

OsmocomBB - Feature #3582

Merge reading of factory RF calibration values

09/20/2018 05:57 PM - fixeria

Status: Stalled	Start date: 09/21/2018
Priority: Normal	Due date:
Assignee: fixeria	% Done: 60%
Category: OsmocomBB Firmware	
Target version:	
Resolution:	Spec Reference:
Description	
Reading of factory RF calibration values was implemented together with adding FCDEV1B board support (see #3581) by Mychaela Falconia, but was not merged to the upstream. The corresponding code changes should be organized as a patch-set, and then uploaded to Gerrit for further review.	
The modified source code archive can be downloaded from: ftp://ftp.freecalypso.org/pub/GSM/FreeCalypso/obb-fcmo...	
Related issues:	
Related to OsmocomBB - Support #2704: set up FCDEV1B board so it can be remot...	Feedback 12/03/2017
Related to OsmocomBB - Feature #3581: Merge FCDEV3B board support	Resolved 09/21/2018
Related to OsmocomBB - Bug #1458: AGC broken (strong cell cannot be synced	New
Related to OsmocomBB - Support #3801: dump flash of Sony Ericsson SJ100i	Resolved 02/13/2019

History

#1 - 09/20/2018 05:57 PM - fixeria

- Related to Support #2704: set up FCDEV1B board so it can be remotely accessed remotely added

#2 - 09/20/2018 05:58 PM - fixeria

- Related to Feature #3581: Merge FCDEV3B board support added

#3 - 02/12/2019 11:33 AM - fixeria

- Related to Bug #1458: AGC broken (strong cell cannot be synced added

#4 - 02/12/2019 01:16 PM - fixeria

- Status changed from New to Feedback

- Assignee set to fixeria

- % Done changed from 0 to 90

Please see:

<https://gerrit.osmocom.org/#/c/osmocom-bb/+12885> firmware/lib: introduce TIFFS filesystem support

<https://gerrit.osmocom.org/#/c/osmocom-bb/+12886> firmware/board/compal_e99: enable reading of the second half of flash

<https://gerrit.osmocom.org/#/c/osmocom-bb/+12887> firmware: implement reading of factory RF calibration values

#5 - 02/12/2019 05:28 PM - falconia

Please note: at the time when I wrote this code (2017-Nov), I did not realize that setting the APC offset (MY_OFFSET macro in the `l1s_tx_apc_helper()` function) to 48 is only correct for TI-classic targets (meaning pristine/unchanged from TI's reference), practically meaning Openmoko and FreeCalypso devices. Later in 2018 I discovered that Mot/Compal's and Pirelli's firmwares (both heavily modified relative to TI) use different APC offset settings: 32 for Compal and 0 for Pirelli. See this change in FC Magnetite firmware for Compal and Pirelli support:

<https://bitbucket.org/falconian/fc-magnetite/commits/395e464e4005ee0ca8afeaa59bcc84478e13cb1b>

(The RF_PA preprocessor symbol is set to 2 for Openmoko/FreeCalypso targets in the above code.)

What does this news mean for the present OsmocomBB change? Answer: the code currently under review is correct for GTA0x and FCDEV3B targets, but is NOT correct for Compal or Pirelli. The per-unit Tx APC calibration values produced by their respective factories were calibrated with the APC offset set to 32 or 0 (Compal and Pirelli, respectively), and if these factory calibration values are used with the APC offset set to 48 instead, the

resulting RF power output levels will be a little too high.

My suggestion is to replace the MY_OFFSET macro with a global variable (named apc_offset perhaps), and define this global variable to the correct number in per-board rf_tables.c files, similarly to what I did with the VCXO slope for AFC.

