

Extra

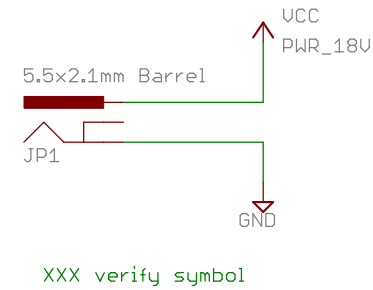


open hardware



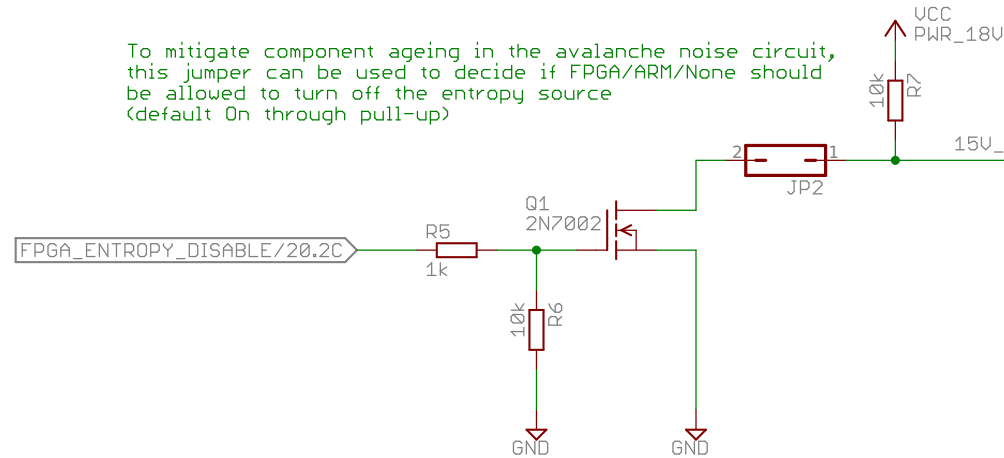
This page intentionally left blank

Main power input
18V DC

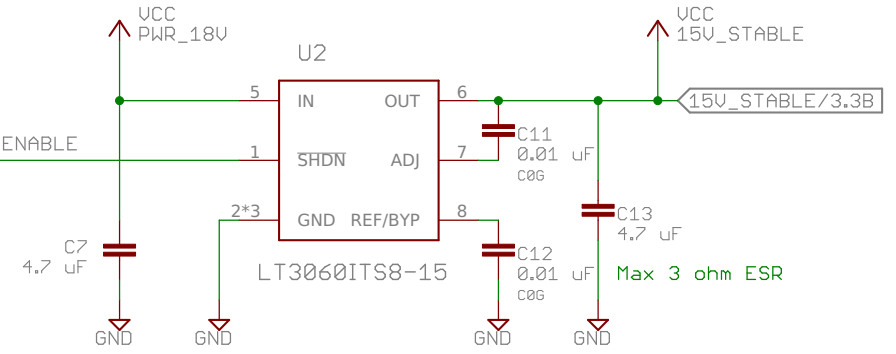


Entropy source power

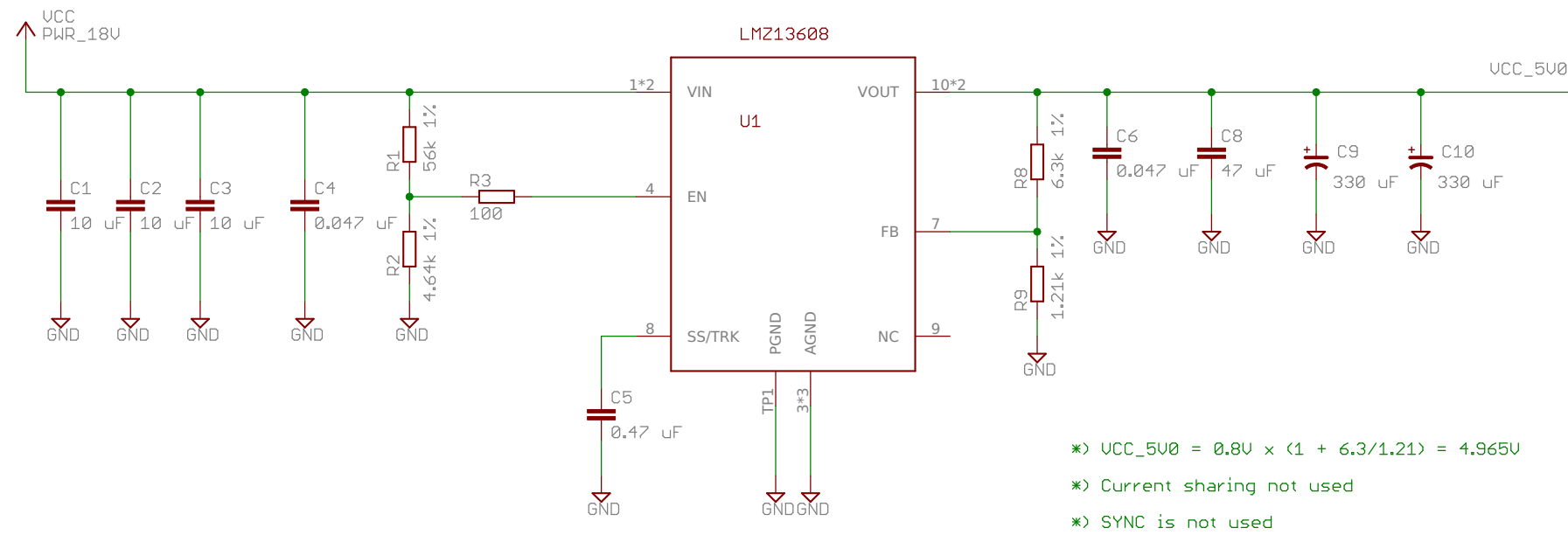
To mitigate component ageing in the avalanche noise circuit, this jumper can be used to decide if FPGA/ARM/None should be allowed to turn off the entropy source (default On through pull-up)



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

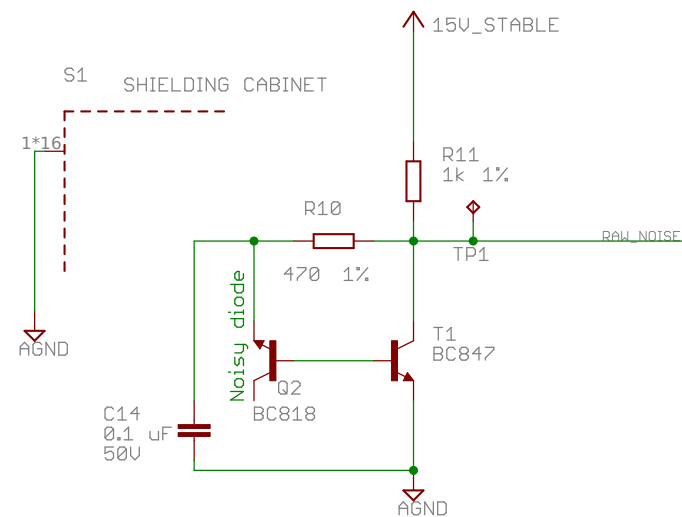


*) Intermediate Regulator: 18V -> 5V



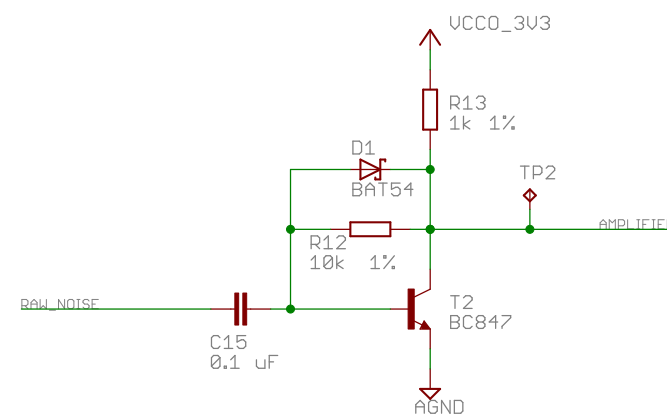
Input power
rev02
10 Feb 2016 15:31:03
Sheet: 2/26

Noise generator

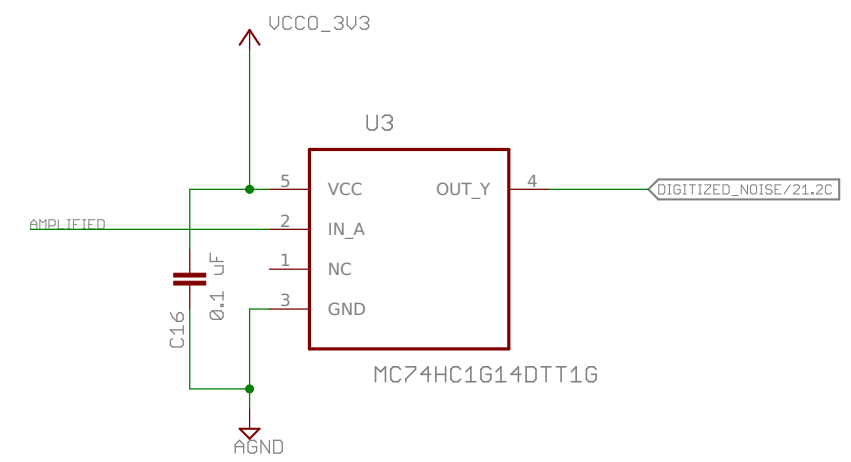


AGND is connected to GND on the board using polygons (found no other good way) - not visible in schematics.

Amplifier



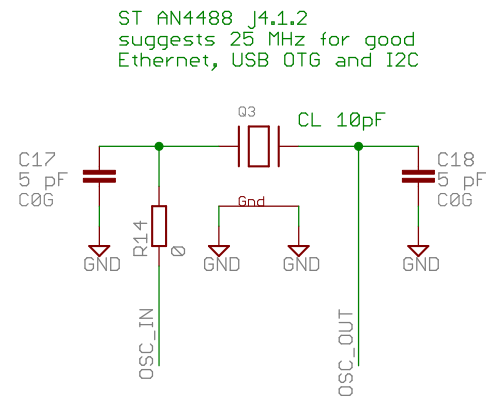
Digitizer



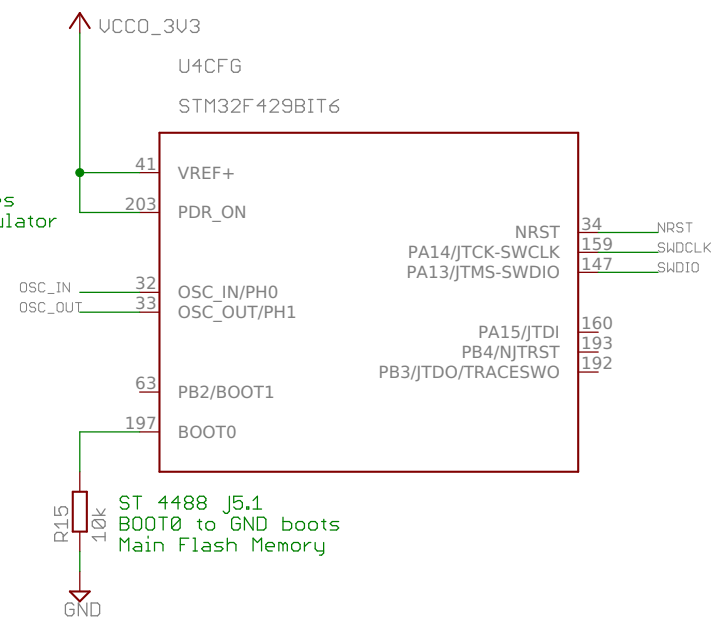
This whole sheets circuitry should be as shielded as possible. Solid isolated ground plane and internal planes connected to the rest of the board at a single point is expected.

