

Extra

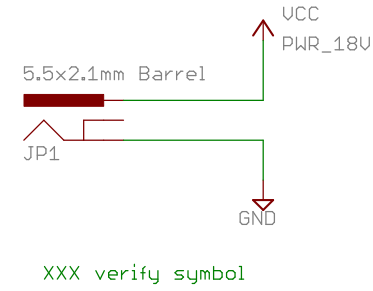


open hardware



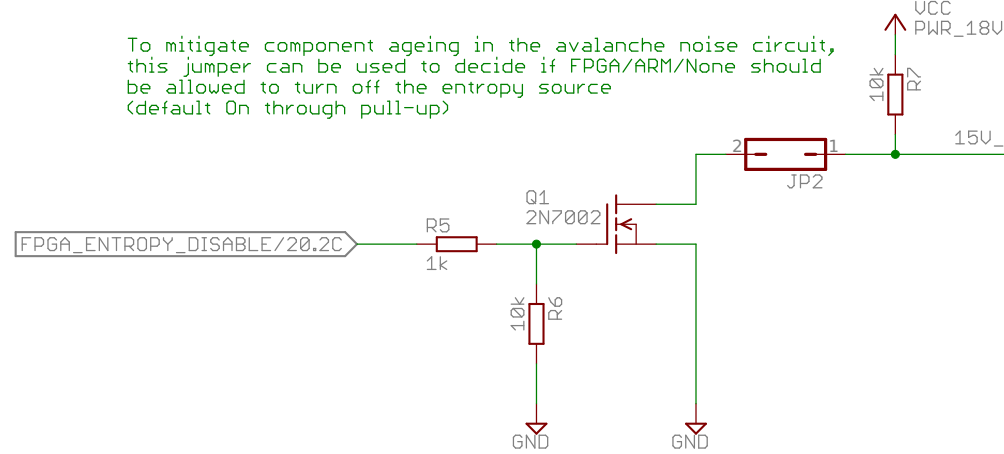
This page intentionally left blank

Main power input  
18V DC

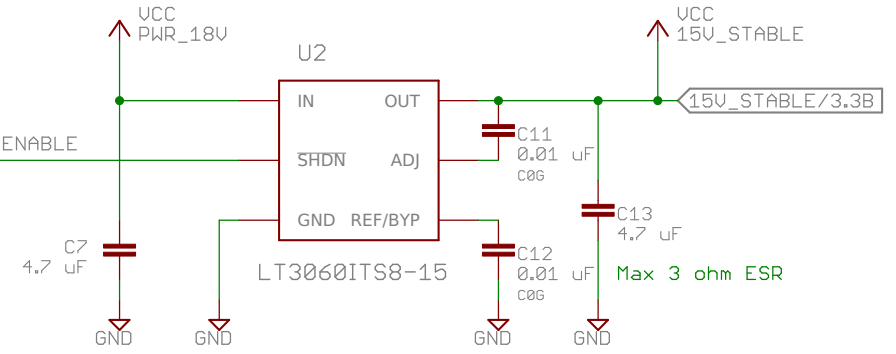


Entropy source power

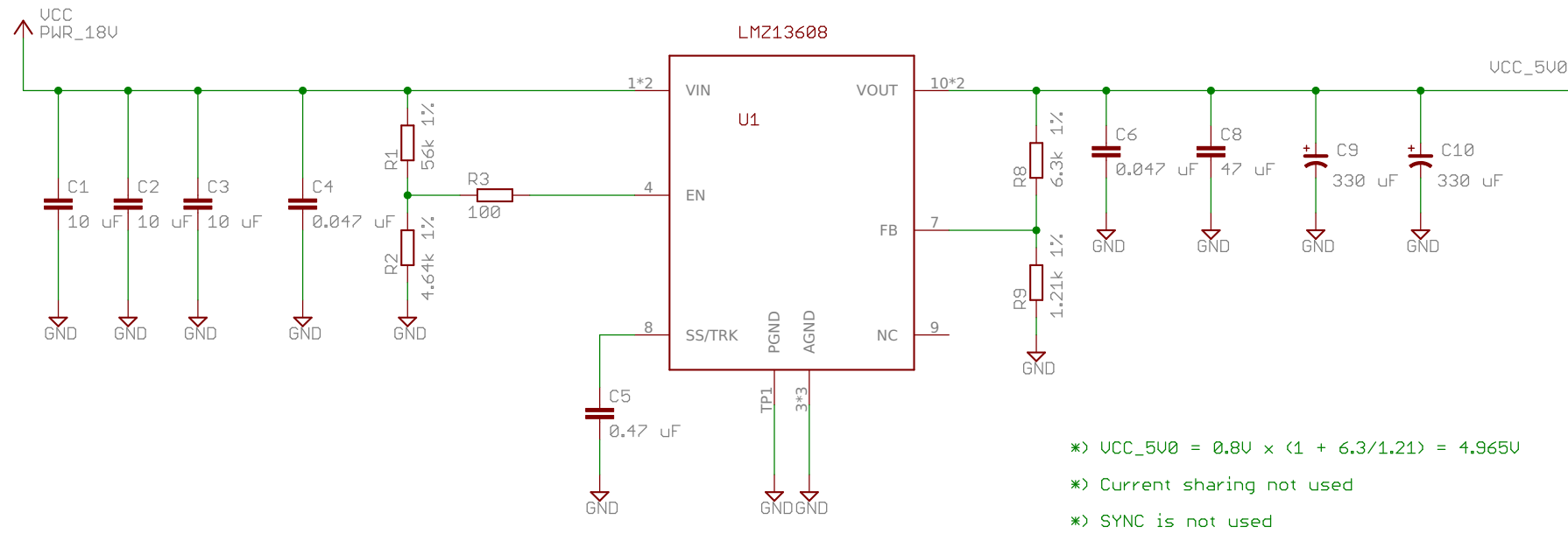
To mitigate component ageing in the avalanche noise circuit, this jumper can be used to decide if FPGA/ARM/None should be allowed to turn off the entropy source (default On through pull-up)



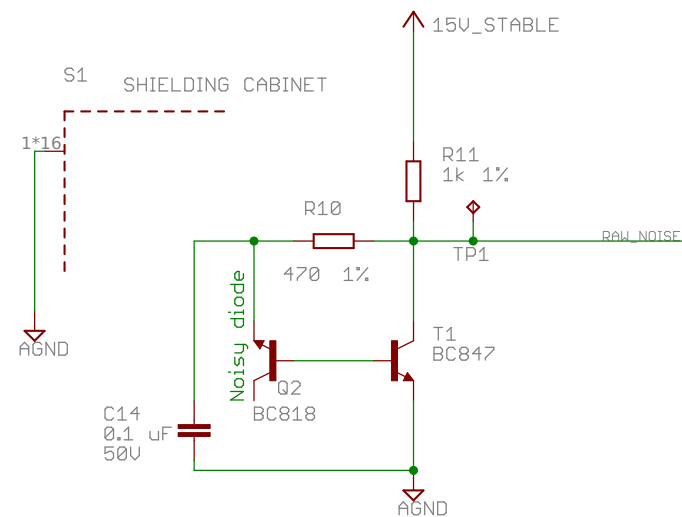
15V LDO powered from external 18V and supplying stable 15V to noise source



\*) Intermediate Regulator: 18V -> 5V

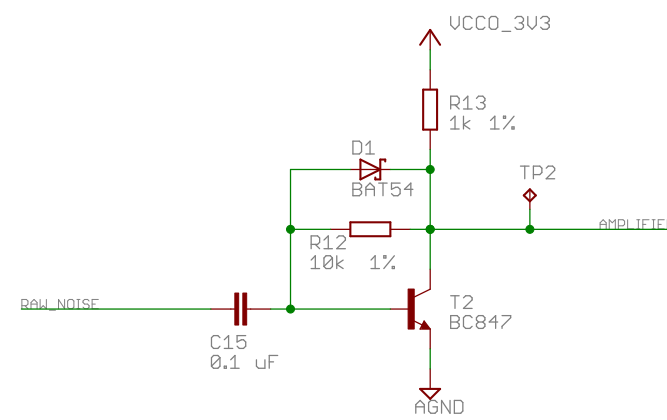


### Noise generator

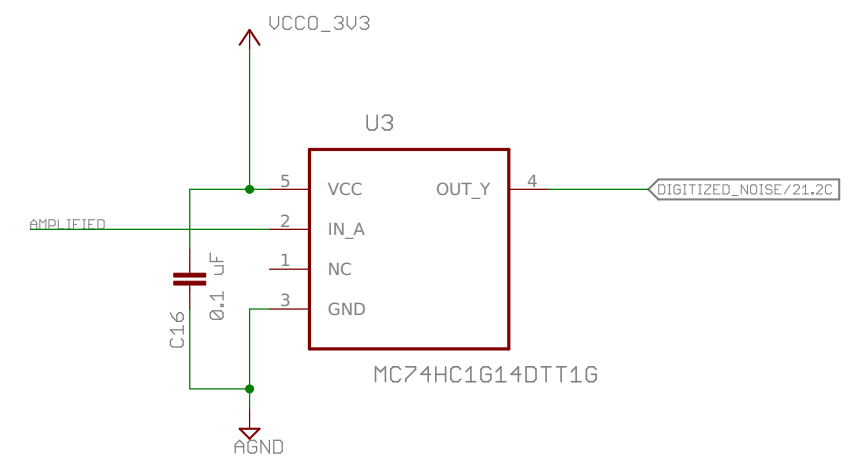


AGND is connected to GND on the board using polygons (found no other good way) - not visible in schematics.

### Amplifier



### Digitizer

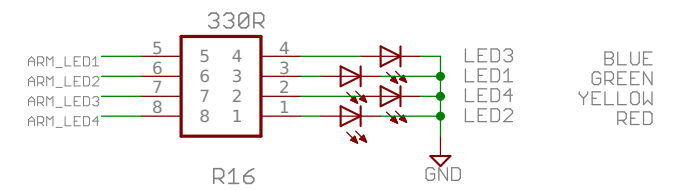
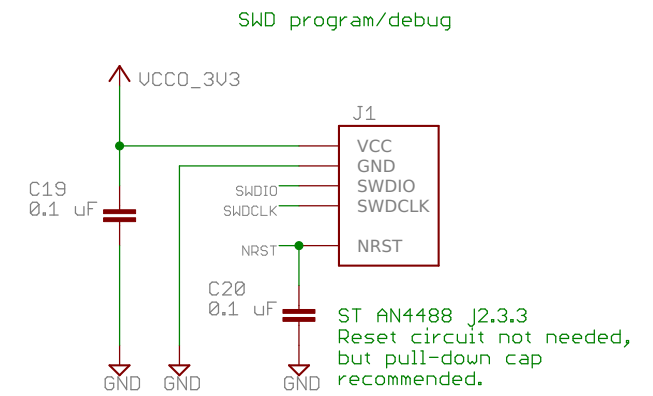
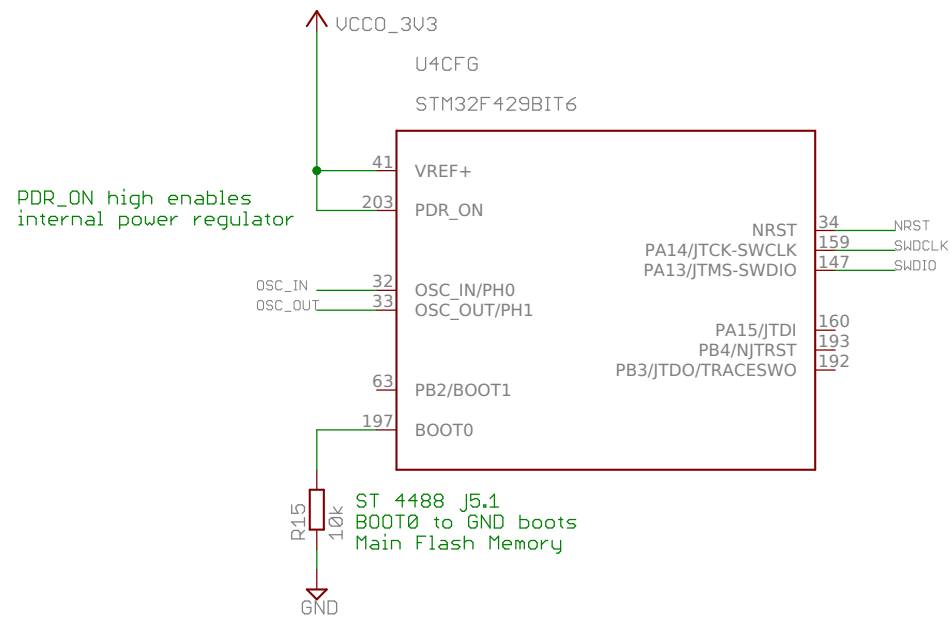
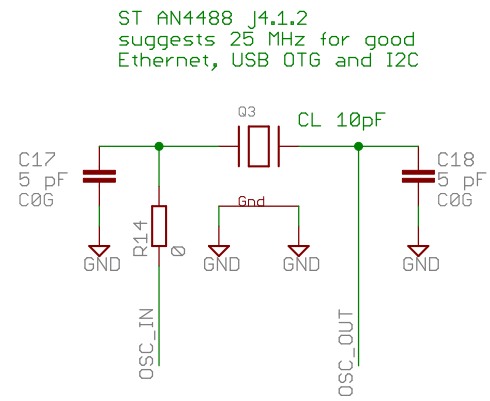


Add optocoupler as per Jacob's suggestion on tech@ 2015-07-24?

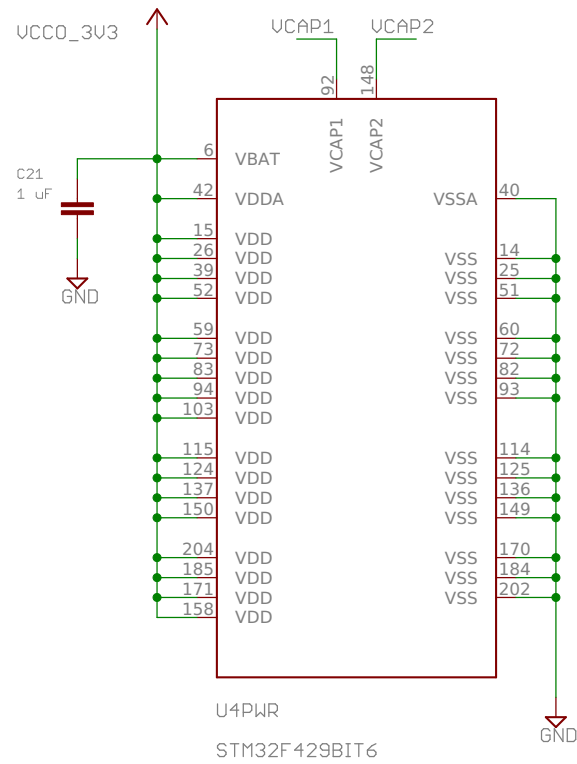
The suggestion is to add a fast optocoupler to really isolate AGND from GND.

As this appears to require a bigger digitizer, we are reluctant to add that for the Alpha.

