

Sti5517 flash dump

Posted by admin - 2009/11/24 20:11

Hi there @YLG80.

Testing with the def file below:

As soon as I start jkeys, I get "Error reading from IRD (DCU peek)", which I think is normal (so I've read), and I carried on. Clicked OK and chose the IRD Model (STB_with_STi5517LWA); the M58LW032C flash comes up on top right field and I try to "Save Mem"; choose path file and upon clicking "Save" I get "Error reading from memory". Click OK, looks like it's reading but saved file is empty (0 bytes).

Same procedure with wall.exe, either already running before jkeys or after, I get the same error...

Thanks for your help.

Quote:

Originally Posted by YLG80

OK, let's go !

What kind of error do you get when you launch jkeys ?

Your jkeys definition file should contain the following lines related to your CPU and Flash

```
:
//
// Microprocessor Definitions:
// Definiciones de Microprocesador:

Micro, 1, 1, "STi5518MVB-X", 0xd405041, 0xffffffff
Micro, 2, 1, "STi5518", 0xd502041, 0xffffffff
Micro, 3, 1, "STi5517LWA", 0xd41f041, 0xffffffff
Micro, 4, 1, "STi5516FWB-X", 0xD41D041, 0xffffffff
Micro, 5, 1, "STi5510", 0xd4cd041, 0xffffffff
Micro, 6, 1, "STi5508", 0xd402041, 0xffffffff
Micro, 7, 1, "STi5505", 0xd4cb041, 0xffffffff
Micro, 8, 1, "STi5500", 0xd4c9041, 0xffffffff
Micro, 9, 1, "ST20-GP6", 0x5196041, 0xffffffff
Micro, 10, 1, "ST20-TP4", 0x5198041, 0xffffffff
Micro, 11, 1, "ST20-TP3", 0x5194041, 0xffffffff
Micro, 12, 1, "ST20-TP2", 0x5193041, 0xffffffff
Micro, 13, 2, "LSI SC2000", 0x400006d, 0xffffffff

// Unknown Devices:

Micro, 14, 1, "Unknown ST device", 0x041,0xfff
Micro, 15, 2, "Unknown LSI device", 0x06d, 0xfff

// =====
// =====IRD=Definitions/IRD=Flash=Definitions=====
// =====DO=NOT=EDIT=HERE=FOR=FFFF/FFFF(JEDEC)=ERRORS!=SEE=NEXT=SECTION=====
// =====

IRD, 3, "STB_with_STi5517LWA", 3, 3, 1, 1, 2, 2, 0x7FFFFFF40, 0x7FFFFFF44, 0x7FFFBFE0, 0x7FFFFFFA8,
0x7FFDFFF4, 0x7FFDFFF8, "10E", 3, 4
IRDFlash, 3, "M58LW032C", 0x8822, 0x7FC00000, 0x400000, 2, 2, 0

// =====
// =====Flash=Definitions/Flash=Sector=Definitions=====
// =====EDIT=HERE=FOR=FFFF/FFFF(JEDEC)=ERRORS=====
// =====

// STB with STi5517ALW and flash M58LW032C
Flash, 3, "M58LW032C",0x8822, 0x400000, 1, 1, 0, 2, 32, 0
Sector, 3, 32, 0, 0x20000 // 128 KByte 32 Sectors

// =====
```

// =====Flash=Manufacturer=Codes=====
// =====

FlashMfg, 0x01, "AMD"
FlashMfg, 0x4, "Amic"
FlashMfg, 0x1F, "ATMEL"
FlashMfg, 0xAD, "Hynix"
FlashMfg, 0x89, "Intel"
FlashMfg, 0xB0, "Intel"
FlashMfg, 0xC2, "MX"
FlashMfg, 0x0000, "Sharp"
FlashMfg, 0xBF, "SST"
FlashMfg, 0x20, "STMicro"
FlashMfg, 0x98, "Toshiba"

// =====
// =====

=====

Re:Sti5517 flash dump

Posted by admin - 2009/11/24 20:15

When you launch jkeys, does it recognize the CPU or does it display 'Unknown ST device'?

Also look at the Slugworth post copy below:
from <http://www.rdi-board.com/showthread.php?p=742753>

This is a post from Slugworth

Peek errors are usually due to a bad ground between pc and receiver or the jtag wires too long or twisted.
Slugworth Rule of arm: Jtag wires should be shorter than your arm.
In st20 research I have noticed that using nRST instead of TRST works better with jkeys for dumping flash for some reason. You have to tie TRST high thru a 100 ohm resistor I use pin 12 on the lpt1 db25.
./..

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/24 23:06

Hi guys.

When I launch jkeys it does recognize the CPU (Device ID -> 0x2D41F041 and Device -> STi5517LWA) so I assume my jtag connections should be ok.
However, I noticed that when trying to measure the voltage on RST board pin, it looks like the board resets. Plus, reading this:
using nRST instead of TRST works better with jkeys for dumping flash for some reason. You have to tie TRST high thru a 100 ohm resistor I use pin 12 on the lpt1 db25
made up my mind about start using nRST instead of nTRST and keeping the latter pulled up to Vcc through a 100 ohm resistor.
I'm going to change it accordingly and let you know the results soon.
Thx.

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/24 23:15

Take many dumps of flash and compare with a hex editor to make sure all dumps are identical. I read about people experimenting and only taking 1 dump of flash- if you manage to erase the flash you must have something good to flash back in.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/24 23:19

Hi guys.

Very good advice, @slugworth. Will definitely do so!
Thx!

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/25 00:02

Jkeys will only dump the flash on the sti5517, but will work using pin 17 instead of pin 19 of a 20pin jtag. This uctap wiring would be needed for a uctap/st20 toolset solution to jtagging the sti5517 anyway, so might as well utilize it.

Toolset compliments of the forum boss.

<http://rapidshare.com/files/310373061/5517ftaci100B.zip>

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/25 00:12

Hi guys.

Well, since I connected nRST to db25/5 and nTRST to db25/12, looks like jKeys resets the board when "Detect" is clicked or the jTag is re-connected but still no flash dump. Keep getting the same error...

Can there be a software block on these flashes?

Running out of test ideas... :(

Best regards.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/25 00:23

Hi guys.

Thank you all. You've been really helpful...

Toolset compliments of the forum boss. <http://rapidshare.com/files/310373061/5517ftaci100B.zip>

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/25 01:04

Like stated before,dcu peek errors are always either insufficient ground between receiver and pc or wires too long/twisted.
I would add another ground wire between pc case and receiver.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/25 01:20

Hi guys.

I will redo the connections and will try to get a shorter printer cable (maybe I'll shorten this one...), but only tomorrow for it's getting late and tomorrow is a working day. :(

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/25 20:46

You should try also to launch jkeys upon reset.

You switch your STB OFF.
Then you switch it ON and immediately launch JKEYS.

The DCU mode needs to be activated during a reset pulse.
This is more easy during a cold reset.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/25 22:15

I've added the PM capability, the very little button under the avatar.
Of course I'd like to avoid displaying the email and other confidential information related to the users.
If you remark something wrong in the PM please let me know. I will immediately change the appropriate parameters.(there are so many !)

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/26 01:04

Hi guys.

Nice one on both previous posts, @YLG80...
Also tried the way you stated on your post #46 and the behaviour was the same.

Today's been one of those days. Anything that I lay my hands on, turns into trash... :angry:
Anyway, I managed to redo connections but haven't tested it yet. :blush:

One thing though: - this board has a 10 pin jTag and looks like it's connected differently than your 10 pin jTag. Attached you'll find what I've been using (it's been given by a friend)...

Best regards. <http://www.avi-plus.com/images/fbfiles/images/BoardJtag.JPG>

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/26 22:55

Here attached is a schematic of the Vestel Sti5105 board.
On the top right you will see a 10 pin JTAG connector.
I've 4 STB's with 20 pin JTAG connector so I don't know about the 10 pin version.
Here is another 10 pin JTAG connector found in a document.
http://www.avi-plus.com/images/fbfiles/images/10pin_jtag_con_type.png

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/26 22:58

Here is the file (STi5105 board schematic) http://www.avi-plus.com/images/fbfiles/files/schematic_Sti5105_VESTEL.zip

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/26 23:40

Hi guys.

Just what I meant, the connection points are not in the same positions.
Thx for the info.

If I get the processor ID and Device data correct, the connections must be OK...
Going for tests again now, will come back later. ;)

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/27 10:17

What is the version of JKEYS that you are using ?

You could try also that flash def (64 sectors)

```
// STB with STi5517ALW and flash M58LW032C
Flash, 3, "M58LW032C",0x8822, 0x400000, 1, 1, 0, 2, 64, 0
Sector, 3, 64, 0x0, 0x10000 // 64 KByte 64 Sectors
```

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/27 13:37

Hi guys.

The jKeys version is 2.9.11 (Build 026).

Connections redone and still the same problem. Also tried with previous flash conf, no luck... :(
Tried dumping the eeprom and it worked (with error nags, probably due to wrong eeprom choosing, but got something out of it...).

Maybe flash's got some protection I'm not aware of that prevents access to it...

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/27 14:24

Jkeys version : should be OK

Flash

Yes, I've seen in the datasheet that this M58LW032x has a lock/protection mode.
That protection is activated by software, changing one register value.
So I guess it needs some utility to unlock it.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/27 14:57

I have found this unusual procedure on Polish website for the Sti5516. (STi5517 is similar with more features)

Launch jkeys

<http://www.avi-plus.com/images/fbfiles/images/Image1.jpg>
enter 7FC00000 in the start field and 400000 in the bytes field

<http://www.avi-plus.com/images/fbfiles/images/Image2.jpg>

Click on flash programming - should display the correct flash type and DCU trap functional at the bottom of the window

<http://www.avi-plus.com/images/fbfiles/images/Image3.jpg>

I guess you have to change the base address to 7FC00000 and Click on Read

What type of STB is it ?

Is there any RS232 utility to update the soft? If yes it could perhaps be used to change the flash lock status.

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/27 15:07

I am skeptical of that one, since the 5516/5517 are dcu3 devices you would never hit the flash programming button. You would just set the correct address/size then hit the save mem button.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/27 15:53

Hi guys.

I also saw that topic @YLG80 and I'm facing the same problem that romeok01 is.

From what I could find on flash's datasheet looks like 0x80 is the address of the protection register. Wouldn't it be possible to write to this address with jKeys?

@slugworth, when I click on "Save mem" I get "Error reading from memory" and the saved file with 0 bytes. :angry:
If I try the method they mentioned on the topic I get: <http://www.avi-plus.com/images/fbfiles/images/Error.JPG>

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/27 18:49

I don't know if the sti5517 has a bfr pin like the sti5518 that sometimes has to be grounded even to read reliably. I would have to look at the pdf for it.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/27 21:19

I don't think you will be able to write in that register if you cannot setup the Diagnostic Controller. One solution would be to establish a ucTAP connection with the ST20 Toolset. But it means compiling an application with the Toolset.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/27 22:35

Hi guys.

@slugworth, don't know either and only have the STi5516 datasheet... :(

@YLG80, that's something that also crossed my mind: - getting ucTap to have this done. As for compiling an application with the toolset I lack all the knowledge to do so, although really keen on learning if someone wants to "waste" some time on making me understand.

One question, if I may: - will I be able to use ucTap to read or is it a "write only" app? I ask this because that's the idea I got from what I read on the web...

Thank you both guys.

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/28 00:01

Normally the 5517 is pin to pin compatible with the 5516, if I remember.

With the ToolSet, you can do whatever you want. If you compile a flash program you can read, verify or write.

The first thing is to setup the Diagnostic Controller (DCU3 in that case) so that you can enter in debug mode. As you have full control on the CPU you can do whatever you want. But it's not really simple because it means programming. Fortunately there are many program samples that can be used as a basis. I guess the flashprog utility that we have used for the Sti5015 could be recompiled for the 5517 but we would need to change the routines for your specific flash chip.

I've not found the 0X80 register in the 5516 datasheet. I'm wondering how they could protect the flash from being read. At least during the first boot stage, the CPU needs to read the flash prior to copy it into RAM. After a complete boot, the CPU could force the flash chip into reset mode without any problem, because it runs now in RAM. This is the reason why I've asked you to try to launch Jkeys upon reset.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/28 00:11

..and good news, the M58LW032 is described in st_flash.c and tt_flash.c source !
(to examples for flash programming)

```
elif defined(mb361)                /* mb361 */
#define DEVICE_TYPE      STFLASH_M58LW032
#define MIN_ACCESS_WIDTH STFLASH_ACCESS_16_BITS
#define MAX_ACCESS_WIDTH STFLASH_ACCESS_16_BITS
```

the mbxxx are development boards for which there are configs and routines available in the ToolSet:

```
parse "include dcu_mb361.cfg\n"      ## STi5516
parse "include dcu_mb382.cfg\n"      ## STi5516/17
```

So in your case the mb382 could be used together with the M58LW032x.

However I don't remember if we were able to recompile that source. I will check in the laptop where I've stored all that stuff.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/28 00:24

schematic of the echostar dp311 showing a sti5517 processor

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/28 00:25

Hi guys.

Nice one. :cheer:

I didn't get why you were looking for the 0x80 register in the STi5516 datasheet; when I mentioned it I was referring to flash's registers (I got mixed up... :blush:).

OK, so what shall I do next? Get the ST20 ToolSet in order to be able to compile for this IRD and flash (after the needed changes)?

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/28 00:28

jkeys first,no st20 toolset program ever let you save flash.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/28 00:41

Hi guys.

OK. I'll be here for whatever is needed.
In the meantime, I go and read some more about DCU3...

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/28 09:25

My mistake, was looking for the 0x80 register in the M58LW032 DS. Sorry.

As test for the pdf upload : <http://www.avi-plus.com/images/fbfiles/files/M58LW032C.pdf>
I've changed the settings and added various file types (.hex,.bin,.pdf.rar)

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/28 12:08

From the M58LW032C datasheet:

The Reset/Power-Down pin is used to apply a Hardware Reset to the memory and to set the device in power-down mode.

The device features an Auto Low Power mode. If the bus becomes inactive during Asynchronous Read operations, the device automatically enters Auto Low Power mode. In this mode the power consumption is reduced to the Auto Low Power supply current.

In the pin description

After Reset/Power-Down goes High, VIH, the memory will be ready for Bus Read and Bus Write operations after tPHQV. Note that Ready/Busy does not fall during a reset, see Ready/Busy Output section.
In an application, it is recommended to associate Reset/Power-Down pin, RP, with the reset signal of the microprocessor.
Otherwise, if a reset operation occurs while the memory is performing an Erase or Program operation, the memory may output the Status Register information instead of being initialized to the default Asynchronous Random Read.

I guess this could be the reason why you cannot read the flash.
If possible you could try to disconnect the Reset Pin from the main circuit and connect it to the jtag nRST pin.
It could be very difficult if your chip is of a BGA type.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/28 13:38

Mornin' to you guys.

You definitely make sense @YLG80...
Right now, I have these connections (refer to post #48):

DB25-----PCB

2tms
3tck
4tdi
5reset (previously ntrst)
12ntrst
13tdo
25gnd

I don't really know how jKeys works but looks to me that the app must get DB25/5 low in order to start the whole process. After what you said, I assume that the PCB reset point should be an output to reset flash and cpu. I can try to find someone who has already taken out the cpu and try to follow this track... Like so, we'd still get problems even if we compile an app with the ToolSet, don't we? We first need to sort out the flash issue, so we can carry on...

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/28 15:25

What type of Flash chip do you have : a TSOP (with pins around) or a BGA with pins below. On the ST Toolset, Slugworth is right : up to now we have no application that can dump the flash to a file. Only verify, erase and flash.

Normally with a TS application we would not have the same problem with the locked flash chip, as the program takes complete control on the CPU upon reset and enter in DCU3 mode. This prevents the STB to enter the first boot stage.

In normal mode, I guess your flash chip is placed in reset/low power mode at the beginning of the second boot stage, when the program continues from RAM. This would mean the flash reset pin is likely connected to a CPU PIO output. Disconnecting the reset pin from that connection and reconnecting it to the main CPU reset pin would resolve that issue.

One thing to try : modify your interface as for ucTAP (pin 17 and 19) or build the simple interface for ucTAP and try with jkeys immediately after the STB power up. When, I do this here, I've seen that the STB cannot boot as long as jkeys is running. (Led is off while jkeys is running and on after shutting down jkeys. As soon as you shutdown jkeys, the boot continues.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/28 16:48

Hi again.

