 01 to the ISE. The first two byte are the channel ID (a table can be found at 6.4 Plain control word calculation)	DVB CRC32

6.3. EMMs

EMM packets can received via the PID 1F4.

EMM packet:

0	1	1	2	3	4	5	6..7 (2)	8	9	A
	7..4	3..0								
82	3	09B 04A		10	99 48	01	0E00	0	0	6
Table ID		Length incl. DVB CRC32		Tag	Length incl. DVB CRC32		0E00 = CAID of Scientific Atlanta			

B	C..F (4)	10	11	12
8F 3E		0	0	3
Length incl. 1st byte of DVB CRC32	Unique Address (UA) If the UA is not equal to the ISE or OSE serial number the IRD will reject this EMM			

The following block with length 1B can appear more then once in a chain (unencrypted EMM typically 2 times / encrypted EMM typically 5 times).

(1B)
if bit 7 (MSB) of the first byte is 0 then this is an unencrypted EMM and processed by the IRD (see 6.3.1 Unencrypted EMMs for details). if bit 7 (MSB) of the first byte is 1 then this is an encrypted EMM and processed by the ISE or OSE (see 6.3.2 Encrypted EMMs for details).

(4)
DVB CRC32

6.3.1. Unencrypted EMMs

Each unencrypted block with length 1B is processed by the IRD (and not by the ISE/OSE). With unencrypted EMMs the content of the Non Volatile Memory (NVM) can be changed. For example if you have locked your IRD menus and forgotten your pin, then Scientific-Atlanta can send an unencrypted EMM to your IRD and change the lock level of the menus to 0 and reset the your pin to the default value “1234”.

0	0	1	1	2
7	6..0	7..2	1..0	
0	0	3		

0 = unencrypted EMM 1 = encrypted EMM		If the value is not 3 then this EMM block will be ignored by the IRD D9234	ADP type Valid values are 8, 9, A, 10 else "Unknown ADP rec'd" will be send to the debug output

If ADP type is 8 continue here:

3	3	3	3	3	3	3	3	...	11
7	6	5	4	3	2	1	0		2..0
				The lock level field is valid			1 = Reset the pin to the default value "1234"		Valid values are 0..4 Set the lock level to this value. If the value is greater than 4 then the lock level will be set to 0.

I don't have analyzed the many other fields, because I'm not so interested in unencrypted IRD EMMs.

6.3.2. Encrypted EMMs

Each encrypted EMM block with length 1B is send separately via Command 03 to the ISE/OSE. The content is encrypted with an individual key, the Secret Serial Number (SSN). The SSN of an ISE/OSE never changes. If you try to manipulate the content than the ISE/OSE will reject it with an ADP check error. If you try to sent a block that is encrypted with SSN 1234 to an ISE/OSE that has SSN 5678 than you will get the same error.
EMMs are used to send the encrypted Multi Session Key (MSK) or tiers changes to the ISE/OSE. All authorized ISE/OSE have the same decrypted MSK. The MSK is used to decrypt a Control Word (CW). A Video, Audio, ... stream is encrypted with the algorithm Data Encryption Standard (DES). The DES mode is Electronic-CodeBook (ECB). As DES key the decrypted CW (the plain CW) is used.

6.4. Plain control word calculation

To calculate the plain CW (DES key) the base CW and a CW seed is necessary.
The base CW can be received via Command 00. The CW seeds for Video, Audio 1 & 2, High Speed Data (HSD), Utility and VBI can be received via Command 01. The CW seeds for Audio 3 & 4 can be received via Command 08.

Base CW is 7 bytes long.

Seed type	Seed length
Video	4
High Speed Data (HSD)	4
Audio 1	3
Audio 2	3
Audio 3	3
Audio 4	3
Utility	2
VBI	2

Concatenate the seed bytes of a seed type to get a 7 byte seed array.
Examples:

```
//calc 7 byte long video seed array
seed7[0] = Video[0];
seed7[1] = Video[1];
seed7[2] = Video[2];
seed7[3] = Video[3];
seed7[4] = Video[0];
seed7[5] = Video[1];
seed7[6] = Video[2];

//calc 7 byte long audio seed array
seed7[0] = Audio1[0];
seed7[1] = Audio1[1];
seed7[2] = Audio1[2];
seed7[3] = Audio1[0];
seed7[4] = Audio1[1];
seed7[5] = Audio1[2];
seed7[6] = Audio1[0];
```

Xor the 7 byte seed array with the 7 byte base CW.