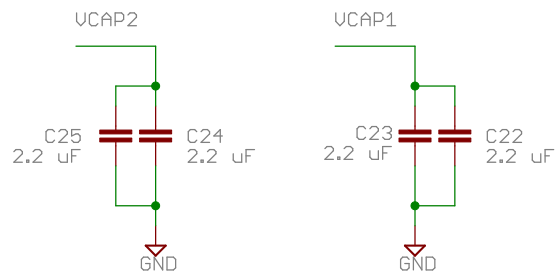
# Basic configuration, STM32



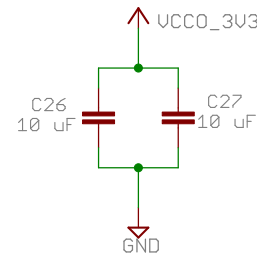
# Power and bypass capacitors, STM32



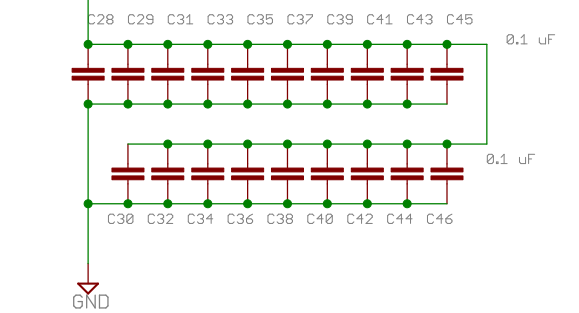
2\*2\*2.2uF LowESR or  
2\*1\*4.7uF LowESR  
< 1 ohm  
(ST AN4488 J2.2)



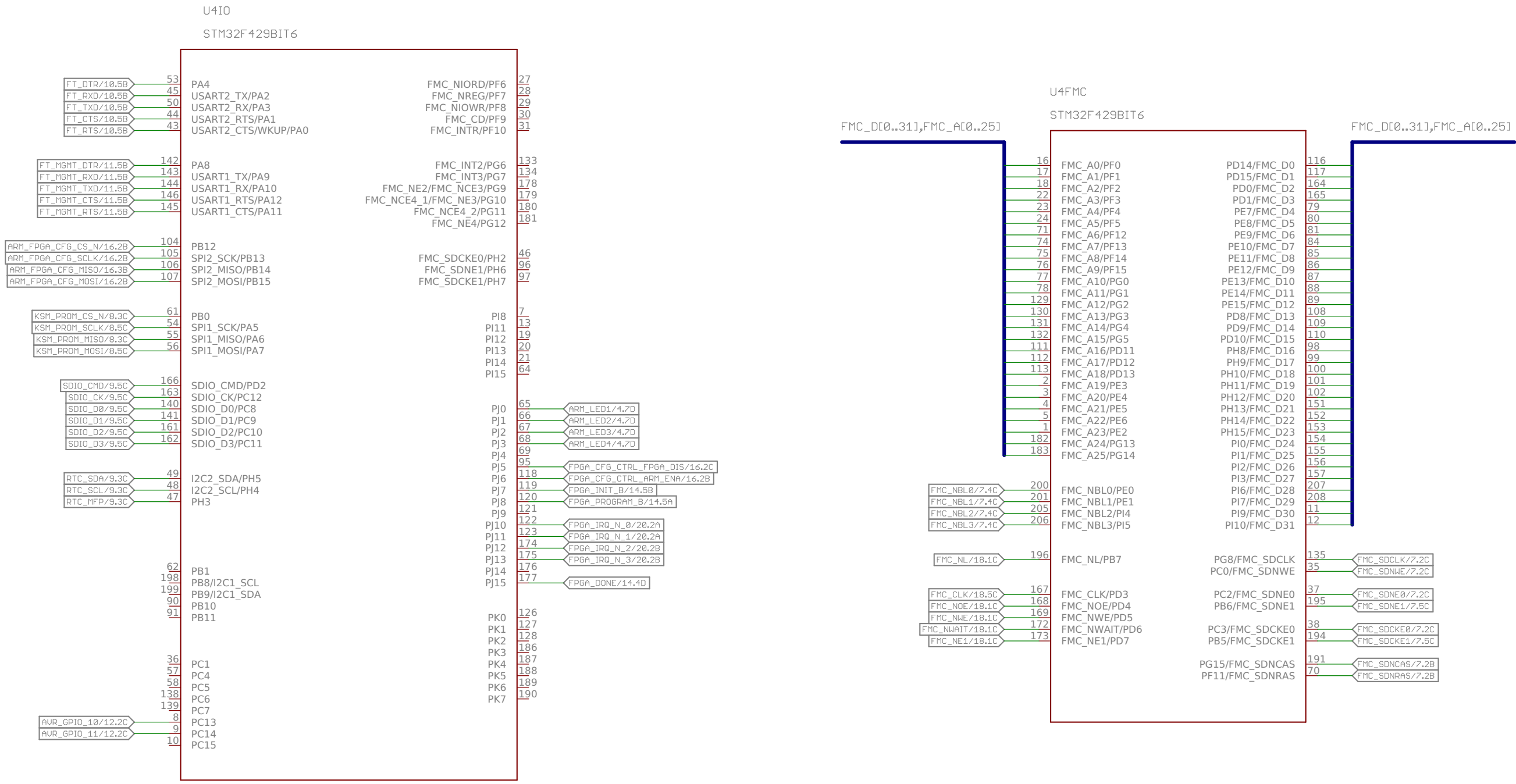
ST AN8844 J2.2  
One 10uF bypass cap for the package.  
(two used for extra comfort)



ST AN8844 J2.2  
One bypass capacitor for every VDD.  
Use 0.1 uF X7R (X5R??) 10U.

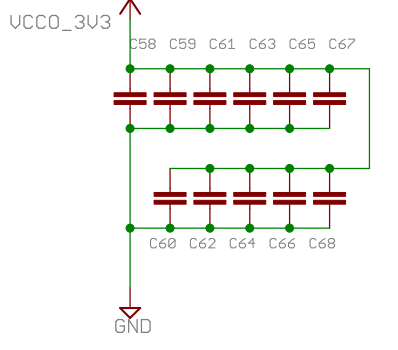
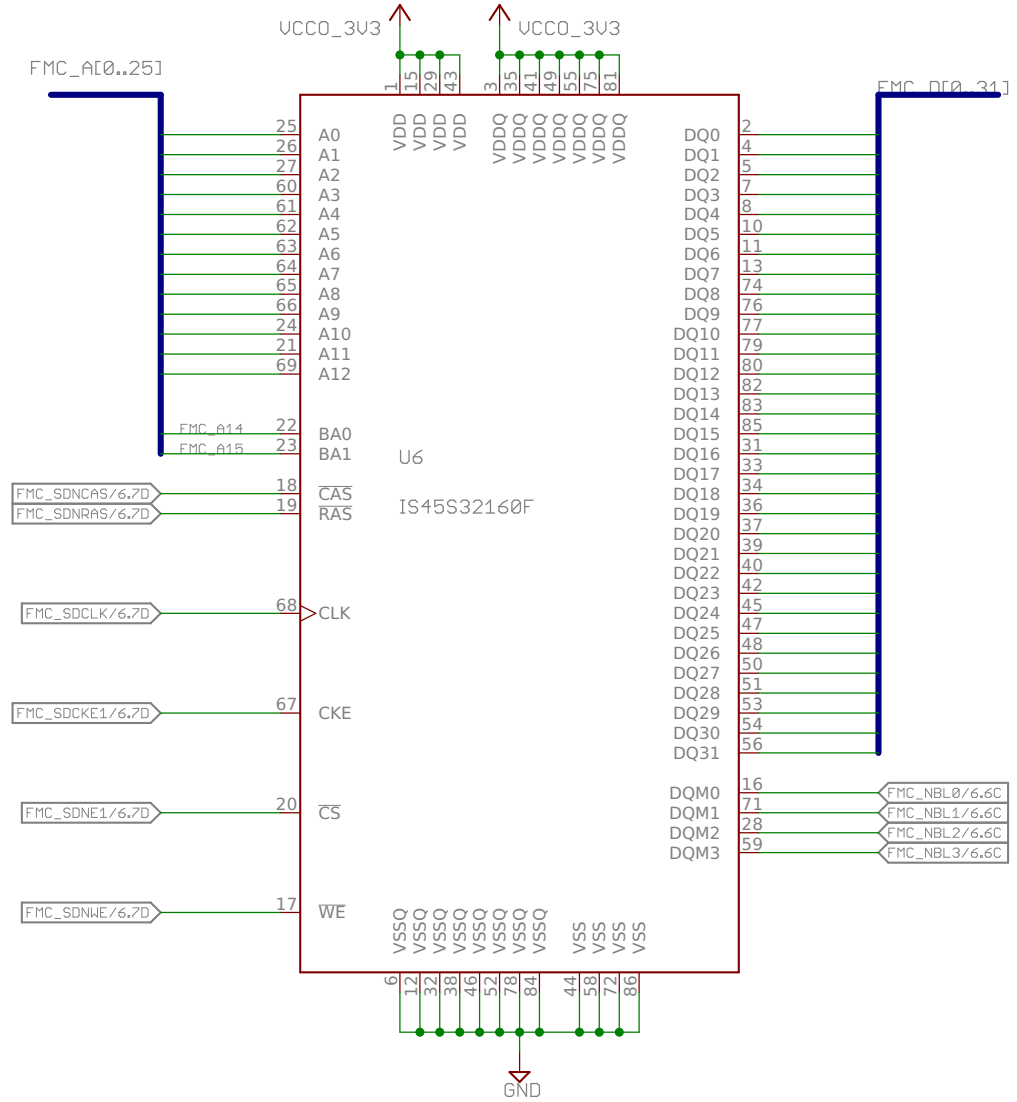
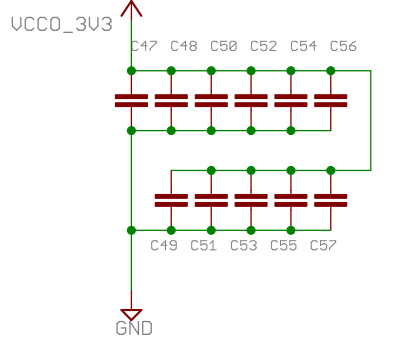
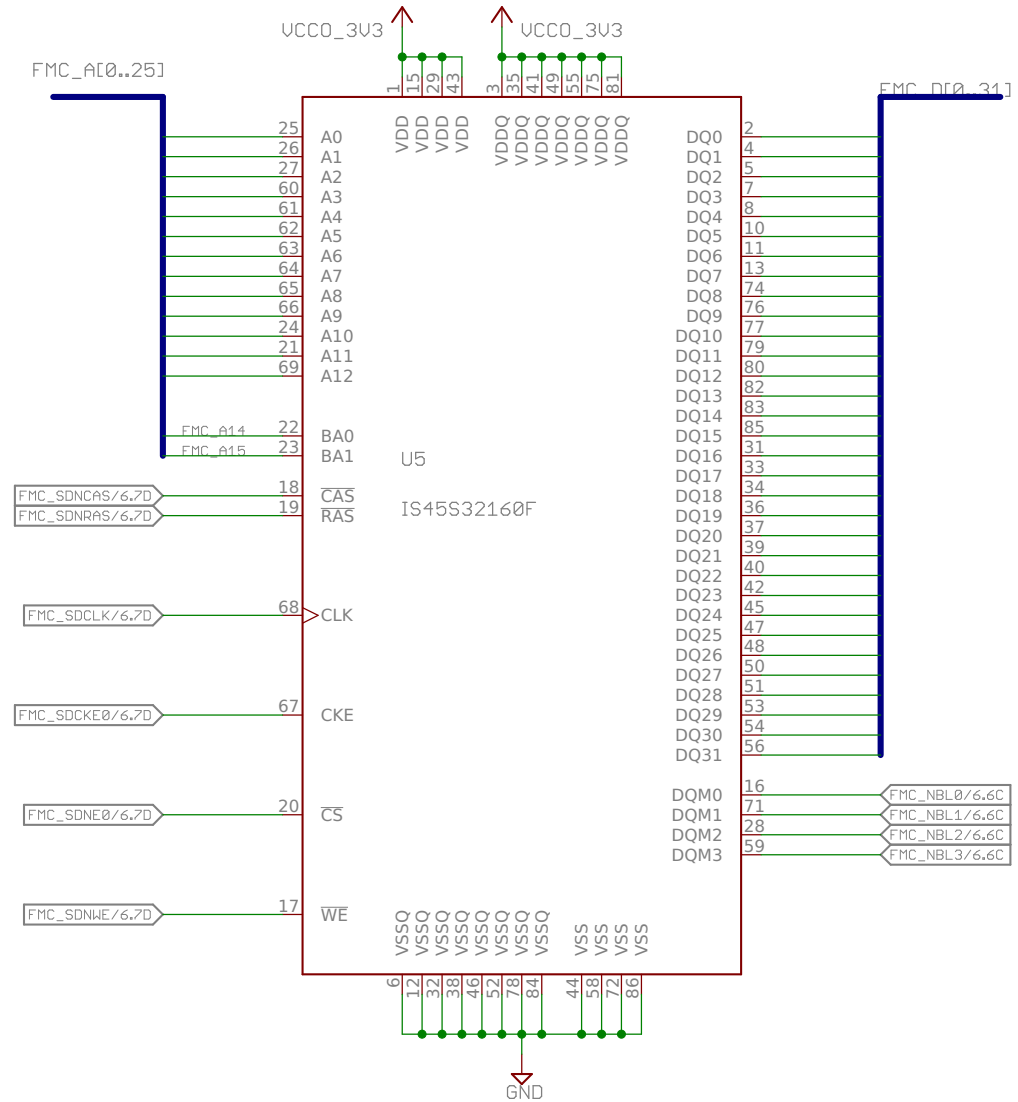


# Input/output, STM32



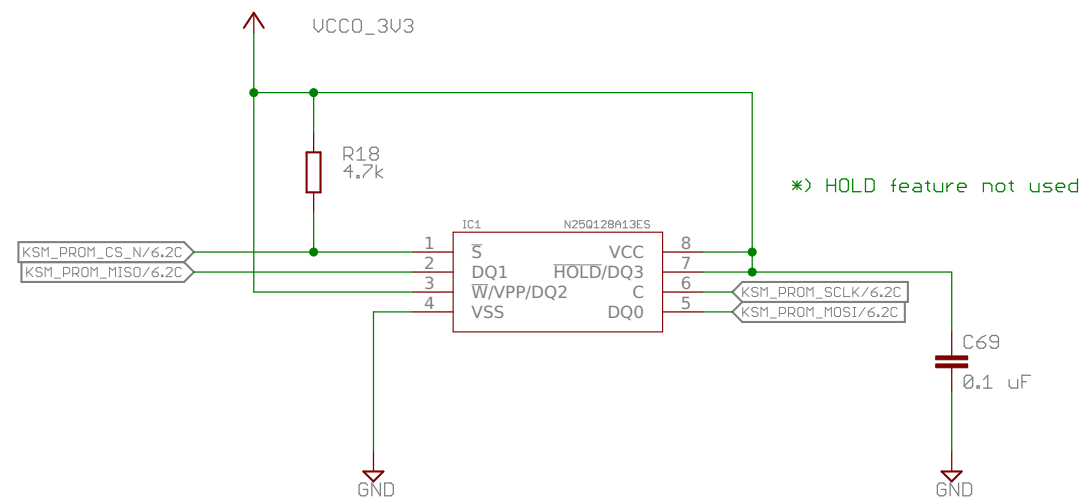
All of these input/outputs can be swapped with equivalent functionality pins.

