EEVblog Electronics Community Forum

A Free & Open Forum For Electronics Enthusiasts & Professionals

Hello volvo_nut_v70
Show unread posts since last visit.
Show new replies to your posts.
October 27, 2021, 02:55:35 pm

This topic Search

News:
No news is good news. Be excellent to each other.

« previous next »

Pages: 1 2 3 4 5 6 ... 13 [All] Go Down REPLY UNNOTIFY MARK UNREAD SEND THIS TOPIC PRINT SEARCH

Author Topic: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B (Read 23224

volvo_nut_v70 and 0 Guests are viewing this topic.

analogRF
Frequent Contributor
Posts: 809
Country:

Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **on:** October 21, 2019, 02:27:26 pm »

Hi
I was wondering if anyone ever hacked these ESA spectrum analyzers to enable options?

some options like 1DR and 1DS (or even 1D5 for S/N > 4421) can be enabled by license key only

https://www.keysight.com/main/editorial.jspx?cc=US&lc=eng&ckey=277453&nid=-11143.0.00&id=277453

Report to moderator Logged

mbielman
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #1 on:** November 08, 2019, 12:41:59 am »

I have the same question! Specifically I want to enable the RF Preamp option. (the hardware should be there) Wondering if I can set a bit in the EEprom on the processor card. OR maybe figure out the key(s) based on the serial number.

Anyone?

Mark B

Report to moderator Logged

analogRF

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote

Frequent Contributor

Posts: 809
Country:

« **Reply #2 on:** November 08, 2019, 02:45:15 am »

I have heard that these analyzers have been cracked but people who know how it's done, won't disclose anything

Report to moderator Logged

mbielman

Contributor

Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #3 on:** November 08, 2019, 03:52:42 am »

I have an idea but it would be tedious and slightly dangerous...

Pull the EEPROM (processor board - an assumption on my part) from a unit that has some options enabled, and read that.
Put it back, disable an option or two, remove it again and reread, then look for changes.

Ug!

Report to moderator Logged

analogRF

Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #4 on:** November 11, 2019, 02:20:05 pm »

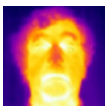
disabling the option in the menus does not remove it from the EEPROM

I am pretty sure someone has found a way to enable the options but it is not shared....

Report to moderator Logged

PA0PBZ

Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #5 on:** November 11, 2019, 02:51:49 pm »

If it's the same as the N1996a CSA and the E7495 it uses FlexLM, I'm the one to blame for the "enhancement" and I have no problem to have a look at these machines as they are discontinued anyway. Does anyone have root access to these machines already?

Report to moderator Logged

Keyboard error: Press F1 to continue.

analogRF

Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #6 on:** November 11, 2019, 03:04:43 pm »

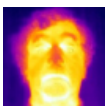
> **Quote from: PA0PBZ on November 11, 2019, 02:51:49 pm**
>
> If it's the same as the N1996a CSA and the E7495 it uses FlexLM, I'm the one to blame for the "enhancement" and I have no problem to have a look at these machines as they are discontinued anyway. Does anyone have root access to these machines already?

that would be awesome. unfortunately I don't have root access . I think N1996A is a much newer machine than ESA series...but of course they might be using the same os

Report to moderator Logged

PA0PBZ

Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #7 on:** November 11, 2019, 03:09:57 pm »

Can you see what format the license code should be? That would probably show if it is FlexLM or something else.

I just downloaded the firmware upgrade but it is 9 discs And the other version for older OS does not run on my PC.
-to be continued-

Report to moderator Logged

Keyboard error: Press F1 to continue.

analogRF

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

Frequent Contributor

Posts: 809
Country:

« **Reply #8 on:** November 11, 2019, 03:16:45 pm »

actually I personally do not have one of these analyzers but have been hunting for one for quite some time. if there is a way to enable some non-hardware options then it would be awesome...I have worked with them though...

maybe this page will help?

https://www.keysight.com/main/editorial.jspx?cc=US&lc=eng&ckey=1000004808:epsg:faq&nid=-35489.384884&id=1000004808:epsg:faq

Report to moderator Logged

Miek

Contributor

Posts: 43
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #9 on:** November 11, 2019, 03:23:24 pm »

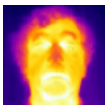
I think you may be able to just concatenate the five ESAFW files, though I'm not completely sure - there might be a header on each.

There are references in the source to FlexLM, and an RTOS named pSOS.

Report to moderator Logged

PA0PBZ

Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #10 on:** November 11, 2019, 05:54:35 pm »

So it runs on some kind of *nix, it is FlexLM and the license file is here: /usr/local/flexlm/licenses/license.dat.
The bad news is that the bytes that have to be patched in the other instruments are not to be found in the ESAFW file.

So, is there any way to communicate with the ESA, is there a prompt on a serial port? I don't think it has ethernet..
~~Is there a harddisk inside that is readable?~~ [Edit] No, it's flash.

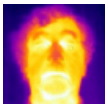
« Last Edit: November 11, 2019, 06:30:34 pm by PA0PBZ »

Report to moderator Logged

Keyboard error: Press F1 to continue.

PA0PBZ

Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #11 on:** November 11, 2019, 06:46:34 pm »

Processor is Motorola Coldfire:

[attachimg=1]

```
jsr     (a3)
move.l  d0,(sp)
jsr     (a2)
adda.w  #$24,sp ; '$'
move.l  d0,(sp)
pea     aDspbootrom     ; "DspBootRom"
pea     (unk_E098).l
bsr.l   sub_3674
adda.w  #$24,sp ; '$'
move.l  #$1E118,(sp)
pea     (unk_3).w
clr.l   -(sp)
clr.l   -(sp)
move.l  #$493E7,-(sp)
pea     (unk_C).w
jsr     (a3)
move.l  d0,(sp)
lea     (unk_60CC).l,a2
jsr     (a2)
addq.w  #4,sp
move.l  d0,(sp)
move.l  #$18E70,-(sp)
pea     (unk_C).w
jsr     (a3)
move.l  d0,(sp)
jsr     (a2)
addq.w  #4,sp
move.l  d0,(sp)
pea     (off_8).w
jsr     (a3)
move.l  d0,(sp)
bsr.l   sub_6240
addq.w  #8,sp
addq.w  #4,sp
move.l  d0,(sp)
move.l  #$493F3,-(sp)
```

E4404B.JPG (45.16 kB, 365x542 - viewed 1917 times.)

Report to moderator Logged

Keyboard error: Press F1 to continue.

mbielman
Contributor
Posts: 24
Country:

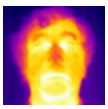
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #12 on:** November 11, 2019, 08:59:44 pm »

Not sure what you are trying to convey here. The ESA instruments use the MC68LC040 (integer only version) and as far as I know do not have a "traditional" OS at all, unlike the newer units.

If there is a way to interrogate the system, I would love to know how!

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #13 on:** November 11, 2019, 09:17:43 pm »

I'm trying to find a way into the ESA to be able to patch the FlexLM part. It looks like the code disassembles fine as a Coldfire processor but you could be right that it is a 68LC040. It looks like it's not that different and it disassembles fine. The method I used to get around the FlexLM stuff in the other instruments is always returning "ok" on an entered license but you have to patch the FlexLM daemon. If you can't get to the file that is going to be difficult so I'm looking at the install.o file to see how it works and if there is a way to install a patched file, that's basically it

Report to moderator Logged

Keyboard error: Press F1 to continue.

mbielman
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #14 on:** November 11, 2019, 09:57:26 pm »

Yeah, not much differs I think between those processors, at least basic op codes. Coldfire is newer than the old MOT 680xx.
As mentioned, don't think these run HP-UX, Windows or any such OS. So no idea if there is anything resembling a file system.

Although it has A: and C: drives (floppy and flash) so who knows! If it's there, you do not see it when the system boots.

Report to moderator Logged

Scopetechniques
Contributor
Posts: 33
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #15 on:** May 20, 2020, 09:25:48 pm »

No, the preamp option is not just software. It actually does have a hardware preamp after the input that can be turned on and off.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

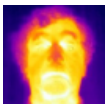
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #16 on:** May 20, 2020, 09:51:05 pm »

> **Quote from: PA0PBZ on November 11, 2019, 09:17:43 pm**
>
> The method I used to get around the FlexLM stuff in the other instruments is always returning "ok" on an entered license but you have to patch the FlexLM daemon. If you can't get to the file that is going to be difficult so I'm looking at the install.o file to see how it works and if there is a way to install a patched file, that's basically it

Have you succeeded? Do you have JTAG access?

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #17 on:** May 21, 2020, 08:01:51 am »

> **Quote from: tv84 on May 20, 2020, 09:51:05 pm**
>
> Have you succeeded? Do you have JTAG access?

I gave up looking at the install file (can't remember why) and I don't have the hardware myself so the motivation is low.

Report to moderator Logged

Keyboard error: Press F1 to continue.

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #18 on:** June 29, 2020, 02:36:22 am »

My turn to chime in. I just got ahold of a broken E4407B from Alltest. I will be posting a blog about the repair once it arrives
in the mean time, this is a topic I am also interested in. I'd love to enable any of the license only options I could.

everything I see says this is not linux at all which I think we agree on
I don't think FLExm is involved, they would have had to port it to their proprietary software which seems a waste.

I wonder if you could brute force this over SCPI. you can enter the license that way.
be interesting to get a few options done.

Me first, I have to wait for mine to arrive then figure out what's broke

Does anyone have the actual CLIP for this I could borrow. I have the scanned version and even it the schematics are hard to read
also anyone have a handle they are not using? Ill post in the wanted section but thought I would ask

edit: I need to walk back the statement over FLEXLM. it is part of the code as was pointed out by @Miek and the OS is PSOS as also pointed out
« *Last Edit: August 23, 2020, 01:12:28 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote

« **Reply #19 on:** July 17, 2020, 07:04:58 am »

Does anyone have a Personality Disk from any of the options and/or a license file
I need your hostID also if anyone is willing to share

Report to moderator Logged

Posts: 623
Country:

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #20 on:** August 23, 2020, 03:03:31 pm »

I extracted strings from the E4407B and found some interesting ones
in particular is SCPI Debuger

Code: [Select]

```
Line 7581: 3942204:@(#)LDS Rev:3.10 - Module Incremental (Mar 26 2007); menu system Rev 3.10
Line 7590: 3950528:@(#)LDS Rev:3.10 - Module Incremental (Jul  8 2003); ptp Rev 3.10
Line 7607: 3990652:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); scum Rev 3.10
Line 7613: 3997792:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Math64 Rev 3.10
Line 7614: 4008452:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); cvt (asm source) Rev 3.
Line 7615: 4009139:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); mcat Rev 3.10
Line 7630: 4012400:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); rlock Rev 3.10
Line 7644: 4017028:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Save-Recall Rev 3.10
Line 7646: 4021306:@(#)LDS Rev:3.10 - Module Incremental (Sep 10 1999); OS wrapper for psos Rev
Line 7723: 4051040:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); HIHR Rev 3.10
Line 7737: 4059944:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Null Happening Reporter
Line 7738: 4060052:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Tee Happening Reporter
Line 7740: 4060976:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Stderr Happening Report
Line 7741: 4061100:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Stdio Happening Reporte
Line 7746: 4061988:@(#)LDS Rev:3.10 - Module Incremental (Oct 11 1999); Scpi Debugger Rev 3.10
```

I also extracted all the FlexLM items i could see
one of interest is

/usr/local/flexlm/licenses/license.dat

Code: [Select]

```
4072496:@(#) FLEXlm 6.0d (liblmgr.a), Copyright (C) 1988-1997 Globetrotter Software, Inc.
4072583:FLEXLM_COMM_TRANSPORT
4074343:FLEXLM_INTERVAL_OK
4074373:FLEXLM_USE_FINDER

4076772:FLEXLM_DIAGNOSTICS
4076795:LM_LICENSE_FILE
4076811:%s_LICENSE_FILE
4076830:%s%s%s%s%s
4078034:FLEXLM_DIAGNOSTICS
4078057:FLEXlm checkout error
4078079:license file(s):
4078103:lm_checkout("%s", %s, %d, 0x%x, ..., 0x%x)
4079117:x%s > %s
4079130:%d-%[^-]-%d
4080510:NOMORE
```

Also of interest is

Code: [Select]

```
0:----- System/pSOS Debug commands:-----
1176785:'?' - this help message.
1176815:'j' - drop into breakpoint.
1176848:'^C' - Abort to monitor.
1176877:'^P' - Process status info, and LOTS of it.
1176925:'[dD]' - Print DLP debug information.
1176965:'[bB]' - Big memory hog report.
1176999:'[pP]' - Process ONLY status info.
1177038:'[eE]' - Exchange info.
1177064:'[gG]' - toggle breakpoint exception handlers on/off
1177119:'[tT]' - Time log.
1177140:'[hH]' - History log.
1177164:'[oO]' - Memory segment ownership.
1177201:'[mM]' - Memory segment summary.
```

```
1177236:'[sS]' - Semaphore ownership, etc.
1177273:'[uU]' - maximum process stack Usage
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #21 on:** August 24, 2020, 12:32:02 pm »

Sandra,

Can you extract your /usr/local/flexlm/licenses/license.dat ?

Do you have JTAG access?

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #22 on:** August 26, 2020, 02:47:59 am »

I don't have JTAG access yet.
my SA has no licenses so its' not the best unit to work with.
my plan is to try several things.
the Serial Port to see if any boot info show up and to see if something I saw is correct as it looks like you can dumb memory thru the serial interface or SCPI interface.

JTAG is a boundary scan only interface on the 68040.
I haven't seen any predefined targets for 68040 in OCD

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #23 on:** August 26, 2020, 01:06:33 pm »

A memdump, a boot log, etc. Everything helps.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #24 on:** August 27, 2020, 01:14:59 am »

Hum
I read out the boot rom and did the string search there and found some interesting things in there like a Rom Monitor, GDB, breakpoints, member dump etc... hummmm

Im going to have to get hooked up the J1 Port RS232

Code: [Select]

```
12714:29F400B
12722:29F400T
12730:29F040
12737:29F010
12744:28F200BX-B
12755:28F200BX-T
12766:MT28F400-B
12777:28F400BX-B
12788:28F400BX-T
12799:28F800BX-B
12810:28F800BX-T
12821:28F001BX-B
12832:28F001BX-T
12843:28F008
```

```
12850:28F020A
12858:28F010
12865:28F020
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #25 on:** August 27, 2020, 11:39:59 am »

Say Thanks Reply Quote

For those interested here's the dump of the bootrom

U77-29F010-PLCC32-E4404-80123-0453 HS.7z (33.44 kB - downloaded 102 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: tv84, analogRF

analogRF
Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #26 on:** August 27, 2020, 12:28:55 pm »

Say Thanks Reply Quote

not an expert here but I am not sure if the bootrom is that useful for cracking the options.
you probably need to access a serial console that is somewhere on the cpu board to access the main firmware files that are unpacked in the flash (or is it EEPROM?)
is there a place that you can enter a license key and see what error it generates?

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #27 on:** August 27, 2020, 12:34:59 pm »

Say Thanks Reply Quote

The reason for posting it is there appears to be monitor functions built in that may help get to the data we're after

My unit has no licenses and the licenses are stored in the Flash memory not in the ERPROM according to the security doc out there from Agilent

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

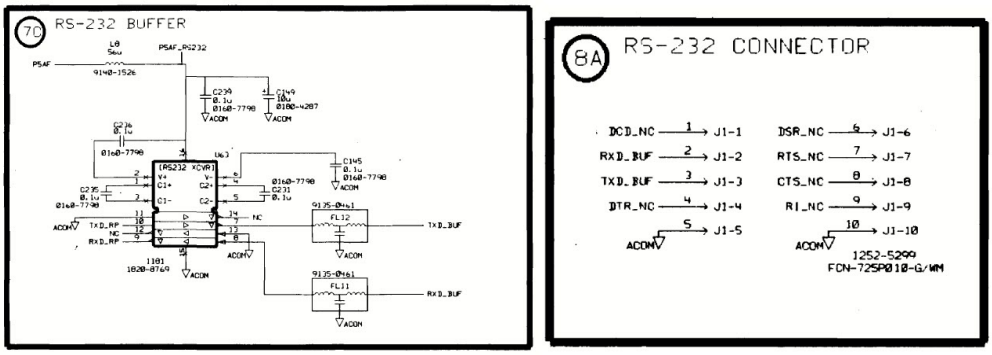
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #28 on:** August 27, 2020, 11:44:31 pm »

Say Thanks Reply Quote

So before trying to attach the J1 connector I figured I better determine if it's RS232 levels or TTL level output

U63 is a MAX232. so RS232 levels

Also J1 is a 2mm 2x5 header. I don't have one so Digikey order (along with stuff for my DSKY EL Display) should be here by Monday I hope.
unless I can rig up something



2020-08-27_19-37-04.jpg (80.96 kB, 1277x459 - viewed 212 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #29 on:** August 28, 2020, 12:57:32 am »

all you need to do is to attach two small grabbers to pin9 and pin10 of the MAX232 chip (TTL level) and you are good to go. Any cheap UART-USB converter will do the job. I prefer my BUSPirate. That's how I have always done this in numerous instruments.

But which RS232 connector is this? Is it the one at the back of instrument? or is it something just on board for debugging?

Because if it is the one at the back of instrument, you won't get any boot log on that or access to the OS

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #30 on:** August 31, 2020, 04:12:44 pm »

Got the connection working. I needed a reboot

this is some of the information I see from it

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 5.00
@(#)LDS Rev: 3.02 - Module Incremental (Sep  9 2003)
@(#)Linked: Sep  9 2003 14:46:44

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #31 on:** September 03, 2020, 12:41:34 am »

The first item needed is a full dump of the memory. a dump of one with licensed options would really help. mine has no licensed options

Posts: 623
Country:

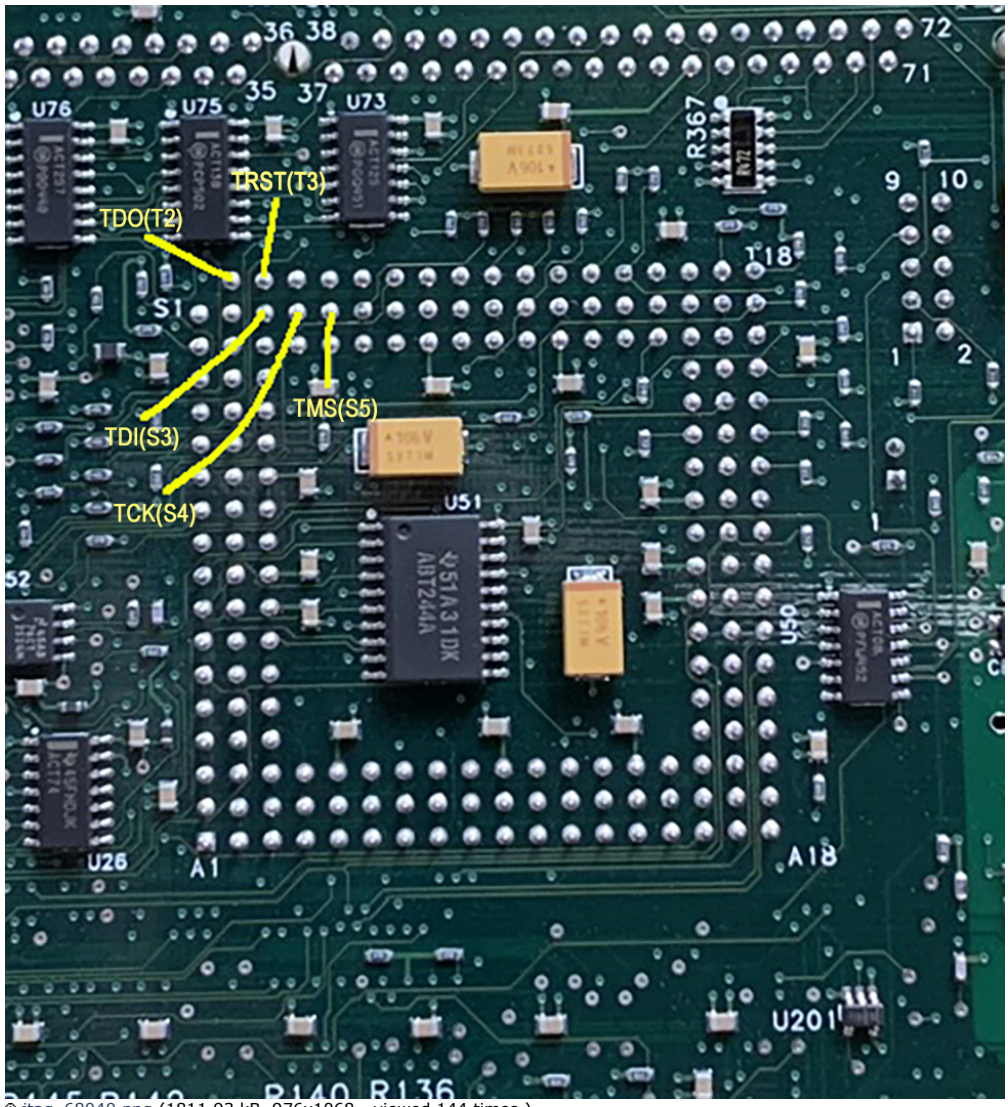
flexlm 6.01 which appears to be in the update file which I extracted strings from has been hacked and there's articles on how to find the different key values.

the part at the moment is how to get that dump, flash and sdram from a running system
i figured out the JTAG pins and where you can pick them up but JTAG is not something I'm good with

if all you have is a boundary scan ability can you get a dump of memory?
[attach=1]

anyone who can help with that and setting up OCD I'll do it on my ESA
I just need the help

the processor is a 68LC040 I believe (its the LC part i'm not 100% sure of off top of the head)



jtag_68040.png (1811.93 kB, 976x1068 - viewed 144 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #32 on:** September 03, 2020, 10:22:20 am »

Say Thanks Reply Quote

Quote from: smgvbest on September 03, 2020, 12:41:34 am

> The first item needed is a full dump of the memory. a dump of one with licensed options would really help. mine has no licensed options
> flexlm 6.01 which appears to be in the update file which I extracted strings from has been hacked and there's articles on how to find the different key values.

the part at the moment is how to get that dump, flash and sdram from a running system

I don't think flexLM is in the update file. It should be already inside the machine. That's why a flash dump would be great.

The FlexLM version should be no problem. Regarding the places where to find the seeds it's not so simple as the several guides don't cover this lang/processor.

Report to moderator Logged

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #33 on:** September 03, 2020, 10:28:48 am »
Say Thanks Reply Quote

Quote from: xymox on September 03, 2020, 05:43:27 am

Ive done jtag in a bunch of things.. Its not normally what is in your pic ? Maybe that is something else ? OR I am just stupid,, I CAN be that.. Normally its a 4 pin header. +5, tx, rx, gnd.. With ther TTL or RS232 voltages. I will look more at the board shortly..

TX,RX,GND is not a JTAG, it's UART . you dont even need the Vcc necessarily.

this thing has a JTAG interface but i dont think it will be of much help. The content of bootrom is not what we need.
you only need the dump of flash memory to access the file system of the main OS, nothing else really.
Another way would be to figure out how to combine the 9 floppy disks to create a single file firmware and then "explore" it

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #34 on:** September 03, 2020, 10:31:32 am »
Say Thanks Reply Quote

Quote from: analogRF on September 03, 2020, 10:28:48 am

Another way would be to figure out how to combine the 9 floppy disks to create a single file firmware and then "explore" it

Where are those 9 disks?

Report to moderator Logged

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #35 on:** September 03, 2020, 10:37:54 am »
Say Thanks Reply Quote

Quote from: tv84 on September 03, 2020, 10:31:32 am

Quote from: analogRF on September 03, 2020, 10:28:48 am

Another way would be to figure out how to combine the 9 floppy disks to create a single file firmware and then "explore" it

Where are those 9 disks?

on keysight website
https://www.keysight.com/main/software.jspx?cc=CA&lc=eng&ckey=1000001085:epsg:sud&nid=-32406.536879915.02&id=1000001085:epsg:sud&cmp

EDIT: i dont have the instrument so I have never gone through the process of making the firmware update. I just know that it creates 9 floppy disks

« Last Edit: September 03, 2020, 10:40:28 am by analogRF »

Report to moderator Logged

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #36 on:** September 03, 2020, 11:59:58 am »
Say Thanks Reply Quote

Posts: 623
Country:

I have combined the 5 disks that make up the ESA Firmware. the other 4 are the power suite I can combine those as well if you want?
There is no guarantee that just combining them will give a correct image.
They may contain loader information that the internal bootrom reads to build the actual firmware that is loaded (just thinking, or over thinking)
This is a full image it's not an upgrade. I had to do a full erase of mines memory to restore it so I can attest everything is on those disks.
I also have the Discs for all the DLPs (personalities) that can be installed.

The reason I provided the boot loader rom is it looks like GDB server is in the bootroom. if you have GDB could you dump memory thur it?
There is also apparently a SCPI Debug interface, maybe there a memory read function in there?

i'll try to attach it here.

If this does not work the other way I could brute force this is I could remove all of the FLASH memory and read them out with the Xgpro (formerly TL866) reader/programmer.
I have a spare processor card I'm willing to experiment on.

ESAFW.zip (1488.79 kB - downloaded 62 times.)

« *Last Edit: September 03, 2020, 12:04:00 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: tv84, analogRF

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #37 on:** September 03, 2020, 12:22:43 pm »

Say Thanks Reply Quote

there is also a series of F000000 to F000003 files that I wonder what they contain...i think they must be combined too.
also there is a bootloader file on the first floppy

have you been able to analyze the single firmware file with tools that are available in linux?

Report to moderator Logged

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #38 on:** September 03, 2020, 12:29:09 pm »

Say Thanks Reply Quote

I think having the actual unpacked firmware image from the flash memory will make it a lot easier and certainly possible to hack this thing
if i am not mistaken there are more than one flash rom, right? so again their contents must be concatenated

EDIT: but then we know that a simple concatenation will give us the whole system
with the firmware installation files, I am not sure about that because each of those 5 files may have a header and when you connect them together you get a broken image of the actual file structure

« *Last Edit: September 03, 2020, 02:47:21 pm by analogRF* »

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #39 on:** September 03, 2020, 01:18:42 pm »

Say Thanks Reply Quote

> **Quote from: analogRF on September 03, 2020, 12:22:43 pm**
>
> there is also a series of F000000 to F000003 files that I wonder what they contain...i think they must be combined too.
> also there is a bootloader file on the first floppy
>
> have you been able to analyze the single firmware file with tools that are available in linux?

When I tried the linux tools they did not recognize the contents

PDISC is the physical Disc Number below whereas the DISC # is the as LABELED Disc for installation

BOOTROM: This looks for a DISK with ESALOADER on it and if so loads and runs it
DISC ESALOADER(PDISC1), This is what's run to install the FIRMWARE.
DISC1-5(PDISC2-6), this is the ESA Firmware Discs (this is the the ESAFW I uploaded)
DISC1-3(PDISC7-9), These contain the ESA Power Suite Software) (the F000000 to F000003 are the Powersuite Image files)

I'll combine and upload the Powersute after work today

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #40 on:** September 03, 2020, 01:24:27 pm »

I'd love to be able to enable all DLP's and License only options
example RF PREAMP is a License only option (hardware is there above certain serial numbers) you only need the 16 digit license key
but DLP for Cable Fault Analyzer requires the Tracking Gen be installed. (i have a TG installed so would like this one)

I'm installing the DLP for Cable Fault Analyzer and grabbing screen caps so you can see the process of installing a DLP

« *Last Edit: September 03, 2020, 01:28:05 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #41 on:** September 03, 2020, 02:41:58 pm »

Quote from: smgvbest on September 03, 2020, 11:59:58 am

> If this does not work the other way I could brute force this is I could remove all of the FLASH memory and read them out with the Xgpro (formerly TL866) reader/programmer.
> I have a spare processor card I'm willing to experiment on.

This seems the best option. How many flash chips are there? Isn't just one?

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #42 on:** September 03, 2020, 05:56:40 pm »

Total of 4
One on cpu board which is main firmware
3 on simm which is where licenses are supposed to be stored

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #43 on:** September 03, 2020, 08:46:24 pm »

Those that want to play in IDA with @smgvbest's ESAFW can use these settings:

Proc: Motorola Coldfire
Load address: 0x04011000

Report to moderator Logged

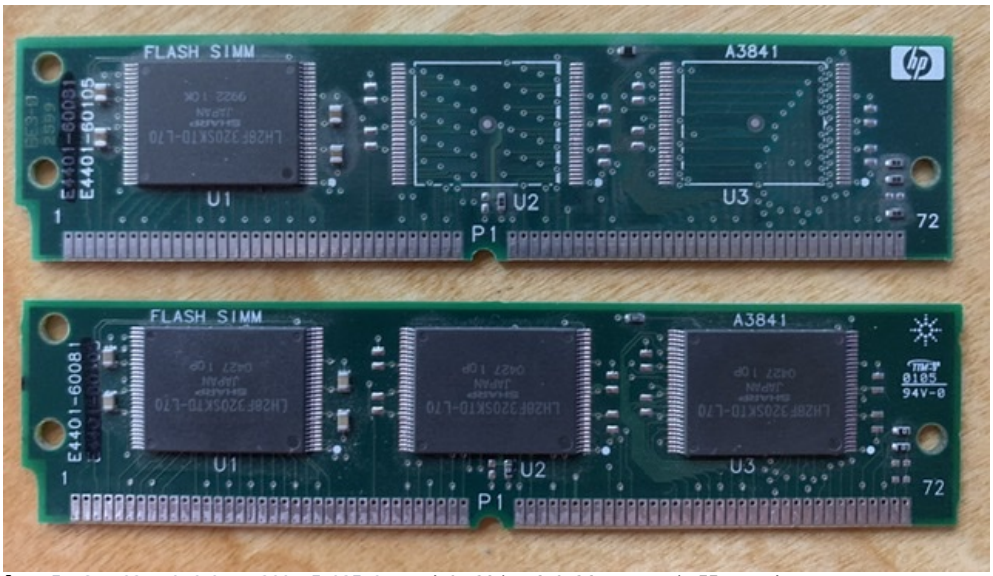
smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #44 on:** September 03, 2020, 08:47:22 pm »

Posts: 623
Country:

Memory module on a memory simm 72 pins old style sdram memory formfactor

It's how the e4407b had its memory expanded



74451FCB-102E-49A0-9BEA-200F15F93540.jpeg (101.28 kB, 640x367 - viewed 155 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: tv84

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #45 on:** September 03, 2020, 08:58:20 pm »

> **Quote from: smgvbest on September 03, 2020, 08:47:22 pm**
>
> Memory module on a memory simm 72 pins old style sdram memory formfactor
>
> It's how the e4407b had its memory expanded

Never had seen one of those expansions!

We don't need a dump from the "license's flashes". The licenses are already visible on the screen.

« *Last Edit: September 03, 2020, 09:01:12 pm by tv84* »

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #46 on:** September 03, 2020, 09:15:37 pm »

> **Quote from: tv84 on September 03, 2020, 08:46:24 pm**
>
> Those that want to play in IDA with @smgvbest's ESAFW can use these settings:
>
> Proc: Motorola Coldfire
> Load address: 0x04011000

Is the Motorla Coldfire same as a M68040?
the Motorola 68LC040 is the actual processor on the board is why I ask

how did you manage to get the load address?

« *Last Edit: September 03, 2020, 09:18:28 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #47 on:** September 03, 2020, 10:54:36 pm »

The static ram is not where licenses are stored. They're in the flash memory so unless you wipe flash you maintain them

Loosing the sram looses the date/time and calibration and other settings like printer setup.
You just do an align all to get it back and reset date/time

« Last Edit: September 04, 2020, 12:35:03 am by smgvbest »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #48 on:** September 04, 2020, 01:41:46 am »

Quote from: xymox on September 03, 2020, 09:46:29 pm

> So are you gals/guys thinking about patching the image and then loading a new image in ? Might be able to add all sorts of stuff that way. Hopefully its not checksummed or anything..
>
> So a personality MUST have a key before running ? So no stripping that requirement from the personality ? The ESA wont run a personality that has no license requirements ?
>
> Just thinking out loud.. And most likely being stupid..

I think what we're after is a keygen more or less.
if we can find all the keys FlexLM uses (I think there 8 total if I understand) then we find out id using the host ID we can generate a valid license we hopefully can generate them all
Yes a personality must also have license , you load the personality (DLP) and license it then its usable the only DLP that's not licensed is the Power Suite

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #49 on:** September 04, 2020, 03:16:18 am »

I don't know that would help
The licenses are to the hostid not the serial number
You could change the serial to match a machine basically. Install the license and it would not work

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #50 on:** September 04, 2020, 09:10:49 am »

Quote from: smgvbest on September 03, 2020, 09:15:37 pm

> how did you manage to get the load address?

Educated trial & error...

I would like to know if there is any way to manually upload a license.dat file to the instrument? (If this is not possible we can't do an universal license file.)

Also, can anyone provide a printscreen of the license input menu?

Edit: Now that you asked...

Quote from: smgvbest on August 31, 2020, 04:12:44 pm

Bootrom Checksum ...
Bootrom DRAM: Testing 69632 bytes at **0x04000000**
Non Destructive SRAM Test ...
Main Firmware DRAM: Testing 33484800 bytes at **0x04011000**
Main FW Checksum ...

