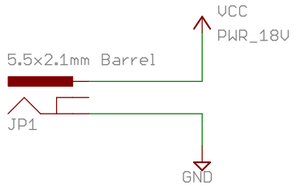
Extra

This page intentionally left blank

rev02	
9 Feb 2016 20:38:51	
Sheet: 1/26	

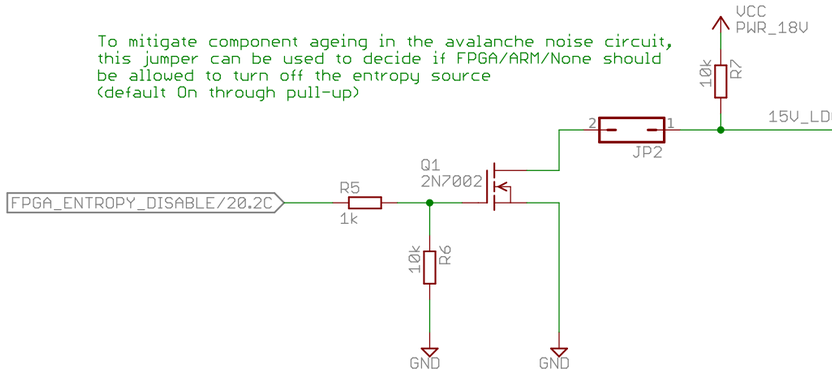
Main power input
18V DC



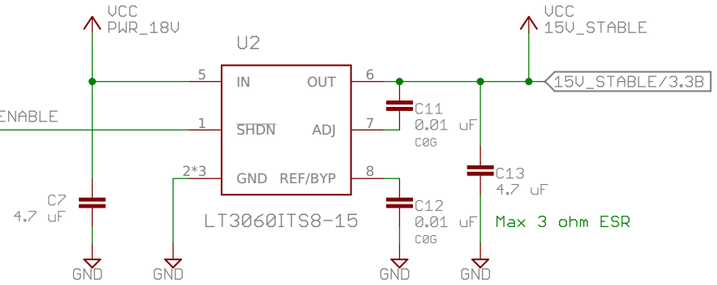
XXX verify symbol

Entropy source power

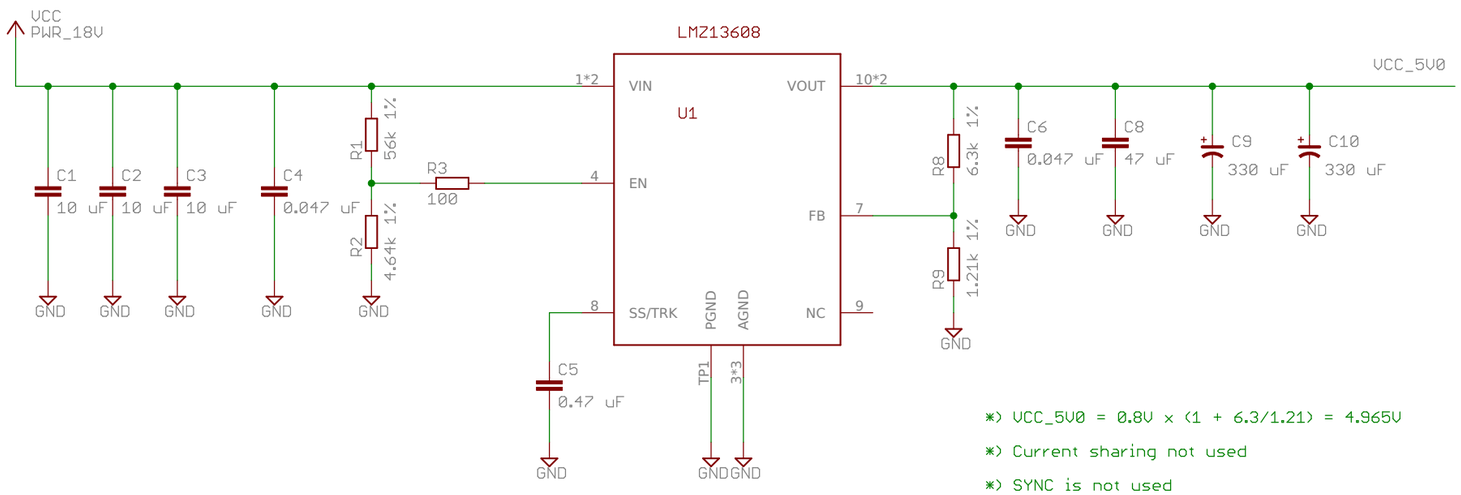
To mitigate component ageing in the avalanche noise circuit, this jumper can be used to decide if FPGA/ARM/None should be allowed to turn off the entropy source (default On through pull-up)



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



*) Intermediate Regulator: 18V -> 5V



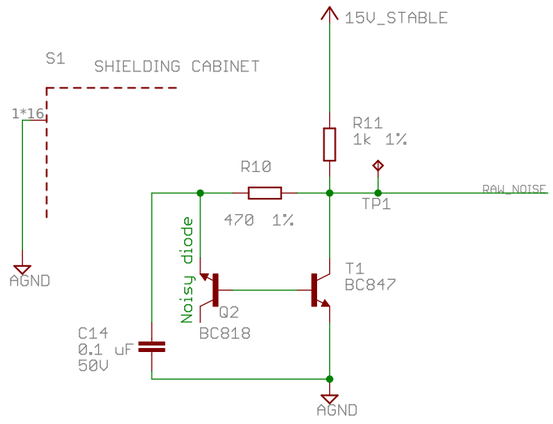
*) VCC_5V0 = 0.8V x (1 + 6.3/1.21) = 4.965V

*) Current sharing not used

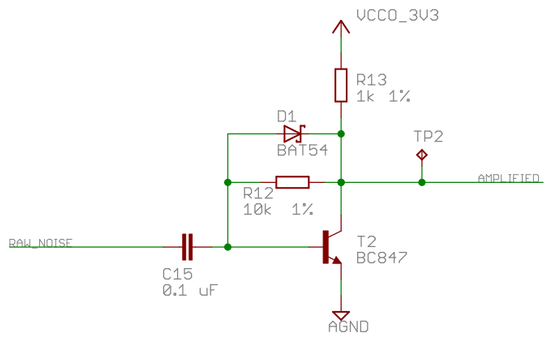
*) SYNC is not used

	Input power
	rev02
	9 Feb 2016 20:38:51
	Sheet: 2/26

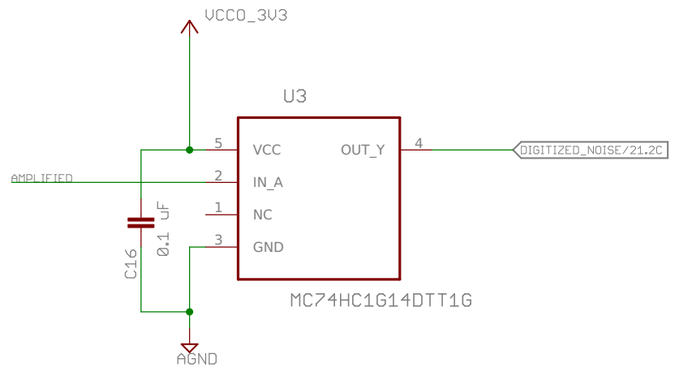
Noise generator



Amplifier



Digitizer



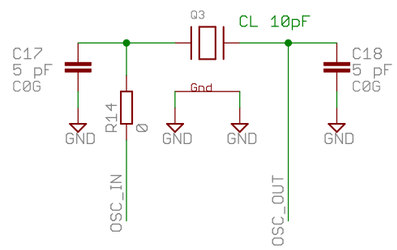
AGND is connected to GND on the board using polygons
(found no other good way) - not visible in schematics.

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.

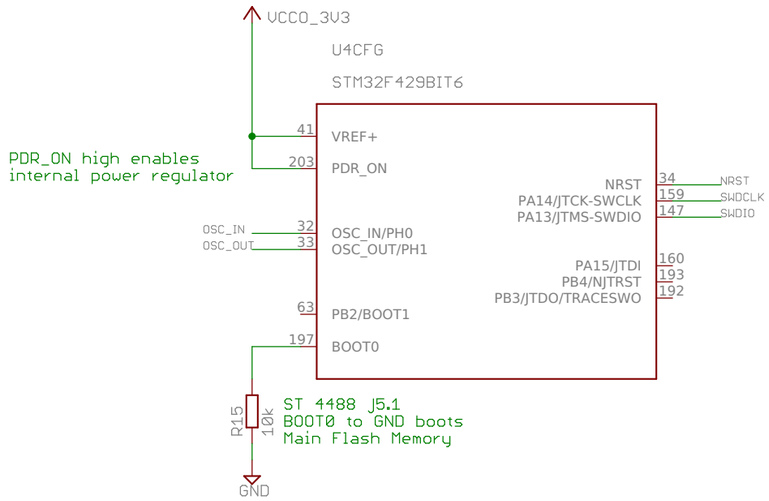
	Noise source
	rev02
	9 Feb 2016 20:38:51
	Sheet: 3/26

Basic configuration, STM32

ST AN4488 J4.1.2
suggests 25 MHz for good
Ethernet, USB OTG and I2C

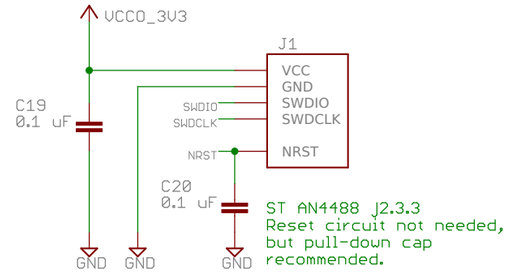


PDR_ON high enables
internal power regulator

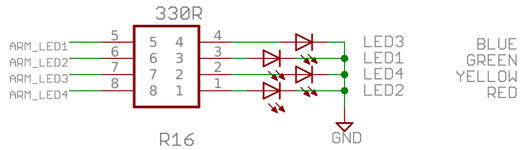


ST 4488 J5.1
BOOT0 to GND boots
Main Flash Memory

SWD program/debug

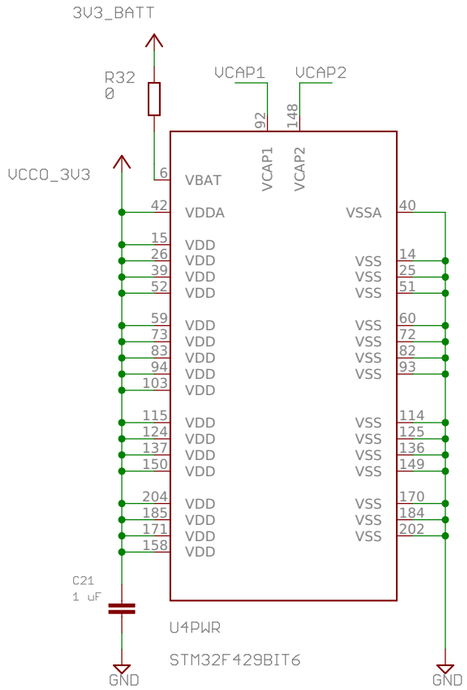


ST AN4488 J2.3.3
Reset circuit not needed,
but pull-down cap
recommended.