# 2x512 Mbit SDRAM memory for the ARM



## Keystore memory, 128 Mbit

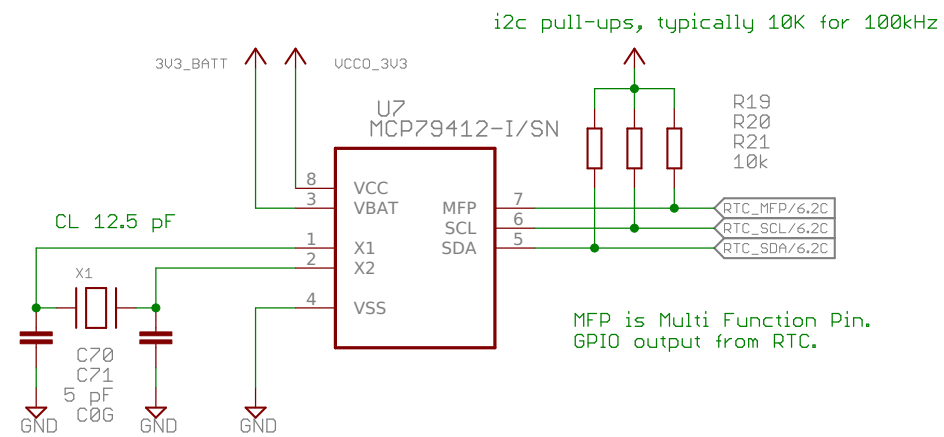
This memory holds cryptographic keys wrapped with the master key.





## Real Time Clock

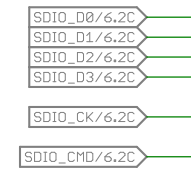
Should we keep this separate chip or rather connect VBAT to the STM32 and use the internal RTC?



## Micro SD card goes here

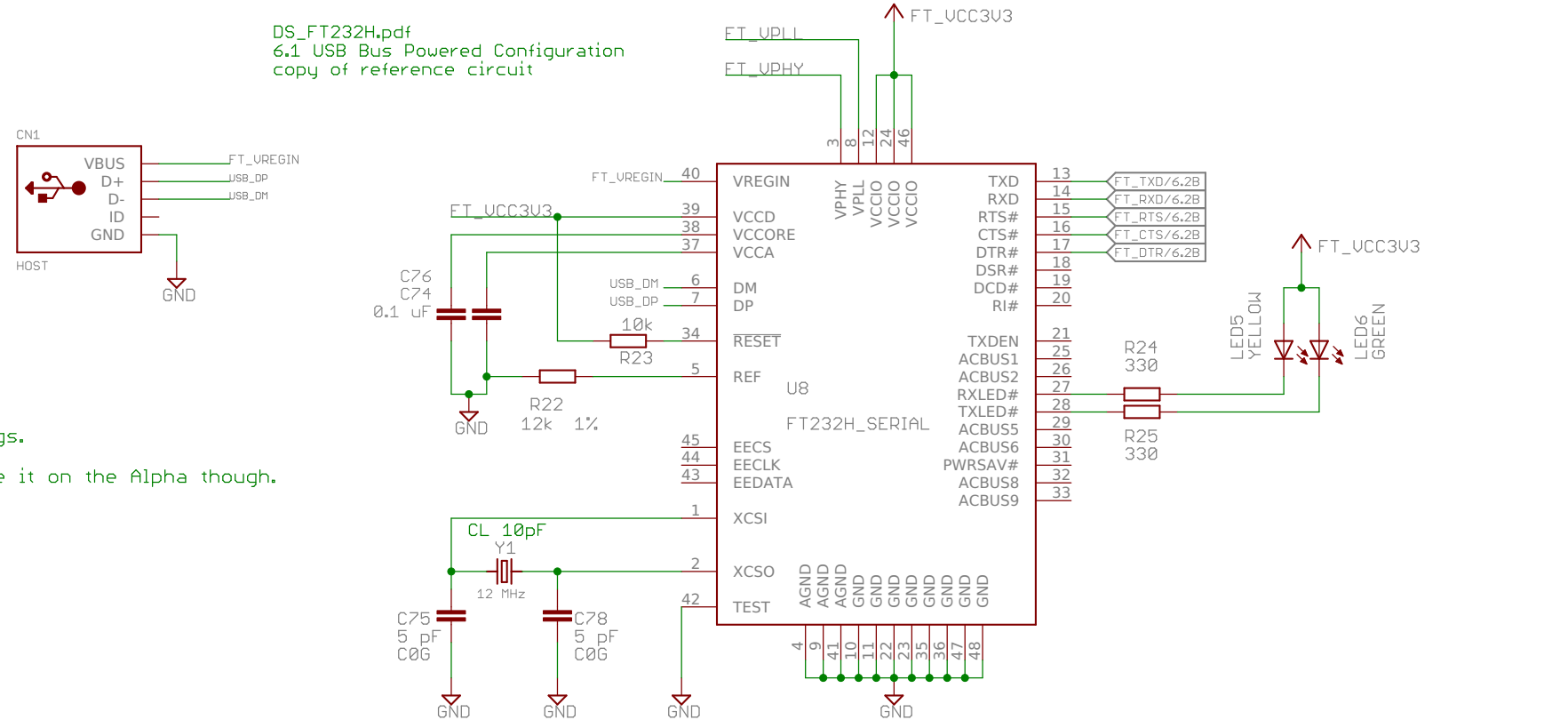
### Questions:

- 1) Which connector to use?  
Haven't found a good one with Eagle symbol. Some different kinds available.
- 2) Novena seems to have card reset capability (power control from MCU).  
Do we want the same?
- 3) Novena has two SD slots, and list power at 200mA.  
Do we need a separate power regulator for the SD card, or can we use VCC0\_3V3?

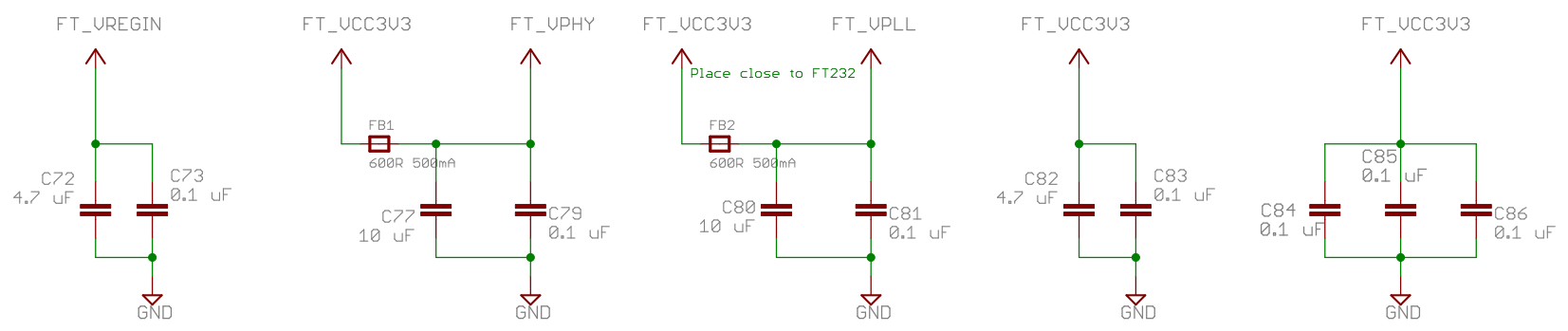


# Application access USB UART

DS\_FT232H.pdf  
6.1 USB Bus Powered Configuration  
copy of reference circuit

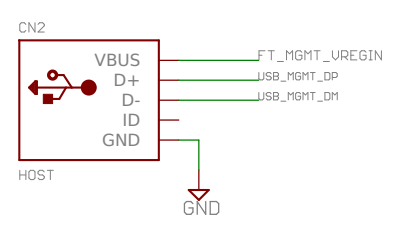


XXX Add EEPROM for USB settings.  
Plan for now is to not populate it on the Alpha though.

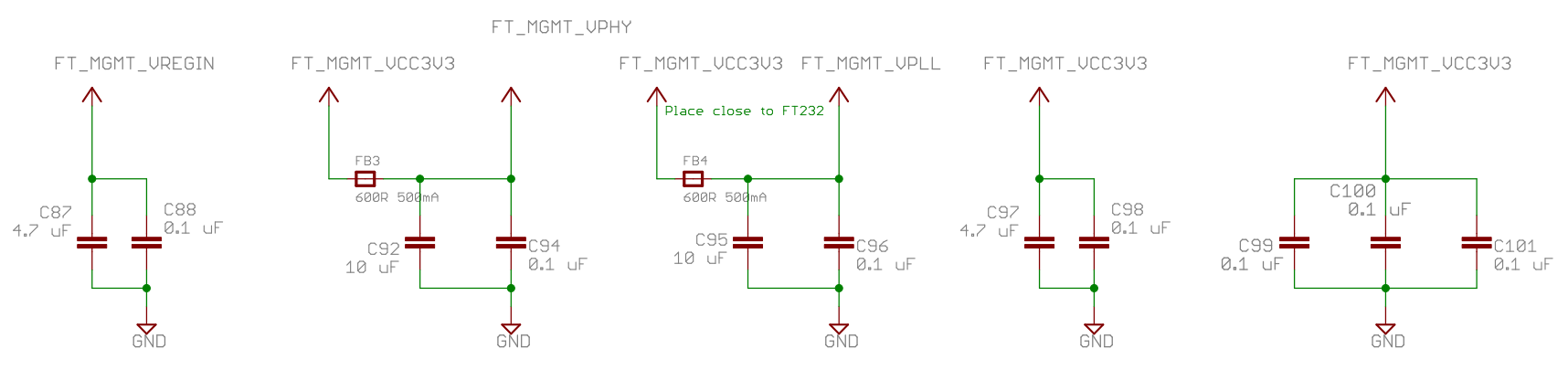
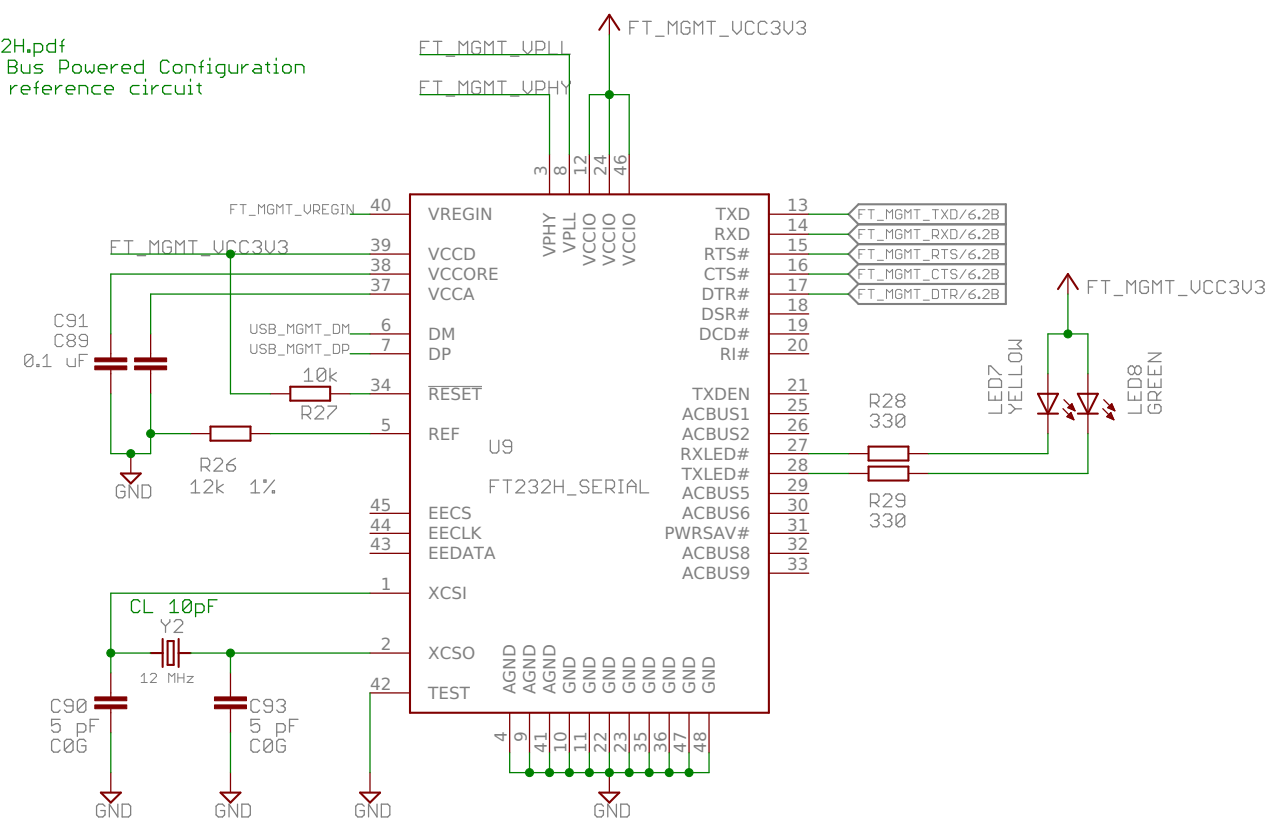


# Management access USB UART

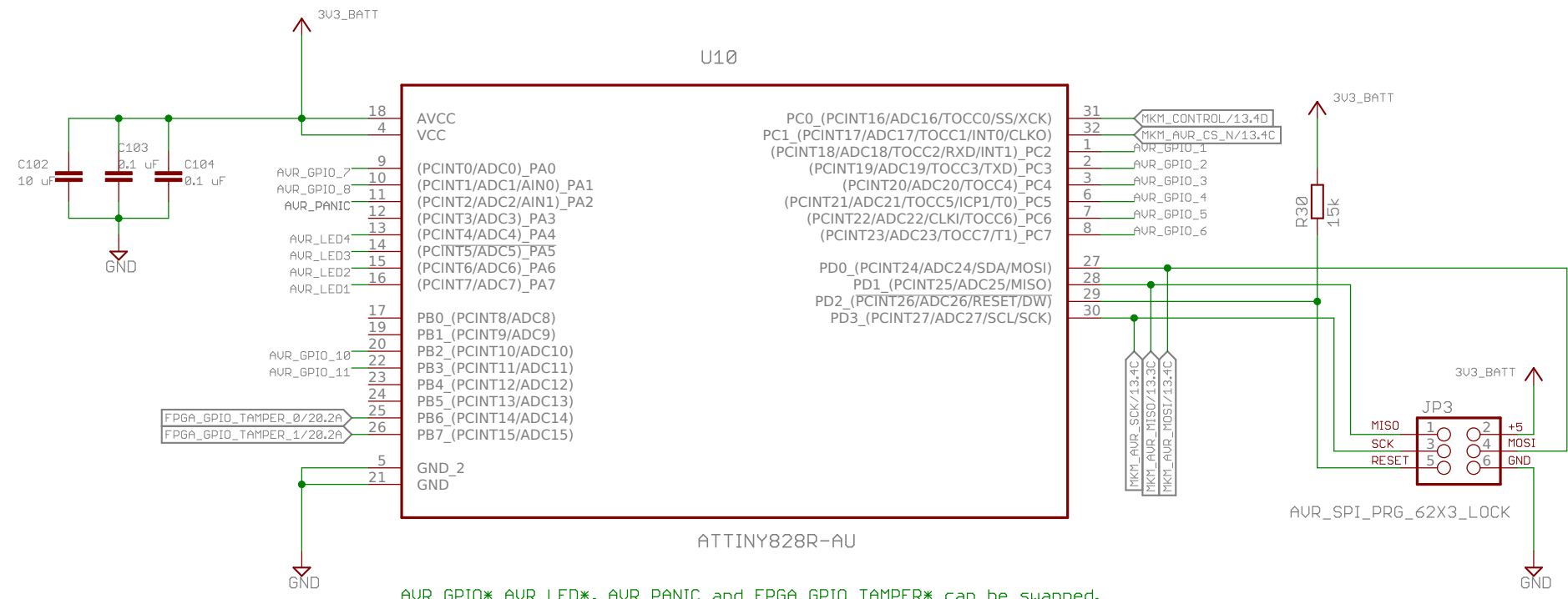
DS\_FT232H.pdf  
6.1 USB Bus Powered Configuration  
copy of reference circuit



XXX Add EEPROM for USB settings.  
Plan for now is to not populate it on the Alpha though.