« *Last Edit: September 04, 2020, 10:22:01 am by tv84* »

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #51 on:** September 04, 2020, 10:41:51 am »

Say Thanks Reply Quote

After a few more educated googles I arrived here.

So, we're halfway there!

The licenses should have this format:

FEATURE **202** TMOMID01 1.0 permanent uncounted **0123456789AB** HOSTID=**E1234567**

Now, we just need the seeds.

Report to moderator Logged

The following users thanked this post: ps, analogRF

analogRF
Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #52 on:** September 04, 2020, 11:57:20 am »

Say Thanks Reply Quote

Quote from: tv84 on September 03, 2020, 08:46:24 pm

Those that want to play in IDA with @smgvbest's ESAFW can use these settings:

Proc: Motorola Coldfire
Load address: 0x04011000

i have been trying to open this in IDA with above settings but still I either get an error (loading address must belong to RAM or ROM) or it opens as a raw binary. any more hint?

Report to moderator Logged

The following users thanked this post: xymox

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #53 on:** September 04, 2020, 01:22:04 pm »

Say Thanks Reply Quote

Quote from: analogRF on September 04, 2020, 11:57:20 am

i have been trying to open this in IDA with above settings but still I either get an error (loading address must belong to RAM or ROM) or it opens as a raw binary. any more hint?

You put the address also in ROM address.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #54 on:** September 06, 2020, 05:00:45 am »

Say Thanks Reply Quote

I'm attaching the ESALOADER file and the install.o which loads the power suite
I'm not sure but I think one or both of these indicate the files on the discs make me think it may be compressed or partially compressed

ESALOADR is from DISC1 and loads the firmware
UPGRADE.O is from DISC6 which is the last disk of the firmware
install.o is the installer from the Power Suite software
all where zipped to allow upload

edit: fixed this missing install.o file

ESALOADR.zip (247.35 kB - downloaded 56 times.)
UPGRADE.zip (11.13 kB - downloaded 53 times.)

install.zip (27 kB - downloaded 50 times.)

« *Last Edit: September 06, 2020, 05:31:17 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #55 on:** September 06, 2020, 11:28:30 am »

Say Thanks Reply Quote

ESALOADR - Load address: 0x04011000
UPGRADE.O - Load address: 0x0 (after removing a 0x20 size header)
INSTALL.O - Load address: 0x0 (after removing a 0x20 size header)

install.o contains (in the beginning) MD5 hashes (in plain ASCII) of the files that it installs.

« *Last Edit: September 07, 2020, 06:20:48 pm by tv84* »

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #56 on:** September 07, 2020, 05:48:07 pm »

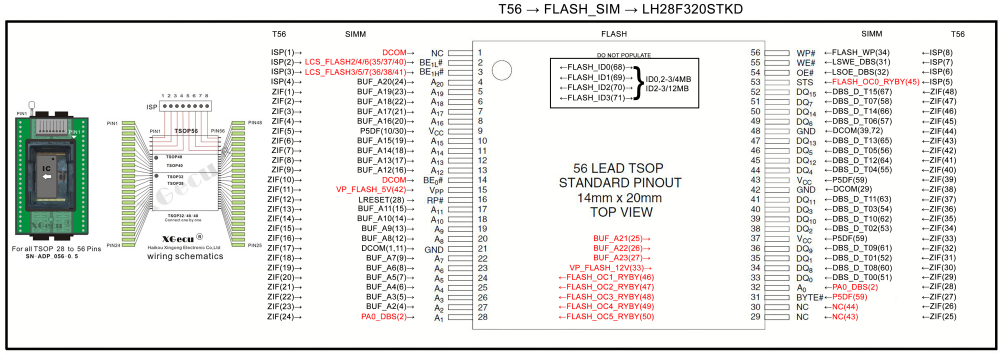
Say Thanks Reply Quote

I'm trying to figure out how to read out the FLASH SIMM without de-soldering the Flash ICs
I've created a map between the LH28F320STKD -> SIMM -> T56 Programmer
There's a few signals that need investigation, shown in RED.

mainly the LCS_FLASH (CS Selects), Program Voltage ,RYBY (why are there 6 of these, 3 makes sense) , PA0 (possible tried low) ,PA1 (should be straight thru), byte# (likely tied high)
I'll have to ohm out the simm to figure out

Ill still have to de-solder U74 from the processor board (no way around that)

has anyone ever use JTAG on a 68040?
I dont' see a def for it in OCD
if all you can do is a boundary scan can you access memory or do you need debug for that?



LH28F320SKTD.png (2367.72 kB, 5044x1900 - viewed 109 times.)

« *Last Edit: September 07, 2020, 06:10:58 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #57 on:** September 07, 2020, 08:15:57 pm »

Say Thanks Reply Quote

Quote from: xymox on September 07, 2020, 08:07:14 pm

"has anyone ever use JTAG on a 68040? "

I have not...

What is that 2x5 J16 ? There is one on every interface card except the GPIB. It happens to have the same number of pins

and 2x5 as a std RS232 header for a typical computer of that era.

ALSO, where can I get a nice complete set of schematics with block diagrams ? The downloadable service manual is missing those.

On the Processor Card that is a STD JTAG Header for the main FPGA, its not connected to the processor.
for the CLIP, http://artekmanuals.com/manuals/hp-manuals/ search for E4400-90310
there are some pages missing.

if anyone has an original CLIP and is willing share (or sell) I'm very interested in getting ahold of it.
PM me off list if you do please

« *Last Edit: September 07, 2020, 08:17:30 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #58 on:** September 07, 2020, 10:42:08 pm »

Say Thanks Reply Quote

I ordered this one off ebay.. Once I get it AND IF ITS COMPLETE,, I will compress and upload for distribution.. Assuming its not just a copy of what is in your link..

https://www.ebay.com/itm/HP-E4401B-Component-Level-Info-Package-Schematics-/390129973036

I have spent hours getting ALL the files related to ESA off Keysight's terribly organized and painful to use web site. I have collected those and organized them far better. This includes manuals, guides, firmware, personalities discs & docs, options, install notes, application notes ESA related, software drivers, software and more.. I intend on organizing it all even better and making a single downloadable file. I Will also include the CL stuff as well once I have it.

One file to rule them all..

« *Last Edit: September 07, 2020, 10:46:43 pm by xymox* »

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #59 on:** September 07, 2020, 10:50:33 pm »

Say Thanks Reply Quote

Yes that's the one.
they are scans of the CLIP but very legible.

I've let them know of missing pages I've found so far. not many 2-3, processor is missing the last page(s) of the BOM but schematics are good
another is missing a schematic page but don't remember which it was

Note the CLIP from Artek can not be distributed

« *Last Edit: September 07, 2020, 10:52:06 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #60 on:** September 07, 2020, 11:00:06 pm »

Say Thanks Reply Quote

Were else was the processor card used ? That Ethernet header and unpopulated parts for it must have been used by something ? I am going to poke around and see what other HP / Agilent devices might have used that same card. I suppose the FPGAs might be loaded totally different tho But maybe it might be possible to load it with ESA firmware and have a Ethernet... Or not.. hahaha.. I am still gonna look around tho..

Report to moderator Logged

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #61 on:** September 07, 2020, 11:15:00 pm »

Say Thanks Reply Quote

I have a Processor Card with Network and there's no way to configure it in the ESA menus.
only the original card had the ethernet parts. it's likely part of their debug system

Report to moderator Logged

Posts: 623
Country:

Sandra
(Yes, I am a Woman :p)

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #62 on:** September 08, 2020, 02:46:08 am »

IS it just me ? Im trying to get all the firmware files and the ones from Keysight for the ESA for win 7/8 produce a SSL error ? https://sa.support.keysight.com/ESA/Firmware/A.14.06.zip?id=2401677

Report to moderator Logged

Miek
Contributor
Posts: 43
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #63 on:** September 08, 2020, 06:20:08 pm »

Yeah, same. "Error code: SSL_ERROR_RX_RECORD_TOO_LONG" almost always means the site is serving plain http on that port (no SSL). Change the link to http and it works:
http://sa.support.keysight.com/ESA/Firmware/A.14.06.zip?id=2401677

Report to moderator Logged

gslick
Frequent Contributor
Posts: 413
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #64 on:** September 08, 2020, 07:23:42 pm »

> **Quote from: xymox on September 07, 2020, 11:00:06 pm**
>
> Were else was the processor card used ? That Ethernet header and unpopulated parts for it must have been used by something ? I am going to poke around and see what other HP / Agilent devices might have used that same card.

There are other instruments which reuse a processor card without using all of the hardware features. For example the 16700 logic analyzers use an E4406 processor card. I was curious about why there is a TI 9914 GPIB controller and 75ALS160 / 75ALS164 bus transceivers on the 16700 processor card but the GPIB connector is unpopulated. Turns out the GPIB connector is populated and used on the E4406A.

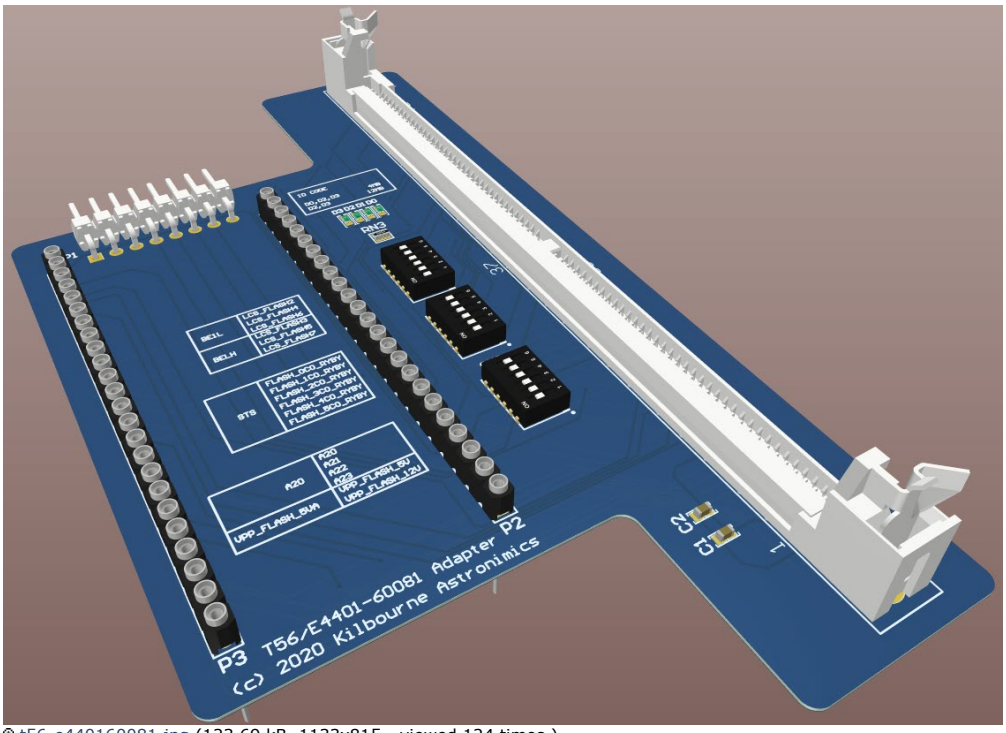
Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #65 on:** September 09, 2020, 03:55:19 am »

Spent a little bit of time making a PCB for the T56 Programmer to work with the FLASH SIMM. nothing fancy, even autorouted, just some switches to let you configure the lines to pick the correct Flash to read out. U1/U2 or U3.

before I send to PCB house I want to verify a few more things



t56-e440160081.jpg (123.69 kB, 1133x815 - viewed 124 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: analogRF

Kean
Supporter

Posts: 1346
Country:
Embedded systems & IT consultant

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #66 on:** September 09, 2020, 04:53:20 am »

Quote from: smgvbest on September 09, 2020, 03:55:19 am

> before I send to PCB house I want to verify a few more things

Maybe fix the spelling mistake on Astronomics

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

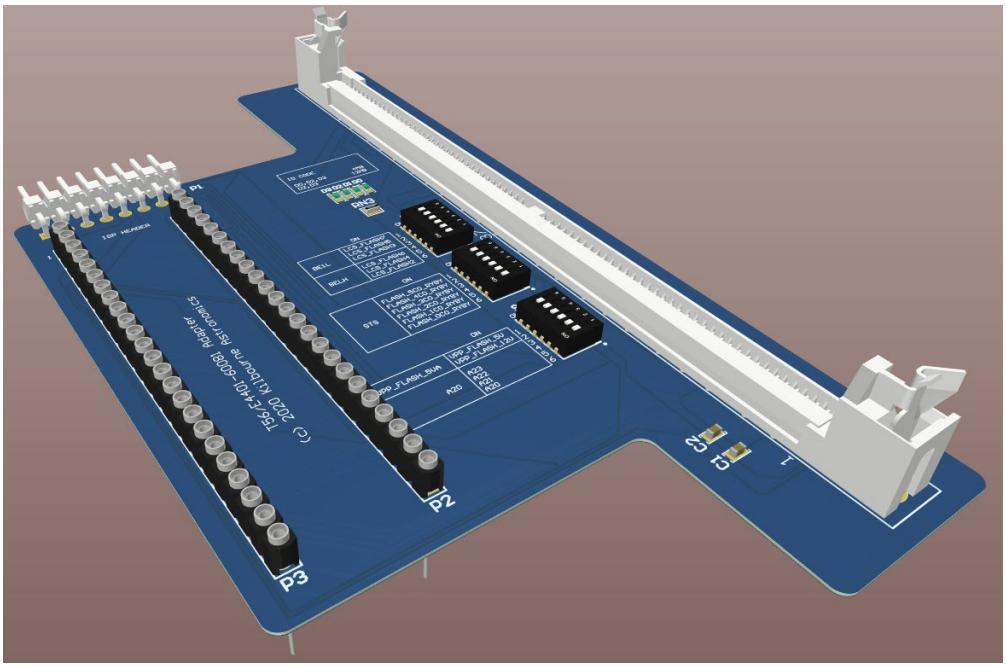
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #67 on:** September 09, 2020, 06:22:39 am »

Quote from: Kean on September 09, 2020, 04:53:20 am

> **Quote from: smgvbest on September 09, 2020, 03:55:19 am**
>
> > before I send to PCB house I want to verify a few more things
>
> Maybe fix the spelling mistake on Astronomics

Yes I caught that and a much bigger issue that I've about fixed. the spacing on the 2 24pin sockets was wrong. it needed to be 600mils not 1060mils
would not have fit the ZIF socket on the programmer.

should be good now, placed order from JCLPCB



t56-e440160081.jpg (111.27 kB, 1172x771 - viewed 112 times.)

« *Last Edit: September 09, 2020, 07:23:14 am by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: Kean, tv84

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #68 on:** September 09, 2020, 10:14:00 am »

Say Thanks Reply Quote

Quote from: smgvbest on September 09, 2020, 03:55:19 am

> Spent a little bit of time making a PCB for the T56 Programmer to work with the FLASH SIMM.
> nothing fancy, even autorouted, just some switches to let you configure the lines to pick the correct Flash to read out.
> U1/U2 or U3.
>
> before I send to PCB house I want to verify a few more things

that's awesome

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #69 on:** September 09, 2020, 03:43:35 pm »

Say Thanks Reply Quote

I injured my back and have been pretty much confined to bed so haven't been able to reflash my SA with a byte change. But you can design things while confined

I'll reflash soon as possible to test that out

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #70 on:** September 09, 2020, 04:05:32 pm »

Say Thanks Reply Quote

Guess what I just found.

This is the monitor program I was after.
to get it i caused an error. the error was planned, getting the monitor program was not

Country:

question will be how to get this when loading normally.

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 3.10
@(#)LDS Rev: 3.02 - Module Incremental (Feb 18 1999)
@(#)Linked: Feb 18 1999 11:46:22

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
    ROM Checksum Failure.  Bad Checksum.  01, 0
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
```

Serial is at 19.2Kb so dumping memory will be slow but may be doable soon (I hope)
and if you notice the menu you can dump and write memory

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: tv84, analogRF

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #71 on:** September 09, 2020, 05:17:16 pm »

Sandra,

Do some dumps of **0x04011000** and beyond just to test and compare with ESAFW.

Later i'll provide some specific addresses.

« *Last Edit: September 09, 2020, 06:12:27 pm by tv84* »

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #72 on:** September 09, 2020, 05:28:47 pm »

I am the owner of the E4407B with AYZ (external mixing) and 1DR (narrow resolution bandwitch) options installed. Also B72 and 1D5. If the memory dump is possible using the monitor program via the J1/RS-232C connector, I can prepare the hardware and do such a dump. Will it be helpful?

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #73 on:** September 09, 2020, 06:28:39 pm »

Quote from: smgvbest on September 09, 2020, 04:05:32 pm

Code: [Select]

```
->dbyte
00000000  00 00 00 00 00 00 ad 34 4e 56 00 00 4e 41 00 00   .......4NV..NA..
->dbyte 1024
00001024  53 49 53 00 6a fa 20 49 72 ff b2 90 67 04 4a 90   SIS.j. Ir...g.J.
```

These are exactly the bytes of bootrom at 0x00 and 0x1024.

Report to moderator Logged

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #74 on:** September 09, 2020, 06:42:21 pm »

Posts: 623
Country:

SO far my Playing around to get a dump off a fully running E4407B has not been successful
biggest issue with a successful load your not in the monitor program where you can dump memory.
I am dumping 0401100 on but it's going to take some time at 19.6Kb

From the System/pSOS menu it says that ^C gets you to the monitor. I've assuming that's CTRL+C and that don't work. get un-recognized char also tried literal ^C didn't recognize the ^. looks like its a single char command so not sure what ^C was to be.

the hmon device command will load from a device into memory but I can't figure out the device names
i do know that hmon alone will try to load from GPIB
i tried hmon GPIB and get un-recognized device

I'm find all the things that don't work. just to find the one that does.
pSOS being so old it's hard to find DOC on as well

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #75 on:** September 09, 2020, 06:50:07 pm »
Say Thanks Reply Quote

Quote from: smgvbest on September 09, 2020, 06:42:21 pm

...
pSOS being so old it's hard to find DOC on as well

I have also Anritsu MS4623B and it use pSOS. I have some DOC's for pSOS.

PSOS_Programmers_reference.zip (3517.09 kB - downloaded 93 times.)
psos_system_call.zip (849.82 kB - downloaded 117 times.)

Report to moderator Logged

The following users thanked this post: analogRF

analogRF
Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #76 on:** September 09, 2020, 06:50:16 pm »
Say Thanks Reply Quote

maybe it just means capital C

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #77 on:** September 09, 2020, 06:51:09 pm »
Say Thanks Reply Quote

Part 2

pSOSystem System Concepts.zip (2482.09 kB - downloaded 84 times.)

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #78 on:** September 09, 2020, 06:52:47 pm »
Say Thanks Reply Quote

Quote from: tv84 on September 09, 2020, 06:28:39 pm

Quote from: smgvbest on September 09, 2020, 04:05:32 pm

Code: [Select]

```
->dbyte
00000000  00 00 00 00 00 00 ad 34 4e 56 00 00 4e 41 00 00   .......4NV..NA..
->dbyte 1024
00001024  53 49 53 00 6a fa 20 49 72 ff b2 90 67 04 4a 90   SIS.j. Ir...g.J.
```

> These are exactly the bytes of bootrom at 0x00 and 0x1024.

Cool, and that would make sense. the boot rom would exist at 0x00000000
if I recall the 1024 bytes on the M68K is the vector table
of course that command dbyte 1024 is dump 0x1024 not dec 1024 :O

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #79 on:** September 09, 2020, 06:52:54 pm »

Be carefull, the address is **0x0401 1000**. Not 0x0040 1100!

For now, just get me this region:

0x048B9200 -> 0x048B9500

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #80 on:** September 09, 2020, 06:53:23 pm »

> **Quote from: analogRF on September 09, 2020, 06:50:16 pm**
>
> maybe it just means capital C

Tried, does not accept it either

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #81 on:** September 09, 2020, 07:03:08 pm »

> **Quote from: tv84 on September 09, 2020, 06:52:54 pm**
>
> Be carefull, the address is **0x0401 1000**. Not 0x0040 1100!
>
> For now, just get me this region:
>
> 0x048B9200 -> 0x048B9500

Here ya go

Code: [Select]

```
**** Mosquito Bootrom ***** 00 00 00 00 00 00 00 00 00 00   ................
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 3.10
@(#)LDS Rev: 3.02 - Module Incremental (Feb 18 1999)
@(#)Linked: Feb 18 1999 11:46:22

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
    ROM Checksum Failure.  Bad Checksum.  01, 0
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #82 on:** September 09, 2020, 09:35:49 pm »

OK, I prepared the hardware to handle the serial port, set up 19200 8n1. After start, E4407B sends information.

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 5.00
@(#)LDS Rev: 3.02 - Module Incremental (Sep  9 2003)
@(#)Linked: Sep  9 2003 14:46:44

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
        End    = 0xa007fa3
```

How do I enter the monitor? Sandra, you wrote about a planned error. How to do it?

I am ready to deliver information from my device with the options installed, please just keep in mind that I am not an experienced hacker
I will also point out that my SA has the A.14.01 firmware installed. Can't install the latest firmware yet, FDD can't read floppy disks reliably. It crashes on 2nd or 3rd disk when trying to update. I have to look for a new FDD.

EDIT

I'm now motivated to solve the FDD problem in my SA. I ordered 2 used SLIM FDD from the local auction site. One type NEC FD3238T and the other Teac FD-05HG. The FDD Teac FD-05HF was originally installed in my E4407B, but I haven't found one. Hope one of them will work well, both have a 26 pin connector. If they work, I will update the firmware to version A.14.06.

« *Last Edit: September 09, 2020, 11:00:07 pm by suj* »
Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #83 on:** September 10, 2020, 03:54:27 pm »

I've had a setback
That FLASH SIMM I used to cause an error that got me into the monitor program. well, it blew the board. fortunately it's my spare processor board I've been using to experiment on but its DEAD
At least it wasn't my actual board I normally use.
DS1-DS7 all on, no boot at all. Likely and hopefully blew a buffer chip (data or address) and not the FPGA.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #84 on:** September 10, 2020, 04:03:08 pm »

Quote from: suj on September 09, 2020, 09:35:49 pm

> How do I enter the monitor? Sandra, you wrote about a planned error. How to do it?

Cause a error.
I was playing with this before I had the issue om the Processor Board and i think if you put in the ESALOADER disc you can get the Monitor Program that way.

of course this might be a problem for you with the FD issue your having

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: suj

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #85 on:** September 10, 2020, 05:38:39 pm »

can you connect a keyboard and keep slapping it during boot up. maybe that will cause the boot loader to redirect to a console monitor
i dont see any message saying this in the boot log you posted but still it might work

Report to moderator Logged

andrew9875
Contributor
Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #86 on:** September 10, 2020, 07:09:03 pm »

Looks like Sandra is correct, you can easily enter the monitor program by booting from the ESALOADR floppy. Just tried it on my E4402B.

When the SA completes booting from the floppy, press 'j' at the serial console then CTRL+C and you're in the monitor program.

Code: [Select]

```
     '?' - this help message.
     'j' - drop into breakpoint.
    '^C' - Abort to monitor.
    '^P' - Process status info, and LOTS of it.
  '[dD]' - Print DLP debug information.
  '[bB]' - Big memory hog report.
  '[pP]' - Process ONLY status info.

  '[eE]' - Exchange info.
  '[tT]' - Time log.
  '[hH]' - History log.
  '[oO]' - Memory segment ownership.
  '[mM]' - Memory segment summary.
  '[sS]' - Semaphore ownership, etc.
  '[uU]' - maximum process stack Usage.
  '[vV]' - memory Validity check.
```

I will attempt a memory dump later today. I have a few options installed (B72, 1DN, B7B, A4H, BAA, AYX, B7D, B7E), so hopefully this will be useful.

Report to moderator Logged

The following users thanked this post: tv84, suj

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #87 on:** September 10, 2020, 07:26:06 pm »

This procedure works for me. Tomorrow I should have a fully functional FDD, then I will upgrade the firmware to the last one. In the older firmware version, from 0x048B9200, they are all zeros.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #88 on:** September 10, 2020, 07:48:37 pm »

Guys, feel bad for Sandra but great news from the others.

Try to make a **dump from 0x0401 1000 up to 0x0490 0000**. Those that don't have any license should try to insert a random license before the dump. Just insert "0123456789AB".

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #89 on:** September 10, 2020, 08:05:06 pm »

> **Quote from: suj on September 10, 2020, 07:26:06 pm**
>
> This procedure works for me. Tomorrow I should have a fully functional FDD, then I will upgrade the firmware to the last one. In the older firmware version, from 0x048B9200, they are all zeros.

That's why it's important to normalize versions. My analysis was done with the A.14.06 ESAFW shared by Sandra.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #90 on:** September 10, 2020, 08:30:19 pm »

> **Quote from: andrew9875 on September 10, 2020, 07:09:03 pm**
>
> Looks like Sandra is correct, you can easily enter the monitor program by booting from the ESALOADR floppy. Just tried it on my E4402B.
> I will attempt a memory dump later today. I have a few options installed (B72, 1DN, B7B, A4H, BAA, AYX, B7D, B7E), so hopefully this will be useful.

If that is the menu you see that is the debug menu not the monitor menu where you can dump memory
the dump command is
dbyte start(in hex),len(in bytes)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #91 on:** September 10, 2020, 09:00:21 pm »

It's working for monitor menu
1. Connect serial to the J1 (19200, 8/N/1)
2. boot from bootloader floppy disk
3. press "j" then "ctrl+c"

After next power cycle (the front power button not working), SA needs full aligment.

Report to moderator Logged

The following users thanked this post: andrew9875

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #92 on:** September 11, 2020, 04:04:09 am »

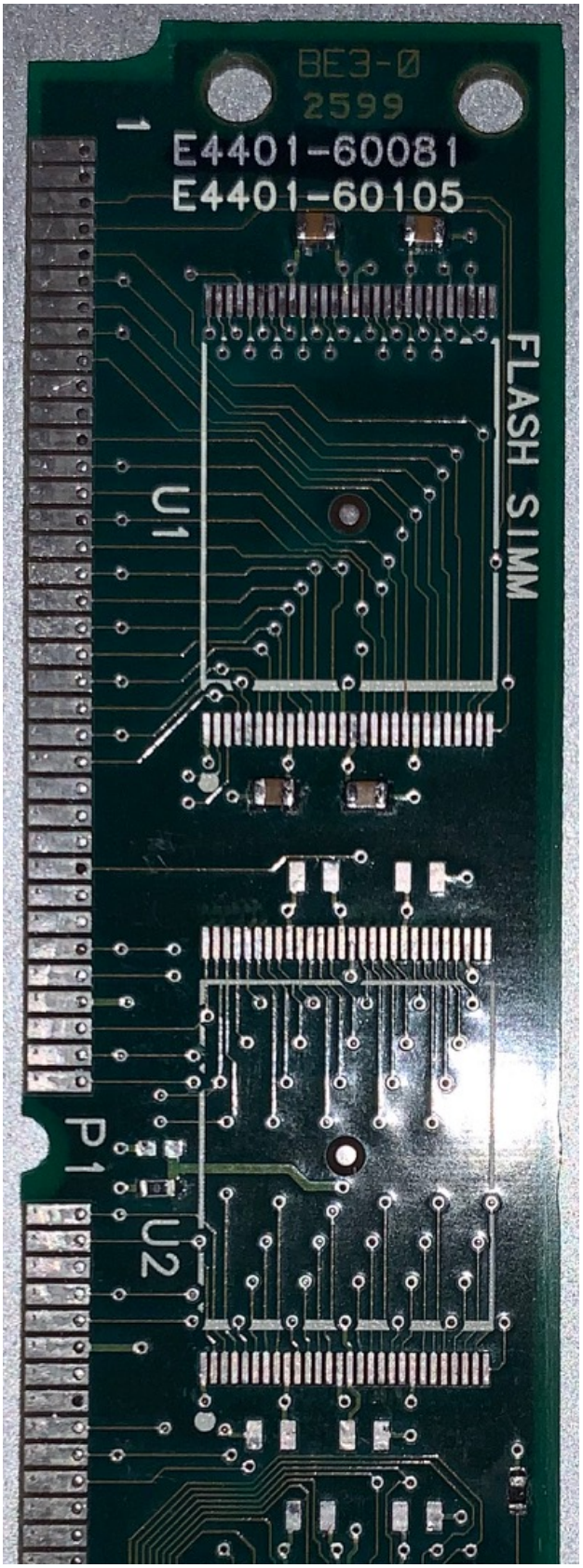
Starting to fix what I broke.
I have noticed looking at the CLIP there is a Bus defined as DBS_D_T[15.0] that goes to all the FLASH memory but goes no where else.
DBS_D[15.0] goes from the Dynamic bus sizer to the IO buffers but there's no Data buffers. Strange

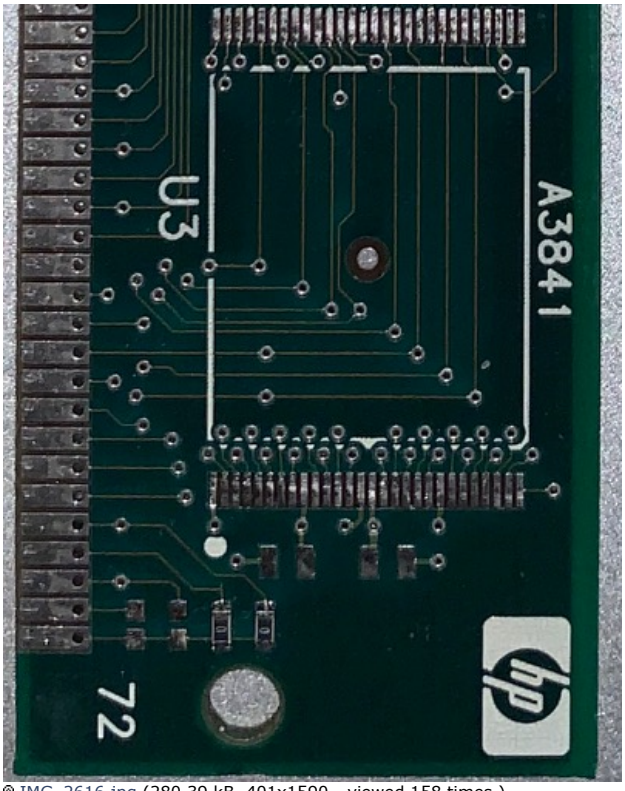
Looking at what the FLASH SIMM was attached to is why I'm looking though I did remove all the FLASH Memory from the SIMM and tested it. All 3 tested Good so thats a plus
I did identify that that 0 ohm is by the U2 Label. if it's on the right side it connect VPP_FLASH_5V to the memory, if on the left it connects VPP_FLASH_12V to the memory
that little resistor at the top of the SIMM pulls #BYTE High
PA0_DBS is not connected to the memory
PA1_DB2 is connected to the A1 ping on all the memory

LCS_FLASH4/5 are connected reverse of the other ones BE1H/BE1L instead of BE1L/BE1H like the others
Only the FLASH OC0_RYBY/U1, FLASH OC1_RYBY/U2 and FLASH OC2_RYBY/U3 are connected the other are NC

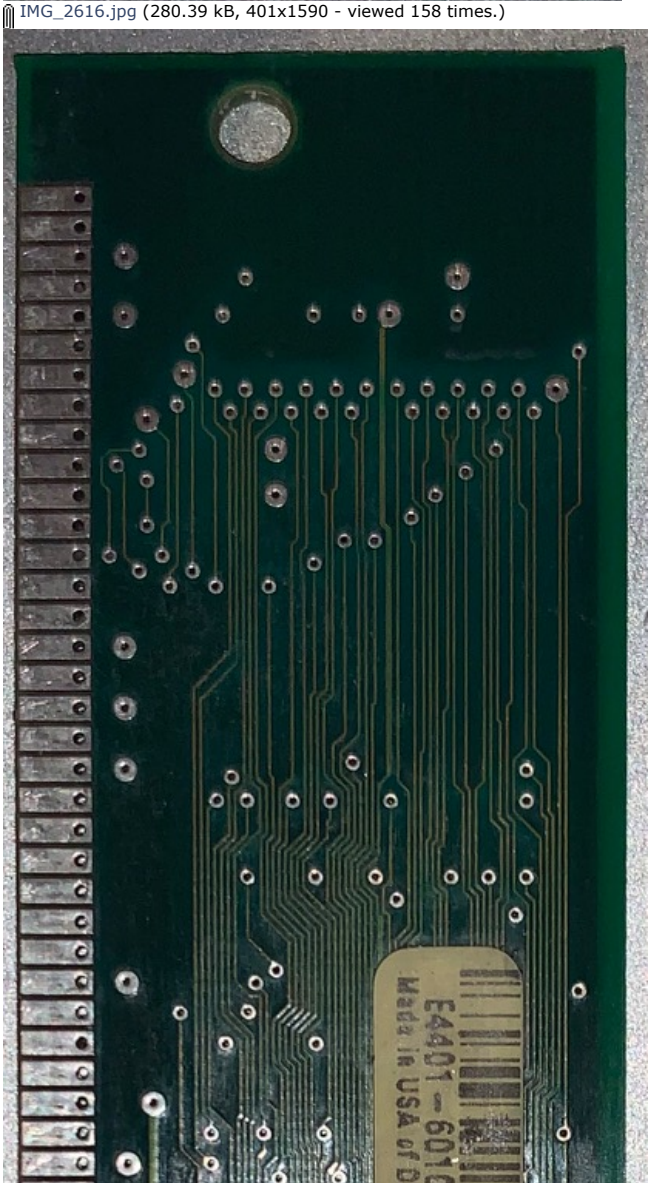
Attaching Some Pic of the unpopulated SIMM module

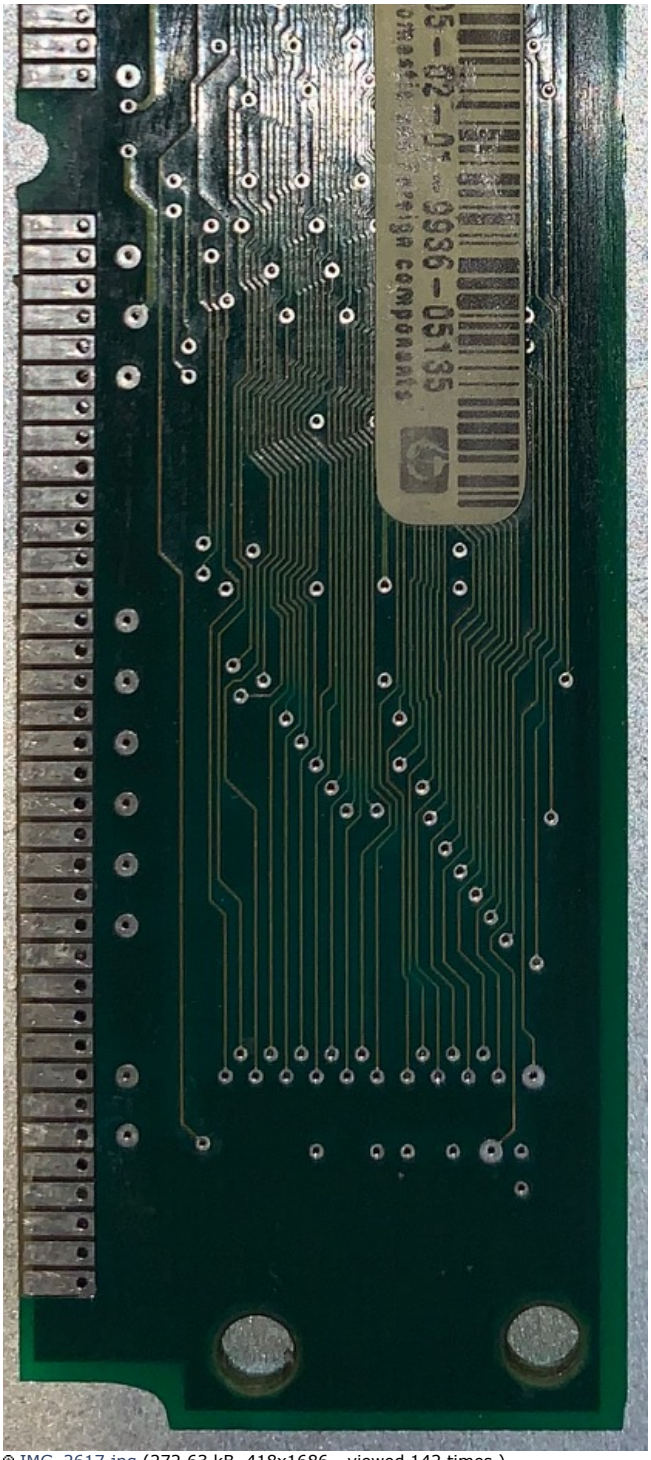
For the Processor Board working with it is difficult while in the SA. I'l going to see if I can supply 5v to it and troubleshoot on the bench
should let me use the scope much easier.





IMG_2616.jpg (280.39 kB, 401x1590 - viewed 158 times.)





IMG_2617.jpg (272.63 kB, 418x1686 - viewed 142 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

andrew9875
Contributor
Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #93 on:** September 11, 2020, 11:18:21 am »

Say Thanks Reply Quote

Quote from: tv84 on September 10, 2020, 07:48:37 pm

> Try to make a **dump from 0x0401 1000 up to 0x0490 0000**.

My memory dump is attached.

FYI, my unit is running the latest A.14.06 firmware.

memdump.7z (654.04 kB - downloaded 45 times.)

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #94 on:** September 11, 2020, 11:42:08 am »

Say Thanks Reply Quote

> **Quote from: andrew9875 on September 11, 2020, 11:18:21 am**
>
> My memory dump is attached.
>
> FYI, my unit is running the latest A.14.06 firmware.

Curious. It seems a correct dump BUT from a different memory bank (as if it was possible)...

I have to take a deeper look.

It's not the ESAFW. But I don't have here the rest of the package...

EDIT: It's the ESALOADR.
« *Last Edit: September 11, 2020, 06:54:01 pm by tv84* »

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #95 on:** September 11, 2020, 12:02:56 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 11, 2020, 11:42:08 am**
>
> > **Quote from: andrew9875 on September 11, 2020, 11:18:21 am**
> >
> > My memory dump is attached.
> >
> > FYI, my unit is running the latest A.14.06 firmware.
>
> Curious. It seems a correct dump BUT from a different memory bank (as if it was possible)...
>
> I have to take a deeper look.
>
> It's not the ESAFW. But I don't have here the rest of the package...

@tv84 Do you run anything to convert these dumps into a bin file or other format?
since they're ascii dumps I figured you might do something like that.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

andrew9875
Contributor

Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #96 on:** September 11, 2020, 01:44:50 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 11, 2020, 11:42:08 am**
>
> Curious. It seems a correct dump BUT from a different memory bank (as if it was possible)...
>
> I have to take a deeper look.
>
> It's not the ESAFW. But I don't have here the rest of the package...

Hmmm. I wonder if this is because ESALOADR is loaded and running.

I think I figured how to access the ROM monitor without ESALOADR running:

1. Boot from ESALOADR floppy, drop into ROM monitor menu (j, CTRL+C)
2. Retry test routine ('rty')
3. Test routine will fail/hang, then remove floppy and power cycle the unit
4. Boot from flash will fail and drop you back into ROM monitor

So far the dump is at least slightly different, just need to wait several hours for it to complete.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #97 on:** September 11, 2020, 02:38:24 pm »

Say Thanks Reply Quote

Quote from: andrew9875 on September 11, 2020, 01:44:50 pm

Quote from: tv84 on September 11, 2020, 11:42:08 am

Curious. It seems a correct dump BUT from a different memory bank (as if it was possible)...

I have to take a deeper look.

It's not the ESAFW. But I don't have here the rest of the package...

Hmmm. I wonder if this is because ESALOADR is loaded and running.

I think I figured how to access the ROM monitor without ESALOADR running:

1. Boot from ESALOADR floppy, drop into ROM monitor menu (j, CTRL+C)
2. Retry test routine ('rty')
3. Test routine will fail/hang, then remove floppy and power cycle the unit
4. Boot from flash will fail and drop you back into ROM monitor

So far the dump is at least slightly different, just need to wait several hours for it to complete.

Have your tried the (J, CTRL+C) on a normal boot
that's what we're after, if it will work

anytime loading ESALOADER you won't get ESAFW loaded off flash and executed.
the ideal is
Boot Normally
Get into Monitor
then Dump Memory

probably should let TV84 know your HOSTID and be sure your running 14.06 of the firmware (I know you are, this is more for anyone else who tries int he future)

« *Last Edit: September 11, 2020, 06:44:35 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #98 on:** September 11, 2020, 04:45:29 pm »

Say Thanks Reply Quote

What do you think about this
1. we need the ESAFW loaded. So far though we cant' get into the monitor to do the dbyte dump command
2. J14 is Reset on the Processor Card

what if we powered up normally. once up and firmware loaded we insert the ESALOADER disc and reset
DRAM should still be loaded.

we can then break into monitor and try to dump memory?

another thought is would it be worth hacking the boot rom to enable the ^C to break into the monitor. it lets you in the monitor when loading the ESALOADER but not the main firmware

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #99 on:** September 11, 2020, 04:59:42 pm »

Say Thanks Reply Quote

Quote from: smgvbest on September 11, 2020, 04:45:29 pm

Posts: 2380
Country:

> another thought is would it be worth hacking the boot rom to enable the ^C to break into the monitor.
> it lets you in the monitor when loading the ESALOADER but not the main firmware

Not so easy because the DEBUG MENU is in the ESALOADR, not the BOOTROM.

« *Last Edit: September 11, 2020, 08:14:05 pm by tv84* »

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #100 on:** September 11, 2020, 06:17:29 pm »

> **Quote from: andrew9875 on September 11, 2020, 11:18:21 am**
>
> My memory dump is attached.
>
> FYI, my unit is running the latest A.14.06 firmware.

In binary format.

This Andrews's dump is a dump of ESALOADR (size 0xB5B48 bytes). Not ESAFW.

memdump.zip (284.6 kB - downloaded 28 times.)

« *Last Edit: September 11, 2020, 06:26:05 pm by tv84* »

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #101 on:** September 11, 2020, 06:28:46 pm »

> **Quote from: smgvbest on September 11, 2020, 04:45:29 pm**
>
> what if we powered up normally. once up and firmware loaded we insert the ESALOADER disc and reset
> DRAM should still be loaded.
>
> we can then break into monitor and try to dump memory?

That is a nice idea. Please try it.

Report to moderator Logged

Gribo
Frequent Contributor

Posts: 527
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #102 on:** September 11, 2020, 06:42:25 pm »

Ctrl+C is also the Break key, you can try that.

Report to moderator Logged

I am available for freelance work.

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #103 on:** September 11, 2020, 07:02:13 pm »

> **Quote from: Gribo on September 11, 2020, 06:42:25 pm**
>
> Ctrl+C is also the Break key, you can try that.

Not working.
What BootRom Version are you on
Mine is E4401 Bootrom, 5.00

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #104 on:** September 11, 2020, 07:07:40 pm »

Posts: 623
Country:

Just to be sure we're all on same Page

This is the Debug menu and not what we need

Code: [Select]