I have a TSOP flash. Right, I think the way I have my interface now is the ucTAP way (nRST is on db25 pin 5 instead of nTRST which, on its turn, is on db25 pin 12).

The test: - as far as I could find out, I don't get the same behaviour you do, @YLG80. Actually, looks like I get the opposite. When I start jKeys right after powering on the board, the led behaves the usual way (stays off for few tenths of seconds, then comes on for ~1 sec, goes off again and back on right after). If I click on "Detect" when power is on, I get exactly the same behaviour.

One thing though, when I close jKeys, led goes off and stays this way until I restart jKeys or power off and back on the PCB. Right now, jKeys is not running (I closed it), power is on and led is off. Makes me wonder... Is this working the other way round?

Hope I expressed myself enough so you can understand... :blush:

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/28 18:23

I will have to try on my STB, but that will for tomorrow as I have to leave in few minutes.

This is the wiring for ucTAP

http://www.avi-plus.com/images/fbfiles/images/uctap_jtag-045caa3cfd9a569d9733ef3a9b618632.JPG

Even if you use a buffered jtag interface, you should swap certain pins in order to have the same connections between the DB25 side and the JTAG side.

I use the PCBWIRE-MULTI JTAG (buffered) and I had to swap pin 17 and 19 and add the missing connection from DB25 pin 12

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/28 19:29

Hi there.

No worries @YLG80, have a nice time... B)

For the ucTAP wiring, the one you posted is the one I checked mine against. I use a passive jTag (only resistors), no buffered one.

Will talk tomorrow.

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/29 10:00

Thanks to you I've verified that my JTAG connections and TS programs are still OK.

You are right on the power LED behaviour when the interface is wired for ucTAP.

In fact the behaviour I've described is for the LED display, displaying Load, Boot, On, Init Menu and channels.

When no jtag program is running, my STB boot is blocked with nothing displayed when I power it ON (black display).

When launching ucTAP the STB remains in the same status.

However when launching JKEYS, the boot continues up to the end.

If I click on the JKEYS Detect button, the STB reboots. (after a reset)

Prior to use any TS application with ucTAP, I need to reset the STB again.

Then any Toolset application is running fine.

So your flash is a TSOP.

If you are good with a soldering iron, you could carefully desolder pin 16, isolate it from the pCB pad and reconnect it to the main reset with thin wire wrapping wire.

Prior to do that type of surgery, you could trace the PCB track that goes to that PIN. It would be easier to have only to cut the track connected to that RP pin.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/29 13:37

Hi guys.

Yes, I was talking about the power LED.

I could lift up flash's pin 16, no worries (done that before in other equipments) but I have a short track connected to this pin, before it disappears via a through hole (multilayer...), so I'm thinking of following your 2nd suggestion. Before I do that, what do you think about checking first if this pin goes low whenever jKeys starts or "Detect" is clicked, so we can pinpoint this is what prevents the flash from being identified?

Best regards.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/29 13:56

Hi again.

Well, just checked flash's pin 16 and it does go low whenever jKeys start or "Detect" is clicked and comes back high after ~0.5 sec... :(
Can't think of anything else that prevents flash's identifying. :angry:

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/29 14:58

9u4rk wrote:

Can't think of anything else that prevents flash's identifying. :angry:

Best regards.

The wrong flash address in the jkeys .def would do that.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/29 16:03

With the pin unconnected, the STB will no longer boot, so you will never see if after the first boot stage, that pin is locked to Low Power mode/Reset.

You need to, at least, RESET the flash IC together with the CPU with the CPU reset signal.

Then you will be able to check on the PCB pad that was connected to the flash if the signal goes low by the end of the first boot stage.

A few months ago I've received a jpeg picture from Slugworth showing JTAG connections for a 5514 Pace 3100. The main RESET signal looked connected directly to the flash IC.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/29 17:16

Yes, agree with Slugworth. The memory mapping is perhaps different in your STB.

The memory mapping for the Sti5516 is the following.

http://www.avi-plus.com/images/fbfiles/images/memory_map.png

The Sti5517 is likely similar.

Here is the config from the 5517FTACI :

```
## Sti5517 EMI configuration file
```

```
##
```

```
## Purpose: Register pokes to configure EMI memory and peripherals on an MB382 eval board
```

##

Bank Memory Space configuration:

##

## Bank0	0x40000000-0x4ffffff	SDRAM 32Mbyte (256 MBit)
## Bank1	0x50000000-0x5ffffff	STEM0/SRAM (256 MBit)
## Bank2	0x60000000-0x6ffffff	STEM1 (256 MBit)
## Bank3	0x70000000-0x7ffffff	ATAPI/DVB-CI (240 MBit)
## Bank4	0x7f000000-0x7f7ffff	DVB-CI (64 MBit)
## Bank5	0x7f800000-0x7ffffff	SFLASH 8Mbyte (64 MBit)

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/29 17:30

Try to change this in your .def file :

IRDFlash, 3, "M58LW032C", 0x8822, 0x7FC00000, 0x400000, 2, 2, 0
to
IRDFlash, 3, "M58LW032C", 0x8822, 0x7F800000, 0x400000, 2, 2, 0

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/29 17:52

you forgot to change the flash size from 4meg to 8meg

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/29 21:56

Hi guys.

Tried what @YLG80 posted, after flash's size correction, but still no success... :(

Been searching the web and found this:

Quote:

Originally posted by dssseller0001

When opening jKeys, it correctly identifies the Microprocessor as STi5516FWB-X.

End quote

This is a TAP identify operation which does not rely on the flash definitions.

Quote:

I changed the IRD Model to DRD435-455.

I changed the Save Memory region to my new Flash 2 setting for the M58 chip.

Clicked on "Save Mem" and waited for a while...

.bin seemed to save correctly, so I opened it up in a HEX editor and compared the beginning of the file to a known, good .bin from a similar flash.

End quote

This uses the DCU READ operation which does not rely on the flash definitions (except maybe the start address and length).

The second quote is what makes me think; again, I don't know how jKeys works so I can't take it any further. Maybe you guys know better...

This is a discussion about the STi5516 and, if you want, you can follow it here: <http://id-discussions.com/forum/showthread.php?t=63320>

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/29 22:29

From your topic #57 showing an error returned by Jkeys, it appears that jkeys is unable to recognize the mfg code. 0xFFFFFFFF means that the data returned was not consistent.

This could happen if the flash chip definition used is not correct for the flash chip.

Jekys could not use the correct sequence to address certain flash registers containing the Mfg data.

You should be absolutely sure that your flash is an M58LW032C not 32D which has a different structure and a different manufacturer code.

The DCU3 trap is not necessary to fetch the CPU ID or read the flash. It's necessary if you want to erase or reprogram the flash or have access to the RAM.

So, if there is no special trick to put the flash in Reset/Low Power Mode, you should be able to read that flash with a standard jkeys compatible interface correctly wired to the jtag connector.

On the M58LW032C

READ MODES

Read operations can be performed in two different ways depending on the settings in the Configuration Register. If the clock signal is 'don't care' for the data output, the read operation is asynchronous; if the data output is synchronized with clock, the read operation is synchronous.

The read mode and format of the data output are determined by the Configuration Register. (See Configuration Register section for details).

On Power-up or after a Hardware Reset the memory defaults to Asynchronous Read mode.

./..

On power-up the memory defaults to Read mode with an asynchronous bus where it can be read in the same way as a non-burst Flash memory.

Jkeys needs to use the correct mode for that flash chip.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/29 22:54

in 2006

./..

I am still having problems about working with the ST M58LW032D and M58LW064D FLASHes in situ even with ST developer project source code written specifically for them at the moment but should soon have it resolved.

./..

Seems to be a difficult chip to read !

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/29 23:33

Hi guys.

I'm pretty sure it's got a M58LW032C flash...

Seems to be a difficult chip to read !

Yes, looks like it is :), but when this happens, the more it drives me. ;)

The main problem is we don't know what's the reason that prevents us from reading it. On the other hand, we read about people that have been able to do it with no hassle at all... :unsure:

Where do we stand...?

Then again, there might be something (a special trick, as you said @YLG80) that keeps us from identifying it correctly.

But what...?

Did I say before this drives me? All right, it drives me... It drives me nuts! :silly:

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/30 00:02

did you ever get past the dcu peek error stage?

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/30 00:11

Hi there.

No @slugworth, never! :(

I guess that might be the reason...

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2009/11/30 04:04

You might want to try a different pc also.

Sometimes parallel ports are finicky.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/30 09:07

http://www.avi-plus.com/images/fbfiles/images/JTAG_10pin_Connector.png

I've examined your JTAG connector picture.

As far as I can see, each pin (except TRIG OUT) is connected via a resistor (located below the connector) to the rest of the circuit.

What are the resistance values ?

If you use a simple unbuffered interface already with resistors in each line, you might have a problems if there are also resistors in series within the circuit.

@ logic levels as low as 3.3V, you interface might be unable to correctly drive the JTAG signals or the signals might be very noisy with two resistors in series.

At 3.3V the noise margin is weak.

Also regarding the picture, what do you mean with PIN0 15 DA FLASH ?

Does that mean that this pad is connected to VPEN on the flash chip ?

I suggest also to wire your interface back to the classic JKEYS type for your next trials

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/30 13:30

Hi guys.

Been busy this morning, hope I get a quieter afternoon...

YLG80 wrote:

I've examined your JTAG connector picture.

As far as I can see, each pin (except TRIG OUT) is connected via a resistor (located below the connector) to the rest of the circuit.

What are the resistance values ?

From left to right:

10K, NC, 75, 10K, 10K, 10K, 10K and 10K (the one furthest to the right and a little above).

YLG80 wrote:

If you use a simple unbuffered interface already with resistors in each line, you might have a problems if there are also resistors in series within the circuit.

@ logic levels as low as 3.3V, you interface might be unable to correctly drive the JTAG signals or the signals might be very noisy with two resistors in series.

At 3.3V the noise margin is weak.

The way I see this, these are either pull-up or pull-down resistors (most of them anyway, didn't check all)

YLG80 wrote:

Also regarding the picture, what do you mean with PIN0 15 DA FLASH ?

Does that mean that this pad is connected to VPEN on the flash chip ?

I suggest also to wire your interface back to the classic JKEYS type for your next trials

This has been given to me and no details were disclosed but I think it's to be connected to flash's Vpen when programming/erasing is needed, for it's a 3.3V line.

I'll follow your suggestion. I'm assuming the classic interface is the way I had it before (just reconnect nTRST to db25/5 and open nRST).

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/30 14:47

You are right, with such high values the resistances are likely pull-up or pull-down.

I'll follow your suggestion. I'm assuming the classic interface is the way I had it before (just reconnect nTRST to db25/5 and open nRST).

That's correct. Keep short wires between the DB25 and the JTAG connector. ;)

ref : <http://jtagcables.com/jtag-cables/unbuffered-jtag-cable-xilinx-dlc5-cable-iii>

With a buffered JTAG interface you can have longer wires (mine is about 30cm/12")

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/30 15:23

Hi guys.

Have to go out again... :(

When I'm back will test some more. There are some issues in the flash's datasheet that I'd like to discuss with you guys.

C u in a bit, hopefully...

Re:Sti5517 flash dump

Posted by YLG80 - 2009/11/30 15:51

OK, in the meantime, I've tried to replicate your 0xFFFFFFFF error while using the Flash programming button the READ in Jkeys.

I can only replicate it when I wire my interface as for ucTAP.(CPU ID is correctly identified)

Even using the DB25 pin 12 signal connected at pin 19 JTAG CON and nothing at pin 17, I can fully read my flash memory.

Have you tried JKEYS on a lower speed PC ?

sti5516

Posted by slugworth - 2009/11/30 20:21

I don't have an sti5517 receiver with jtag points, but my sti5516 had the same error until I used pin 17 instead of pin 19 on the db25.

4meg flash

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/30 21:52

Hi guys.

YLG80 wrote:

Have you tried JKEYS on a lower speed PC ?

I'm going to try it on a PIII (1.1GHz) running Fedora 11. Will let you know the outcome...

@slugworth, I may be doing something wrong. The problem is I haven't been able to find out what... :angry:

Will cable length be too long or some misconnection, give me such errors?

Another thing, your CPU is STi5516 and what about flash, is it M59LW032C also?

Best regards.

P.S.: forum is looking nicer as time goes by. :cheer:

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/11/30 23:54

Hi guys (again... :blush:).

Have found out some interesting info (maybe...). Maybe, what I'm about to say is rubbish but I thought it might be relevant to what's happening to this board.

The way I see it, my problem starts when jKeys tries to identify the flash and fails to do so. Reading the M58LW032C's datasheet, trying to find a reason for jKeys' behaviour and came across this:

Read Electronic Signature Command. The Read Electronic Signature command is used to read the

Manufacturer Code, the Device Code, the Block Protection Status, the Burst Configuration Register and the Protection Register. One Bus Write cycle is required to issue the Read Electronic Signature command. Once the command is issued subsequent Bus Read operations read the Manufacturer Code, the Device Code, the Block Protection Status, the Burst Configuration Register or the Protection Register until another command is issued. Refer to Table 8, Read Electronic Signature, Table 9, Read Protection Register and Figure 8, Protection Register Memory Map for information on the addresses.

When it says "One Bus Write cycle is required to issue the Read Electronic Signature command", it looks to me that this should be jKeys' job. The application is responsible to send all these commands into the bus, so they can be interpreted by the flash's Command Interface and proceed accordingly. I also think that jKeys sends not one, but several commands in order to get all the info we are expecting...

My point being: - is there a way, through jKeys (Development Pannel or other...), we can send whatever command we want and try to figure out what's going on? This being possible, I'd have some manner of checking flash's registers and might even be able to find out what's preventing me from reading it. If any of you guys have another idea that might sort this out, please do feel free to bring it out for I'll be more than happy to listen and try it. :cheer:

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/01 00:32

you wouldn't get the peek error-jkeys would just come up with all ff's for the id.
The question is:can you find a jkeys.def that already had that chip listed?
If so,odds are somebody else already had it working for that chip.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/01 01:03

Hi guys.

Well, I haven't been able to find a jKeys.def with M58LW032C already listed (will look for it though...) but I've seen some posts of people saying they have done it. One is here:
<http://id-discussions.com/forum/showthread.php?t=63320>, maybe you have to be logged in to see it...
This goes back to 2004 and this guy says he's had no hassle doing it. He was working with STi5516 and this flash. Only had problems when trying to write into it...
I will have a go with his configuration when the PIII finishes all the updates. Fedora's still updating; hadn't been on for a while...

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/01 02:45

The id discussion was from 2004 and they didn't realize the sti5516 was a dcu3

device making jkeys useless for writing.
I didn't know the 58lw032 was a 4meg chip,so ignore anything I said about 8meg previously.I will search for a jkeys.def the good ones are usually >30k

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/01 03:06

they had the same problem with the sti5517,but you can download the jkeys.def without logging in.

<http://www.elektroda.pl/rtvforum/topic419564.html>

```
// Gaeboa - M58LW032C (8822)
Flash, 7, "M58LW032C", 0x8822, 0x400000, 1, 1, 0, 2, 64, 0
Sector, 7, 64, 0x0, 0x10000 // 64 KByte 64 sectors
```

```
// Gaeboa - M58LW032A (8816)
Flash, 8, "M58LW032A", 0x8816, 0x400000, 1, 1, 0, 2, 64, 0
Sector, 8, 64, 0x0, 0x10000 // 64 KByte 64 sectors
```

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/01 09:47

Another flash definition with 32 sectors instead of 64:

```
IRDFlash, 15, "Flash 4 (M58LW032C)", 0x8822, 0x7FC00000, 0x400000, 2, 2, 0
```

```
Flash, 21, "M58LW032C",0x8822, 0x400000, 1, 1, 0, 2, 32, 0
Sector, 21, 32, 0, 0x20000 // 128 KByte 32 Sectors
```

Re:Was a test for pdf upload

Posted by 9u4rk - 2009/12/01 13:50

Hi guys.

Thank you for all your help, again. You've been great...

Will try to test the new .def and flash configuration this afternoon.

I might be off the web for the next 2 or 3 days (I'm not sure where I'm going there'll be wireless access...) starting from tonight. :(

Hopefully I'll have time to do some more reading about the subject...

Anyway, there's still this afternoon and when I come back I'll get back at it. ;)

Best regards.