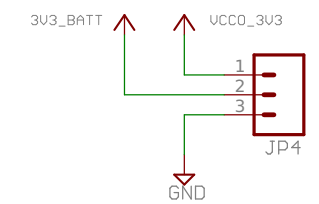


# AVR Tiny Tamper Detect MCU

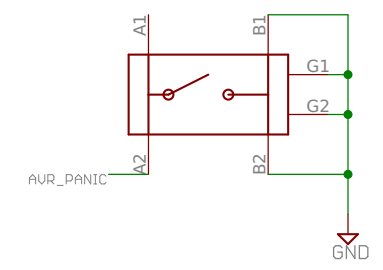


AVR\_GPIO\* AVR\_LED\*, AVR\_PANIC and FPGA\_GPIO\_TAMPER\* can be swapped.

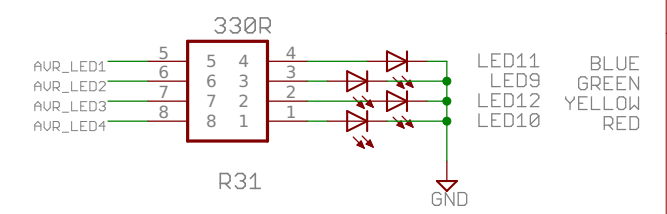
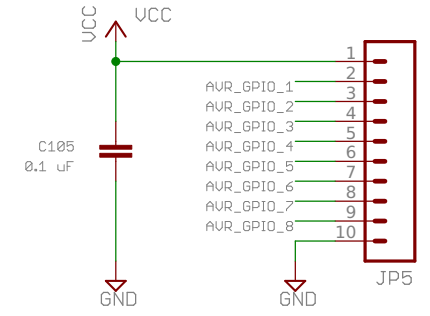
Connector for external 3V3 battery.  
Place a jumper between pins 1-2 to "emulate" having a battery present.



Panic button

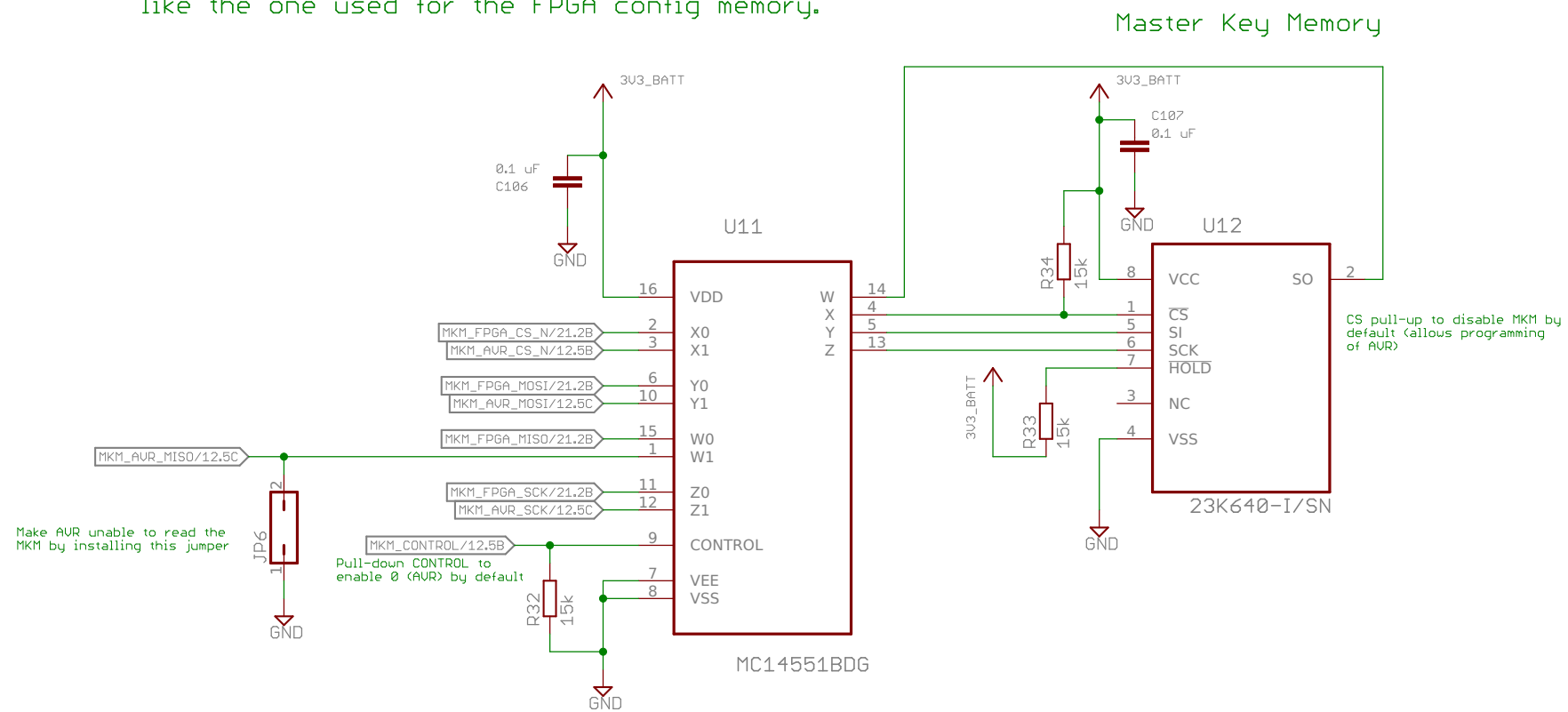


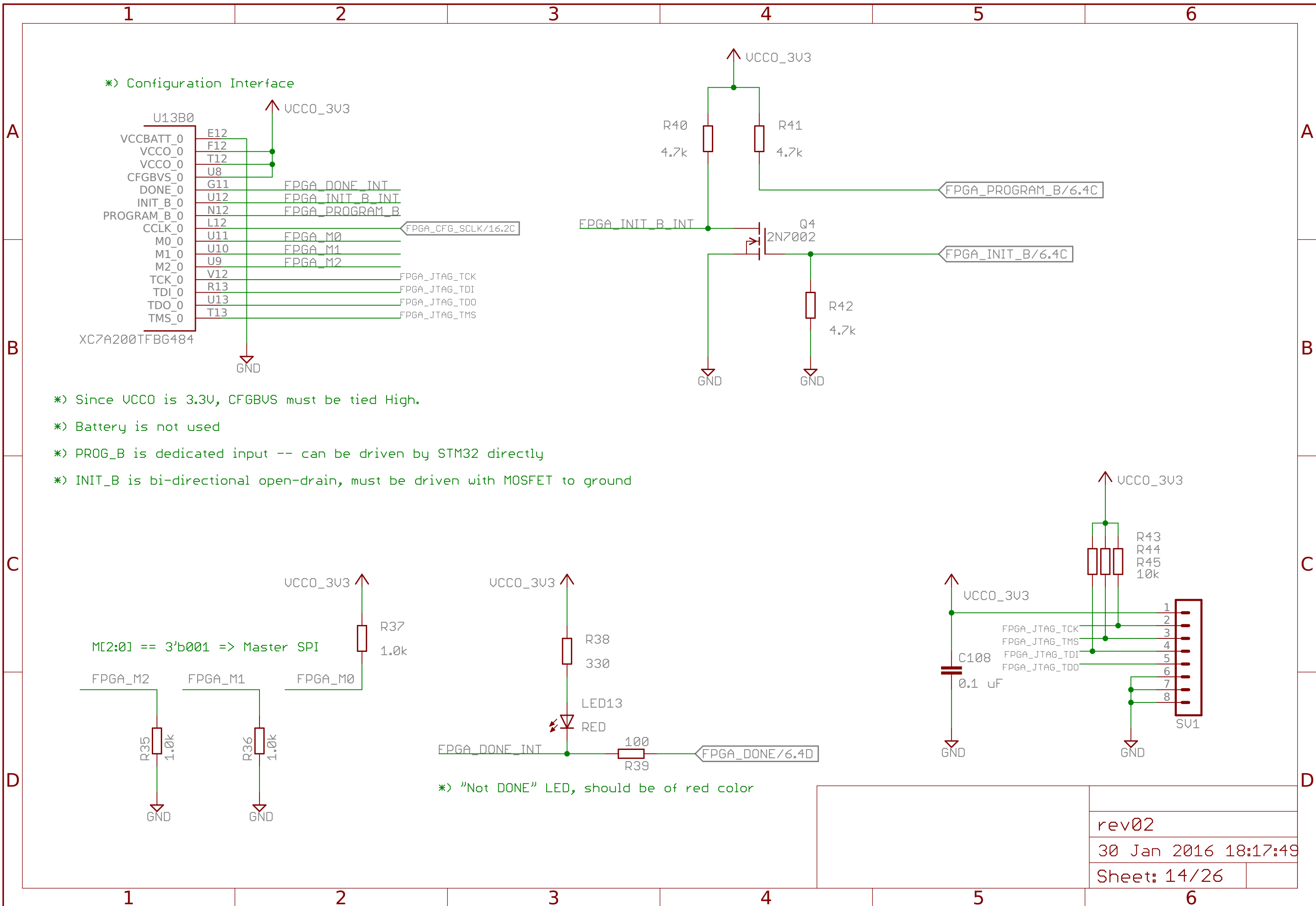
Expansion GPIO



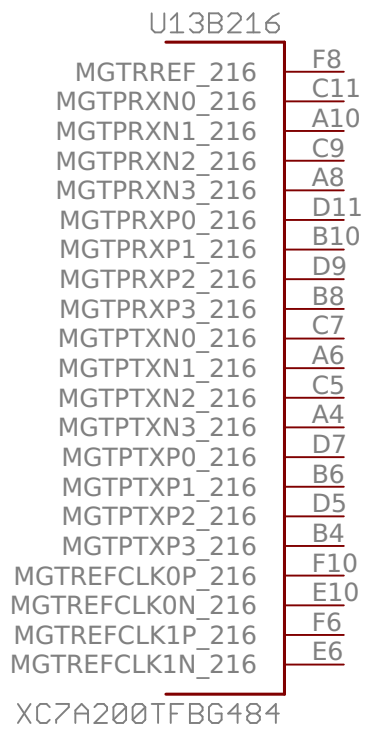
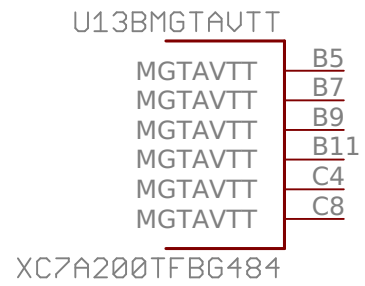
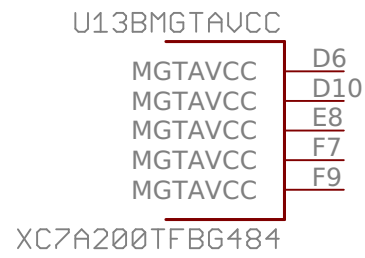
Analog switch controlling access to the MKM.

XXX suggest changing this chip to an 74AC244,  
like the one used for the FPGA config memory.

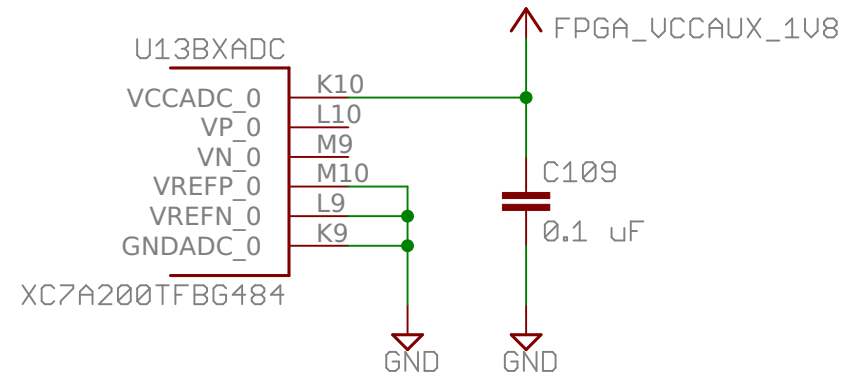




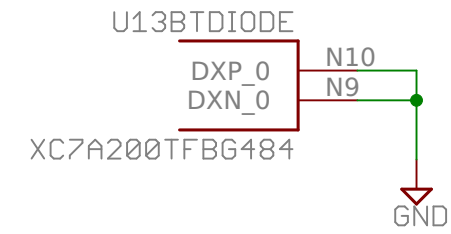
\*> Transceivers [NOT USED]



\*> XADC [NOT USED]



\*> Temperature Sensor [NOT USED]



rev02

30 Jan 2016 18:17:49

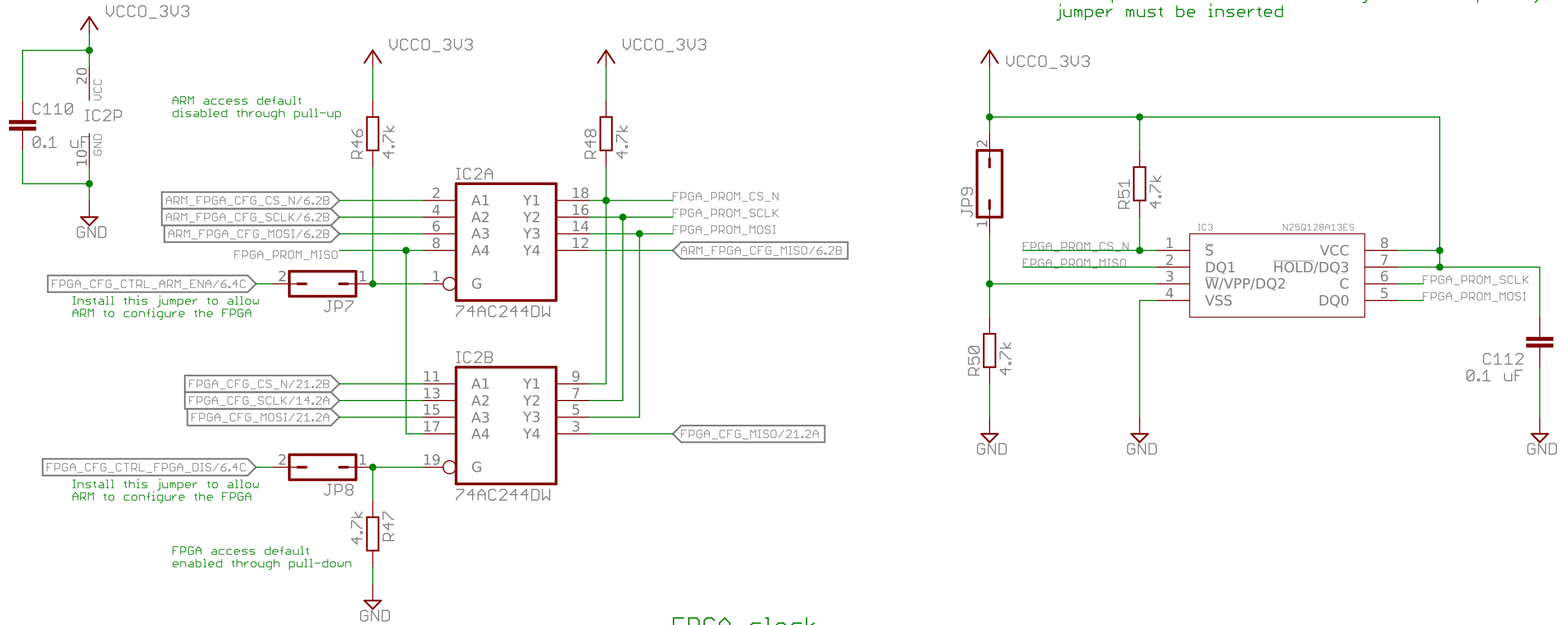
Sheet: 15/26

SPI mux to let ARM override access to FPGA config memory (to reprogram FPGA)