```
----- System/pSOS Debug commands: -----
    '?' - this help message.
    'j' - drop into breakpoint.
   '^C' - Abort to monitor.
   '^P' - Process status info, and LOTS of it.
 '[dD]' - Print DLP debug information.
 '[bB]' - Big memory hog report.
 '[pP]' - Process ONLY status info.

 '[eE]' - Exchange info.
 '[gG]' - toggle breakpoint exception handlers on/off
 '[tT]' - Time log.
 '[hH]' - History log.
 '[oO]' - Memory segment ownership.
 '[mM]' - Memory segment summary.
 '[sS]' - Semaphore ownership, etc.
```

This is the Monitor Menu and what we're after.

Code: [Select]

```
bc      [<hex boot config>] - set the bootrom configuration (see bchelp)
bootvars- display bootrom variables
bs      - force a breakpoint when starting
dbyte   [<hex start address> [num bytes]] - display memory using bytes
dlong   [<hex start address> [num bytes]] - display memory using longs
dmem    [<hex start address> [num bytes]] - display memory using bytes
dword   [<hex start address> [num bytes]] - display memory using words
gbreak  - force a gdb breakpoint
gdb     - enable gdb trapping of exceptions
gu      [<hex start addr>]      - go to start address
hmon    [device] - download into memory
rty test routine
sbyte   <hex start address> <hexchars> - set memory using bytes
slong   <hex start address> <hexchars> - set memory using longs
smem    <hex start address> <hexchars> - set memory using bytes
sword   <hex start address> <hexchars> - set memory using words
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #105 on:** September 11, 2020, 07:19:24 pm »

Say Thanks Reply Quote

Please dump from 0x0400 0000 to 0x0401 1000. Just to check if this is BOOTROM-related.

I think this can be done with ESALOADR. No need for ESAFW.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #106 on:** September 11, 2020, 07:20:50 pm »

Say Thanks Reply Quote

Quote from: smgvbest on September 11, 2020, 07:07:40 pm

> Just to be sure we're all on same Page

How do you trigger DEBUG MENU?

For information:

DEBUG MENU is inside ESALOADR

MONITOR MENU is inside BOOTROM (called from within DEBUG MENU via ^C)

« *Last Edit: September 11, 2020, 08:02:56 pm by tv84* »

Report to moderator Logged

andrew9875
Contributor
Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #107 on:** September 11, 2020, 08:12:52 pm »

Say Thanks Reply Quote

Using this procedure:

Quote from: andrew9875 on September 11, 2020, 01:44:50 pm

1. Boot from ESALOADR floppy, drop into ROM monitor menu (j, CTRL+C)
2. Retry test routine ('rty')
3. Test routine will fail/hang, then remove floppy and power cycle the unit
4. Boot from flash will fail and drop you back into ROM monitor

My memory dump (0x04011000-0x04900000) looks nearly identical to the concatenated ESAFW file that Sandra shared earlier with only a handful of addresses differing, and differs quite a lot from the ESALOADR.

I believe this dump is the ESAFW from flash. On the second boot (step 4 of my procedure), the ESALOADR disk is not present so the unit must load from flash.

memdump1.7z (1095.55 kB - downloaded 32 times.)

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #108 on:** September 11, 2020, 08:15:20 pm »

Say Thanks Reply Quote

when you boot normally the Debug Menu "----- System/pSOS Debug commands: ----- " is always there.
when you boot from the ESALOADER you don't initially see a menu. Pressing ? when show same menu above, you can CTRL+C and it causes an exception then you're in the Monitor menu where you can dump memory

I've hooked up a reset switch, booted normally, entered AXZ for the opt and 0123456789ABC for the code.
inserted the ESALOADER, and hit reset.
once rebooted I got into the mornitor and did 2 dumps (ones still dumping)

first is will be
0x0400 0000 to 0x0401 1000

second will be
0x0401 1000 to 0x0490 0000

soon as done i'll edit and post to this message
My HostID is 29611027
My BootRom is V5.00

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor
Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #109 on:** September 11, 2020, 08:32:11 pm »

Say Thanks Reply Quote

Quote from: andrew9875 on September 11, 2020, 08:12:52 pm

My memory dump (0x04011000-0x04900000) looks nearly identical to the concatenated ESAFW file that Sandra shared earlier with only a handful of addresses differing, and differs quite a lot from the ESALOADR.

I believe this dump is the ESAFW from flash. On the second boot (step 4 of my procedure), the ESALOADR disk is not present so the unit must load from flash.

This dump is exactly Sandra's ESAFW with 8 bytes different (in the middle of the code).

The problem is that you didn't run the app before taking the dump. We need the dump after the app has run/is running. Because all the rest of the mem is 0x00s.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #110 on:** September 11, 2020, 08:38:49 pm »

Say Thanks Reply Quote

It MUST be possible to abort into Monitor mode from within ESAFW because ESAFW also has the DEBUG MENU in the code (with the ^C option). Just saw that in the code.

Report to moderator Logged

andrew9875
Contributor

Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #111 on:** September 11, 2020, 08:41:18 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 11, 2020, 08:32:11 pm**
>
> This dump is exactly Sandra's ESAFW with 8 bytes different (in the middle of the code).
>
> The problem is that you didn't run the app before taking the dump. We need the dump after the app has run/is running. Because all the rest of the mem is 0x00s.

Got it, didn't quite grasp what the issue was before. The application was definitely not running when I created the new dump.

Looking forward to seeing Sandra's results

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #112 on:** September 11, 2020, 08:41:40 pm »

Say Thanks Reply Quote

When I boot from the ESALOADER and see the Menu ^C works fine
when I boot normally and see the Menu, even though ^C is in the menu all I see is a message that it doesn't recognize the keypress

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #113 on:** September 11, 2020, 08:45:28 pm »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 11, 2020, 08:41:40 pm**
>
> When I boot from the ESALOADER and see the Menu ^C works fine
> when I boot normally and see the Menu, even though ^C is in the menu all I see is a message that it doesn't recognize the keypress

Ohhh. That's another story. Let's wait for your dumps. I've got my fingers crossed.

If not successfull, I'll ask you to do me a log dump of all the submenu options of the DEBUG MENU (just the 1st screen) so that I can crosscheck the functions.

Report to moderator Logged

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #114 on:** September 11, 2020, 08:53:04 pm »

Say Thanks Reply Quote

> **Quote from: andrew9875 on September 11, 2020, 08:41:18 pm**

Posts: 623
Country:

> **Quote from: tv84 on September 11, 2020, 08:32:11 pm**
>
> This dump is exactly Sandra's ESAFW with 8 bytes different (in the middle of the code).
>
> The problem is that you didn't run the app before taking the dump. We need the dump after the app has run/is running. Because all the rest of the mem is 0x00s.

Got it, didn't quite grasp what the issue was before. The application was definitely not running when I created the new dump.

Looking forward to seeing Sandra's results

still dumping, it's up to 0x040Dxxxx and it's all zero's in this area

i'm trying to figure our device addressing
the max address is 0x07FFFFFF only ADDRESS BIT 0..27 are used
21,22,23 are used to address the FLASH memory (thru a 74138)

U55 controls the addressing which is the communications controller which goes to the enable pin on the 74138

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #115 on:** September 11, 2020, 09:01:36 pm »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 11, 2020, 08:41:40 pm**
>
> all I see is a message that it doesn't recognize the keypress

What is the specific msg?

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #116 on:** September 11, 2020, 09:05:23 pm »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 11, 2020, 08:53:04 pm**
>
> the max address is 0x07FFFFFF only ADDRESS BIT 0..27 are used

I saw somewhere that the app and mem would not go upper that 0x06000000. Maybe in your boot logs...

That doesn't mean that physically it couldn't go to that limit mentioned by you.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #117 on:** September 11, 2020, 09:09:56 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 11, 2020, 09:05:23 pm**
>
> I saw somewhere that the app and mem would not go upper that 0x06000000. Maybe in your boot logs...
>
> That doesn't mean that physically it couldn't go to that limit mentioned by you.

From the hardware side it's physically limited to 0x07FFFFFF (A0..A27) the remaining bits are NC

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #118 on:** September 11, 2020, 09:14:03 pm »

> **Quote from: tv84 on September 11, 2020, 09:01:36 pm**
>
> > **Quote from: smgvbest on September 11, 2020, 08:41:40 pm**
> >
> > all I see is a message that it doesn't recognize the keypress
>
> What is the specific msg?

Unknown debug char: 'C' (0x43). Press '?' for help.
if I do CTRL+C its
Unknown debug char: ' ' (0x03). Press '?' for help. (i think) still dumping so I can't check

I do not miss dialup speeds

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #119 on:** September 11, 2020, 09:16:17 pm »

> **Quote from: tv84 on September 11, 2020, 08:45:28 pm**
>
> > **Quote from: smgvbest on September 11, 2020, 08:41:40 pm**
> >
> > When I boot from the ESALOADER and see the Menu ^C works fine
> > when I boot normally and see the Menu, even though ^C is in the menu all I see is a message that it doesn't recognize the keypress
>
> Ohhh. That's another story. Let's wait for your dumps. I've got my fingers crossed.
>
> If not successfull, I'll ask you to do me a log dump of all the submenu options of the DEBUG MENU (just the 1st screen) so that I can crosscheck the functions.

There are no sub menus
each option is a direct action in the menus
the may take parms but that is passed with the option you want

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #120 on:** September 11, 2020, 09:27:28 pm »

Is anyone able when booting normally (no ESALOADER Disc) able to do the CTRL+C and enter the Monitor Program?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #121 on:** September 11, 2020, 09:30:02 pm »

> **Quote from: tv84 on September 11, 2020, 09:25:30 pm**
>
> > **Quote from: smgvbest on September 11, 2020, 09:16:17 pm**
> >
> > There are no sub menus
> > each option is a direct action in the menus
> > the may take parms but that is passed with the option you want

> Sure, all I want is a dump of the 1st page of those direct actions (just to identify the strings in it).
>
> You don't need to try other keys. The DEBUG in ESAFW doesn't have the code for "^C". So we would need to patch it.
>
> BTW, the DEBUG MENUs of ESAFW and ESALOADR have slight differences. I think ESAFW has more options.

I do have some spare FLASH memory for the BootLoader so if a patch isnt to hard maybe thats the way to go???

These are the menu options seen when booting

This is the Debug menu when booting Normally, you have to do a ? to see it

Code: [Select]

```
----- System/pSOS Debug commands: -----
    '?' - this help message.
    'j' - drop into breakpoint.
   '^C' - Abort to monitor.
   '^P' - Process status info, and LOTS of it.
 '[dD]' - Print DLP debug information.
 '[bB]' - Big memory hog report.
 '[pP]' - Process ONLY status info.

 '[eE]' - Exchange info.
 '[gG]' - toggle breakpoint exception handlers on/off
 '[tT]' - Time log.
 '[hH]' - History log.
 '[oO]' - Memory segment ownership.
 '[mM]' - Memory segment summary.
 '[sS]' - Semaphore ownership, etc.
```

This is the Monitor Menu from when using ESALOADER.

Code: [Select]

```
bc      [<hex boot config>] - set the bootrom configuration (see bchelp)
bootvars- display bootrom variables
bs      - force a breakpoint when starting
dbyte   [<hex start address> [num bytes]] - display memory using bytes
dlong   [<hex start address> [num bytes]] - display memory using longs
dmem    [<hex start address> [num bytes]] - display memory using bytes
dword   [<hex start address> [num bytes]] - display memory using words
gbreak  - force a gdb breakpoint
gdb     - enable gdb trapping of exceptions
gu      [<hex start addr>]      - go to start address
hmon    [device] - download into memory
rty test routine
sbyte   <hex start address> <hexchars> - set memory using bytes
slong   <hex start address> <hexchars> - set memory using longs
smem    <hex start address> <hexchars> - set memory using bytes
sword   <hex start address> <hexchars> - set memory using words
```

« *Last Edit: September 11, 2020, 09:32:13 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #122 on:** September 11, 2020, 09:30:17 pm »

Say Thanks Reply Quote

I tried but it did not work.
I didn't get FDD todayso I still have older firmware.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #123 on:** September 11, 2020, 09:31:38 pm »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 11, 2020, 09:30:02 pm**
>
> that was these then

No, maybe I explained wrong:

I want the next steps in each of those options (just DEBUG MENU).

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #124 on:** September 11, 2020, 09:37:12 pm »

Say Thanks Reply Quote

Quote from: tv84 on September 11, 2020, 09:31:38 pm

Quote from: smgvbest on September 11, 2020, 09:30:02 pm

that was these then

No, maybe I explained wrong:

I want the next steps in each of those options (just DEBUG MENU).

if I type a option it executes the command so if thats what you want heres some
is this what you're after?

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 5.00
@(#)LDS Rev: 3.02 - Module Incremental (Sep  9 2003)
@(#)Linked: Sep  9 2003 14:46:44

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: tv84

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #125 on:** September 11, 2020, 10:19:08 pm »

Say Thanks Reply Quote

I found a debug interface command that is undocumented. Pressing "F4" had the effect shown below.
I can't interpret it, but it might mean something.
(Firmware still A14.01, probably until Monday ...)

capture.zip (108.32 kB - downloaded 53 times.)

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #126 on:** September 12, 2020, 03:34:47 am »

Say Thanks Reply Quote

Quote from: smgvbest on September 11, 2020, 08:53:04 pm

Quote from: andrew9875 on September 11, 2020, 08:41:18 pm

Quote from: tv84 on September 11, 2020, 08:32:11 pm

This dump is exactly Sandra's ESAFW with 8 bytes different (in the middle of the code).

The problem is that you didn't run the app before taking the dump. We need the dump after the app has run/is running. Because all the rest of the mem is 0x00s.

Got it, didn't quite grasp what the issue was before. The application was definitely not running when I created the new dump.

> Looking forward to seeing Sandra's results

still dumping, it's up to 0x040Dxxxx and it's all zero's in this area

i'm trying to figure our device addressing
the max address is 0x07FFFFFF only ADDRESS BIT 0..27 are used
21,22,23 are used to address the FLASH memory (thru a 74138)

U55 controls the addressing which is the communications controller which goes to the enable pin on the 74138

Ok here's my 2 dumps

one is from ESALOADER
second is after normal boot, entering a license, getting a fail. hit reset into ESALOADER then dump memory

esaloader_boot.zip (49.05 kB - downloaded 29 times.)
esafw_boot_after_reset.zip (1241.76 kB - downloaded 40 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #127 on:** September 12, 2020, 07:36:28 am »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 12, 2020, 03:34:47 am**
>
> Ok here's my 2 dumps

Binary form.

esafw_boot_after_reset.zip (259.46 kB - downloaded 38 times.)
esaloader_boot.zip (20.71 kB - downloaded 34 times.)

Report to moderator Logged

The following users thanked this post: smgvbest

smgvbest
Supporter

Posts: 623
Country:

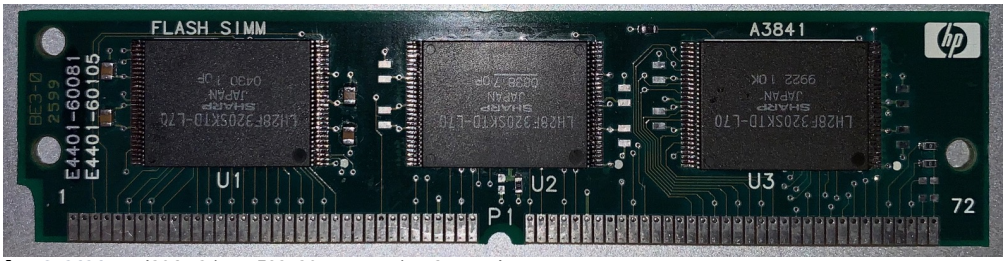
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #128 on:** September 12, 2020, 07:36:50 am »

Say Thanks Reply Quote

SIMM Repaired

the simm that caused the processor board to blow has been repaired. it apparently was upgraded from 4M to 12M of flash and the soldering was , um poor
I removed all flash and caps. tested all of the them. flash was read, erased, programmed, read, erased and read for each of the 3 flash memories.
checked caps and replaced all.

also started work on the processor board. FWIW,
On J3 you can supply 5v @ 1.3A to 3rd (of the longer) pin from right side and on P7 for GND and youv'e got power.
it does need more voltages but Boots with just 5V



IMG_2626.jpg (306.42 kB, 1582x397 - viewed 116 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #129 on:** September 12, 2020, 07:37:32 am »

Say Thanks Reply Quote

> **Quote from: tv84 on September 12, 2020, 07:36:28 am**
>
> > **Quote from: smgvbest on September 12, 2020, 03:34:47 am**
> >
> > Ok here's my 2 dumps
>
> Binary form.

what tool(s) did you use to do that?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

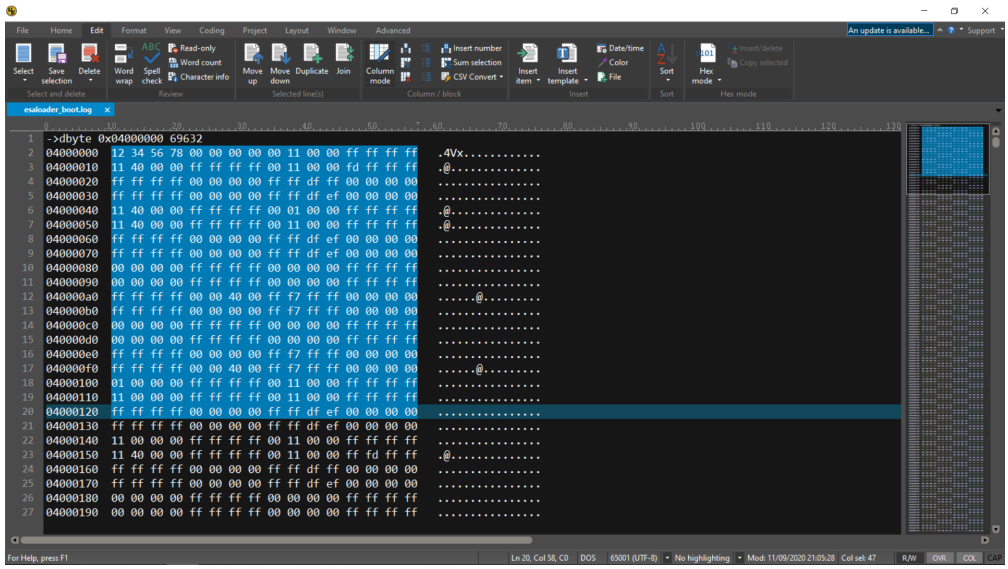
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #130 on:** September 12, 2020, 07:54:42 am »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 12, 2020, 07:37:32 am**
>
> what tool(s) did you use to do that?

I use UltraEdit in "Column Mode" which allows me to strip the left and right columns of text. Then do a Select All and paste it in HxD (in the binary zone). It's very simple and doesn't require any scripting and/or custom programming.

It's the same as selecting/copying just the binary dump bytes (in UltraEdit's "Column Mode") and paste them in HxD. See image.



esaloader_boot.png (295 kB, 1918x1079 - viewed 96 times.)

« *Last Edit: September 12, 2020, 08:07:33 am by tv84* »

Report to moderator Logged

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #131 on:** September 12, 2020, 01:43:30 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 12, 2020, 07:54:42 am**

Posts: 623
Country:

> I use UltraEdit in "Column Mode" which allows me to strip the left and right columns of text. Then do a Select All and paste it in HxD (in the binary zone). It's very simple and doesn't require any scripting and/or custom programming.
>
> It's the same as selecting/copying just the binary dump bytes (in UltraEdit's "Column Mode") and paste them in HxD. See image.

And here I was thinking it was some python or other script to do it
Ultraedit I have, ever since V1, love it.

> **Quote from: tv84 on September 12, 2020, 07:51:55 am**
>
> That's it! Please send the other options.

I will get other options today, some take awhile to dump

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #132 on:** September 12, 2020, 10:23:00 pm »
Say Thanks Reply Quote

> **Quote from: smgvbest on September 12, 2020, 01:43:30 pm**
>
> I will get other options today, some take awhile to dump

Sandra, repeat also your ESAFW dump because yours is incomplete. You didn't dump from 0x0401 1000 up to 0x0490 0000.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #133 on:** September 12, 2020, 10:44:36 pm »
Say Thanks Reply Quote

> **Quote from: tv84 on September 12, 2020, 10:23:00 pm**
>
> > **Quote from: smgvbest on September 12, 2020, 01:43:30 pm**
> >
> > I will get other options today, some take awhile to dump
>
> Sandra, repeat also your ESAFW dump because yours is incomplete. You didn't dump from 0x0401 1000 up to 0x0490 0000.

Yeh, think power died on the surface tablet before it finished

I'll do again with power plugged in this time

edit:
Here's all the Debug menu options with thier output
I edited to show the option selected as its not echoed normally

ESAFW dump is running, tablet is plugged in this time
I entered 2 licenses
AYZ 888888888888
IDS 999999999999

debug.zip (134.26 kB - downloaded 35 times.)

« Last Edit: September 13, 2020, 12:27:43 am by smgvbest »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: tv84

smgvbest

Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #134 on:** September 13, 2020, 07:06:51 pm »

ok it took many hours to dump that amount of memory but here's the "complete" dump this time

esafw.zip (2306.31 kB - downloaded 39 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: analogRF

suj

Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #135 on:** September 14, 2020, 04:20:43 pm »

I just finished the firmware upgrade, I have the A14.06 version installed now. I have SA open, if necessary, I can disassemble the controller card and boot it on the table. I can make a memory dump, please just write me according to the procedure from which post

EDIT
https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3228528/#msg3228528
should I do according to this description (post #120 written by Sandra)?
As I understand it, reset is a shorting of the pins of connector J14.

« *Last Edit: September 14, 2020, 05:12:32 pm by suj* »

Report to moderator Logged

tv84

Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #136 on:** September 14, 2020, 05:17:36 pm »

Quote from: suj on September 14, 2020, 04:20:43 pm

> EDIT
> https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3228528/#msg3228528
> should I do according to this description (post #120 written by Sandra)?

That method is what she has just tried and doesn't work. It dumps the ESALOADR environment. The reset crushes all the ESAFW previous state.

Report to moderator Logged

suj

Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #137 on:** September 14, 2020, 08:15:52 pm »

OK, I get it. It would be best to have access to hardware ICE. I checked on ebay, there is no one unnecessary, dusty, complete Lauterbach ICE32_LA-6780_LA-6782_LA-6786. There is also no HP 64783A/B with the HP 9000 series 300 included. Anyway, none of them would cost $ 200...
As a last resort, I see a solution in the ICE type. The board between the PGA socket and the processor. There is an additional uC on it. After system boots up, it stops MC68EC040 and reads memory and sends via its own serial port. Dynamic memory refresh is handled by the MC68EN360, but there can be tons of bus arbitration issues. It's just a rather complicated project ...

Report to moderator Logged

smgvbest

Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #138 on:** September 14, 2020, 08:23:09 pm »

Quote from: tv84 on September 14, 2020, 05:17:36 pm

> **Quote from: suj on September 14, 2020, 04:20:43 pm**
>
> > EDIT
> > https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3228528/#msg3228528
> > should I do according to this description (post #120 written by Sandra)?

> That method is what she has just tried and doesn't work. It dumps the ESALOADR environment. The reset crushes all the ESAFW previous state.

yeh it was worth a try but its a no-go
it looks like we need to find out who to get the monitor menu from a normal boot.
You mention though that CTRL+C is disabled in the BootRom? or is it disabled in the ESAFW?
would it be hard to patch to enable that function?

the other thing is SCPI, There's suppose to be a debug interface (but undocumented) via SCPI and it may be faster than the serial interface.