Noise source
rev02
10 Feb 2016 15:31:03
Sheet: 3/26

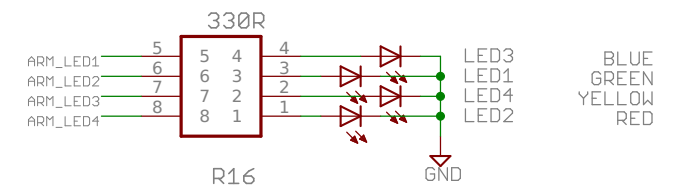
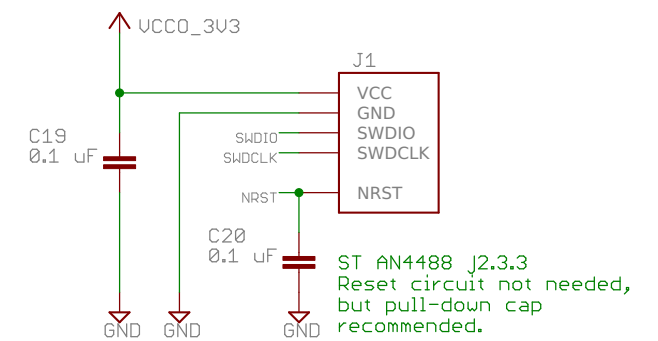
Basic configuration, STM32



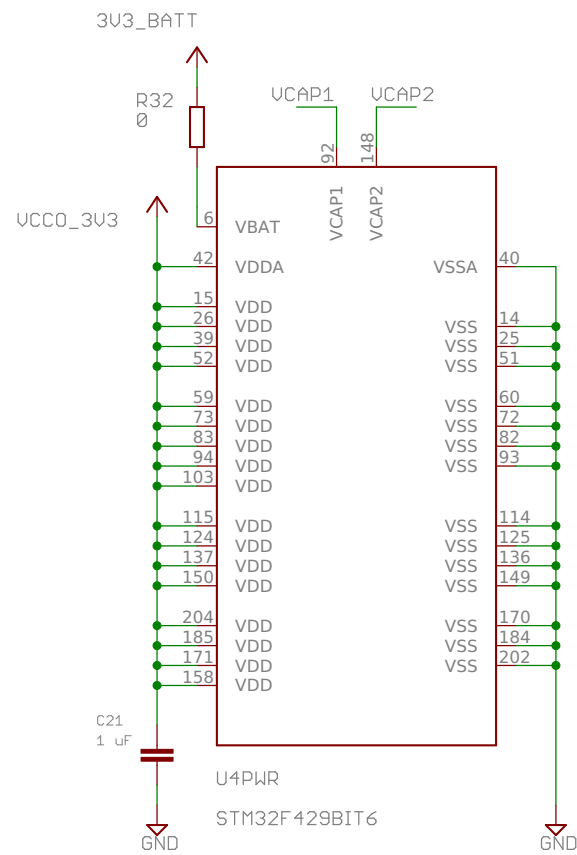
PDR_ON high enables internal power regulator



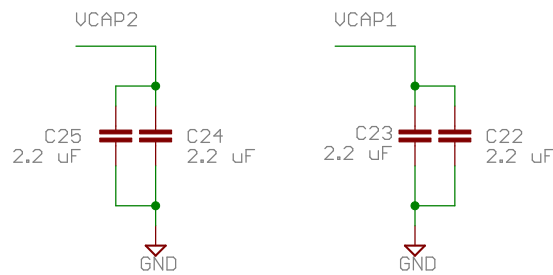
SWD program/debug



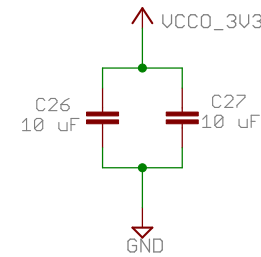
Power and bypass capacitors, STM32



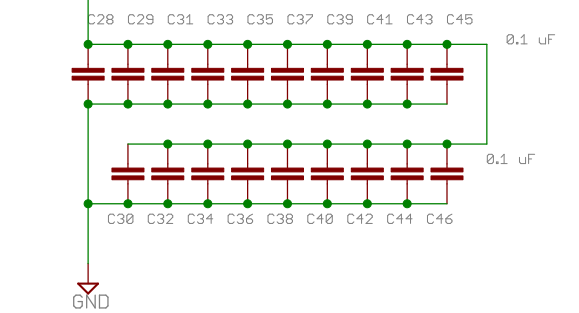
2*2*2.2uF LowESR or
2*1*4.7uF LowESR
< 1 ohm
(ST AN4488 J2.2)



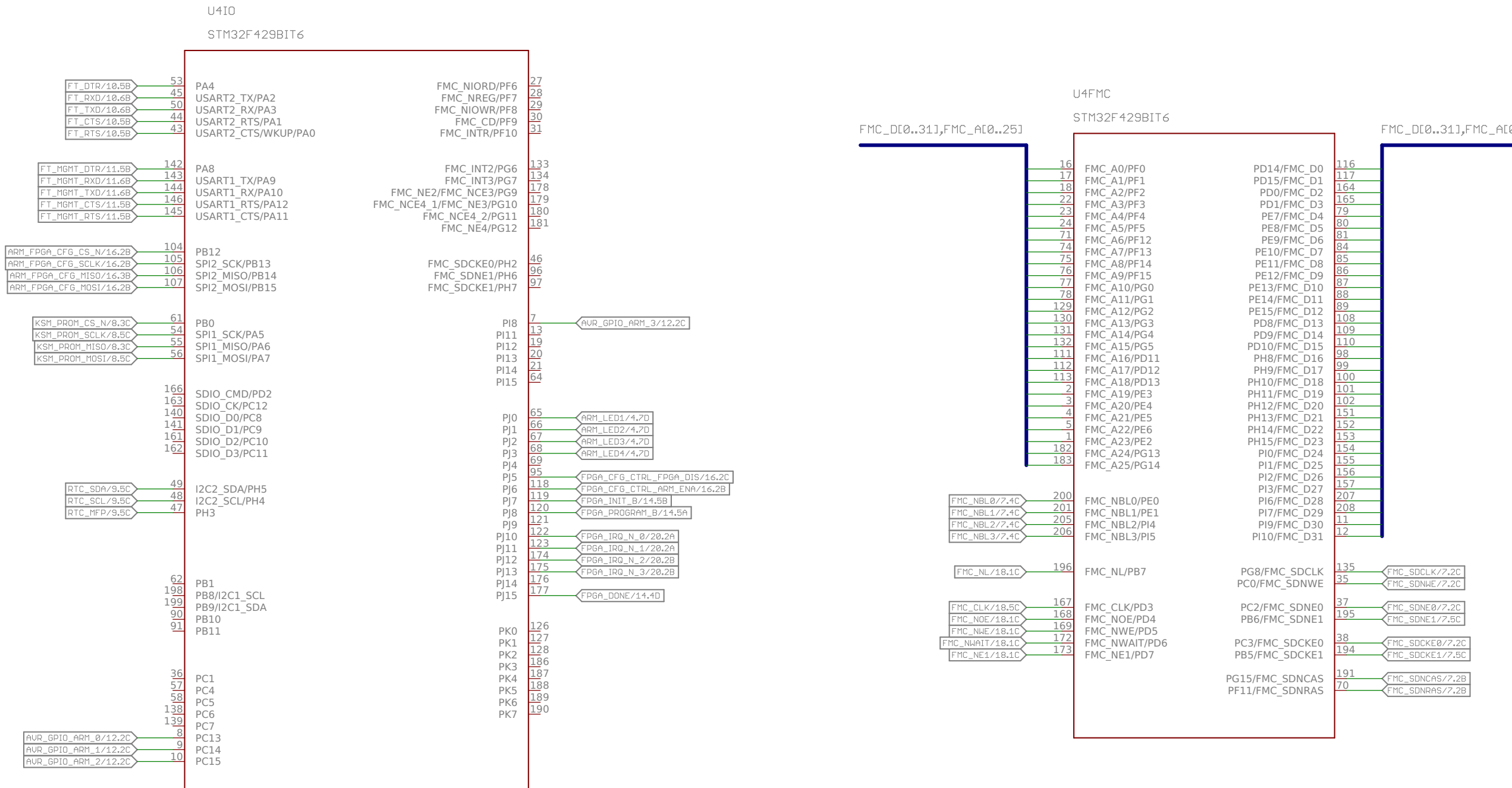
ST AN8844 J2.2
One 10uF bypass cap for the package.
(two used for extra comfort)



ST AN8844 J2.2
One bypass capacitor for every VDD.
Use 0.1 uF X7R 10V.



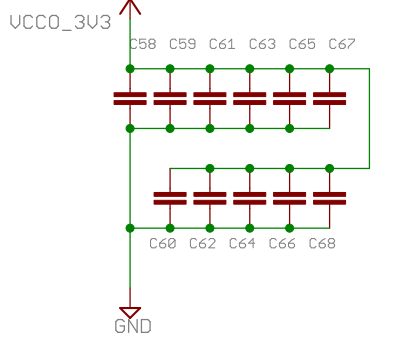
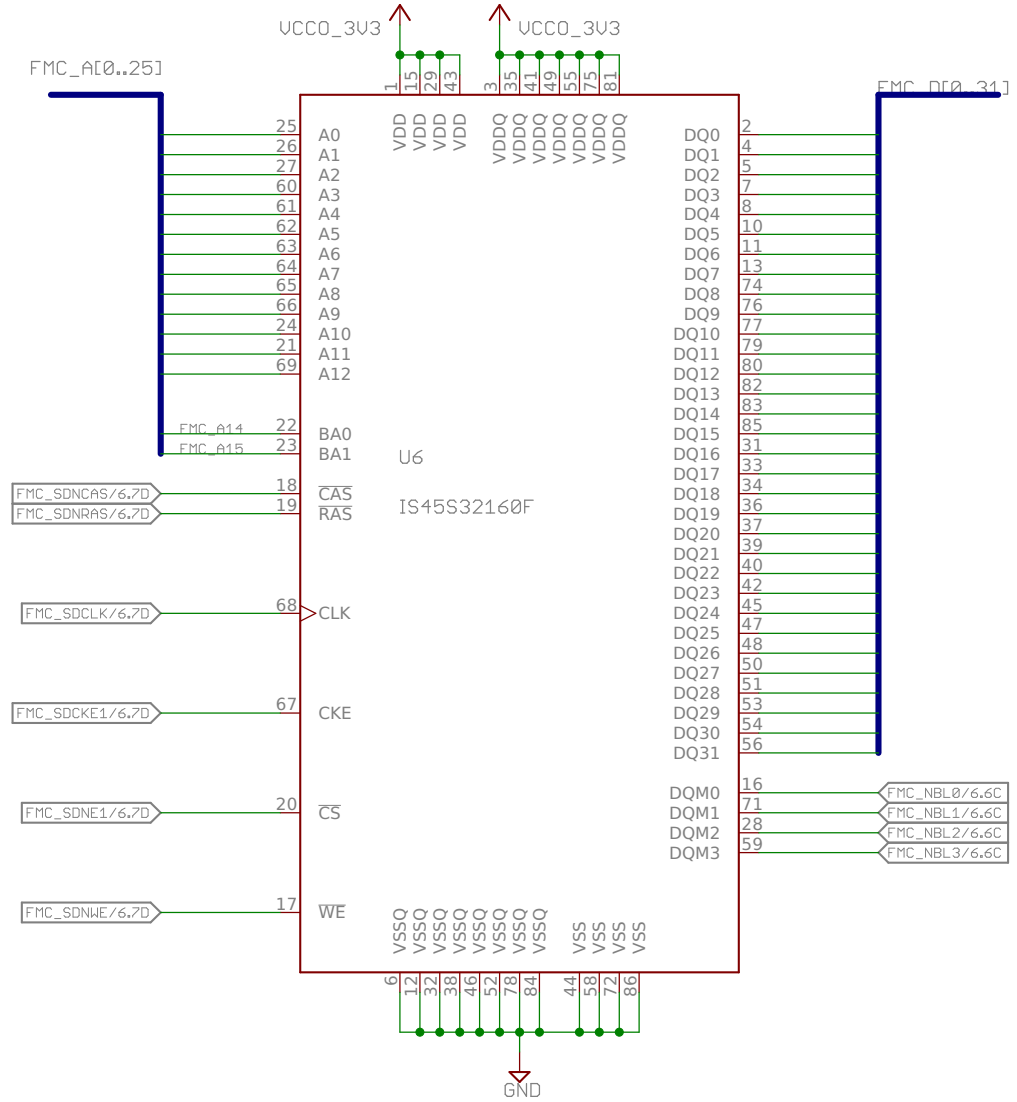
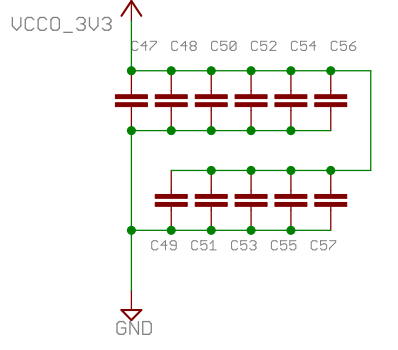
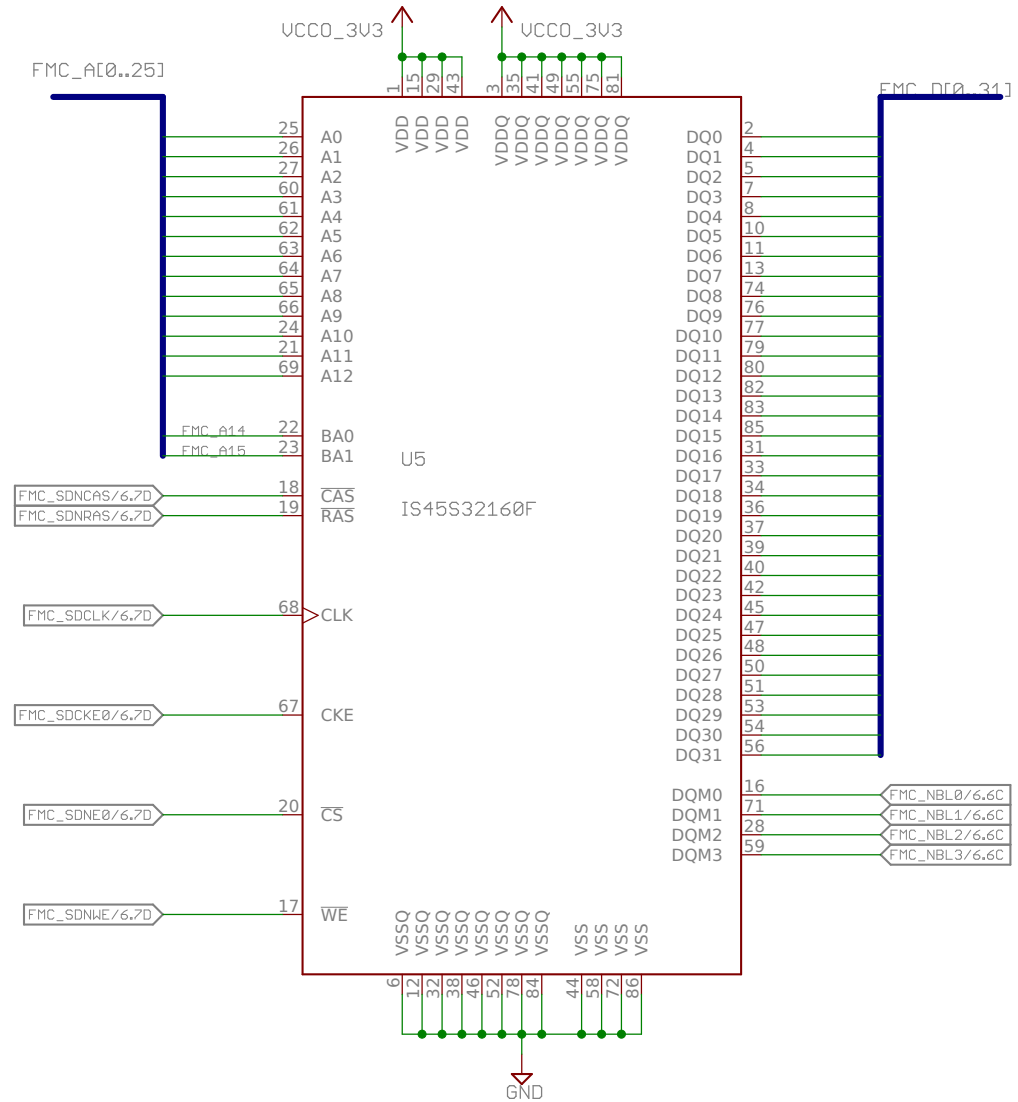
Input/output, STM32