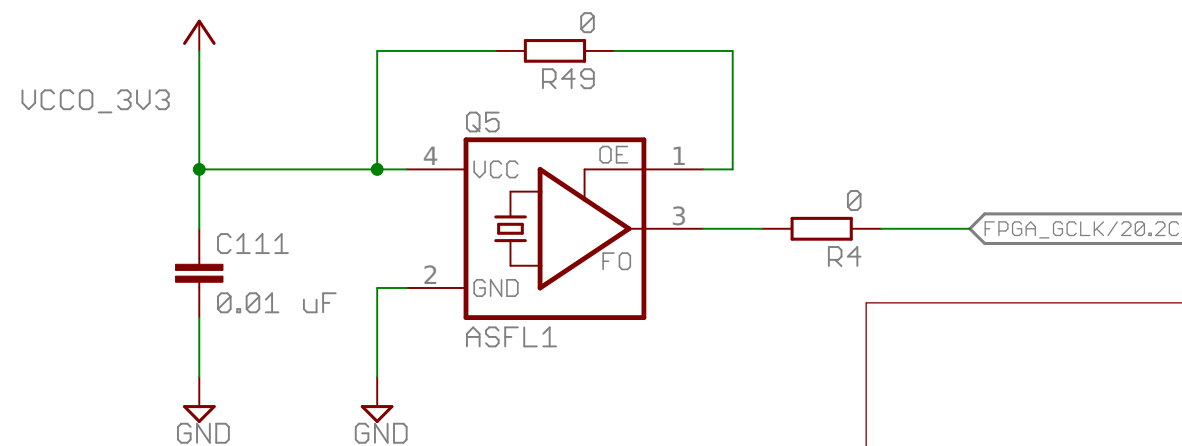
FPGA config memory, 128 Mbit

\*) HOLD feature not used

\*) PROM is write-protected by default, to disable write protection (such as during firmware update), jumper must be inserted



FPGA clock



rev02

30 Jan 2016 18:17:49

Sheet: 16/26



1

2

3

4

5

6

\*> Middle Right Bank

\*> Upper Left Bank

U13B15

U13B35

VCCO\_15 G19 VCCO\_3V3  
 VCCO\_15 H16  
 VCCO\_15 J13 \*> Completely unused banks  
 VCCO\_15 K20 still must be powered  
 VCCO\_15 L17  
 VCCO\_15 N21

VCCO\_35 C1 VCCO\_3V3  
 VCCO\_35 F2  
 VCCO\_35 H6 \*> Completely unused banks  
 VCCO\_35 J3 still must be powered  
 VCCO\_35 M4  
 VCCO\_35 N1

IO\_0\_15 J16  
 IO\_L1P\_T0\_AD0P\_15 H13  
 IO\_L1N\_T0\_AD0N\_15 G13  
 IO\_L2P\_T0\_AD8P\_15 G15  
 IO\_L2N\_T0\_AD8N\_15 G16  
 IO\_L3P\_T0\_DQS\_AD1P\_15 J14  
 IO\_L3N\_T0\_DQS\_AD1N\_15 H14  
 IO\_L4P\_T0\_15 G17  
 IO\_L4N\_T0\_15 G18  
 IO\_L5P\_T0\_AD9P\_15 J15  
 IO\_L5N\_T0\_AD9N\_15 H15  
 IO\_L6P\_T0\_15 H17  
 IO\_L6N\_T0\_VREF\_15 H18  
 IO\_L7P\_T1\_AD2P\_15 J22  
 IO\_L7N\_T1\_AD2N\_15 H22  
 IO\_L8P\_T1\_AD10P\_15 H20  
 IO\_L8N\_T1\_AD10N\_15 G20  
 IO\_L9P\_T1\_DQS\_AD3P\_15 K21  
 IO\_L9N\_T1\_DQS\_AD3N\_15 K22  
 IO\_L10P\_T1\_AD11P\_15 M21  
 IO\_L10N\_T1\_AD11N\_15 L21  
 IO\_L11P\_T1\_SRCC\_15 J20  
 IO\_L11N\_T1\_SRCC\_15 J21  
 IO\_L12P\_T1\_MRCC\_15 J19  
 IO\_L12N\_T1\_MRCC\_15 H19  
 IO\_L13P\_T2\_MRCC\_15 K18  
 IO\_L13N\_T2\_MRCC\_15 K19  
 IO\_L14P\_T2\_SRCC\_15 L19  
 IO\_L14N\_T2\_SRCC\_15 L20  
 IO\_L15P\_T2\_DQS\_15 N22  
 IO\_L15N\_T2\_DQS\_ADV\_B\_15 M22  
 IO\_L16P\_T2\_A28\_15 M18  
 IO\_L16N\_T2\_A27\_15 L18  
 IO\_L17P\_T2\_A26\_15 N18  
 IO\_L17N\_T2\_A25\_15 N19  
 IO\_L18P\_T2\_A24\_15 N20  
 IO\_L18N\_T2\_A23\_15 M20  
 IO\_L19P\_T3\_A22\_15 K13  
 IO\_L19N\_T3\_A21\_VREF\_15 K14  
 IO\_L20P\_T3\_A20\_15 M13  
 IO\_L20N\_T3\_A19\_15 L13  
 IO\_L21P\_T3\_DQS\_15 K17  
 IO\_L21N\_T3\_DQS\_A18\_15 J17  
 IO\_L22P\_T3\_A17\_15 L14  
 IO\_L22N\_T3\_A16\_15 L15  
 IO\_L23P\_T3\_F0E\_B\_15 L16  
 IO\_L23N\_T3\_FWE\_B\_15 K16  
 IO\_L24P\_T3\_RS1\_15 M15  
 IO\_L24N\_T3\_RS0\_15 M16  
 IO\_25\_15 M17

IO\_0\_35 F4  
 IO\_L1P\_T0\_AD4P\_35 B1  
 IO\_L1N\_T0\_AD4N\_35 A1  
 IO\_L2P\_T0\_AD12P\_35 C2  
 IO\_L2N\_T0\_AD12N\_35 B2  
 IO\_L3P\_T0\_DQS\_AD5P\_35 E1  
 IO\_L3N\_T0\_DQS\_AD5N\_35 D1  
 IO\_L4P\_T0\_35 E2  
 IO\_L4N\_T0\_35 D2  
 IO\_L5P\_T0\_AD13P\_35 G1  
 IO\_L5N\_T0\_AD13N\_35 F1  
 IO\_L6P\_T0\_35 F3  
 IO\_L6N\_T0\_VREF\_35 E3  
 IO\_L7P\_T1\_AD6P\_35 K1  
 IO\_L7N\_T1\_AD6N\_35 J1  
 IO\_L8P\_T1\_AD14P\_35 H2  
 IO\_L8N\_T1\_AD14N\_35 G2  
 IO\_L9P\_T1\_DQS\_AD7P\_35 K2  
 IO\_L9N\_T1\_DQS\_AD7N\_35 J2  
 IO\_L10P\_T1\_AD15P\_35 J5  
 IO\_L10N\_T1\_AD15N\_35 H5  
 IO\_L11P\_T1\_SRCC\_35 H3  
 IO\_L11N\_T1\_SRCC\_35 G3  
 IO\_L12P\_T1\_MRCC\_35 H4  
 IO\_L12N\_T1\_MRCC\_35 G4  
 IO\_L13P\_T2\_MRCC\_35 K4  
 IO\_L13N\_T2\_MRCC\_35 J4  
 IO\_L14P\_T2\_SRCC\_35 L3  
 IO\_L14N\_T2\_SRCC\_35 K3  
 IO\_L15P\_T2\_DQS\_35 M1  
 IO\_L15N\_T2\_DQS\_35 L1  
 IO\_L16P\_T2\_35 M3  
 IO\_L16N\_T2\_35 M2  
 IO\_L17P\_T2\_35 K6  
 IO\_L17N\_T2\_35 J6  
 IO\_L18P\_T2\_35 L5  
 IO\_L18N\_T2\_35 L4  
 IO\_L19P\_T3\_35 N4  
 IO\_L19N\_T3\_VREF\_35 N3  
 IO\_L20P\_T3\_35 R1  
 IO\_L20N\_T3\_35 P1  
 IO\_L21P\_T3\_DQS\_35 P5  
 IO\_L21N\_T3\_DQS\_35 P4  
 IO\_L22P\_T3\_35 P2  
 IO\_L22N\_T3\_35 N2  
 IO\_L23P\_T3\_35 M6  
 IO\_L23N\_T3\_35 M5  
 IO\_L24P\_T3\_35 P6  
 IO\_L24N\_T3\_35 N5  
 IO\_25\_35 L6

XC7A200TFBG484

XC7A200TFBG484

rev02

30 Jan 2016 18:17:49

Sheet: 17/26

1

2

3

4

5

6

A

B

C

D

A

B

C

D

1

2

3

4

5

6

\*) Lower Left Bank

\*) Bottom Bank

A

A

B

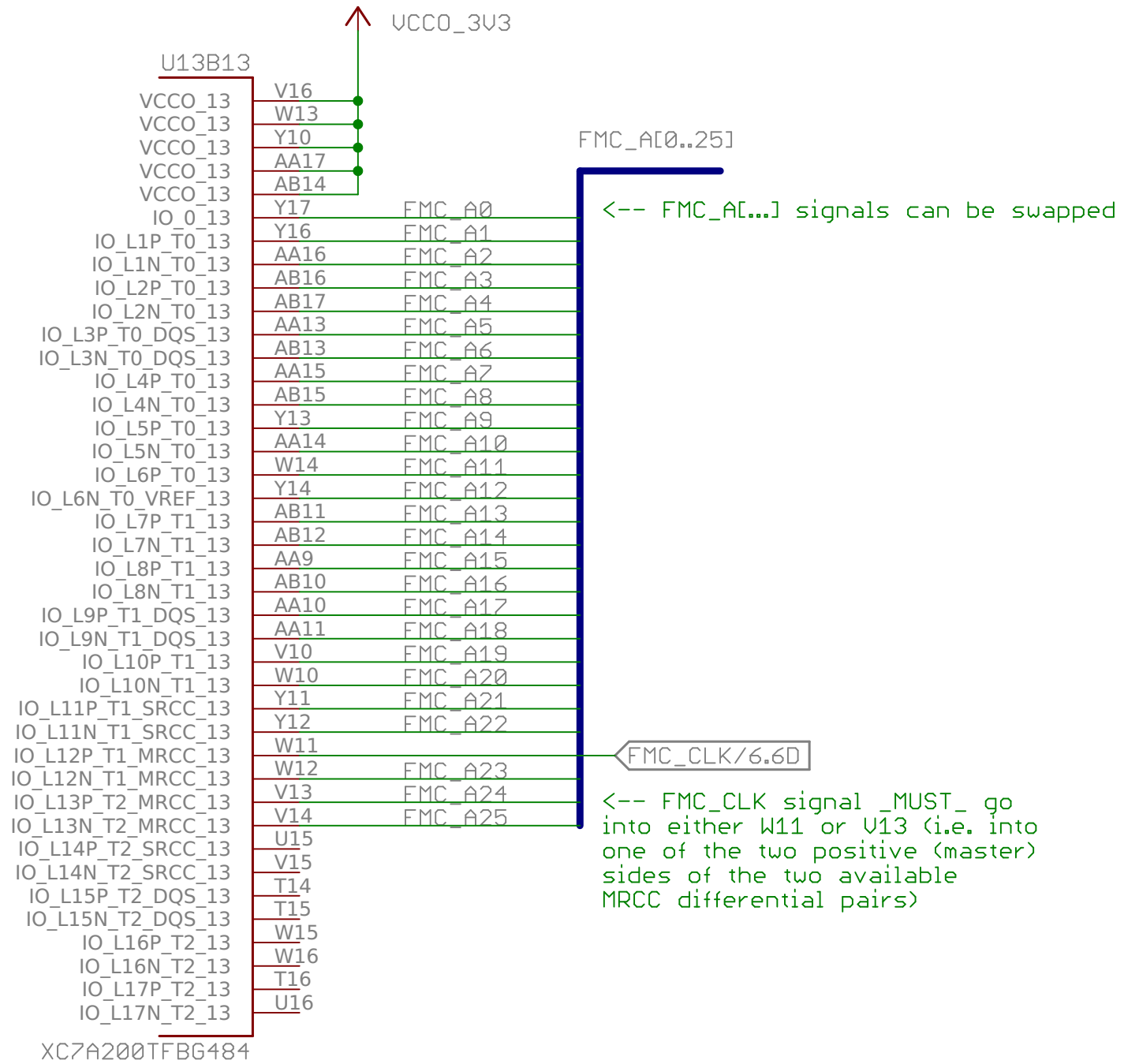
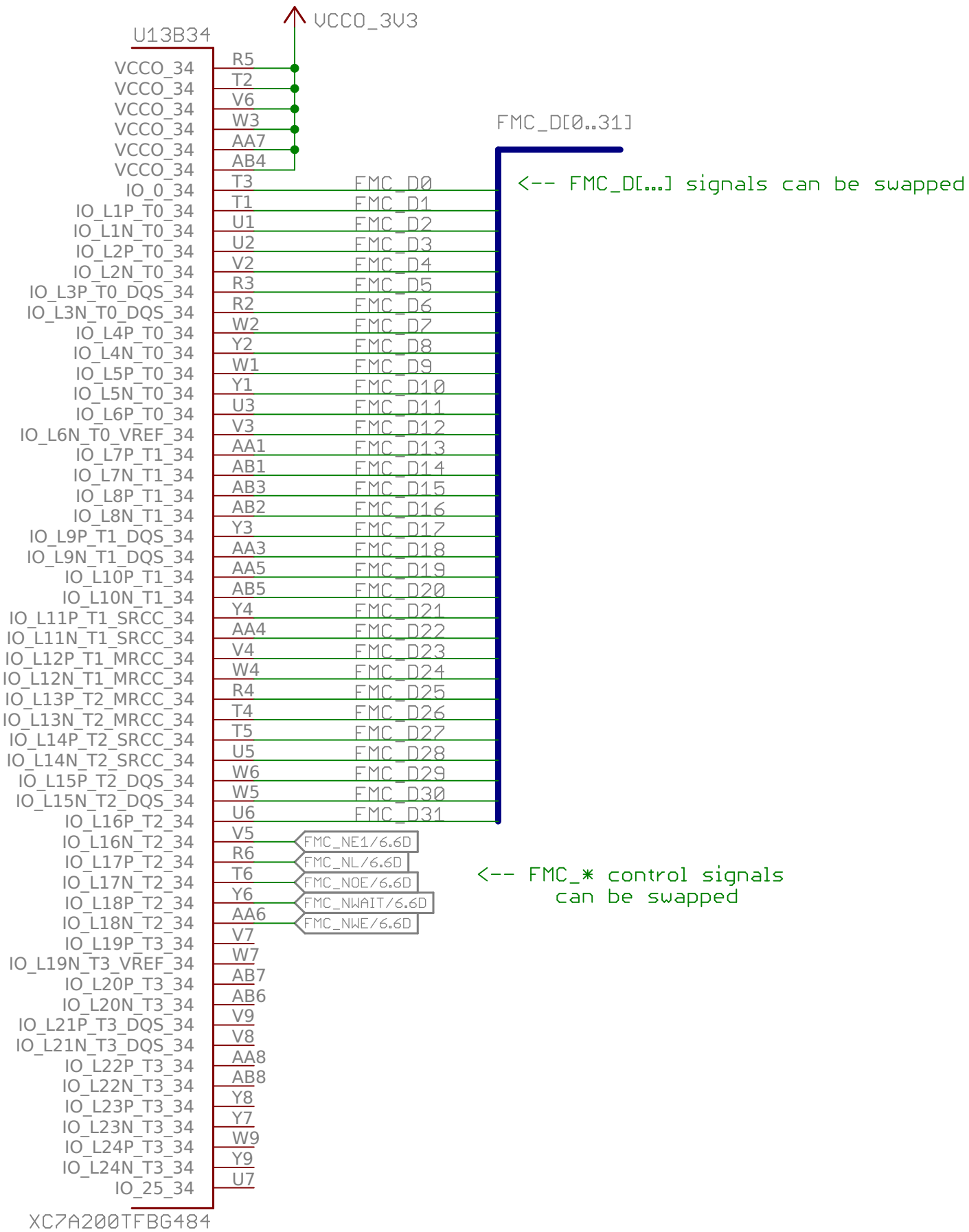
B