Trials

Posted by YLG80 - 2009/12/01 14:40

This is what I would try with your JTAG connections :

http://www.avi-plus.com/images/fbfiles/images/JTAG_10pin_Connector_trials.png

Swapping the connections on RESET, leaving the nRST pin unconnected, then swapping the connections on nRST leaving RESET unconnected.

Re:Was a test for pdf upload

Posted by 9u4rk - 2009/12/01 14:51

Hi guys.

The PIII is ready now so I'll try all that on both PCs. Will let you know the outcome as soon as possible.

Best regards.

Connections trials

Posted by YLG80 - 2009/12/01 19:08

Thanks to Slugworth post in the other thread (Sti5517 schematic in jpeg). I believe that you will have to do more tests.:silly:

Swapping also pin 12 and pin 5 on jtag pads RESET and nRST.

Re:Connections trials

Posted by 9u4rk - 2009/12/05 22:00

Hi guys.

Tests have been done but with no success... :(
<http://www.avi-plus.com/images/fbfiles/images/Table.JPG>
Note: in these tests whenever NTRST was connected, RESET was not and vice-versa.

Testing jKeys' response with NTRST5 and RESET12:

- same*.

Testing jKeys' response with NTRST12 and RESET5:

- receiver's power led stays OFF unless we start jKeys and like so the application detects cpu correctly, but still no flash reading; whenever jKeys is stopped power led goes back OFF.

same* - jKeys detects cpu but hasn't been able to read flash.

nope* - jKeys doesn't even detect cpu.

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/06 05:43

The original uctap diagram I used pin17 instead of pin19 and pin19 had to be pulled high; in that case I tied it to pin12 on the db25.

The only sti5517 receiver I have the processor is bga mount, I would have to desolder to trace the pins but I would never be able to get it soldered again.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/06 10:55

One additional test :

You could connect pin 5/DB25 signal to both RESET and nRST on the jtag connector.

Then try with pin 12/DB25 on both jtag pines. (could be a timing problem)

The RESET pin is perhaps used to RESET the flash or other circuits (MCU) while pin 12 is used to RESET the CPU and the JTAG port.

Have a look at the 5517 schematic (Europe) posted by Slugworth : DCU-RESET is used to RESET the flash and the MCU while nRST is used to RESET the CPU)

nRST and RESET signals coming from the DB25 should be both active low.(RESET while voltage LOW)

So use nRST signal coming from the DB25 on both nRST and RESET on the jtag connector side.

If you STB uses a similar config, connecting one pin only on nRST would allow you only to "talk" with the CPU and never with the CPU and MCU together.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/06 15:04

Hi guys.

slugworth wrote:

The original uctap diagram I used pin17 instead of pin19 and pin19 had to be pulled high; in that case I tied it to pin12 on the db25.

The only sti5517 receiver I have the processor is bga mount,I would have to desolder to trace the pins but I would never be able to get it soldered again.

That's the way I think I have it now @slugworth, NTRSTdb25/5 and RESETdb25/12 or 3.3V onboard.

No need to unsolder your STi5517 my friend, unless you have someone with a reballing station. Actually, I know such a person :) and if I can't find someone with a board with no cpu so I can follow the tracks, maybe I'll be requiring his services. We'll see how it goes...

YLG80 wrote:

One additional test :

You could connect pin 5/DB25 signal to both RESET and nRST on the jtag connector.

Then try with pin 12/DB25 on both jtag pines. (could be a timing problem)

That's something that has crossed my mind, maybe I'll have to have both signals, NTRST and RESET on my board, as if they were the same signal. Will do that test this afternoon...

Just to let you know, although I don't get always the same data (might have a synchronism or configuration problem...), I'm able to read the EEPROM. So this makes me think that the jTag interface, TAP and jKeys are working, not 100% ok but close...

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/06 21:17

I thought you have to set a trap to dump the eeprom,which would be impossible with jkeys/sti5517?

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/07 02:16

Hi guys.

And you may be right, @slugworth. I'm not sure that what I'm reading is the EEPROM data. What happens is when I click on EEPROM Programming on jKeys, then click on OK, next I get the EEPROM Programming menu where I can choose the IRD and EEPROM models and on bottom right it says Trap Functional. Next, if I click on Save it gives an error (Error reading from memory), click OK, error again but I get some data in the newly created EEPROM.bin file. Maybe it's a bug, don't know...

@YLG80, all tests done, still no success. Same behaviour as before. :(

This board is driving me nuts... :angry:

Anyway, hopefully I'll be getting this week either a photo or the actual PCB without the cpu, so I can try to trace down some tracks. Maybe this can help us sort this out. :)

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/07 21:43

Not sure, but I believe you are facing the same problem that I have with an Sti7100 box.

I believe that you have to prevent the box from booting, because after the boot, the IN_TRAP bit in the DCU_CTRL register can be set to 1 by the f/w which disables the DCU (tap port).

This would be kind of a protection against dumping the flash or using a debugger.

This could explain why you can only read the CPU ID.

If you have an RS232 port on your box, have you tried to see what happen when booting using a simple communication prog. (hyperterminal).

On my Sti7109 box, it writes the following sequence (twice)

```
Jump main
STTBX initialized
Jump main
STTBX initialized
```

I believe that it is waiting for a special character at the very beginning of the first boot stage, but I don't know which character.

The Kathrein Sti7100 box is waiting for a space.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/07 21:54

BTW, on the Sti7109 CPU, there are two pines that can be used to change the reset behaviour by means of jumpers. This could be used to allow the tap port to be used... but again the chip is a BGA so how to find these two pines....

Re:Sti5517 flash dump

Posted by Daggi_Duck - 2009/12/08 08:49

YLG80 wrote:

Not sure, but I believe you are facing the same problem that I have with an Sti7100 box.

I believe that you have to prevent the box from booting, because after the boot, the IN_TRAP bit in the DCU_CTRL register can be set to 1 by the f/w which disables the DCU (tap port).

This would be kind of a protection against dumping the flash or using a debugger.
This could explain why you can only read the CPU ID.

If you have an RS232 port on your box, have you tried to see what happen when booting using a simple communication prog. (hyperterminal).

On my Sti7109 box, it writes the following sequence (twice)

```
Jump main
STTBX initialized
Jump main
STTBX initialized
```

I believe that it is waiting for a special character at the very beginning of the first boot stage, but I don't know which character.

The Kathrein Sti7100 box is waiting for a space.

Some other receivers awaiting some returns from the terminal and before anything is displaying at the terminal.

The HOMECAST HS5101 CI (Sti7100) boot can be stopped with CTRL-H (Backspace) typed in the terminal connected to the RS232 port.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/08 12:45

Hi guys.

I'm afraid there's no RS232 port on this board, @YLG80. :(
But, what I can try is a port sniffer to see if I can make some sense out of jTag comms. I'll have a go at it later on...
As for there's any cpu pins that need to be short-circuited in order to get into boot from DCU, as you said it's BGA.
Maybe when/if I get the board without the cpu, I'll be able to figure something out.

I do have a network port though, but couldn't find any RS232 one. :(

Best regards.

=====

Re:Sti5517 flash dump

Posted by Daggi_Duck - 2009/12/08 18:17

Some receivers have a RS232 port at the SCART connector pin 10,12 and 14 (GND). Some uses TTL (0/5V) signal levels and need external level convertes for real RS232 levels, some have build in level converters for real RS232 levels (-10V/+10V).

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/08 19:05

On the STi7100 stb, I've been able to stop the boot via the RS232 port typing CTRL-H during the boot.

It stopped at the loader level.

But still no luck to connect with ucTAP.

I'm more and more convinced that they are using the antifuse bit to block the jtag access.

Could be the same thing with the Sti5517 as I've seen that this chip is similar to the STi5116 "with additional security" features ...

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/08 21:55

Hi guys.

This has been quite a task. :S

From what I could see with a parallel port monitor, everything's ok. I spent the whole afternoon rechecking connections and double checking jTag points. They're all good. There's not much more I can do before the PCB without cpu arrives...

YLG80 wrote:

On the STi7100 stb, I've been able to stop the boot via the RS232 port typing CTRL-H during the boot.

It stopped at the loader level.

But still no luck to connect with ucTAP.

I'm more and more convinced that they are using the antifuse bit to block the jtag access.

Could be the same thing with the Sti5517 as I've seen that this chip is similar to the STi5116 "with additional security" features ...

Maybe that's the reason, @YLG80. If that's so, will we be able to overcome it?

Daggi_Duck wrote:

Some receivers have a RS232 port at the SCART connector pin 10,12 and 14 (GND)

Will check on that, @Daggi_Duck, thx.

One question, though: - let's assume that we have flash's /W (pin 55) disconnected for some reason. Will jKeys still be able to identify and read the flash?

Best regards.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/09 23:25

Hi guys.

Daggi_Duck wrote:

Some receivers have a RS232 port at the SCART connector pin 10,12 and 14 (GND). Some uses TTL (0/5V) signal levels and need external level convertes for real RS232 levels, some have build in level converters for real RS232 levels (-10V/+10V).

Some easy way of checking this, @Daggi_Duck?

If I already had the PCB without cpu...

Best regards.

=====

Re:Sti5517 flash dump

Posted by Daggi_Duck - 2009/12/10 08:10

9u4rk wrote:

Hi guys.

Daggi_Duck wrote:

Some receivers have a RS232 port at the SCART connector pin 10,12 and 14 (GND). Some uses TTL (0/5V) signal levels and need external level convertes for real RS232 levels, some have build in level converters for real RS232 levels (-10V/+10V).

Some easy way of checking this, @Daggi_Duck?

If I already had the PCB without cpu...

Best regards.

To check this, it's very easy with a fully functional receiver and if some communication comes up then the receiver starts.

I have a SEG (Vestel) DSR-6012 which don't have a RS232 port. But I have seen at the PCB that one of the two SCART connectors (TV and VCR) have connected SCART pins 10 and 12. Just I have made a simple RS232 adapter cable for

the PC with 10k series resistors (to prevent the level problem) to the SCART pins 10 and 12 and using pin 14 as GND.

Connect in this way the receiver with the PC COM-port, start a terminal program at the PC (the communication parameters are unimportant for the first tests), and switch on the receiver. You should see any transmission character at the terminal. If you don't see any characters, change the connection to the both SCART pins 10 and 12 vice versa and make the test again.

If you see any communications you can try to change the communication parameters, so that you can see readable characters. If you cannot see readable characters with any combination of the communication parameters, it should be possible that the receiver works with TTL levels and you need a level translator (e.g. MAX232). This is because the level translators are inverters. Be carefully and leave for the tests the series resistors direkt at the SCART pins 10 and 12, also if you try a level translator.

With this way I have found, that the SEG DSR-6012 have at the TV-SCART pin 10 and 12 (14 GND) a real RS232 port with real RS232 levels. So at the end I removed the series resistors and use a direkt connection to the PC COM-port.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/10 16:55

Hi guys.

Thx for your help, @Daggi_Duck. Looks like I got lucky this time, it seems to have pins 10 and 12 connected somewhere on the board. Actually, looks like it has extra connecting pads just in case one wants to connect something there...
:ohmy:

I'll just wait some more days to see if the board without cpu arrives and then back on testing. I still have to check one connection on this board...

Best regards.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/10 23:49

Hi guys.

YLG80 wrote:

Not sure, but I believe you are facing the same problem that I have with an Sti7100 box.

I believe that you have to prevent the box from booting, because after the boot, the IN_TRAP bit in the DCU_CTRL register can be set to 1 by the f/w which disables the DCU (tap port).

This would be kind of a protection against dumping the flash or using a debugger.

This could explain why you can only read the CPU ID.

So, if I had a way of preventing this bit from being set, maybe I had the problem solved?

Look at this, I may be "dreaming" but:

IN_TRAP_LOCK: Disables IN_TRAP from being cleared automatically on an IPTR jump.

This bit is set automatically on entering the diagnostics trap handler. It is cleared by the user at the end of

the trap handler to re-enable the DCU functions on exiting the trap handler. Interrupts need to be turned

off before clearing this bit to ensure that the first jump with this bit clear is the trap return.

Is the last paragraph stating what I think it is? I need someone to interpret this so I can double check what I'm thinking...

Thx.

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/12 14:39

IN_TRAP_LOCK: Disables IN_TRAP from being cleared automatically on an IPTR jump.
This bit is set automatically on entering the diagnostics trap handler. It is cleared by the user at the end of the trap handler to re-enable the DCU functions on exiting the trap handler. Interrupts need to be turned off before clearing this bit to ensure that the first jump with this bit clear is the trap return.

Is the last paragraph stating what I think it is? I need someone to interpret this so I can double check what I'm thinking...

Normally, when you have installed the trap handler routine, this bit is set to 1 when you jump into the handler routine. By the end of the handler routine that bit has to be cleared to 0 within the DCU3 handler routine before exiting. That mechanism can be seen in a ucTAP window log : the DCU3_CTRL register is continuously polled to check that flag.

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/12 16:37

not a factor with jkeys and dumping flash.
Don't dig yourself deeper into a hole.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/12 16:41

Hi guys.

Right, when you say:
Normally, when you have installed the trap handler routine
This means the handler is already in flash, from what I can understand. I don't think that is the case when we're working with jKeys, is it?

Regards.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/12 17:26

Hi guys.
slugworth wrote:
not a factor with jkeys and dumping flash.
Don't dig yourself deeper into a hole.
I was thinking that something could be done by keeping an interrupt active (one of the external ones), so the cpu wouldn't come out of DCU mode...

Regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2009/12/13 20:09

Yes, a handler (don't necessary mean that this handler is the one used to burn the flash) is normally installed since the first boot stage.
But normally you don't need a DCU3 handler if you only need to read the flash.

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/14 20:58

Hi guys.

You're right @YLG80. But for some unknown reason looks like the cpu is expecting nothing else but DCU protocol... Must find a way of preventing the cpu from booting, that's the only thing I can think of.

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2009/12/15 01:08

Maybe you have to play with dcu_trigger_in

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2009/12/17 21:56

Hi guys.

Have already tried something, @slugworth. No success so far... :(

Do you have any suggestions on how to do it, @slugworth?

Best regards.

=====

trigger

Posted by slugworth - 2009/12/18 03:08

I never played with the dcu trigger in or out, but they must have a purpose.

=====

Re:trigger

Posted by 9u4rk - 2009/12/19 02:02

Hi guys.

Well, from what I've read it's supposed to be connected to a logic analyzer or identical device. I imagine something to act as a detector for certain pre-defined conditions (watchpoints, breakpoints, etc). Already tried to short circuit the 2 of them, connect either one to GND or Vcc but, no success.

Don't really know if it's something I can use to read flash's data...

Best regards.

=====

emi_boot_mode0

Posted by slugworth - 2009/12/19 03:33

You may want to play with that pin.

It sounds like the equivalent of pin 115 from the sti5518 days.

From the sti5516 pdf

22.3.2 Booting from ROM

Any value other than 0 on the EMIBOOTMODE0 pin causes the STi5516 to boot from ROM as it comes out of reset.

On the dp311 schematic it is on page 2

On that receiver it is pin H3 and is connected to ground via a resistor.

Try finding it on your receiver.

Re:emi_boot_mode0

Posted by 9u4rk - 2009/12/19 18:45

Hi guys.

Thx for your concern, @slugworth...

In fact, I already checked that and found out on STi5517 EMIBootMode0 is on L4 which, on this PCB, is connected directly to GND (so I've been told...), so we have boot from whatever else than ROM enabled all the time. Something else is preventing it to happen... :(

Best regards.

Re:emi_boot_mode0

Posted by YLG80 - 2009/12/24 19:09

Have you already tried to test the JTAG/TAP port to see whether or not it is locked. Or if only the flash chip is locked against reading.

I've recompiled a little "hello world" test for your 5517 chip (ST20-C2 core).
(see zip attached)

Install first the Toolset R2.3.1

Unzip that test5517.zip file under the examples directory in the ST20 Toolset tree.

Be sure to have wired your interface as for ucTAP.

Launch ucTAP.

In another DOS window, cd to the sti5517test directory.

Type GO.

You should see many peek and pokes in the ucTAP if the TAP port is unlocked.

If everything is OK you should even see the Hello message.

If you can see at least peeks and pokes, that means that your JTAG port can be used in debug mode.

Please post a snapshot/capture of your ucTAP session.