Any recommendations on how to proceed?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #139 on:** September 14, 2020, 09:13:22 pm »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 14, 2020, 08:23:09 pm**
>
> Any recommendations on how to proceed?

I don't know if the Bootrom is somewhat old and maps the **^C jump address** in a memory place that the ESALOADR A.05.00 knows where to find but the ESAFW A.14.06 doesn't (I've seen that both use different addresses, I think). Just a guess... I've tried to discover that to force the jump but... arghhh. damn language...

The way to proceed is to try a patch.

Please test if you can flash a patched FW (or live patch the ESAFW). You can test with a string used in any message onscreen.

If you are successful, I think I can craft a special patch.

Report to moderator Logged

andrew9875
Contributor

Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #140 on:** September 14, 2020, 10:08:55 pm »

Say Thanks Reply Quote

> **Quote from: smgvbest on September 14, 2020, 08:23:09 pm**
>
> Any recommendations on how to proceed?

Has anyone looked at the service information for these analyzers? Maybe another vector we can explore:

DRAM and flash EPROM can be erased by flipping switches on S1 or holding down front panel buttons during boot. Maybe there's some hidden features there...

service-guide-agilent-e4402b-e4404b-e4405b-e4407b-e4411b-e4403b-e4408b.7z (3547.42 kB - downloaded 60 times.)

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #141 on:** September 14, 2020, 10:49:40 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 14, 2020, 09:13:22 pm**
>
> > **Quote from: smgvbest on September 14, 2020, 08:23:09 pm**
> >
> > Any recommendations on how to proceed?
>
> I don't know if the Bootrom is somewhat old and maps the **^C jump address** in a memory place that the ESALOADR A.05.00 knows where to find but the ESAFW A.14.06 doesn't (I've seen that both use different addresses, I think). Just a guess... I've tried to discover that to force the jump but... arghhh. damn language...

> The way to proceed is to try a patch.
>
> Please test if you can flash a patched FW (or live patch the ESAFW). You can test with a string used in any message onscreen.
>
> If you are successful, I think I can craft a special patch.

If you know the address where the ctrl+c code is then I think in the debug menu the gu address command will jump to that address???

Maybe we can force it there?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #142 on:** September 15, 2020, 03:48:01 am »

The HOSTID is based on the PROCESSOR board. so if you change processor boards you do change the hostid
you are correct in that flash has nothing to do with it.

I have tried all the DIP switches but not all combinations. most seem to do nothing. SW2/SW3 erase SRAM/FLASH

if you load any software you don't get a running version of the ESAFW into DRAM and thats' what we need. We need it running

edit:
The Keys are stored on the FLASH SIMM according to the Security Manual
The Processor is a 68LC040. kind of old

« Last Edit: September 16, 2020, 04:32:36 pm by smgvbest »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #143 on:** September 17, 2020, 12:44:07 am »

Before actually re-flashing my SA I thought I would try just changing the ESALOADR and after I changed some text the ESALOADR would not load, it just skipped it and booted normally.
I watched the serial port and saw nothing special there

can someone else try this on the loader disc and change some text and see if you get same result?

I know we're not after the loader for this but its a test before going thru a full re-flash, I only cried 9 times

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

andrew9875
Contributor

Posts: 7
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #144 on:** September 17, 2020, 01:12:41 am »

> **Quote from: smgvbest on September 17, 2020, 12:44:07 am**
>
> can someone else try this on the loader disc and change some text and see if you get same result?

I can try it out tomorrow, just change a few bytes in the ESALOADR image?

But, I have the feeling that it will fail. The boot ROM indicates that it calculates a checksum on flash before attempting to boot, and I have the feeling it does the same before booting from floppy.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #145 on:** September 17, 2020, 01:23:35 am »

> **Quote from: andrew9875 on September 17, 2020, 01:12:41 am**
>
> > **Quote from: smgvbest on September 17, 2020, 12:44:07 am**
> >
> > can someone else try this on the loader disc and change some text and see if you get same result?
>
> I can try it out tomorrow, just change a few bytes in the ESALOADR image?
>
> But, I have the feeling that it will fail. The boot ROM indicates that it calculates a checksum on flash before attempting to boot, and I have the feeling it does the same before booting from floppy.

This is to find out if we can patch the FW ultimately. this was just a test using the esaloader. i'm using a USB floppy drive and I have had problems writting disc so I want to see it its that causing my problem and not a checksum problem. I dont 'think it is.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

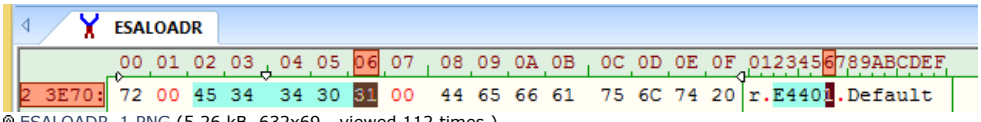
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

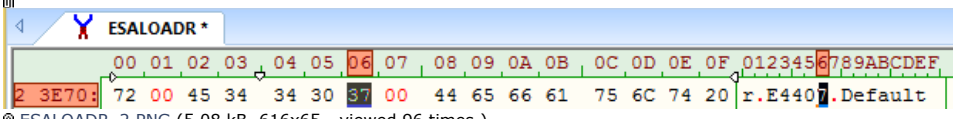
Say Thanks Reply Quote

« **Reply #146 on:** September 17, 2020, 09:57:06 am »

Be extremely careful! I just partially bricked my unit. In the first step, I made a little modification to the ESALOADR file (ESALOADR_1.PNG, ESALOADR_2.PNG). I restarted SA from FDD and it loaded. It showed a message to insert a second floppy disk, I was able to enter the monitor etc. Then I tried larger modifications to the ESALOADR file (shortened, more characters changed in the texts etc.). But after such modifications, he no longer wanted to load. At this point, I noticed that my options are not working and the maximum upper frequency is 6.78 GHz instead of 26.5 GHz. The options (1D5, 1DR, AYZ) could be restored by retyping the keys that are displayed on the licensing screen. But with maximum frequency there is a problem. Factory preset doesn't help. Only when I load my previous "User Preset" the frequency range is up to 26.5 GHz, but the following messages are displayed: LO Unlock, LO Unlevel.
In the evening I will look at the problem in more detail.



ESALOADR_1.PNG (5.26 kB, 632x69 - viewed 112 times.)



ESALOADR_2.PNG (5.08 kB, 616x65 - viewed 96 times.)

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #147 on:** September 17, 2020, 10:41:22 am »

OK, I'm changing the level from DEFCON1 to DEFCON5. In the service menu, it's possible to limit the upper frequency to 6.7 or 13.2 GHz (Initialize Instrument/Max Freq). After switching to 26.5 GHz, rebooting and full align, everything returned to the normal state.
Be careful!

Report to moderator Logged

tv84
Super Contributor

Posts: 2380

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #148 on:** September 17, 2020, 01:02:59 pm »

Please don't do changes in the ESALOADR. Try them in the ESAFW.

Report to moderator Logged

Country:

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #149 on:** September 17, 2020, 01:58:31 pm »

Quote from: suj on September 17, 2020, 09:57:06 am

> Be extremely careful! I just partially bricked my unit. In the first step, I made a little modification to the ESALOADR file (ESALOADR_1.PNG, ESALOADR_2.PNG). I restarted SA from FDD and it loaded. It showed a message to insert a second floppy disk, I was able to enter the monitor etc. Then I tried larger modifications to the ESALOADR file (shortened, more characters changed in the texts etc.). But after such modifications, he no longer wanted to load. At this point, I noticed that my options are not working and the maximum upper frequency is 6.78 GHz instead of 26.5 GHz. The options (1D5, 1DR, AYZ) could be restored by retyping the keys that are displayed on the licensing screen. But with maximum frequency there is a problem. Factory preset doesn't help. Only when I load my previous "User Preset" the frequency range is up to 26.5 GHz, but the following messages are displayed: LO Unlock, LO Unlevel.
> In the evening I will look at the problem in more detail.

The issue is you changed the base identifier for the SA. while E4407B is the specific model. E4401 is the line of SA and which almost all use to identify parts.
when doing these tests I would advise against changing E4401 to anything else. change other TEXT

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

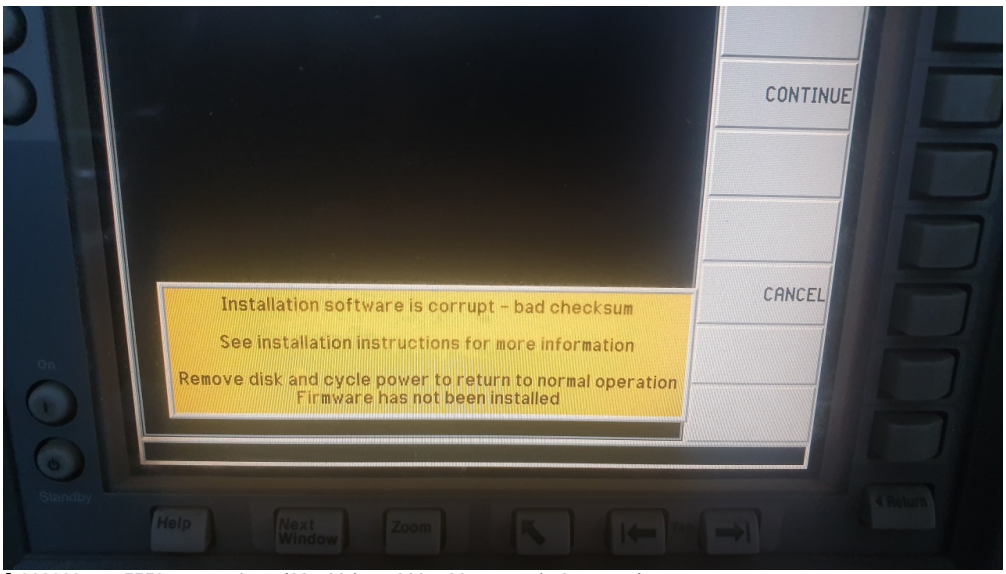
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #150 on:** September 17, 2020, 02:06:37 pm »

Quote from: tv84 on September 17, 2020, 01:02:59 pm

> ..Try them in the ESAFW.

I tried. I changed the text on the first floppy disk (first disk of the upgrade, not loader disk). In the menu for the external mixer, I changed the text: "Presel" to "11974Q". I started the upgrade. After the last floppy disk was loaded, a message was displayed on the SA screen. Nothing special on the serial terminal.



20200917_155521_resized.jpg (227.39 kB, 1280x720 - viewed 121 times.)

« *Last Edit: September 17, 2020, 02:09:27 pm by suj* »

Report to moderator Logged

The following users thanked this post: tv84, smgvbest

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #151 on:** September 17, 2020, 03:57:08 pm »

Quote from: tv84 on September 17, 2020, 01:02:59 pm

Please don't do changes in the ESALOADR. Try them in the ESAFW.

Posts: 623
Country:

The reason for this is a FW update takes a very long time, about 30-45 minutes to read all the discs and then flash the firmware.
ESALOADR loads in a minute or so to see if a cksum error occurred there. it sounds like @suj was able to load so we can move on to changing the ESAFW

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #152 on:** September 17, 2020, 04:07:58 pm »

Quote from: suj on September 17, 2020, 02:06:37 pm

Quote from: tv84 on September 17, 2020, 01:02:59 pm

..Try them in the ESAFW.

I tried. I changed the text on the first floppy disk (first disk of the upgrade, not loader disk). In the menu for the external mixer, I changed the text: "Presel" to "11974Q". I started the upgrade. After the last floppy disk was loaded, a message was displayed on the SA screen. Nothing special on the serial terminal.

Well Pooh
So the LOADER must run a cksum on the FW before continuing

That would mean either find that routine in the loader or find how to patch the active system I would think

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #153 on:** September 17, 2020, 04:50:54 pm »

On the serial terminal there were only the number of bytes loaded from each disk. Nothing more.

Report to moderator Logged

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #154 on:** September 17, 2020, 05:26:58 pm »

Checksum-relates fields:
Code: [Select]

```
+2C  db NumInterleavedBanks = 02
+38  db BankSizeH[NumInterleavedBanks] = 00, 00
        db BankSizeMH[NumInterleavedBanks] = 2C, 2C
        db BankSizeML[NumInterleavedBanks] = 95, 95
        db BankSizeL[NumInterleavedBanks] = CE, CE
        db ChecksumH[NumInterleavedBanks] = 58, B2
        db ChecksumL[NumInterleavedBanks] = 5C, A4
```

- so BankSize[0]=BankSize[1]=2C95CE, BankSize[0]+BankSize[1]=2C95CE+2C95CE=592B9C - matches file size
Checksum[bank] = sum(all bytes of bank):
Checksum[0] = 585C - matches sum of all even bytes of file
Checksum[1] = B2A4 - matches sum of all odd bytes of file

Edit: note that checksum calculation includes the checksum bytes themselves! (yes, they are not zeroed/skipped)
« *Last Edit: September 17, 2020, 05:30:24 pm by abyrvalg* »

Report to moderator Logged

The following users thanked this post: tv84, smgvbest, suj

abyrvalg
Frequent Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote

Posts: 603
Country:

« **Reply #155 on:** September 17, 2020, 07:02:57 pm »

More info:
"bulk" flash starts from C000000.

How to enter ROM monitor before jumping to FW:
BootROM loads ESALOADER (from floppy) or main fw (from bulk flash) to DRAM then sends a 05 byte (ascii ENQ char) and waits for 06 (ascii ACK) reply with timeout. If this wait times out - jump to DRAM normally, otherwise - bypass jump and enter ROM monitor.

This can be used to try patches without flashing them:
- don't insert ESALOADER floppy
- interrupt normal start by replying to 05 with 06
- modify firmware in RAM (with smem/sbyte/sword/slong cmds)
- jump to modified firmware (with gu cmd)

Report to moderator Logged

The following users thanked this post: tv84

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #156 on:** September 17, 2020, 07:28:08 pm »

The timeout is very short, it looks like 0.5 seconds maybe. These are probably those marked with 05, because the transmission stops for a moment at this point.

Code: [Select]

```
0D 0A 2A 2A 2A 2A 2A 20 4D 6F 73 71 75 69 74 6F 20 42 6F 6F 74 72 6F 6D
20 2A 2A 2A 2A 2A 0D 0A 43 6F 70 79 72 69 67 68 74 20 31 39 38 38 2D 31
39 39 37 2C 0D 0A 48 65 77 6C 65 74 74 2D 50 61 63 6B 61 72 64 20 43 6F
6D 70 61 6E 79 2C 20 61 6C 6C 20 72 69 67 68 74 73 20 72 65 73 65 72 76
65 64 2E 0D 0A 0D 0A 40 28 23 29 48 45 57 4C 45 54 54 2D 50 41 43 4B 41
52 44 2C 20 45 34 34 30 31 20 42 6F 6F 74 72 6F 6D 2C 20 35 2E 30 30 0D
0A 40 28 23 29 4C 44 53 20 52 65 76 3A 20 33 2E 30 32 20 2D 20 4D 6F 64
75 6C 65 20 49 6E 63 72 65 6D 65 6E 74 61 6C 20 28 53 65 70 20 20 39 20
32 30 30 33 29 0D 0A 40 28 23 29 4C 69 6E 6B 65 64 3A 20 53 65 70 20 20
39 20 32 30 30 33 20 31 34 3A 34 36 3A 34 34 0D 0A 0D 0A 42 6F 6F 74 72
6F 6D 20 43 68 65 63 6B 73 75 6D 20 2E 2E 2E 0D 0A 42 6F 6F 74 72 6F 6D
20 44 52 41 4D 3A 20 20 20 20 20 54 65 73 74 69 6E 67 20 36 39 36 33 32
20 62 79 74 65 73 20 61 74 20 30 78 30 34 30 30 30 30 30 30 0D 0A 4E 6F
6E 20 44 65 73 74 72 75 63 74 69 76 65 20 53 52 41 4D 20 54 65 73 74 20
2E 2E 2E 0D 0A 4D 61 69 6E 20 46 69 72 6D 77 61 72 65 20 44 52 41 4D 3A
20 20 20 20 20 54 65 73 74 69 6E 67 20 33 33 34 38 34 38 30 30 20 62 79
```

Report to moderator Logged

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #157 on:** September 17, 2020, 07:38:04 pm »

I think this should be done with a software, not manually. Short timeout, non-printable characters - this is not for humans.
But. If you have a terminal software capable of sending a 06 char you don't need to wait for 05 and react fast - just send that 06 continuously from power on until you see ROM Monitor command prompt.

« *Last Edit: September 17, 2020, 07:40:40 pm by abyrvalg* »

Report to moderator Logged

The following users thanked this post: smgvbest, suj

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #158 on:** September 17, 2020, 08:44:58 pm »

Quote from: suj on September 17, 2020, 07:28:08 pm

> The timeout is very short, it looks like 0.5 seconds maybe. These are probably those marked with 05, because the transmission stops for a moment at this point.

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 5.00
```

```
@(#)LDS Rev: 3.02 - Module Incremental (Sep  9 2003)
@(#)Linked: Sep  9 2003 14:46:44

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
        End    = 0xa007fa3
```

05

Code: [Select]

```
>>> mainMain()
 text segment:          0x4011000 thru 0x4435e14 ( 424e14 bytes)
data segment:           0x4600000 thru 0x476dd88 ( 16dd88 bytes)
bss  segment:           0x476dd88 thru 0x48bcce8 ( 14ef60 bytes)

ROM size:               0x00592b9c ( 592b9c bytes of 4194304 max.)

memory pool (all):      0x048bcce8 thru 0x05ffffff (24392472 bytes)
Calling start_psos() ...
>>>> debug() process starting
DLP Loaded - Power Suite Utilities, A.06.05, Nov 21 2003 15:45:40
```

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #159 on:** September 17, 2020, 08:48:01 pm »

Quote from: abyrvalg on September 17, 2020, 07:38:04 pm

> I think this should be done with a software, not manually. Short timeout, non-printable characters - this is not for humans.
> But. If you have a terminal software capable of sending a 06 char you don't need to wait for 05 and react fast - just send that 06 continuously from power on until you see ROM Monitor command prompt.

And we're in, normal boot, SecureCRT set to expect a 0x05 and send a 0x06 in response

What next?

Code: [Select]

```
***** Mosquito Bootrom *****
Copyright 1988-1997,
Hewlett-Packard Company, all rights reserved.

@(#)HEWLETT-PACKARD, E4401 Bootrom, 5.00
@(#)LDS Rev: 3.02 - Module Incremental (Sep  9 2003)
@(#)Linked: Sep  9 2003 14:46:44

Bootrom Checksum ...
Bootrom DRAM:     Testing 69632 bytes at 0x04000000
Non Destructive SRAM Test ...
Main Firmware DRAM:     Testing 33484800 bytes at 0x04011000
Main FW Checksum ...
Self-tests complete.SRAM selftest results:
        Start  = 0xa000000
        End    = 0xa007fa3
```

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #160 on:** September 17, 2020, 08:50:28 pm »

Quote from: smgvbest on September 17, 2020, 08:48:01 pm

> What next?

"In like Flynn...."

Get us the memdump. You can make from 0x0401 1000 up to 0x0490 0000.

Great progress from abyrvalg!

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #161 on:** September 17, 2020, 08:54:10 pm »
Say Thanks Reply Quote

Now I'm in the monitor software too. I will try memory dump.
« *Last Edit: September 17, 2020, 09:03:31 pm by suj* »

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #162 on:** September 17, 2020, 09:03:51 pm »
Say Thanks Reply Quote

> **Quote from: tv84 on September 17, 2020, 08:50:28 pm**
>
> > **Quote from: smgvbest on September 17, 2020, 08:48:01 pm**
> >
> > What next?
>
> "In like Flynn...."
>
> Get us the memdump. You can make from 0x0401 1000 up to 0x0490 0000.
>
> Great progress from abyrvalg!

Given it looks like it interupted the flash did it have a chance to copy it?
can we dump a smaller segment to verify before spending many hours reading out something that may not be good?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #163 on:** September 17, 2020, 09:35:43 pm »
Say Thanks Reply Quote

IMO there is no point in 0x4011000 dump, that should be an exact copy of ESAFW image. I see BootROM getting the image size from the same offset 0x38 (from flash at C000000), then just copying that amount of bytes from C000000 to 4011000. Dumping first 0x80-0x100 bytes and comparing them against ESAFW start should be enough to verify this.

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #164 on:** September 17, 2020, 10:10:15 pm »
Say Thanks Reply Quote

> **Quote from: abyrvalg on September 17, 2020, 09:35:43 pm**
>
> IMO there is no point in 0x4011000 dump, that should be an exact copy of ESAFW image. I see BootROM getting the image size from the same offset 0x38 (from flash at C000000), then just copying that amount of bytes from C000000 to 4011000. Dumping first 0x80-0x100 bytes and comparing them against ESAFW start should be enough to verify this.

What's our next step then?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #165 on:** September 18, 2020, 07:33:40 am »
Say Thanks Reply Quote

> **Quote from: smgvbest on September 17, 2020, 10:10:15 pm**
>
> What's our next step then?

Posts: 2380
Country:

OK, do a memdump from 0x045A 0000 up to 0x0490 0000.

Before doing it, try to license 1 or 2 options, as you did before.

Your msg raised me a doubt: when you are in ROM Monitor, the equipment is not running? I ask this because we need to take the dump AFTER the licensing attempt. So if going into ROM monitor stopped the boot process we still need to finish booting.

If it's not like this then we need to setup a breakpoint. Tell me and I'll suggest an address.

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #166 on:** September 18, 2020, 07:38:00 am »

> **Quote from: tv84 on September 18, 2020, 07:33:40 am**
>
> > **Quote from: smgvbest on September 17, 2020, 10:10:15 pm**
> >
> > What's our next step then?
>
> ...when you are in ROM Monitor, the equipment is not running?...

The application does not appear to be running. Nothing is displayed on the SA screen, the off button does not work and you need to disconnect the mains plug to turn off the SA.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #167 on:** September 18, 2020, 07:45:44 am »

> **Quote from: suj on September 18, 2020, 07:38:00 am**
>
> The application does not appear to be running. Nothing is displayed on the SA screen, the off button does not work and you need to disconnect the mains plug to turn off the SA.

Damn. Then we need to place a breakpoint and try to continue booting.

@abyrvalg, any suggestion for the restart address?

If we didn't intersect boot, where would the next addresses be?

Or, if you can say where is the address of ROM Monitor function, we can patch ESAFW to safely run monitor after it has tried licensing.

« Last Edit: September 18, 2020, 07:50:09 am by tv84 »

Report to moderator Logged

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #168 on:** September 18, 2020, 10:13:48 am »

"gu" command without parameters should start the loaded image (without parameter it jumps to "image entry point" variable that is set to 4011000. That's where the normal uninterrupted start goes).
But there is one problem that I didn't noticed before: depending on some peripheral reg bit (addr 200200C, mask 100) the jump function will reload the firmware image from flash before jumping (resetting any patches). And it looks like this bit is in wrong (for us) state: "Download to Flash Selected" message in log depends on it (otherwise it will say "Download to DRAM Selected").
This hw bit looks like one of the DIP switches. Someone please try this:
- enter ROM monitor
- dump reg with "dword 200200C" command
- flip one of the DIP switches
- dump reg again to check if it is changed
- repeat with the next switch

@tv84, ROM Monitor address is D8A4. Interesting, there is a "syscall" to execute a single ROM Monitor command from the main app (at 04132418: trap #0E with arg=0A. All "trap #0E" functions are BootROM calls leading to handler at D1EC), but I see no refs to it.

« Last Edit: September 18, 2020, 10:15:29 am by abyrvalg »

Report to moderator Logged

tv84

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote

Super Contributor

Posts: 2380
Country:

« **Reply #169 on:** September 18, 2020, 10:29:45 am »

Quote from: abyrvalg on September 18, 2020, 10:13:48 am

> Interesting, there is a "syscall" to execute a single ROM Monitor command from the main app (at 04132418: trap #0E with arg=0A. All "trap #0E" functions are BootROM calls leading to handler at D1EC), but I see no refs to it.

What about patching one of the ones that we (I mean you!)know how to trigger, like arg=03, 04, 05 ?

Report to moderator Logged

abyrvalg

Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #170 on:** September 18, 2020, 10:42:28 am »

Invoking a single command via syscall would require a command string to be prepared somewhere in memory and passed to the syscall. If the goal is to capture the data section contents after a single action then it should be easier just to jump to the monitor.

Or do this:
- start the ESA normally
- do the action (enter license key)
- prepare 05-06 boot interruption
- reset the ESA to go to ROM mon
- dump the data section (4600000+)
The data section gets reinitialized by ESAFW, so if we don't start it after reboot - there will be previous content available for dump.

Another option (if you want to watch some specific var and do it many times) is to patch some debug printf to output the desired data.

Report to moderator Logged

The following users thanked this post: tv84

suj

Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #171 on:** September 18, 2020, 10:51:03 am »

give me a few minutes please I have a MB reset connected with an external button, it should work.

Report to moderator Logged

abyrvalg

Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #172 on:** September 18, 2020, 10:53:55 am »

To verify that RAM content is still alive (before going for long dumps) you can do this: dlong 4600020 - should display 04028318

Report to moderator Logged

suj

Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #173 on:** September 18, 2020, 10:56:05 am »

Quote from: abyrvalg on September 18, 2020, 10:53:55 am

> To verify that RAM content is still alive (before going for long dumps) you can do this: dlong 4600020 - should display 04028318

It's god tip. I'm not sure about DRAM refreshing after reset.

Report to moderator Logged

suj

Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #174 on:** September 18, 2020, 11:25:51 am »

Not working. I Will try one's more but after reset (using motherboard reset connector) I have this result:

Code: [Select]

```
->dlong 0x04600020
```

```
04600020  00000000 00000000 00000000 00000000   ................
```

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #175 on:** September 18, 2020, 11:45:22 am »
Say Thanks Reply Quote

I've studied the PSOS debug handler: nothing like "^C" handling there, but there is one undocumented cmd with unclear functionality: lowercase "r".

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #176 on:** September 18, 2020, 11:48:07 am »
Say Thanks Reply Quote

Ok, so we need patching. Could someone try figuring out the DIP switch responsible for Flash/DRAM boot as described here: https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3238002/#msg3238002 ?

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #177 on:** September 18, 2020, 11:48:56 am »
Say Thanks Reply Quote

I conducted an experiment. In the monitor:

Code: [Select]

```
->slong 04600020 04028318
->dlong 04600020
04600020  04028318 00000000 00000000 00000000   ................
```

Then reset and:

Code: [Select]

```
->dlong 04600020
04600020  00000000 00000000 00000000 00000000   ................
```

Clearly the contents of the DRAM cannot survive the hardware reset.

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #178 on:** September 18, 2020, 11:50:01 am »
Say Thanks Reply Quote

Quote from: abyrvalg on September 18, 2020, 11:48:07 am

> Ok, so we need patching. Could someone try figuring out the DIP switch responsible for Flash/DRAM boot as described here: https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3238002/#msg3238002 ?

I need some time. MB need to be removed to change dip-switch settings

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #179 on:** September 18, 2020, 12:03:38 pm »
Say Thanks Reply Quote

Could you try the "r" cmd (in normal mode) also?

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #180 on:** September 18, 2020, 12:06:10 pm »
Say Thanks Reply Quote

Of course. I have SA opened and its possible to change dip-switch without removing MB.

Report to moderator Logged

suj
Regular Contributor
Posts: 85

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #181 on:** September 18, 2020, 12:23:58 pm »
Say Thanks Reply Quote

Country:

"r" like RESET. But:

Code: [Select]

```
->dlong 04600020
04600020  00000000 00000000 00000000 00000000
```

Report to moderator Logged

tv84

Super Contributor

Posts: 2380

Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #182 on:** September 18, 2020, 12:38:30 pm »

Quote from: suj on September 18, 2020, 11:48:56 am

I conducted an experiment. In the monitor:

Code: [Select]

```
->slong 04600020 04028318
->dlong 04600020
04600020  04028318 00000000 00000000 00000000   ................
```

Then reset and:

Code: [Select]

```
->dlong 04600020
04600020  00000000 00000000 00000000 00000000   ................
```

Clearly the contents of the DRAM cannot survive the hardware reset.

I missed something...

@abyrvalg, when is that location filled with the 04028318 ?

Report to moderator Logged

suj

Regular Contributor

Posts: 85

Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #183 on:** September 18, 2020, 12:47:22 pm »

I can't get consistent readings from address 0x0200200c when changing dip-switches. It looks different after the reset. Sometimes, with the same settings, the readings are different depending on the time in which the reading is made.

Report to moderator Logged

abyrvalg

Frequent Contributor

Posts: 603

Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #184 on:** September 18, 2020, 01:09:53 pm »

DRAM not surviving: found the reason - BootROM clears entire DRAM at each start, so reset is not our friend

Inconsistent switch reg reading: there can be some other bits not related to switches, ignore them. We are interested in bit 8 (hex mask 0100), normally it should be 0 (for "Download to Flash Selected") and we need to switch it to 1 (for "Download to DRAM Selected").

Report to moderator Logged

abyrvalg

Frequent Contributor

Posts: 603

Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #185 on:** September 18, 2020, 01:16:07 pm »

@tv84, a function at 04011078 in ESAFW initializes data section (04600000-0476DD88) by copying from 04435E14 and clears bss section (0476DD88-048BCCE8)

Report to moderator Logged

suj

Regular Contributor

Posts: 85

Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #186 on:** September 18, 2020, 01:29:45 pm »

DIP switch #4, ON position (default)

Code: [Select]

```
->dword 0x0200200c
0200200c  0400   ..
```

DIP switch #4, OFF position

Code: [Select]

```
->dword 0x0200200c
0200200c  0500   ..
```

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #187 on:** September 18, 2020, 01:43:20 pm »

After booting with DIP switch #4 in OFF position:

Code: [Select]

```
        Start  = 0xa000000
        End    = 0xa007fa3
        Errors = 0x0
DRAM selftest results:
        Start  = 0x4011000
        End    = 0x6000000
        Errors = 0x0
hpibPort = 0x8005000
hpibPort = 0x8005000, bus Address = 19

Cache Enabled
16MBytes of FLASH

Download to DRAM Selected
ROM Monitor
Enter ? for help.
```

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #188 on:** September 18, 2020, 01:49:30 pm »

Great! That's it!
So, what we can do now:
- set DIP4 to ON (to enable ESAFW loading from flash)
- start the ESA with boot interruption
--- now we have stock ESAFW loaded from flash into DRAM, but we are in ROM Monitor
- patch ESAFW in RAM (with smem/sbyte/sword/slong)
- set DIP4 to OFF (to disable ESAFW reload in "gu" command)
- send gu command to start the patched image from DRAM

@tv84, any ideas what to patch?
I'm going to prepare some patch to jump from ESAFW back to ROM Monitor (i.e. with some of the psos debug commands) without reset to dump the data section content finally.

Report to moderator Logged

The following users thanked this post: smgvbest

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #189 on:** September 18, 2020, 01:59:54 pm »

Code: [Select]

```
sword 04139614 4ef9
sword 04139618 d8a4
gu
```

- ESAFW should start normally after this. Then, when it is running already, press "r" and you should get back to ROM Monitor with DRAM keeping the content (try dlong 04600020 there to see).

Report to moderator Logged

tv84
Super Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #190 on:** September 18, 2020, 02:29:07 pm »

Quote from: abyrvalg on September 18, 2020, 01:49:30 pm

Posts: 2380
Country:

> @tv84, any ideas what to patch?
> I'm going to prepare some patch to jump from ESAFW back to ROM Monitor (i.e. with some of the psos debug commands) without reset to dump the data section content finally.

I think I can patch the license validation ATM. Although, having some idea of how flexlm tests licenses, I don't know what are the consequences of activating all licenses.

I would prefer 1st to have the dump, so that I can search for the seeds. If I can find the seeds in the dump, the keygen will be instantaneous.

Report to moderator Logged

The following users thanked this post: smgvbest

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #191 on:** September 18, 2020, 02:37:32 pm »

Code: [Select]