C

C

D

D



1

2

3

4

5

6

rev02

30 Jan 2016 18:17:49

Sheet: 18/26

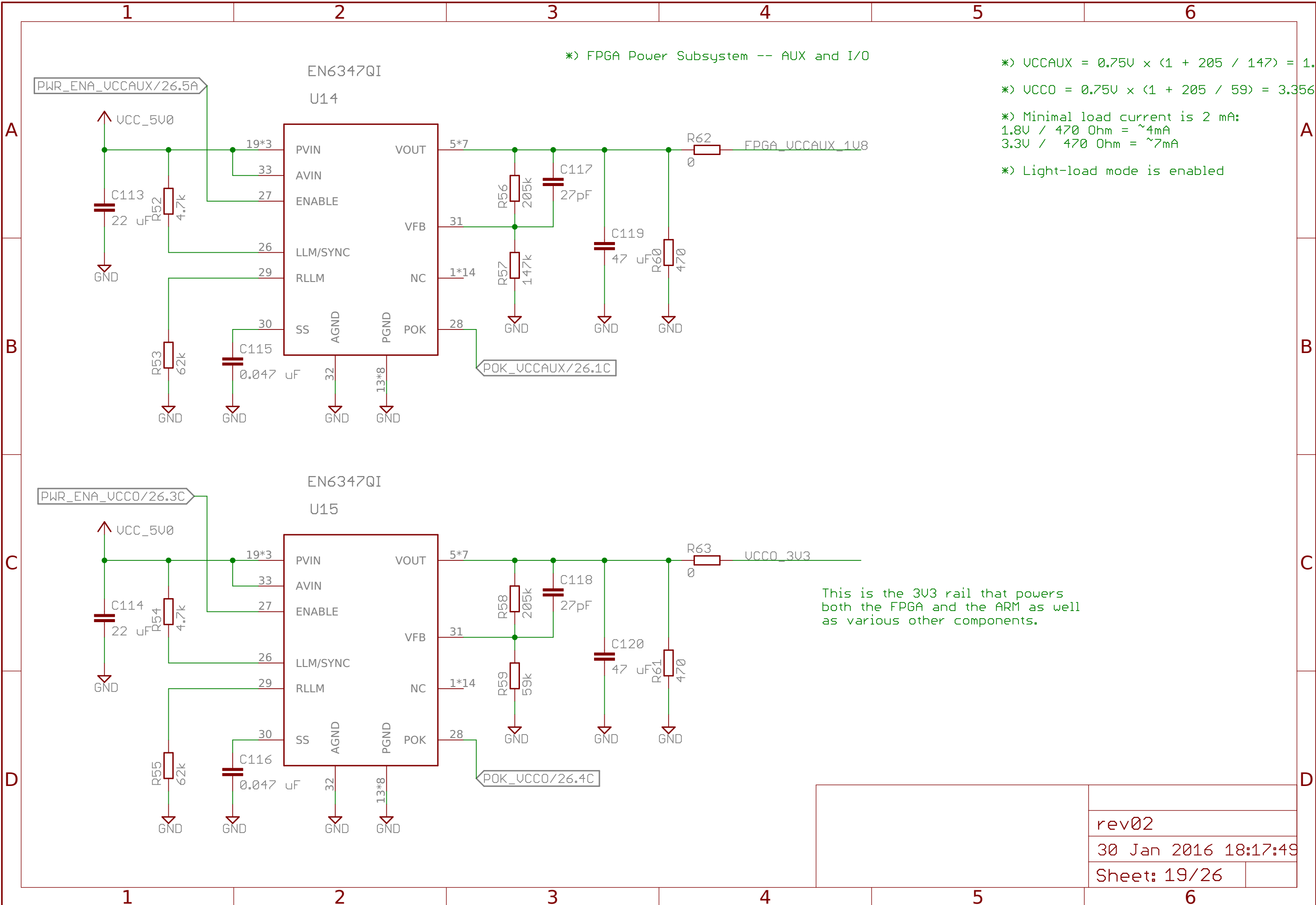
\*) FPGA Power Subsystem -- AUX and I/O

$$*) V_{CCAUX} = 0.75V \times (1 + 205 / 147) = 1.796V$$

$$*) V_{CC0} = 0.75V \times (1 + 205 / 59) = 3.356V$$

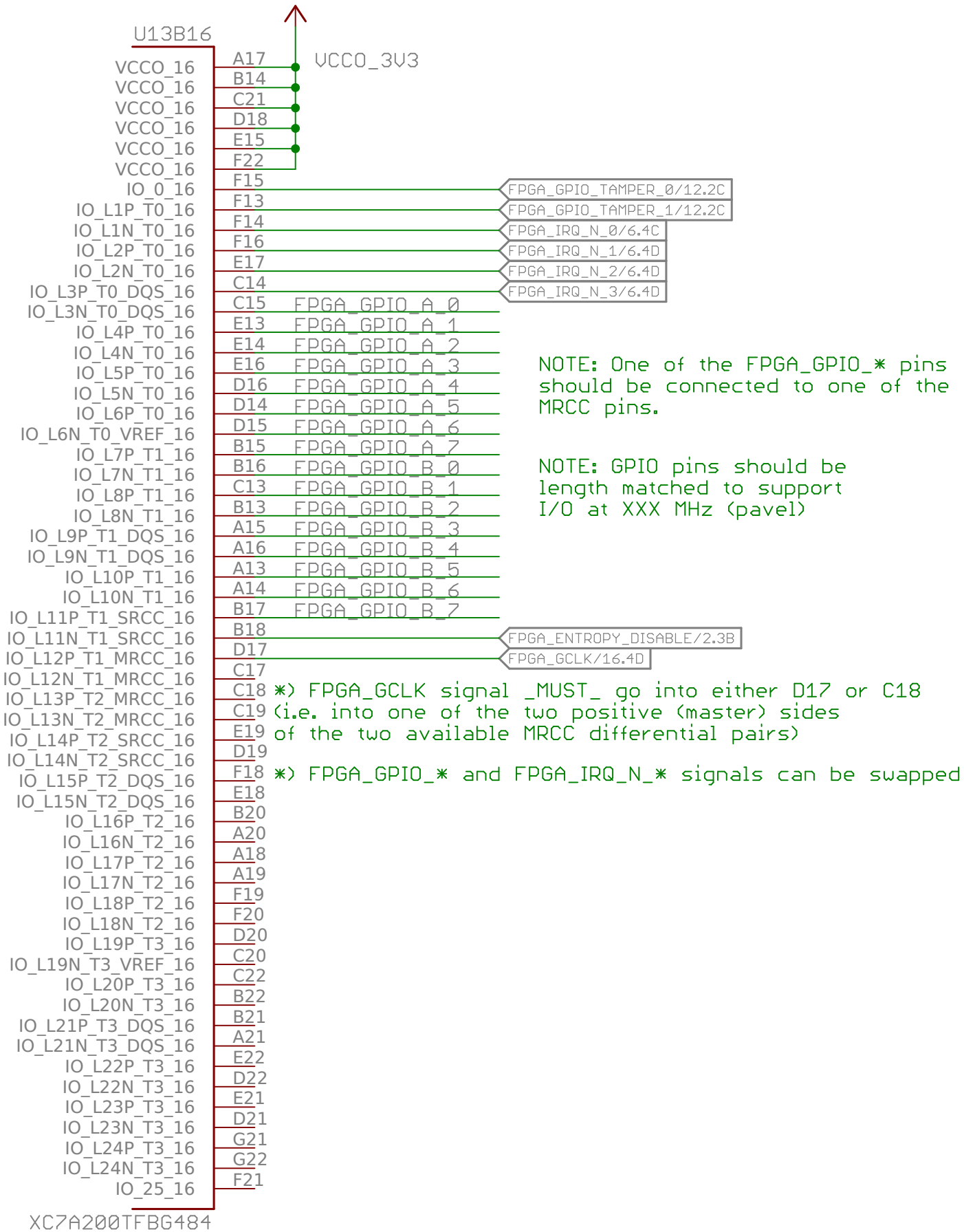
\*) Minimal load current is 2 mA:  
 $1.8V / 470 \text{ Ohm} = \sim 4mA$   
 $3.3V / 470 \text{ Ohm} = \sim 7mA$

\*) Light-load mode is enabled

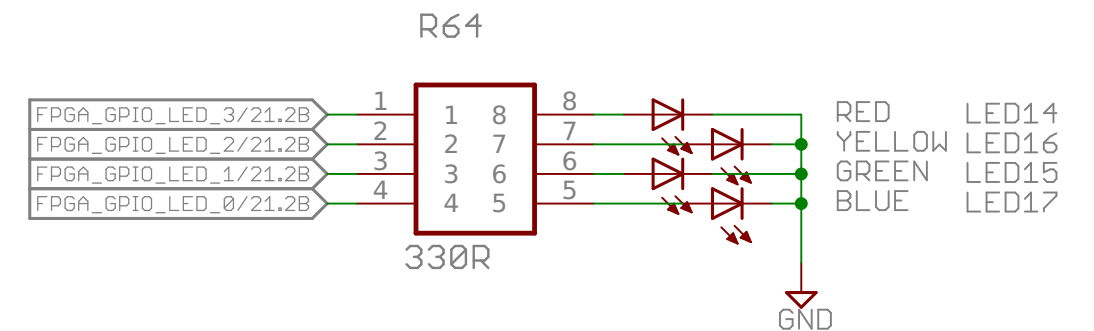
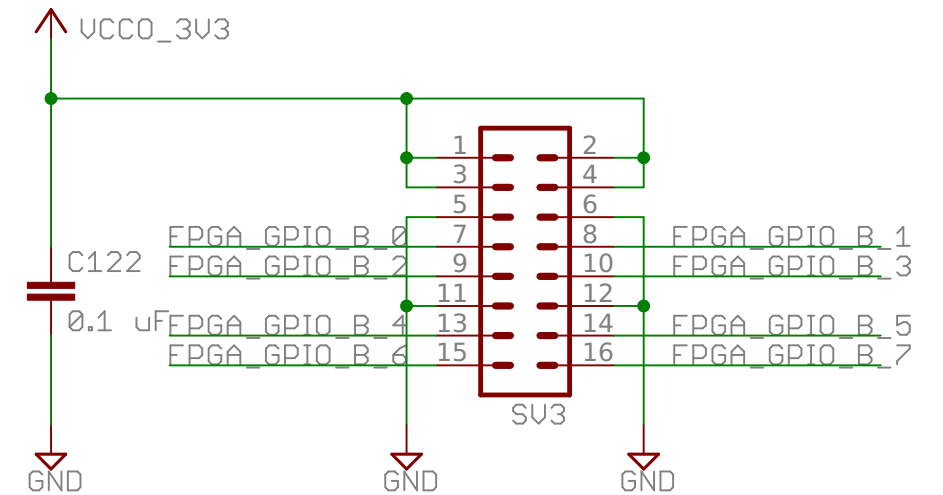
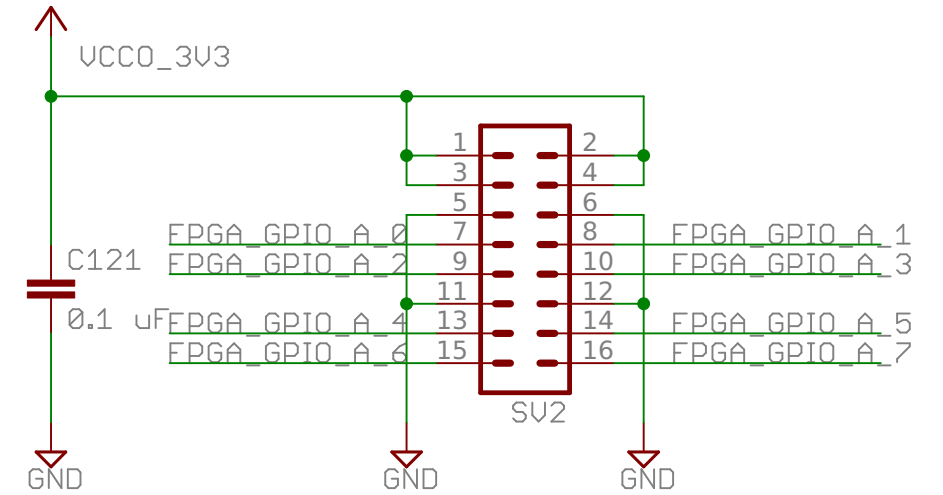


This is the 3V3 rail that powers both the FPGA and the ARM as well as various other components.

\* Upper Right Bank



\* Signals, that are allowed to be swapped, can be swapped with each other and/or moved to different pins within their bank.



rev02

30 Jan 2016 18:17:49

Sheet: 20/26

1

2

3

4

5

6

\*) Lower Right Bank

\*) Signals, that are allowed to be swapped, can be swapped with each other and/or moved to different pins within their bank.