I'm interested to see the peek/pokes for that CPU. <http://www.avi-plus.com/images/fbfiles/files/test5517.zip>

Re:emi_boot_mode0

Posted by slugworth - 2009/12/24 19:27

9u4rk wrote:

Hi guys.

In fact, I already checked that and found out on STi5517 EMIBootMode0 is on L4 which, on this PCB, is connected directly to GND (so I've been told...)

That is strange,since the dp311 schematic shows it as pin h3,and a sti5517 is a sti5517
the pinouts wouldn't be different from receiver to receiver. http://www.avi-plus.com/images/fbfiles/images/emi_boot_mode0.JPG

=====

Re:emi_boot_mode0

Posted by 9u4rk - 2009/12/25 22:09

Hi guys.

First, merry xmas to you all!!!

I've had no time these last 2 days for it's xmas season, ho, ho, ho... ;)

Back to biz.

YLG80 wrote:

Have you already tried to test the JTAG/TAP port to see whether or not it is locked. Or if only the flash chip is locked against reading.

I've recompiled a little "hello world" test for your 5517 chip (ST20-C2 core).

(see zip attached)

Install first the Toolset R2.3.1

Unzip that test5517.zip file under the examples directory in the ST20 Toolset tree.

Be sure to have wired your interface as for ucTAP.

Launch ucTAP.

In another DOS window, cd to the sti5517test directory.

Type GO.

You should see many peek and pokes in the ucTAP if the TAP port is unlocked.

If everything is OK you should even see the Hello message.

If you can see at least peeks and pokes, that means that your JTAG port can be used in debug mode.

Please post a snapshot/capture of your ucTAP session.

I'm interested to see the peek/pokes for that CPU. <http://www.avi-plus.com/images/fbfiles/files/test5517.zip>

Thanx @YLG80, really appreciated it! :cheer:

Where can I find Toolset R2.3.1? :blush:

I will follow your directions and post the results (will try to do it tomorrow...).

slugworth wrote:

That is strange,since the dp311 schematic shows it as pin h3,and a sti5517 is a sti5517

You're right, a STi5517 is always a STi5517 but on this board we have a different pin arrangement. Again, I can only be sure when I have the PCB with no cpu but I already checked with someone who has one of them boards and the jTag pins are assigned differently than what we have on dp311's schematic...

Santa's not delivered the PCB yet but I've been told it's on its way here. It's a long way from North Pole... :P

Best regards.

=====

SnapShot

Posted by 9u4rk - 2009/12/27 21:57

Hi guys.

YLG80 wrote:

If you can see at least peeks and pokes, that means that your JTAG port can be used in debug mode.

Please post a snapshot/capture of your ucTAP session.

I'm interested to see the peek/pokes for that CPU.

Well, looks like, for now, we're out of luck... :(

Best regards.

Re:SnapShot

Posted by 9u4rk - 2009/12/27 22:05

Hi guys.

There's the snapshot: :blush:

<http://www.avi-plus.com/images/fbfiles/images/SnapShot5517.jpg>

Best regards.

Re:SnapShot

Posted by YLG80 - 2009/12/28 10:16

No stress !

You don't have the right version of ucTAP. Should be v 0.2 beta

Here is the right one.

I've added the 5517 cpu signature. http://www.avi-plus.com/images/fbfiles/files/ucTAPv02beta_sti5517.zip

Please use a batch file like that to launch ucTAP.(ucTAP.bat)

```
uctapsrv.exe -p 0x378 -v 3
```

If your CPU is not correctly identified with that version, that means that your interface wiring is not correct for ucTAP. ucTAP should at least start the two servers @ 9737 and 9735 without errors

Re:SnapShot

Posted by 9u4rk - 2009/12/29 02:41

Hi guys.

YLG80 wrote:

If your CPU is not correctly identified with that version, that means that your interface wiring is not correct for ucTAP.

ucTAP should at least start the two servers @ 9737 and 9735 without errors

Maybe I've got the wiring wrong... :blush:

Right now I have the same wiring as in post #69:

- DB25/5 connected to RESET and DB25/12 connected to nTRST (also refer to post #48, pls). Have been told that the jTag points on post #48 are correct; wouldn't get the processor ID if otherwise, I should think...

I'll come back later on with some screen's capture.

It's been quite a mess today for we've had no mains all day long. :angry:

Best regards.

Re:SnapShot

Posted by YLG80 - 2009/12/29 09:19

:lol: This is what I've installed 3 day's ago in my garden. (Not the big ones in the background !)

Could be helpful for you !

http://www.avi-plus.com/images/fbfiles/images/IMG_0071.JPG

Black 600 wind turbine

On your interface, you should try again to swap nRST and TRST. The rest looks OK.

Re:SnapShot

Posted by 9u4rk - 2009/12/29 22:58

Hi guys.

Ehehehehheeh, for sure. Today, same problem. Less hours, but same problem. I wish I had a garden like yours but, unfortunately, I live in an apartment...

Maybe on the roof but have to ask for permission to the building's administration. :(

Will try to swap nTRST and RESET and will let you know the outcome tomorrow.

Best regards.

Re:SnapShot

Posted by 9u4rk - 2009/12/30 18:14

Hi guys.

Well, looks like things are a bit better. I do have some communication. At the end I get:

Test conditions - RESET DB25/12 and nTRST DB25/5

<http://www.avi-plus.com/images/fbfiles/images/STManswer.JPG>

Best regards.

P.S.: will make another post for the ucTap comms (don't know how to post more than one snapshot, separated by some text, in the same post).

Re:SnapShot

Posted by 9u4rk - 2009/12/30 18:26

Hi guys.

As for the ucTap comms, I got:

Same test conditions

Starting a server on 9737

Starting a server on 9735

data = 128

05 00 00 00 00 00 00 00

packet 05

data = 128

01 00 00 00 00 00 00 00

data = 128

00 00 00 00 75 63 72 2e

data = 16384

71 21 58 72 e0 71 22 50

data = 1136

48 76 2d 29 2f 92 25 fa

data = 16384

21 51 72 e1 71 22 23 59

data = 1136

2f f1 72 71 23 28 31 2f
data = 16384
f0 71 63 2f 2d 98 c2 c0
data = 1136
23 28 9d 75 f4 a2 64 0c
data = 16384
2d 21 95 72 37 ef 43 72
data = 1136
76 28 25 2c 5c d6 21 01
data = 13624
f9 a9 7a 59 13 22 25 29
data = 16384
30 00 00 00 00 00 16 00
data = 1136
00 44 01 10 02 00 00 00
data = 16384
04 00 00 00 10 00 00 00
data = 1136
00 00 00 00 00 00 00 00
data = 16384
00 03 00 00 00 00 14 fe
data = 1136
00 00 00 00 00 00 00 00
data = 16384
00 00 00 00 60 00 00 00
data = 1136
03 00 00 0c 00 00 31 00
data = 16384
11 0a 00 40 09 00 00 15
data = 1136
00 00 29 ff 80 01 00 00
data = 16384
04 00 4c 90 09 06 00 26
data = 1136
00 00 00 00 00 00 00 00
data = 16384
00 01 20 00 00 00 00 02
data = 1136
00 04 80 00 10 00 02 00
data = 16384
00 00 00 00 00 00 00 00
data = 1136
00 00 00 00 00 00 00 00
data = 4688
00 00 00 00 00 00 00 00
data = 3416
00 00 00 00 08 00 00 00
data = 28
c7 1f 01 00 bc 3b 01 00
data = 16
33 22 01 00 2b 20 01 00
data = 10
74 6d 6a 65 69 2e 64 62
data = 128
01 00 00 00 75 63 72 2e
closing 9735
And then:
02 00 00 00
02 00 00 00 81 01
IDCODE read 759296065
06 00 00 00
06 00 00 00 a1 01 41 f0
Reset with no boot.
Check IDCODE 2d41f041
val = 000000ff

P02 00 00 00
02 00 00 00 a0 01
peek 1 words from 30003000
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 30003040
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 30003000
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 30003040
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
02 00 00 00
02 00 00 00 88 01
Poke 19 words.
POKE 80000000 to 80000000 mask fffffff
POKE 80000000 to 80000004 mask fffffff
POKE 80000000 to 80000008 mask fffffff
POKE 80000000 to 8000000c mask fffffff
POKE 80000000 to 80000010 mask fffffff
POKE 80000000 to 80000014 mask fffffff
POKE 80000000 to 80000018 mask fffffff
POKE 80000000 to 8000001c mask fffffff
POKE 80000000 to 80000020 mask fffffff
POKE 80000000 to 80000024 mask fffffff
POKE 80000000 to 80000028 mask fffffff
POKE 80000000 to 8000002c mask fffffff
POKE 80000000 to 80000030 mask fffffff
POKE 80000000 to 80000034 mask fffffff
POKE 80000000 to 80000038 mask fffffff
POKE 80000000 to 8000003c mask fffffff
POKE 000000ff to 20013300 mask fffffff
POKE 00000000 to 20013300 mask fffffff
POKE 00000000 to 200130f8 mask fffffff
peek 1 words from 200130f8
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 200130f8
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
02 00 00 00
02 00 00 00 82 01
RECV ERROR: err=10053
closing 9737
I'll leave the interpretation of this data to you guys but looks to me that I haven't had any luck... :huh:

Best regards.

Re:SnapShot

Posted by YLG80 - 2009/12/30 22:42

At first reading I thought it was good when I saw the peeks and pokes.
But unfortunately each peek returns fffffff which means that nothing can be peeked.

I guess that the jtag port is locked.:blush:
You can only read the CPU ID.

Re:SnapShot

Posted by 9u4rk - 2009/12/30 23:47

Hi guys.

Well, back to square one... :(

I need to prevent the cpu from booting. What can be done in order to achieve it? :blink:

Best regards.

Re:SnapShot

Posted by YLG80 - 2009/12/31 10:15

Not sure.

I'm wondering if they use a 5517 on your board just because it has an additional security option ... on jtag.
Preventing the STB from booting will not resolve the problem.

But before concluding that you DCU access is locked, could you describe your configuration :

CPU : STi5517

Memory : M58LW032C

SDRAM : ?????

I've seen that the 5517FTACI100 was compiled using other board config .
I will make other compilations.

Another compilation with MB361

Posted by YLG80 - 2009/12/31 13:45

http://www.avi-plus.com/images/fbfiles/files/test5516_MB361.zip

Re:SnapShot

Posted by 9u4rk - 2009/12/31 14:51

Hi guys.

YLG80 wrote:

Not sure.

I'm wondering if they use a 5517 on your board just because it has an additional security option ... on jtag.
Preventing the STB from booting will not resolve the problem.

But before concluding that you DCU access is locked, could you describe your configuration :

CPU : STi5517

Memory : M58LW032C

SDRAM : ?????

I've seen that the 5517FTACI100 was compiled using other board config .
I will make other compilations.

For the SDRAM have a look here pls: http://www.elpida.com/eolpdfs/E0411E50_EOL.pdf

Thx for the new compilation. I'll try it this afternoon.

Best regards.

Re:SnapShot

Posted by 9u4rk - 2009/12/31 15:50

Hi guys.

Same test conditions as before:

RESET DB25/12 and nTRST DB25/5

Starting a server on 9737

Starting a server on 9735

data = 128

05 00 00 00 00 00 00 00

packet 05

data = 128

01 00 00 00 00 00 00 00

data = 128

00 00 00 00 75 63 72 2e

data = 16384

71 21 58 72 e0 71 22 50

data = 16384

48 76 2d 29 2f 92 25 fa

data = 16384

67 49 6e 74 20 20 20 20

data = 16384

b1 22 f0 22 f0 20 20 20

data = 16384

d1 74 70 24 ff d0 72 77

data = 16384

d6 72 74 21 9d d6 42 d0

data = 16384

00 04 08 04 06 82 c6 44

data = 16384

00 00 00 00 00 ec 80 05

data = 16384

00 00 00 00 00 00 00 00

data = 16384

00 00 08 00 78 fc 40 80

data = 16384

00 00 00 00 00 00 00 00

data = 16384

02 40 00 08 00 01 20 00

data = 3412

1e 80 83 00 00 00 00 00

my_write() failed; 532 -1 err=10054closing 9735

And then:

02 00 00 00

02 00 00 00 81 01

IDCODE read 759296065

06 00 00 00

06 00 00 00 a1 01 41 f0

peek 1 words from 30003000

!!!WaitStart failed

failed

!!!WaitStart failed

failed

!!!WaitStart failed

failed

!!!WaitStart failed

failed

!!!WaitStart failed

failed

!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 30003040
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 30003000
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 30003040
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
Reset with no boot.
Check IDCODE 2d41f041
val = 000000ff
P02 00 00 00
02 00 00 00 a0 01
02 00 00 00
02 00 00 00 88 01
Poke 18 words.
POKE 80000000 to 80000000 mask ffffffff
POKE 80000000 to 80000004 mask ffffffff

```
POKE 8000000 to 8000008 mask fffffff
POKE 8000000 to 800000c mask fffffff
POKE 8000000 to 8000010 mask fffffff
POKE 8000000 to 8000014 mask fffffff
POKE 8000000 to 8000018 mask fffffff
POKE 8000000 to 800001c mask fffffff
POKE 8000000 to 8000020 mask fffffff
POKE 8000000 to 8000024 mask fffffff
POKE 8000000 to 8000028 mask fffffff
POKE 8000000 to 800002c mask fffffff
POKE 8000000 to 8000030 mask fffffff
POKE 8000000 to 8000034 mask fffffff
POKE 8000000 to 8000038 mask fffffff
POKE 8000000 to 800003c mask fffffff
POKE 00000ff to 20013300 mask fffffff
POKE 0000000 to 20013300 mask fffffff
peek 1 words from 200130f8
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 200130f8
peeked fffffff
06 00 00 00
06 00 00 00 87 01 ff ff
02 00 00 00
02 00 00 00 82 01
RECV ERROR: err=10053
closing 9737
Got a different message on the other window:
C:\STM\ST20R2.3.1\examples\test5516_MB361>go
Warning: the product id specified in the lookup table, 0x0000d41d, does not match
the product id extracted from the device, 0x0000d41f
Error - CLOCKGEN not in X1 mode. Reconfiguration not possible
Aborting !
```

```
C:\STM\ST20R2.3.1\examples\test5516_MB361>
```

Best regards.

Re:SnapShot

Posted by YLG80 - 2009/12/31 18:28

Still not good.
The only thing that is correct is the CPU ID code reading.
The CPU cannot fall into bypass mode.

Re:SnapShot

Posted by 9u4rk - 2010/01/01 00:07

Hi guys.

Yep, unfortunately I also realise that... :S

Anyway,

Happy New Year to you all!!!

Best regards.

=====

HAPPY NEW YEAR

Posted by YLG80 - 2010/01/01 10:50

H A P P Y
N E W
Y E A R
2 0 1 0
to all posters !

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/01/01 20:20

Hello everybody, sorry for my bad english.

Congratulations to @YLG80 and @slugworth friends for the work and effort that you had been with the STI5517, and also to the @9u4rk friend for his efforts in trying to come to good results over the Dcu3 of STI5517_Kub Europe. Happy new year,2010!:P

It's been a while since I've been following this topic, I think this issue is interesting, and I want to thank you for your dedication on this issue and your spirit of solidarity, but I regret is the fact that in Ptg there's not so much dedication because there are private groups (theams) that dedicates more effort on earning (\$\$) than on the study and divulgation on this area (Exemple: CS) and for that it's a little problematic in terms of divulgation. There are ppl who dump the M58LW032C with jkeys, and they come here, to this forum, but I understand that they don't want to reveal.

The google translator is the men best friend,:laugh: .

Thanks for your time

The_onsitbin http://www.avi-plus.com/images/fbfiles/files/JTAG_STI5517_NEW_HAPPY_2010.pdf

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/02 11:51

Hi @onsitbin

Happy New Year and a big thank for your colourful contribution that will likely help 9u4rk to resolve his problem. I just want to remind here that this forum and more specifically this thread is dedicated to the repair/recovery of death boxes due to a wrong update, or interrupted update.

I guess that the other people you are talking about are trying to make money from hacking paytv which is not the goal here.

Here is the Grundig service manual part with the STi5517 CPU board.

http://www.avi-plus.com/images/fbfiles/files/Grundig_TV_ChassisLM_STi5517.pdf

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/02 22:10

Hi guys.

I have to thank you @YLG80, for your clarification as for the purpose of this thread/forum and also for the service manual. Hopefully, it'll help me on this issue but, if not, it'll definitely increase my knowledge of 5517's applications. :cheer:

Best regards.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/08 00:58

Hi guys.