```
->dlong 04600020
04600020  04028318 04028324 0402832a 04028331   .......$...*...1
```

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #192 on:** September 18, 2020, 02:45:58 pm »

My steps:
0. Set the serial terminal to 19200,8n1
1. DIP sw #4 set to ON
2. break the boot process with 0x06
3. sword 04139614 4ef9
4. sword 04139618 d8a4
5. DIP sw #4 set to OFF
6. gu
7. SA restart in normal mode
8. Press "r" and we are in the monitor now
9. Change the serial port speed.
>slong 815F4 1001A
10. Change speed of the serial terminal to 115200, 8n1

Respect for you

« *Last Edit: September 18, 2020, 04:34:35 pm by suj* »

Report to moderator Logged

The following users thanked this post: smgvbest, analogRF

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #193 on:** September 18, 2020, 02:54:58 pm »

Quote from: suj on September 18, 2020, 02:45:58 pm

> My steps:
> 1. DIP sw #4 set to ON
> 2. break the boot process with 0x06
> 3. sword 04139614 4ef9
> 4. sword 04139618 d8a4
> 5. DIP sw #4 set to OFF
> 6. gu
> 7. SA restart in normal mode
> 8. Press "r" and we are in the monitor now
>
> Respect for you

Cool, I wake up and you all have done allot.

@suj how are you flipping the DIP SW without removing the Processor Card?
a long stick??? LOL

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

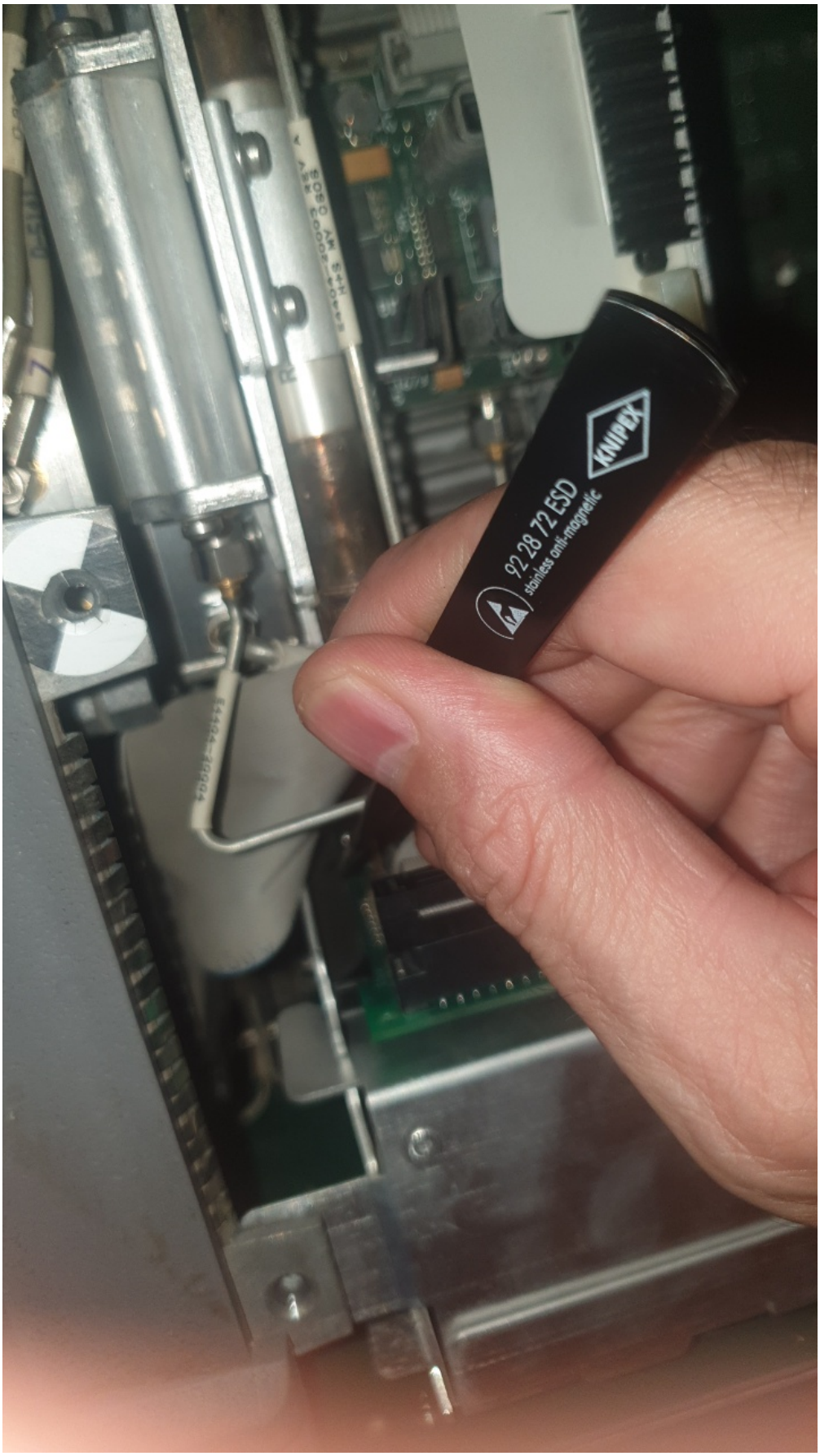
suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #194 on:** September 18, 2020, 02:59:17 pm »

Say Thanks Reply Quote

Quote from: smgvbest on September 18, 2020, 02:54:58 pm

> @suj how are you flipping the DIP SW without removing the Processor Card?
> a long stick??? LOL



20200918_165616_resized.jpg (241.73 kB, 720x1280 - viewed 152 times.)

Report to moderator Logged

The following users thanked this post: smgvbest

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #195 on:** September 18, 2020, 03:01:51 pm »

> **Quote from: suj on September 18, 2020, 02:59:17 pm**
>
> > **Quote from: smgvbest on September 18, 2020, 02:54:58 pm**
> >
> > @suj how are you flipping the DIP SW without removing the Processor Card?
> > a long stick??? LOL

Ah, right angle tweezers and coming in from that angle, thanks.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #196 on:** September 18, 2020, 03:05:10 pm »

Great!
@tv84, your turn!

Btw, does anyone know what UART IC is used in ESA? Perhaps it is possible to raise the baudrate by writing to some regs manually from the Monitor.

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #197 on:** September 18, 2020, 03:09:42 pm »

> **Quote from: abyrvalg on September 18, 2020, 03:05:10 pm**
>
> Btw, does anyone know what UART IC is used in ESA? Perhaps it is possible to raise the baudrate by writing to some regs manually from the Monitor.

It's part of the 68EN360 QICC. Its working in "companion" mode with 68LC040

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #198 on:** September 18, 2020, 03:24:26 pm »

> **Quote from: abyrvalg on September 18, 2020, 03:05:10 pm**
>
> Great!
> @tv84, your turn!
>
> Btw, does anyone know what UART IC is used in ESA? Perhaps it is possible to raise the baudrate by writing to some regs manually from the Monitor.

Given where we are I don't know if this is worth pursuing or not but there appears to be some kind of undocumented SCPI debug interface and FLASH from SCPI is a supported option as well
found it by mistake ,
hmon [device] - download into memory
defaults to loading from SCPI
I've not been able to find what [device] is supported
SCPI does not work but hmon on own loads from it
tried FLOPPY, FLASH, 0-1, A-Z, A:-C: and a few more
even things like /dev/fd0

if we want to avoid that, that's fine I defer to the Guru's here.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #199 on:** September 18, 2020, 03:46:38 pm »

> **Quote from: tv84 on September 18, 2020, 02:29:07 pm**
>
> > **Quote from: abyrvalg on September 18, 2020, 01:49:30 pm**
> >
> > @tv84, any ideas what to patch?
> > I'm going to prepare some patch to jump from ESAFW back to ROM Monitor (i.e. with some of the psos debug commands) without reset to dump the data section content finally.
>
> I think I can patch the license validation ATM. Although, having some idea of how flexlm tests licenses, I don't know what are the consequences of activating all licenses.
>
> I would prefer 1st to have the dump, so that I can search for the seeds. If I can find the seeds in the dump, the keygen will be instantaneous.

Do you want the same dump we've had before or a different one?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #200 on:** September 18, 2020, 03:52:42 pm »

I would not like to look too far into the future, but maybe it would also be worth reflecting on one of the problems. Probably most owners of the E4401 series hope to unlock the 219 option. Due to the measurement method (Y-factor), cooperation with the equipment is required. And here comes the problem under the name E4401-60123. It is not described in CLIP and there is no schematic diagram. I only found one low resolution photo on the internet. The card works with two types of noise sources: traditional sources of the 346 series and newer SNS series (N4000A, N4001A, N4002A). Cooperation with newer ones is more demanding. The noise source has a memory (probably EEPROM) with a stored ENR table and measures its temperature. Working out this can be very difficult. The type 346 sources, on the other hand, only require +28 V voltage switch. A DC/DC converter is placed on the card. One bit is required for ON/OFF keying only. The card itself should work without option 219, there is an option "Press Service, More, Noise Source (On)" in the service menu. And that could be a hook for finding the address of that bit that needs to be switched. Another thing is the card identification. FW should think the card is inserted. This is a way to create hardware that emulates part of the E4401-60123 card to work with 346 series sources. Connectors such as on the E4401 series expansion cards are available from Mouser. The E4401-60123 card itself is available in Keysight as far as I remember. Over $2800...

s-l400.jpg (27.79 kB, 400x300 - viewed 114 times.)

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #201 on:** September 18, 2020, 04:08:21 pm »

Supported hmon devices:
DOWNLOAD - this is wrong, no such device in device table

HPIB - HP's GPIB ?
RS232BINARY - self-explanatory
this command invokes a dedicated protocol handler supporting commands like "jump to address", "write to RAM", "write to flash", "start fw from flash", so nothing new there.

Baudrate:
there are 4 baud rate generators (each can be assigned to one of 4 ports independently), all of them are initialized to the same value corresponding to 19200 @25MHz source. I didn't searched for BRG->port assignment, it looks faster to try writing to divider regs one by one until we loose the communication (that will mean that speed is changed, time to reconfigure the PC port and try the new speed).

Divider register addresses:
815F0
815F4
815F8
815FC
- all are 32-bit, so use slong cmd to write to them

Values for different baud rates:
100A0 - 19200 (current setting)
10050 - 38400
10034 - 57600
1001A - 115200

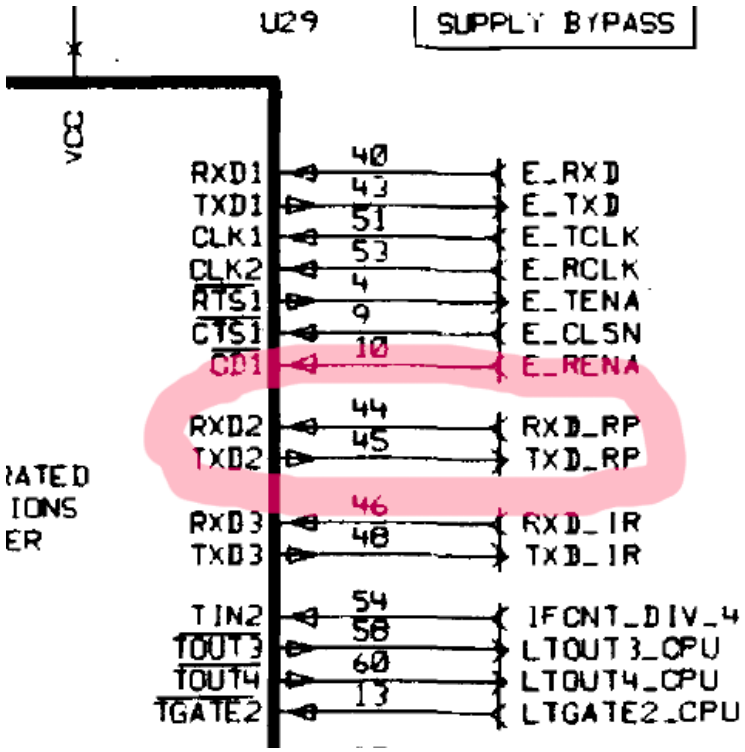
Report to moderator Logged

The following users thanked this post: tv84

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #202 on:** September 18, 2020, 04:16:00 pm »

I'll try. This is the serial port which we use.



serial.PNG (39.88 kB, 523x481 - viewed 68 times.)

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #203 on:** September 18, 2020, 04:28:10 pm »

So the correct register is 815F4

- write new value with slong
- check if communication is lost
- change the baudrate of PC to the new value
- check if communication is back
- do dumps at high speed
...
- profit!

« *Last Edit: September 18, 2020, 04:30:11 pm by abyrvalg* »

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #204 on:** September 18, 2020, 04:28:48 pm »

> **Quote from: abyrvalg on September 18, 2020, 04:08:21 pm**
>
> Supported hmon devices:
> DOWNLOAD - this is wrong, no such device in device table
> HPIB - HP's GPIB ?
> RS232BINARY - self-explanatory
> this command invokes a dedicated protocol handler supporting commands like "jump to address", "write to RAM", "write to flash", "start fw from flash", so nothing new there.
>
> Baudrate:
> there are 4 baud rate generators (each can be assigned to one of 4 ports independently), all of them are initialized to the same value corresponding to 19200 @25MHz source. I didn't searched for BRG->port assignment, it looks faster to try writing to divider regs one by one until we loose the communication (that will mean that speed is changed, time to reconfigure the PC port and try the new speed).
>
> Divider register addresses:
> 815F0
> 815F4
> 815F8
> 815FC
> - all are 32-bit, so use slong cmd to write to them
>
> Values for different baud rates:
> 100A0 - 19200 (current setting)
> 10050 - 38400
> 10034 - 57600
> 1001A - 115200

BINGO
dlong 815F4 1001A
wrote, disconnect, reconnect at 115200

btw:
dlong 815f0 1001a loose connect and can not reconnect

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #205 on:** September 18, 2020, 04:34:46 pm »

Great!
Looks like 815F0 controls some internal module-to-module port, so the CPU looses the communication with some essential part of hw.

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #206 on:** September 18, 2020, 04:38:39 pm »

I have edited my list in the post https://www.eevblog.com/forum/testgear/enabling-options-on-agilent-esa-series-e4402b-e4404b-e4405b-e4407b/msg3238350/#msg3238350. As memo.

Report to moderator Logged

The following users thanked this post: smgvbest, analogRF

tv84
Super Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #207 on:** September 18, 2020, 05:00:38 pm »

Posts: 2380
Country:

> **Quote from: smgvbest on September 18, 2020, 03:46:38 pm**
>
> Do you want the same dump we've had before or a different one?

To start let's do:

A memdump from 0x045A 0000 up to 0x0490 0000.

Before doing it, try to license 1 or 2 options, as you did before.

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #208 on:** September 18, 2020, 05:44:31 pm »

Say Thanks Reply Quote

My memory dump with real licences.

capture.7z (328.35 kB - downloaded 59 times.)

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #209 on:** September 18, 2020, 06:02:56 pm »

Say Thanks Reply Quote

> **Quote from: tv84 on September 18, 2020, 05:00:38 pm**
>
> > **Quote from: smgvbest on September 18, 2020, 03:46:38 pm**
> >
> > Do you want the same dump we've had before or a different one?
>
> To start let's do:
>
> A memdump from 0x045A 0000 up to 0x0490 0000.
>
> Before doing it, try to license 1 or 2 options, as you did before.

Order is important on this
follow the steps from @suj

dump started @ 115Kb
dbyte 045a0000 3538944

lincenses entered
AYZ 888888888888
IDS 999999999999

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #210 on:** September 18, 2020, 06:12:06 pm »

Say Thanks Reply Quote

> **Quote from: suj on September 18, 2020, 05:44:31 pm**
>
> My memory dump with real licences.

What options/keys did you have installed? might help searching for them

FWIW , according the sanatazation guide. Options/Licenses are stored in FLASH.
the FLASH on the BOARD is for FW, the FLASH SIMM is where your c: drive is an likely where options are stored permamently

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #211 on:** September 18, 2020, 06:16:35 pm »

My E4407B came to me with the following licensed options:
1D5 Hi Stability Freq Ref
1DR Narrow Resolution BW
AYZ External Mixing

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #212 on:** September 18, 2020, 06:25:53 pm »

> **Quote from: suj on September 18, 2020, 06:16:35 pm**
>
> My E4407B came to me with the following licensed options:
> 1D5 Hi Stability Freq Ref
> 1DR Narrow Resolution BW
> AYZ External Mixing

1DR Narrow Resolution BW
this is where I think we should start. most by not all SA's have the hardware for this built in

Mine has no licensed options installed, but hardware options that do not require licenses I have

1D5 Hi Stability Freq Ref
1DN TG 3.0Ghz
IDN

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #213 on:** September 18, 2020, 06:28:47 pm »

BTW, with modern serial ports supporting fractional baud rates (i.e. FTDI-based) and terminal sw supporting arbitrary baudrate numbers (not a dropdown list of fixed values) it should be possible to achieve speeds higher than 115200. The relation is: baudrate=25000000/(16*(((BRG & FFFF)>>1)+1), so the theoretical maximum is 1.56mbps. With 25MHz base frequency higher speeds deviate too much from the standard values, but fractional-capable ports should handle it. The only question is ESA's hardware limit (i.e. some slow buffers in the signal path).

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #214 on:** September 18, 2020, 06:30:49 pm »

> **Quote from: tv84 on September 18, 2020, 05:00:38 pm**
>
> > **Quote from: smgvbest on September 18, 2020, 03:46:38 pm**
> >
> > Do you want the same dump we've had before or a different one?
>
> To start let's do:
>
> A memdump from 0x045A 0000 up to 0x0490 0000.
>
> Before doing it, try to license 1 or 2 options, as you did before.

dbyte 045a0000 3538944

lincenses entered
AYZ 888888888888
IDS 999999999999

dump attached

session.7z (336.6 kB - downloaded 46 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #215 on:** September 18, 2020, 06:34:01 pm »

Say Thanks Reply Quote

> **Quote from: abyrvalg on September 18, 2020, 06:28:47 pm**
>
> BTW, with modern serial ports supporting fractional baud rates (i.e. FTDI-based) and terminal sw supporting arbitrary baudrate numbers (not a dropdown list of fixed values) it should be possible to achieve speeds higher than 115200. The relation is: baudrate=25000000/(16*(((BRG & FFFF)>>1)+1), so the theoretical maximum is 1.56mbps. With 25MHz base frequency higher speeds deviate too much from the standard values, but fractional-capable ports should handle it. The only question is ESA's hardware limit (i.e. some slow buffers in the signal path).

The RXD_RP and TXD_RP go direct to U63/MAX232ACWE

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #216 on:** September 18, 2020, 06:39:10 pm »

Say Thanks Reply Quote

From DS MAX232ACWE

Code: [Select]

```
High Data Rates
These transceivers maintain the RS-232 ±5.0V minimum
driver output voltages at data rates of over
120kbps. For data rates above 120kbps, refer to the
Transmitter Output Voltage vs. Load Capacitance
graphs in the Typical Operating Characteristics.
Communication at these high rates is easier if the
capacitive loads on the transmitters are small; i.e.,
short cables are best.
```

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #217 on:** September 18, 2020, 08:08:11 pm »

Say Thanks Reply Quote

@suj

Do you by chance have a XGecu T56 Universal programmer by chance?
I just got my PCB to try to read the FLASH SIMM
assuming it works I could send a board to you to read out yours.

unless we know the address for that FLASH SIMM and we can read out thru the monitor now?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #218 on:** September 18, 2020, 08:25:37 pm »

Say Thanks Reply Quote

I don't have this programmer. I have an older SEPROG programmer that supports some FLASH but I have to check. I doubt if such large memories. I finished using the programmer and EPROM emulator with the end of the 8051 and EPROM with a UV window era. Maybe send me your PCB gerbers? I will order from JLCPCB or locally and I will have it in a week. I would also have to order a 72 pin SIMM socket from Mouser. I haven't seen a SIMM anymore at the local main supplier, but I will check with smaller sellers.
I can also locally look for a more modern programmer. Any suggestion of type of the programmer?

Report to moderator Logged

smgvbest

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

Supporter

Posts: 623
Country:

« **Reply #219 on:** September 18, 2020, 08:43:41 pm »

Quote from: suj on September 18, 2020, 08:25:37 pm

> I don't have this programmer. I have an older SEPROG programmer that supports some FLASH but I have to check. I doubt if such large memories. I finished using the programmer and EPROM emulator with the end of the 8051 and EPROM with a UV window era. Maybe send me your PCB gerbers? I will order from JLCPCB or locally and I will have it in a week. I would also have to order a 72 pin SIMM socket from Mouser. I haven't seen a SIMM anymore at the local main supplier, but I will check with smaller sellers.
> I can also locally look for a more modern programmer. Any suggestion of type of the programmer?

I'm making some changes to the PCB to fix some minor issues I encountered. happy to share the gerbers though
this could be used with any programmer that supports the FLASH Memory but is designed for the T56 the T56 is the TL866II Plus (very popular unit) bigger brother and the direction they are going.
supports 25K+ memorys and logic IC's

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #220 on:** September 18, 2020, 08:50:40 pm »

My quick research favors TL866II+. Over 3x cheaper in my country than the T56.

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #221 on:** September 18, 2020, 09:05:33 pm »

Quote from: suj on September 18, 2020, 08:50:40 pm

> My quick research favors TL866II+. Over 3x cheaper in my country than the T56.

But it can't read the flash on the simm module
T56 has extra I/O to do it

If you want a unit for general use the TL866II+
Is a great unit

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #222 on:** September 18, 2020, 09:08:26 pm »

I performed a memory dump after a reset. It's different

capture2.7z (330.55 kB - downloaded 29 times.)

Report to moderator Logged

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #223 on:** September 18, 2020, 09:11:45 pm »

I can derive a rough memory map from QUICC's BRx/ORx regs initialization:
0: 00000000 [20000] SRAM-like, slow timing - this is BootROM as we already know
1: 04000000 [400000] DRAM-like, fast timing - this is DRAM bank 0
2: 04400000 [400000] DRAM-like, fast timing - this is DRAM bank 1
3: 02000000 [20000] SRAM-like, external timing - FPGA ? DIP switches regs are here, flash size reg, DRAM size reg
4: 08000000 [100000] SRAM-like, external timing - ??
5: 0A000000 [80000] SRAM-like, external timing - this is SRAM
6: 0C000000 [400000] SRAM-like, external timing - this is firmware flash
7: 0E000000 [20000] SRAM-like, external timing - ??

Try dumping a small piece from each of the two unknown regions (08000000, 0E000000), maybe the content will provide some ideas.

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #224 on:** September 18, 2020, 09:20:39 pm »

Say Thanks Reply Quote

Code: [Select]

```
08000000  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000010  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000020  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000030  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000040  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000050  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000060  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000070  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000080  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
08000090  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
080000a0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
080000b0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
080000c0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
080000d0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
080000e0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
080000f0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
```

Code: [Select]

```
->dbyte 0E000000 256
0e000000  05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00   ................
0e000010  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000020  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000030  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000040  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000050  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000060  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000070  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000080  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e000090  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e0000a0  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e0000b0  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e0000c0  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e0000d0  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
0e0000e0  bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00 bc 00   ................
```

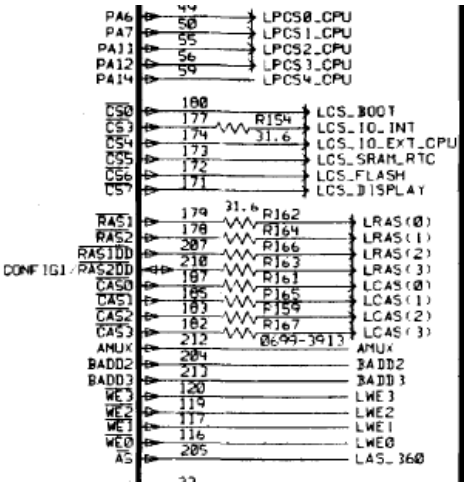
Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #225 on:** September 18, 2020, 09:31:51 pm »

Say Thanks Reply Quote

Maybe this memory map is related to CS signals from QICC?



QICC.PNG (24.73 kB, 335x309 - viewed 85 times.)

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #226 on:** September 18, 2020, 09:53:09 pm »

I'm currently analyzing the encrypt function (pretty old flexlm) and have not been following all your new debug/dump capabilities.

@abyrvalg, can we place an infinite loop in the code and prepare to do some selected dumps? can you provide the patch? Later I'll provide the address(es).

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #227 on:** September 18, 2020, 10:24:16 pm »

Quote from: tv84 on September 18, 2020, 09:53:09 pm

> I'm currently analyzing the encrypt function (pretty old flexlm) and have not been following all your new debug/dump capabilities.
>
> @abyrvalg, can we place an infinite loop in the code and prepare to do some selected dumps? can you provide the patch? Later I'll provide the address(es).

Yeh flexlm should be 6.0d so yeh very old

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #228 on:** September 18, 2020, 11:02:33 pm »

@tv84, you want to stop some function in an infinite loop before it destroys FLEXlm seeds and enter dump mode in that state?
Just patch the instruction where you want to stop to "jmp ROMMonitor":
sword YourAddr 4EF9 - "jmp imm32" opcode
slong YourAddr+2 0000D8A4 - address of ROMMonitor

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #229 on:** September 19, 2020, 09:33:48 am »

Should I try to add new licenses or in my case the installed ones are enough?

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #230 on:** September 19, 2020, 09:53:07 am »

Quote from: suj on September 19, 2020, 09:33:48 am

> Should I try to add new licenses or in my case the installed ones are enough?

The installed are enough because, when it tries to validate the installed ones (at app start), it will break into ROM Monitor so you won't be able to try a new one.

In the case of Sandra, where there is no license, I think she must force the licensing.

Report to moderator Logged

suj
Regular Contributor

Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #231 on:** September 19, 2020, 10:50:32 am »

From my calculations, the memory dump should end around 15:40 CET (13:40 GMT). Approximately 120 MB text file.

Now I go to the grocery store to do my shopping, allowing me to stay within 20 meters from my "laboratory" for the next week.

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #232 on:** September 19, 2020, 11:00:14 am »

@tv84, now I understand why you need such big dumps, your values of interest are local variables with no fixed addresses - right?
What we can do is to patch the code to save a register to some fixed unused location, then dump it from there.
A patch to save "vendor key 5" to 045FFFFC (this address is unused) and continue normally:

Code: [Select]

