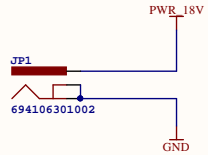


This document contains the electrical schematics for the Cryptech Alpha board.
The latest version of these schematics can be found here:
<https://wiki.cryptech.is/browser/hardware/eagle/alpha>
For more information about the Alpha board including functionality, goals
and block diagram, please see:
<https://wiki.cryptech.is/wiki/AlphaBoardStrategy>
For more information about the Cryptech project, please see:
<https://cryptech.is/>



Title		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_0.SchDoc	Drawn By:

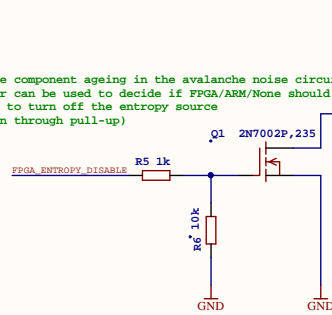
Main power input
18V DC



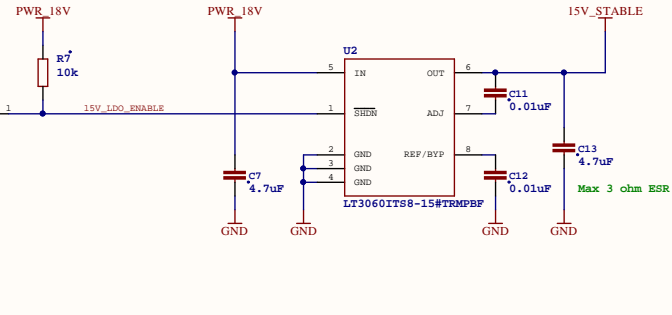
XXX verify symbol

Entropy source power

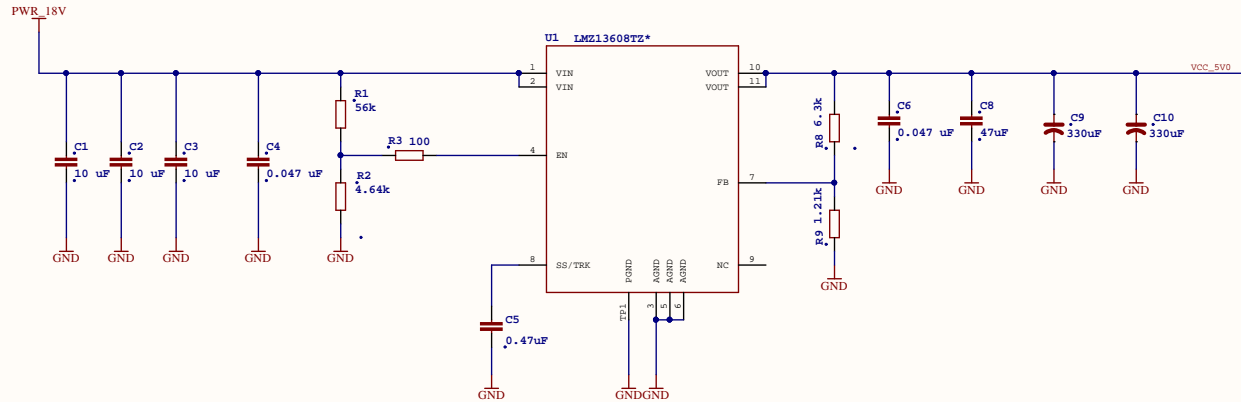
To mitigate component ageing in the avalanche noise circuit, this jumper can be used to decide if FPGA/ARM/None should be allowed to turn off the entropy source (default On through pull-up)



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



*) Intermediate Regulator: 18V -> 5V

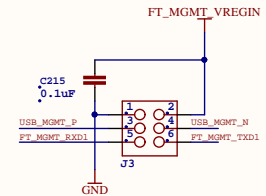
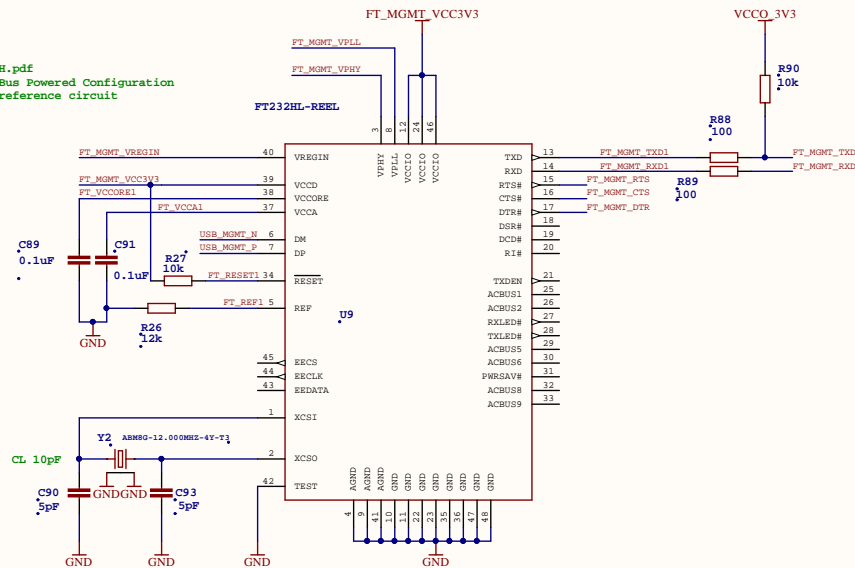
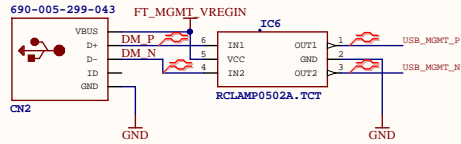


*) $VCC_5V0 = 0.8V \times (1 + 6.3/1.21) = 4.965V$
 *) Current sharing not used
 *) SYNC is not used