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

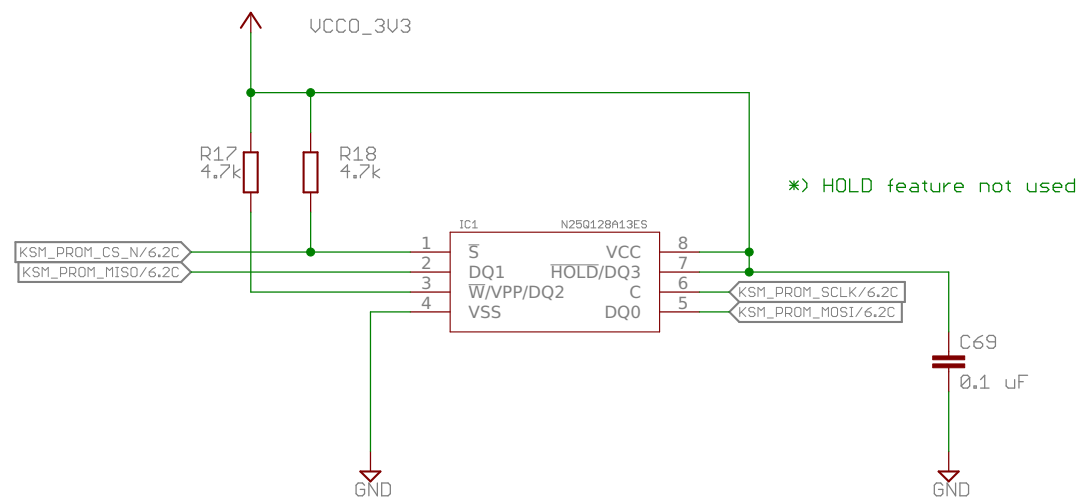
2x512 Mbit SDRAM memory for the ARM

These packages are TSSOP, but if new packages are to be created for layout, BGA package is preferred.

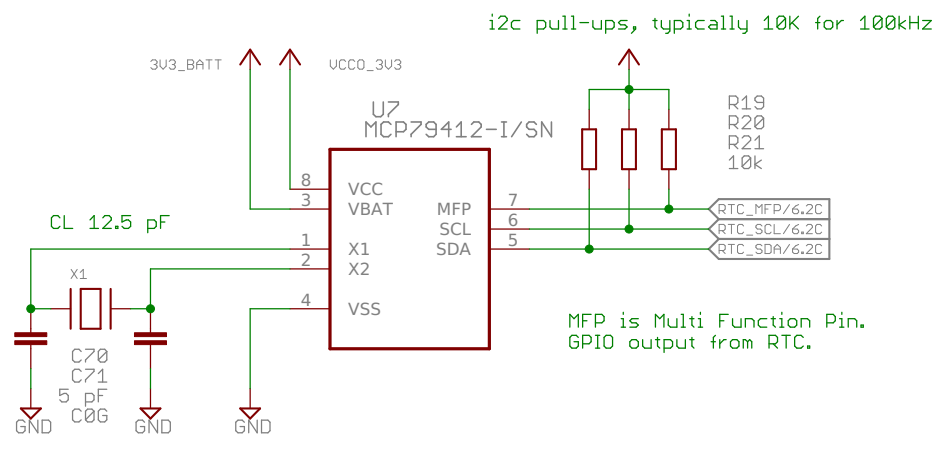


Keystore memory, 128 Mbit

This memory holds cryptographic keys wrapped with the master key.

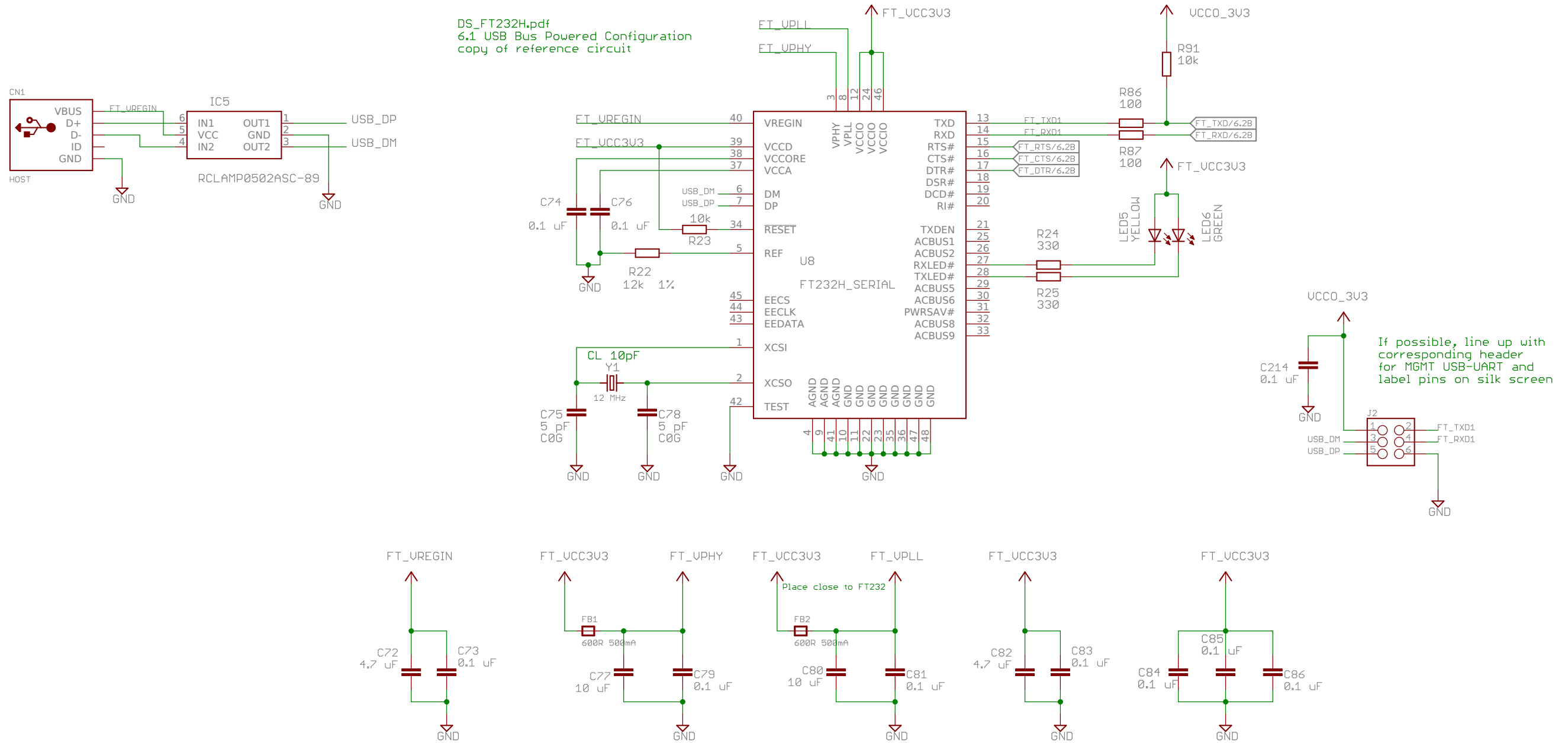


Real Time Clock



Application access USB UART

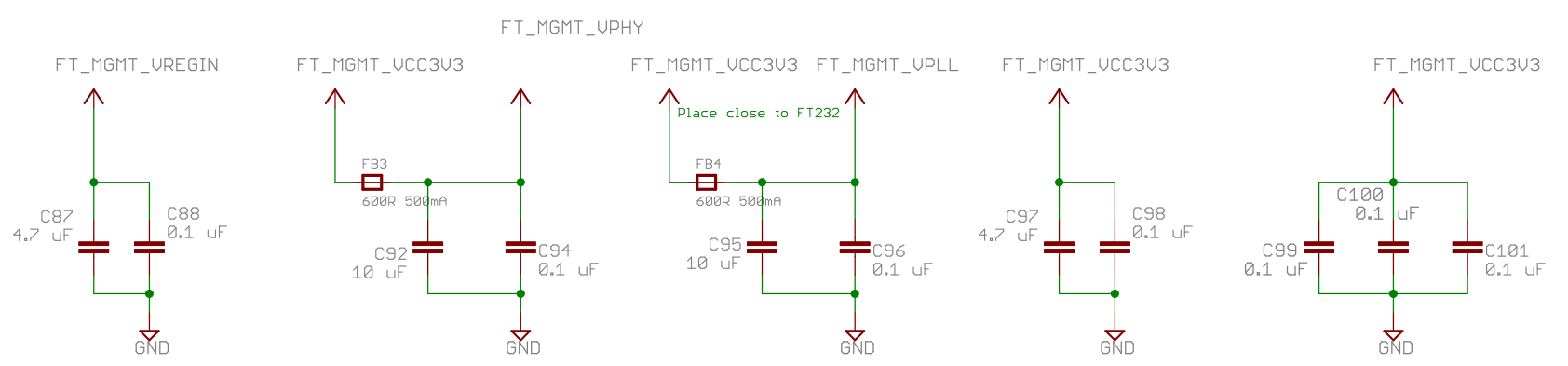
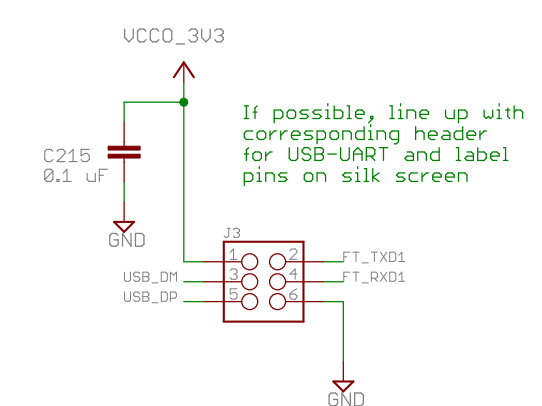
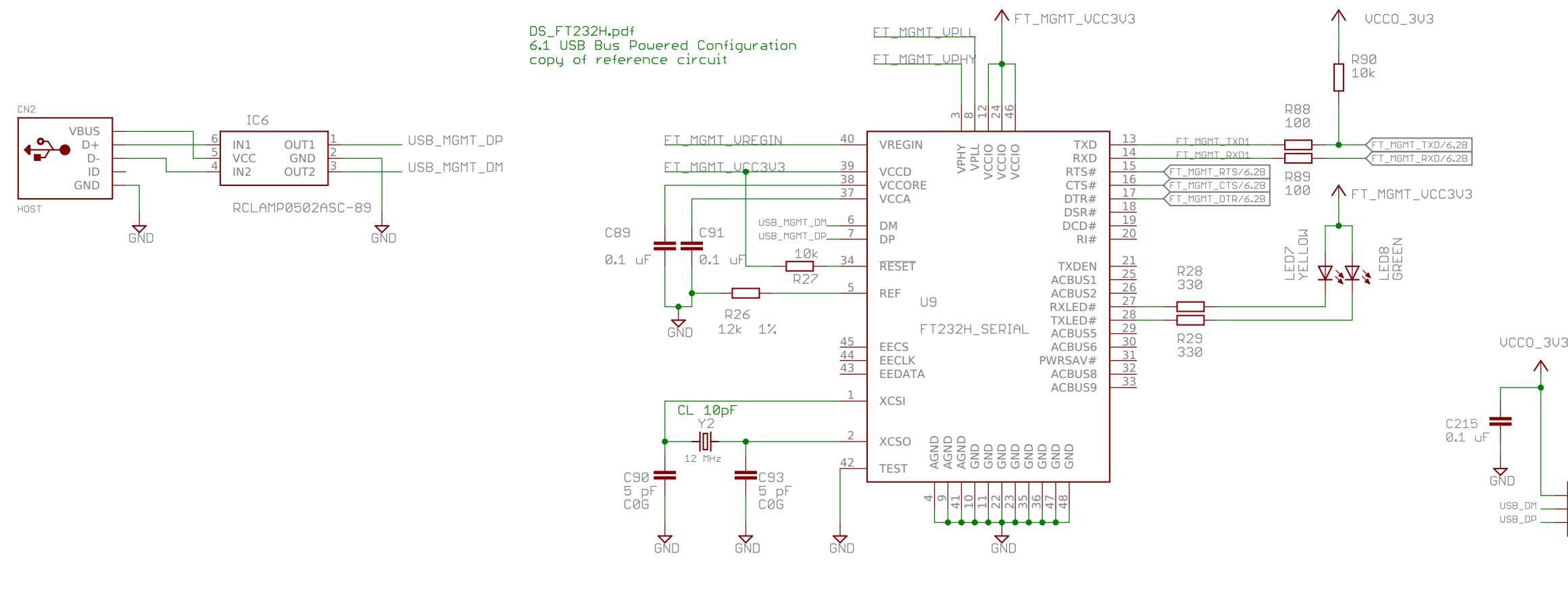
DS_FT232H.pdf
6.1 USB Bus Powered Configuration
copy of reference circuit