This xor'd value is the 56 bit DES key without parity.

The IRD then expands the 7 byte DES key to a 8 byte DES key with parity by inserting an parity bit (odd parity) after each 7th data bit (because the hardware DES chip in the IRD need an 8 byte key).

This 8 byte DES key with odd parity is the plain CW.
The plain CW can be logged via a PC terminal program using the in 2.2 CCDEBUG mode described control word debug screen.

By logging the I saw that the base CW has the **same** value on **all** ECM PIDs during a crypto period.

Here an example of fictive ISE answers and the corresponding 8 control words (DES keys):

```
command 00 (Get base CW)
result: (08) 00 11 22 33 44 55 66 77 [1C]

command 01 (Get CW seeds for Video, Audio 1 & 2, High Speed Data (HSD), Utility and
VBI)
result: (20) BF 11 11 11 11 22 22 22 33 33 33 33 44 44 44 55 55 66 66 00 00 00 00 00 00
00 00 00 00 00 00 00 [69]

command 08 (Get CW seeds for Audio 3 & 4)
result: (09) C0 00 00 AA AA AA BB BB BB [08]


(0) 0119C84A 5423DCCD  (VID)
(1) 2308400E 76325489  (HSD)
(2) 3280042C 67BA10AB  (A1 )
(3) 54B39DE0 01898967  (A2 )
(4) BAC4263D EFFE32BA  (A3 )
(5) AB4C621F FE767698  (A4 )
(6) 453BD9C2 1001CD45  (UTL)
(7) 76A215A4 23980123  (VBI)
```

6.5. Channel ID table

Program (decimal)	10.775 GHz	11.096 GHz	PMT PID	ECM PID	CHID / virtual channel	Description
1	x		1389	1771	0010	Sports/FoxSports/ESPN/Conting
2	x		138A	1772	0020	AFN Atlantic/PowerR/AFNEZ/NPR
3	x		138B	1773	0030	Spectrum/Touch
4	x		138C	1774	0040	Pacific/Pure Gold
5	x		138D	1775	0050	News/BrightAC/Country/ARock
6		x	138E	1776	0060	AFN Korea/Time Code
7	x		138F	1777	0070	Guide/AFNEPRadio/HotAC/Hero/Vo

8		x	1390	1778	0080	Pentagon Channel
9		x	1391	1779	0090	AFN Family
10		x	1392	177A	00A0	AFN Movie Channel
11	x		1393	177B	00B0	Wuerzburg
12	x		1394	177C	00C0	Region 3
13	x		1395	177D	00D0	Region 4
14		x	1396	177E	00E0	Vicenza
20	x		139C	1784	0140	Guide/Newswheel
21	x		139D	1785	0150	Guide/Bright AC
22	x		139E	1786	0160	Guide/Country
23	x		139F	1787	0170	Guide/Adult Rock
24	x		13A0	1788	0180	Guide/NPR
25	x		13A1	1789	0190	Guide/Voice/UIVoice/SplitUI
26	x		13A2	178A	01A0	Guide/UI Voiceline/SplitUI/Voi
27	x		13A3	178B	01B0	Guide/The Touch
28	x		13A4	178C	01C0	Guide/Pure Gold
29	x		13A5	178D	01D0	Guide/Hot AC
30	x		13A6	178E	01E0	Guide/Z-rock ABC Hard Rock
31	x		13A7	178F	01F0	Guide/Fox Sports Talk
32	x		13A8	1790	0200	Guide/ESPN Radio
33	x		13A9	1791	0210	Guide/UI Split/UIVoice/Voice
34	x		13AA	1792	0220	Guide/SMPTE Time Code
35	x		13AB	1793	0230	Guide/AFNE Power Radio
36	x		13AC	1794	0240	Guide/Contingency
37	x		13AD	1795	0250	Guide/AFNE Z-Rock
38	x		13AE	1796	0260	Guide/Bavcaria Z-FM
39	x		13AF	1797	0270	Guide/Bavaria PowerNet AM
40	x		13B0	1798	0280	Backhaul to Bagdad
41		x	13B1	1799	0290	Z-106 Vicenza (audio only)
42		x	13B2	179A	02A0	Power 107 Vicenza (audio only)
43		x	13B3	179B	02B0	AFN Vicenza Contingency