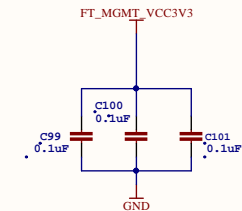
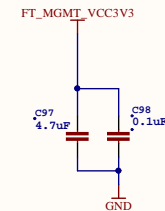
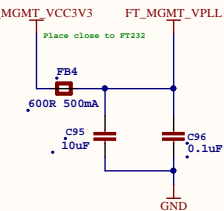
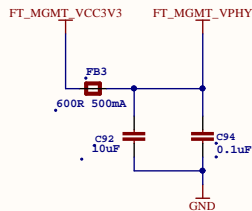
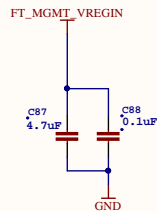
Title		
Input power		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_1.SchDoc	Drawn By:

Management access USB UART

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



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

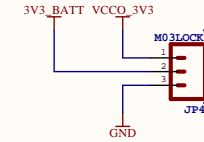


Title		
MGMT USB-UART		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_10.SchDoc	Drawn By:

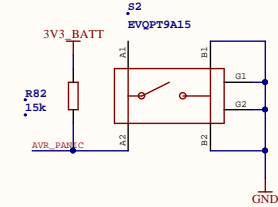
AVR Tiny Tamper Detect MCU



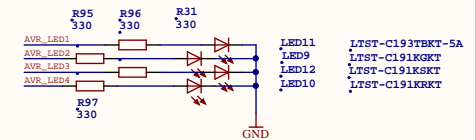
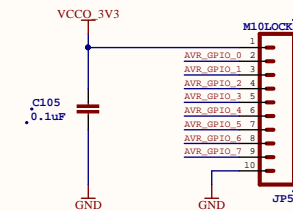
Connector for external 3V3 battery.
Place a jumper between pins 1-2
to "emulate" having a battery present.



Panic button

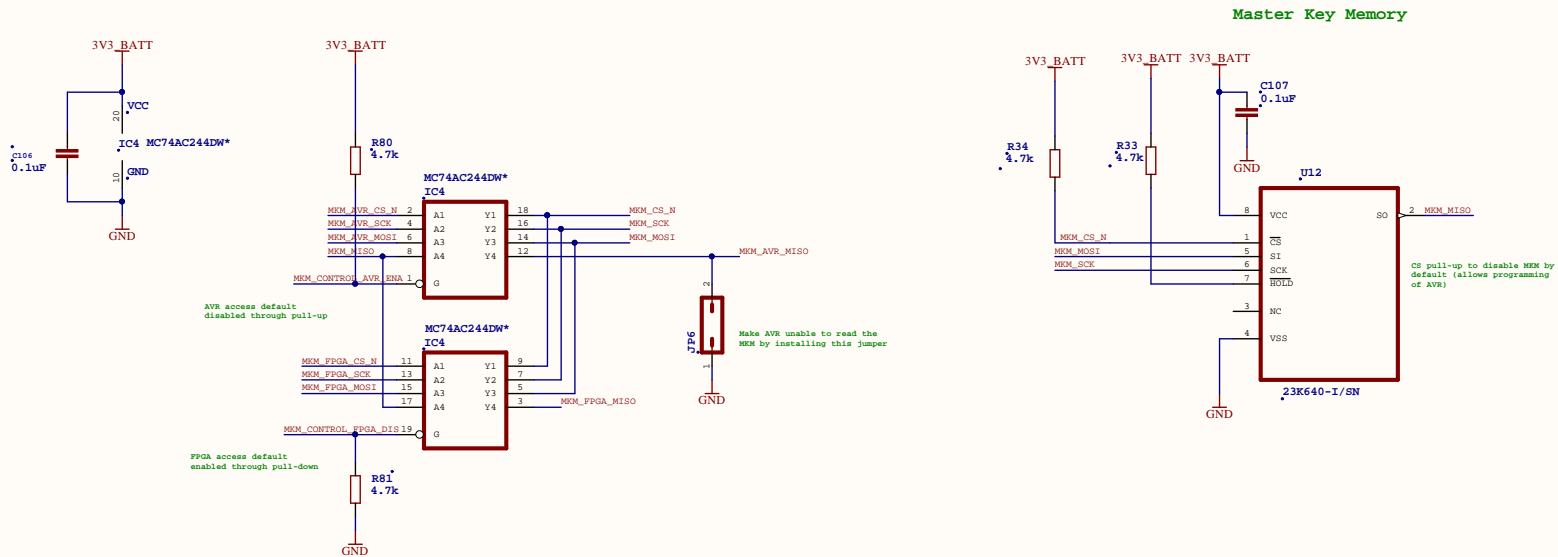


Expansion GPIO



Title		
AVR Tamper circuit		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_11.SchDoc	Drawn By:

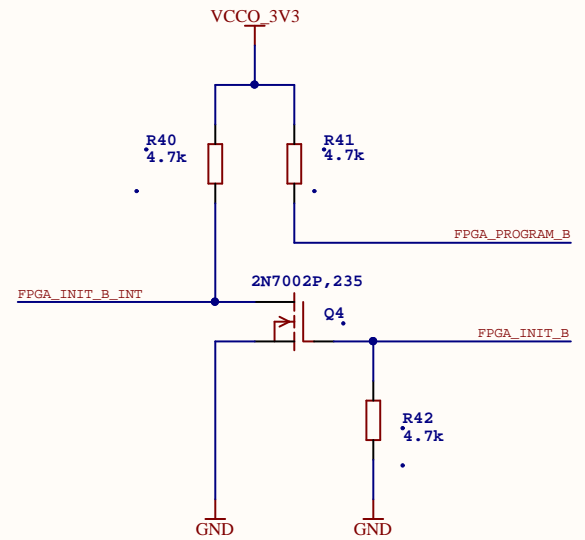
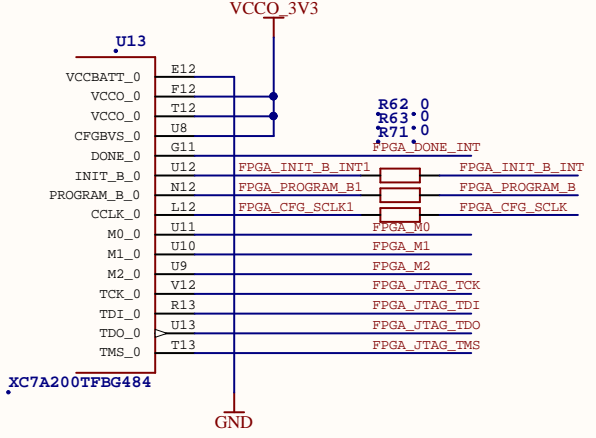
SPI mux controlling access to the MKM.
 Normally, the FPGA has R/W access to the MKM but on a
 tamper event the tamper detect MCU (AVR) will grab access
 to the MKM and erase the contents.