#6 - 02/12/2019 06:35 PM - falconia

Regarding the linking of this feature to bug [#1458](#), please note that my patch from 2017-Nov only makes OsmocomBB make use of the factory calibration values for the Tx path (plus the AFC initial setting for FB search), but does not do anything for the Rx path. I couldn't figure out how to make OBB make use of the factory calibration values for Rx because OBB's architecture is too different from TI's in this regard. But if someone else wishes to put in the extra work to make use of factory calibration values for Rx, they are there: there is a GMagic number for each band, as well as per-band tables of finer subband corrections. On Openmoko and FreeCalypso devices, look in the agcparams and calchan files under /gsm/rf/rx in FFS, on the Pirelli DP-L10 the factory data block contains Rx calibration structures which directly correspond to these agcparams and calchan files. Mot/Compal's version is different, but both the per-band GMagic number and a table of subband corrections for each supported band are still there, and here is the code that groks those Mot/Compal data structures:

<https://bitbucket.org/falconian/freecalypso-tools/src/368ffb8a08e5491c58ed29823e3658d06821545c/ffstools/caltools/c1xx-calextr.c?at=default&fileviewer=file-view-default>

And here is my article that describes the theory behind these numbers:

<https://bitbucket.org/falconian/fc-rfcal-tools/src/9f09a7c3607a63cd406ce593ef99e547de399ab3/doc/Rx-cal-theory?at=default&fileviewer=file-view-default>

#7 - 02/12/2019 07:53 PM - falconia

I just took another look, and the hard-coded Rx path gain settings used by the current OsmocomBB code (not touched at all by my 2017-Nov patch) correspond to GMagic=196 (98.0 dB) in TI's universe. How did I get this number? Answer: SYSTEM_INHERENT_GAIN setting of 71 in board/*/rffe*.c files + TRF6151_FE_GAIN_HIGH defined to 27 in rf/trf6151.c = 98; TI's GMagic units are half-dB, hence the GMagic=196 result.

For comparison, the center-of-band GMagic numbers calibrated on my FCDEV3B boards with the use of a CMU200 instrument (test instrument itself calibrated at R&S Maryland, cable insertion loss accounted for) fall in the range from 199 to 201 (99.5 to 100.5 dB); the numbers I have read out of Openmoko-made units I laid my hands on similarly fall in the range from 199 to 202 (99.5 to 101.0 dB). Thus if it is too difficult to apply the calibrated numbers because of firmware architectural differences, GMagic=200 makes a very reasonable hard-coded default. Thus the GMagic equivalent used by the current OBB is a little low in comparison, but it is only off by 2 dB - not much.

If you wish to make your Rx gain control spot-on, you might want to change the SYSTEM_INHERENT_GAIN definition in board/gta0x/rffe_gta0x_triband.c from 71 to 73 - it would produce the equivalent of GMagic=200. I did not make this change in my 2017-Nov patch because at that time I wasn't as certain regarding the correct numbers - I only got my CMU200 instrument officially calibrated in 2018-Feb - it cost a non-trivial amount of money, hence the delay.

#8 - 02/12/2019 08:11 PM - fixeria

Hi Mychaela,

Please note: at the time when I wrote this code (2017-Nov), I did not realize that setting the APC offset (MY_OFFSET macro in the l1s_tx_apc_helper() function) to 48 is only correct for TI-classic targets (meaning pristine/unchanged from TI's reference), practically meaning Openmoko and FreeCalypso devices. Later in 2018 I discovered that Mot/Compal's and Pirelli's firmwares (both heavily modified relative to TI) use different APC offset settings: 32 for Compal and 0 for Pirelli.

thank you very much for this clarification!

My suggestion is to replace the MY_OFFSET macro with a global variable (named apc_offset perhaps), and define this global variable to the correct number in per-board rf_tables.c files, similarly to what I did with the VCXO slope for AFC.

I just updated the change following your recommendations.

Regarding the linking of this feature to bug [#1458](#), please note that my patch from 2017-Nov only makes OsmocomBB make use of the factory calibration values for the Tx path (plus the AFC initial setting for FB search), but does not do anything for the Rx path.

Yep, I already noticed that the Rx path remains unchanged.

This also needs to be noted in the commit message (TODO for me).