A

A

B

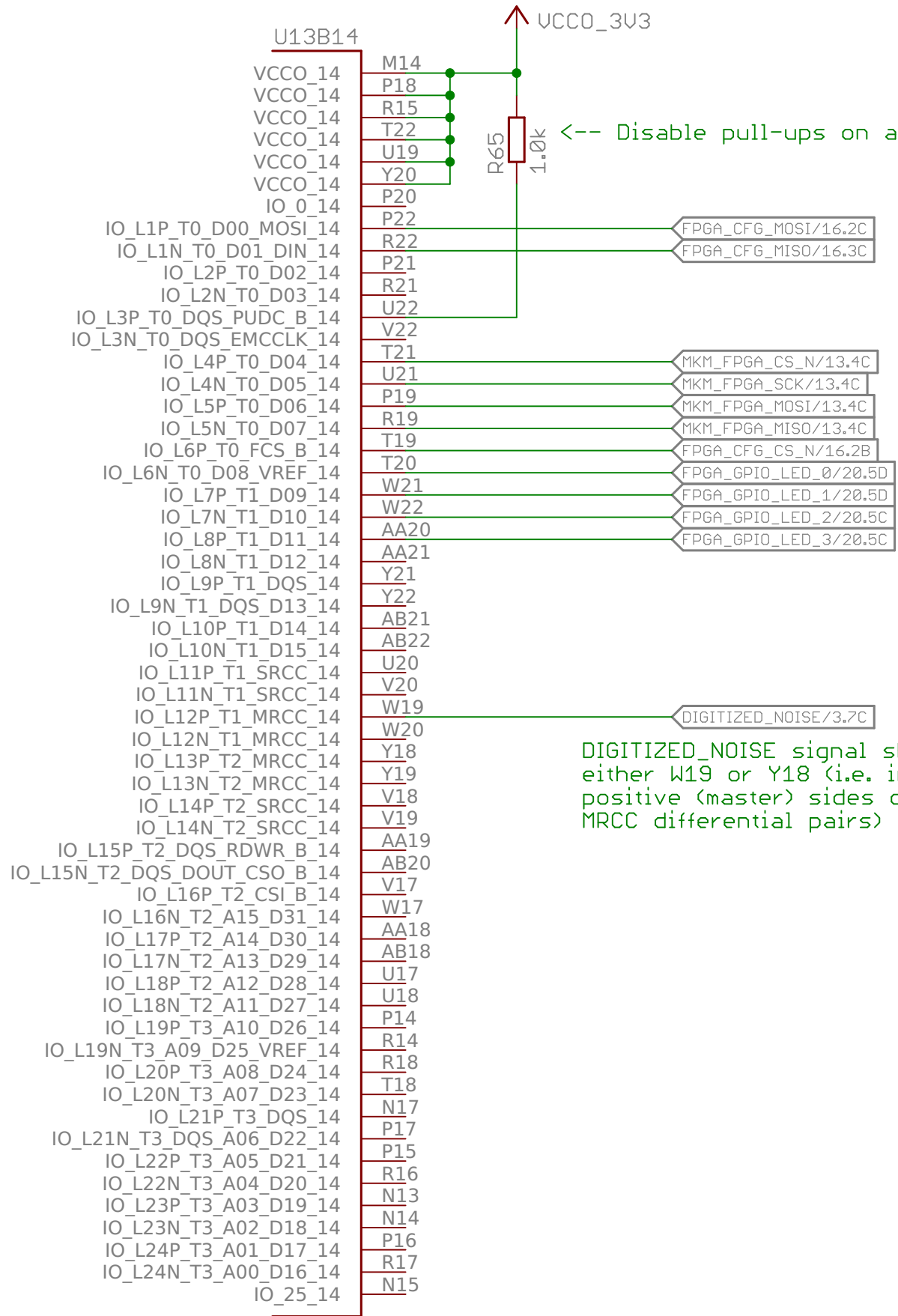
B

C

C

D

D



<-- FPGA\_GPIO\_\* and FPGA\_IRQ\_N\_\* signals can be swapped

DIGITIZED\_NOISE signal should go into either W19 or Y18 (i.e. into one of the two positive (master) sides of the two available MRCC differential pairs)

1

2

3

4

5

6

XC7A200TFBG484

1

2

3

4

5

6

A

A

\*) Ground Pins

\*) Power - CORE & BRAM

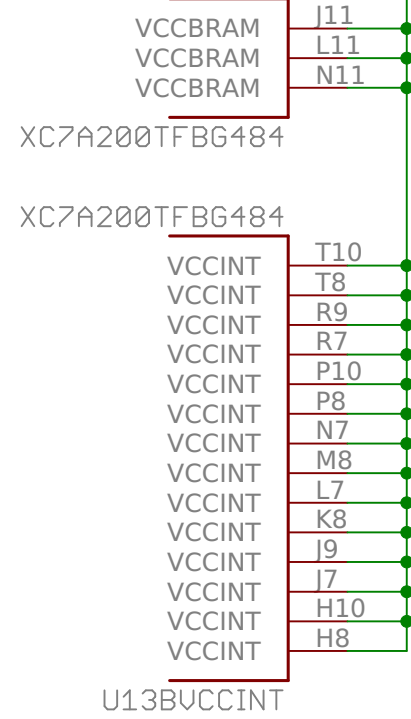
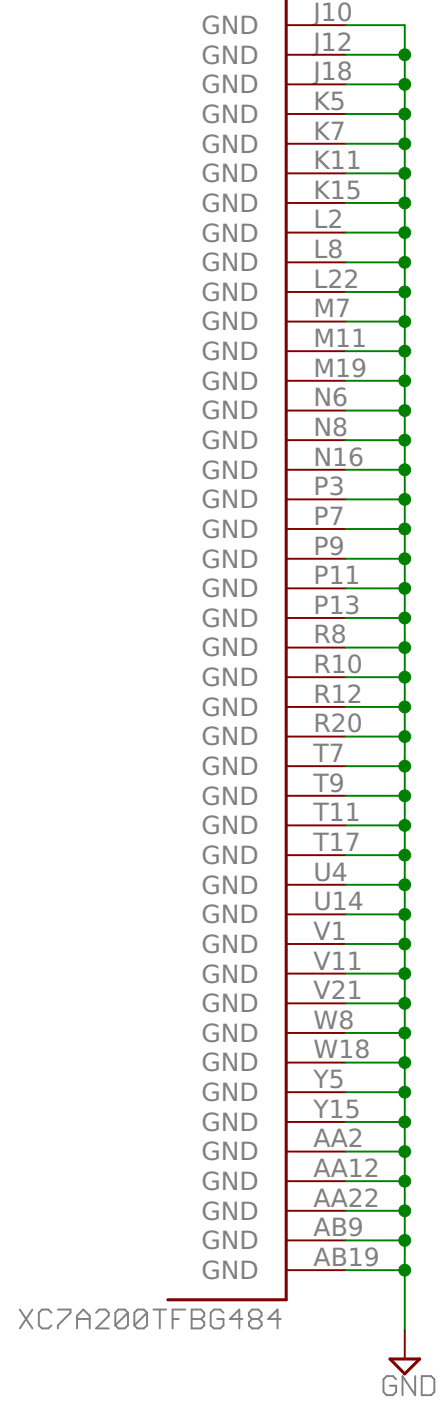
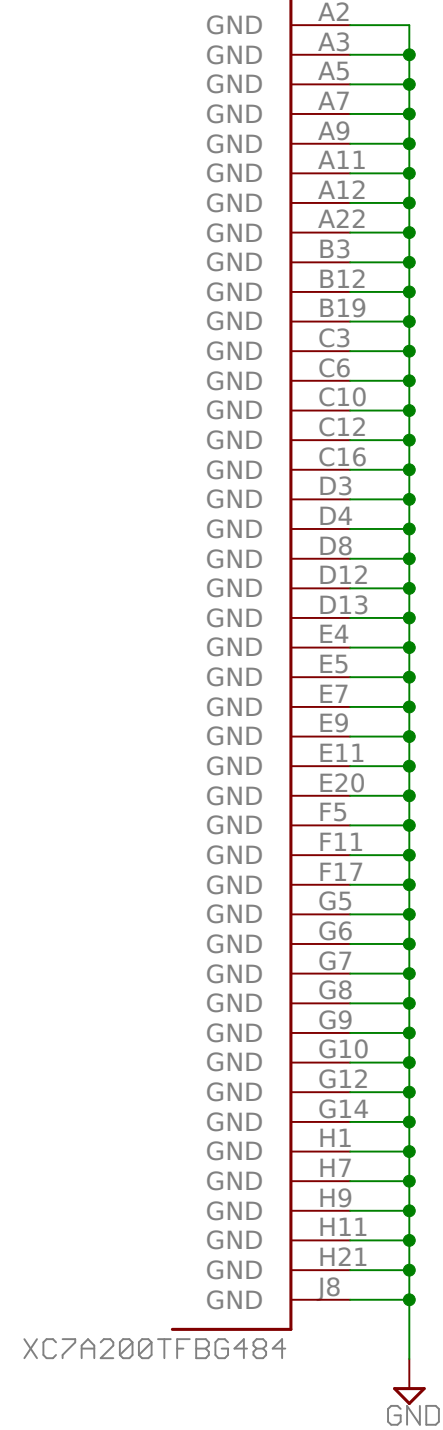
\*) Power - AUX

U13BGNDA

U13BGNDB

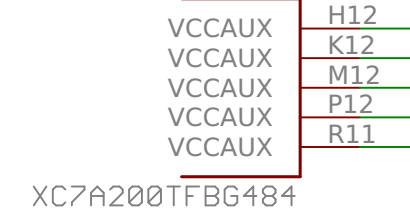
U13BUCCBRAM

U13BUCCAUX



FPGA\_UCCINT\_1V0

FPGA\_UCCAUX\_1V8



B

B

C

C

D

D

1

2

3

4

5

6

1 2 3 4 5 6

A

A

B

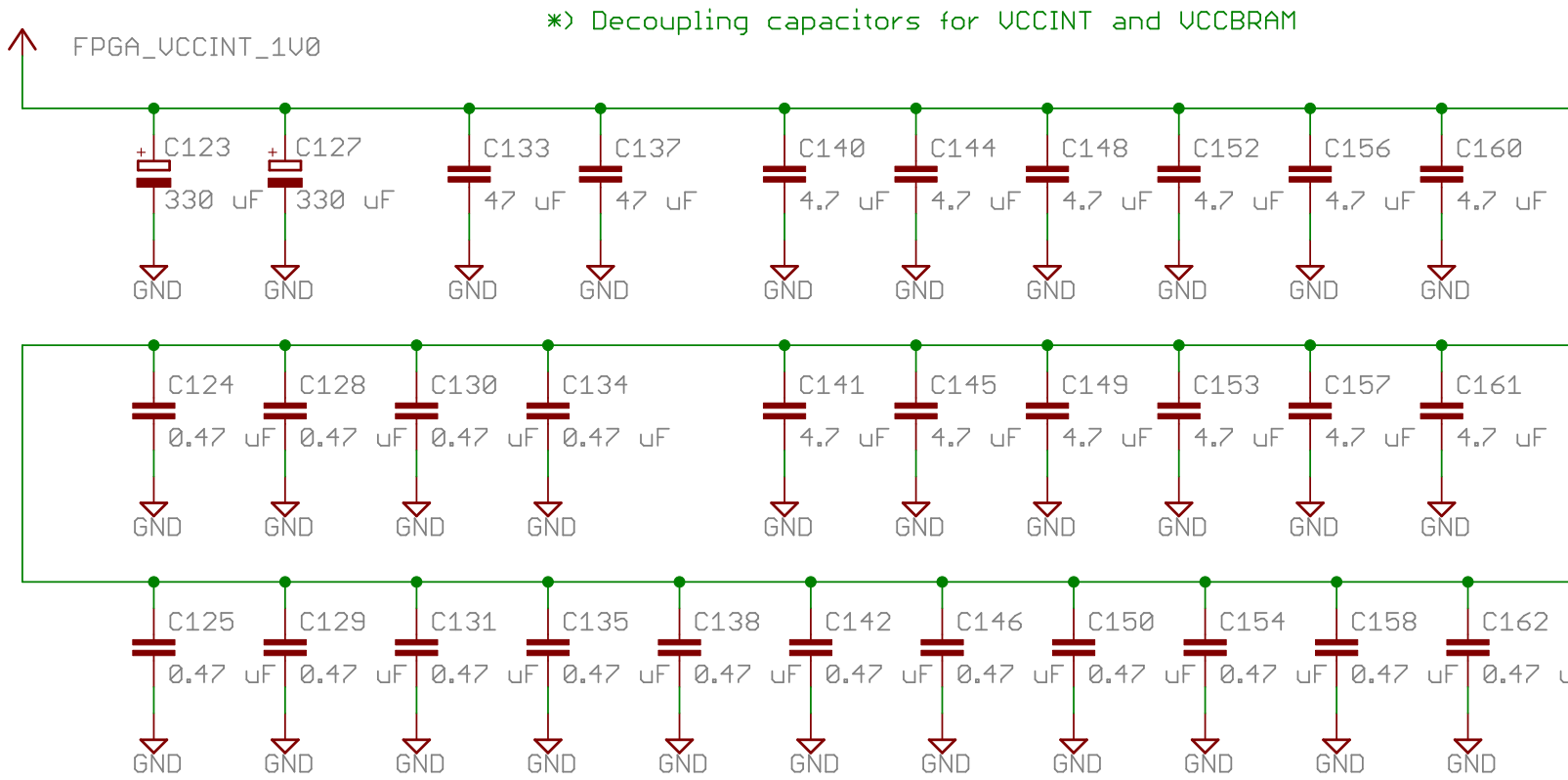
B

C

C

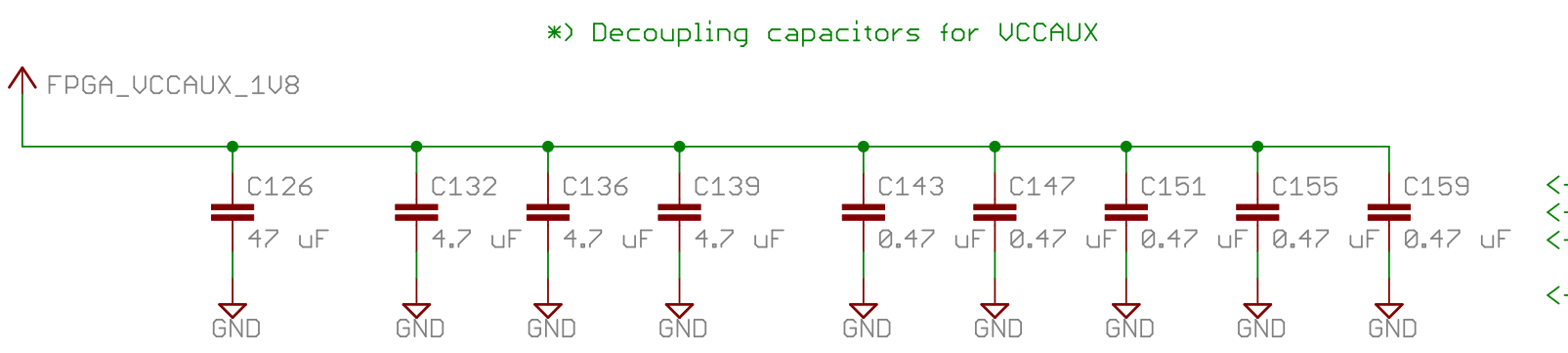
D

D



<-- Place small 0.47 uF caps right under the BGA package  
 <-- Place medium 4.7 uF caps very close to the BGA package  
 <-- Place large 47 uF and 330 uF caps not far from the BGA package

<-- Distribute smaller caps evenly under the BGA package  
 <-- Distribute larger caps evenly around the BGA package



<-- Place small 0.47 uF caps right under the BGA package  
 <-- Place medium 4.7 uF caps very close to the BGA package  
 <-- Place large 47 uF caps not far from the BGA package