Title		
Master Key Memory		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_12.SchDoc	Drawn By:

A

*) Configuration Interface

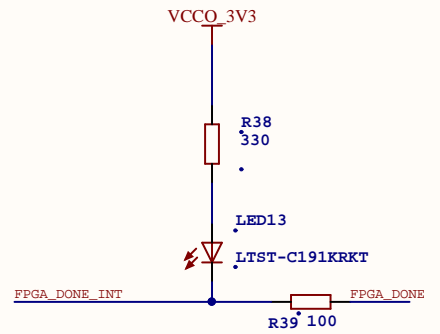
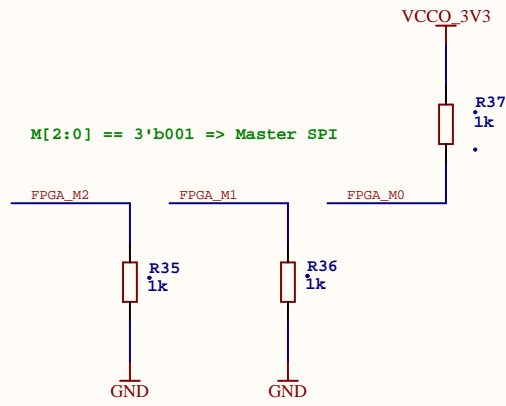


B

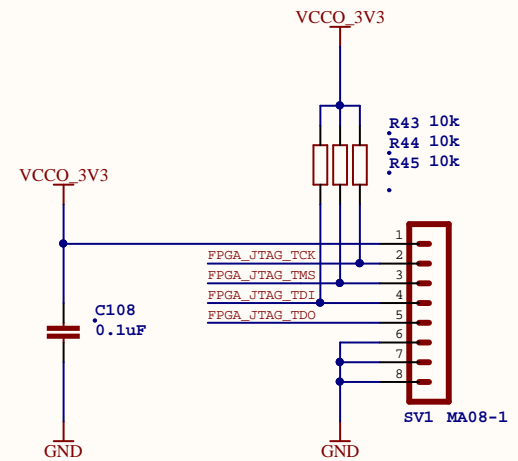
A

B

- *) 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



C

C

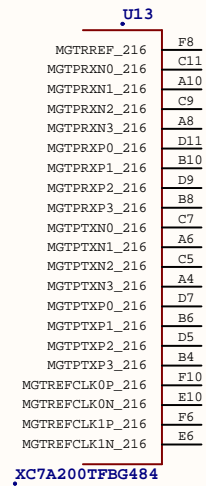
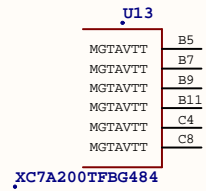
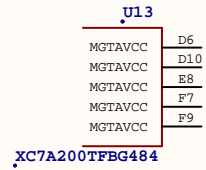
D

D

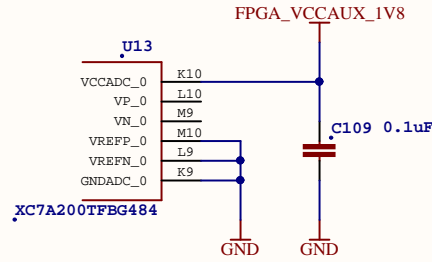
Title		
FPGA configuration interface		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_13.SchDoc	Drawn By:

A

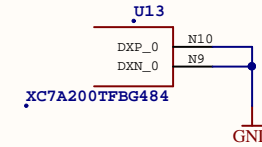
*) Transceivers [NOT USED]



*) XADC [NOT USED]



*) Temperature Sensor [NOT USED]