Thanks for your tips regarding the Rx path, I'll have a look at your code and documentation :)

#9 - 02/12/2019 11:25 PM - falconia

It should also be noted that my original 2017-Nov patch adds the reading and parsing of factory RF Tx calibration values for all previously supported targets with the single exception of Sony Ericsson J100. Of all OBB-supported Calypso phone models, SE J100 is the only one I have never laid my hands on, hence I do not currently know where and how its RF calibration values are stored. If someone can send me a flash dump from one of those SE J100 phones, I would be able to tell you pretty much immediately how to read and apply its calibration values, making all target support complete.

#10 - 02/13/2019 08:30 AM - laforge

On Tue, Feb 12, 2019 at 11:25:51PM +0000, falconia [REDMINE] wrote:

Of all OBB-supported Calypso phone models, SE J100 is the only one I have never laid my hands on, hence I do not currently know where and how its RF calibration values are stored.

If you'd like, I can send one to you by postal mail. Please contact me privately with a postal address to where I can mail it. The phone and shipping would be free of charge.

If someone can send me a flash dump from one of those SE J100 phones, I would be able to tell you pretty much immediately how to read and apply its calibration values, making all target support complete.

I guess that's also an option. Is there a "ready made" firmware / tool for dumping the flash, or would I need to write that code on my own? I'm only aware of the compal_dsp_dump, but that's not for flash...

#11 - 02/13/2019 09:31 AM - fixeria

Hi Harald,

I guess that's also an option. Is there a "ready made" firmware / tool for dumping the flash, or would I need to write that code on my own? I'm only aware of the compal_dsp_dump, but that's not for flash...

FreeCalypso has all required tools and great documentation. Not sure if J100i is supported by fc-loadtool though.

Please see:

<https://bitbucket.org/falconian/freecalypso-tools/>
<https://bitbucket.org/falconian/freecalypso-tools/src/6f804a5ff3bc895e405ca711cbff620a62365385/doc/Loadtools-usage?at=default&fileviewer=file-view-default>

General steps of dumping the firmware:

```
# Make sure you have freecalypso-tools installed
$ cd /opt/freecalypso/bin/
# Also, make sure you have the payloads compiled
$ ls /opt/freecalypso/target-bin/

# Start the fc-loadtool (similar to our osmocon)
# "-h compal" corresponds to "compalstage-plain.bin" payload,
# which is valid for Mot C11x/123. According to our wiki,
# the RAM loader of the J100i is the same as used on the
# MotorolaC140 series, but expects a "1003" magic word
# to be present at address 0x803ce0, thus we need another
# payload called "compalstage-1003.bin":
$ ./fc-loadtool -h compal -c 1003 /dev/ttyUSB0

# See "help flash" for more details
$ flash dump2bin OUTFILE
```

Alternatively, you can use OsmocomBB:

```
$ cd osmocom-bb/src/
$ host/osmocon/osmocon -p /dev/ttyUSB0 -m c140 -c target/firmware/board/se_j100/loader.highram.bin
```

```
# Check the info about flash
$ host/osmocon/osmoload finfo

# Dump the whole flash (example for Mot C11x/123, check your finfo)
$ host/osmocon/osmoload memdump 0x00000000 0x200000 /tmp/dump.bin
```

#12 - 02/13/2019 07:01 PM - laforge

- Related to Support #3801: dump flash of Sony Ericsson SJ100i added

#13 - 02/25/2019 05:43 AM - falconia

Seeing that the big patch for reading and making use of factory RF calibration values is still languishing in gerrit, I have put out an updated version of my FTP tarball package:

<http://ftp.freecalypso.org/pub/GSM/FreeCalypso/obb-fcmodes-r2.tar.bz2>

It consists of the current OBB mainline plus the patch currently in gerrit plus one additional change for the Rx path, namely a better value for the SYSTEM_INHERENT_GAIN constant for GTA0x and FCDEV3B targets.

I have yet to receive an SE J100 phone or a flash dump from one, hence I still have no authoritative answer for where and how their RF calibration values are stored, but my guess is that it is most likely the same as on the lower Mot C1xx models with 4 MiB flash, and I have incorporated this assumption into the above tarball release as well.

I also saw a comment from Vadim in gerrit saying that he would like to split the big patch into a few smaller ones. Here is one way to do it:

Patch 1: add the board/*/rf_tables.c files and the new include/rf headers they depend on.