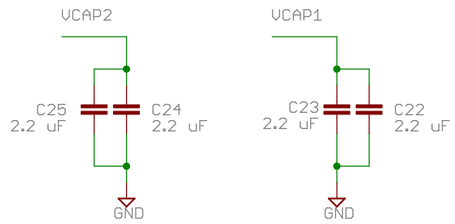


	ARM configuration
	rev02
	9 Feb 2016 20:38:51
	Sheet: 4/26

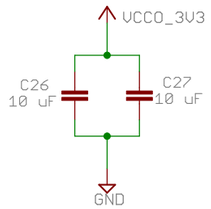
Power and bypass capacitors, STM32



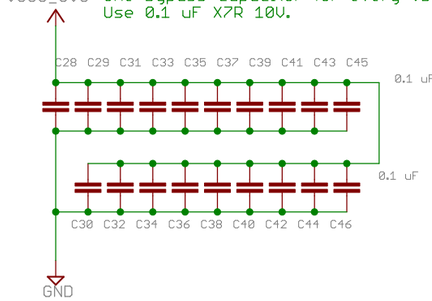
2*2*2.2uF LowESR or
2*1*4.7uF LowESR
< 1 ohm
(ST AN4488 J2.2)



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

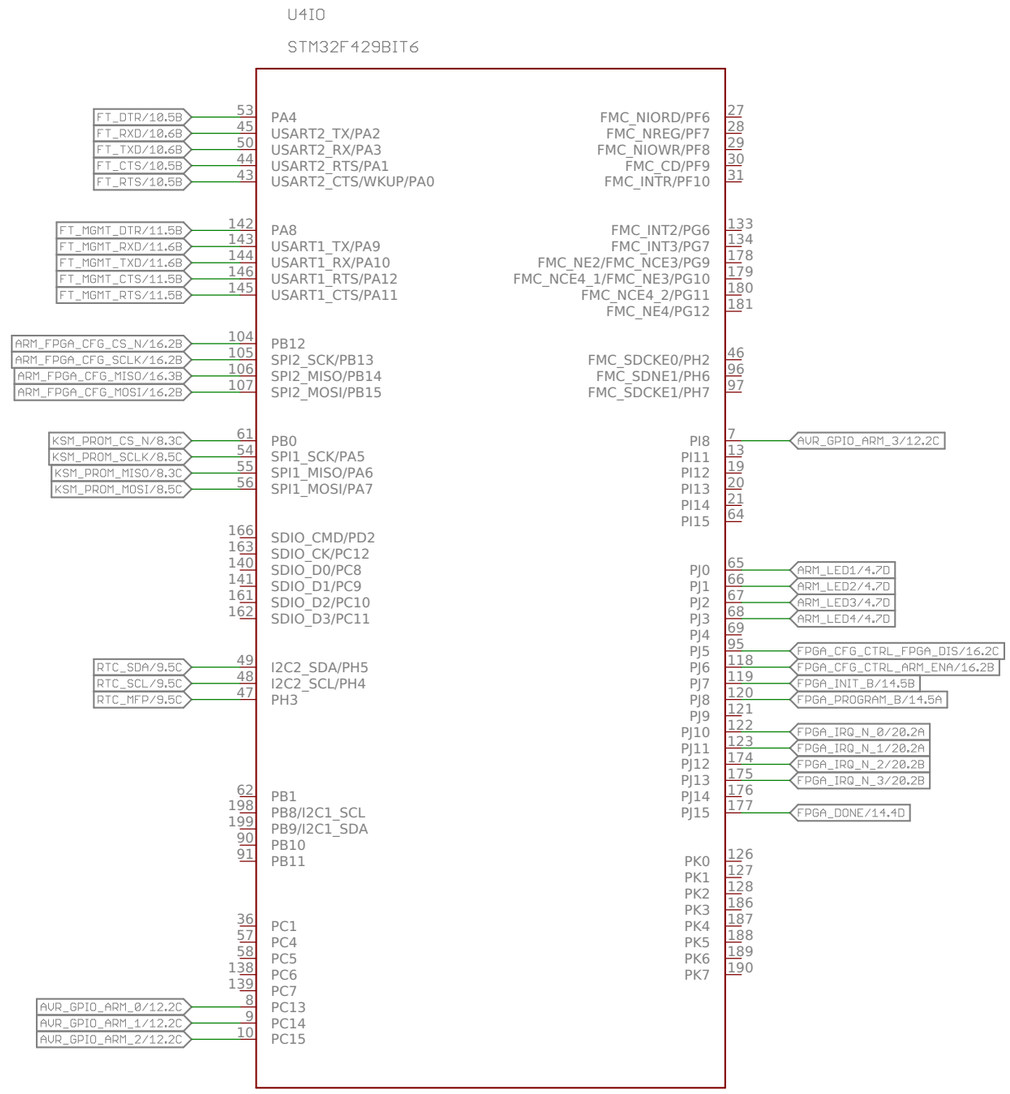


ST AN8844 J2.2
One bypass capacitor for every VDD.
Use 0.1 uF X7R 10V.



	ARM power
	rev02
	9 Feb 2016 20:38:51
	Sheet: 5/26

Input/output, STM32

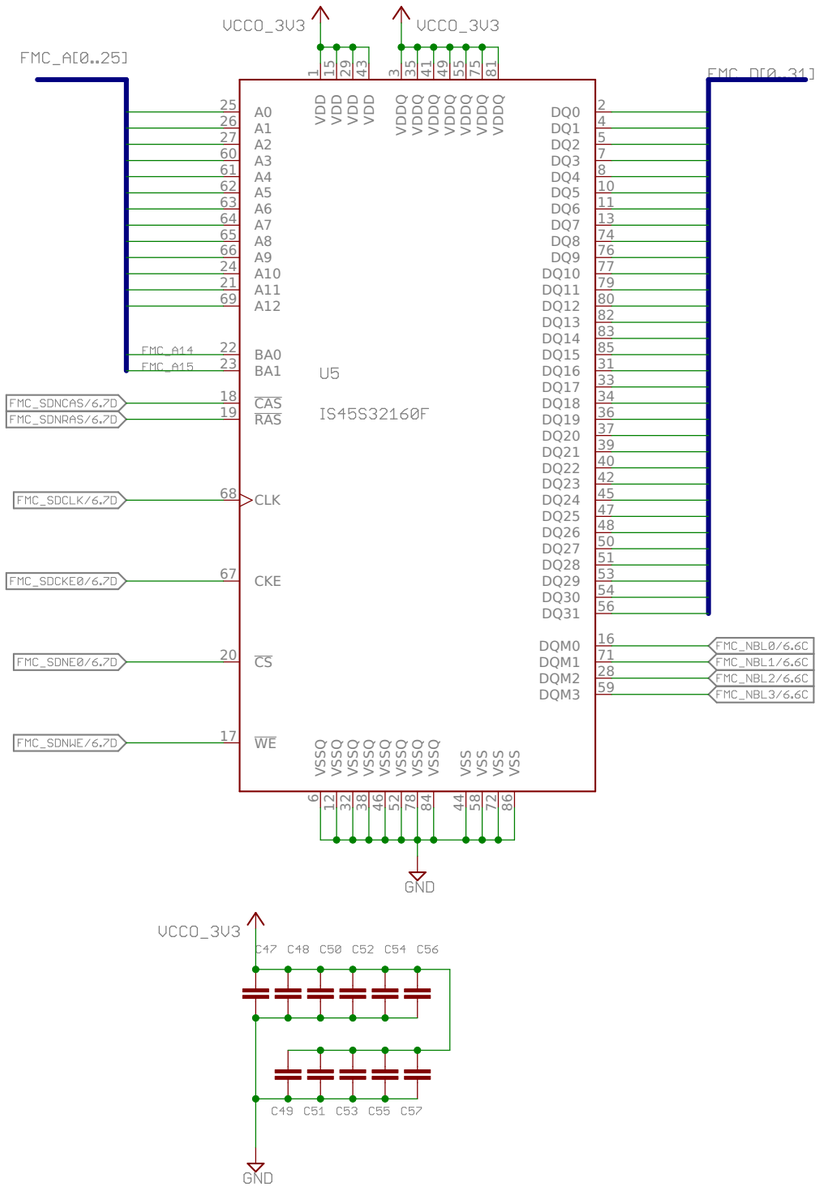


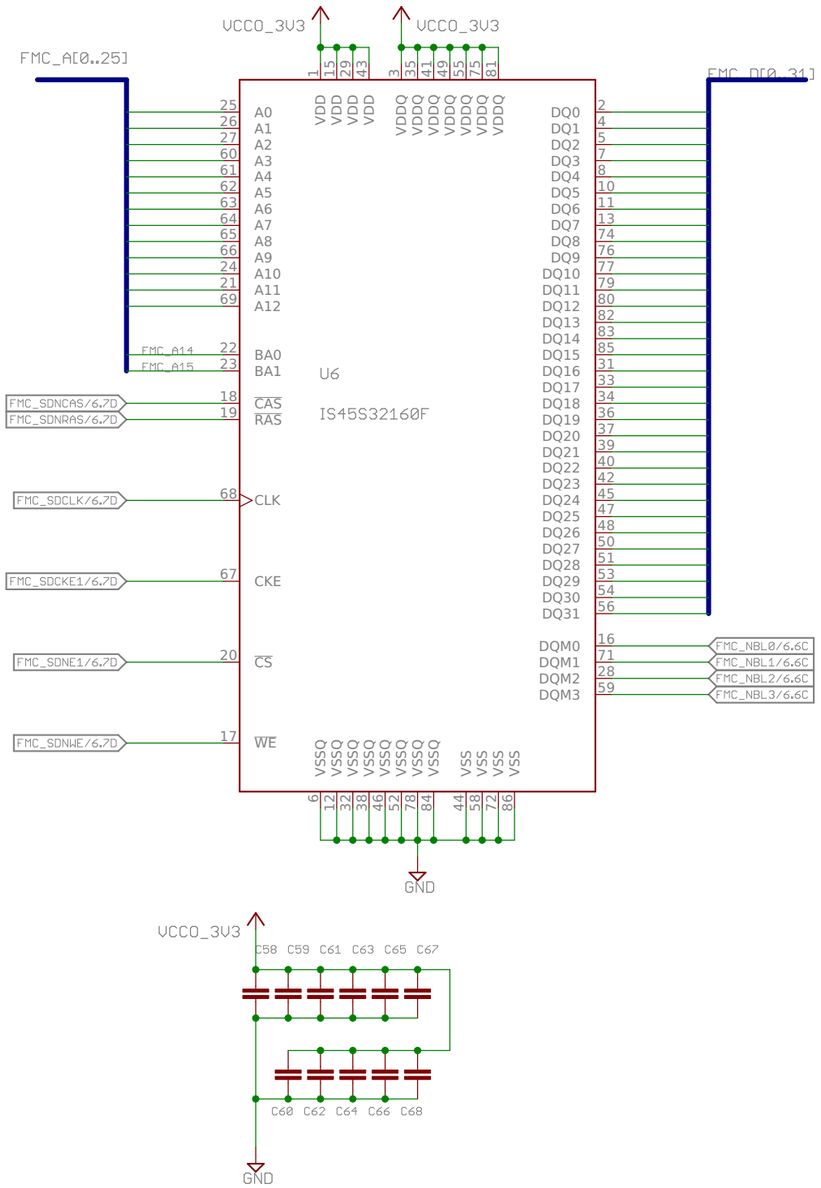
All of these input/outputs can be swapped
with equivalent functionality pins.

	ARM I/O
	rev02
	9 Feb 2016 20:38:51
	Sheet: 6/26

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.

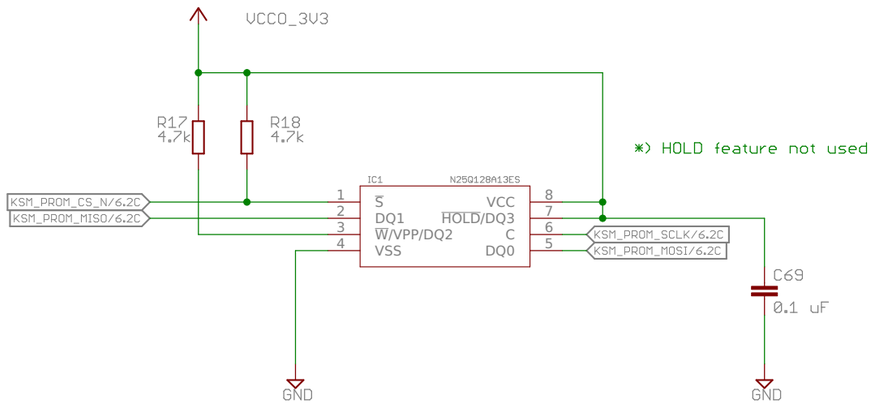




	SDRAM
	rev02
	9 Feb 2016 20:38:51
	Sheet: 7/26

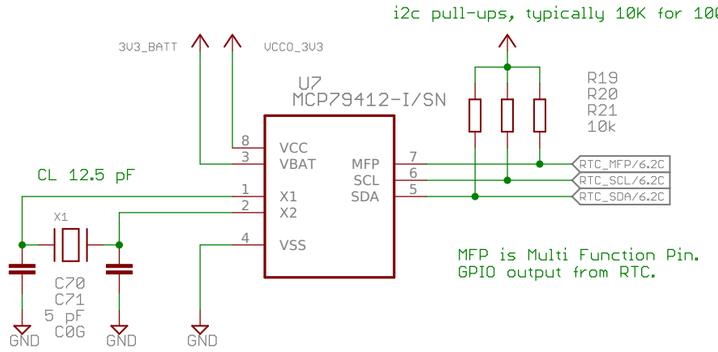
Keystore memory, 128 Mbit

This memory holds cryptographic keys
wrapped with the master key.