B

B

C

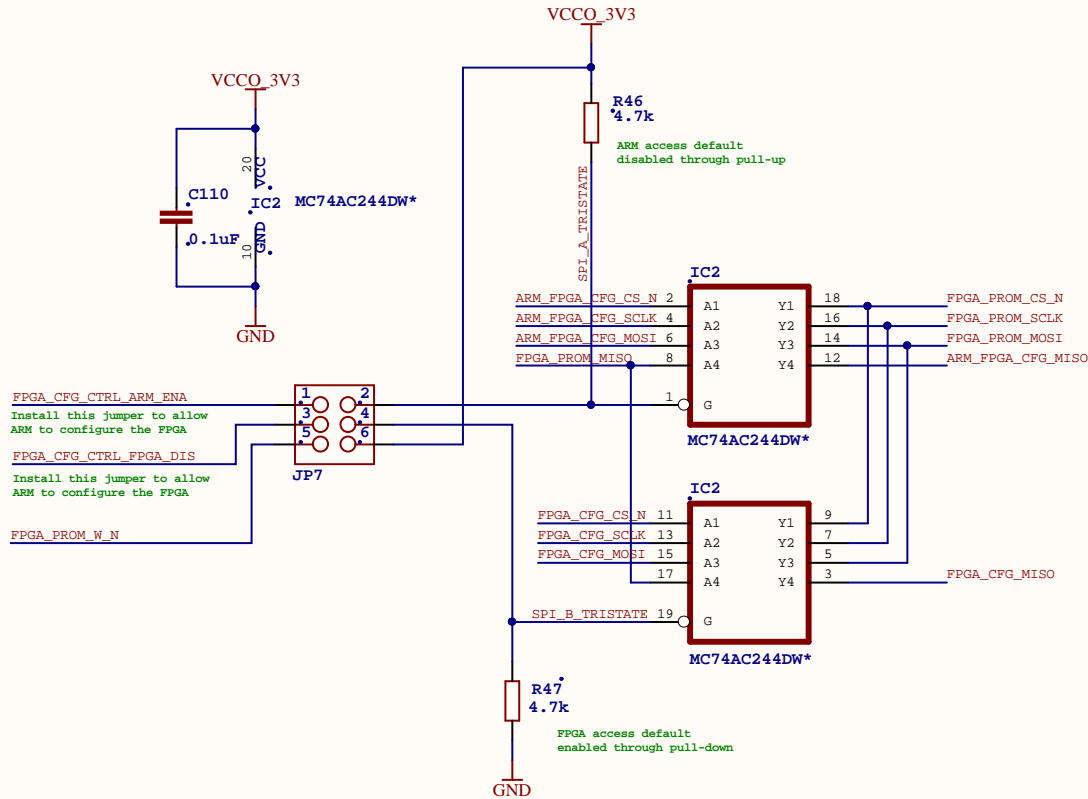
C

D

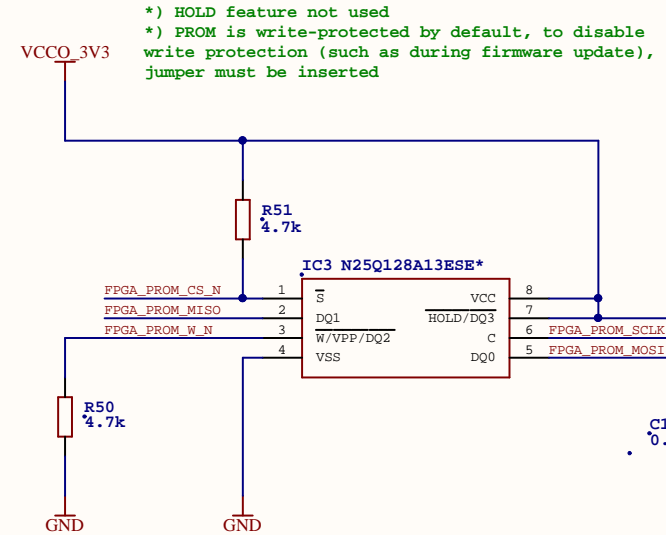
D

Title		
FPGA unused		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_14.SchDoc	Drawn By:

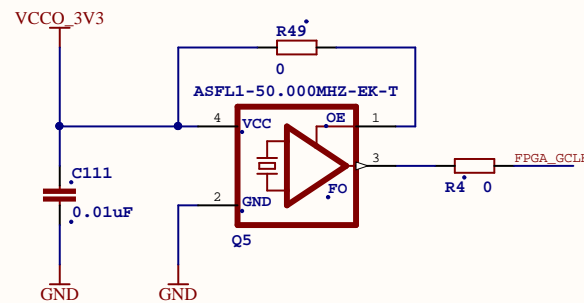
SPI mux to let ARM override access to
FPGA config memory (to reprogram FPGA)



FPGA config memory, 128 Mbit



FPGA clock



Title		
FPGA supporting components		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_15.SchDoc	Drawn By:

A

A

B

B

C

C

D

D

***) Middle Right Bank**

VCCO_3V3

U13

- VCCO_15 G19
- VCCO_15 H16
- VCCO_15 J13
- VCCO_15 K20
- VCCO_15 L17
- VCCO_15 N21
- VCCO_15 J16

***) Completely unused banks still must be powered**

- IO_0_15 H13
- IO_L1P_T0_AD0P_15 G13
- IO_L1N_T0_AD0N_15 G15
- IO_L2P_T0_AD8P_15 G16
- IO_L2N_T0_AD8N_15 J14
- IO_L3P_T0_DQS_AD1P_15 H14
- IO_L3N_T0_DQS_AD1N_15 G17
- IO_L4P_T0_15 G18
- IO_L4N_T0_15 J15
- IO_L5P_T0_AD9P_15 H15
- IO_L5N_T0_AD9N_15 H17
- IO_L6P_T0_15 H18
- IO_L6N_T0_VREF_15 J22
- IO_L7P_T1_AD2P_15 H22
- IO_L7N_T1_AD2N_15 H20
- IO_L8P_T1_AD10P_15 G20
- IO_L8N_T1_AD10N_15 K21
- IO_L9P_T1_DQS_AD3P_15 K22
- IO_L9N_T1_DQS_AD3N_15 M21
- IO_L10P_T1_AD11P_15 L21
- IO_L10N_T1_AD11N_15 J20
- IO_L11P_T1_SRCC_15 J21
- IO_L11N_T1_SRCC_15 J19
- IO_L12P_T1_MRCC_15 H19
- IO_L12N_T1_MRCC_15 K18
- IO_L13P_T2_MRCC_15 K19
- IO_L13N_T2_MRCC_15 L19
- IO_L14P_T2_SRCC_15 L20
- IO_L14N_T2_SRCC_15 N22
- IO_L15P_T2_DQS_15 M22
- IO_L15N_T2_DQS_ADV_B_15 M18
- IO_L16P_T2_A28_15 L18
- IO_L16N_T2_A27_15 N18
- IO_L17P_T2_A26_15 N19
- IO_L17N_T2_A25_15 N20
- IO_L18P_T2_A24_15 M20
- IO_L18N_T2_A23_15 K13
- IO_L19P_T3_A22_15 K14
- IO_L19N_T3_A21_VREF_15 M13
- IO_L20P_T3_A20_15 L13
- IO_L20N_T3_A19_15 K17
- IO_L21P_T3_DQS_15 J17
- IO_L21N_T3_DQS_A18_15 L14
- IO_L22P_T3_A17_15 L15
- IO_L22N_T3_A16_15 L16
- IO_L23P_T3_FOE_B_15 K16
- IO_L23N_T3_FWE_B_15 M15
- IO_L24P_T3_RS1_15 M16
- IO_L24N_T3_RS0_15 M17
- IO_25_15