```
sword 043F398E 23C0
slong 043F3990 045FFFFC
slong 043F3994 60000018
+ our earlier patch to go to Mon with r key press
sword 04139614 4ef9
sword 04139618 d8a4
```

- enter any license
- press "r" to go to Mon
- dump 4 bytes from 045FFFFC

« *Last Edit: September 19, 2020, 11:04:24 am by abyrvalg* »

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #233 on:** September 19, 2020, 11:13:02 am »

Quote from: abyrvalg on September 19, 2020, 11:00:14 am

> @tv84, now I understand why you need such big dumps, your values of interest are local variables with no fixed addresses - right?

Right. Your suggestion was also on my mind. I hope we don't need it but, if we do, I will need your help. I also need to have a full confirmation of what is being hashed and, for that, the dump should provide the definitive answer.

I have a hard time recognizing how the registers of this thing work. It's almost like Blackfin!

Report to moderator Logged

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #234 on:** September 19, 2020, 11:31:57 am »

Dumping "vendor key 5" should be enough - this is old FLEXlm, the seeds are stored in VENDORCODE xored with this vk5 (look down from the location I'm patching - they verify if the seeds are "demo" 12345678 87654321 by direct xoring with this value. Various tutorials from 6.0 era says the same).

I have an universal recipe how to start feeling at home with any CISC asm - spend some time in QDSP (Hexagon) asm

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #235 on:** September 19, 2020, 11:37:43 am »

Quote from: abyrvalg on September 19, 2020, 11:31:57 am

> Dumping "vendor key 5" should be enough - this is old FLEXlm, the seeds are stored in VENDORCODE xored with this vk5 (look down from the location I'm patching - they verify if the seeds are "demo" 12345678 87654321 by direct xoring with this value. Various tutorials from 6.0 era says the same).

Sure but where is vendorcode? You still need it. With vendorcode, we would be done.

« *Last Edit: September 19, 2020, 11:44:42 am by tv84* »

Report to moderator Logged

abyrvalg
Frequent Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #236 on:** September 19, 2020, 11:45:22 am »

Posts: 603
Country:

At 04600D5C. A search for "6.0" gets you there easily. You need to have the data section initialized of course, mentioned that earlier - copy from 04435E14 to 04600000-0476DD88. But a copy of that structure can be found in the "source" area too.

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #237 on:** September 19, 2020, 12:51:20 pm »
Say Thanks Reply Quote

Stop the press! (and the dumps...)

Enc_seeds validated OK!

@suj license correctly validated.

How dumb!! How could I've missed that structure!!!!

EDIT: Mystery solved! This proc is BIG ENDIAN and my search function only searches in LITTLE ENDIAN (will correct it)! Sorry all for all the trouble but it was a new experience. A special recognition to @abyrvalg. Amazing talent!
« *Last Edit: September 19, 2020, 01:02:55 pm by tv84* »

Report to moderator Logged

The following users thanked this post: smgvbest, suj

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #238 on:** September 19, 2020, 01:02:54 pm »
Say Thanks Reply Quote

Quote from: tv84 on September 19, 2020, 12:51:20 pm

> Stop the press! (and the dumps...)
>
> Enc_seeds validated OK!
>
> @suj license correctly validated.
>
> How dumb!! How could I've missed that structure!!!!

Other than some banging head on wall this sounds good right?
I was just getting ready to do the dump
« *Last Edit: September 19, 2020, 01:05:30 pm by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #239 on:** September 19, 2020, 01:09:35 pm »
Say Thanks Reply Quote

Quote from: smgvbest on September 19, 2020, 01:02:54 pm

> Other than some banging head on wall this sounds good right?

AYZ EA726914DBAD

Report to moderator Logged

The following users thanked this post: smgvbest

smgvbest
Supporter

Posts: 623

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #240 on:** September 19, 2020, 01:24:05 pm »
Say Thanks Reply Quote

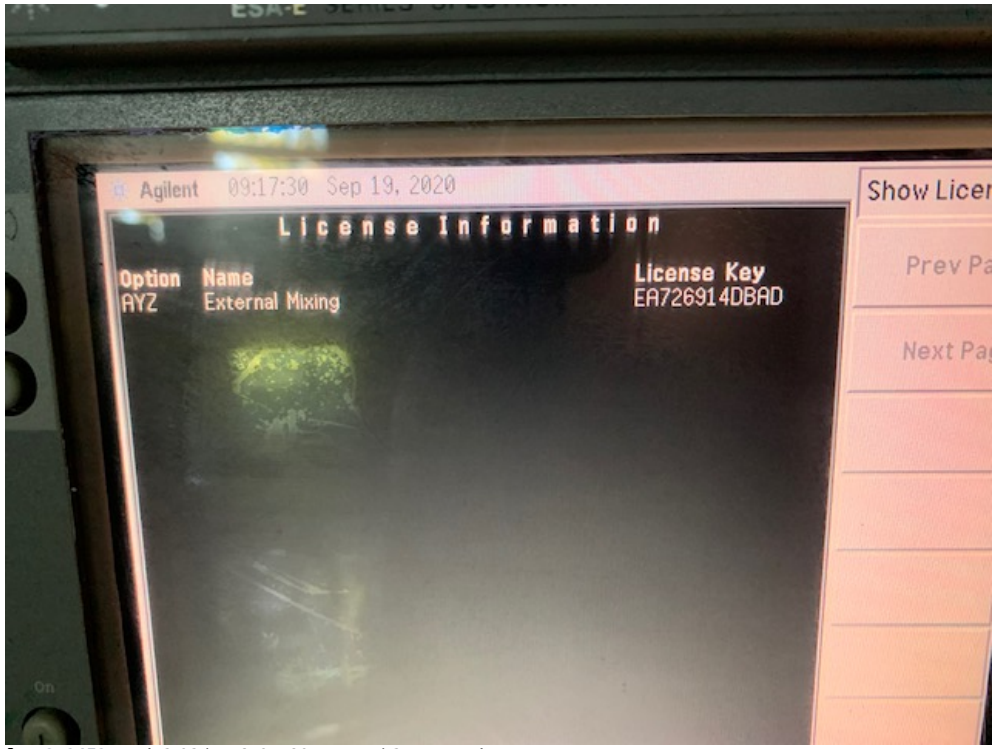
Quote from: tv84 on September 19, 2020, 01:09:35 pm

> **Quote from: smgvbest on September 19, 2020, 01:02:54 pm**
>
> > Other than some banging head on wall this sounds good right?

Country:

AYZ EA726914DBAD

I will let a picture speak for me



IMG_2652.jpg (72.93 kB, 640x480 - viewed 317 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #241 on:** September 19, 2020, 01:26:17 pm »

To check option AYZ you can go to "Input" menu and check if you can change mixer to external. To use this you must connect connector J6 from the A8A4 module and J4 from the same module to external sockets (IF in, LO Out). And you can use unpreselected harmonic mixers (for example 11970 series). To use preselected (11974) you need the frequency extension module.

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #242 on:** September 19, 2020, 01:26:36 pm »

That was a straight OPTION
can we try a personality to see if those work?
if so try Option 225

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

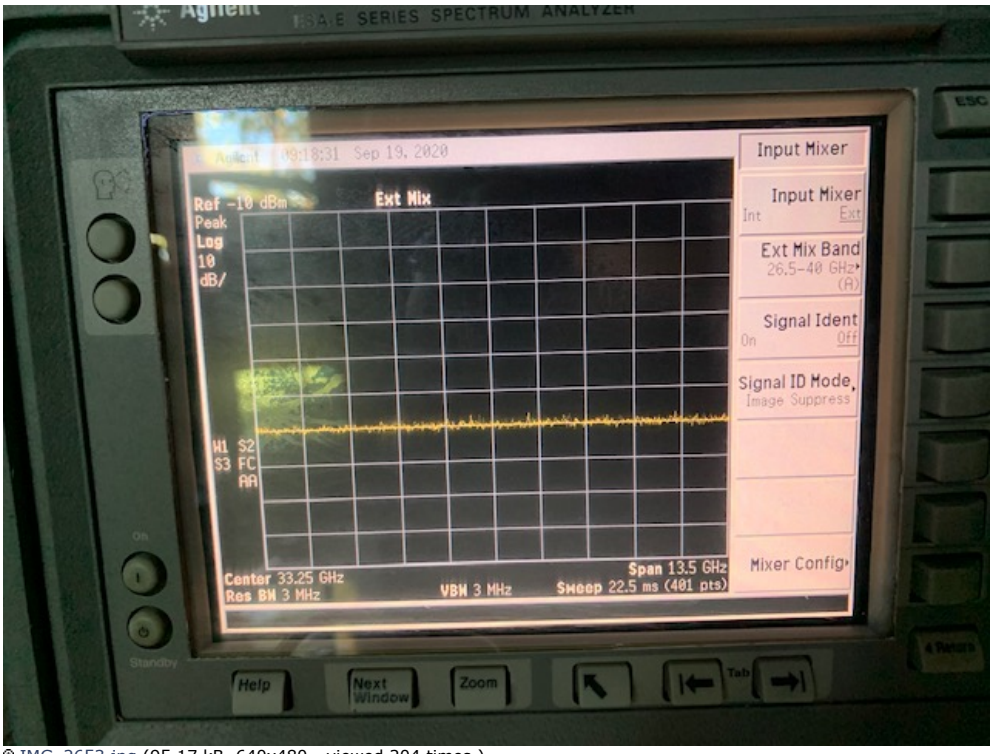
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #243 on:** September 19, 2020, 01:29:03 pm »

Quote from: suj on September 19, 2020, 01:26:17 pm

Posts: 623
Country:

> To check option AYZ you can go to "Input" menu and check if you can change mixer to external. To use this you must connect connector J6 from the A8A4 module and J4 from the same module to external sockets (IF in, LO Out). And you can use unpreselected harmonic mixers (for example 11970 series). To use preselected (11974) you need the frequency extension module.

I don't have the external mixers but I do have a 4407B with frequency extension and the menu is available



IMG_2653.jpg (95.17 kB, 640x480 - viewed 204 times.)

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

tv84

Super Contributor

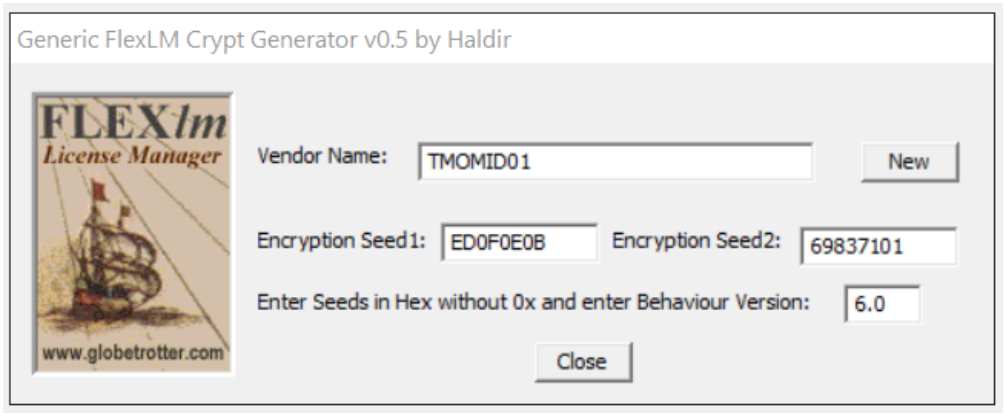
Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #244 on:** September 19, 2020, 01:56:04 pm »

Here is the fishing rod. (a little homework is always beneficial)



keygen.png (54.42 kB, 651x266 - viewed 570 times.)

Report to moderator Logged

The following users thanked this post: smgvbest, ps, analogRF, pquadrat, eplpwr

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #245 on:** September 19, 2020, 02:08:14 pm »

That was a great teamwork, thanks to everyone! See you in the next "instrument improvement" thread

Report to moderator Logged

The following users thanked this post: tv84, smgvbest, suj, analogRF, andrew9875

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #246 on:** September 19, 2020, 02:15:20 pm »

> **Quote from: abyrvalg on September 19, 2020, 02:08:14 pm**
>
> That was a great teamwork, thanks to everyone! See you in the next "instrument improvement" thread

Sure it was. Always a pleasure when it is like this. smgvbest and suj also had a special recognition for all their hard work.

I've just checked a BAC personality and all is good! See you in next quest (now with BigEnd activated!).

Report to moderator Logged

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #247 on:** September 19, 2020, 02:20:54 pm »

A big thank you to the whole team. You are geniuses!
I will now work on addressing cards via the E4401. When I have conclusions, I will ask you for help in finding this I/O address that allows to turn the noise source on and off.

EDIT
If you are looking for a challenge, I am always ready to provide support. LE, BE who wants what...

lab1.jpg (154.04 kB, 1280x720 - viewed 260 times.)

lab2.jpg (115.8 kB, 1280x720 - viewed 211 times.)

« *Last Edit: September 19, 2020, 02:35:57 pm by suj* »

Report to moderator Logged

The following users thanked this post: tv84

abyrvalg
Frequent Contributor
Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #248 on:** September 19, 2020, 03:50:15 pm »

Some info on card addressing:
there are 8 "I/O slots" (0-7), each one gets an address window at 08000000+0x4000*slot_number
register at BASE+3FFE (size: byte) looks like "device type":
1 - HPIB adapter
4 - floppy controller
Edit: other card types recognized by ESAFW:
6
8
3, 7, 10 - some similar types handled by common code

« *Last Edit: September 19, 2020, 04:13:21 pm by abyrvalg* »

Report to moderator Logged

tv84
Super Contributor
Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #249 on:** September 19, 2020, 04:14:49 pm »

This can also be used in the old **E44xxB ESG Signal Generators**.

Just checked.

Report to moderator Logged

The following users thanked this post: analogRF, eplpwr

suj
Regular Contributor
Posts: 85
Country:

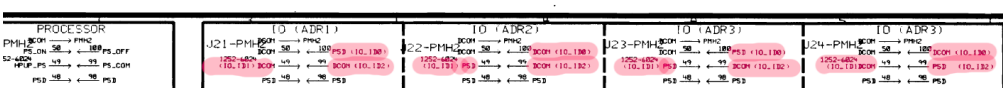
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #250 on:** September 19, 2020, 04:48:06 pm »

Quote from: abyrvalg on September 19, 2020, 03:50:15 pm

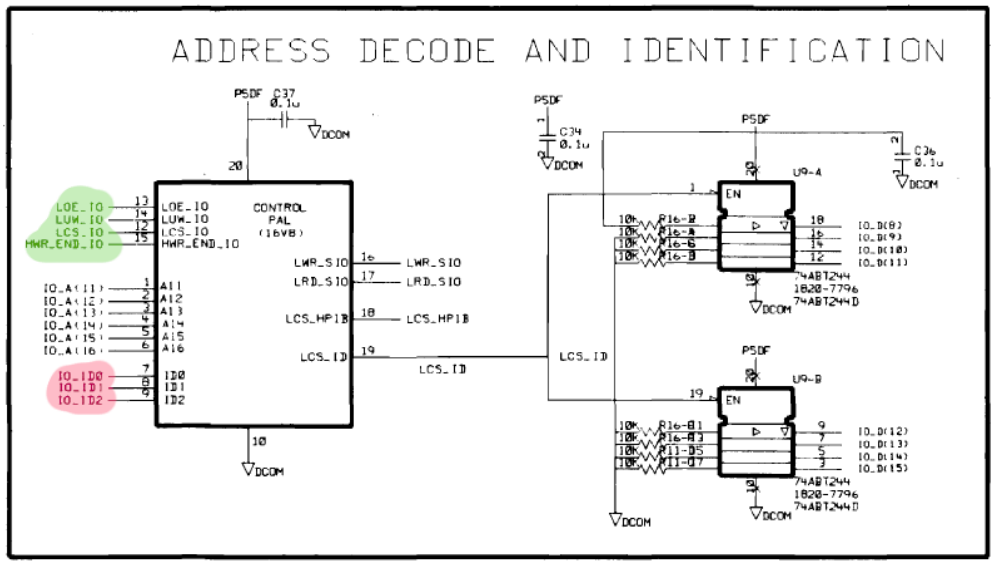
> Some info on card addressing:
> there are 8 "I/O slots" (0-7), each one gets an address window at 08000000+0x4000*slot_number
> register at BASE+3FFE (size: byte) looks like "device type":
> 1 - HPIB adapter
> 4 - floppy controller
> Edit: other card types recognized by ESAFW:
> 6
> 8
> 3, 7, 10 - some similar types handled by common code

My first analyzes:
1. Backplane is hardcoded, card known in whitch slot is inserted (red)

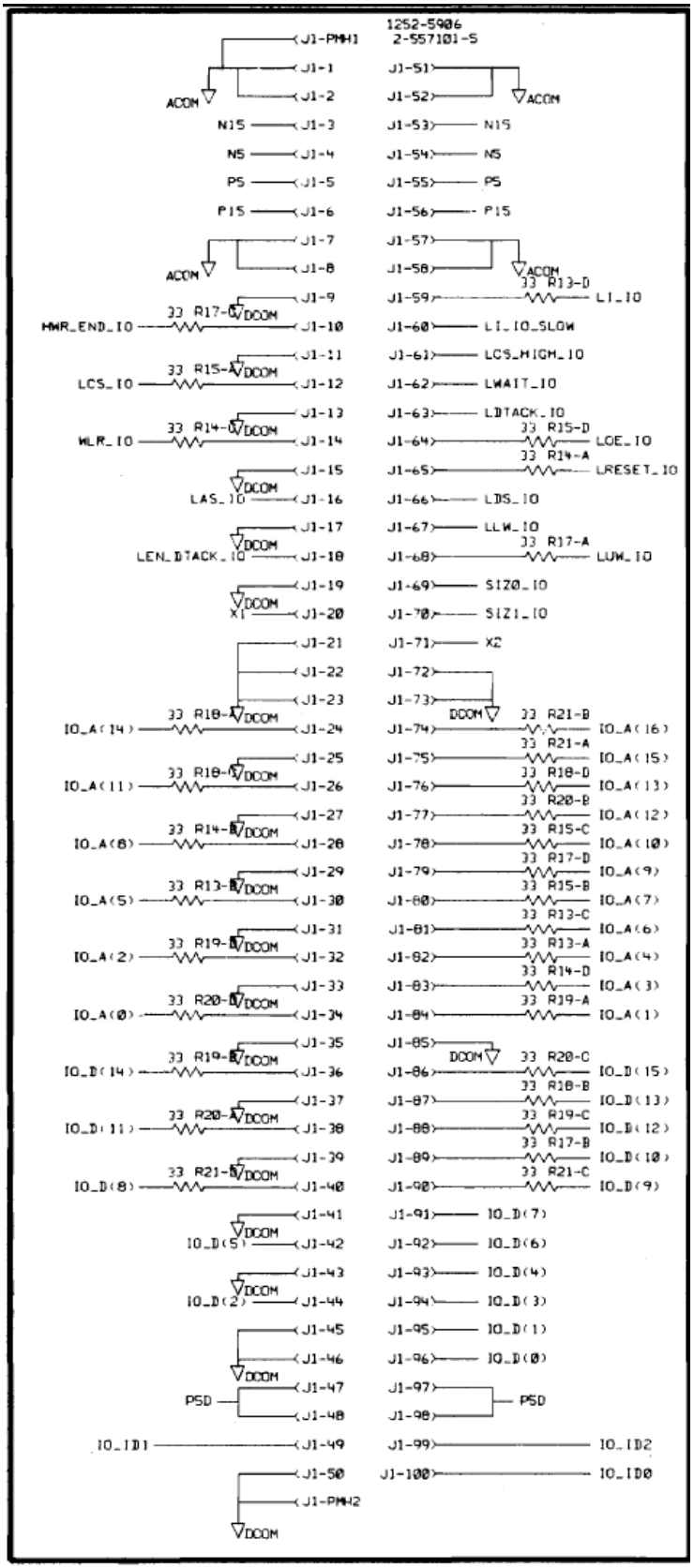
2. Adress decode and initialization. For example GPIB/Parallel card (red/green)
3. Signals for above at the cpu card (green)



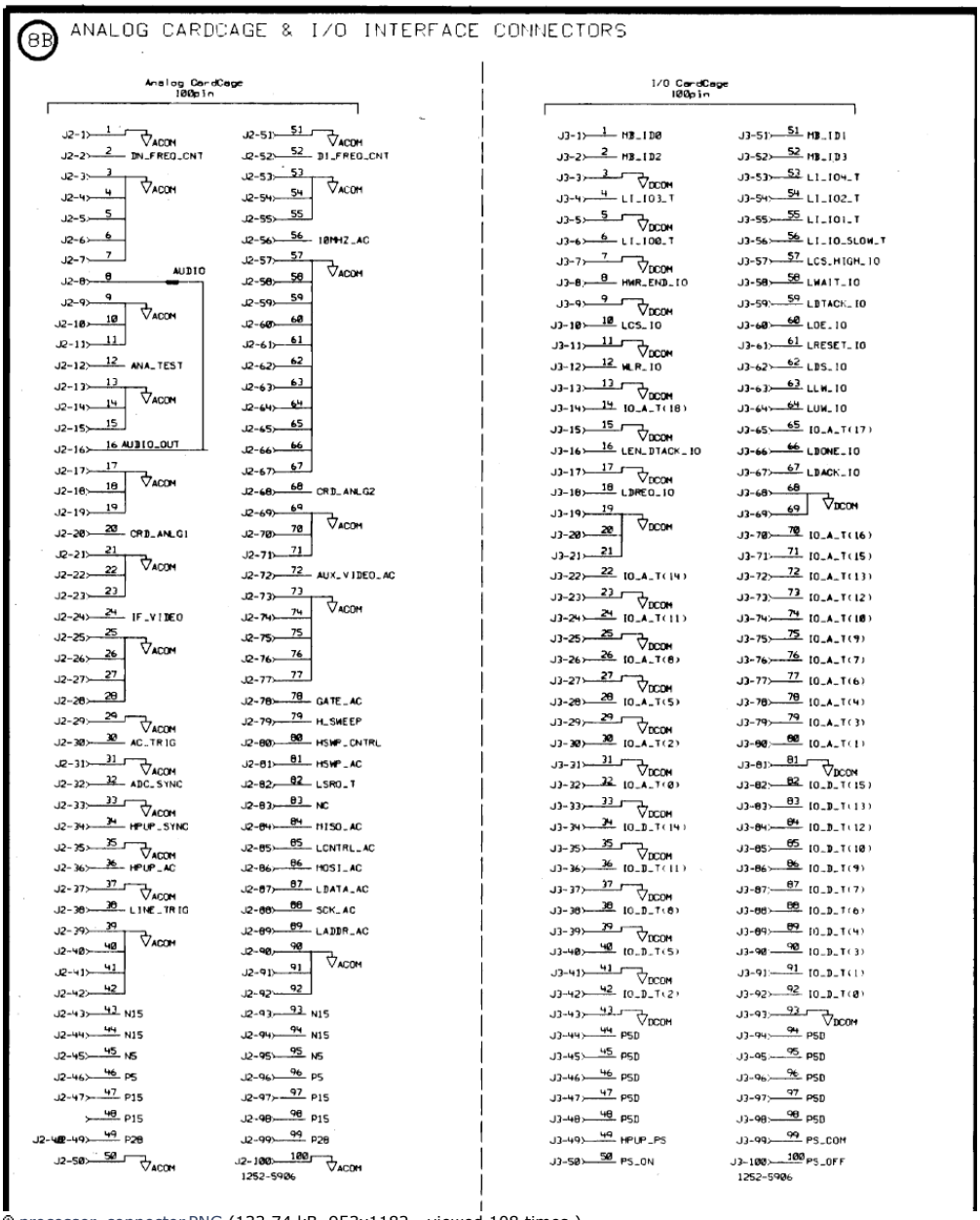
Backplane.PNG (48.01 kB, 1409x162 - viewed 103 times.)



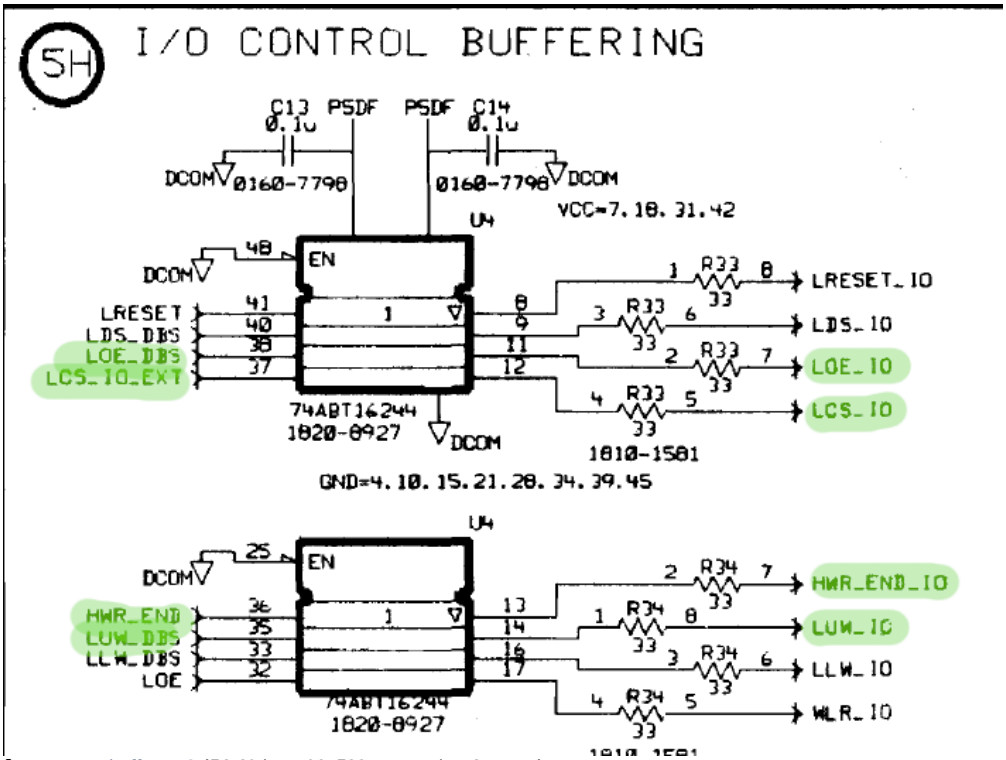
GPIB_Parallel_1.PNG (56.95 kB, 799x459 - viewed 160 times.)



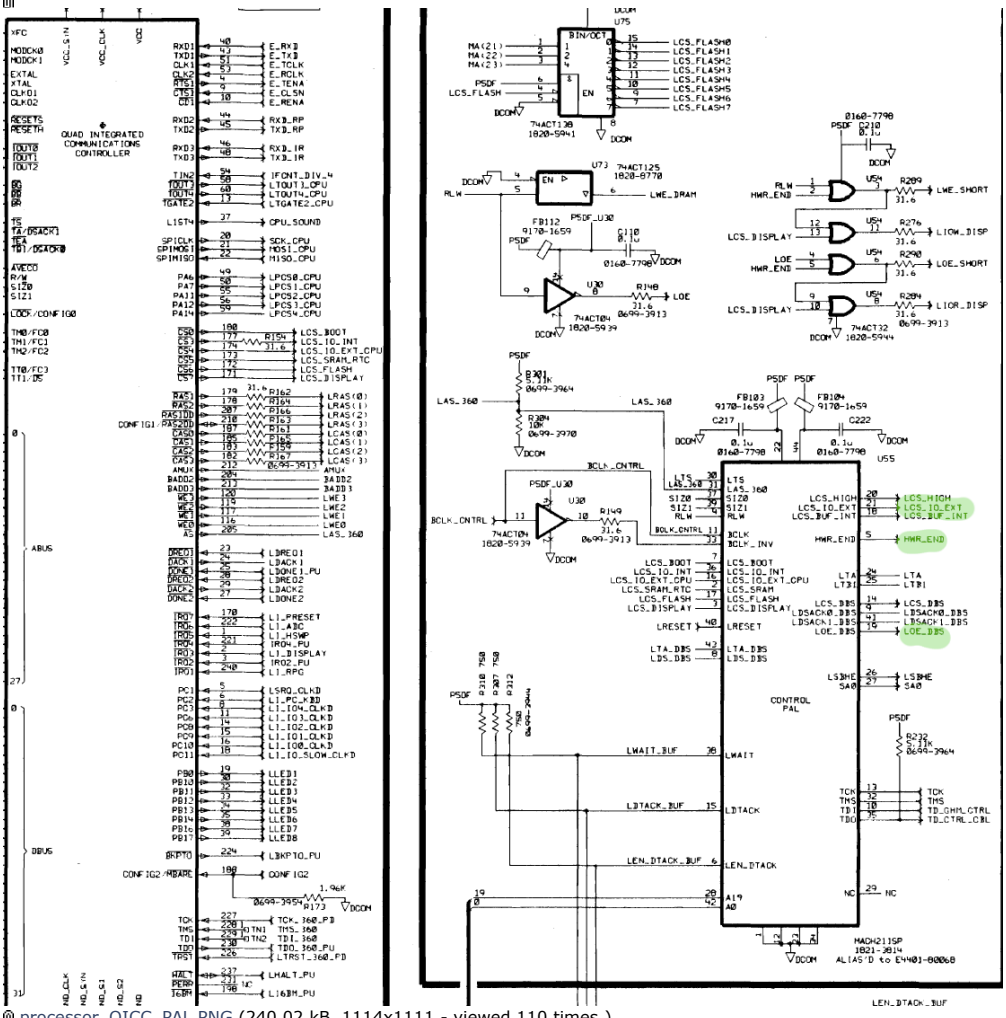
GPIB_Parallel_connector.PNG (65.49 kB, 475x1083 - viewed 128 times.)



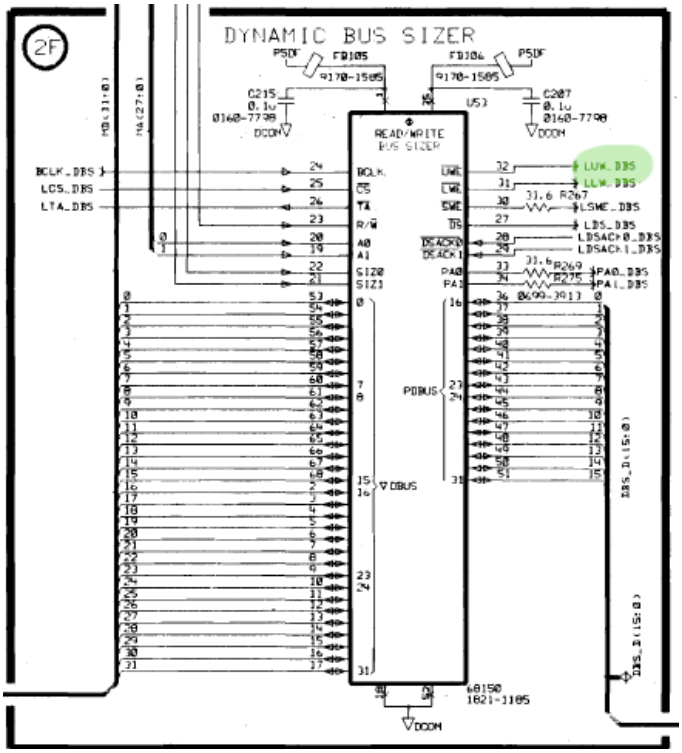
processor_connector.PNG (133.74 kB, 953x1182 - viewed 108 times.)



processor_buffer.PNG (56.69 kB, 708x532 - viewed 116 times.)



processor_QICC_PAL.PNG (240.02 kB, 1114x1111 - viewed 110 times.)



processor_68150.PNG (83.04 kB, 438x483 - viewed 113 times.)

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #251 on:** September 19, 2020, 05:06:15 pm »

Say Thanks Reply Quote

Just got back from work, amazing whats gets done when I am tied up

@tv84
@abyrvalg

you both are awesome!! thanks for the hard work
I would love to have a PM chat to understand a bit of how you do this, it intrigues me

@suj thank you for your help as well

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

abyrvalg
Frequent Contributor

Posts: 603
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #252 on:** September 19, 2020, 05:13:10 pm »

Say Thanks Reply Quote

BootROM HPIB init loops through 0-7 slot numbers, getting a byte from 08000000+4000*slot+3FFE and looking for 01 value, then uses base address of the matched slot for all further IO operations. Same is for floppy (but looking for value 04). Not sure if all slots are equal, maybe some card types must be installed in a specific slot to get i.e. right RF connections, but they are still identified by that +3FFE byte in sw, no hardcoded slots there.

Report to moderator Logged

smgvbest
Supporter

Posts: 623

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #253 on:** September 19, 2020, 07:45:21 pm »

Say Thanks Reply Quote

Quote from: abyrvalg on September 19, 2020, 05:13:10 pm

> BootROM HPIB init loops through 0-7 slot numbers, getting a byte from 08000000+4000*slot+3FFE and looking for 01 value, then uses base address of the matched slot for all further IO operations. Same is for floppy (but looking for value 04). Not sure if all slots are equal, maybe some card types must be installed in a specific slot to get i.e. right RF connections, but they are still identified by that +3FFE byte in sw, no hardcoded slots there.

Country:

Each IO card has a 93c66 eeprom on board used to identification and some store calibration data for that card.
i wonder if that address is the address used for the eeprom and getting that byte?

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #254 on:** September 21, 2020, 09:03:43 am »

Try to start from this point:
https://www.eevblog.com/forum/testgear/hp-agilent-e4433b-esg-d-series-signal-generator-250khz-4-0ghz/msg3240634/#msg3240634

Report to moderator Logged

The following users thanked this post: analogRF

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #255 on:** September 21, 2020, 03:21:24 pm »

Quote from: tv84 on September 04, 2020, 10:41:51 am

After a few more educated googles I arrived here.

So, we're halfway there!

The licenses should have this format:

FEATURE **202** TMOMID01 1.0 permanent uncounted **0123456789AB** HOSTID=**E1234567**

Now, we just need the seeds.

~~what does 0123456789AB represent. I am almost there~~

EDIT: I got it to work for one example that was in the posts, so I think I got it right
« *Last Edit: September 21, 2020, 03:28:38 pm by analogRF* »

Report to moderator Logged

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #256 on:** September 21, 2020, 03:27:30 pm »

I finally got it
thanks to the one example that was in the posts

Report to moderator Logged

tv84
Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #257 on:** September 21, 2020, 05:29:22 pm »

Quote from: analogRF on September 21, 2020, 03:27:30 pm

I finally got it
thanks to the one example that was in the posts

Here is the example of a good student that does his homework.

Report to moderator Logged

The following users thanked this post: analogRF

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #258 on:** September 21, 2020, 05:32:06 pm »

Quote from: tv84 on September 21, 2020, 05:29:22 pm

> **Quote from: analogRF on September 21, 2020, 03:27:30 pm**
>
> I finally got it
> thanks to the one example that was in the posts
>
> Here is the example of a good student that does his homework.

now I need to buy one of these SAs....have been trying to for quite some time with no success

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #259 on:** September 21, 2020, 05:45:10 pm »
Say Thanks Reply Quote

> **Quote from: analogRF on September 21, 2020, 05:32:06 pm**
>
> > **Quote from: tv84 on September 21, 2020, 05:29:22 pm**
> >
> > > **Quote from: analogRF on September 21, 2020, 03:27:30 pm**
> > >
> > > I finally got it
> > > thanks to the one example that was in the posts
> >
> > Here is the example of a good student that does his homework.
>
> now I need to buy one of these SAs....have been trying to for quite some time with no success

I was in same boat. Finally got one from alltest on eBay. Made an offer. Plead my case and they accepted at a bit higher than I wanted (ie could afford) to go but took it

Ended up being bricked was all. I don't think it had a bad flash. As I've now tested that flash many times and no failures

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

analogRF
Frequent Contributor
Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #260 on:** September 21, 2020, 05:58:25 pm »
Say Thanks Reply Quote

> **Quote from: smgvbest on September 21, 2020, 05:45:10 pm**
>
> > **Quote from: analogRF on September 21, 2020, 05:32:06 pm**
> >
> > > **Quote from: tv84 on September 21, 2020, 05:29:22 pm**
> > >
> > > > **Quote from: analogRF on September 21, 2020, 03:27:30 pm**
> > > >
> > > > I finally got it
> > > > thanks to the one example that was in the posts
> > >
> > > Here is the example of a good student that does his homework.
> >
> > now I need to buy one of these SAs....have been trying to for quite some time with no success
>
> I was in same boat. Finally got one from alltest on eBay. Made an offer. Plead my case and they accepted at a bit higher than I wanted (ie could afford) to go but took it
>
> Ended up being bricked was all. I don't think it had a bad flash. As I've now tested that flash many times and no failures

a bricked, broken, defective is what I dig

but still too expensive when they have the "basic" important (for me) HW options on them (1D5,AYX,BAA)

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #261 on:** September 21, 2020, 09:26:14 pm »

Say Thanks Reply Quote

> **Quote from: xymox on September 21, 2020, 08:41:52 pm**
>
> So no one wants $1000 ?
>
> Just checking..

Everything you need to do this is in this thread.
And it's fairly easy to do

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

The following users thanked this post: eplpwr

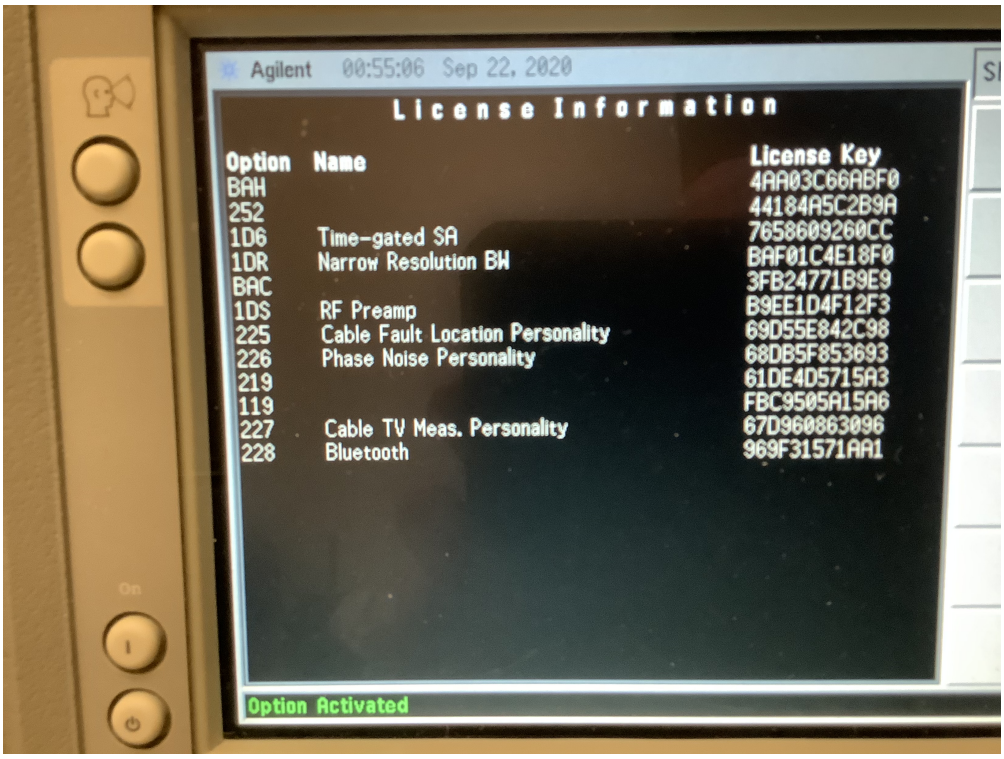
xymox
Contributor

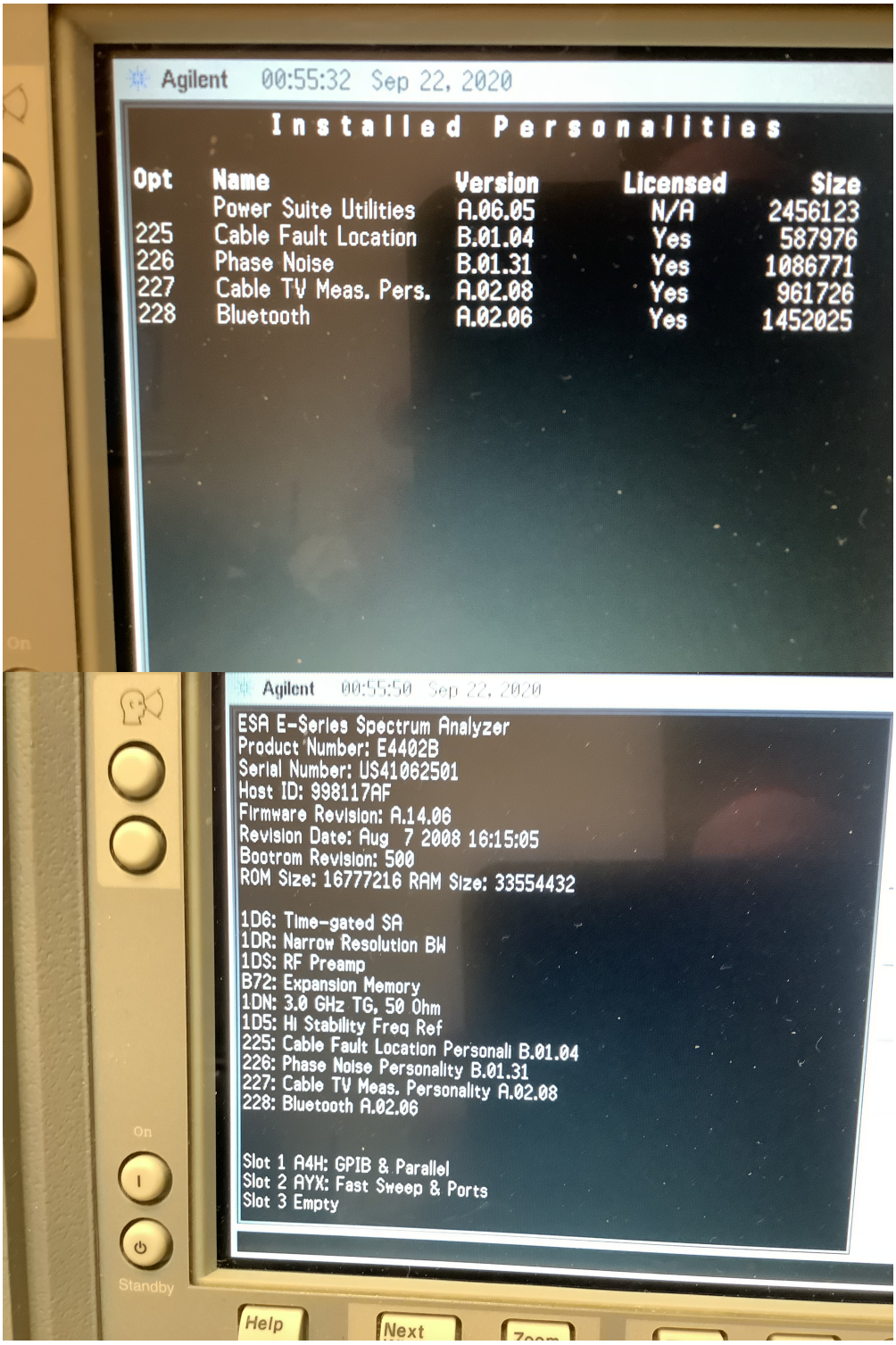
Posts: 24
Country:

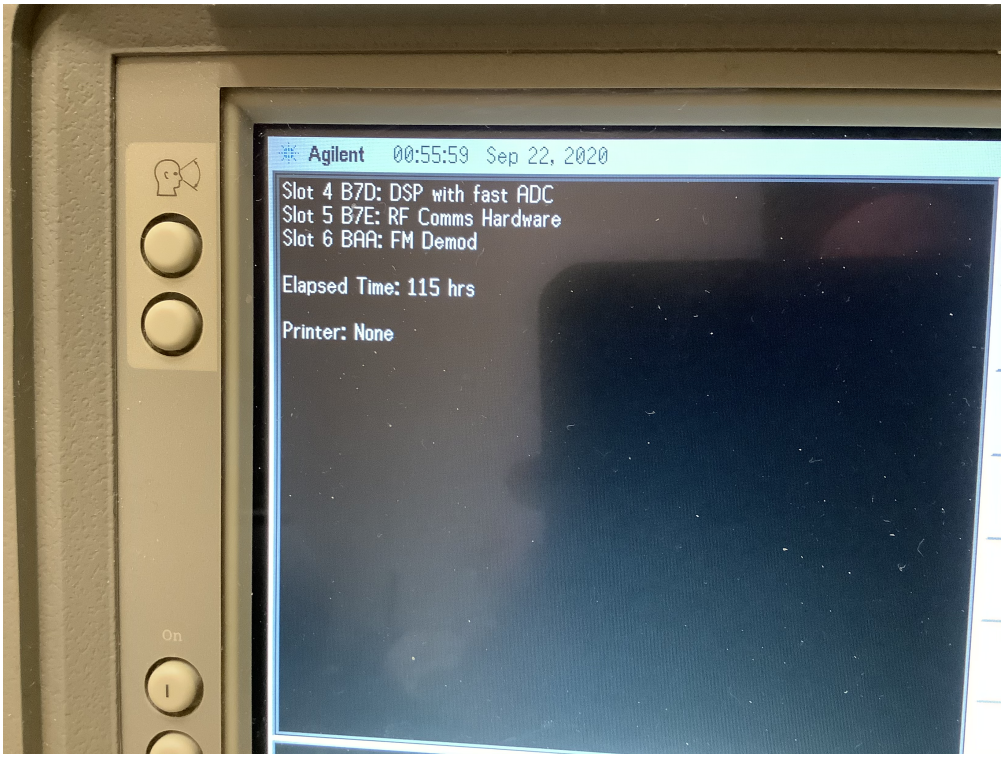
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #262 on:** September 22, 2020, 08:02:22 am »

Say Thanks Reply Quote

Well no doubt this works.. I tried EVERY option that I had hardware for.. Discovered I want a card, option 119..




Agilent 00:55:32 Sep 22, 2020
Installed Personalities
Opt Name Version Licensed Size
Power Suite Utilities A.06.05 N/A 2456123
225 Cable Fault Location B.01.04 Yes 587976
226 Phase Noise B.01.31 Yes 1086771
227 Cable TV Meas. Pers. A.02.08 Yes 961726
228 Bluetooth A.02.06 Yes 1452025
Agilent 00:55:50 Sep 22, 2020
ESA E-Series Spectrum Analyzer
Product Number: E4402B
Serial Number: US41062501
Host ID: 998117AF
Firmware Revision: A.14.06
Revision Date: Aug 7 2008 16:15:05
Bootrom Revision: 500
ROM Size: 16777216 RAM Size: 33554432
1D6: Time-gated SA
1DR: Narrow Resolution BW
1DS: RF Preamp
B72: Expansion Memory
1DN: 3.0 GHz TG, 50 Ohm
1D5: Hi Stability Freq Ref
225: Cable Fault Location Personali B.01.04
226: Phase Noise Personality B.01.31
227: Cable TV Meas. Personality A.02.08
228: Bluetooth A.02.06
Slot 1 A4H: GPIB & Parallel
Slot 2 AYX: Fast Sweep & Ports
Slot 3 Empty
On
Standby
Help
Next



« *Last Edit: September 22, 2020, 08:07:32 am by xymox* »

Report to moderator Logged

xymox

Contributor

Posts: 24

Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #263 on:** September 22, 2020, 06:46:18 pm »

NEW CHALLENGE...

One other thing that would be REALLY useful is to find the SCPI (GPIB) commands to do some adjustments (especially the frequency response adjustment.).
Keysight doesn't want to share the commands - They do use them in their own calibration software (N7800A) - but I think they don't want to enable others....

Perhaps if somebody has this calibration software (Keysight doesn't sell it anymore - they stopped selling it a few years back) - then the GPIB commands can be traced using a tracing/logging tool that logs
all GPIB activity...

The calibration software requires a license. There are older versions that run on older versions of windows that might be less protected.. https://cal.software.keysight.com/

Also I really need software that does waterfall plots and spectrograms. Logging to a computer. Etc..

There is Benchlink Web and I think that takes a key. It only runs on NT or Win 2000. Which I have setup..

Now that the SA is more unlocked I will look into all this more..

Report to moderator Logged

suj

Regular Contributor

Posts: 85

Country:

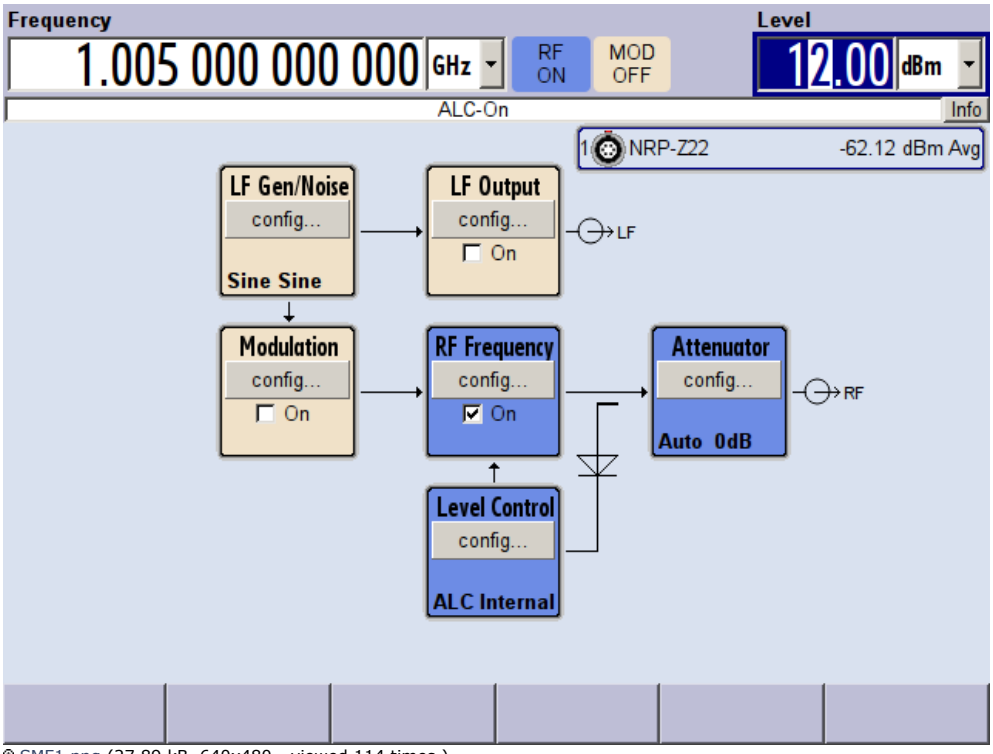
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

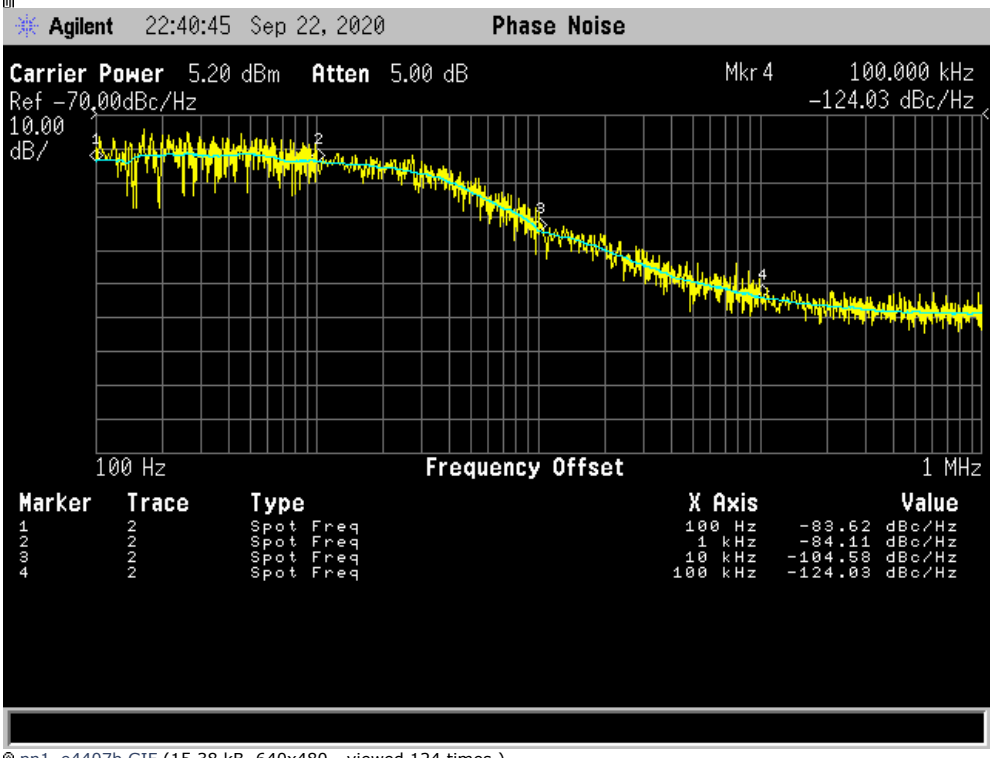
« **Reply #264 on:** September 22, 2020, 09:54:27 pm »