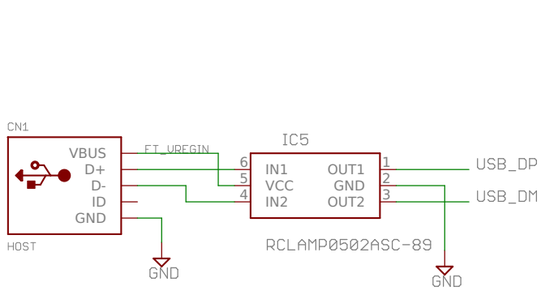
	Keystore memory
	rev02
	9 Feb 2016 20:38:51
	Sheet: 8/26

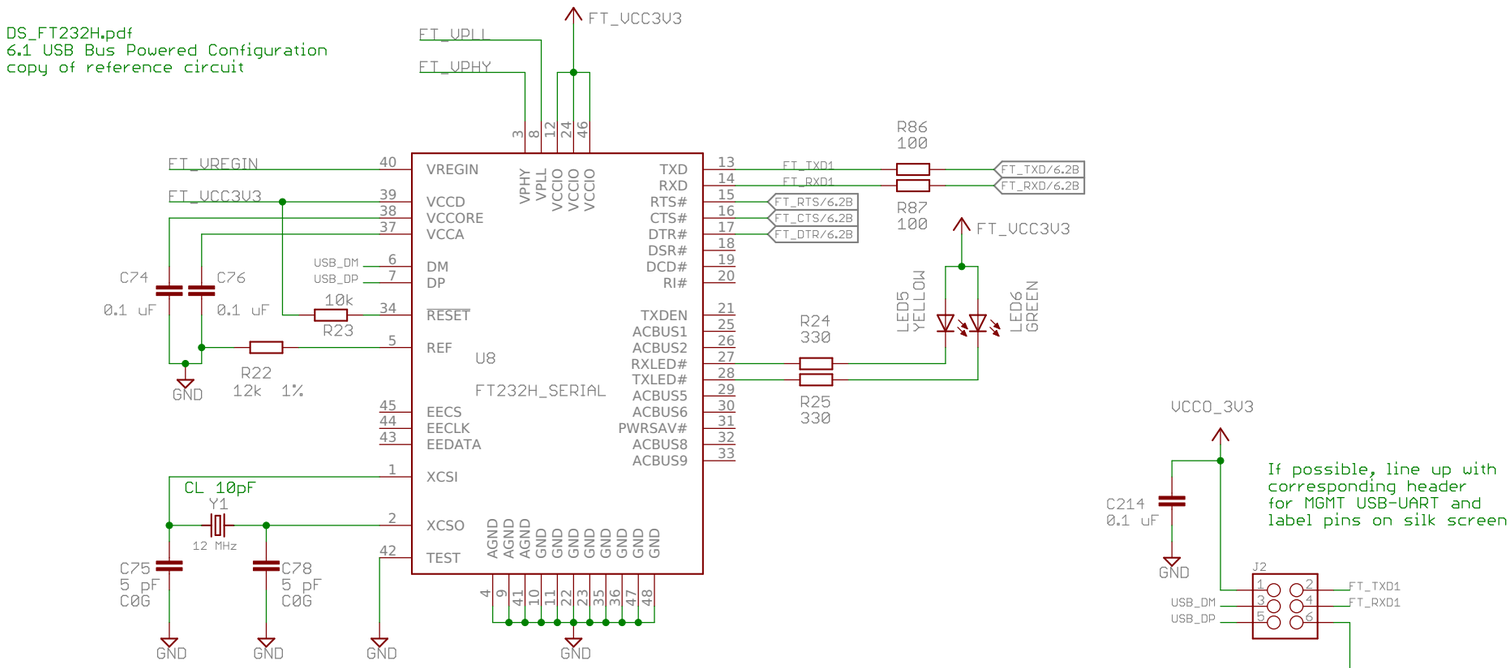
Real Time Clock

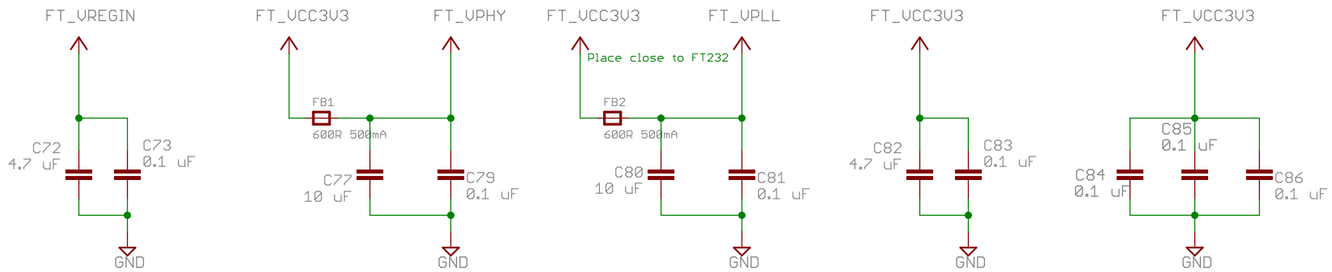


	Real Time Clock
	rev02
	9 Feb 2016 20:38:51
	Sheet: 9/26

Application access USB UART



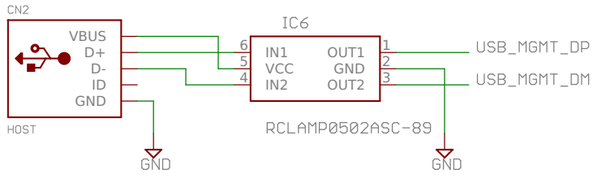


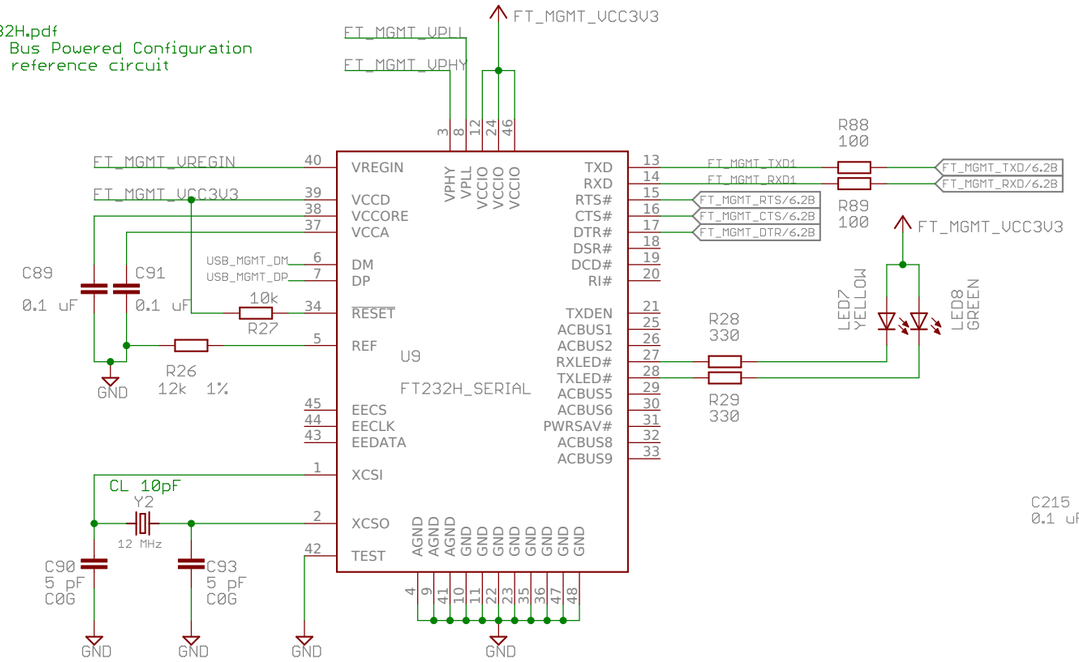


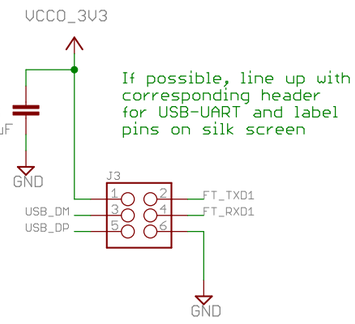
	USB-UART interface
	rev02
	9 Feb 2016 20:38:51
	Sheet: 10/26

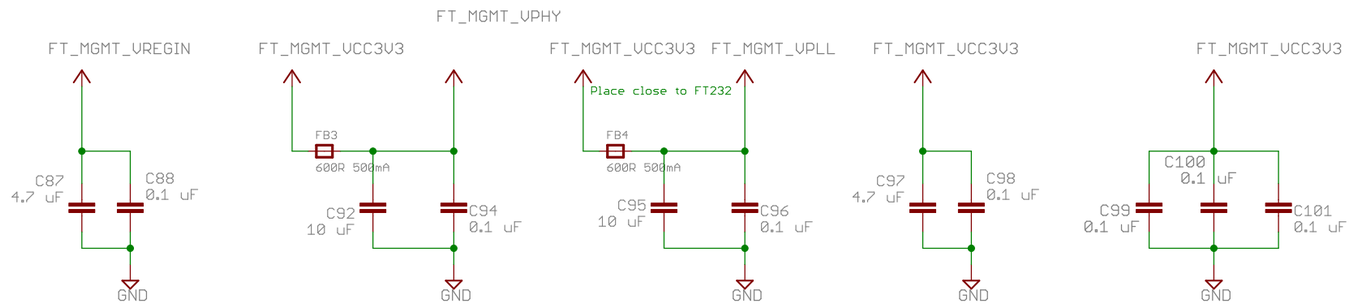
Management access USB UART

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







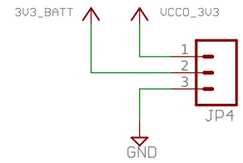


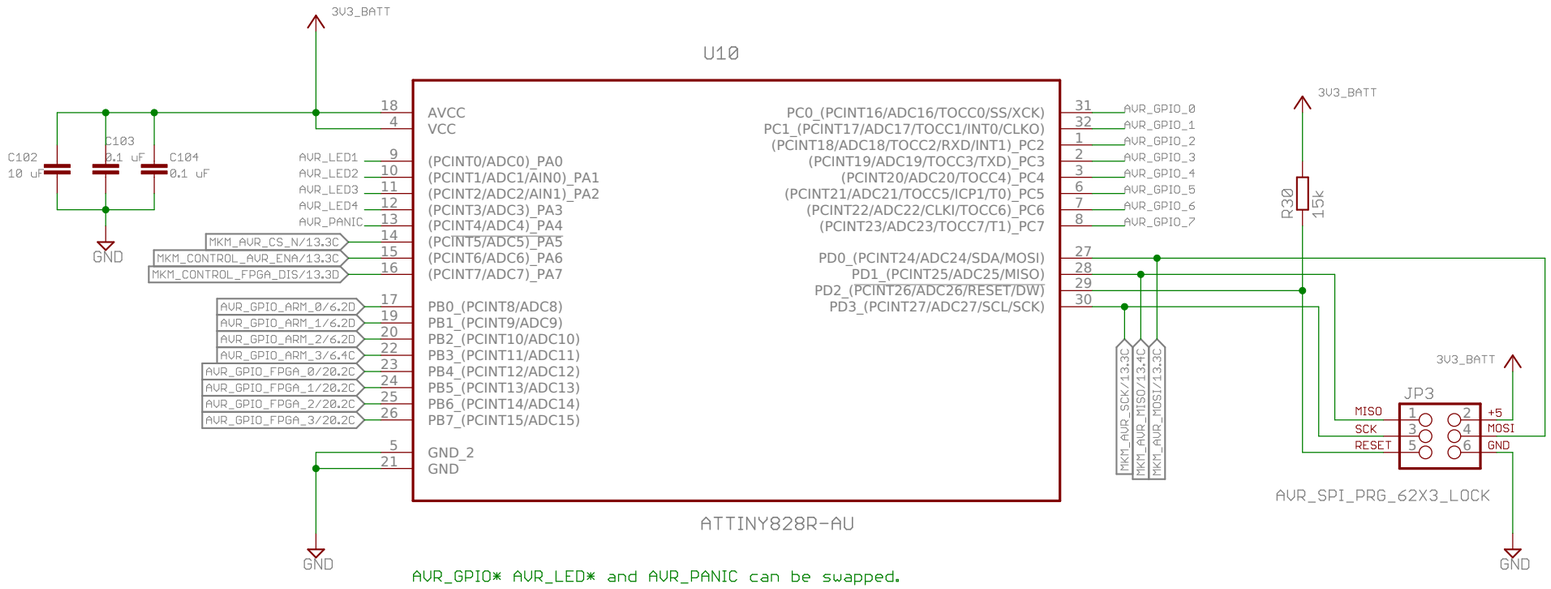
	MGMT USB-UART
	rev02
	9 Feb 2016 20:38:51
	Sheet: 11/26

AVR Tiny Tamper Detect MCU

Connector for external 3V3 battery.