Patch 2: add the code that reads and parses factory RF calibration records and applies them to the variables and arrays in those rf_tables.c modules.

Patch 3: switch the AFC code in layer1/afc.c from hard-coded constants to using AFC variables in the RF tables modules. No functional impact on Compal targets with this change, only GTA0x, FCDEV3B and Pirelli.

Patch 4: the brave one: switch the APC code to use the entirely new Tx calibration framework.

Patch 5: my new change to the SYSTEM_INHERENT_GAIN constant for GTA0x and FCDEV3B targets.

Also please note that all of my code contributions are in the public domain and are NOT copyrighted by me, and I strenuously object to anyone taking it upon themselves to insert a copyright notice with my name in it. I am a stateless person, holding no valid citizenship in any currently existing country, whichever country I happen to live in, I live there illegally with no rights whatsoever (if you were to attack me in the street, I have NO right to call the police for protection, I can only defend myself with my own personal means, and if you were to successfully kill me, you should not only NOT be prosecuted for it, but may be entitled to a bounty on my head), and it is my stance that I cannot meaningfully hold copyright on anything. Every piece of software code that I have ever written from the day I was born and every piece of code I will ever write in the future until the day I die is in the public domain, uncopyrighted, and that includes the present small pieces of code which I have written for OsmocomBB in the spirit of harm reduction.

#14 - 02/25/2019 01:15 PM - falconia

My obb-fcmodes-r2.tar.bz2 package includes fixes for the copyright statements which I find objectionable, with diffs of the following form:

```
- * (C) 2017 by Mychaela Falconia <mychaela.falconia@gmail.com>
- *
- * All Rights Reserved
+ * This code was written by Mychaela Falconia <falcon@freecalypso.org>
+ * who refuses to claim copyright on it and has released it as public domain
+ * instead. NO rights reserved, all rights relinquished.
```

and

```
- * (C) 2017 by Mychaela Falconia <mychaela.falconia@gmail.com>
- * Tweaked (coding style changes) by Vadim Yanitskiy <axilibrator@gmail.com>
+ * This code was written by Mychaela Falconia <falcon@freecalypso.org>
+ * who refuses to claim copyright on it and has released it as public domain
+ * instead. NO rights reserved, all rights relinquished. *
- * All Rights Reserved
+ * Tweaked (coding style changes) by Vadim Yanitskiy <axilibrator@gmail.com>
```

Please apply these public domain fixes to the already-merged TIFFS reader code and to the main patch which is still pending in gerrit.

#15 - 03/05/2019 07:28 PM - fixeria

- Status changed from Feedback to Stalled

- % Done changed from 90 to 60

Hello Mychaela,

[...] I have put out an updated version of my FTP tarball package [...]
It consists of the current OBB mainline plus the patch currently in gerrit plus one additional change for the Rx path, namely a better value for the SYSTEM_INHERENT_GAIN constant for GTA0x and FCDEV3B targets.

thanks a lot! I'll have a look when I get a chance.

I also saw a comment from Vadim in gerrit saying that he would like to split the big patch into a few smaller ones. Here is one way to do it [...]

The proposed sequence of patches looks good to me.
I have had (when I've been working on it) something similar in my mind.

Also please note that all of my code contributions are in the public domain and are NOT copyrighted by me, and I strenuously object to anyone taking it upon themselves to insert a copyright notice with my name in it.

Sorry, I didn't know that. This should have been negotiated before sending the changes to review.

Please apply these public domain fixes to the already-merged TIFFS reader code and to the main patch which is still pending in gerrit.

Regarding already-merged TIFFS reader, please see:

<https://gerrit.osmocom.org/#/c/osmocom-bb/+13134>

regarding the WIP change in Gerrit, I will update the copyright statements together with splitting this change into a few patches.

#16 - 03/05/2019 07:48 PM - falconia

Regarding already-merged TIFFS reader, please see:

<https://gerrit.osmocom.org/#/c/osmocom-bb/+13134>

LGTM.