6.6. The ISE interception and manipulation interface

The ISE chip is connected to the ISE socket on the motherboard of the IRD.
It is possible to remove the ISE chip and make a connection from the ISE socket to the COM port of a computer and a connection from a 2nd COM port to the ISE chip. Don't forget to exchange the IRD oscillator as described in 6.1 Internal Security Element (ISE).

To log the traffic, manipulate answers or send own commands to the ISE you can use the "PowerVu-ISE-Tool" from my homepage.

6.6.1. PC to ISE Chip interface

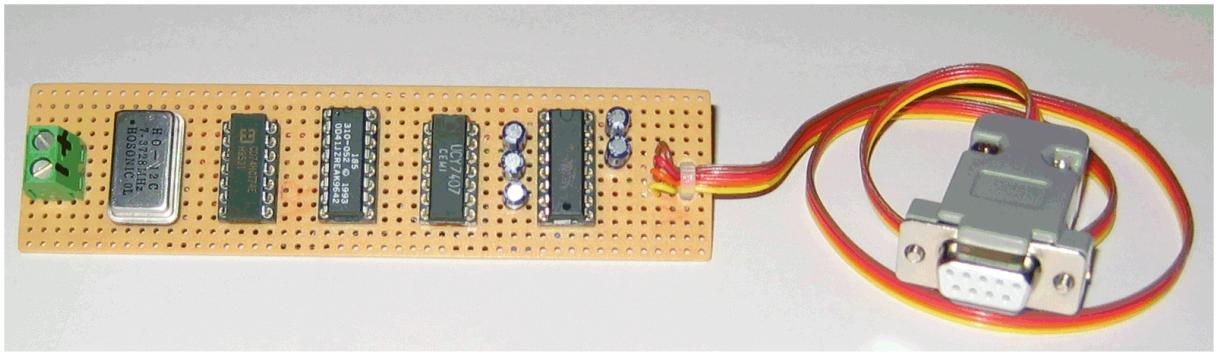

Figure 24 - PC2ISE_Chip interface circuit design

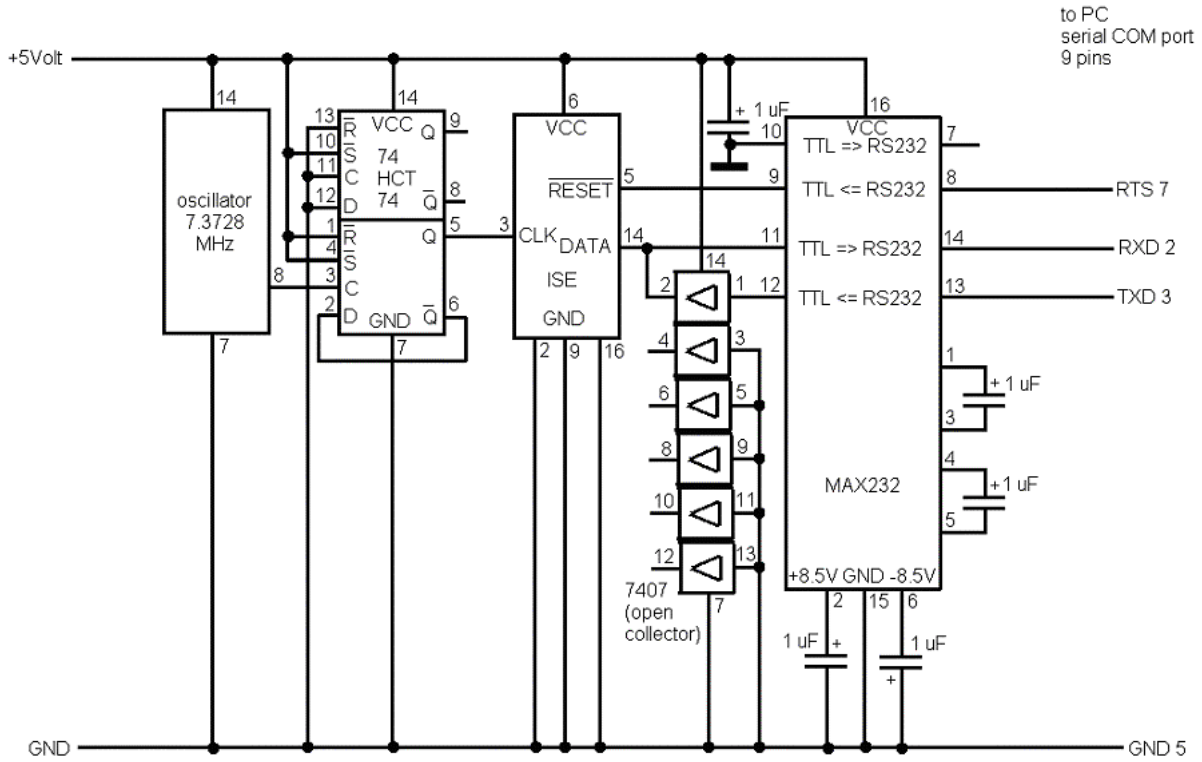

Figure 25 - PC2ISE_Chip interface connection diagram

6.6.2. PC to ISE Socket interface

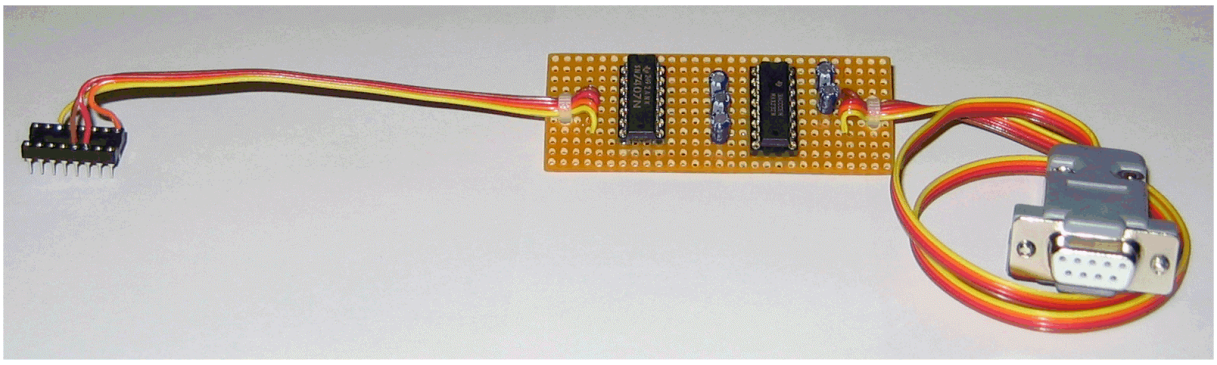

Figure 26 - PC2ISE_Socket interface circuit design

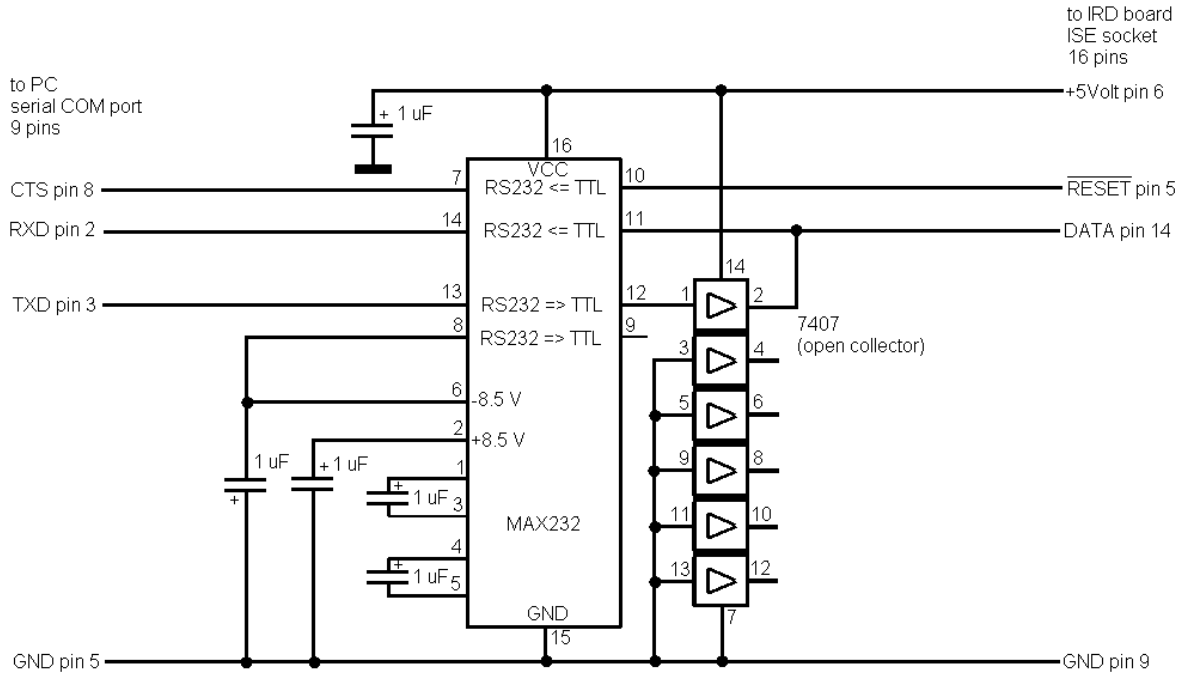

Figure 27 - PC2ISE_Socket interface connection diagram