XC7A200TFBG484

***) Upper Left Bank**

VCCO_3V3

U13

- VCCO_35 C1
- VCCO_35 F2
- VCCO_35 H6
- VCCO_35 J3
- VCCO_35 M4
- VCCO_35 N1
- VCCO_35 F4
- IO_0_35 B1

***) Completely unused banks still must be powered**

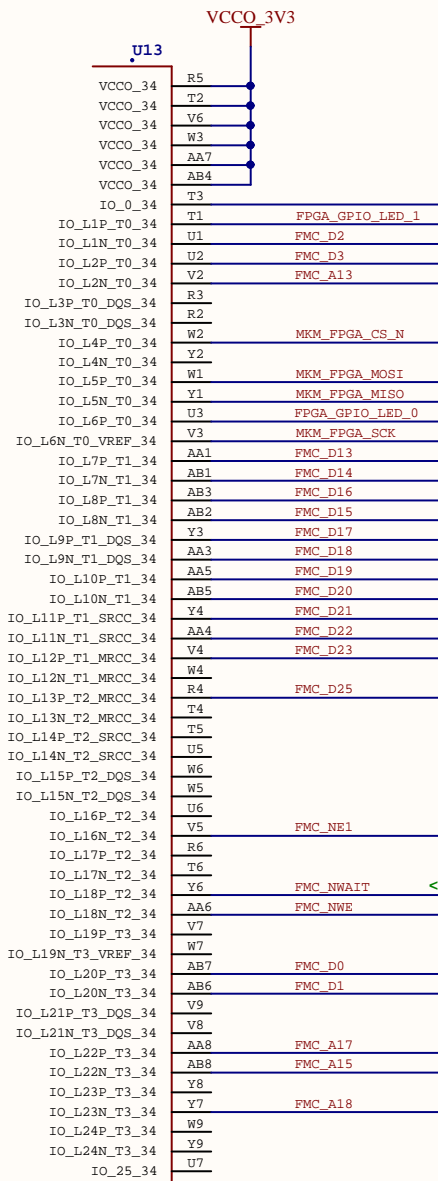
- IO_L1P_T0_AD4P_35 A1
- IO_L1N_T0_AD4N_35 C2
- IO_L2P_T0_AD12P_35 B2
- IO_L2N_T0_AD12N_35 E1
- IO_L3P_T0_DQS_AD5P_35 D1
- IO_L3N_T0_DQS_AD5N_35 E2
- IO_L4P_T0_35 D2
- IO_L4N_T0_35 G1
- IO_L5P_T0_AD13P_35 F1
- IO_L5N_T0_AD13N_35 F3
- IO_L6P_T0_35 E3
- IO_L6N_T0_VREF_35 K1
- IO_L7P_T1_AD6P_35 J1
- IO_L7N_T1_AD6N_35 H2
- IO_L8P_T1_AD14P_35 G2
- IO_L8N_T1_AD14N_35 K2
- IO_L9P_T1_DQS_AD7P_35 J2
- IO_L9N_T1_DQS_AD7N_35 J5
- IO_L10P_T1_AD15P_35 H5
- IO_L10N_T1_AD15N_35 H3
- IO_L11P_T1_SRCC_35 G3
- IO_L11N_T1_SRCC_35 H4
- IO_L12P_T1_MRCC_35 G4
- IO_L12N_T1_MRCC_35 K4
- IO_L13P_T2_MRCC_35 J4
- IO_L13N_T2_MRCC_35 L3
- IO_L14P_T2_SRCC_35 K3
- IO_L14N_T2_SRCC_35 M1
- IO_L15P_T2_DQS_35 L1
- IO_L15N_T2_DQS_35 M3
- IO_L16P_T2_35 M2
- IO_L16N_T2_35 K6
- IO_L17P_T2_35 J6
- IO_L17N_T2_35 L5
- IO_L18P_T2_35 L4
- IO_L18N_T2_35 N4
- IO_L19P_T3_35 N3
- IO_L19N_T3_VREF_35 R1
- IO_L20P_T3_35 P1
- IO_L20N_T3_35 P5
- IO_L21P_T3_DQS_35 P4
- IO_L21N_T3_DQS_35 P2
- IO_L22P_T3_35 N2
- IO_L22N_T3_35 M6
- IO_L23P_T3_35 M5
- IO_L23N_T3_35 P6
- IO_L24P_T3_35 N5
- IO_L24N_T3_35 L6
- IO_25_35

XC7A200TFBG484

Title		
FPGA unused banks		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\..rev02_16.SchDoc	Drawn By:

A

*) Lower Left Bank



FMC_D[0...31]
FMC_D[...] signals can be swapped

<-- FMC_* control signals can be swapped

XC7A200TFBG484

A

B

B

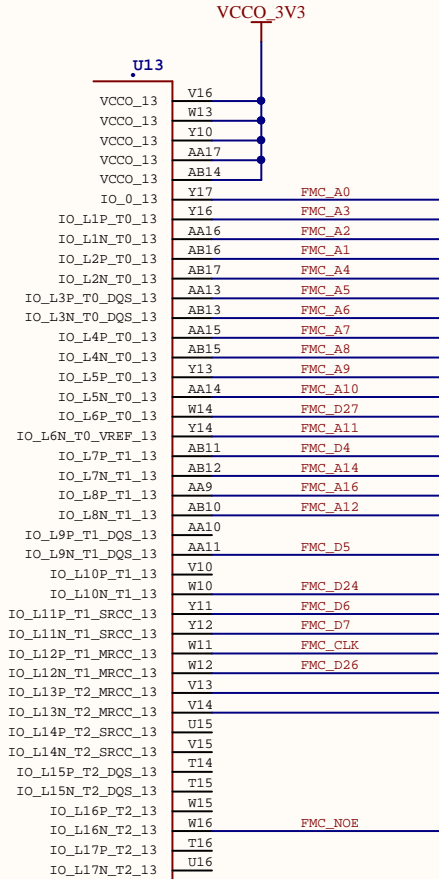
C

C

D

D

*) Bottom Bank



FMC_A[0...25]
FMC_A[...] signals can be swapped

<-- 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)