Back from a forced absence... :(

OK, I think it could help if I understood how the interface works when it comes to jTAG access. Reading the STi5516 datasheet I've come to "Table 122: Instruction codes" and the 4 public instructions: - extest, idcode, sample/preload and bypass. Looks to me that I get always stuck on one of the last 2 instructions because, if they happen sequentially and in that order, the first 2 are overcome for I always get idcode. It fails after, either on sample/preload or bypass.

The way I see it, sample/preload is when the app communicates with the cpu to find out what other, if any, devices are on the scan chain and bypass is when the actual access is achieved.

Maybe if I knew what cpu is expecting when it starts sample/preload, I might be able to figure out what's going on...

Don't really know where else to go. :(

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/09 11:36

Here is the JTAG access source from T. Vlad.

It could help you figure out how it works. (this is a CPP source code)

http://www.avi-plus.com/images/fbfiles/files/jtag_p.zip

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/09 14:49

I would get jkeys working first,since that is the only program that will dump flash at this stage of the game.

Then play with the stburner.lku that came with the sti5517 toolset.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/09 21:53

Hi guys.

Thank you both.

I found something strange on the PCB which is the EMIBOOTMODE0 pin connected to the cpu's ground plane. In accordance to the STi5516 datasheet, this should enable the cpu get into bypass mode:

Any value other than 0 on the EMIBOOTMODE0 pin causes the STi5516 to boot from ROM as it comes out of reset. But the cpu doesn't get into bypass mode...

Could it be that this cpu version works the other way around when it comes to EMIBOOTMODE0 pin?

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/09 22:56

Yes this looks not normal.

If that pin is connected to ground via a pull down or a 0 ohm resistor, I would try to remove the resistor and connect that pin via a pull up to 3.3V.

But this will also put the EMI port size in 8 bit mode.

This is not a problem if you want just to test jkeys or a a tool with ucTAP.

There is perhaps an error in the DS.

I cannot imagine your set top box not cold booting from ROM and you have EMIBOOTMODE0 tied to the ground.

This is a strange sentence : "Any other value than 0 " .

I would say that an attorney has written that phrase....not an engineer !

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/10 00:26

Hi guys.

YLG80 wrote:

Yes this looks not normal.

If that pin is connected to ground via a pull down or a 0 ohm resistor, I would try to remove the resistor and connect that pin via a pull up to 3.3V.

Yes, that would be a solution if this pin was connected to GND via a pull up/down to 3.3v/GND but, what I have here is this pin as an "extension" of the ground plane which is located in the middle of the cpu area so there's no way I can disconnect GND from it. There's no resistor or anything (not even a small line...) between GND and this pin. :(

<http://www.avi-plus.com/images/fbfiles/images/CpuPad.JPG>

YLG80 wrote:

There is perhaps an error in the DS.

I cannot imagine your set top box not cold booting from ROM and you have EMIBOOTMODE0 tied to the ground.

This is a strange sentence : "Any other value than 0 " .

I would say that an attorney has written that phrase....not an engineer !

Eheheheh, it should've been an attorney... B) (no offense to the attorneys because we'd be the same if we were writing about laws in some detail...)

Anyway, how I understand the sentence, it makes sense if EMIBOOTMODE works the opposite way in this cpu version: - "Any other value than 1". It could actually work as a jTag access security, as I understand it. :(

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/10 09:15

I'm wondering if EMIBOOTMODE0 is really located there.(see also Slugworth previous post)

The DP311 schematic shows that pin in H3 which is in accordance with the STi5516 DS.

However the Grundig 5517 schematic shows that pin in L4 like shown on your picture.

Really "bizarre".

I thought that both CPU's where pin to pin compatible.

Have you been able to trace the JTAG pins up to the CPU in order to verify if they are located in accordance with the Sti5516 DS or with the Grundig schematic ?

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/10 20:22

Hi guys.

Well, it must be on L4 not H3. All the jTag pins (and a few more I tested just to make sure) checked in the same position

against Grundig schematic. That leaves us with 2 options, as far as I can understand it:

1. EMIBOOTMODE behaves as it's stated on STi5516's datasheet and so jTag is always enabled.
2. EMIBOOTMODE behaves the other way around as it's stated on STi5516's datasheet and so jTag is always disabled (here, this cpu's datasheet would be very useful to check it properly). :(

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/10 20:47

Thanks for that.

This is a clear cut between the two 5517 schematics.

suffix

Posted by slugworth - 2010/01/11 01:00

I am wondering about the H3 L4 difference also.

The dp311 schematic is genuine, not made by somebody reverse engineering a receiver. Maybe the sti5517 has different sub types? sti5517-xxx? Info on the sti5517 mention security features to confound pirates, but the sti5517 toolset has the stburner like previous processors.

Re:suffix

Posted by 9u4rk - 2010/01/11 17:08

Hi guys.

Looking further into the two schematics, dp311 and Grundig, looks to me that the first one refers to STi5516 and the latter to STi5517. If we look at the dp311 we'll find the EMIBOOTMODE on H3 and also all the JTAG pins are in accordance to STi5516. On Grundig schematic the EMIBOOTMODE is on L4 and all the JTAG pins are in accordance to STi5517. The cpu version of this board I'm "pursuing", is KUB; as Onsitbin stated on his post. I've also been told that this board can use either one of these cpus (5516 or 5517) but now, I'm not so sure (the pinout is not compatible :()...

Best regards.

Re:suffix

Posted by 9u4rk - 2010/01/12 00:12

Hi guys.

Just to let you know and try to sort out a little problem.

New test conditions:

- . ucTapv2.0_sti5517
- . test5516_MB361
- . DB25/5 RESET and DB25/12 /TRST

When I start test5516_MB361, after run ucTapv2.0_sti5517, I get:

```
POKE 00000e38 to 200130c0 mask ffffffff
POKE 00000000 to 200130c4 mask ffffffff
POKE 00000071 to 200130c8 mask ffffffff
```

POKE 00000e38 to 200130d0 mask ffffffff
POKE 00000000 to 200130d4 mask ffffffff
POKE 00000071 to 200130d8 mask ffffffff
POKE 0000038e to 200130e0 mask ffffffff
POKE 00000000 to 200130e4 mask ffffffff
POKE 00000071 to 200130e8 mask ffffffff
POKE 000002b5 to 20013140 mask ffffffff
POKE 00003333 to 20013144 mask ffffffff
POKE 000002ed to 20013130 mask ffffffff
POKE 000048a7 to 20013134 mask ffffffff
POKE 00000231 to 20013120 mask ffffffff
POKE 00003600 to 20013124 mask ffffffff
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed

peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed

!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed

failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
02 00 00 00
02 00 00 00 82 01
RECV ERROR: err=10053
closing 9737

Now the peeked value is 0x00000000, before was 0xFFFFFFFF.

Also, this window doesn't show all the comms for some reason I'm not aware of. There's no comms on 9735 port and no ID code; it was scrolling down but there came a point the window was refreshed and all the old info was gone. Like this I'm not sure if ucTap is detecting the cpu ID code or not. :(

On the other window I get:

C:\STM\ST20R2.3.1\examples\test5516_MB361>go

Warning: the product id specified in the lookup table, 0x0000d41d, does not match the product id extracted from the device, 0x0000d41f

_ST_local_PLL failed to LOCK, Aborting Setup!

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/12 01:12

Sti5516 based receivers usually have jtag ports,all the sti5516 based receivers I have also have a jtag port.Sti5517 based receivers may or may not have jtag ports, the d10 receiver I have and the dp311 receiver don't have jtag ports.I have never seen or heard of a dp311 with an sti5516.

I think this week I will start to play with jtag on my sti5516 based receiver.

The flash chip will be a problem,it is the intel 28f320 4meg that has the boot sector protected and will have to be unlocked.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/12 19:40

Hi guys.

It might have to do with the cpu revision, @slugworth...

One thing is for sure, I have 2 schematics with STi5517, one from Samsung and another one from Grundig. Both have the same pinout when it comes to jTag (maybe some more...) and it's a different pinout than the one on Echostar DP311 (I think this schematic I downloaded it from here). Also, comparing the jTag pinout of the dp311 with the STi5516 datasheet, it's a 100% match. This might be the reason why @YLG80 said earlier that STi5516 and STi5517 should be pin compatible.

Looks like we can have, at least, two different pinouts for the STi5517 (maybe it depends on the suffix, as you said earlier...).

Best regards.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/15 13:05

Hi guys.

slugworth wrote:

Sti5516 based receivers usually have jtag ports, all the sti5516 based receivers I have also have a jtag port. Sti5517 based receivers may or may not have jtag ports, the d10 receiver I have and the dp311 receiver don't have jtag ports. I have never seen or heard of a dp311 with an sti5516.

I think this week I will start to play with jtag on my sti5516 based receiver.

The flash chip will be a problem, it is the intel 28f320 4meg that has the boot sector protected and will have to be unlocked.

So, the dp311 you have doesn't have jTag ports. Is this receiver's schematics the one we have here in the forum or is it a different one, @slugworth?

Best regards.

=====

d10

Posted by slugworth - 2010/01/15 15:08

I have the directv D10 receiver, which is sti5517 based and has no jtag port.

I would have to remove the processor to trace out the jtag pins.

The dp311 others have has a jpeg with the jtag "spots" identified.

=====

Re:d10

Posted by 9u4rk - 2010/01/15 16:57

Hi guys.

Thx for your answer @slugworth!

I asked it because I'm wondering if the dp311 has the same problem I do on this board I'm trying to get through. They could both share the same problem and, if so, one more reason to look for schematic's similarities that might cause the same behaviour.

Best regards.

=====

Re:d10

Posted by slugworth - 2010/01/15 17:22

Since we are the only ones playing with dcu3 jtagging,you have probably gotten the furthest along.I have never even seen jtag dumps from the dp311,even tho the jtag "spots" were known via the jpeg somebody took of the mainboard without the processor. Tough being a pioneer. <http://www.avi-plus.com/images/fbfiles/images/dp311jtagpoints.jpg>

=====

Re:d10

Posted by 9u4rk - 2010/01/15 21:10

Hi guys.

Thx for your concern, @slugworth.
Precisely what I first thought were the jTag points:

AC7 - TDI
AD7 - TMS
AE6 - TRST
AE7 - RESET
AF6 - TDO
AF7 - TCK

This is in accordance with STi5516's datasheet, but not the jTag points we have on this board and on Grundig's schematic (kindly uploaded by @YLG80).

Best regards.

=====

Re:Sti5517 flash dump

Posted by zmeura - 2010/01/28 15:27

Hi my friends.

I have one receiver with STi5517 (FUB) and M58LW032A flash.I have past trough all the things @9u4rk has test untill now and I'm exactly in the same situation.DCU peek error in Jtag and same response in ST20tool.Like this:

```
-in ucTap
02 00 00 00
02 00 00 00 81 01
IDCODE read 759296065
06 00 00 00
06 00 00 00 a1 01 41 f0
Reset with no boot.
Check IDCODE 2d41f041
val = 000000ff
P02 00 00 00
02 00 00 00 a0 01
peek 1 words from 30003000
peeked ffffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 30003040
peeked ffffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 30003000
peeked ffffffff
06 00 00 00
```

```
06 00 00 00 87 01 ff ff
peek 1 words from 30003040
peeked ffffffff
06 00 00 00
06 00 00 00 87 01 ff ff
02 00 00 00
02 00 00 00 88 01
Poke 19 words.
POKE 80000000 to 80000000 mask ffffffff
POKE 80000000 to 80000004 mask ffffffff
POKE 80000000 to 80000008 mask ffffffff
POKE 80000000 to 8000000c mask ffffffff
POKE 80000000 to 80000010 mask ffffffff
POKE 80000000 to 80000014 mask ffffffff
POKE 80000000 to 80000018 mask ffffffff
POKE 80000000 to 8000001c mask ffffffff
POKE 80000000 to 80000020 mask ffffffff
POKE 80000000 to 80000024 mask ffffffff
POKE 80000000 to 80000028 mask ffffffff
POKE 80000000 to 8000002c mask ffffffff
POKE 80000000 to 80000030 mask ffffffff
POKE 80000000 to 80000034 mask ffffffff
POKE 80000000 to 80000038 mask ffffffff
POKE 80000000 to 8000003c mask ffffffff
POKE 000000ff to 20013300 mask ffffffff
POKE 00000000 to 20013300 mask ffffffff
POKE 00000000 to 200130f8 mask ffffffff
peek 1 words from 200130f8
peeked ffffffff
06 00 00 00
06 00 00 00 87 01 ff ff
peek 1 words from 200130f8
peeked ffffffff
06 00 00 00
06 00 00 00 87 01 ff ff
02 00 00 00
02 00 00 00 82 01
RECV ERROR: err=10053
closing 9737
```

-in ST20

C:\STM\ST20R2.3.1\examples\test5517>go

Error - CLOCKGEN not in X1 mode. Reconfiguration not possible

Aborting !

L4 (EMIBOOTMODE0) is pull down to ground ,I have tried to pull up at 3.3V,receiver don't boot but processor still recongnized and it's the same situation like before.Same with jtag and ucTap.

Pinout is exactly like in Grundig schematic.

First part from ucTap is like this:

Starting a server on 9737

Starting a server on 9735

data = 128

05 00 00 00 00 00 00 00

packet 05

data = 128

01 00 00 00 00 00 00 00

data = 128

00 00 00 00 75 63 72 2e

data = 16384

71 21 58 72 e0 71 22 50

data = 1136

48 76 2d 29 2f 92 25 fa

data = 16384

21 51 72 e1 71 22 23 59

data = 1136

```
2f f1 72 71 23 28 31 2f
data = 16384
f0 71 63 2f 2d 98 c2 c0
data = 1136
23 28 9d 75 f4 a2 64 0c
data = 16384
2d 21 95 72 37 ef 43 72
data = 1136
76 28 25 2c 5c d6 21 01
data = 13624
f9 a9 7a 59 13 22 25 29
data = 16384
30 00 00 00 00 00 16 00
data = 1136
00 44 01 10 02 00 00 00
data = 16384
04 00 00 00 10 00 00 00
data = 1136
00 00 00 00 00 00 00 00
data = 16384
00 03 00 00 00 00 14 fe
data = 1136
00 00 00 00 00 00 00 00
data = 16384
00 00 00 00 60 00 00 00
data = 1136
03 00 00 0c 00 00 31 00
data = 16384
11 0a 00 40 09 00 00 15
data = 1136
00 00 29 ff 80 01 00 00
data = 16384
04 00 4c 90 09 06 00 26
data = 1136
00 00 00 00 00 00 00 00
data = 16384
00 01 20 00 00 00 00 02
data = 1136
00 04 80 00 10 00 02 00
data = 16384
00 00 00 00 00 00 00 00
data = 1136
00 00 00 00 00 00 00 00
data = 4688
00 00 00 00 00 00 00 00
data = 3416
00 00 00 00 08 00 00 00
data = 28
c7 1f 01 00 bc 3b 01 00
data = 16
33 22 01 00 2b 20 01 00
data = 10
74 6d 6a 65 69 2e 64 62
data = 128
01 00 00 00 75 63 72 2e
closing 9735
Administrator@xxx connected on Thu Jan 28 14:58:32 2010
```

```
val = 000000ff
P02 00 00 00
02 00 00 00 81 01
IDCODE read -1
06 00 00 00
06 00 00 00 a1 01 ff ff
closing 9737
```

but this appears even if the receiver is stoped,so I guess is nothing useful.

Re:Sti5517 flash dump

Posted by zmeura - 2010/01/28 16:18

And another thing: in ucTAPsrv.cpu is a little mistake.Put this line:
STi5517, 0x2d41f041, 0x30003004, 0x00000200

and ucTAP will recognize the CPU.Now the errors are like before plus this:

```
.....
POKE 0000038e to 200130e0 mask fff
POKE 00000000 to 200130e4 mask fff
POKE 00000071 to 200130e8 mask fff
POKE 000002b5 to 20013140 mask fff
POKE 00003333 to 20013144 mask fff
POKE 000002ed to 20013130 mask fff
POKE 000048a7 to 20013134 mask fff
POKE 00000231 to 20013120 mask fff
POKE 00003600 to 20013124 mask fff
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
```

06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed

failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed

06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
02 00 00 00
02 00 00 00 82 01
RECV ERROR: err=10053
closing 9737

In ST20:

C:\STM\ST20R2.3.1\examples\test5517>go
PLL failed to LOCK, Aborting Setup!

other screen

Posted by slugworth - 2010/01/28 19:13

I never paid any attention to the uctap screen when I was playing with the sti5105 jtag lku. I was more interested in the lku screen and error messages. The lku may have the wrong ram size/addresses or other problems.

needful things

Posted by slugworth - 2010/01/28 19:18

All you need in the .cpu file is:

STi5517, 0x2d41f041,

uctap will come up with it's own values for the other addresses.