If possible, line up with corresponding header for MGMT USB-UART and label pins on silk screen

Management access USB UART

DS_FT232H.pdf
6.1 USB Bus Powered Configuration
copy of reference circuit



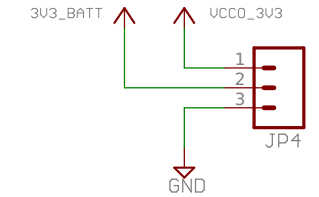
MGMT USB-UART	
rev02	
10 Feb 2016 15:31:03	
Sheet: 11/26	

AVR Tiny Tamper Detect MCU

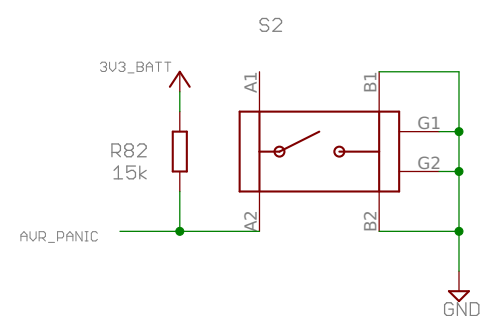


AVR_GPIO* AVR_LED* and AVR_PANIC can be swapped.

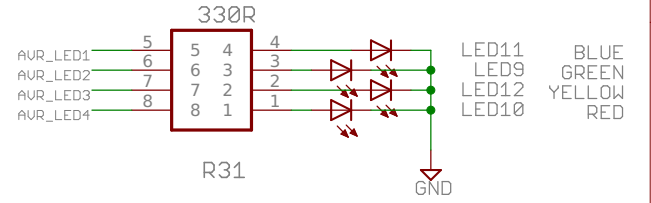
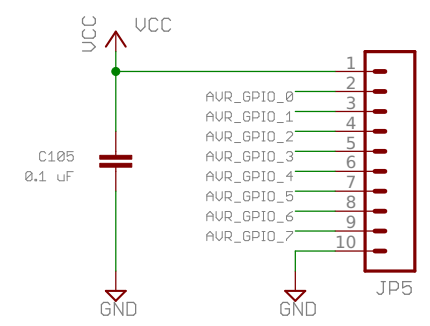
Connector for external 3V3 battery.
Place a jumper between pins 1-2 to "emulate" having a battery present.



Panic button



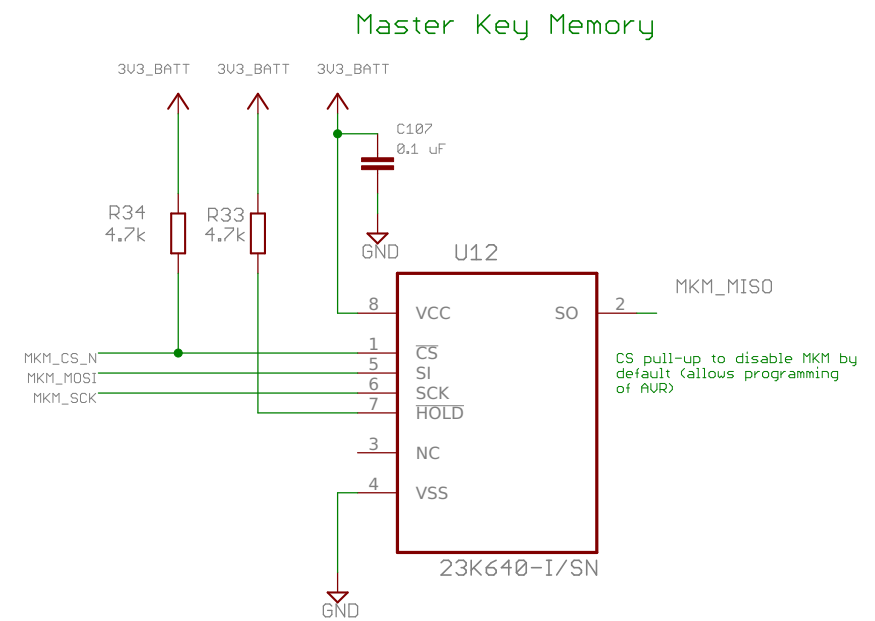
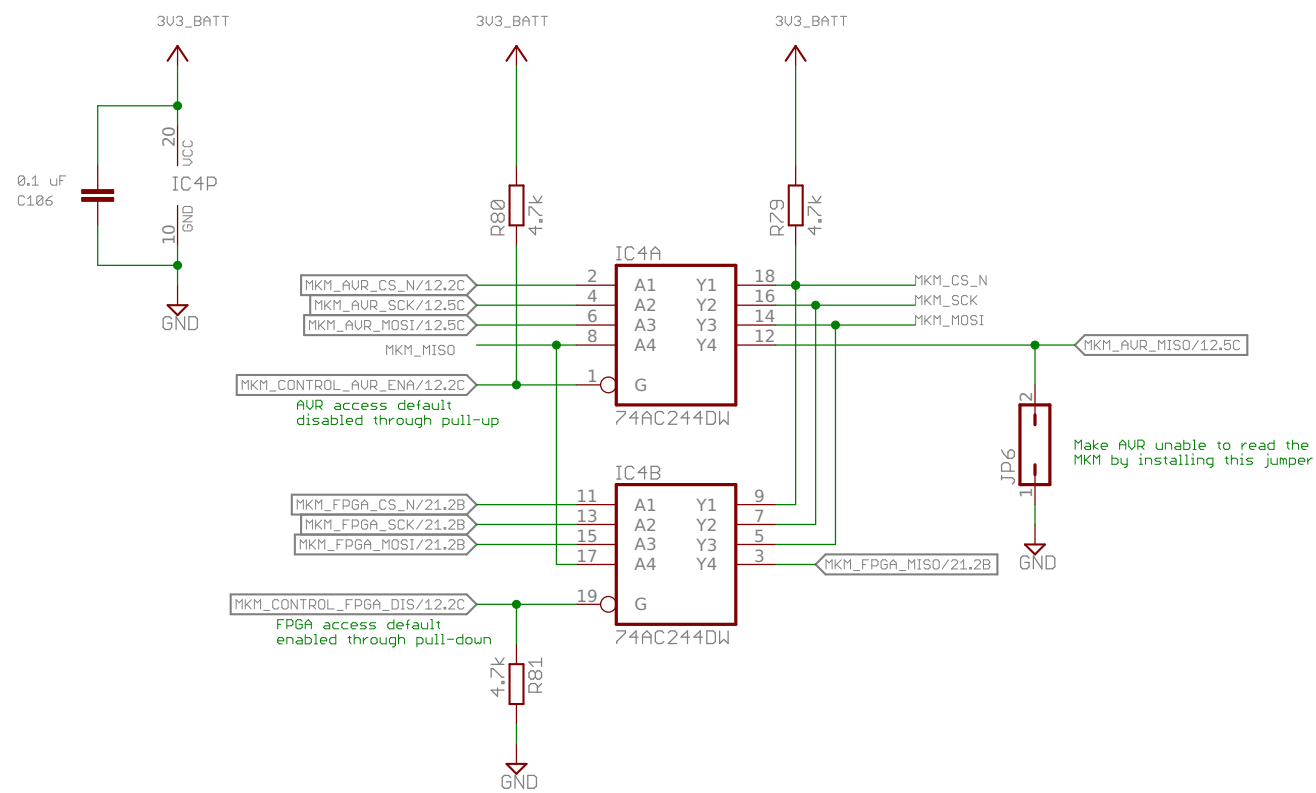
Expansion GPIO

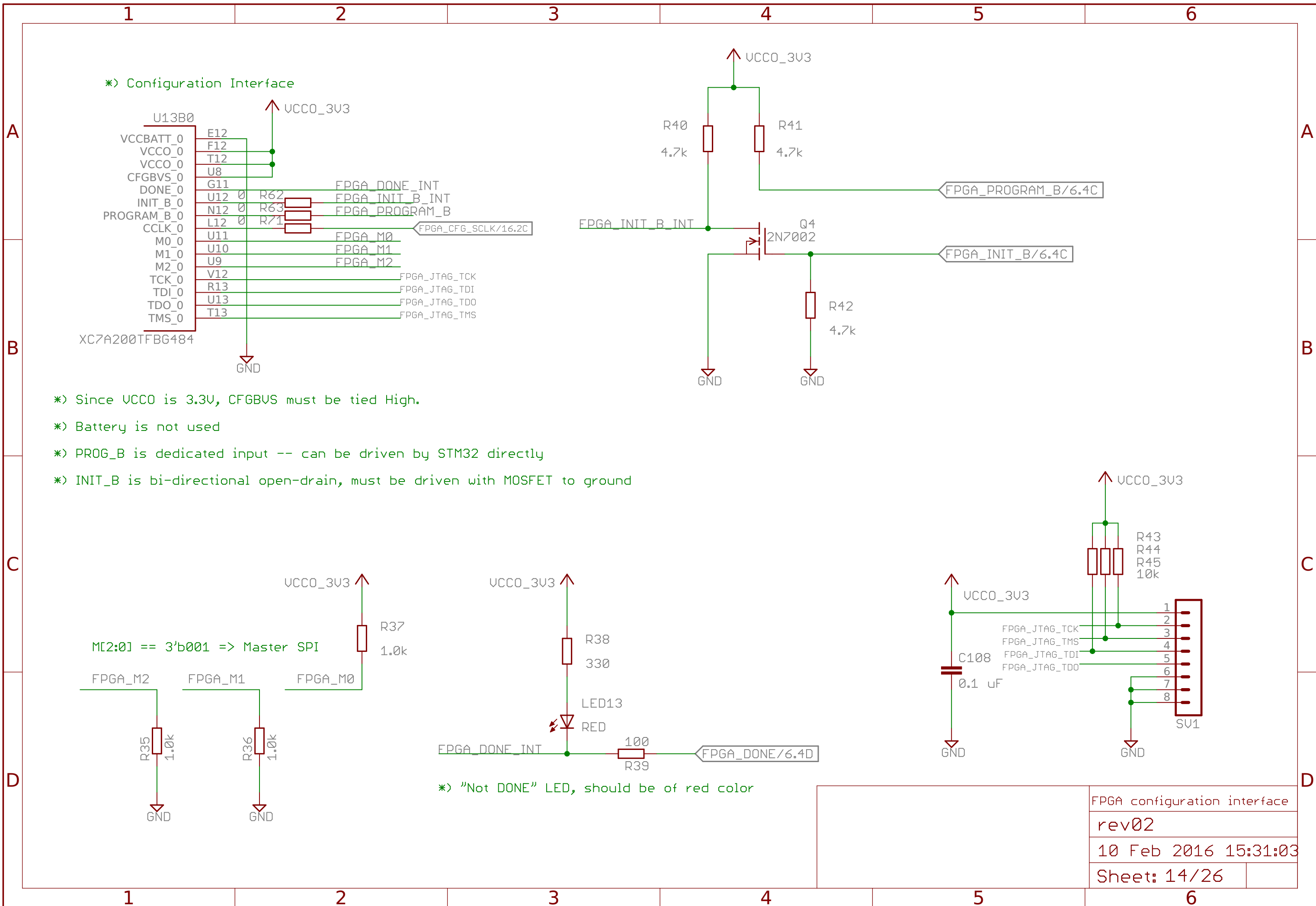


AVR Tamper circuit	
rev02	
10 Feb 2016 15:31:03	
Sheet: 12/26	

SPI mux controlling access to the MKM.

