SIMtrace 2 - Bug #4118

VCC_PHONE strong pull on SIMtrace board

07/18/2019 11:54 AM - tsaitgaist

Status:	New	**Start date:**	07/18/2019
Priority:	Normal	**Due date:**	
Assignee:	tsaitgaist	**% Done:**	0%
Category:	hardware		
Target version:			
Spec Reference:			

Description

A complex behavior I identified while testing card emulation:
- although the phone does not power the card (the SIMtrace board, v1.4) through VCC_PHONE, VCC_PHONE was at 3.2V (after power up)
- VCC_PHONE should be pulled down by R19 (100k resistor)
- VCC_PHONE is also connected to the FLAGB output of the FPF2109. but this output is only an open-drain (can't drive high), and connected through a 100k resistor R22 (driving high could not be strong enough to set VCC_PHONE to 3.2V)
- when VCC_PHONE is briefly shorted to ground (pulling low with less than 1kR), VCC_PHONE then goes and stays at 0.6V

the issue comes from the FPF2109.
VCC_PHONE is connected to VIN, which should only be an input. VCC_SIM is connected to VOUT, which should only be an output.
VCC_SIM is also the output of the AP7332 voltage regulator.
the output from AP7332 goes in FPF2109 as VCC_SIM, through the FPF2109 internal MOSFET body diode (presumably), back out to VCC_PHONE.
the FPF2109 has an internal reverse blocking mechanism. this is probably kicking in when VIN is shorted to ground. 0.6V still pass through.

this is an issue because holding VCC_PHONE high prevents the firmware to properly detect activation (power up) and cold reset of the card.
some card readers pull/drive VCC low (omnikey 6321), but I'm not sure all modems do.

TODOs:
- R22 is not needed and can be removed (the FLAGB output is not used)
- the R19 pull down resistor is also not needed since R20+R21 (resistor divider) already form a 20k pull down resistor
- ensure the on-board regulator for VCC_SIM is switched off
- switching the regulator off would prevent using SIMtrace as independent card reader while card emulation is used (this is not an issue for MitM since the phone powers the card when needed)
- better find out/test how the reverse current protection works