It is more important to have the correct dcu3 settings in the .lku

Ram size/addresses are critical as people that played with the sti5105

jtag will tell you.

=====

jkeys

Posted by slugworth - 2010/01/28 19:21

I still say you have to get jkeys working first without dcu peek errors.

Shorten your jtag cable down to a stub if necessary.

You need a good flash dump anyway before you even think of erasing.

=====

Re:Sti5517 flash dump

Posted by zmeura - 2010/01/28 19:48

Don't know when I'm gonna have time again,maybe next week.Gonna try again with jtag and studdy more about st20,hard to find adresses if there is no dump.

=====

Re:needful things

Posted by 9u4rk - 2010/01/28 23:16

Hi guys.

slugworth wrote:

All you need in the .cpu file is:

STi5517, 0x2d41f041,

uctap will come up with it's own values for the other addresses.

It is more important to have the correct dcu3 settings in the .lku

Ram size/addresses are critical as people that played with the sti5105

jtag will tell you.

I must agree with @slugworth: - As long as we have "DCU peek error" when we start jKeys, we won't be able to do anything.

On the other hand, @YLG80 compiled this little "Hello world" program to see if any comms were going through but, as far as I could test, nothing went. :(

It's good to have more people trying to play with this cpu, @zmeura... ;)

Best regards.

=====

Re:Sti5517 flash dump

Posted by Boxy - 2010/01/29 17:18

Hi,

I have a box with an OMEGA STi5517SWA chip onboard and am having similar problems to the above both with a

buffered Jtag and a proper STi jtag/DCU unit.

The pinout i'm using for Jtag is identical to the STi5516 chip and this get me as far as being able to read the chip Id. No problem there !

However, as soon as I try and use the DCU then I get a similar result to some of the above posts. The return is pretty much always (with a very few exceptions) all 00's or all FF's. The exception seems to be that I can read a few processor registers and it looks like they may have sensible values (hard to tell though - could just be random values). The proper STi Jtag/DCU unit tends to disconnect as soon as you try to use it as it fails to change the DCU control register in order to stall the processor.

The buffered Jtag goes further although its obvious its having the same problems. Its just not too bothered about the errors.

When I stick the scope on the TDO pin of the processor, you can see that it goes into 3-state mode almost immediately you try to put the processor into DCU mode. Thats why either 00's or FF's are returned, its just whatever logic value is lying around. You can flip the value returned by briefly touching the pin to 3.3v or Gnd to confirm.

This behaviour seems to indicate the device is not properly accepting entry to DCU3 mode which sort of leads me to believe that either the command sequence has changed, something else is needed or the device had been DCU disabled somehow.

Anybody any thoughts ?

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/29 18:00

I would try dumping the flash with jkeys.
And don't forget, that program is almost 10 years old now.
Sometimes you are better off with an older version of windows on a slower pc.
The first versions of the sti5105 jtag had to be run on a 700mhz pc or slower,
as an example.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/29 18:19

Make sure you are using pin17 on the jtag instead of the standard pin19.
I wasted many weeks on that mistake with the sti5105 jtag program.

=====

Re:Sti5517 flash dump

Posted by Boxy - 2010/01/29 20:54

Jkeys does very little except Id the processor. Even a manual dump only produces a file full of 00's or FF's. As I said above, the jtag pins simply go into a 3-state mode when a DCU transfer is initiated.

The ST Jtag i'm running is a proper Micro-Connect DCU3 unit. Its only a couple years old so should be designed to run with these processors. It certainly runs fine with later DCU3 processors. It connects to the ST toolset via ethernet using an IP address so parallel port configuration or PC speed shouldn't enter into it. This unit simply aborts with an error when connected to this particular chip. Apparently it cannot manipulate the DCU registers so it just gives up. (Checking on the scopt and yes, the TDI output is still in 3-state mode).

For the buffered Jtag using parallel port, i've been through testing on quite a few PC's ranging from an old 66Mhz 486 through various speeds upto 2.5Ghz. Results are pretty much identical regardless so i'm convinced its not a PC speed problem.

Pin configuration makes no real difference. On the ST unit its connected as per the manufacturer recommendations. On the buffered Jtag i've tried just about every configuration you or anybody else has ever mentioned but results are pretty much always the same. Except for the chip ID, the output stays in a 3-state mode.

Initially, I thought the driver on the chip TDO output might be broken but its exactly the same on a further two boxes tested.

There's definately something preventing access to this chip. Perhaps initiating DCU mode requires some kind of "key" or some other register manipulation.

Re:Sti5517 flash dump

Posted by Boxy - 2010/01/29 20:57

(Checking on the scopt and yes, the TDI output is still in 3-state mode).

Type: The TDI should, of course, have been TDO

For some reason, cant edit the post to correct.

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/29 21:24

You have to highlight your post then hit edit.

I don't know what program you are running so I can't really comment further.

For the sti5105 I had to make my own .lku file to run under the st20 toolset.

It would only erase/program,I relied on jkeys to do the dumping.

It was mentioned the sti5517 has some kind of security to foil pirates.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/29 23:36

Hi guys.

Boxy wrote:

However, as soon as I try and use the DCU then I get a similar result to some of the above posts. The return is pretty much always (with a very few exceptions) all 00's or all FF's. The exception seems to be that I can read a few processor registers and it looks like they may have sensible values (hard to tell though - could just be random values). The proper STi Jtag/DCU unit tends to disconnect as soon as you try to use it as it fails to change the DCU control register in order to stall the processor.

Which registers are you able to read, @Boxy? Can you post a screenshot so I can compare with mine, pls?

Boxy wrote: When I stick the scope on the TDO pin of the processor, you can see that it goes into 3-state mode almost immediately you try to put the processor into DCU mode. Thats why either 00's or FF's are returned, its just whatever logic value is lying around. You can flip the value returned by briefly touching the pin to 3.3v or Gnd to confirm.

This behaviour seems to indicate the device is not properly accepting entry to DCU3 mode which sort of leads me to believe that either the command sequence has changed, something else is needed or the device had been DCU disabled somehow.

Anybody any thoughts ?

I wish I had anything to add but I don't. I'm only starting on JTAG access and still trying to understand how things work but I agree that something might be missing...

Best regards.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/30 13:44

Hi guys.

From what I can understand, we're able to control DCU by writing into its registers. So far, all peeked messages we got were either 0x00000000 or 0xFFFFFFFF. Doesn't this mean that we're getting no message at all (I'm repeating what @Boxy said, I know...)? If this is so, couldn't it mean that the target isn't allowed, somehow, to communicate with the host? Are the TARGET_PEEK_ENABLE and TARGET_POKE_ENABLE activated by test compilation?

Sry for all these beginner questions, that you all know the answer... :blush:

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/30 16:52

Hello,

Unfortunately, as you cannot have full access to the registers through JTAG, you have no control on the DCU_CONTROL register bit 7 and Bit 6.

These bits could be disabled if IN_TRAP is set. (see my previous post on IN_TRAP)

So the test compilation cannot change these bits.

This is not a compilation problem.

I've executed that 5517 test compilation on my STi5105 board and the first few peek and poke were returning consistent values.

After reading the CPU ID, the JTAG program (JKEYS or others) needs to setup the tap interface in BYPASS mode which does not happen with your board, likely because there is a protection against JTAG.

=====

readfile

Posted by slugworth - 2010/01/30 17:26

But if you look at the stburner that comes with the sti5517 toolset, it has a readfile function in the menu for reading the flash to pc like our old sti5518 stburner .lku's

That toolset was specifically for the sti5514/16/17 so it must be doable.

If the sti5517 was protected from reading ST would have left the stburner out of the toolset one would think.

There is a guy selling a blackcat usb jtag cd/cable on ebay and he claims it does the sti5516/17 processor. This is probably a scam because that program is geared to cable modem processors. Do a google search for blackcat sb5120

=====

tt_flash.c

Posted by slugworth - 2010/01/30 18:06

A chunk of that file included in the sti5517 toolset stburner files. It shows the readfile function is available.

```
/*-----  
* Function : ReadFile  
*         Read HEX file into memory  
* Input   :  
* Output  :  
* Return  : File size  
*-----*/
```

```
U32 FLASH_ReadFile( char *Filename )
```

```

{
long int  HexFile_p;      /* datafile descriptor */
long int  HexFileSize;   /* size in bytes of the file */

/* Open and Read file into memory */
HexFileSize = 0;

HexFile_p = debugopen(Filename, "rb");
if (HexFile_p < 0)
{
STTBX_Print(("Error opening file '%s'\n", Filename ));
}
else
{
HexFileSize = debugfilesize(HexFile_p);

/* allocate File data buffer */
FreeFileDataBuffer();
FlashData_p = (char*) memory_allocate( SystemPartition, (U32) HexFileSize );
if ( FlashData_p != NULL )
{
STTBX_Print(("Loading '%s'\ into memory, wait .. ", Filename ));
debugread(HexFile_p, FlashData_p, (size_t) HexFileSize);
STTBX_Print((" %d bytes\n", HexFileSize ));
}

debugclose(HexFile_p);
}

if ( HexFileSize > 0 )
{
/* convert buffer to binary and resize memory */
STTBX_Print(("Converting file in memory, wait .. "));
FlashSize = ConvertMemory( HexFileSize );
STTBX_Print(("Now %d bytes\n", FlashSize ));
if ( FlashSize > 0 )
{
FlashData_p = (char*) memory_reallocate( SystemPartition, FlashData_p, FlashSize );
}
}

if ( FlashData_p == NULL )
{
STTBX_Print(("Not enough memory for HEX file\n"));
FlashSize = 0;
}

return( FlashSize );
} /* end of FLASH_ReadFile */

```

=====

Re:tt_flash.c

Posted by YLG80 - 2010/01/30 19:15

I'm still questioning myself on the reason why the CPU pinout on their board is different .

I've checked that readfile routine, but, to me, it is used to read the file from the PC.

They should try to use that 5517FTACI.

The stburner_bak directory can be compiled with no error.

The other directory (stburner) generates some errors, but I've not taken the time to check why.

In the stburner directory, there are additional routines in the main.c : flash WPen, device ID check etc ..

=====

Re:tt_flash.c

Posted by slugworth - 2010/01/30 20:15

YLG80 wrote:

I'm still questioning myself on the reason why the CPU pinout on their board is different .
People on other forums get violent when you mention that.
But they still haven't jtagged their way yet.
Once I get done with other projects I may remake the sti5105 jtag to see if I can add
the read flash function.
I have a bricked sb5120 modem I have to fix first.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/30 20:19

I wish I had the source code to the pvr2flash .lku
That probably would have worked with minor tweaking since the sti5514
is also dcu3 core2
Was there ever a .lku disassembler?

=====

Re:tt_flash.c

Posted by 9u4rk - 2010/01/30 22:49

Hi guys.

slugworth wrote:

YLG80 wrote:

I'm still questioning myself on the reason why the CPU pinout on their board is different .
People on other forums get violent when you mention that.
But they still haven't jtagged their way yet.
People get violent? What do you mean, @slugworth?
I'm glad we take it easy here... :)

Best regards.

=====

Re:tt_flash.c

Posted by 9u4rk - 2010/01/31 01:52

Hi guys.

When I start ucTap I keep having these errors:

ucTAP v 0.2 beta May 31 2006 (c) 2006 TAPDancers

ucTAP is a program to emulate ST20 Micro Connect functions over a basic JTAG in
terface.

The specified service has been marked for deletion.

The specified service has been marked for deletion.

The service cannot be started, either because it is disabled or because it has n
o enabled devices associated with it.

OR

The specified service does not exist as an installed service.

The specified service does not exist as an installed service.

The specified service does not exist as an installed service.

Your CPU is an STi5517 DCU_CTRL 30003004, DCU_DEVICE_ACCESS_MASK 00000200

Starting a server on 9737

Starting a server on 9735

I think I should be getting something like:

ucTAP v 0.1 beta Apr 12 2006 (c) 2006 TAPDancers

ucTAP is a program to emulate ST20 Micro Connect functions over a basic JTAG interface.

Operation successfull.

Operation successfull.

Operation successfull.

Your CPU is an STi5517 DCU_CTRL 30003004, DCU_DEVICE_ACCESS_MASK 00000200

but never do... :(

I'm not sure if these errors stop ucTap from doing what's supposed to or not and, if they do, don't know how to get it right.

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/31 02:24

Those are bogus errors, usually from starting/stopping uctap.

As long as you see

Starting a server on 9737

Starting a server on 9735

everything is copacetic. <http://www.avi-plus.com/images/fbfiles/images/kosher.jpg>

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/31 02:28

The version of uctap v0.2 I have never had a readme.

But if you look at the .exe with a hex editor you can see helpful hints.

The following ripped from the .exe file.

ucTAP v 0.2 beta

(c) 2006 TAPDancers ..May 31 2006.

ucTAP is a program to emulate ST20 MicroConnect functions over a basic JTAG interface...

ucTAPsrv ...

-t: Uses a fast memset using a trap, speeds up the loading..

-i port: The MicroConnect Boot port..

-d port: The MicroConnect Data port..

-v debug_level: debug output 0 (off/default).

1 (Command summary)..

2 (+Specific data details)

3 (+RAW ethernet payload data)

-c DCU_CTRL_ADR: Address of the DCU control register ..

Set automatically if CPU is detected ..

-m DCU_CTRL_MASK: Bitmask of DCUControl for device access enable..

Set automatically if CPU is detected ..

(so theoretically these don't have to be set in the .cpu file)

example:.. ucTAPsrv -p 0x378 -i 9735 -d 9737 -c 0x3000 -m 0x00080000

uctap needs a modified jtag connection; instead of the usual

pin 9,11,13,15,19- pin 17 has to be used instead of pin 19 and pin 19

has to go to the db25 connector pin12.

Uctap is a command line program, so you have to drop to dos in the directory where the file is located then run the bat file(just type tap)and hit the enter key.

It should show success 3x then minimize the screen.

Re:Sti5517 flash dump

Posted by slugworth - 2010/01/31 02:32

An example of a bogus error.

Uctap still worked. Always use v 0.2, it was the last release. http://www.avi-plus.com/images/fbfiles/images/uctap_error_to_ignore.JPG

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/31 07:57

Also double check your firewall, if you have errors like these.
You should add an exception for ucTAP in the firewall settings.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/31 13:24

Hi guys.

Once again, always learning. :cheer:

Never thought of checking the .exe for instructions... :huh:

Also, will add an exception on my firewall.

Thx.

@YLG80, I'd like to give 5517ftaci100B a shot but I'm not sure how to do it. Any chances on help, pls?

Thx.

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2010/01/31 17:06

I've placed an stburner (5517FTACI_STBURNER.zip) compilation in the usual directory (slugworth will also know where it is)

The target defined is called ucTAP.

I cannot test it, but when I type NOGUI, I only have a target connect error.

At compile time I did not get any error.

If you get a target error (error 1) that means that you have not changed the target definitions in other directories in the tree.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/01/31 18:44

Hi guys.

Thx @YLG80. :)

Looks like the way I was wiring my JTAG interface, was not the better one. It makes no big difference when it comes to bypass/DCU mode but, like this, ucTAP is now able to reset cpu.
Going through the Google's cache kindly recovered by @YLG80, I found out that ucTAP has support for nRST. So, the interface wiring is as follows:

DB25.....JTAG
2.....R100....TMS
3.....R100....TCK
4.....R100....TDI
5.....R100....nTRST
6.....R100....nRST
13...R100....TDO
25.....GND

Maybe this is a mistake so I'd like to hear from you guys...

Best regards.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/01 00:54

Hi guys.

YLG80 wrote:

If you get a target error (error 1) that means that you have not changed the target definitions in other directories in the tree.

Thx.

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/01 01:57

for uctap I always used this one.

lots of people fixed their sti5105 based receivers with it.

http://www.avi-plus.com/images/fbfiles/images/Sheme_Jtag_5119.jpg

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/01 16:46

Hi guys.