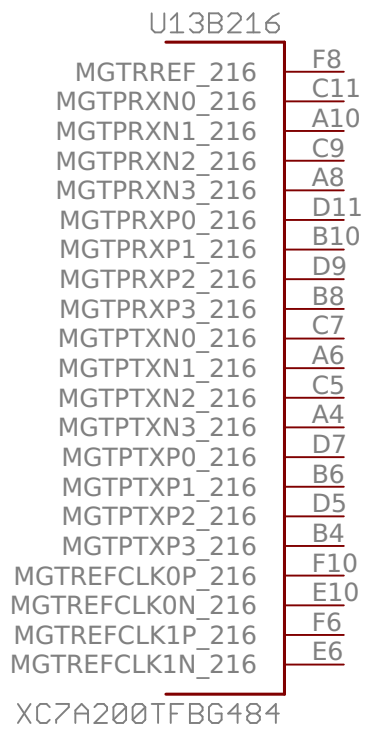
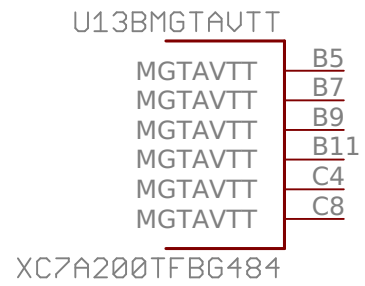
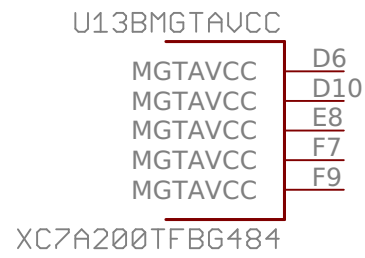
Normally, the FPGA has R/W access to the MKM but on a tamper event the tamper detect MCU (AVR) will grab access to the MKM and erase the contents.



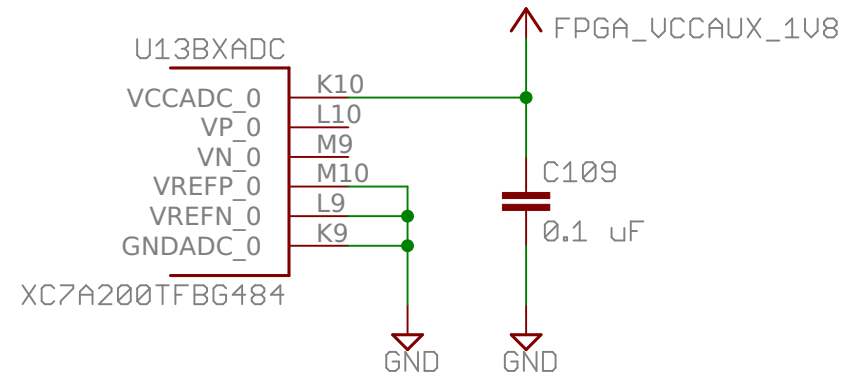


FPGA configuration interface	
rev02	
10 Feb 2016 15:31:03	
Sheet: 14/26	

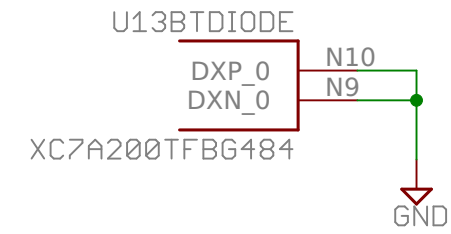
*> Transceivers [NOT USED]



*> XADC [NOT USED]



*> Temperature Sensor [NOT USED]



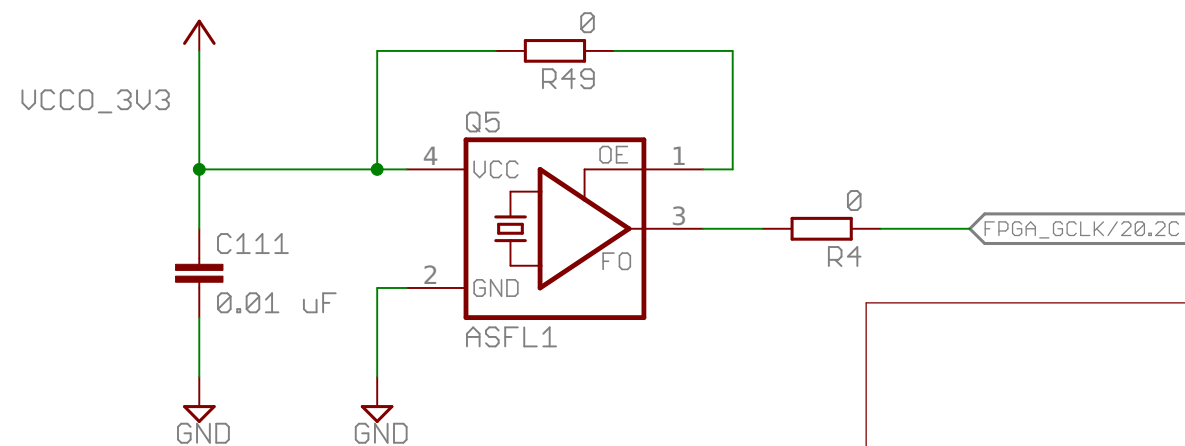
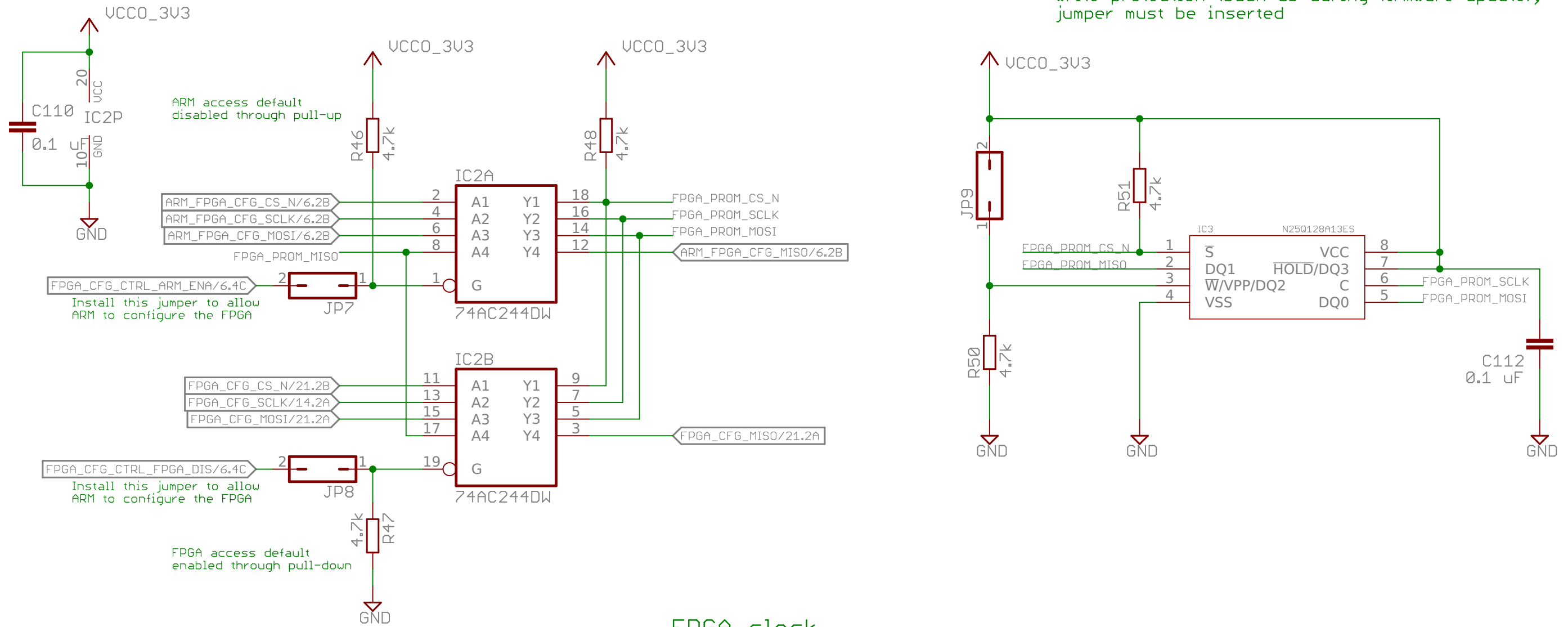
FPGA unused
 rev02
 10 Feb 2016 15:31:03
 Sheet: 15/26

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 supporting components	
rev02	
10 Feb 2016 15:31:03	
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