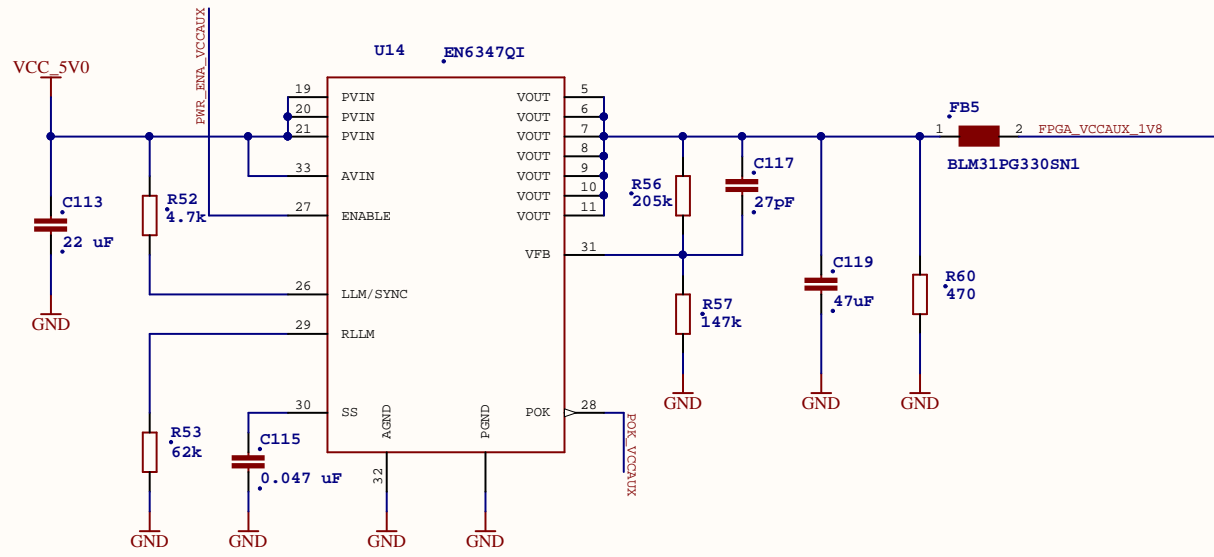
XC7A200TFBG484

Title		
FPGA FMC interface		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\..rev02_17.SchDoc	Drawn By:

A

A

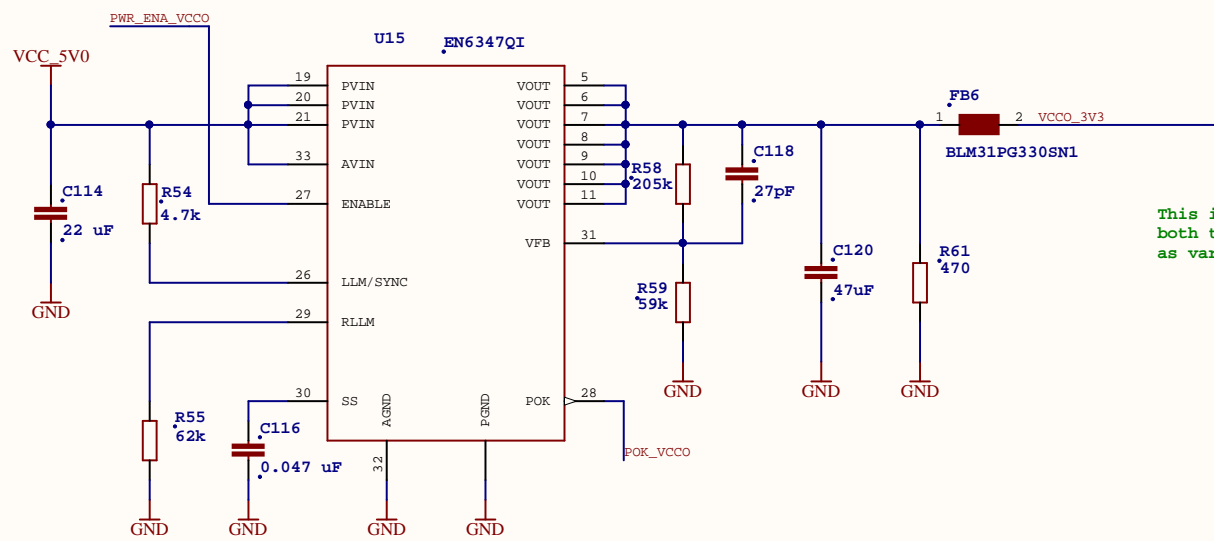
*) FPGA Power Subsystem -- AUX and I/O



*) $VCCAUX = 0.75V \times (1 + 205 / 147) = 1.796V$
 *) $VCCO = 0.75V \times (1 + 205 / 59) = 3.356$
 *) Minimal load current is 2 mA:
 1.8V / 470 Ohm = ~4mA
 3.3V / 470 Ohm = ~7mA
 *) Light-load mode is enabled

B

B



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

C

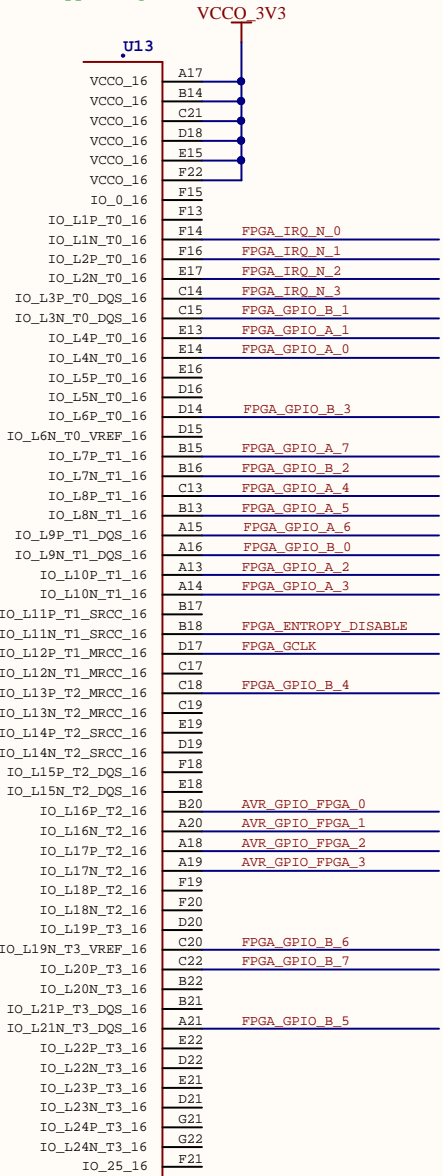
C

D

D

Title		
FPGA voltage regulators		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\..rev02_18.SchDoc	Drawn By:

*) Upper Right Bank

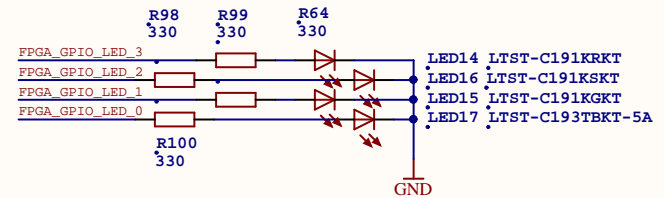
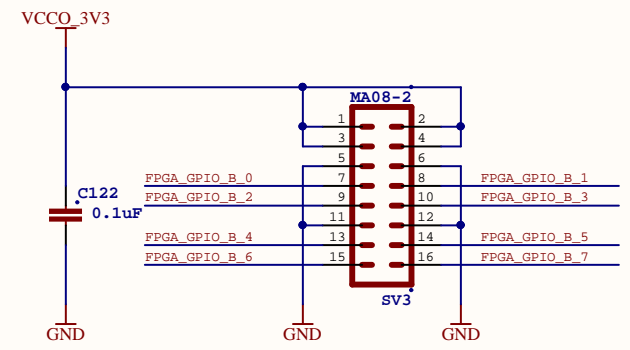
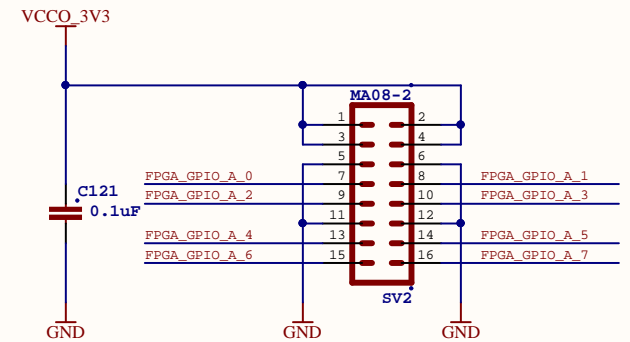


XC7A200TFBG484

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.

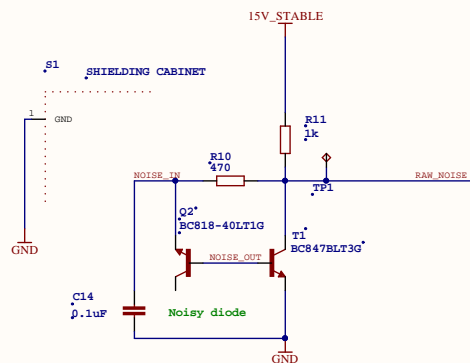
- *) FPGA_GCLK signal **MUST** go into either D17 or C18 (i.e. into one of the two positive (master) sides of the two available MRCC differential pairs)
- *) FPGA_GPIO_* and FPGA_IRQ_N_* signals can be swapped

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



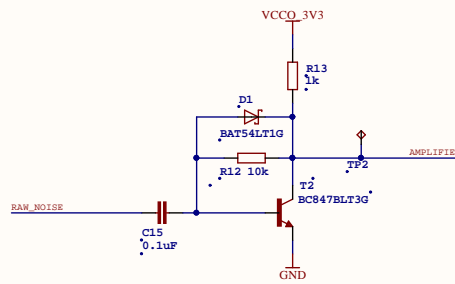
Title			
FPGA GPIO			
Size	Number	Revision	
A4			
Date:	30.05.2016	Sheet of	
File:	C:\SHARE\...\rev02_19.SchDoc	Drawn By:	

Noise generator

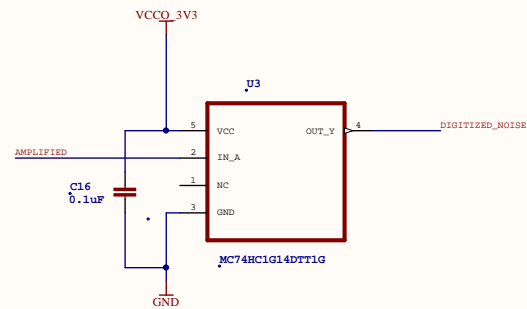


AGND is connected to GND on the board using polygons
(found no other good way) - not visible in schematics.