You must be right @slugworth. So far, I have no way of confirming either wiring for I've only gone up to cpu IDCode and nothing else. I was just testing the connections that are on Google's cache, page 25. I know it refers to STIControl but when I used pin DB25/6 connected to nRST I could see my board's power led going off and back on whenever I started the test programs on ST Toolset. The same happens when starting ucTAP...

Best regards.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/03 23:14

Hi guys.

Well, I tried to do something with 5517FTACI100B but didn't go any further than before, unfortunately. ucTAP gives the same peeked values... :(

I also noticed that when I set up the environment for stburner, it referred ST20R1.9.6 on the work space concole. I changed it accordingly but still the same problem.

In the meantime, had a look at 5517FTACI_docs and found this on page 13 of 5517FTACI_100B.pdf:

Support of DCU1.9.6 / DCU2.0.5

This release of the software currently supports ST20 Toolset Version 1.9.6 . The Chip Sti5518 command for instance enables you to readily monitor all on-chip registers thru the GUI (Figure 8.2).

However the command st20cc -runtimeos20 is not used in this release. It means that the setting DVD_OS20=RUNTIME has not been used to build this software tree.

This release is tested with ST20 Toolset Version 1.9.6P6 .

Future releases of the software tree will support a newer version of the DCU toolset which is 2.0.5.

Does this mean we need a newer version of 5517FTACI in order to have support for DCU3 or this revision is OK? I'm using ST20 Toolset R2.3.1 at the moment...

Thx.

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/03 23:48

Other toolsets had the mb382.cfg which covers the sti5517,the 5517FTACI100B just had extra goodies for making firmware,which isn't an issue here.

I still haven't seen screendumps other than the uctap ones here,so your settings may still be off.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/04 01:21

Hi guys.

slugworth wrote:

Other toolsets had the mb382.cfg which covers the sti5517,the 5517FTACI100B just had extra goodies for making firmware,which isn't an issue here.

I still haven't seen screendumps other than the uctap ones here,so your settings may still be off.

I think I've just realised precisely that, @slugworth. 5517FTACI100B is very good but for firmware compilation. Most probably it won't solve the problem I'm facing with this board of mine. :(

Anyway, I will post some screenshots tomorrow (it's getting late...) of what I get when running stburner.

The JTAG wiring I have now is according to the one you posted for ucTAP (nRST on DB25/5 and nTRST on DB25/12) but if you're talking about configuration files, I'm still using the same as before. As for these I don't yet feel comfortable enough to modify them. I'd thank you all guidance you feel necessary in order to improve my understanding how things work.

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/04 16:39

All it takes is 1 setting to be off in the .lku file and the program won't work. You must know how much ram the receiver has, as an example. This is the error you get when you don't use pin17 on the jtag. http://www.avi-plus.com/images/fbfiles/images/not_pin17.jpg

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/04 23:46

Hi guys.

Using the ucTAP wiring I run the 5517FTACI and on the ucTAP window I got:

```
POKE 00000e38 to 200130c0 mask ffffffff
POKE 00000000 to 200130c4 mask ffffffff
POKE 00000071 to 200130c8 mask ffffffff
POKE 00000e38 to 200130d0 mask ffffffff
POKE 00000000 to 200130d4 mask ffffffff
POKE 00000071 to 200130d8 mask ffffffff
POKE 00000e38 to 200130e0 mask ffffffff
POKE 00000000 to 200130e4 mask ffffffff
POKE 00000071 to 200130e8 mask ffffffff
POKE 000002b5 to 20013140 mask ffffffff
POKE 00003333 to 20013144 mask ffffffff
POKE 000002ed to 20013130 mask ffffffff
POKE 000048a7 to 20013134 mask ffffffff
POKE 00000231 to 20013120 mask ffffffff
POKE 00003600 to 20013124 mask ffffffff
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
```

failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed

06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed

!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013004
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
peek 1 words from 20013008
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
!!!WaitStart failed
failed
peeked 00000000
06 00 00 00
06 00 00 00 87 01 00 00
02 00 00 00
02 00 00 00 82 01
RECV ERROR: err=10053
closing 9737
On the 5517FTACI Workspace:
<http://www.avi-plus.com/images/fbfiles/images/Workspace.JPG>
Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/05 00:06

so product id is the first thing to fix.
A picture is worth a 1000 uctap dumps.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/05 01:10

Hi guys.

You're right, @slugworth: - "A picture is worth 1000 words". :)

OK, I think that's hapenning because it's calling the STi5516 and mb361 setup. I tried to find where this is but no success. :(

Any advice, pls?

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/05 01:49

that would be in the .c and .h files the .lku is made from.

If you only have the .lku you would have to start from scratch to make your own .lku.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/05 12:14

Hi guys.

I'm not sure (I'm not on my home PC) @slugworth but I think that I only have the .lku, so I must start thinking of creating my own. This is not an easy thing to do for a beginner like me and, so far, I've only been able to go as far as simulating the getstart example that comes on Quick Start Guide. I definitely need much more practice on compiling a .lku, but I'm keen on doing so...

Anyway, I will try to give it a go and come back here, if you guys don't mind, looking for guidance whenever I get stuck. :huh:

Maybe on another thread for this one is large enough already and also it's somewhat off topic...

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/05 17:35

It's not easy,I haven't played with .lku making in 2 years and I have no jtaggable sti5517 based receiver to try it on.In the past I tried helping people with the sti5107 and sti5119 based receivers and they didn't make out very well.Often it's just a minor tweak that gets you going,like with the sti5105 based jtag a delay had to be added to the flash erase/write to get it to work.Without an actual receiver to play with,I would just be guessing.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/05 22:11

Hi guys.

Anyway, I thank you for whatever help you might provide...
By trying this I'll be "playing" for quite a long time, which I find interesting.

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/06 01:23

I mentioned it before, but a lot of the .h and .c files used to make the .lku files are from the 1990's and those vintage pc's. So even if you make a .lku it may only work on slow pc's until you tweak some more. Many people actually practice on other sti5518 based receivers, then graduate to the receiver/processor they actually need to jtag. A lot more info was available for the sti5518 than the sti5516/17.

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/06 23:37

Hi guys.

Makes sense working my way through with a 5518 based receiver @slugworth before trying on 5517, but but I don't have any at the moment... :(
I'll be looking for one.

Best regards.

Re:Sti5517 flash dump

Posted by YLG80 - 2010/02/07 09:25

Preferably an Sti5517KUx....

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/07 14:21

Hi guys.

Instead of a 5517KUx (I wish...), I'm going to have a 5518 to get my Carnival's bonfire started. :P
As far as I understand it's still a DCU3 based cpu.
Not the greatest news but good enough...

Best regards.

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/07 16:33

9u4rk wrote:
Hi guys.

As far as I understand it's still a DCU3 based cpu.

If it were we wouldn't be having this conversation.
Sti5518 is the original dcu based, not dcu3, that is why jkeys ,skymax and other jtag programs work with it.
But there are lku based burners that work and have the sourcecode, so it is regarded
as a training tool for making same even though using jkeys is much easier.

=====

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/07 18:58

Hello good afternoon everyone, continuing with the test sti5517 already damaging two boards n3, came a new version of EJTAG (04/02/2010

Version 0.1.0.1427 CPLD EJTAG

Added work with ST20c1 DCU3 (sti5119, 5105,5517, etc.).

Rewritten work with files (now working through the mapping file into memory)

that supposedly supports the ST20 c1 sti5xxx conform image attachment, do not know whether it is fake, but the friend @ Slugworth will be more comfortable talking about this soft for me,

I take it I'm also having trouble in STI5100 dcu3 and have problems in setting the flash 28F640J3 *. def jkeys, and have the id but the error selecting this flash

thank aid

Thank you and sorry for my bad English

Regards

Onsitbin http://www.avi-plus.com/images/fbfiles/images/Possible_Jtag-e6110d347f91ef3ff5e37d0aece4c499.jpg

<http://www.avi-plus.com/images/fbfiles/files/jkeys.rar>

=====

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/07 19:09

Please remove post n^a 309

error C/P

sorry

tanks

Onsitbin

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2010/02/07 21:34

Hello @Onsitbin

Thanks for the info.

Despite of the fact that I successfully registered on the russian web site, I'm still not allowed to download that promising program.

On your Sti5100.

Could you specify the suffix?

Is that a Sti5100KUx ?

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/07 22:03

I could be wrong but I think that was the usb version that you had to pay for, not free or public.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/02/07 22:06

Hi guys.

slugworth wrote:

9u4rk wrote:

But there are lku based burners that work and have the sourcecode,so it is regarded as a training tool for making same even though using jkeys is much easier.

Thx for clarifying that for me @slugworth, I was thinking otherwise... :S

When I get the 5518 I'll come back to the subject.

I think you need to wait several days and be posting to be allowed to download any files from that site, @YLG80.

Best regards.

=====

Re:Sti5517 flash dump

Posted by YLG80 - 2010/02/07 22:40

That EJTAG version looks interesting.

A bit difficult to interpret the russian buttons.

But it looks like it has really the DCU3 capability.

I guess I don't have the right interface to work with that program because I get multiple timeout errors.

But it recognizes the CPU on the second tab although it does not print the correct CPU id in the logger window.

(There is a strange message from Avira when downloading that file :

Compressed with an odd runtime algorithm : pck/obsidium.

Avira does not like that and erase the executable)

=====

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/07 23:30

YLG80 wrote:

Hello @Onsitbin

Thanks for the info.

Despite of the fact that I successfully registered on the russian web site, I'm still not allowed to download that promising program.

On your Sti5100.

Could you specify the suffix?

Is that a Sti5100KUx ?

Hello dear @YLG80 already sent you a PM, my processor is Sti5100Luc

Tanks

=====

tiny tool

Posted by slugworth - 2010/02/07 23:53

the tiny tools is only for dcu3 core1 judging from the screenshot.
The sti5517 and the sti5100 are core2 so not doable with that program.
The sti5105 to sti5119 are core1 dcu3.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/08 02:28

YLG80 wrote:

That EJTAG version looks interesting.

A bit difficult to interpret the russian buttons.

But it looks like it has really the DCU3 capability.

I guess I don't have the right interface to work with that program because I get multiple timeout errors.

But it recognizes the CPU on the second tab although it does not print the correct CPU id in the logger window.

(There is a strange message from Avira when downloading that file :

Compressed with an odd runtime algorithm : pck/obsidium.

Avira does not like that and erase the executable)

If it is like the old ejtag_tt the jtag wiring isn't standard.

A buffered jtag was a must when I was playing with the old ejtag_tt and conexant processors.It was no speed demon back then either.

Re:Sti5517 flash dump

Posted by romeok01 - 2010/02/08 17:45

CPLD EJTAG 0.1.0.1427 - ST20c1 DCU3 (sti5119,5105,5517,...)

http://rapidshare.com/files/347737793/CPLD_EJTAG_0_1_.1.0.1427.rar.html

http://rapidshare.com/files/347737793/CPLD_EJTAG_0_1_.1.0.1427.rar.html http://www.avi-plus.com/images/fbfiles/images/CPLD_EJTAG_0.jpg

ejflash ini

Posted by slugworth - 2010/02/08 19:38

The ejflash.ini has to be edited to include the flash chip you are playing with.

I think the cable pinout is the ejtag wiring,not the standard simple jtag.

The jtag cable wiring must match the program,so you can't use wigglers or other wiring designed for other jtag programs.

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/08 22:09

Tanks

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/08 23:33

I may not be a simple jtag,it looks like something you would have to buy.
From the tele-sat forum. <http://www.avi-plus.com/images/fbfiles/images/b5a6b2db5e9b.jpg>

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/08 23:56

Schema Russian amending the LPT pin 8/11 so that anything http://www.avi-plus.com/images/fbfiles/files/EJTAG_tt_2.pdf <http://www.avi-plus.com/images/fbfiles/images/Usb.jpg>

Structurally, combined with the JTAG programmer (SPI Saketa SPI).

Working in EPP mode, this version of JTAG adapter provides speeds of 2-4 more than the usual scheme of NS244.

Environment:

Connecting to the JTAG port, run the program CPLD_EJTAG_TT, connect the power from USB JTAG. After connecting the power supply is usually the LPT port is in the SSP and the standby LED green card "Act" is off. Press the "Connect", "act" should be lit. If you click "Connect" indicator "lights ACT 'and then leave after a few seconds (do not change the port mode EPP), you must:

1. Try changing the mode of LPT port in BIOS to EPP 1.9

2. Dopyat ohm resistor between 68-100 feet 13 LPT connector and the general conclusion of feeding (18-25 contacts LPT), as shown below

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/09 00:11

Programer SPI :P http://www.avi-plus.com/images/fbfiles/files/SPI_TT_CPLD.rar

Re:Sti5517 flash dump

Posted by Onsitbin - 2010/02/09 02:14

Manual Ejtagg_TT http://www.avi-plus.com/images/fbfiles/files/Manual_Ejtag_tt_pdf.rar

Re:Sti5517 flash dump

Posted by YLG80 - 2010/02/09 16:41

It's interesting to note that EJTAG developers have decided to upload the DCU3 trap routine into internal memory (0x80000400) so that they don't have to setup the external RAM.

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/09 22:00

The sti5105 jtag was for a 4meg flash.

It was 1000 blocks of 4k each.

It would be tedious making an ejflash.ini for that.

nyet

Posted by slugworth - 2010/02/10 01:29

It won't work with a simple jtag, the program crashes.
Probably looking for the missing atmel interface.
Strike 2 is the fact it will only do up to 2meg flashes,
my sti5105 receivers have 4meg flashes.

ejset.ini

Posted by slugworth - 2010/02/10 02:07

If you look at the ejset.ini you will see the program was linked to a particular pc. Sounds like you have to pay\$\$\$ to get a working version.

Re:Sti5517 flash dump

Posted by sergiuss - 2010/02/15 10:18

:)

<http://s39.radikal.ru/i086/1002/79/e29946bf57ba.jpg>

My EJTAG_TT is program of module type.
Flash module possible to flashing up to 16mb flash (tested on 8mb Intel 28F640, more 8mb i not have for test).
In ST20 core DCU2/3 flashing/reading speed 20-25kbyte/sec.

Re:Sti5517 flash dump

Posted by romeok01 - 2010/02/15 10:44

Sergius very sorry for the upload EJTAG CPLD software in rapidshare.com
I have ban in tele-sat.ru for upload EJTAG CPLD software in rapidshare.com.
Many people are interested in handling processors DCU3.
Sergius whether it could add support to the program DCU3 procesors EJTAG Tiny Tools?
Very many people would be happy if they would be able to read and write flash in processor DCU3 (STI5517. ..)

free dcu3 jtag

Posted by slugworth - 2010/02/15 15:54

The biggest gains in sat hacking have been made right after programs were released free to the public. By the time a free dcu3 core1/2 program has been made public those processors will be obsolete.
The sti5516/17 has been around since the 1990's and is already an antique.
I have no urge to buy a jtag device/program if I am only going to use it once.

Re:free dcu3 jtag

Posted by Boxy - 2010/02/28 02:38

aha !

It seems the ST DCU3 unit is lockable on most of the 5514/16/17 devices (and probably others as well). From what I've been told the unit can either be locked permanently or put into a mode where it requires an unlock key (which seems to be customer definable).

When locked, the DCU unit will ignore virtually everything except the unlock command. The TDO pin will tend to stay in its 3-state hi impedance state whenever the DCU should be outputting data. This behaviour is pretty much what I've been seeing on my test board :(

DCU lock doesn't interfere with the jtag ID command.

Looks like the only way to jtag these boards might be to replace the processor with an unlocked chip. Probably not really very practical for the majority of people.

Re:Sti5517 flash dump

Posted by slugworth - 2010/02/28 04:14

I was always able to get full flash dumps from my sti5516 based receivers using jkeys. The pvr2flash files were for fixing the pace3100 receiver, which was sti5514 based. If those old processors were locked, it must have just been a fad that didn't catch on. Later more modern processors just don't have jtag spots to thwart pirates.

Re:Sti5517 flash dump

Posted by Boxy - 2010/03/03 20:22

Seems there is an extra set of commands to the DCU.

1. Permanent DCU external connection disable
2. DCU lock
3. DCU unlock

Looks like nothing particularly fancy but once the DCU has been locked with a key then it can only be opened with that same key. The ST specs say that all processors with DCU3 or later debug units have this capability.