Today I did the initial verification of the E4407B phase noise measurement. I have put together a measuring system consisting of the following elements:
1. R&S SMF100A generator
2. Power divider Anritsu 11N50B
3. DUT1: E4407B
4. DUT2: Advantest R3681
I made the measurements at the frequency of 1.005 GHz.
The first measurement was performed without modulation.
Then I modulated the carrier frequency with the noise generator signal. With the following settings, the result should be a signal with phase noise falling by 20 dB per decade.

It is not a device with outstanding parameters, because probably HP was not supposed to be like that. After all, it could not compete with the higher-end SA (for example PSA).

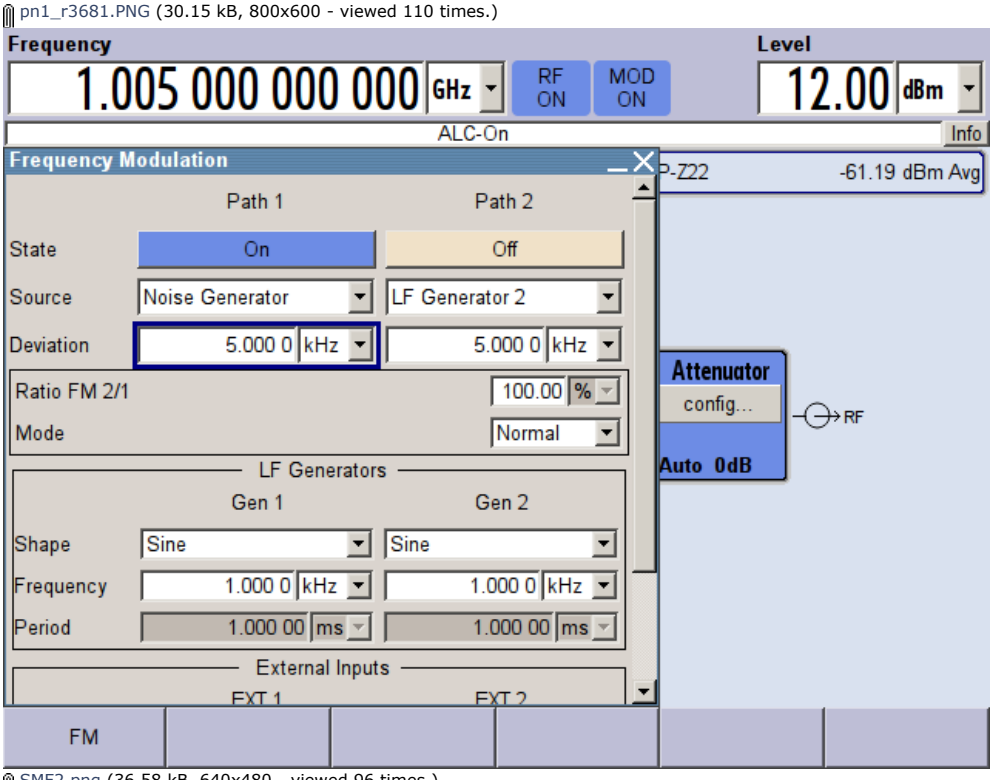


SMF1.png (27.89 kB, 640x480 - viewed 114 times.)

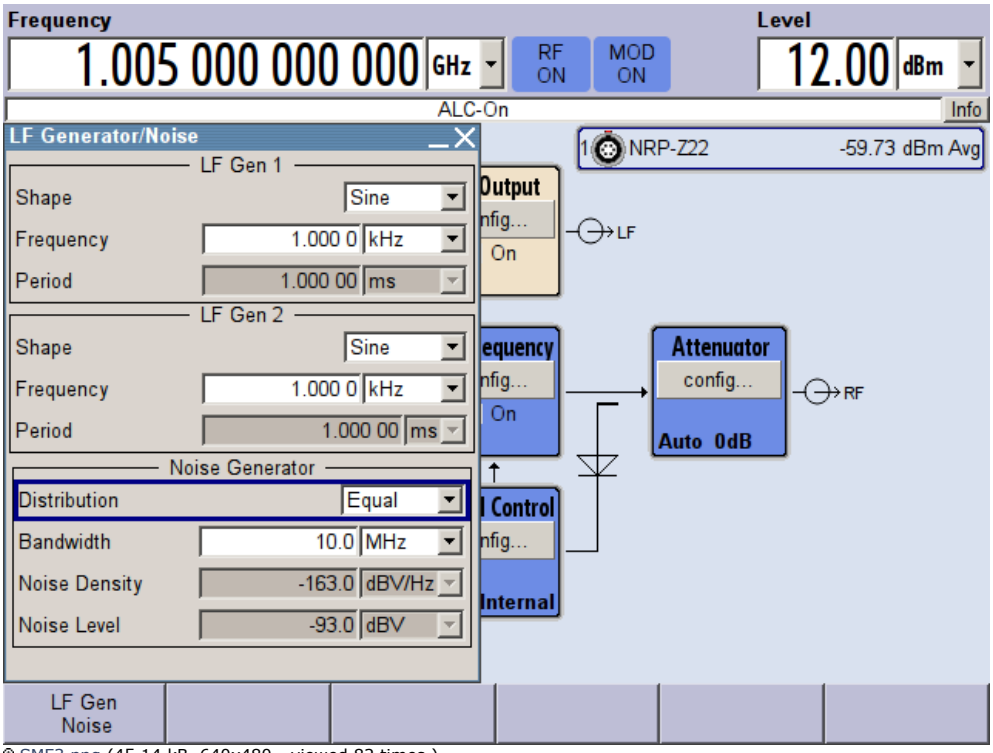


pn1_e4407b.GIF (15.38 kB, 640x480 - viewed 124 times.)

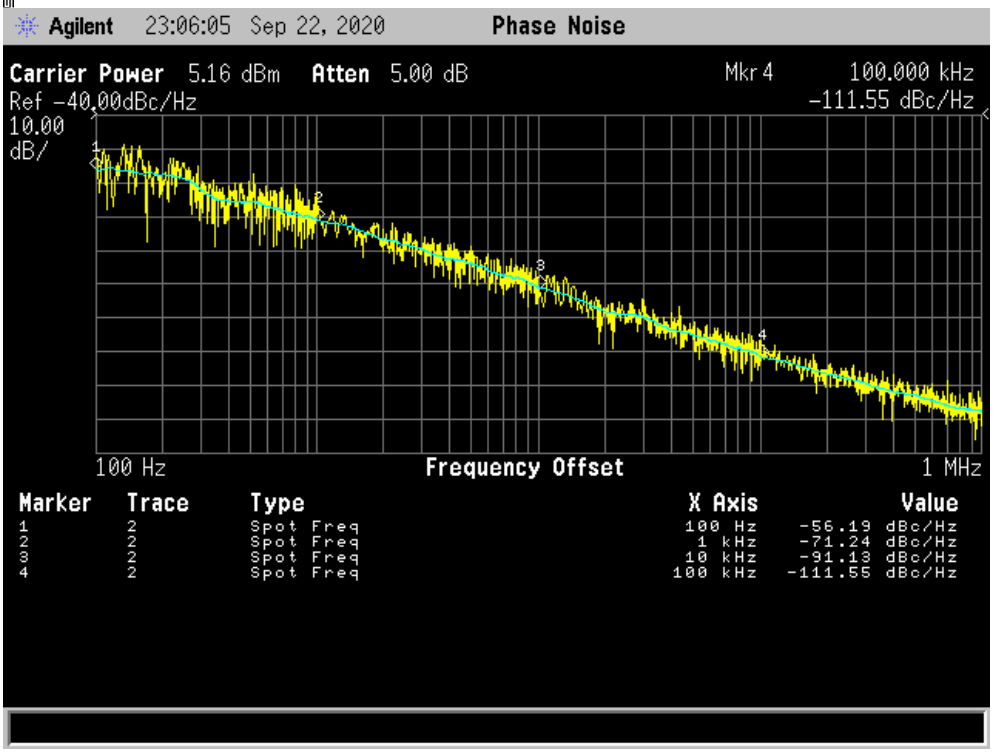
pn1_r3681.PNG (30.15 kB, 800x600 - viewed 110 times.)



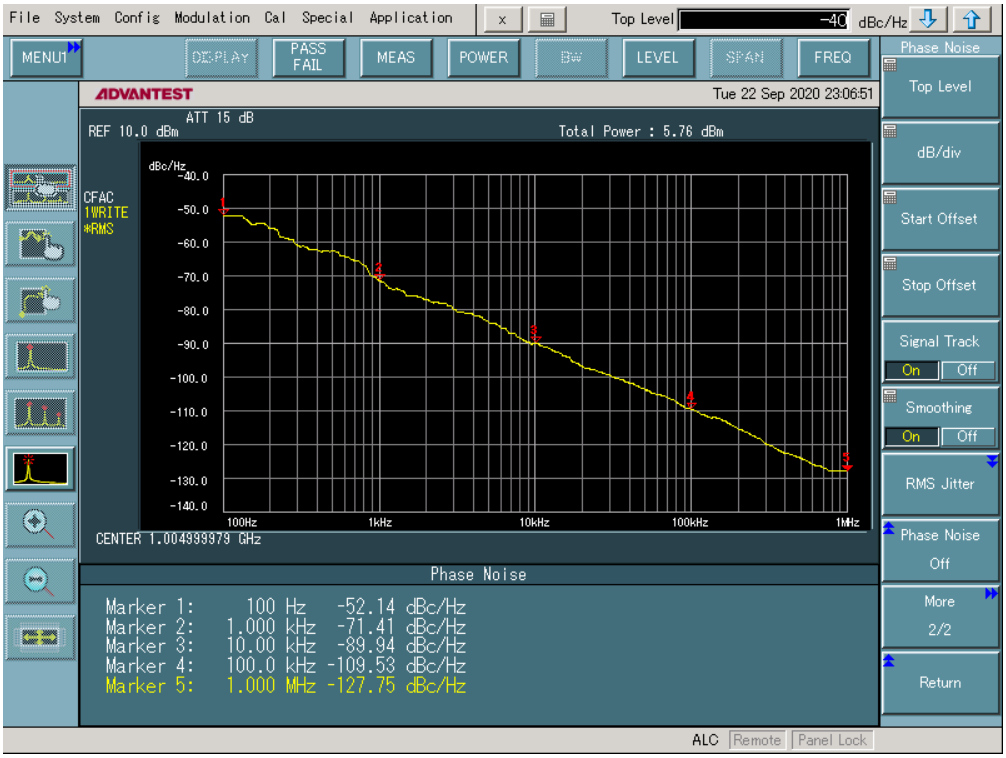
SMF2.png (36.58 kB, 640x480 - viewed 96 times.)



SMF3.png (45.14 kB, 640x480 - viewed 82 times.)



pn2_e4407b.GIF (15.79 kB, 640x480 - viewed 113 times.)



pn2_r3681.PNG (30.45 kB, 800x600 - viewed 107 times.)

Report to moderator Logged

The following users thanked this post: analogRF

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #265 on:** September 23, 2020, 12:46:46 am »

Say Thanks Reply Quote

Yes i saw that.. I was also after phase noise.. A bit dissapointing, but, its still useful

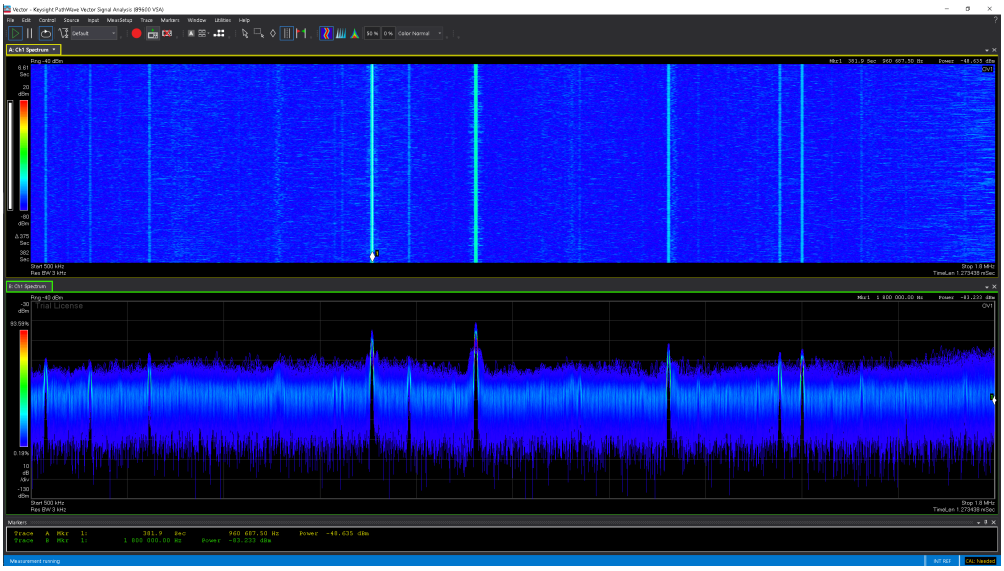
SO... I spent half my day playing with software..

I got Keysight VSA working on it. This is expensive software and seriously licensed using very modern methods. No hacking this one.. It is however REALLY powerful software.. It does exactly what I want from it.. You gotta install the Lk-VSA personality on the unit. "ESA to 89601A Software Link Utility" Its 2 floppies.

It seriously takes over the unit, complete with turning off the screen..

This software can turn the ESA into a VERY powerful device and can do things never possible from the ESA alone..

This are the AM radio stations around me..



Report to moderator Logged

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #266 on:** September 23, 2020, 01:52:54 am »

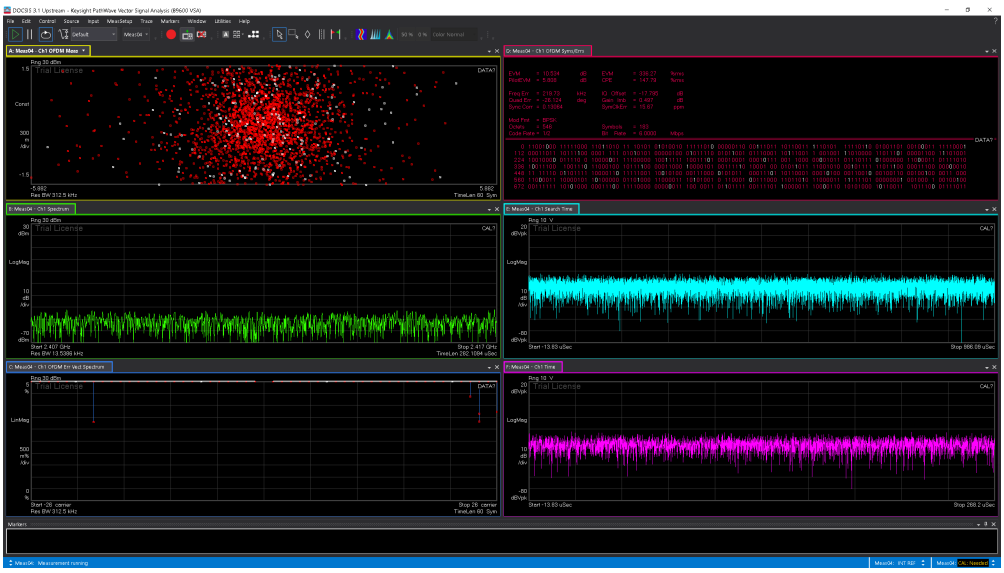
The VSA software does a great many things you can't do with just the unit.

It seems to be tryign to do 5G, all forms of Wifi, DOCSIS 3.1, OFDM, QAM just tons of stuff..

I cant quite get it to decode my cable company DOCSIS 3.1 or my own wifi.. Its trying. I just dont know enough about settings on this yet.. The trial software gives me 1 month.. So I will have some time to play with it fully...

BUT at at least $500 PER YEAR,,, this is not friendly.. Its the PER YEAR part that bothers me... The spectrogram stuff is great.. Thats all I really want..

I am a tad confuzed by one thing, but, im sure its me.. I can't get a span more then 10Mhz for some reason..



Report to moderator Logged

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #267 on:** September 23, 2020, 05:23:07 am »

Well this software is nearly unusable for my use. For some freaky reason its limited to a 10Mhz span no matter what I do. This is comeplty useless for me. At the high freq is useless. Like how do you look at wifi ? This limitation seems to be with the hardware. I can simulate other devices and they have

different max spans, but still not full. Even brand new keysight gear does not do the full span like the actual device will..

Because of this, the software seems crippled for my use.

Report to moderator Logged

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #268 on:** September 23, 2020, 06:15:35 am »

Say Thanks Reply Quote

Well that is interesting...

I have a second ESA-E Very basic.

I licensed 1DR narrow resolution bandwidth and 1D5 Hi Stability Freq Ref... These work.. I can now hit a span of 100hz and a Res BW of 1 hz.. OK Sure I enabled the software, but, I dont have those right ? WELL its performance exactly the same as my main one which has those options for real. BUT this can't be right

SO.. One thing for sure.. Its now possible to cheat.. Units could be made to look like they have more options then they actually have.. So thats not good.. However,, in this case, it added to functionality, even if its a bit wonky.

Makes me wonder what other options could be enabled this way..

Report to moderator Logged

xymox
Contributor
Posts: 24
Country:

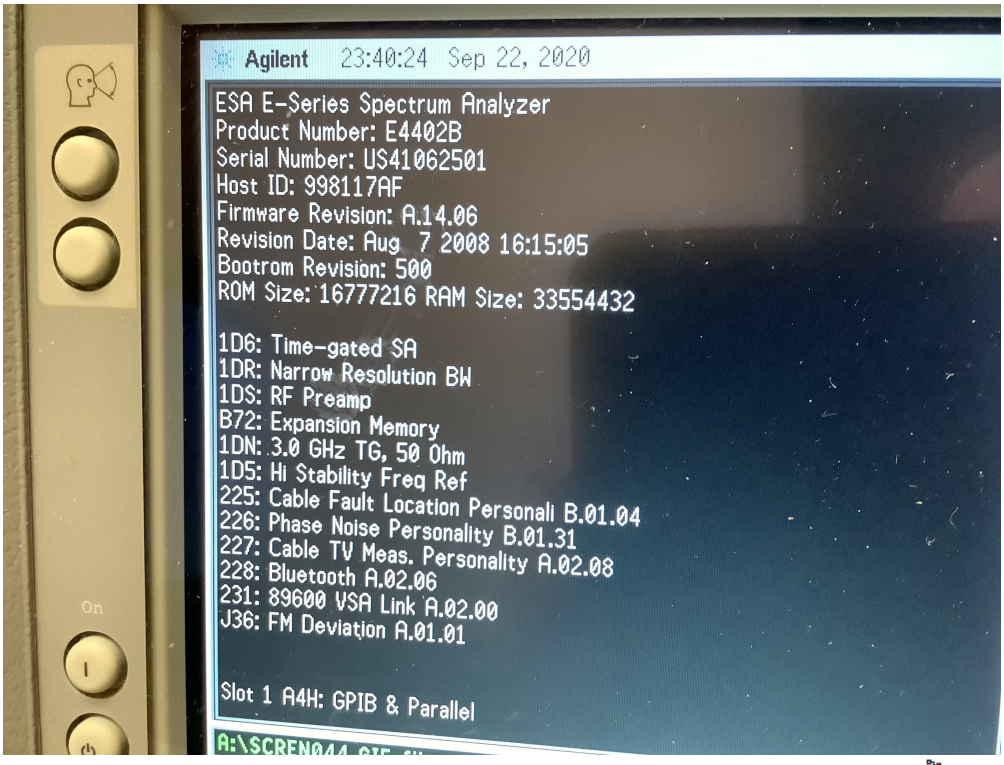
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #269 on:** September 23, 2020, 06:47:35 am »

Say Thanks Reply Quote

I truly stuffed full ESA... I cant fit anything else..

There is hardware I dont have which limits me. Low freq extension, modulation analysis board, noise measurement board..

GPIB can do a lot. I will have to explore this. I would imagine any software written for GPIB Spectrum Analyzers will work as the GPIB commands look pretty universal. Well. I can load a number of standards, so, hopefully.. VSA does not do what I need and is stupid expensive with little hope of a keygen and patch.



Report to moderator Logged

smgvbest

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

Supporter

Posts: 623
Country:

« **Reply #270 on:** September 23, 2020, 09:28:14 pm »

Quote from: xymox on September 23, 2020, 06:15:35 am

> Well that is interesting...
>
> I have a second ESA-E Very basic.
>
> I licensed 1DR narrow resolution bandwidth and 1D5 Hi Stability Freq Ref... These work.. I can now hit a span of 100hz and a Res BW of 1 hz.. OK Sure I enabled the software, but, I dont have those right ? WELL its performance exactly the same as my main one which has those options for real. BUT this can't be right
>
> SO.. One thing for sure.. Its now possible to cheat.. Units could be made to look like they have more options then they actually have.. So thats not good.. However,, in this case, it added to functionality, even if its a bit wonky.
>
> Makes me wonder what other options could be enabled this way..

There are items that are License Only.
1DR i think is one, Preamp is another past a certain serial number
there 5-6 that are license only

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

xymox

Contributor

Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #271 on:** September 24, 2020, 01:31:36 am »

I dont suppose in any of the dumps is a list of things that can be turned on ? Maybe there are some undocumented ones ? It knows all these because it populates names for them after you enable them.. You never know, maybe there is some fun option that enables something interesting.

Report to moderator Logged

smgvbest

Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #272 on:** September 24, 2020, 01:40:07 am »

Quote from: xymox on September 24, 2020, 01:31:36 am

> I dont suppose in any of the dumps is a list of things that can be turned on ? Maybe there are some undocumented ones ? It knows all these because it populates names for them after you enable them.. You never know, maybe there is some fun option that enables something interesting.

They are all in the ESAFW file and dumps
I do not recall anything thats not already listed on the keysight page

https://www.keysight.com/main/editorial.jspx?cc=US&lc=eng&ckey=277453&nid=-32406.536881907.02&id=277453

BTW: I just started a new thread in the repair forum for repairing the Tracking Generator thats getting a Source Unlevel error if anyone is interest
https://www.eevblog.com/forum/repair/e4407b-tracking-generator-repair/msg3246922/#msg3246922

« *Last Edit: September 24, 2020, 01:42:27 am by smgvbest* »

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

xymox

Contributor

Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #273 on:** September 24, 2020, 03:26:45 am »

Quote from: smgvbest on September 24, 2020, 01:40:07 am

> BTW: I just started a new thread in the repair forum for repairing the Tracking Generator thats getting a Source Unlevel error if anyone is interest

You will eventually need to calibrate it. We gotta figure out how to do that..

I am trying to get Keysight to simply quote me on TME.. I want a license for "self Maintainers" and for

a single serial number unit. They responded once and asked me what the company name was, I told them it was for personal use and they never responded again. I would pay them for this.. As long as it was not a insane number. BUT they seem to be going in the direction that will lead to the system getting hacked into. At the least the GPIB stuff that goes back and forth during calibration can be captured and easily figured out. Im going to ask one more time.

I want this https://cal.software.keysight.com/?id=2525023 under this license..
https://www.keysight.com/us/en/assets/7018-01623/data-sheets/5989-6956.pdf for 1 unit, a ESA E4402B.. Its supported..

I VASTLY prefer to use software legitly. As long as its not too expensive, I am happy to pay it.

Keysight seems to be unpleasant and stupid.

What they should do is just allow all these tools and things to go free. Real businesses are not buying these older devices, hobbyists are. Like me, a Ham radio guy.. They are NOT loosing sales to this old gear...

Maybe I need to target someone higher up the chain at Keysight..

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #274 on:** September 24, 2020, 03:45:43 am »

Say Thanks Reply Quote

Quote from: xymox on September 24, 2020, 03:26:45 am

Quote from: smgvbest on September 24, 2020, 01:40:07 am

BTW: I just started a new thread in the repair forum for repairing the Tracking Generator thats getting a Source Unlevel error if anyone is interest

You will eventually need to calibrate it. We gotta figure out how to do that..

I am trying to get Keysight to simply quote me on TME.. I want a license for "self Maintainers" and for a single serial number unit. They responded once and asked me what the company name was, I told them it was for personal use and they never responded again. I would pay them for this.. As long as it was not a insane number. BUT they seem to be going in the direction that will lead to the system getting hacked into. At the least the GPIB stuff that goes back and forth during calibration can be captured and easily figured out. Im going to ask one more time.

I want this https://cal.software.keysight.com/?id=2525023 under this license..
https://www.keysight.com/us/en/assets/7018-01623/data-sheets/5989-6956.pdf for 1 unit, a ESA E4402B.. Its supported..

I VASTLY prefer to use software legitly. As long as its not too expensive, I am happy to pay it.

Keysight seems to be unpleasant and stupid.

What they should do is just allow all these tools and things to go free. Real businesses are not buying these older devices, hobbyists are. Like me, a Ham radio guy.. They are NOT loosing sales to this old gear...

Maybe I need to target someone higher up the chain at Keysight..

Keysight is not in business to support hobbyist. that's not their business model. for TME you're looking at 5K+ i believe.
Hobbyist arent buying these usually either, at a cost of 3K+ for a broken one most hobbyist can not afford that. every now and then you find you for much less. I did, I got very lucky and the repair was simple. the TG may be a different issues. it's been repaired before. I need to figure out if the Source Unlevel is the LO Control board (i hope) or the BITG which is not documented

Far as calibration, first run a performance test to see if it need to be calibrated. All documented in the calibration guide

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

xymox
Contributor

Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #275 on:** September 24, 2020, 04:18:19 am »

Say Thanks Reply Quote

Yea I have been thru the "calibration" guide.. Hehehe.. Im still not sure how to set Course and Fine in the timebase in the service menu..

I do have something off on both my units. If I give them my rubidihum clock std 10Mhz it displays slightly off center if I set the SA for 1hz res bw and 100 hz span. Also the freq counter is off a bit..

Amplitute is reading slightly off at various frequency points.

These are not much off, but with this many years on these devices, its normal to have drift.

Also if we want to swap boards around between units and maintain these over the next 10 years we just gotta be able to calibrate them.

These calibration adjustments must also be kept in some flash. If the flash goes or gets wiped, thats it. No hope of recovery.

We gotta be able to do TME.. I can't find old versions of TME. Or maybe some old different program used to calibrate.

I have sent a nice email to Ron Nersesian. He has a awesome career that goes way back with HP. Back to the good old days of HP. I have suggested that hobbyists fuel young engineers and so thier future customers could well be buying this older gear from ebay. i suggested its helpful for EoL devices that are locked away with keys to maybe get a free online key gen process. This would fuel many hobbyists into engineers and maybe future customers. It wont hurt Keysight sales as hobbyists cannot afford to buy new gear and companies using this kind of test equipment don't buy old gear like this.

Im sure I wont get a response. BUT the email did not reflect back. So I did find the right email to use for him.

WTH... Why not try...

BTW the self calibration license has provisions for a single serial number instrument. That would have to be way cheaper then a single seat.

Maybe I can get a trial license. If so, I can capture all the GPIB..AND calibrate my unit at least once..

Report to moderator Logged

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #276 on:** September 24, 2020, 05:21:45 am »

OoooOo... TMA has a help file for the ESA series.. It has a lot of interesting things in it..

It *SEEMS* like you could set the freq limit and pick the model when you replace the processor board.. I believe there are hardware differences tho between models, so, its not JUST a setting. BUT its interesting tho.. Plus there are a lot of things in here that are interesting.. The part about processor initialization is interesting. http://www.xymox1.com/Misc/Utilities.pdf

All the adjustments you can do.. http://www.xymox1.com/Misc/Adjustments.pdf

I am still unsure if you can manually enter any values. It may be the TSE software forces hooking up automated bench gear and standards and then operates all that via GPIB and does the calibration fully automated.. This would not be useful. It would be better, for hobbyist use, that we could enter values manually.

Report to moderator Logged

xymox
Contributor
Posts: 24
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #277 on:** September 25, 2020, 12:07:59 am »

THIS is the software I want... I think... Its old too so maybe hackable.. This can do spectrograms with full width spans..

BUT its OLD... Runs on Windows 2000.. But thats fine I have a laptop of that vintage AND there is always VM..

https://www.keysight.com/en/pd-1000004487%3Aepsg%3Apro/esa-and-psa-option-230-benchlink-web-remote-control-software?pm=PL&nid=-32406.536880458&cc=US&lc=eng

Report to moderator Logged

smgvbest
Supporter

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #278 on:** September 25, 2020, 01:20:51 am »

Posts: 623
Country:

Quote from: xymox on September 25, 2020, 12:07:59 am

> THIS is the software I want... I think... Its old too so maybe hackable.. This can do spectrograms with full width spans..
>
> BUT its OLD... Runs on Windows 2000.. But thats fine I have a laptop of that vintage AND there is always VM..
>
> https://www.keysight.com/en/pd-1000004487%3Aepsg%3Apro/esa-and-psa-option-230-benchlink-web-remote-control-software?pm=PL&nid=-32406.536880458&cc=US&lc=eng

Far as I understand this one just need Option 230 enabled on the SA. you can do that.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #279 on:** September 25, 2020, 01:24:04 am »
Say Thanks Reply Quote

TME is Keysights premier package used to calibrate instruments and sold to calibration shops all over the world
I can see in any way Keysight is going to give that up to hobbyist. Hobbyist are not any major part of their sales revenue.
I would love it but I'll put my money on no reply or a negative reply

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

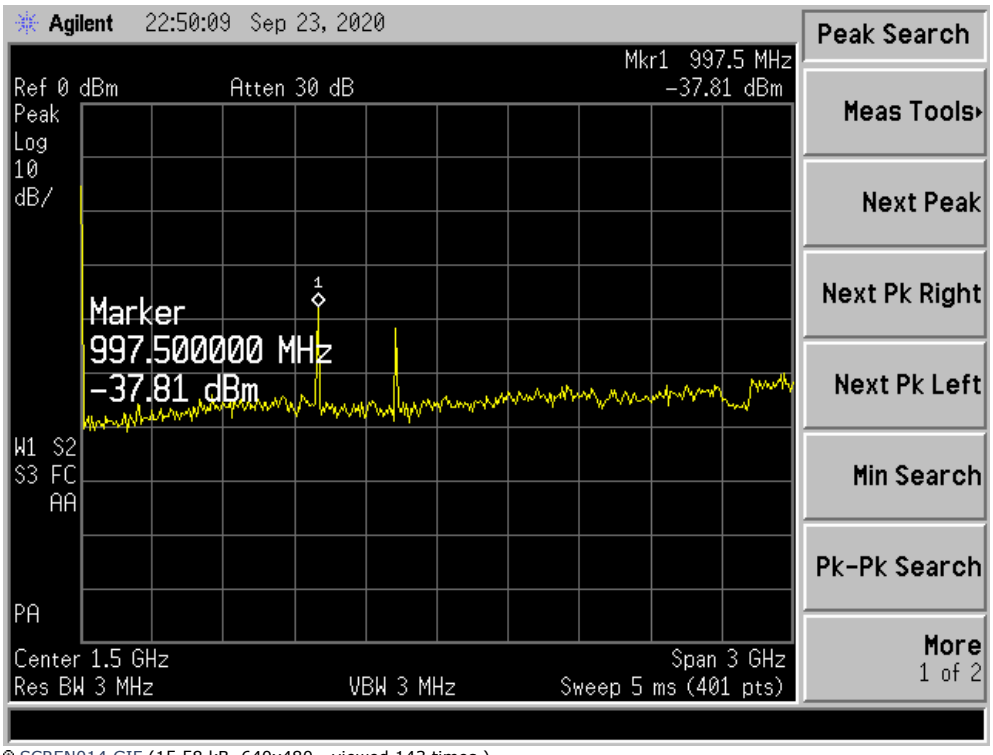
apples
Newbie
Posts: 3
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #280 on:** September 25, 2020, 10:21:58 pm »
Say Thanks Reply Quote

Just want to thank the people on this thread for their wonderful effort.

I have 3 x ESA 4402Bs that now have RF Pre-Amp which is what I needed. One of them though is showing two distinct spikes (actually holes I suppose) in the response at 997.5MHz and 1.32GHz and when you turn the RF Pre Amp, the others don't do this. Outside these gaps, the pre-amp is working fine.

Anyone know what could cause this? Loose connectors ??



SCREN014.GIF (15.58 kB, 640x480 - viewed 143 times.)

« *Last Edit: September 25, 2020, 10:23:36 pm by apples* »

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #281 on:** September 25, 2020, 10:30:44 pm »

Say Thanks Reply Quote

What's the serial number on the unit?
The preamp hardware is only installed after a certain serial number
Maybe you don't have the actual hardware

Just guessing but might be worth a check

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

analogRF
Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #282 on:** September 26, 2020, 12:59:33 am »

Say Thanks Reply Quote

Quote from: apples on September 25, 2020, 10:21:58 pm

> Just want to thank the people on this thread for their wonderful effort.
>
> I have 3 x ESA 4402Bs that now have RF Pre-Amp which is what I needed. One of them though is showing two distinct spikes (actually holes I suppose) in the response at 997.5MHz and 1.32GHz and when you turn the RF Pre Amp, the others don't do this. Outside these gaps, the pre-amp is working fine.
>
> Anyone know what could cause this? Loose connectors ??

first of all to figure out if your preamps are working, a simple test is to set your Ref Lvl to something small like -40dBm (no signal needs to be connected) and then turn on/off the preamp. your noise floor must jump up and down by about 15-20db depending on the gain of the preamp

i am not sure if those spikes are created by the preamp. maybe as Sandra said you dont actually have the hardware for it and it is creating garbage
otherwise the preamp is self oscillating!

Report to moderator Logged

analogRF

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

Frequent Contributor

Posts: 809
Country:

« **Reply #283 on:** September 26, 2020, 01:03:12 am »

this thread has been going off rail for quite some time. it must have been pretty much closed after the final solution. things that came after that, though interesting and useful, should have been in threads of their own.

Report to moderator Logged

apples

Newbie

Posts: 3
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #284 on:** September 26, 2020, 06:40:27 am »

@analogRF -fair point.