FPGA unused banks

rev02

10 Feb 2016 15:31:03

Sheet: 17/26

1

2

3

4

5

6

A

B

C

D

A

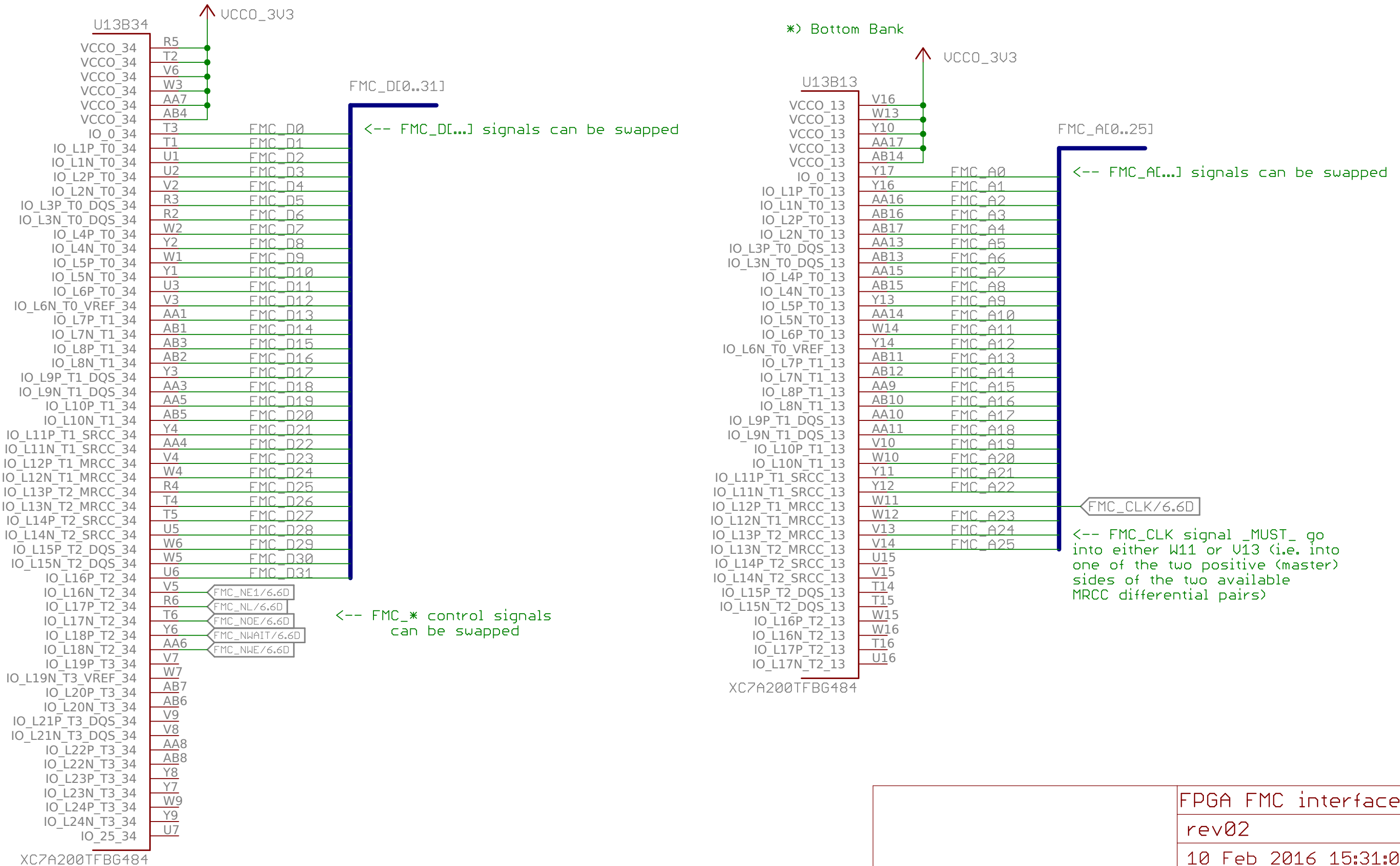
B

C

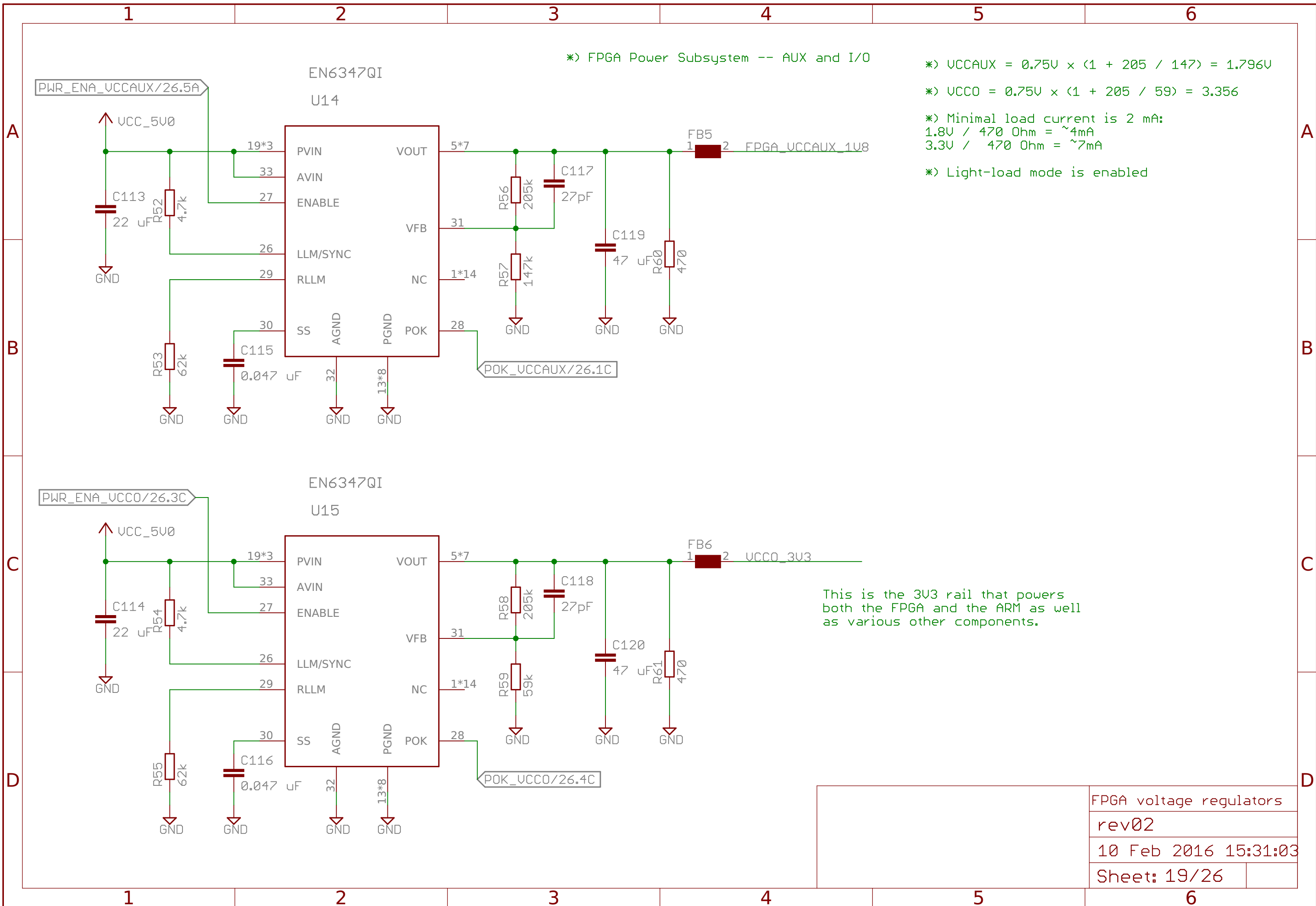
D

* Lower Left Bank

* Bottom Bank

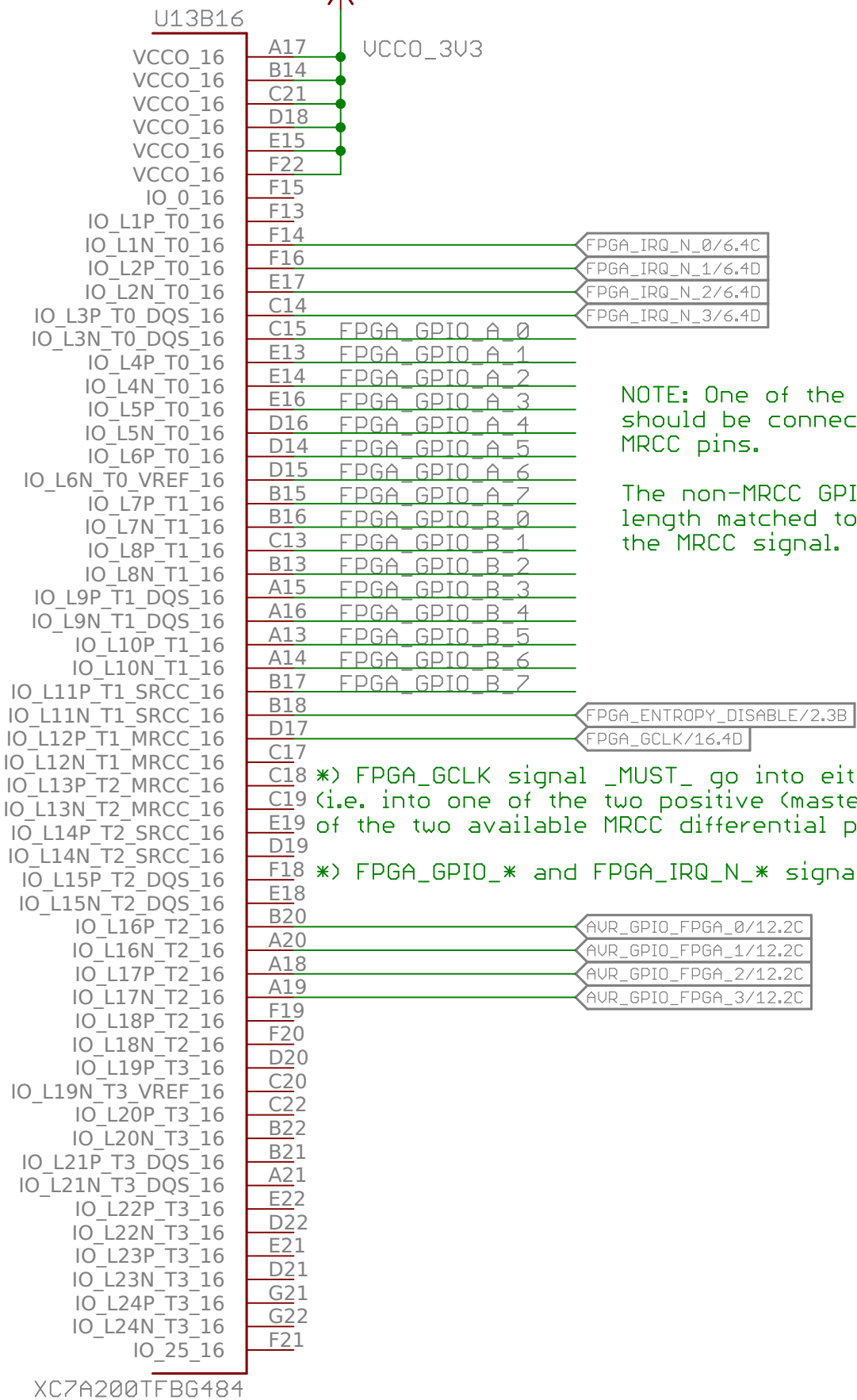


FPGA FMC interface	
rev02	
10 Feb 2016 15:31:03	
Sheet: 18/26	



FPGA voltage regulators	
rev02	
10 Feb 2016 15:31:03	
Sheet: 19/26	

* Upper Right Bank



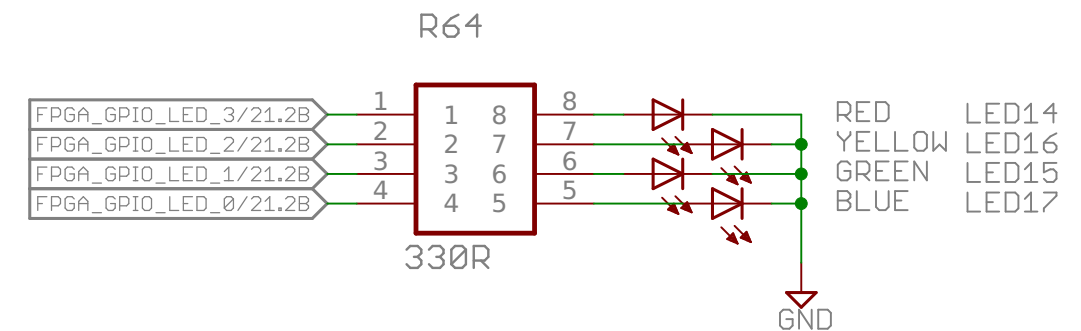
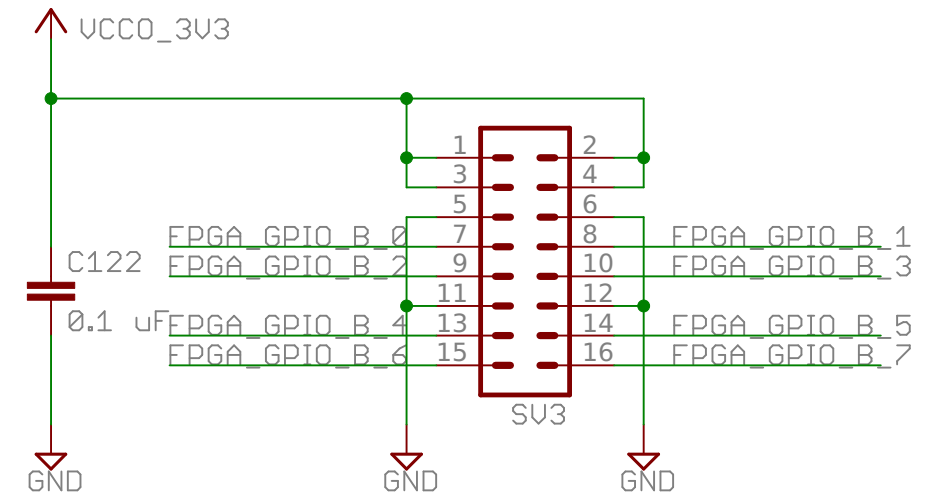
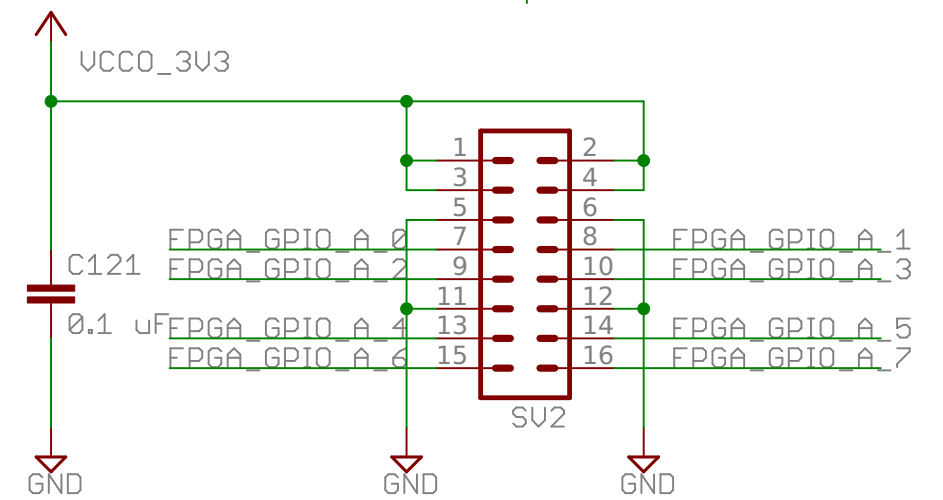
NOTE: One of the FPGA_GPIO_* pins should be connected to one of the MRCC pins.

The non-MRCC GPIO signals should be length matched to within 500 ps of the MRCC signal.

* FPGA_GCLK signal MUST go into either D17 or C18 (i.e. into one of the two positive (master) sides of the two available MRCC differential pairs)

* FPGA_GPIO_* and FPGA_IRQ_N_* signals can be swapped

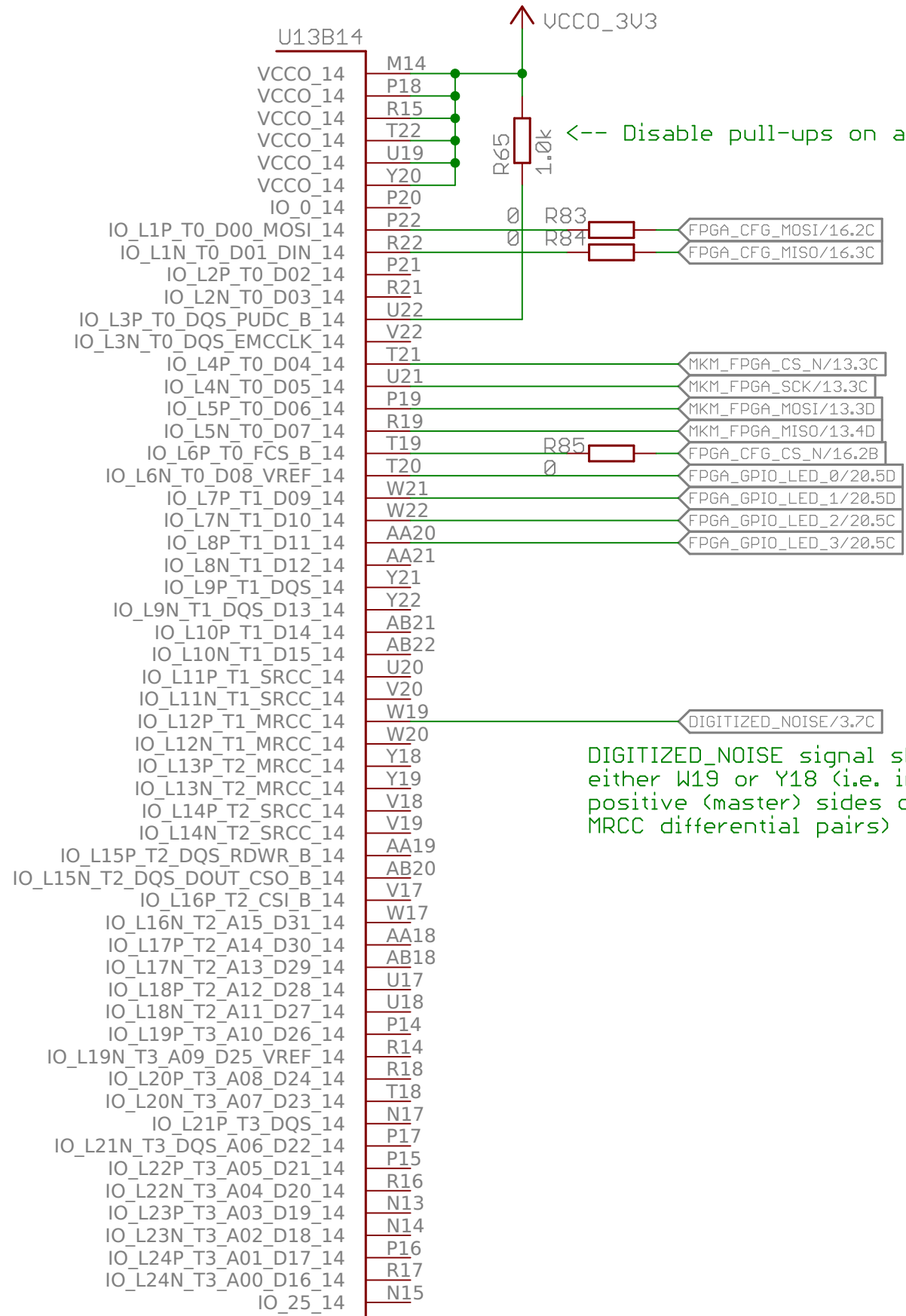
* Signals, that are allowed to be swapped, can be swapped with each other and/or moved to different pins within their bank.