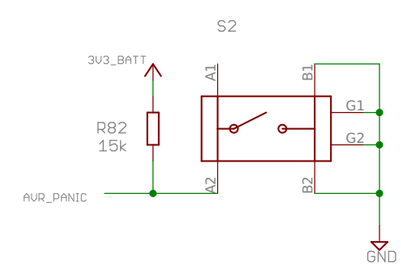
Place a jumper between pins 1-2
to "emulate" having a battery present.



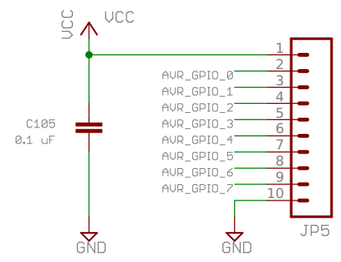


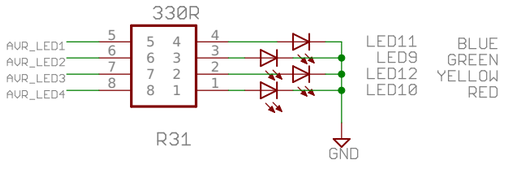
AVR_GPIO* AVR_LED* and AVR_PANIC can be swapped.

Panic button



Expansion GPIO

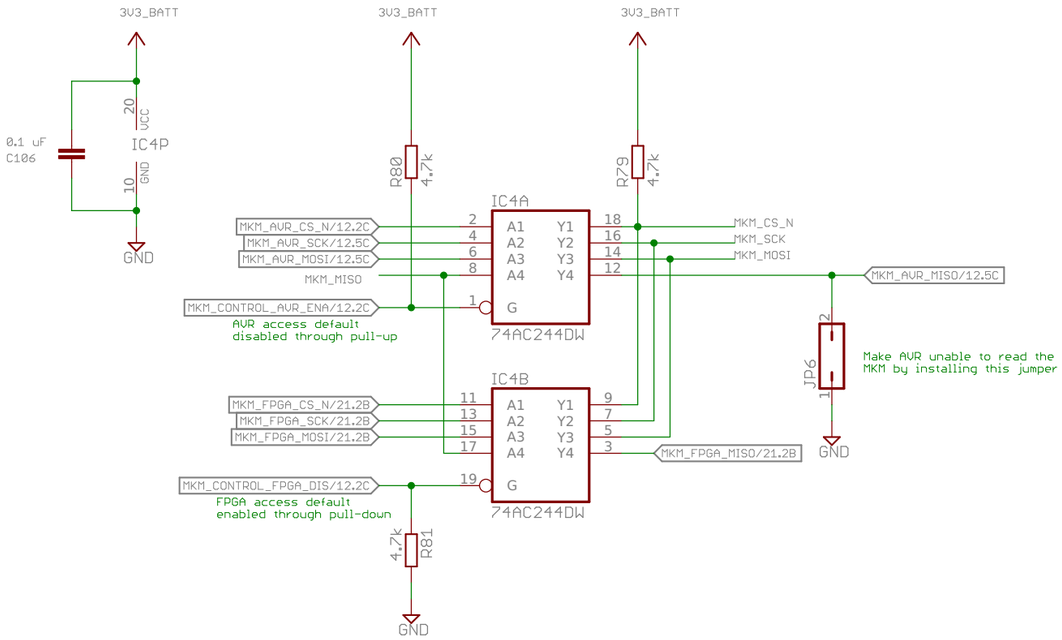




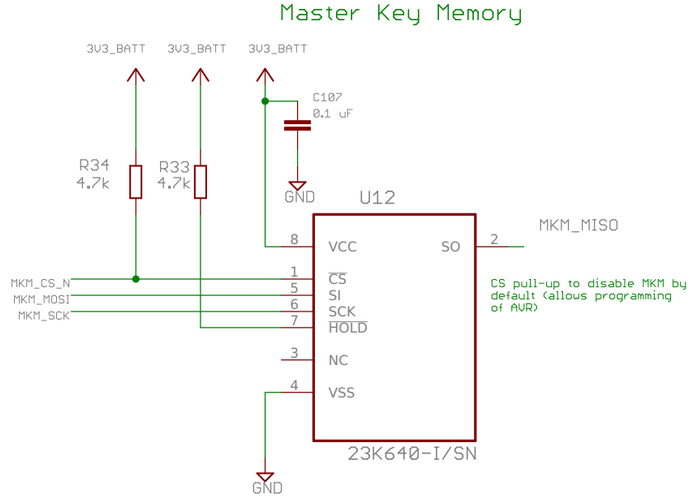
	AVR Tamper circuit
	rev02
	9 Feb 2016 20:38:51
	Sheet: 12/26

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.

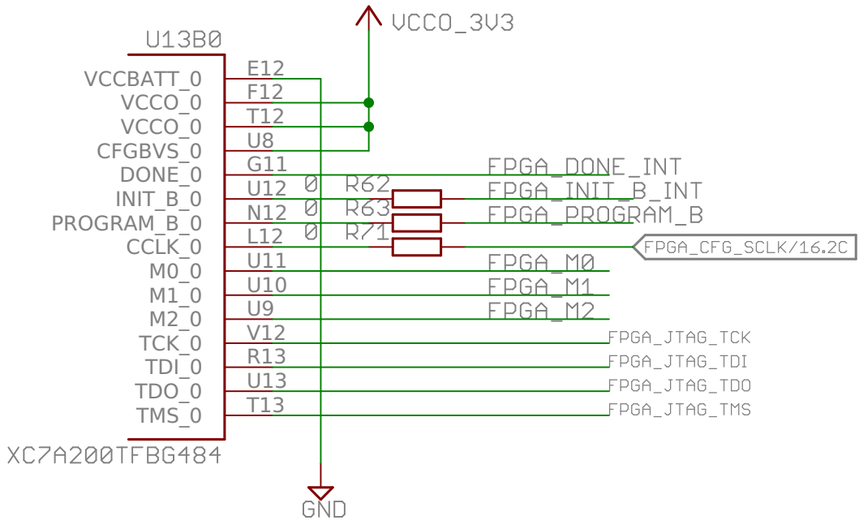


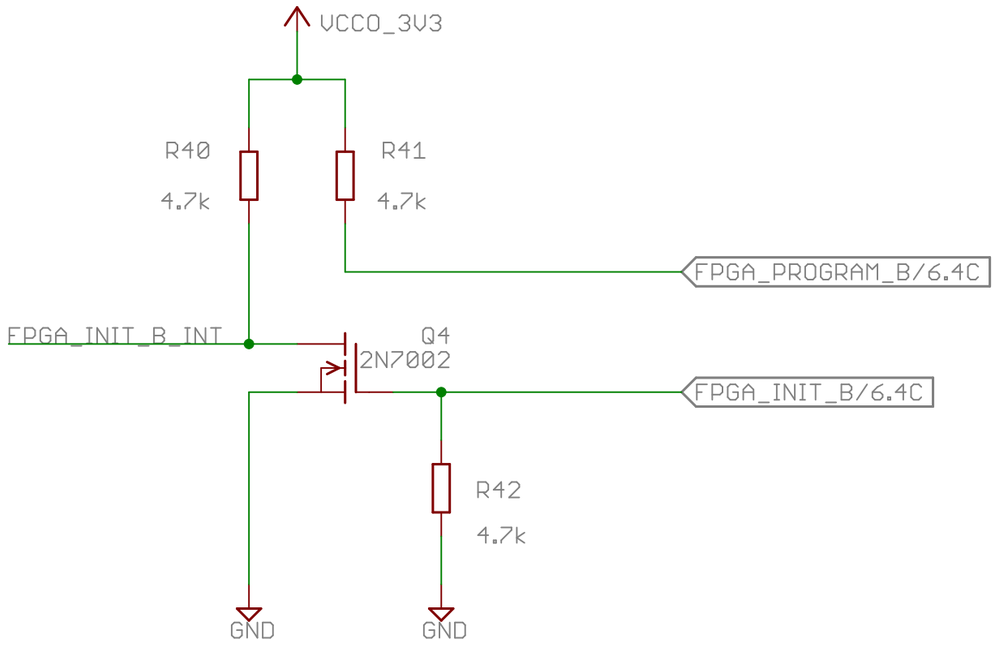
Master Key Memory



	Master Key Memory
	rev02
	9 Feb 2016 20:38:51
	Sheet: 13/26

*) Configuration Interface



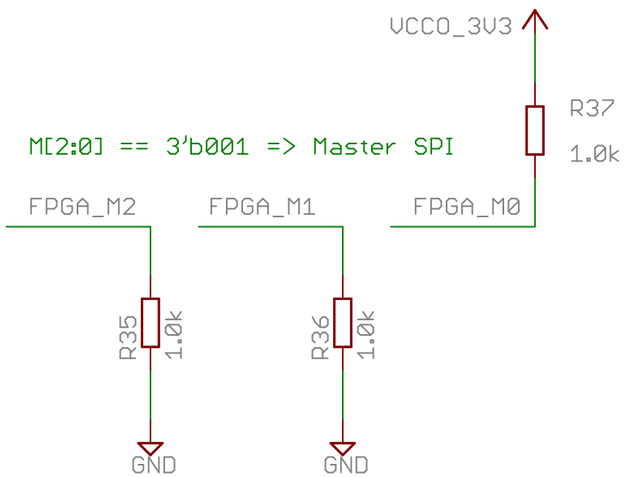


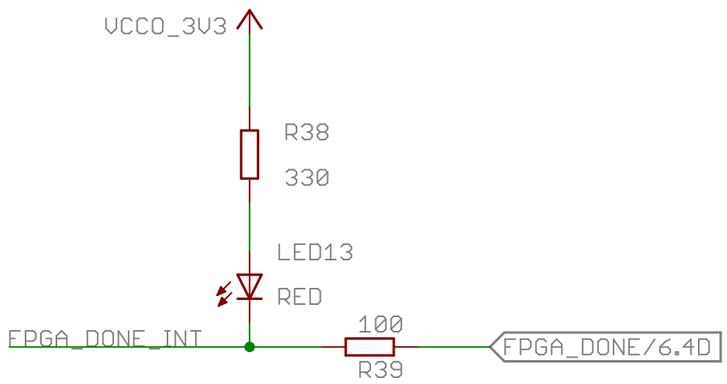
*) Since VCCO is 3.3V, CFGBVS must be tied High.

*) Battery is not used

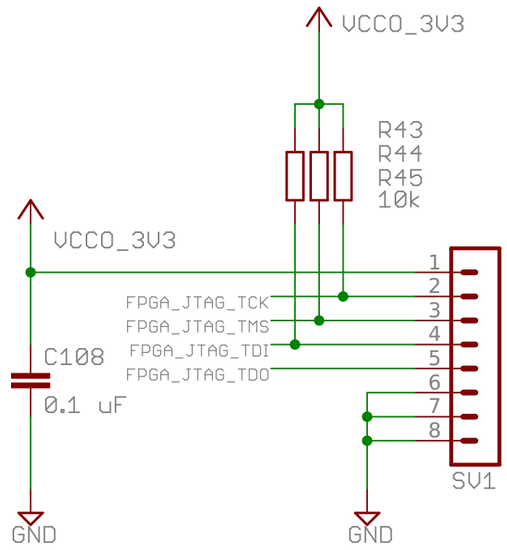
*) PROG_B is dedicated input -- can be driven by STM32 directly

*) INIT_B is bi-directional open-drain, must be driven with MOSFET to ground





*) "Not DONE" LED, should be of red color



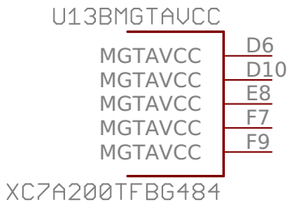
FPGA configuration interface

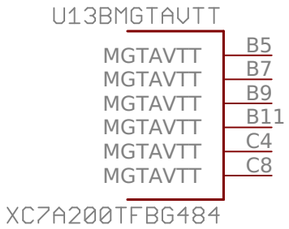
rev02

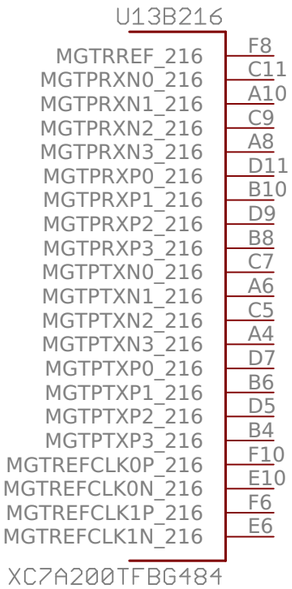
9 Feb 2016 20:38:51

Sheet: 14/26

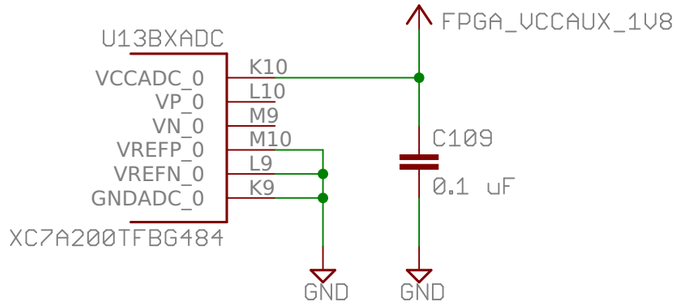
*) Transceivers [NOT USED]