I considered it was somewhat relevant as others are sure to use the method for this and what I'm seeing might just be a limitation of just turning the 1DS option on without having the correct re-calibration software.

For completeness, I can confirm that in my case at least the preamp IS installed and IS working as expected apart from these 'spikes'. I'll carry on the conversation as necessary on a new thread.

Report to moderator Logged

tv84

Super Contributor

Posts: 2380
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #285 on:** September 26, 2020, 07:57:44 am »

> **Quote from: analogRF on September 26, 2020, 01:03:12 am**
>
> this thread has been going off rail for quite some time. it must have been pretty much closed after the final solution. things that came after that, though interesting and useful, should have been in threads of their own.

I think we are now seeing the consequences of enabling options on Agilent ESA series so not much of a derailing here, IMHO. Of course, some themes may deserve a thread on their own.

Report to moderator Logged

analogRF

Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #286 on:** September 30, 2020, 06:58:11 pm »

let me pose a fresh and more useful and interesting challenge with regard to these analyzers:

how can we convert E4404B (6.7GHz) to E4405B (13.2GHz) if at all?

All boards and modules including the critical ones (attenuator and RYTHM) are common between these two
so the frequency must be limited by software only

of course calibration after such upgrade is a must and can pose a problem since the cal procedure is not possible by hobbyist

but still it would be awesome

Report to moderator Logged

smgvbest

Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #287 on:** September 30, 2020, 09:37:43 pm »

Service menu allow change of model and frequency range.
SERVICE/-2010/SERVICE

Other way is to program EEPROM on back of Processor card

Last if you have TME and ESA Module can do it there

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

analogRF

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

Frequent Contributor

Posts: 809
Country:

« **Reply #288 on:** October 01, 2020, 01:54:46 am »

Quote from: smgvbest on September 30, 2020, 09:37:43 pm

> Service menu allow change of model and frequency range.
> SERVICE/-2010/SERVICE
>
> Other way is to program EEPROM on back of Processor card
>
> Last if you have TME and ESA Module can do it there

What's the catch then? Could it be just the calibration thing? if it can be converted so easily then why did Agilent even sell E4404B? or why did anybody buy E4405B? Their original prices were hugely different...

Report to moderator Logged

smgvbest

Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #289 on:** October 01, 2020, 02:28:01 am »

Quote from: analogRF on October 01, 2020, 01:54:46 am

> **Quote from: smgvbest on September 30, 2020, 09:37:43 pm**
>
> > Service menu allow change of model and frequency range.
> > SERVICE/-2010/SERVICE
> >
> > Other way is to program EEPROM on back of Processor card
> >
> > Last if you have TME and ESA Module can do it there
>
> What's the catch then? Could it be just the calibration thing? if it can be converted so easily then why did Agilent even sell E4404B? or why did anybody buy E4405B? Their original prices were hugely different...

IDK, I've used it to change mine to the EMC model (same firmware), the service menu with the right password looks to even permit you to change the serial number. the -2010 does not permit then though. the Serial Number and Save Serial Number are greyed out so there's additional service passwords.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

mankan

Contributor

Posts: 42
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #290 on:** October 02, 2020, 11:19:58 am »

Quote from: tv84 on September 19, 2020, 04:14:49 pm

> This can also be used in the old **E44xxB ESG Signal Generators**.
>
> Just checked.

Really with the same vendor name and seeds? I cannot get it to work with a lmcrypt.exe that works for ESA. I've also tried HOST_ID variations like the VSA but with ESG and ESG-D instead. None of them produce a working code (i.e. a code for an option I already have installed).

Report to moderator Logged

analogRF

Frequent Contributor

Posts: 809
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B

Say Thanks Reply Quote

« **Reply #291 on:** October 02, 2020, 11:22:39 am »

Quote from: smgvbest on September 30, 2020, 09:37:43 pm

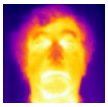
> Service menu allow change of model and frequency range.
> SERVICE/-2010/SERVICE
>
> Other way is to program EEPROM on back of Processor card
>
> Last if you have TME and ESA Module can do it there

maybe it is only possible to downgrade or convert to equivalent EMC model from ESA and vice versa.

someone with E4404B should try this

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #292 on:** October 02, 2020, 11:44:14 am »

> **Quote from: mankan on October 02, 2020, 11:19:58 am**
>
> > **Quote from: tv84 on September 19, 2020, 04:14:49 pm**
> >
> > This can also be used in the old **E44xxB ESG Signal Generators**.
> >
> > Just checked.
>
> Really with the same vendor name and seeds? I cannot get it to work with a lmcrypt.exe that works for ESA. I've also tried HOST_ID variations like the VSA but with ESG and ESG-D instead. None of them produce a working code (i.e. a code for an option I already have installed).

The ESG uses the following format:

FEATURE ABC TMOMID01 1.0 permanent uncounted 0123456789AB VENDOR_STRING=0 HOSTID=12345678

Report to moderator Logged

Keyboard error: Press F1 to continue.

The following users thanked this post: mankan

mankan
Contributor

Posts: 42
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #293 on:** November 20, 2020, 05:22:39 pm »

I've got my E4407B today
Juggled floppies and upgraded it to latest FW and Power Suite.

Also generated codes for possible options for my HW config and successfully installed installed 1D6 Time gating.

Now I'm having a hard time downloading and extracting the additional options. I either fail to extract the file due to corruption or errors that implies I need a real floppy and not a USB one.

Anyone that could share the following options SW in a better way than Keysight:
~~225 Cable fault~~
226 Phase noise
227 Cable TV
~~BAH GSM/GPRS~~
J36 FM deviation (I assume J35 is included in J36)

TIA

Edits: Realized 225 and BAH requires HW options that I currently do not have.
« *Last Edit: November 20, 2020, 06:01:53 pm by mankan* »

Report to moderator Logged

smgvbest
Supporter

Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #294 on:** November 20, 2020, 06:50:36 pm »

I had to use a real floppy for some reason

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

mankan
Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #295 on:** November 20, 2020, 07:06:09 pm »

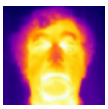
Posts: 42
Country:

Good to know, unfortunately I do not have a computer with a real floppy available without hours of Frankensteinian work.

Besides that it's only option 225 (which I do not have HW for) that gets downloaded properly. All the others are really small files (16-32kB) and corrupt so even with a computer with a proper floppy I cannot advance further. That is why I am doing this request.

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #296 on:** November 20, 2020, 07:26:29 pm »
Say Thanks Reply Quote

The download indeed turns up a bit of a fight, I was not able to download 226, tried 4 different browsers. However 227 worked, and also J36 which offered me 2 different files, please see the attachment.

ESA.zip (2085.3 kB - downloaded 92 times.)

Report to moderator Logged

Keyboard error: Press F1 to continue.

mankan
Contributor

Posts: 42
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #297 on:** November 20, 2020, 08:44:40 pm »
Say Thanks Reply Quote

Many thanks PA0PBZ, now have a updated option 227 to A.02.08 and latest version of J25/J36 B01.02. A friend reminded me that I have a oscilloscope running Windows 98. HP54820A FTW

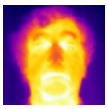
I tried 2 browsers myself, Firefox and Chrome on Windows 7. How did you succeed?

So now I'm just lacking the 226 Phase noise.

Regarding J35/J36: I could install both, but I ended up keeping the J35/J36 B.01.02 version since its newer and it seems option J36 is included in J35 newer versions which requires extra memory A72. My unit reports personality J35 as installed but reports no name for its J35 license. However J36 license is still installed and reports FM deviation.

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #298 on:** November 21, 2020, 08:27:12 am »
Say Thanks Reply Quote

> **Quote from: mankan on November 20, 2020, 08:44:40 pm**
>
> I tried 2 browsers myself, Firefox and Chrome on Windows 7. How did you succeed?

Chrome on Windows 10 downloaded the 2 J36 files without a problem and 227 on the second try, 226 failed on Chrome, Edge, Firefox and IE.

Report to moderator Logged

Keyboard error: Press F1 to continue.

mankan
Contributor

Posts: 42
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #299 on:** November 21, 2020, 10:00:36 am »
Say Thanks Reply Quote

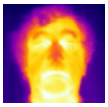
Found the file URL with Edge: https://www.keysight.com/upload/cmc_upload/All/226_B0131.exe . But all my wget tricks ends up with " Connection closed at byte 32272"

Report to moderator Logged

PA0PBZ
Super Contributor

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #300 on:** November 21, 2020, 11:02:05 am »
Say Thanks Reply Quote

I have more to offer



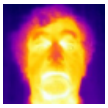
Posts: 4618
Country:

226_B0131.zip (584.26 kB - downloaded 164 times.)

Report to moderator Logged

Keyboard error: Press F1 to continue.

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #301 on:** November 21, 2020, 12:31:47 pm »

Say Thanks Reply Quote

Yes, I clicked it for fun and this time it worked

Report to moderator Logged

Keyboard error: Press F1 to continue.

mankan
Contributor

Posts: 42
Country:

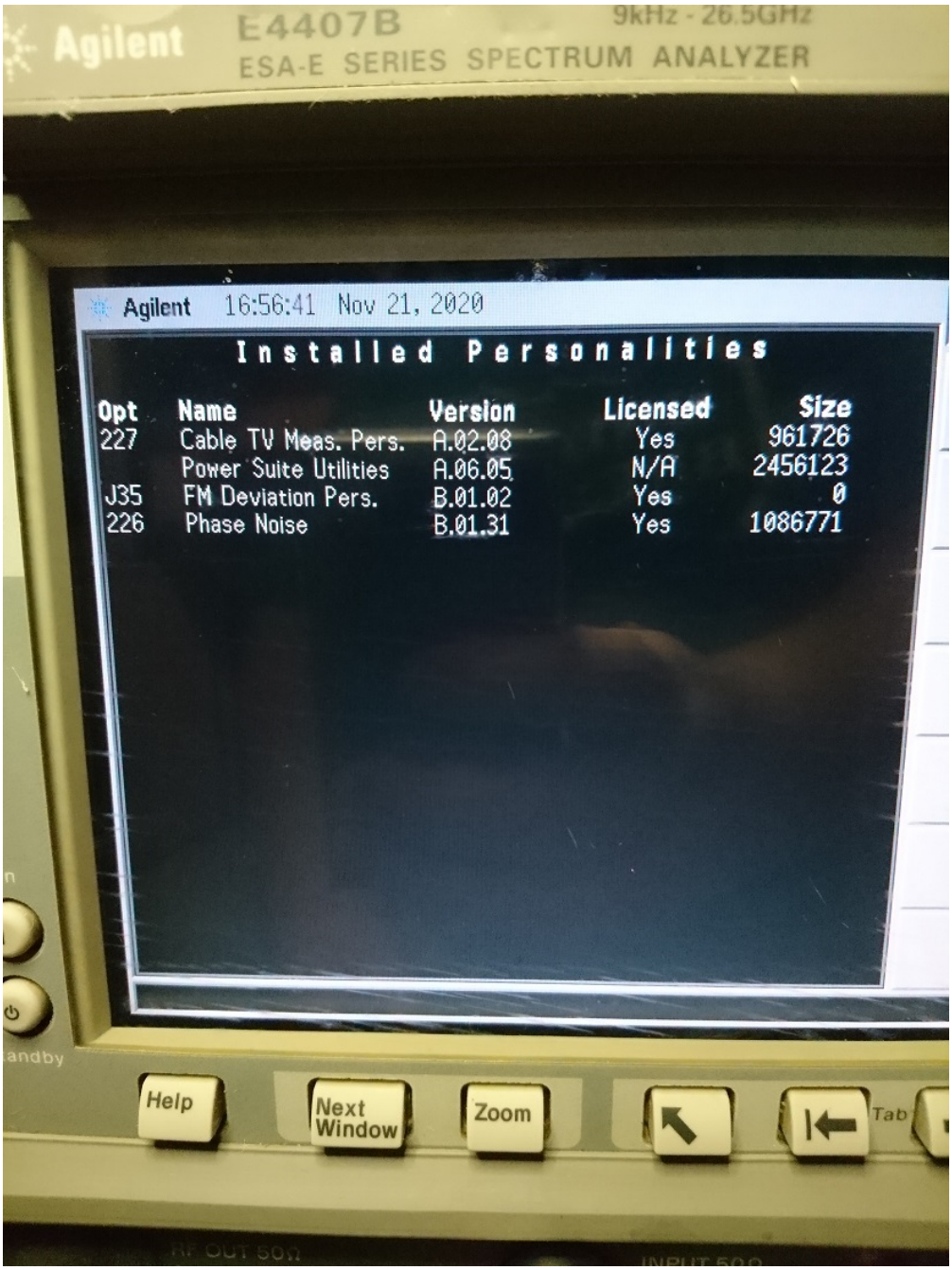
Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #302 on:** November 21, 2020, 04:12:07 pm »

Say Thanks Reply Quote

Thanks again PA0PBZ

Now I have the options that is useful for my HW.
[attachimg=1]

As a way of paying it forward, I've attached zipped disk folders so no need for real floppy drives. I also managed to run the disk image SW in my XP Virtual Box, it was the fastest floppy drive I have ever used



personalities.JPG (310.09 kB, 828x1104 - viewed 337 times.)
226_B0131.zip (284.62 kB - downloaded 113 times.)
227_A0208.zip (168.08 kB - downloaded 95 times.)
J35_J36_B0102.zip (93.9 kB - downloaded 90 times.)
J36_A0101.zip (147.07 kB - downloaded 101 times.)

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #303 on:** November 22, 2020, 04:33:33 am »

Say Thanks Reply Quote

Quote from: hpls on November 22, 2020, 04:08:44 am

Hi
I have an e4403B, I would like to start activating the option 049 color display ...
I tried to follow these steps but I believe I am doing something ...
can someone detail the steps more?
I'm using Putty as a serial monitor ...
I can make the morning calls until 9 ...

doing this procedure I need to do what else?

My steps:
0. Set the serial terminal to 19200,8n1
1. DIP sw # 4 set to ON
2. break the boot process with 0x06
3. sword 04139614 4ef9
4. sword 04139618 d8a4
5. DIP sw # 4 set to OFF
6. gu
7. SA restart in normal mode
8. Press "r" and we are in the monitor now
9. Change the serial port speed.
> slong 815F4 1001A
10. Change speed of the serial terminal to 115200, 8n1

---

does you SA actually have a Color Display?
depending on the Unit some where not shipped with a Color Display and hence the need for Opt 049 when installing a color display
if you have a color display and its not showing color then you need to create a license for 049, information of which is in this thread on how to do

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

suj
Regular Contributor
Posts: 85
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #304 on:** November 22, 2020, 02:26:56 pm »

Quote from: hpls on November 22, 2020, 02:21:16 pm

...
I don't know if I'm doing it wrong or skipping some process to activate the licenses ...

after this procedure what do i need to do more?

0. Set the serial terminal to 19200.8n1
1. DIP sw # 4 set to ON
2. interrupt the boot process with 0x06
3. sword 04139614 4ef9
4. sword 04139618 d8a4
5. DIP sw # 4 set to OFF
6 .gu
7. Restart SA in normal mode
8. Press "r" and we are on the monitor now
9. Change the speed of the serial port.
> slong 815F4 1001A
10. Change the speed of the serial terminal to 115200, 8n1

That was a procedure to get a dump for debugging, not useful to you. The solution is in post #244.

Report to moderator Logged

---

mankan
Contributor

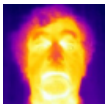
Posts: 42
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #305 on:** November 29, 2020, 10:21:00 am »

Weirdly enough I have the same download issue again, this time its the latest ESG fw that fails the same way. Can I bother some of the master downloaders in this thread for assistance?
https://www.keysight.com/main/software.jspx?cc=US&lc=eng&nid=-32463.536880925&id=1000001137:epsg:sud&pageMode=CV

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #306 on:** November 29, 2020, 11:08:01 am »

No problem for me with this one.

EPSG090623.zip (2843.21 kB - downloaded 100 times.)

Report to moderator Logged

Keyboard error: Press F1 to continue.

The following users thanked this post: mankan, roxbox

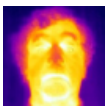
Electrole
Contributor
Posts: 40
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #307 on:** February 08, 2021, 08:42:51 pm »

Dear all,
I have read this thread with interest and utter admiration! I have recently acquired an almost working E4411B which I'm trying to fix. Eventually, and if the repair session goes well, the E4411B will deserve to have option 1DR (narrow BW) enabled. However, I fail to see exactly which steps to carry out in order to enable this option. Could some of you perhaps be persuaded to write up a small tutorial that takes the reader through the concrete steps? My E4411B has FW version A.14.03 and was born with B72 Expansion Memory, so I guess an update should be doable.
Best regards

Report to moderator Logged

PA0PBZ
Super Contributor



Posts: 4618
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #308 on:** February 08, 2021, 09:17:00 pm »

> **Quote from: Electrole on February 08, 2021, 08:42:51 pm**
> Eventually, and if the repair session goes well, the E4411B will deserve to have option 1DR (narrow BW) enabled. However, I fail to see exactly which steps to carry out in order to enable this option.

Send me a PM with your hostid and the required option and I think we can work it out

Report to moderator Logged

Keyboard error: Press F1 to continue.

The following users thanked this post: VRCW

n8ur
Newbie
Posts: 3
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #309 on:** February 21, 2021, 08:54:15 pm »

I've been trying to do my homework, but a day of searching the interwebs for lmcryptgui has only turned up references in message boards 10 years ago with links to locations that are long gone.

If anyone here has, or can help me find, the file, I'd really appreciate it.

Thanks!
John

Report to moderator Logged

roxbox
Newbie
Posts: 4
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #310 on:** April 22, 2021, 05:32:43 pm »

This would be nice, I have TME!

added: I looked at the E4406A bin and the E4440A and found the flexlm structure,
the data is the same for both so I would think that the keys and seeds for the E4406A would work with the E444xA specans.

has anyone tried this?
I can not seem to get the keys and or seeds correct to reproduce any of the lic codes I have. can anyone point me in the correct direction?

frank

« Last Edit: May 13, 2021, 07:35:59 pm by roxbox »

Report to moderator Logged

ps
Contributor
Posts: 32
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #311 on:** May 07, 2021, 09:11:51 pm »

For early units, option 1D5 is added by installing a Corning / VECTRON MC867X4-002W OCXO (10MHz +12V sinewave EFC) to the reference/third converter board.

Is this OCXO controlled by the same DACs as the regular timebase, i.e. using the System - Alignments - Timebase menu?

Or does it require the N7811A software package to set the control voltage? If so, does anybody know the required GPIB commands? Otherwise it could be easier to use some precision resistors and a pot to provide the tune voltage in hardware.

Generally, have any of the N7811A alignment procedures been reverse engineered, so that they could be done with a simple GPIB interface and some own code?

Report to moderator Logged

msraya
Supporter
Posts: 106
Country:
EA7EE

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #312 on:** May 08, 2021, 10:40:49 am »

I managed to unlock my ESA-L E4411, but the question I have is if it is possible to convert an ESA-L SA to ESA-E through service manual?
I will screw up the set?

Unhappily I don't have boards to use extended functions either ...

Regards
Manuel

Report to moderator Logged

smgvbest
Supporter
Posts: 623
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #313 on:** May 09, 2021, 07:54:39 pm »

Quote from: msraya on May 08, 2021, 10:40:49 am

> I managed to unlock my ESA-L E4411, but the question I have is if it is possible to convert an ESA-L SA to ESA-E through service manual?
> I will screw up the set?
>
> Unhappily I don't have boards to use extended functions either ...
>
> Regards
> Manuel

you can change the model in the service manual but your SA has to have all the hardware needed to do it successfully.
you can not convert up either you can only convert down from what I see.
I also do not know of any ramification of doing so.

Report to moderator Logged

Sandra
(Yes, I am a Woman :p)

msraya
Supporter
Posts: 106
Country:
EA7EE

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
Say Thanks Reply Quote
« **Reply #314 on:** May 12, 2021, 06:13:36 am »

Thank You Sandra!

I don't have hardware options, so I cannot upgrade the instruments and I think It would be complicated.

The ESA-E E4411B was bottom line feature-wise SA from HP. No hardware options. So little more can I do.
I was looking for the option table and I manage to find it.
But the only option I can really use was the pre-amplifier. All other options were crippled or not applicable.

I suppose it is lacking some hardware as there are no way to select low BW filter although I enabled 1D5 option.
So, now only pre-amplifier and 200Hz EMI filter is working.

Regards
Manuel

Report to moderator Logged

KD4PBS
Contributor
Posts: 34
Country:

Re: Enabling options on Agilent ESA series E4402B E4404B E4405B E4407B
« **Reply #315 on:** October 05, 2021, 07:23:17 pm »

Say Thanks Reply Quote

I, too, am looking for the magic program which is required to add options to the E4400 series, and no matter my google duck duck fu, I also only find dead links to sites which no longer exist. And this isn't my first rodeo.
Anyone have any ideas?
Regards-

Report to moderator Logged