FPGA GPIO	
rev02	
10 Feb 2016 15:31:03	
Sheet: 20/26	

*) 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.



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)

<-- FPGA_GPIO_* and FPGA_IRQ_N_* signals can be swapped

<-- Disable pull-ups on all pins during configuration

1

2

3

4

5

6

A

A

*) Ground Pins

*) Power - CORE & BRAM

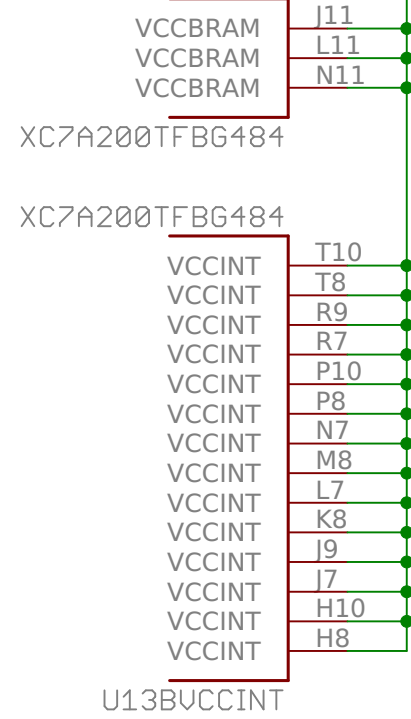
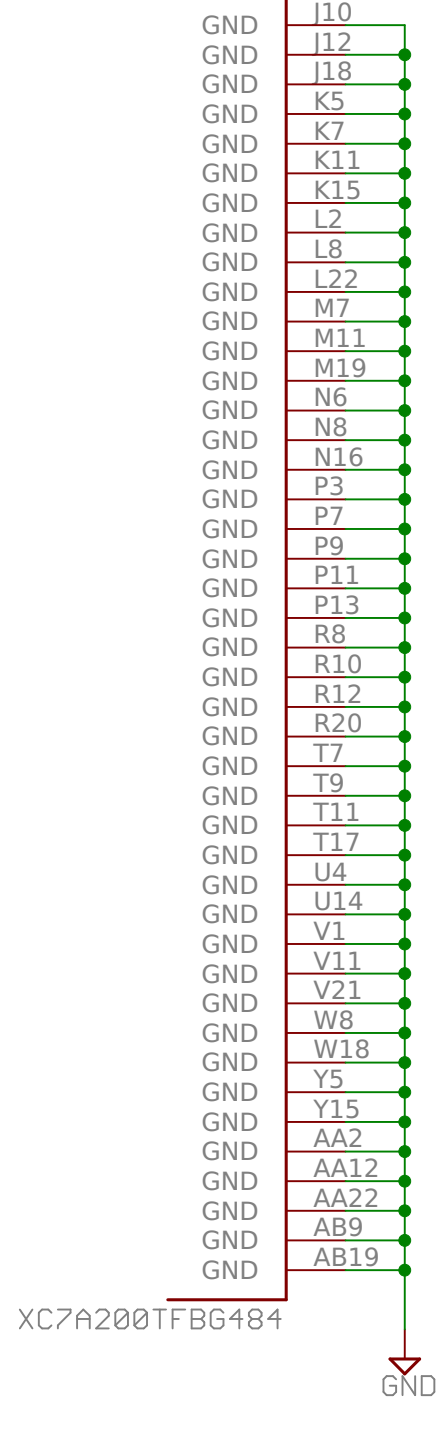
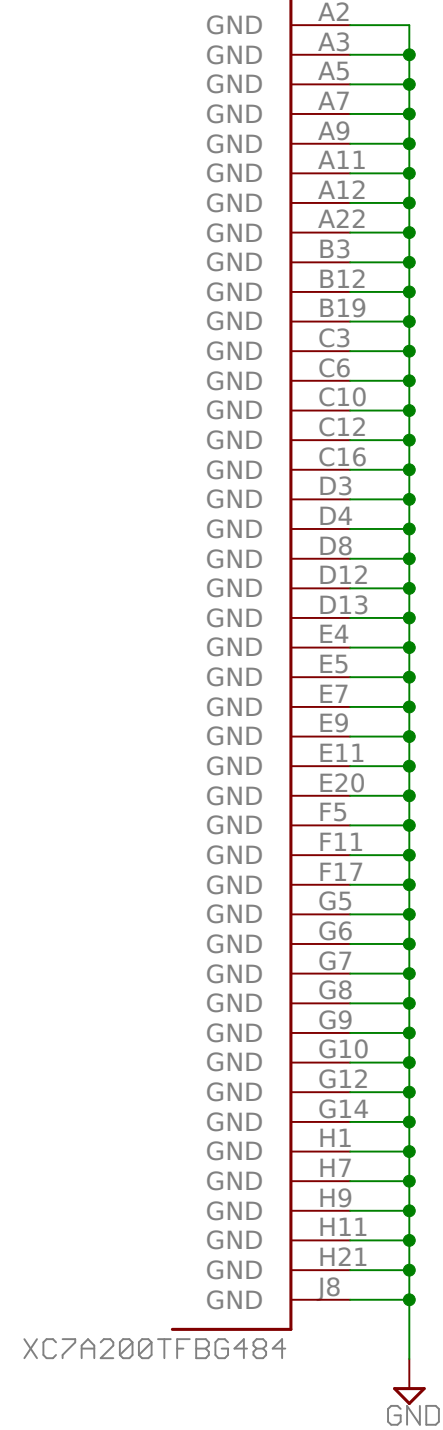
*) Power - AUX