7. KeyCodes

If you have disassembled (ARM big endian) the firmware and see that the keys sequence e.g. “11 00 19 0C” will enter an back door menu, then this is useless to you because you don’t know which key is represented by e.g. keycode 11. The following table will solve this problem. It will show for example that the key sequence “11 00 19 0C” = “Favorite → 0 → Pause → Channel Up”.

KeyCode	Where?	What?
00 .. 09	Remote control	0 .. 9
0A 0A	Remote control Front panel	Power Power
0B	Remote control	PPV
0C	Remote control	Channel up
0D	Remote control	Channel down
0E	Remote control	Volume up
0F	Remote control	Volume down
10	Remote control	Mute
11	Remote control	Favorite
12	Remote control	Info
13	Remote control	Last
14 14	Remote control Front panel	Select Select
15 15	Remote control Front panel	Down Down
16 16	Remote control Front panel	Up Up
17 17 17	Remote control Remote control Front panel	Left Back Left
18 18 18	Remote control Remote control Front panel	Right FWD Right
19	Remote control	Pause
1A	Remote control	Prev day
1B	Remote control	Next day
1C	Remote control	Guide
1D 1D	Remote control Front panel	Menu Menu
1E	Remote control	Sleep
39	Front panel	Select + Right

3A	Front panel	Select + Left
3B	Front panel	Select + Up
3C	Front panel	Select + Down
3D	Front panel	Left + Right
3E	Front panel	Up + Down
3F	-	No key was pressed

8. Links

- http://colibri.de.ms On my homepage you can find the newest version of this document, PowerVu firmware, the original manual and the PowerVu-ISE-Tool.

- http://www.growl.de/d9234 An interesting hobbyists page about the PowerVu Receiver "D9234" made by Scientific Atlanta

- http://www.sciatl.com/products/customers/whitepapers.htm Select “Content Origination and Distribution Part II - Secure Broadcasts with Originator Encoder” to read basics about the PowerVu Conditional Access (CA) system.