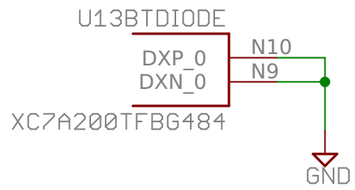




*) XADC [NOT USED]

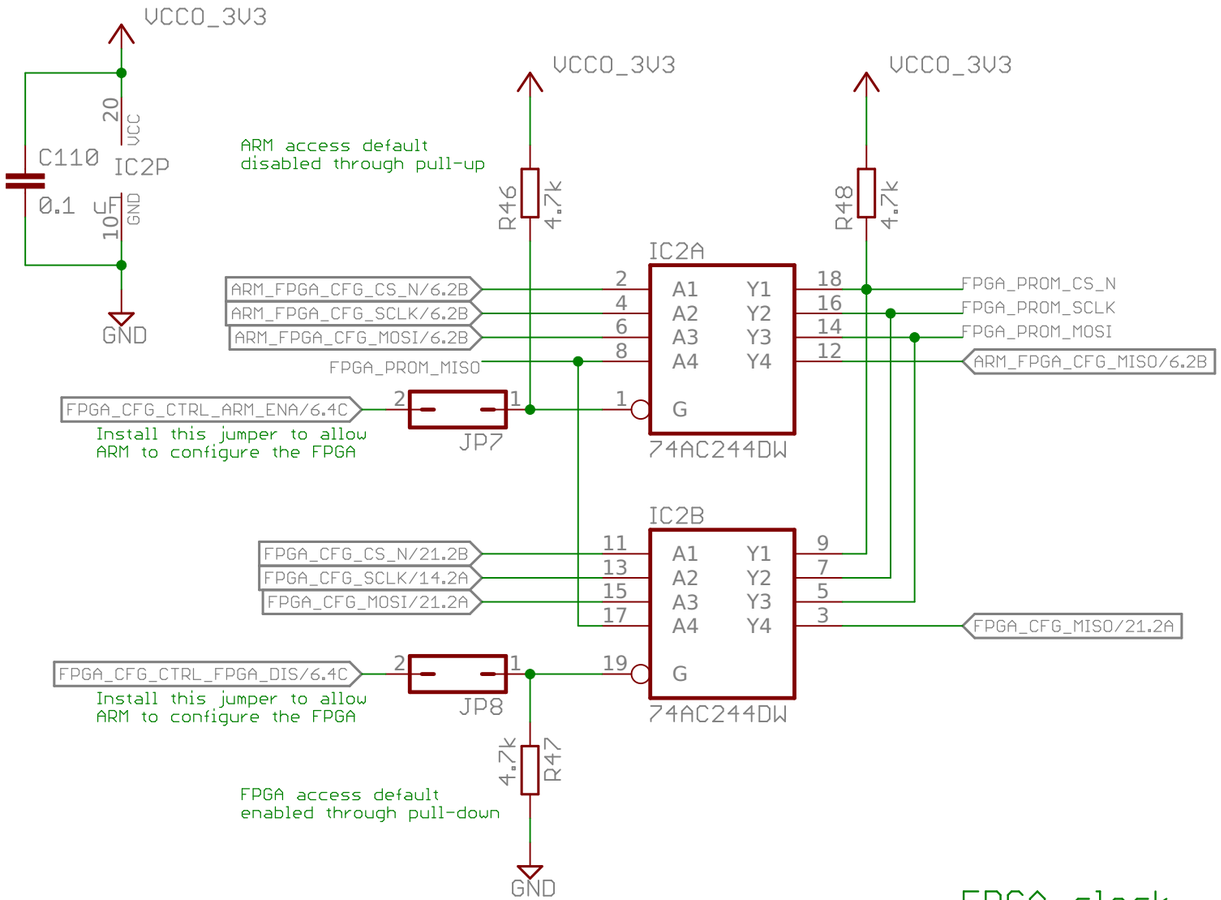


*) Temperature Sensor [NOT USED]



	FPGA unused
	rev02
	9 Feb 2016 20:38:51
	Sheet: 15/26

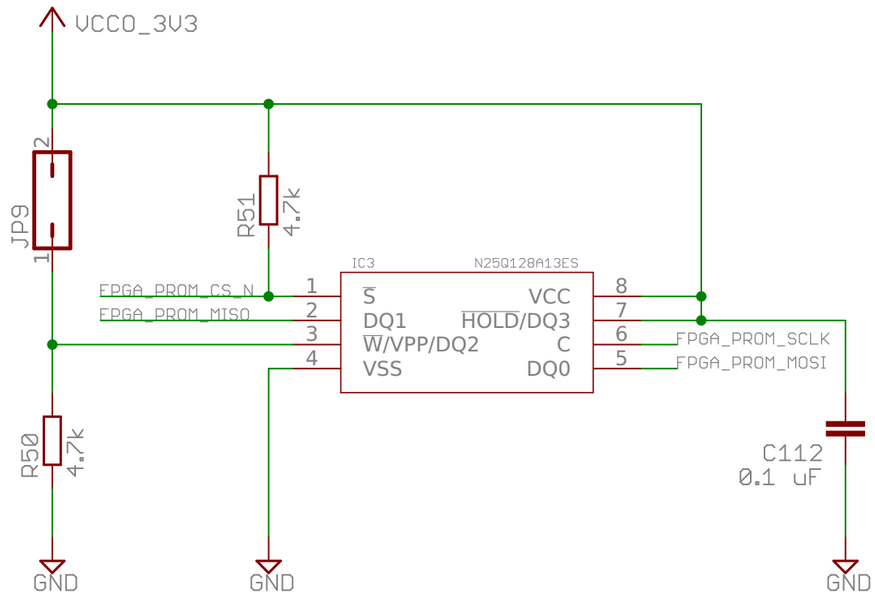
SPI mux to let ARM override access to FPGA config memory (to reprogram FPGA)



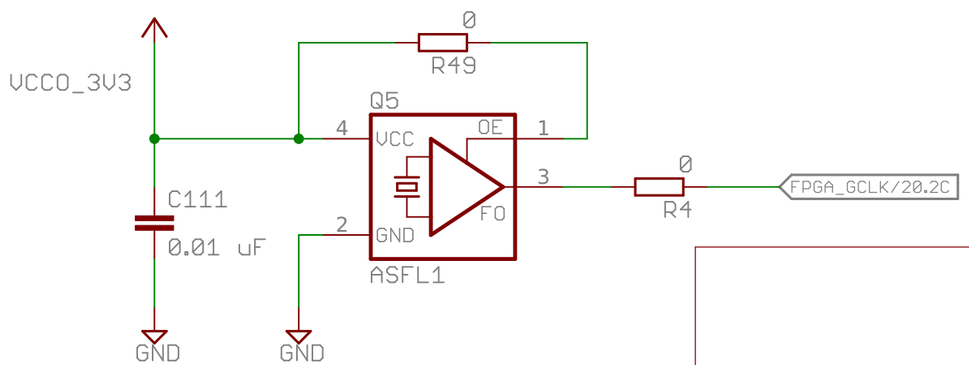
FPGA config memory, 128 Mbit

*) 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



FPGA supporting components	
rev02	
9 Feb 2016 20:38:51	
Sheet: 16/26	

*) Middle Right Bank

U13B15

VCCO_15	G19	VCCO_3V3
VCCO_15	H16	
VCCO_15	J13	*) Completely unused banks still must be powered
VCCO_15	K20	
VCCO_15	L17	
VCCO_15	N21	
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_FOE_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	

XC7A200TFBG484

*) Upper Left Bank

U13B35

VCCO_35	C1	VCCO_3V3
VCCO_35	F2	
VCCO_35	H6	*) Completely unused banks still must be powered
VCCO_35	J3	
VCCO_35	M4	
VCCO_35	N1	
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

FPGA unused banks

rev02

9 Feb 2016 20:38:51

Sheet: 17/26

*) Lower Left Bank

U13B34

VCCO_3V3

VCCO_34	R5	
VCCO_34	T2	
VCCO_34	V6	
VCCO_34	W3	
VCCO_34	AA7	
VCCO_34	AB4	
IO_0_34	T3	FMC_D0
IO_L1P_T0_34	T1	FMC_D1
IO_L1N_T0_34	U1	FMC_D2
IO_L2P_T0_34	U2	FMC_D3
IO_L2N_T0_34	V2	FMC_D4
IO_L3P_T0_DQS_34	R3	FMC_D5
IO_L3N_T0_DQS_34	R2	FMC_D6
IO_L4P_T0_34	W2	FMC_D7
IO_L4N_T0_34	Y2	FMC_D8
IO_L5P_T0_34	W1	FMC_D9
IO_L5N_T0_34	Y1	FMC_D10
IO_L6P_T0_34	U3	FMC_D11
IO_L6N_T0_VREF_34	V3	FMC_D12
IO_L7P_T1_34	AA1	FMC_D13
IO_L7N_T1_34	AB1	FMC_D14
IO_L8P_T1_34	AB3	FMC_D15
IO_L8N_T1_34	AB2	FMC_D16
IO_L9P_T1_DQS_34	Y3	FMC_D17
IO_L9N_T1_DQS_34	AA3	FMC_D18
IO_L10P_T1_34	AA5	FMC_D19
IO_L10N_T1_34	AB5	FMC_D20
IO_L11P_T1_SRCC_34	Y4	FMC_D21
IO_L11N_T1_SRCC_34	AA4	FMC_D22
IO_L12P_T1_MRCC_34	V4	FMC_D23
IO_L12N_T1_MRCC_34	W4	FMC_D24
IO_L13P_T2_MRCC_34	R4	FMC_D25
IO_L13N_T2_MRCC_34	T4	FMC_D26
IO_L14P_T2_SRCC_34	T5	FMC_D27
IO_L14N_T2_SRCC_34	U5	FMC_D28
IO_L15P_T2_DQS_34	W6	FMC_D29
IO_L15N_T2_DQS_34	W5	FMC_D30
IO_L16P_T2_34	U6	FMC_D31
IO_L16N_T2_34	V5	FMC_NE1/6.6D
IO_L17P_T2_34	R6	FMC_NL/6.6D
IO_L17N_T2_34	T6	FMC_NOE/6.6D
IO_L18P_T2_34	Y6	FMC_NWAIT/6.6D
IO_L18N_T2_34	AA6	FMC_NWE/6.6D
IO_L19P_T3_34	V7	
IO_L19N_T3_VREF_34	W7	
IO_L20P_T3_34	AB7	
IO_L20N_T3_34	AB6	
IO_L21P_T3_DQS_34	V9	
IO_L21N_T3_DQS_34	V8	
IO_L22P_T3_34	AA8	
IO_L22N_T3_34	AB8	
IO_L23P_T3_34	Y8	
IO_L23N_T3_34	Y7	
IO_L24P_T3_34	W9	
IO_L24N_T3_34	Y9	
IO_25_34	U7	

FMC_D[0..31]

<-- FMC_D[...] signals can be swapped

<-- FMC_* control signals can be swapped

XC7A200TFBG484

*) Bottom Bank

U13B13

VCCO_3V3

VCCO_13	V16	
VCCO_13	W13	
VCCO_13	Y10	
VCCO_13	AA17	
VCCO_13	AB14	
IO_0_13	Y17	FMC_A0
IO_L1P_T0_13	Y16	FMC_A1
IO_L1N_T0_13	AA16	FMC_A2
IO_L2P_T0_13	AB16	FMC_A3
IO_L2N_T0_13	AB17	FMC_A4
IO_L3P_T0_DQS_13	AA13	FMC_A5
IO_L3N_T0_DQS_13	AB13	FMC_A6
IO_L4P_T0_13	AA15	FMC_A7
IO_L4N_T0_13	AB15	FMC_A8
IO_L5P_T0_13	Y13	FMC_A9
IO_L5N_T0_13	AA14	FMC_A10
IO_L6P_T0_13	W14	FMC_A11
IO_L6N_T0_VREF_13	Y14	FMC_A12
IO_L7P_T1_13	AB11	FMC_A13
IO_L7N_T1_13	AB12	FMC_A14
IO_L8P_T1_13	AA9	FMC_A15
IO_L8N_T1_13	AB10	FMC_A16
IO_L9P_T1_DQS_13	AA10	FMC_A17
IO_L9N_T1_DQS_13	AA11	FMC_A18
IO_L10P_T1_13	V10	FMC_A19
IO_L10N_T1_13	W10	FMC_A20
IO_L11P_T1_SRCC_13	Y11	FMC_A21
IO_L11N_T1_SRCC_13	Y12	FMC_A22
IO_L12P_T1_MRCC_13	W11	
IO_L12N_T1_MRCC_13	W12	FMC_A23
IO_L13P_T2_MRCC_13	V13	FMC_A24
IO_L13N_T2_MRCC_13	V14	FMC_A25
IO_L14P_T2_SRCC_13	U15	
IO_L14N_T2_SRCC_13	V15	
IO_L15P_T2_DQS_13	T14	
IO_L15N_T2_DQS_13	T15	
IO_L16P_T2_13	W15	
IO_L16N_T2_13	W16	
IO_L17P_T2_13	T16	
IO_L17N_T2_13	U16	

