SIMtrace 2 - Bug #1704

test/port card emulation firmware for SAM3S based SIMtrace2

05/09/2016 07:45 PM - laforge

Status:	In Progress	**Start date:**	05/09/2016
Priority:	Normal	**Due date:**	
Assignee:	tsaitgaist	**% Done:**	0%
Category:	firmware		
Target version:			

Description

We have card emulation working on a different board already, but the changes need to be re-tested against a real SIMtrace board with SAM3S

Related issues:

Related to SIMtrace 2 - Bug #1705: re-integrate tracing + card reader modes i...	**Stalled**	**05/09/2016**

History

#1 - 04/26/2018 04:10 PM - laforge

- Assignee changed from laforge to tsaitgaist

#2 - 05/11/2018 04:29 PM - laforge

- Project changed from SIMtrace to SIMtrace 2

- Category deleted (SIMtrace firmware)

- Status changed from New to In Progress

#3 - 08/03/2018 09:08 AM - tsaitgaist

current state of cardem firmware on SIMtrace board, as reported by a user on the mailing list:
I've built (make BOARD=simtrace APP=cardem) the cardemulation-firmware of
the current master-branch (0.4.131-8f70) and flashed the resulting
simtrace-cardem-dfu.bin using dfu-util.

Furthermore I compiled the host binaries, triggered a reset on my simtrace2
device to make sure it's in runtime mode and then executed the remote-sim
program (sudo ./simtrace2-remsim -V 1d50 -P 60e3 -C 1 -I 0 -A `sudo
./simtrace2-list | cut -d = -f 2 | cut -d , -f 1 | tail -1`). The simtrace2
device, as well as an USB-CCID compliant omnikey cardreader are attached to
my linux computer as described in the QMOD manual. During runtime mode the
red LED on the simtrace2 is blinking, while the green LED is off.

I noticed that when the simtrace2-remsim program tries to send an ATR to
the simtrace2 device via usb (cardem_request_set_atr), the
libusb_bulk_transfer function is blocking, before returning
LIBUSB_ERROR_TIMEOUT. The serial debugging-output I got on the simtrace2
doesn't show any futher information (last state is "-I- USB is now
configured").

When I reset the usb-modem that is connected to the simtrace2 device I get
the following messages on the debug-serial:
ǂ Changed to ISO 7816-3 state 1
reset de-asserted
ǂ WT updated to 9600
ǂ Changed to ISO 7816-3 state 0
reset asserted
ǂ Changed to ISO 7816-3 state 1
reset de-asserted
[...]

while the simtrace2-remsim program is also receiving some garbage:
URB:
-> 03 00 00 00 00 00 0c 00 04 00 00 00
unknown simtrace msg type 0x00
URB:

-> 03 00 00 00 00 00 0c 00 08 00 00 00
unknown simtrace msg type 0x00
URB:
-> 03 00 00 00 00 00 0c 00 04 00 00 00
unknown simtrace msg type 0x00
[...]

I've also tried several older versions/commits - however I didn't get any
of them working properly.
When using version 0.4.13-ba2a (from this commit:
https://git.osmocom.org/simtrace2/commit/?id=ba2ad563cc0e389213a3f6f6ebe79dc21dfb26a3)
I was able to send the ATR to the simtrace and directly entered the main
loop on the host program.
The serial debugging-output (after a manual modem-reset) also looked
somehow more promising, but didn't work either:
ł 0: VCC activated
ł 0: CLK activated
ł 0: RST released
ł 0: computed Fi(1) Di(1) ratio: 372
ł 0: send_tpdu_header: 00 a4 00 04 02
ł 0: VCC deactivated
ł 0: CLK deactivated
ł 0: VCC activated
ł 0: CLK activated
ł 0: VCC deactivated
ł 0: CLK deactivated
[...]

#4 - 08/09/2018 12:14 PM - laforge

- Category set to firmware

#5 - 08/13/2018 04:54 PM - tsaitgaist

- Related to Bug #1705: re-integrate tracing + card reader modes into SIMtrace2 firmware (SAM3S) added

#6 - 08/13/2018 04:55 PM - tsaitgaist

- Status changed from In Progress to Stalled

will do once cardem is tested automatically on sysmoQMOD.

#7 - 10/25/2018 09:14 AM - tsaitgaist

- Status changed from Stalled to In Progress

resumed to continue osmo-remsim work