U13BGNDA

U13BGNDB

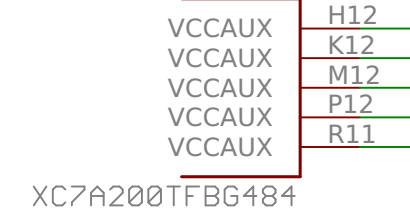
U13BUCCBRAM

U13BUCCAUX



FPGA_UCCINT_1V0

FPGA_UCCAUX_1V8



B

B

C

C

D

D

1

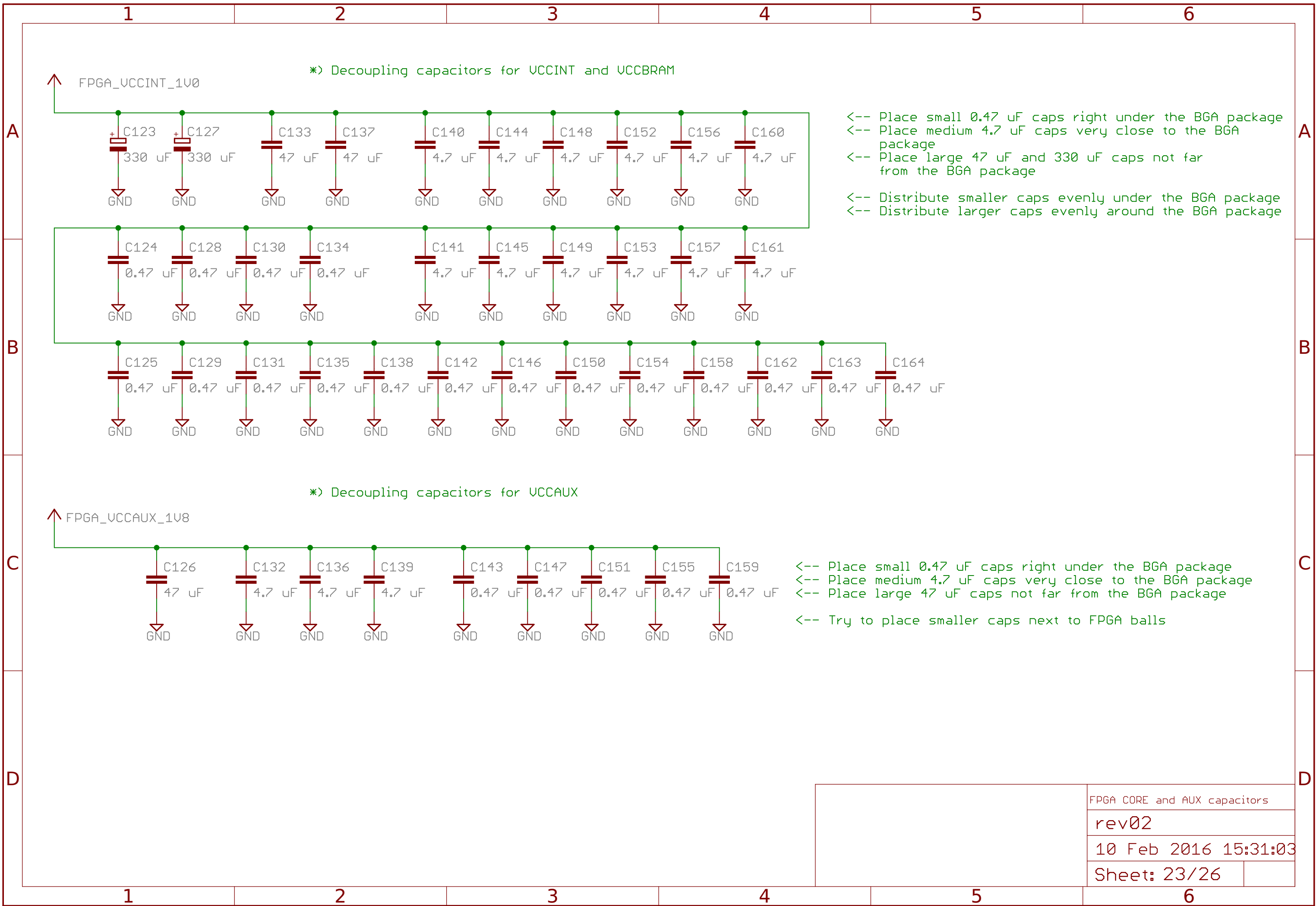
2

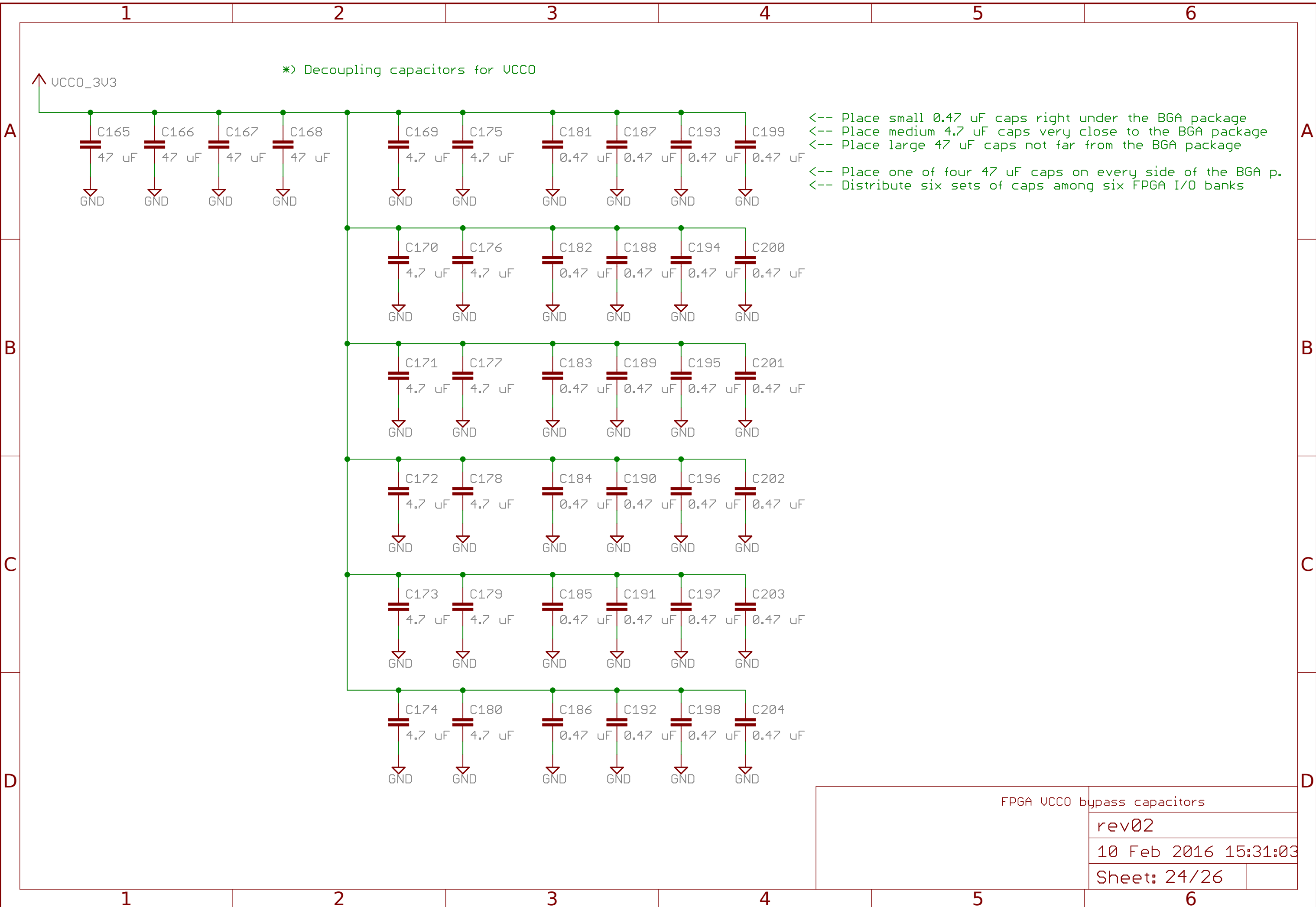
3

4

5

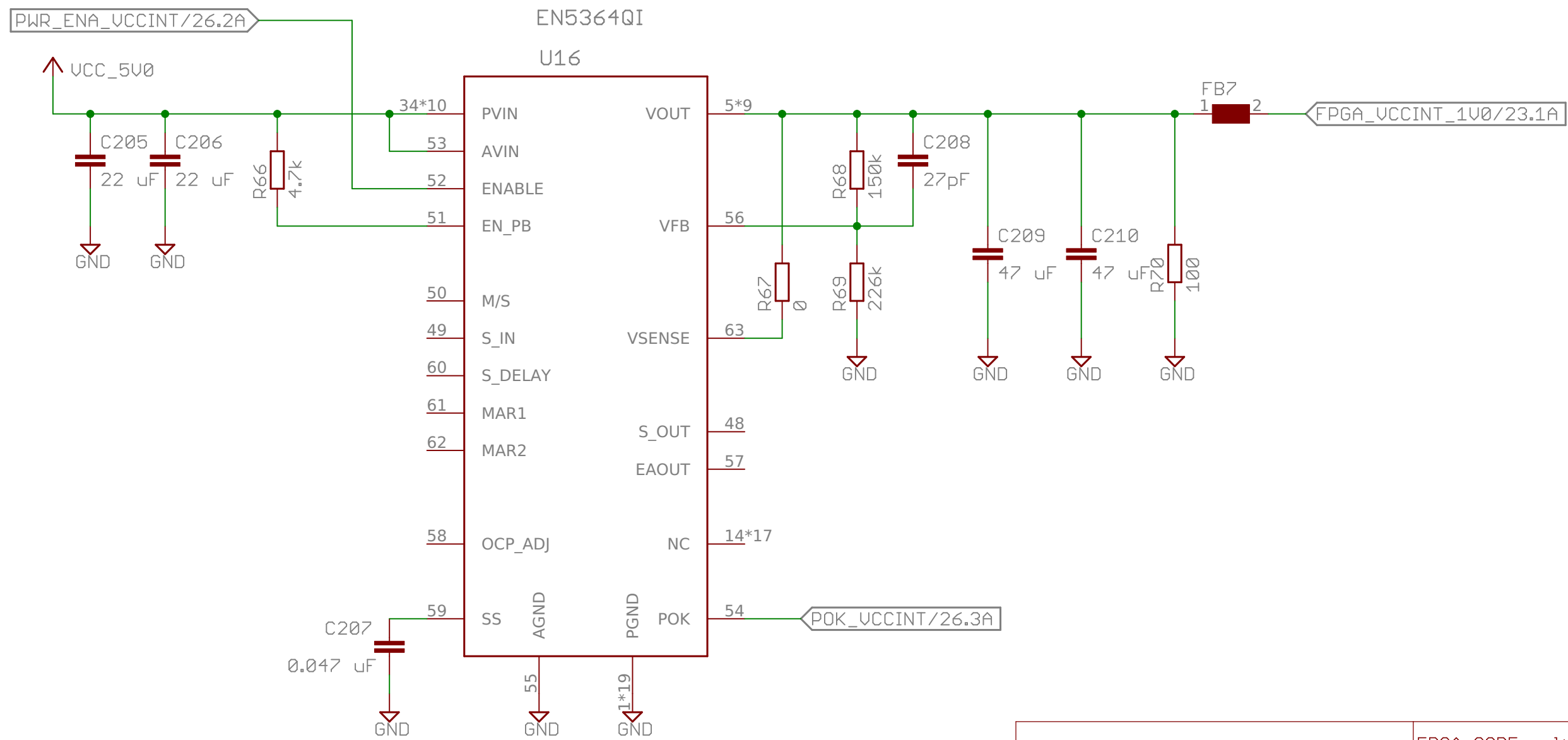
6





*) 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)



FPGA CORE voltage regulators	
rev02	
10 Feb 2016 15:31:03	
Sheet: 25/26	

1

2

3

4

5

6

A

A

B

B

C

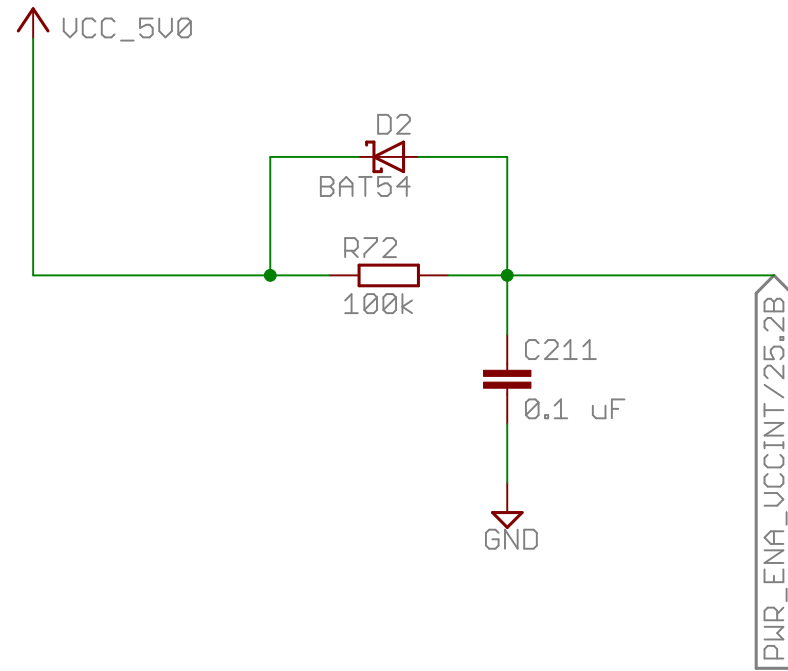
C

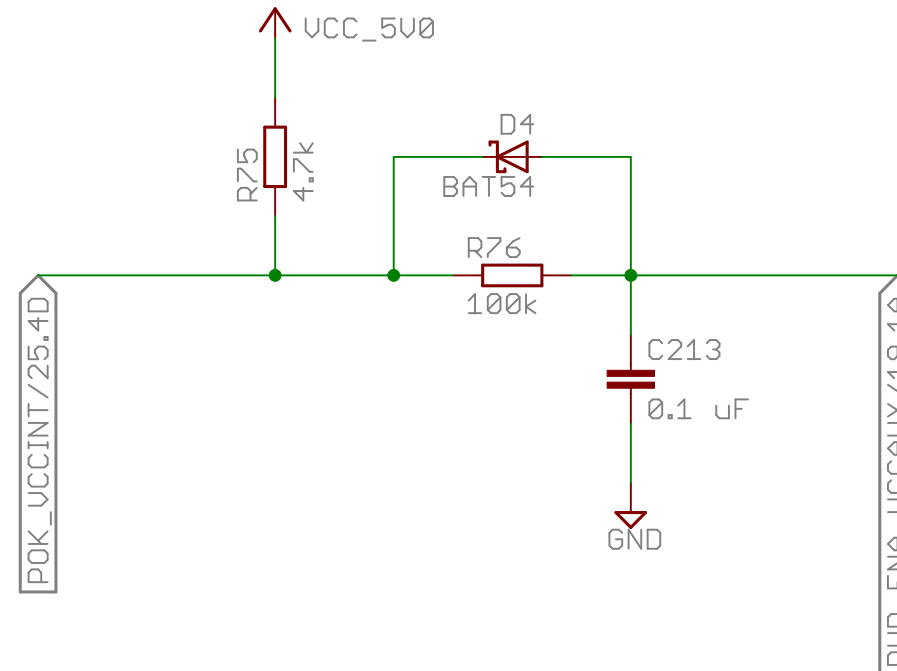
D

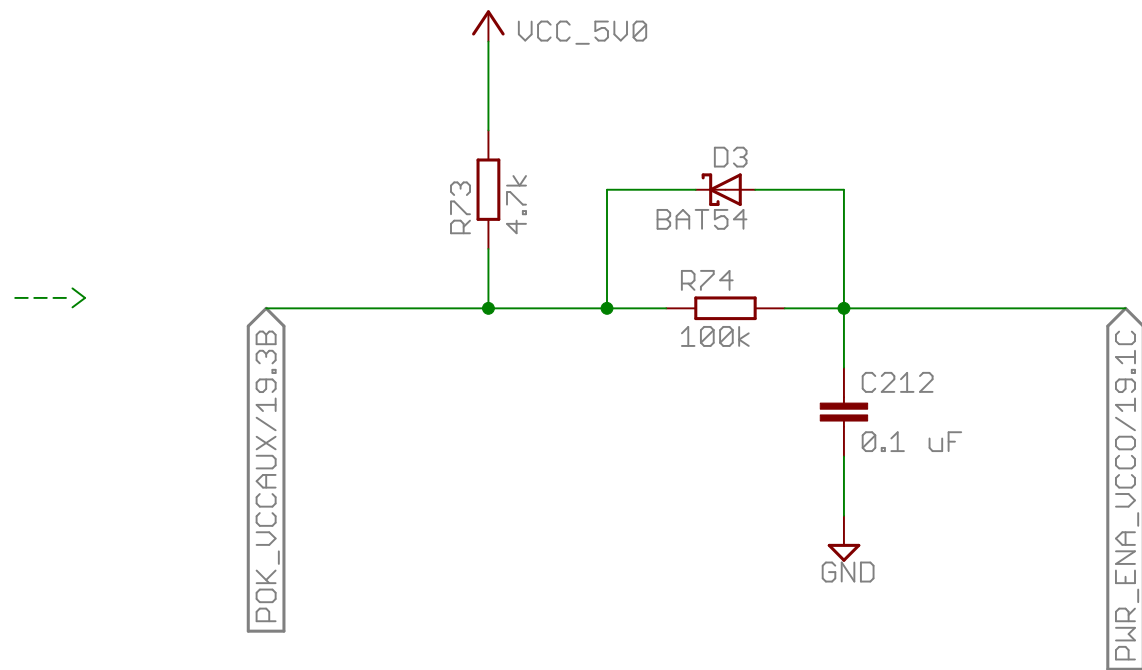
D

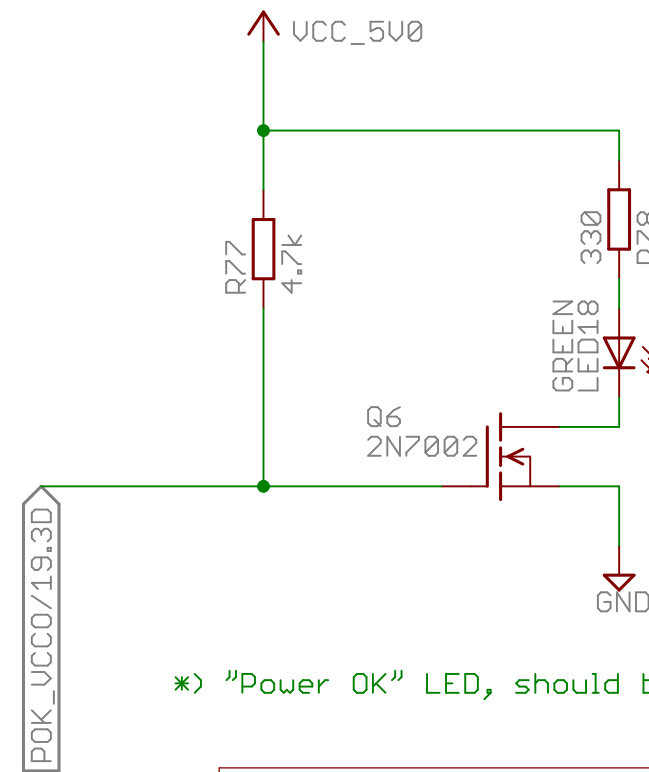
*) Recommended power-up sequence:
 1) UCCINT
 2) UCCAUX
 3) UCC0

RC network values are preliminary,
 should be tweaked after experiments









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

1

2

3

4

5

6