<-- Try to place smaller caps next to FPGA balls

rev02
30 Jan 2016 18:17:49
Sheet: 23/26

1 2 3 4 5 6

1 2 3 4 5 6

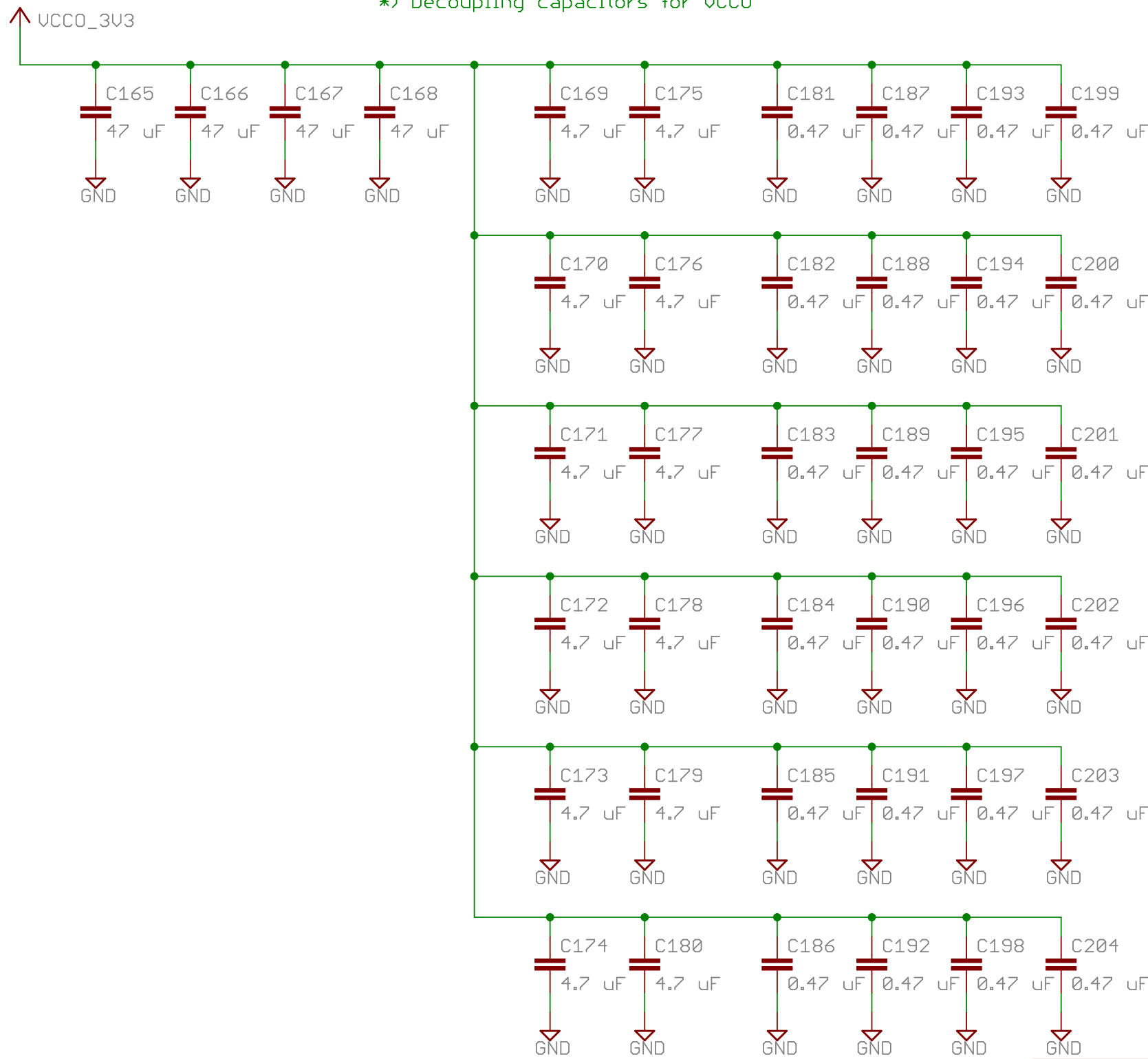
A

B

C

D

\*> Decoupling capacitors for VCC0



- <-- Place small 0.47 uF caps right under the BGA package
- <-- Place medium 4.7 uF caps very close to the BGA package
- <-- Place large 47 uF caps not far from the BGA package
- <-- Place one of four 47 uF caps on every side of the BGA package
- <-- Distribute six sets of caps among six FPGA I/O banks

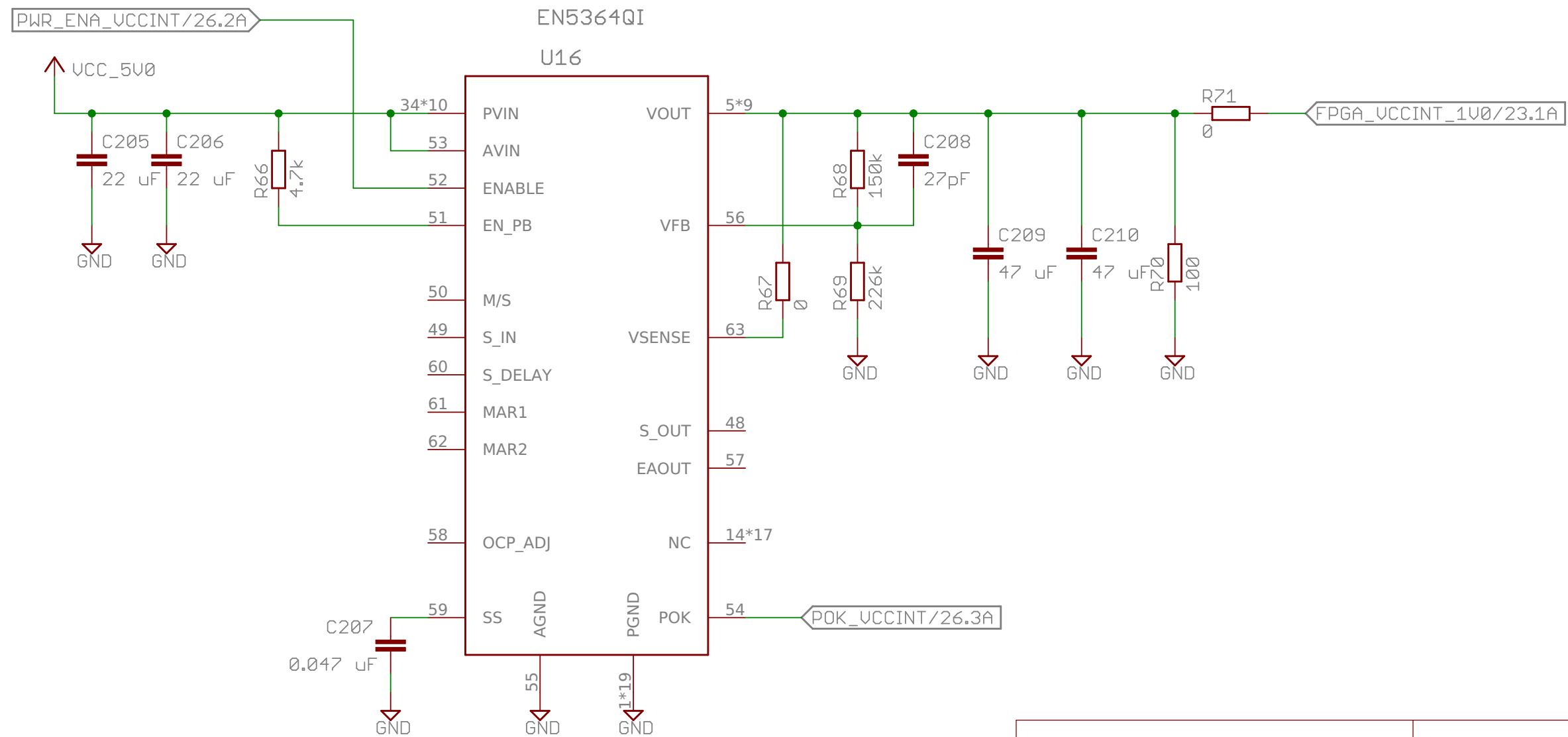
rev02
30 Jan 2016 18:17:49
Sheet: 24/26

1 2 3 4 5 6



\*) FPGA Power Subsystem -- CORE

- \*)  $UCCINT = 0.6V \times (1 + 150 / 226) = 0.998V$
- \*) OCP\_ADJ is not used (default over-current threshold)
- \*) MARx are not used (output at nominal 100%)
- \*) S\_IN/S\_OUT are not used (single regulator mode)
- \*) S\_DELAY is not used (single regulator mode)
- \*) M/S is not used (parallel operation not needed)
- \*) EA\_OUT is not used (default control loop)
- \*) Minimal load current is 0A, but we still place load of 100 Ohms just in case (gives 10 mA)



rev02
30 Jan 2016 18:17:49
Sheet: 25/26

1

2

3

4

5

6

A

A

B

B

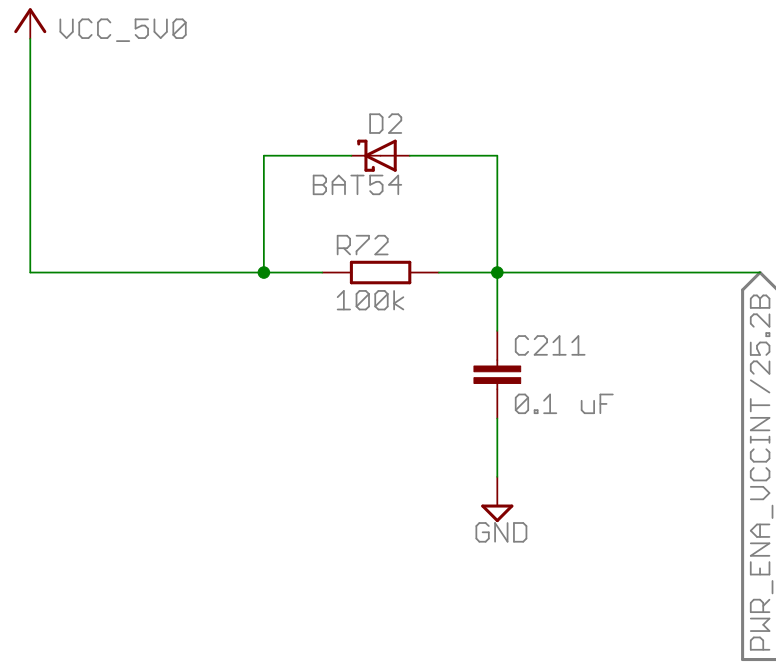
C

C

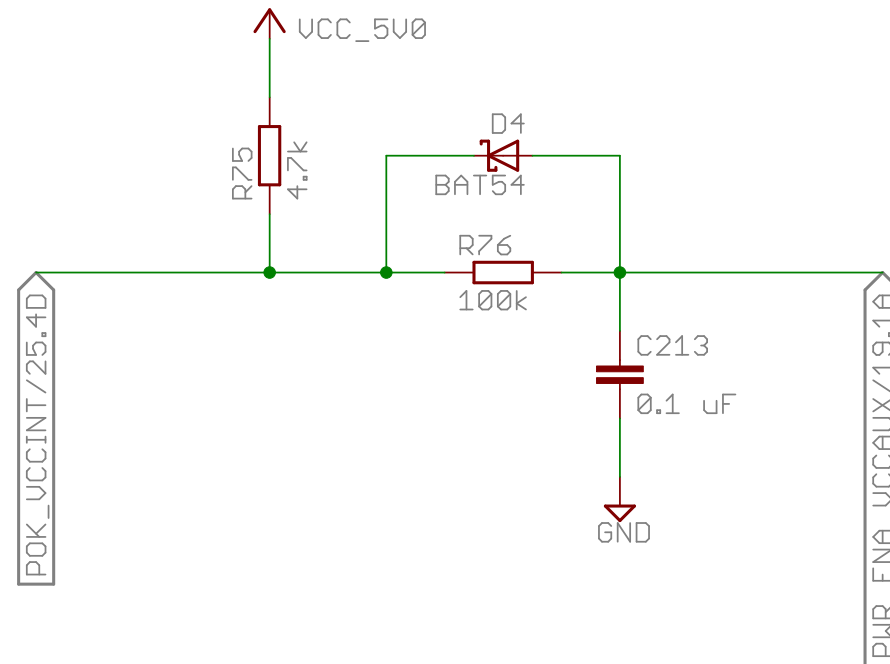
D

D

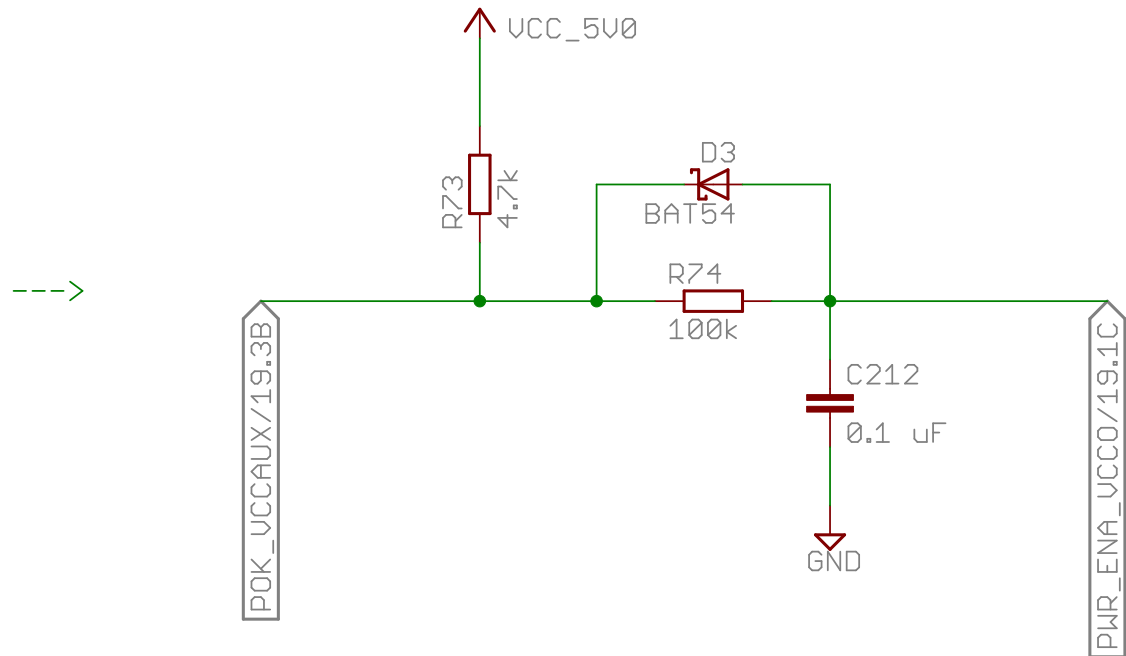
\*) Recommended power-up sequence:  
 1) VCCINT  
 2) VCCAUX  
 3) VCC0  
 RC network values are preliminary,  
 should be tweaked after experiments



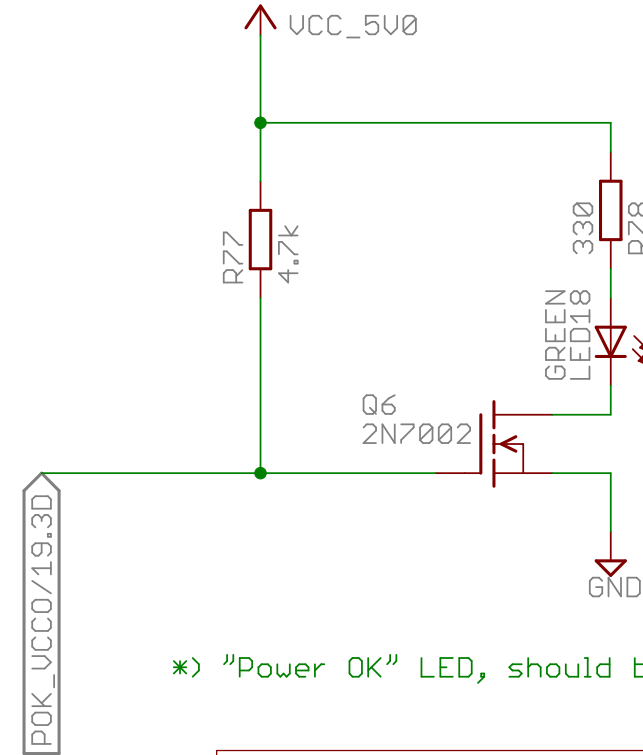
--->



--->



--->



\*) "Power OK" LED, should be of green color

rev02
30 Jan 2016 18:17:49
Sheet: 26/26

1

2

3

4

5

6