Must admit it is strange that some boxes seem to implement this system whilst some don't, even from the same manufacturer. I've even seen a Pace pvr 3100 that appears locked whilst another one reads no problem (with exactly the same jtag hardware). It seems quite random !

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/03/03 21:04

Hi guys.

Do you know what type of key can be used, @Boxy?

I also think that TDO doesn't always stay hi-Z after cpulD. It actually burps out something...

Best regards.

Re:Sti5517 flash dump

Posted by Boxy - 2010/03/03 21:14

9u4rk wrote:
Hi guys.

Do you know what type of key can be used, @Boxy?
I also think that TDO doesn't always stay hi-Z after cpULD. It actually burps out something...

Best regards.

I think its an 8 byte key. I'd guess it will just be 8 bytes that get stuck in a set of non-volatile registers when you program the lock key. When you try to unlock, the key will be compared to the lock key previously entered.

I have no idea what the actual DCU commands are for setting these various modes. ST generic equipment neither mentions or uses such things. I think this is something that was requested of ST by various customers. If you know the command I would be a little careful as there may well be a 5-try lockout on the code.

The TDO output seems to be selectively open circuit. Various things like Jtag Id still work perfectly well and even certain DCU commands may work ok

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/03/03 21:43

Hi guys.

Unfortunately, I don't know the DCU command... :(
Well, we're being shut out! :angry:

Best regards.

=====

Re:Sti5517 flash dump

Posted by alarm - 2010/03/13 23:57

9u4rk wrote:
Hi guys.

Unfortunately, I don't know the DCU command... :(
Well, we're being shut out! :angry:

Best regards.

.....

=====

Re:Sti5517 flash dump

Posted by alarm - 2010/03/14 00:01

.....

=====

Re:Sti5517 flash dump

Posted by dvbuser - 2010/03/25 06:28

Hi 9u4rk,

Any progress in this Front? Did you have success dumping the flash?

Best regards

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/03/26 20:54

Hi guys.

Unfortunately, nothing at all... :(

Best regards.

=====

Re:Sti5517 flash dump

Posted by pif - 2010/05/18 17:27

Hello.. people, i like to thanks to evreybody on this forum for this wonderfull thread wich helping me to see many thinks...

About my first jtaging experience, i try to dumping a STi5107, 10 pinout, and after many research i am preety sure the connection is the same like STi5517, but the definiton file for 5107 is missing me!

Hop i'll fiind the needed help here...

Great Day

=====

Rar Repair Tool 4.0

Posted by jomyjk7 - 2010/07/08 06:53

Tired of continuous searching? Here's what you are looking for - Rar Repair Tool 4.0

=====

Re:Rar Repair Tool 4.0

Posted by admin - 2010/08/10 10:10

It seems that they continue to work on the DCU3 cpu's on that site

<http://forum.tele-sat.ru/showthread.php?t=3570>

But you need at least 5 posts to be able to download the utilities.

Rgds.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/11 03:13

I could never even register there,so forget that one.

=====

anti-jtag

Posted by slugworth - 2010/08/11 03:16

I have seen examples of sti5518 based firmware that had anti-jtag code to disable the jtag port.So it may be possible that other processor firmware has the same thing.That would also explain the serious lack of dcu3 jtag programs.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/08/11 12:31

Hi guys.

It's been quite a while since I last tried anything on the 5517. Sort of given up because, as far as I could understand it and in my particular case, looks like after the initial data exchange, the processor waits for a code to be inputted to proceed any further. Maybe brute-force would be the next step but, unfortunately, I have no time to carry on testing it...

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/11 18:09

The sti5517 toolset has a flashburner program to compile,so if people can't do that and burn the flash there must be something in the firmware preventing it.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/11 18:12

I assume you have to prevent the receiver from booting into the firmware, similar to the BFR on a sti5518 processor.If the receiver boots all the way the jtag port is probably then disabled.The sti5517 was supposed to have enhanced security to prevent pirating.

=====

Re:Sti5517 flash dump

Posted by Boxy - 2010/08/13 00:30

The enhanced security is basically a a command and client PIN number. Unless you know the correct PIN then you cannot initialise the DCU unit beyond very basic jtag functions.

Unfortunately, there's also a lockout on the PIN. Get it wrong 5 times and the chip effectively locks out further attempts permanently. There is probably a manufacturer reset code but this is unknown

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/13 04:13

Strange,since the sti5517 toolset never mentions it.

SMI=8MB

#####

Copyright (c) STMicroelectronics

##

5517FTACI UNIFIED MEMORY Board configuration for STBURNER

##

##=====

8K of internal SRAM starting at 0x80000000 :

0x140 is committed for System use

```

## 0x1EC0 is uncommitted (can be used for on-chip data, stack or
## time critical code)
##
## 08MB of SMI SDRAM starting at 0xC0000000
## 08MB of FLASH starting at 0x7FE00000
##
#####

## very important !! This file is provided with the Toolset it includes chip command etc...
include "alliref_clk.cfg"
include "asus_clk.cfg"

##Useful Variables
K=1024
M=(1024 * 1024)

## Shared Memory address & size
SMI_BASE      = 0xC0000000
SMI_SIZE      = (7*M)

AVMEM_SMI_SIZE = (1*M)

AVMEM_SMI_BASE = (SMI_BASE)
SMI_CACHED_BASE = (AVMEM_SMI_BASE + AVMEM_SMI_SIZE)
SMI_CACHED_SIZE = (SMI_SIZE - AVMEM_SMI_SIZE)

## External Memory address & size
##EXTMEM_BASE      = 0x40000000
##EXTMEM_SIZE      = (16 * M) ## original is 32

## Address & size of Debug Traphandler area (place at end of External Memory)
TH_SIZE          = 0x400
TH_BASE          = (SMI_BASE + SMI_SIZE - TH_SIZE)

TRACE_BUFFER_SIZE = (64 * K)
TRACE_BUFFER_BASE = (SMI_BASE + SMI_SIZE - TH_SIZE - TRACE_BUFFER_SIZE)

## Addresses & sizes of cached & non-cached areas of External Memory.
## The area defined by NCACHE_BASE and NCACHE_SIZE will contain the
## 'Non-cached' memory partition. The size of this area may be reduced if
## required (NB subject to hardware limitations!)
## IMPORTANT: These definitions reflect the constants of the same
## name in mb361.h. If one of these files is modified then the
## other must be manually updated accordingly. */

##NCACHE_SIZE      = (2*M)
## Louie: CBR1300
NCACHE_SIZE        = (512 * K)

NCACHE_BASE        = SMI_CACHED_BASE
CACHED_BASE        = (NCACHE_BASE + NCACHE_SIZE)
CACHED_SIZE        = (SMI_SIZE - NCACHE_SIZE - TH_SIZE - TRACE_BUFFER_SIZE)

proc Mem5516Space progSMI BootFromFlash useAsusClk{

    if ($# != 0) { progSMI = $1 }
    if ($# == 2) { BootFromFlash = $2 ; useAsusClk = 0}
    if ($# >= 3) { BootFromFlash = $2 ; useAsusClk = $3}

## This procedure calls proc STi5516MB361_noexternal in dcu_mb361.cfg
## which does the "chip STi5516" command (supports DCU3)
    STi5516MB361_noexternal (1) (progSMI)

## Call clocks configuration procedure (in clks_5516.cfg)
    if(useAsusClk == 1) {

```

```

    asus_clock_gen
} else {
    clock_gen
}

## define memory areas
memory NONCACHED (NCACHE_BASE) (NCACHE_SIZE) RAM
memory iEXTERNAL (CACHED_BASE) (CACHED_SIZE) RAM
memory mytracebuffer (TRACE_BUFFER_BASE) (TRACE_BUFFER_SIZE) RAM
memory TRAPHANDLER (TH_BASE) (TH_SIZE) DEBUG

## memory STEM0 0x50000000 (32*M) DEVICE
## memory STEM1 0x60000000 (32*M) DEVICE
## memory AT_DVB 0x70000000 (240*M) DEVICE

## FLASH1 is currently undefined as this causes problems
## when booting from FLASH. By default sections are placed
## in the first rom segment when building a ROM image.
## If the code is placed in FLASH1 then it cannot run
## because the bank sizes need to be setup before this
## section can be accessed.
memory FLASH0 0x7FE00000 (2*M) ROM
memory SDRAM 0xC0000000 (8*M) RAM

##set up code placement sections
if (BootFromFlash == 1) {
    place iEXTERNAL
    place iEXTERNAL
    place def_code iEXTERNAL ## To copy def_code to SDRAM and execute from there ##FLASH0##
    place def_data iEXTERNAL
    place def_bss iEXTERNAL
    place def_const iEXTERNAL

    place os20_th_code iEXTERNAL
    place os20_task_queue INTERNAL
    place os20_th_data INTERNAL
    place os20_root_tdesc INTERNAL
    place os20_int_complex_text iEXTERNAL
    place os20_int_moderate_text iEXTERNAL
    place os20_int_simple_text iEXTERNAL

} else {
    place iEXTERNAL
    place iEXTERNAL
    place def_code iEXTERNAL
    place def_data iEXTERNAL
    place def_bss iEXTERNAL
    place def_const iEXTERNAL

    place os20_th_code iEXTERNAL
    place os20_task_queue INTERNAL
    place os20_th_data INTERNAL
    place os20_root_tdesc INTERNAL
    place os20_int_complex_text iEXTERNAL
    place os20_int_moderate_text iEXTERNAL
    place os20_int_simple_text iEXTERNAL

}

## Section for partitions in internal (on-chip) memory.
###place internal_section INTERNAL
###place internal_section_noinit INTERNAL -noinit

## Section for partitions in general external (off-chip) memory.
###place system_section EXTERNAL

```

```

###place system_section_noinit    EXTERNAL -noinit

## Section for non-cached partitions.
###place ncache_section          NONCACHED -noinit

PlaceDebugTrapHandler            iEXTERNAL

## divide the stack and heap
stack                             iEXTERNAL (128*K)
heap                               iEXTERNAL (1*M)

define NcachePartitionBase "NCACHE_BASE"
define NcachePartitionSize "NCACHE_SIZE"
define InternalPartitionBase "(addressof INTERNAL) + (sizeused INTERNAL)"
define InternalPartitionSize "(sizeof INTERNAL) - (sizeused INTERNAL)"
define SystemPartitionBase "(addressof iEXTERNAL) + (sizeused iEXTERNAL)"
define SystemPartitionSize "(sizeof iEXTERNAL) - (sizeused iEXTERNAL)"
define CacheBaseAddress "CACHED_BASE"
define CacheSize "CACHED_SIZE"
define AVMEM_BASE_ADDRESS "AVMEM_SMI_BASE"
###define AVMEM_SMI_BASE "AVMEM_SMI_BASE"
define AVMEM_SMI_SIZE "AVMEM_SMI_SIZE"

## bootdata location changes if FLASH hex image
if (BootFromFlash == 1) {
    bootdata                FLASH0
} else {
    bootdata                iEXTERNAL
}

}

#####
## procedure called during link time
proc board_init {
    write Setup5516
    reset
    Mem5516Space (1) (0)
    ST20C2MemoryInit  ## procedure written by MCDT, replaces c2MemoryInit, reserves area 0x80000000 to 0x80000040
}

proc board_init_hex {
    write Setup5516
    reset
    Mem5516Space (1) (1)
    ST20C2MemoryInit  ## procedure written by MCDT, replaces c2MemoryInit, reserves area 0x80000000 to 0x80000040
}

#####
## procedure called during run time
proc board_runtime_init {
    board_init
    EMIpokes5516      ## from mb361_emi.cfg
    sti5516ConfigureSDRAM  ## from sti5516sd.cfg for SMI
}

proc asus_runtime_init {
    write Setup AsusBoard
    reset
    Mem5516Space (0) (0) (1)
    ST20C2MemoryInit  ## procedure written by MCDT, replaces c2MemoryInit, reserves area 0x80000000 to 0x80000040
    EMIpokes5516      ## from mb361_emi.cfg
    sti5516ConfigureSDRAM  ## from sti5516sd.cfg for SMI
}

```

```

}

proc board_runtime_init_nor {
  write Setup5516
  reset
  STi5516MB361_noexternal (1) (0)
  memory NONCACHED (NCACHE_BASE) (NCACHE_SIZE) RAM
  memory EXTERNAL (CACHED_BASE) (CACHED_SIZE) RAM
  memory mytracebuffer (TRACE_BUFFER_BASE) (TRACE_BUFFER_SIZE) RAM
  memory TRAPHANDLER (TH_BASE) (TH_SIZE) DEBUG
  memory FLASH0 0x7FC00000 (4*M) ROM
  memory SDRAM 0xC0000000 (8*M) RAM

  ST20C2MemoryInit
  EMIpokes5516 ## from mb361_emi.cfg
  informs -enable
  program -new flash.dbg
}

```

```

#####
##                END of FILE                ##
#####

```

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/08/14 18:16

Hi guys.

You're right @slugworth, there's no such mention on that document and that might be the reason why we can find some 5517's configurations where JTag access is possible and others, is not (if I remember well...). Also, I remember reading a not recent European Patent Application having ST as the applicant, that dealt precisely with this issue. This security feature introduced a "password" verification before any BFL (boot from link) could be obtained. The number of possible attempts before the device locks permanently any further access was not specified, but one has to admit that it wouldn't be difficult to implement as well.
 Good to see this topic still "moving"...

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/14 18:46

The sti5517 toolset wasn't one that was freely (publicly) available. You had to sign an agreement with stmicro to get it. There were 2 versions, one with dvb/dss support and one with only dvb support. So I find it strange that it never mentions any security features. Although it covers a few processors-5514,5516,5517 so it may not go into detail on the 5517. The previous code I posted actually only mentions the 5516 and the mb361.
 I regret not having a sti5517 based receiver with a jtag port.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/08/14 18:59

Hi guys.

Didn't know there were 2 versions...

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/15 23:04

this is from the relnotes.pdf that comes with the toolset.

Distribution

The 5517ref Production is available in the following formats:

- WinZip archive, for PC users.
5517ref-1.0.0.zip DVB & DIRECTV WinZip file
5517ref-1.0.0-DVB.zip DVB-only WinZip file
- Compressed TAR Archive for Unix users.
5517ref-1.0.0.tar.Z DVB & DIRECTV Unix archive
5517ref-1.0.0-DVB.tar.Z DVB-only Unix archive

I dare you to find them tho

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/08/16 01:03

Hi guys.

C'mon @slugworth, I never wanted to disbelief you. It was never my intention...

Let it be clear that I believed you when you said that there were 2 versions for the STi5517 toolset, one public and another one less so.

When I said that looked to me that the 5517 was waiting for a password, was what I find best to explain its behaviour but, of course, I might be wrong. So far and as far as I'm aware, none of us knows what's happening when we try the BFL...

Another thing: - I haven't even been able to find the public one so how can I find the less public one...? :blush:

Best regards.

=====

Re:Sti5517 flash dump

Posted by slugworth - 2010/08/16 01:59

I didn't mean to insult,I was just implying that you or anyone will have a hard time finding it.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/08/17 21:07

Hi guys.

No worries @slugworth, no insult taken. :)

Best regards.

=====

Re:Sti5517 flash dump

Posted by Boxy - 2010/08/25 20:06

slugworth wrote:

Strange,since the sti5517 toolset never mentions it.

Very few security matters are mentioned in the toolset unless its directly relevent to a particular example or task they want to outline. There are seperate security bulletins for those that need to know about such things.

One of the bulletins outlines the procedure you need to go through to request a batch of processors with the secure jtag feature enabled. When you get the secured versions they basically have a passcode masked into some OTP Rom and some extra jtag commands enabled to handle "logging" in to the DCU3 unit. before you log in you you get very little from the DCU3, just a few responses to some basic Jtag commands. Every other command will give you nothing but an apparent open-circuit jtag output.

The security is actually present on all of the later STii55* processors but is de-activated by default. For security active processors you have to request the feature when you order a batch. ST will then either allocate a passcode or use your already allocated passcode.

Security feature options tend to be only open to customers who purchase large quantities of the processor in single batches (>5000 I think it is) and who have signed all the relevant non disclosure agreements (very different than the agreements they use for the toolsets). If you dont know such a customer (or a friendly rep) then you'll never get to know about the options.

=====

Re:Sti5517 flash dump

Posted by 9u4rk - 2010/08/25 20:25

Hi guys.

Your words are in complete accordance from what I could understand out of that european patent I mentioned before, @Boxy.

Best regards.

=====