FMC_A[0..25]

<-- FMC_A[...] signals can be swapped

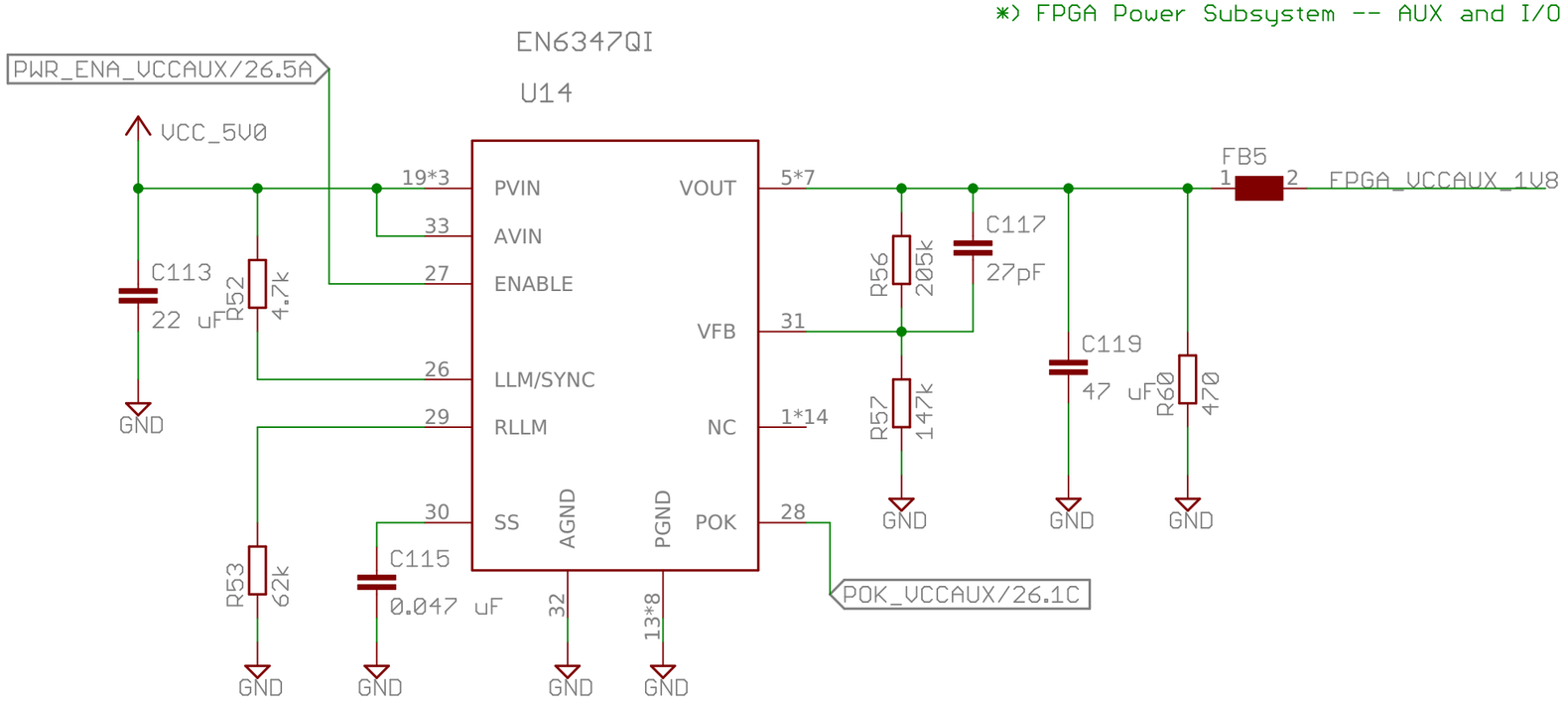
FMC_CLK/6.6D

<-- FMC_CLK signal _MUST_ go into either W11 or V13 (i.e. into one of the two positive (master) sides of the two available MRCC differential pairs)

XC7A200TFBG484

FPGA FMC interface	
rev02	
9 Feb 2016 20:38:51	
Sheet: 18/26	

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

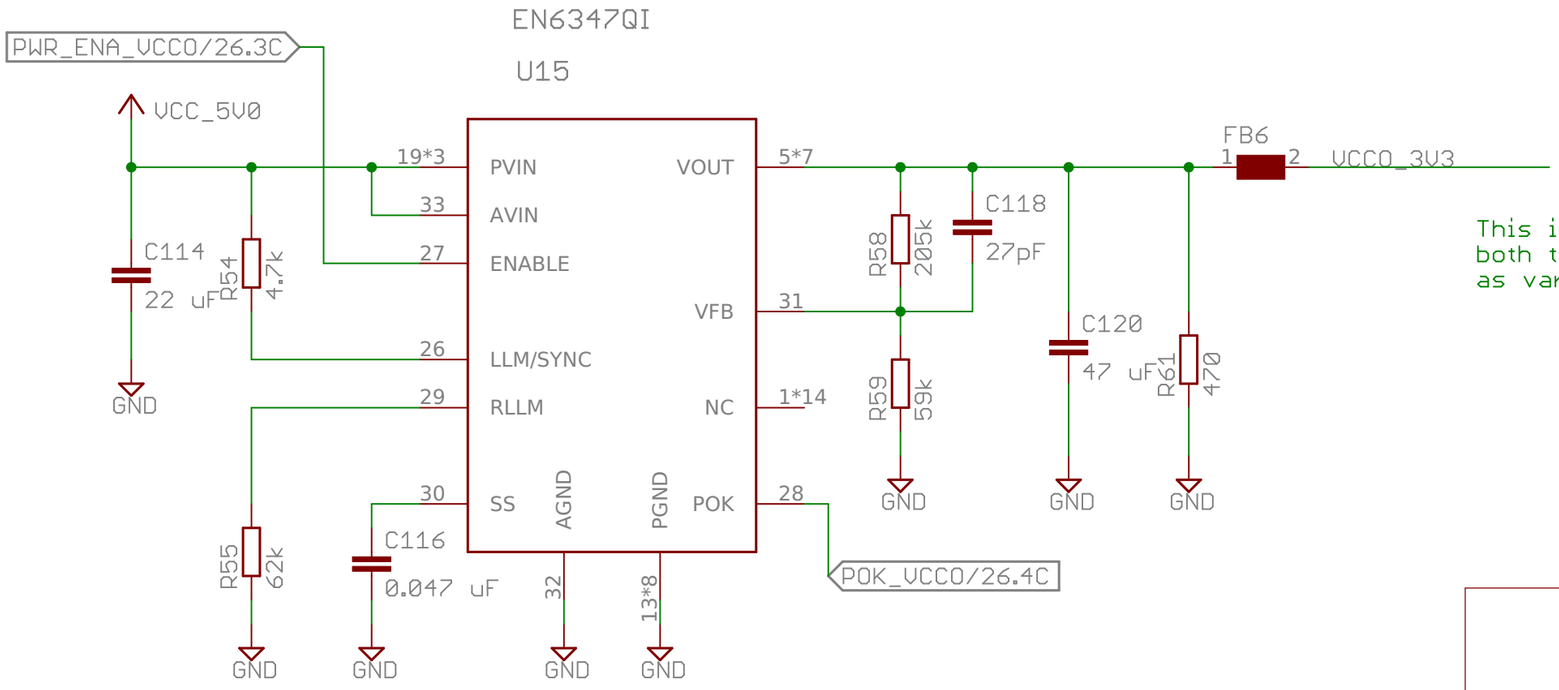


*) VCCAUX = 0.75V x (1 + 205 / 147) = 1.796V

*) VCCO = 0.75V x (1 + 205 / 59) = 3.356

*) Minimal load current is 2 mA:
1.8V / 470 Ohm = ~4mA
3.3V / 470 Ohm = ~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.

	FPGA voltage regulators
	rev02
	9 Feb 2016 20:38:51
	Sheet: 19/26

*) Upper Right Bank

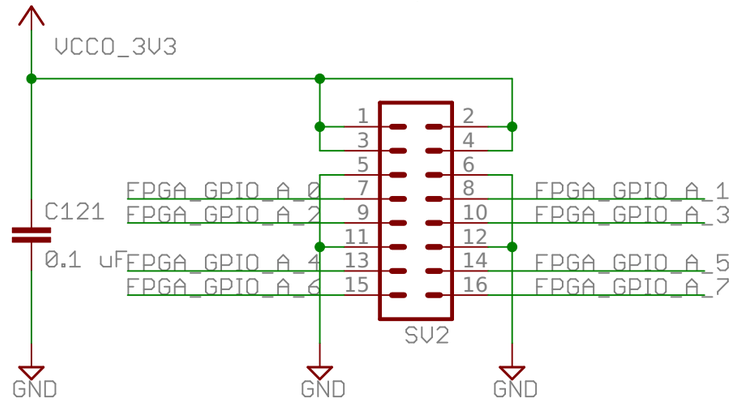
NOTE: One of the FPGA_GPIO_* pins should be connected to one of the MRCC pins.

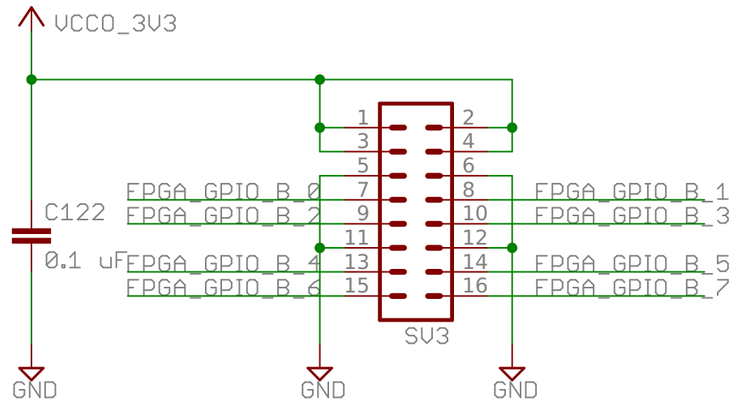
The non-MRCC GPIO signals should be length matched to within 500 ps of the MRCC signal.

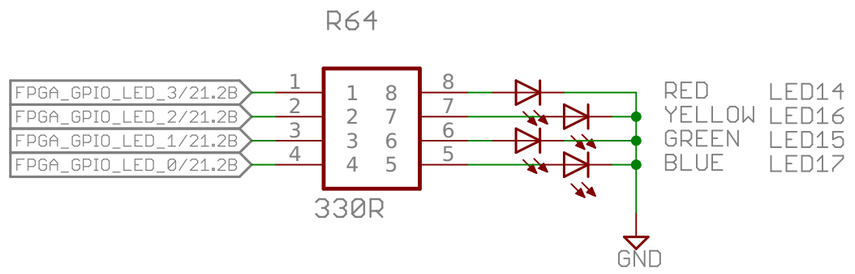
*) FPGA_GCLK signal _MUST_ go into either D17 or C18 (i.e. into one of the two positive (master) sides of the two available MRCC differential pairs)