#17 - 03/06/2019 05:00 AM - falconia

Regarding factory RF calibration values on the SE J100i model, I have now confirmed (see ticket [#3801](#)) that they are stored in exactly the same location and format on this model as on Motorola C139/140, i.e., you can read and parse them exactly the same way as on the lower Mot C1xx subfamilies.

#18 - 03/10/2019 03:32 AM - falconia

- File `rf_tables_e86.c` added

Today I have confirmed through testing on my CMU200 station that different Compal hardware subfamilies require different Tx ramp template tables. The Tx ramps in `board/compal/rf_tables.c` in my `obb-fcm0ds-r1` and `obb-fcm0ds-r2` tarball packages are correct only for `compal_e88` and `compal_e99`, but not for `compal_e86`. The different set of tables needed for `compal_e86` (Mot C139/140) is in the attached `rf_tables_e86.c` file.

As far as SE J100 goes, I will only know in another week or two which Tx ramp template tables it needs (I will need to get FreeCalypso running on that phone in order to connect it to the CMU200 - OBB does not work with the CMU200 at all), but I am betting that it is probably the same as `compal_e86`, not the other one.

#19 - 03/10/2019 04:12 AM - falconia

- File `rf_tables_e86_correct.c` added

Oops, please disregard my previous rf_tables_e86.c file, please use the new rf_tables_e86_correct.c instead. My previous file had no actual change in the numbers from the E88/E99 version, as I reinserted those same old numbers by mistake. I messed it up because I was making the opposite change in my own FreeCalypso fw, where I previously had only C139 Tx ramp templates.

#20 - 03/10/2019 04:19 AM - falconia

I also have to point out that Vadim's change to the indentation makes the tables of Tx ramp templates very difficult to read or edit on a standard 80-column screen. My original indentation is a product of my fc-rftab2c program, which is how all of these tables of numbers have been generated: in FreeCalypso we have our own machine-readable and human-editable ASCII interchange format for RF parameter tables, and among many other users of this interchange format there is a utility called fc-rftab2c that converts these tables into C code snippets for inclusion into the firmware.

#21 - 03/17/2019 12:44 AM - falconia

- File os3582-20190316.patch added

The attached patch (os3582-20190316.patch) is the final revision of my proposed change adding the reading of factory RF calibration values and switching the Tx APC levels, APC offset and ramp-up and ramp-down profiles to the correct numbers used by each target's respective original firmware. This final revision of the present patch supersedes all of my previous versions - please don't use any of those earlier versions.

All of the various tables of numbers included in this patch (not all numbers can be read from factory calibration records, some need to be hard-coded in the firmware, namely Tx ramp template tables on Compal targets and the APC offset for all targets) are known to be correct because my own FreeCalypso firmware now runs on the complete set of targets supported by OBB, using these same tables of numbers and the same method of extracting original factory RF calibration values on non-FreeCalypso hardware, and the resulting RF Tx output is fully within specifications as verified with the CMU200 RF test instrument here at Falconia Partners LLC.

But as discussed before, this patch alone is not sufficient to bring OBB's radio transmissions into compliance: it is necessary, but not sufficient.

#22 - 03/17/2019 09:10 AM - laforge

Hi falconia,

On Sun, Mar 17, 2019 at 12:44:27AM +0000, falconia [REDMINE] wrote:

The attached patch (os3582-20190316.patch) is the final revision of my proposed change adding the reading of factory RF calibration values and switching the Tx APC levels, APC offset and ramp-up and ramp-down profiles to the correct numbers used by each target's respective original firmware. This final revision of the present patch supersedes all of my previous versions - please don't use any of those earlier versions.

Thanks a lot!

But as discussed before, this patch alone is not sufficient to bring OBB's radio transmissions into compliance: it is necessary, but not sufficient.

Well understood. Thanks again for your contributions!

Files

rf_tables_e86.c	18.7 KB	03/10/2019	falconia
rf_tables_e86_correct.c	18.7 KB	03/10/2019	falconia
os3582-20190316.patch	133 KB	03/17/2019	falconia