*) FPGA_GPIO_* and FPGA_IRQ_N_* signals can be swapped

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



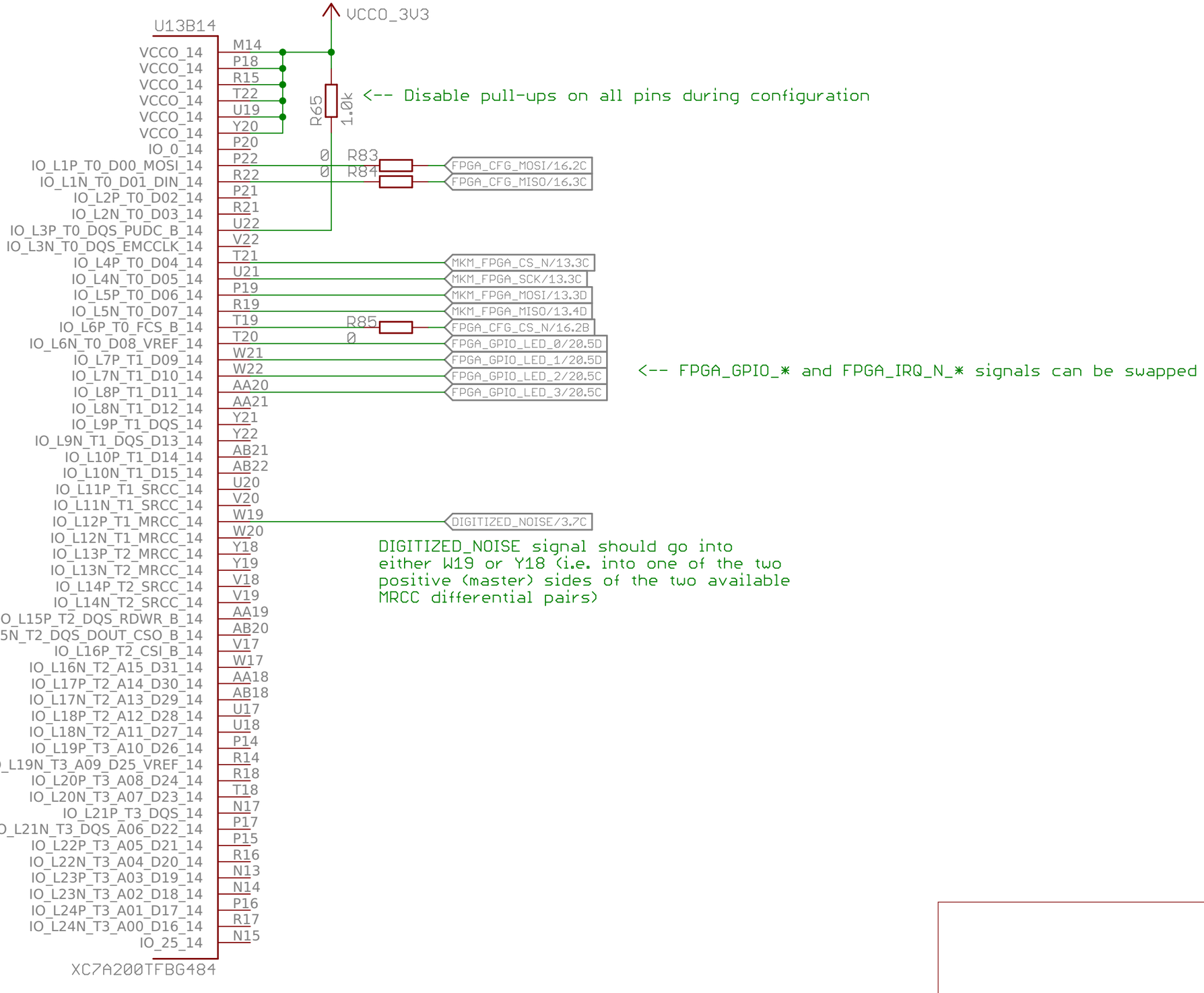




	FPGA GPIO
	rev02
	9 Feb 2016 20:38:51
	Sheet: 20/26

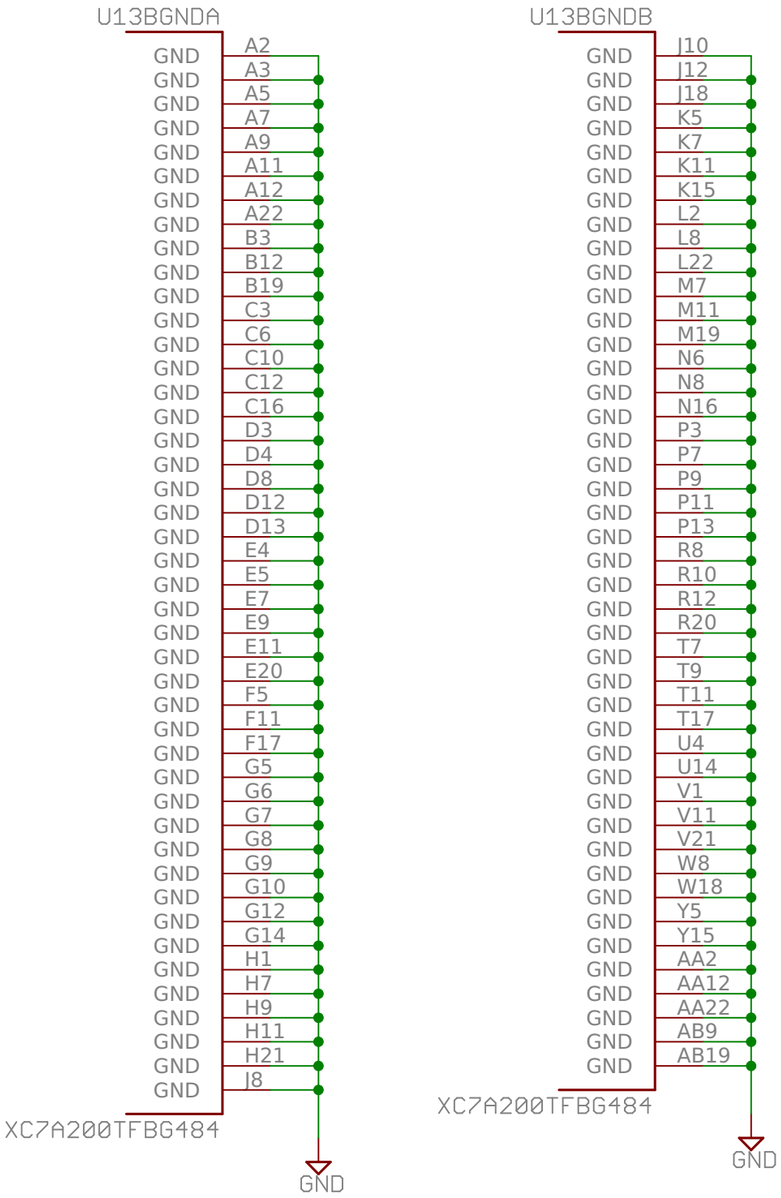
*) Lower Right Bank

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

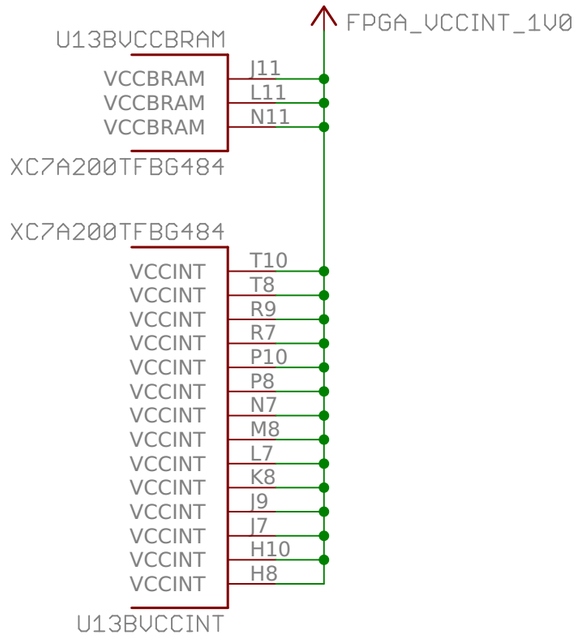


FPGA MKM interface	
rev02	
9 Feb 2016 20:38:51	
Sheet: 21/26	

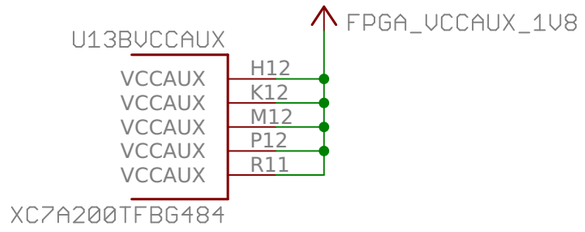
*) Ground Pins



*) Power - CORE & BRAM

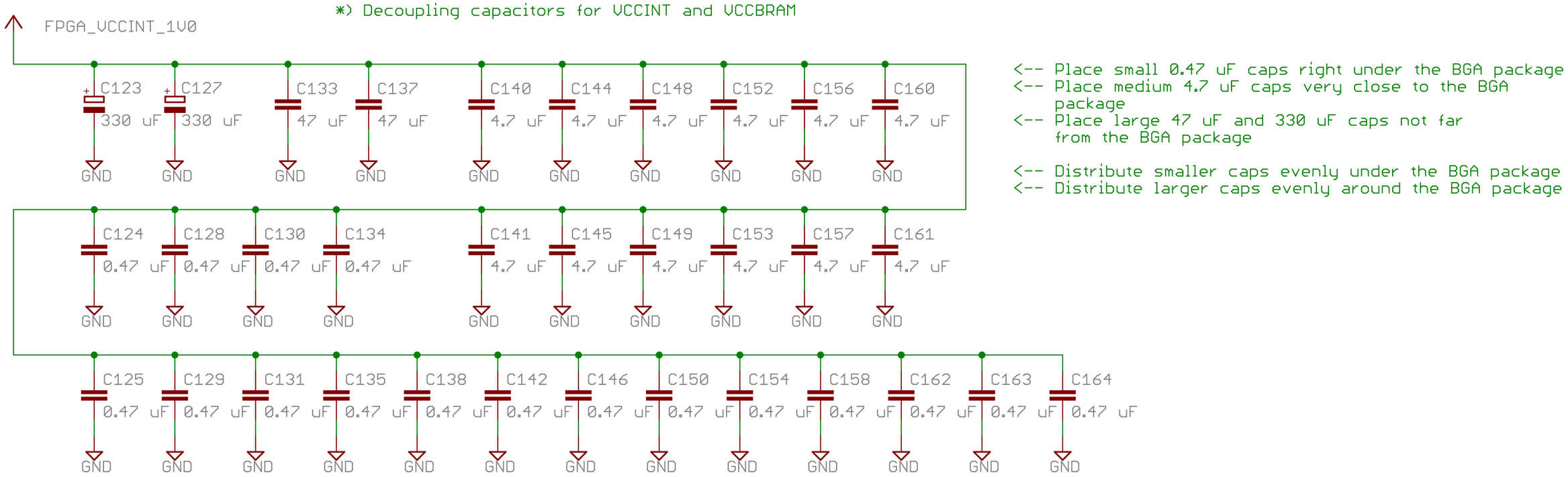


*) Power - AUX



	FPGA power and ground
	rev02
	9 Feb 2016 20:38:51
	Sheet: 22/26

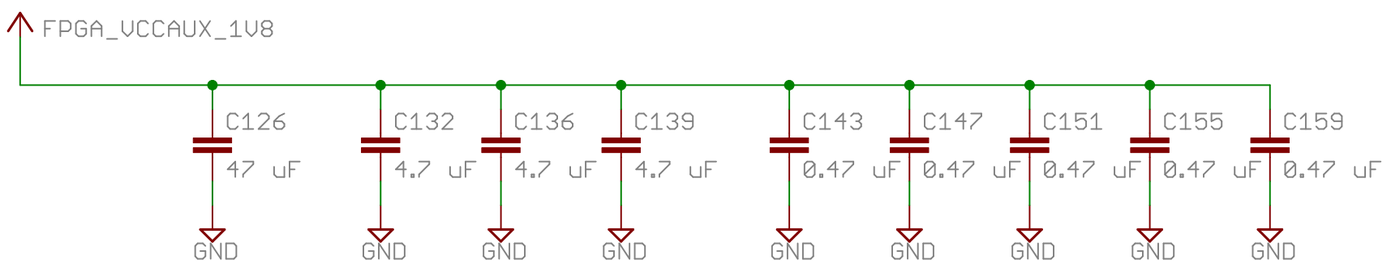
*) Decoupling capacitors for VCCINT and VCCBRAM



<-- 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

*) Decoupling capacitors for VCCAUX

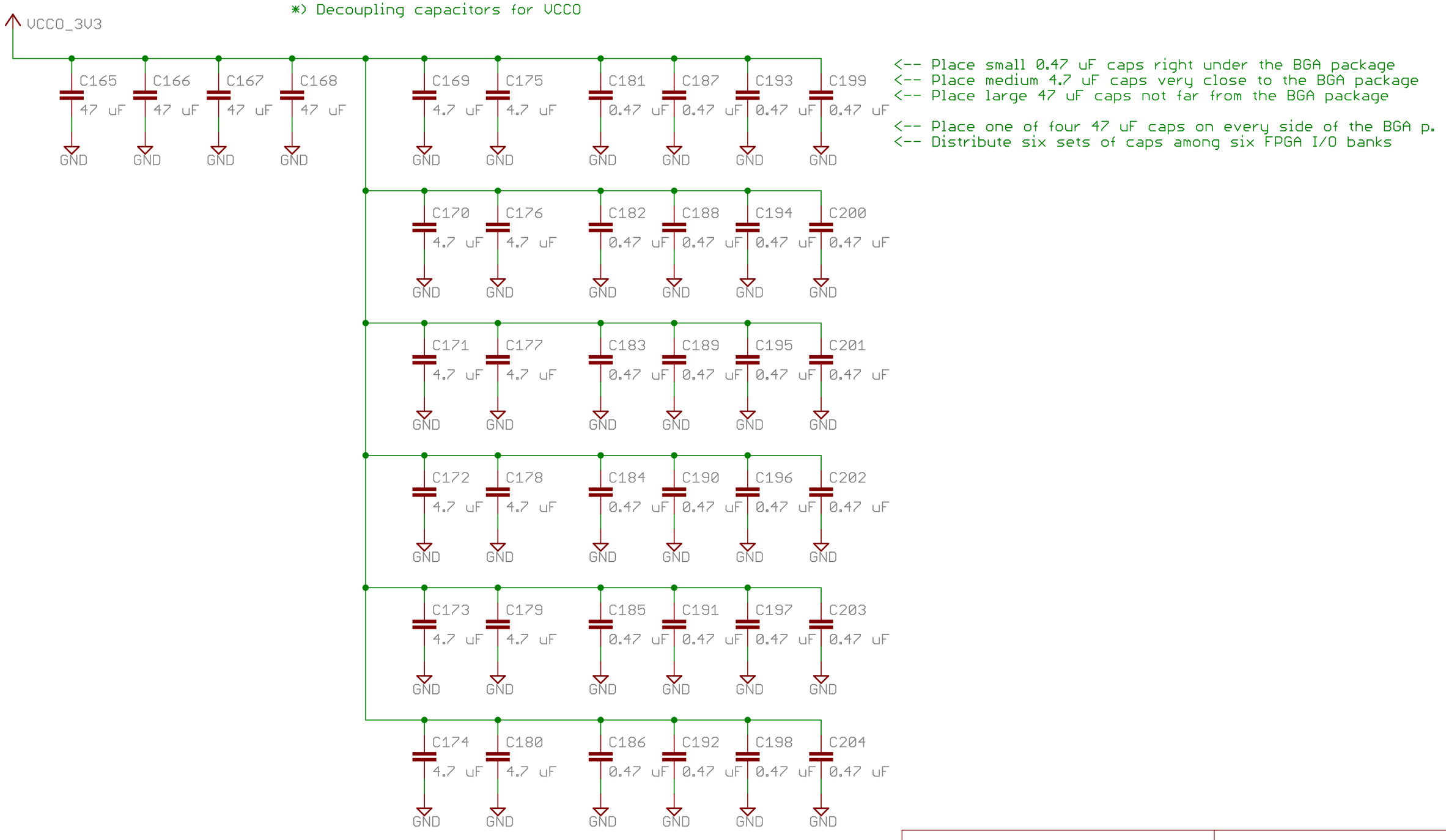


<-- Place small 0.47 uF caps right under the BGA package
<-- Place medium 4.7 uF caps very close to the BGA package
<-- Place large 47 uF caps not far from the BGA package

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

FPGA CORE and AUX capacitors
rev02
9 Feb 2016 20:38:51
Sheet: 23/26

*) Decoupling capacitors for VCCO



<-- 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 p.
<-- Distribute six sets of caps among six FPGA I/O banks

FPGA VCCO bypass capacitors

rev02

9 Feb 2016 20:38:51

Sheet: 24/26

*) FPGA Power Subsystem -- CORE

*) VCCINT = 0.6V x (1 + 150 / 226) = 0.998V

*) OCP_ADJ is not used (default over-current threshold)

*) MARx are not used (output at nominal 100%)

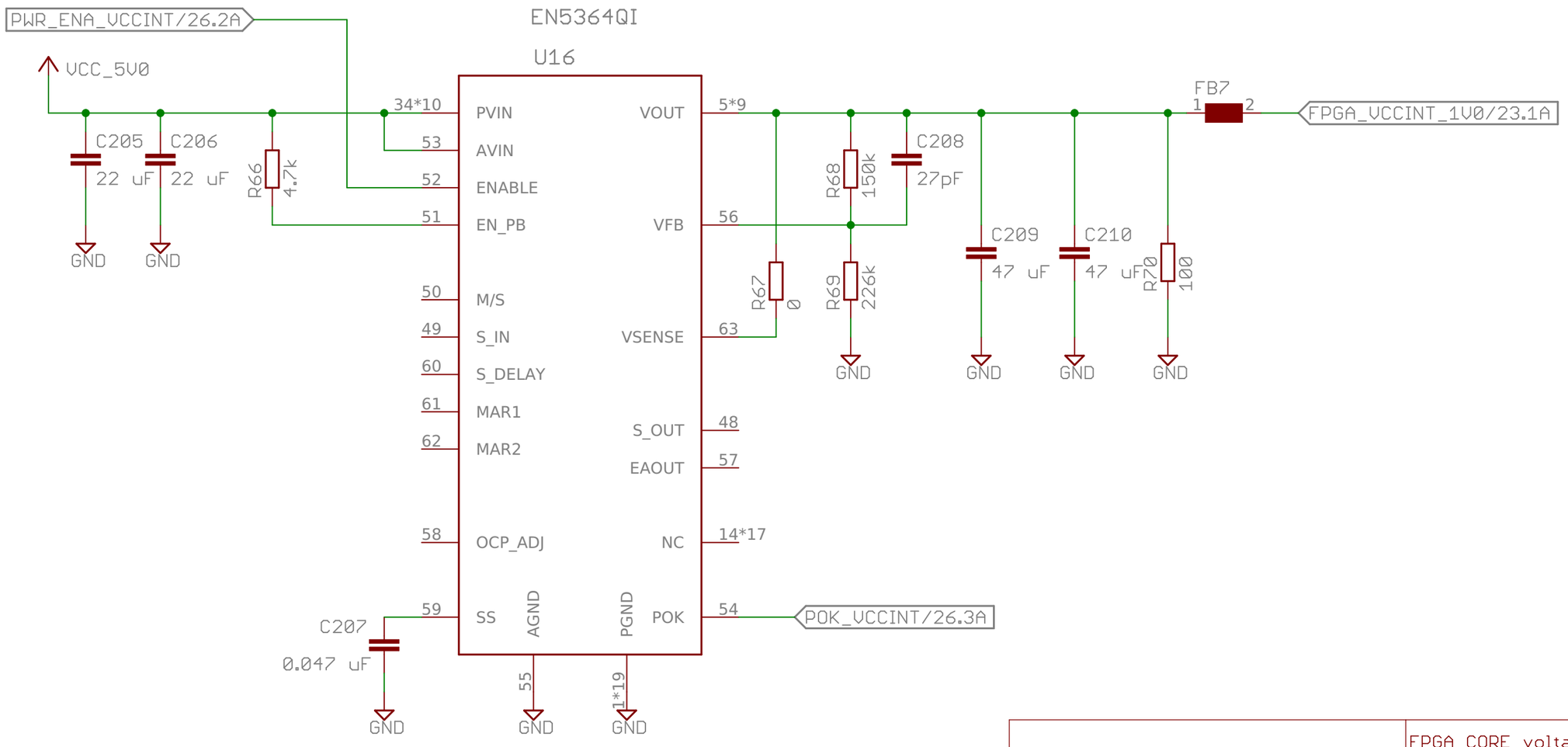
*) S_IN/S_OUT are not used (single regulator mode)

*) S_DELAY is not used (single regulator mode)

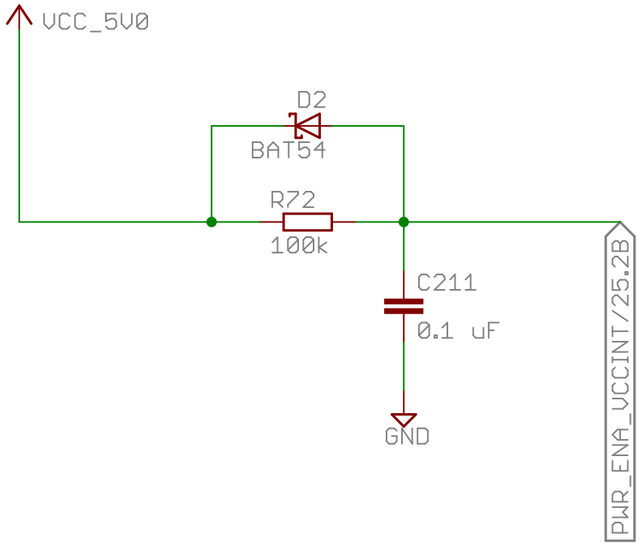
*) M/S is not used (parallel operation not needed)

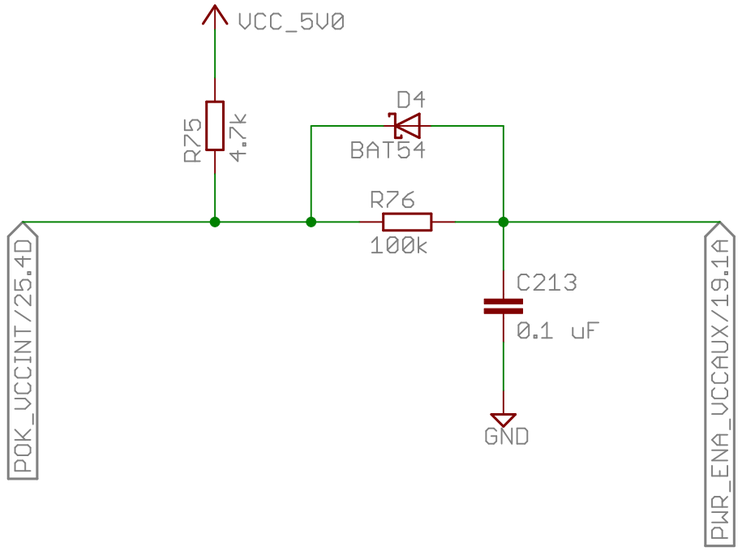
*) EA_OUT is not used (default control loop)

*) Minimal load current is 0A, but we still place load of 100 Ohms just in case (gives 10 mA)



	FPGA CORE voltage regulators
	rev02
	9 Feb 2016 20:38:51
	Sheet: 25/26





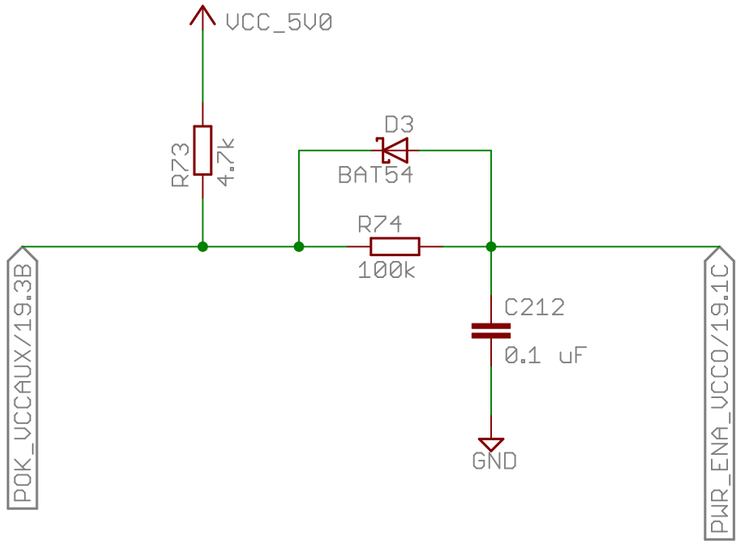
*) Recommended power-up sequence:

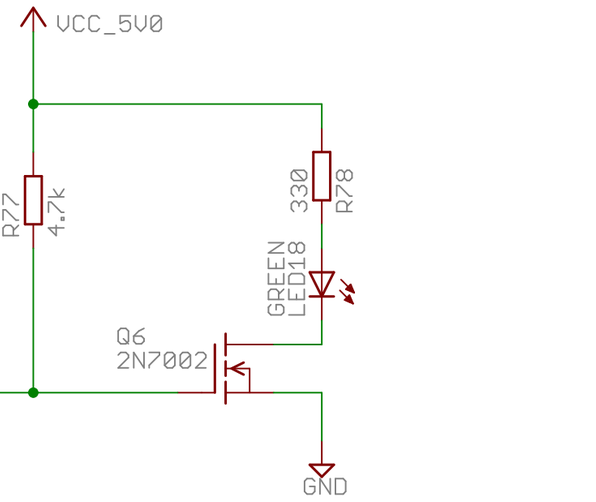
1) VCCINT

2) VCCAUX

3) VCCO

RC network values are preliminary,
should be tweaked after experiments





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

	FPGA power sequencing
	rev02
	9 Feb 2016 20:38:51
	Sheet: 26/26