Amplifier



Digitizer

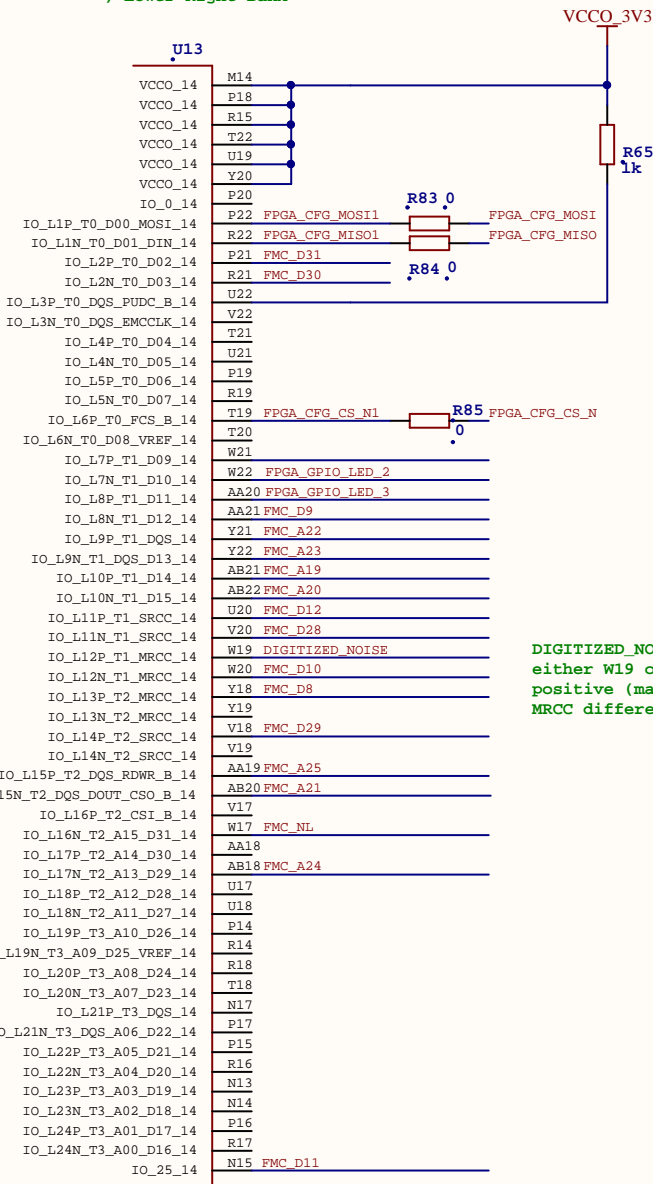


This whole sheets circuitry should be as shielded as possible.
Solid isolated ground plane and internal planes connected
to the rest of the board at a single point is expected.

Title		
Noise source		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_2.SchDoc	Drawn By:

***) 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.



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

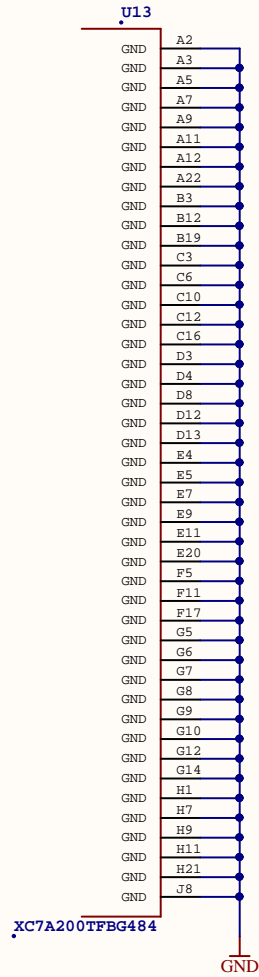
<-- FPGA_GPIO_* and FPGA_IRQ_N_* signals can be swapped

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)

XC7A200TFBG484

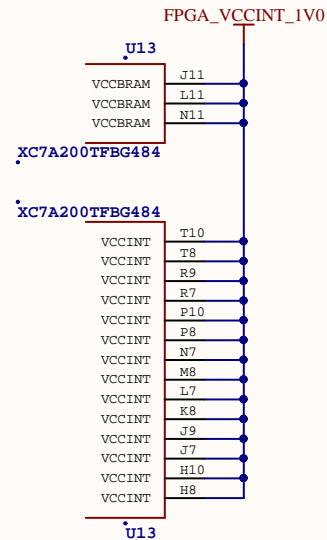
Title			FPGA MKM interface		
Size	Number		Revision		
A4					
Date:	30.05.2016		Sheet of		
File:	C:\SHARE\...\rev02_20.SchDoc		Drawn By:		

*) Ground Pins



XC7A200TFBG484

*) Power - CORE & BRAM

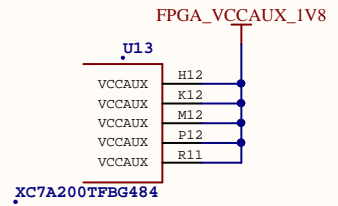


XC7A200TFBG484

XC7A200TFBG484

U13

*) Power - AUX



XC7A200TFBG484

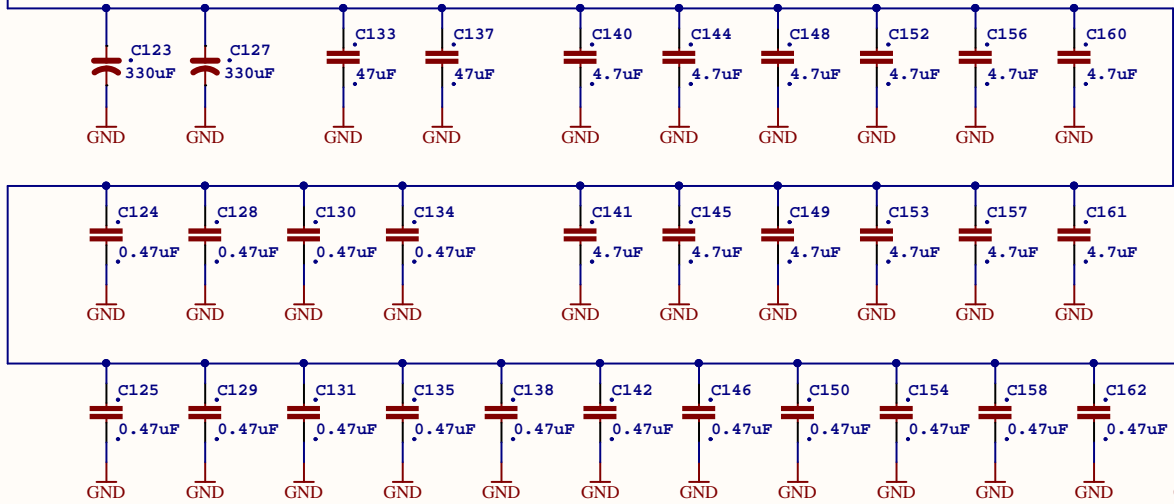
Title		
FPGA power and ground		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_21.SchDoc	Drawn By:

A

A

FPGA_VCCINT_1V0

*) 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

B

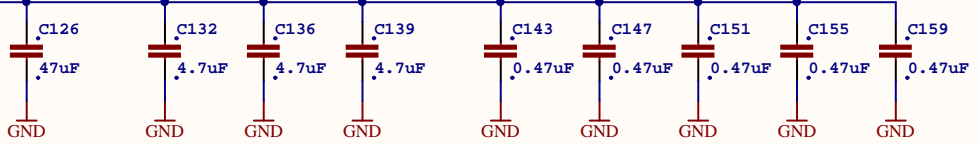
B

C

C

FPGA_VCCAUX_1V8

*) 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

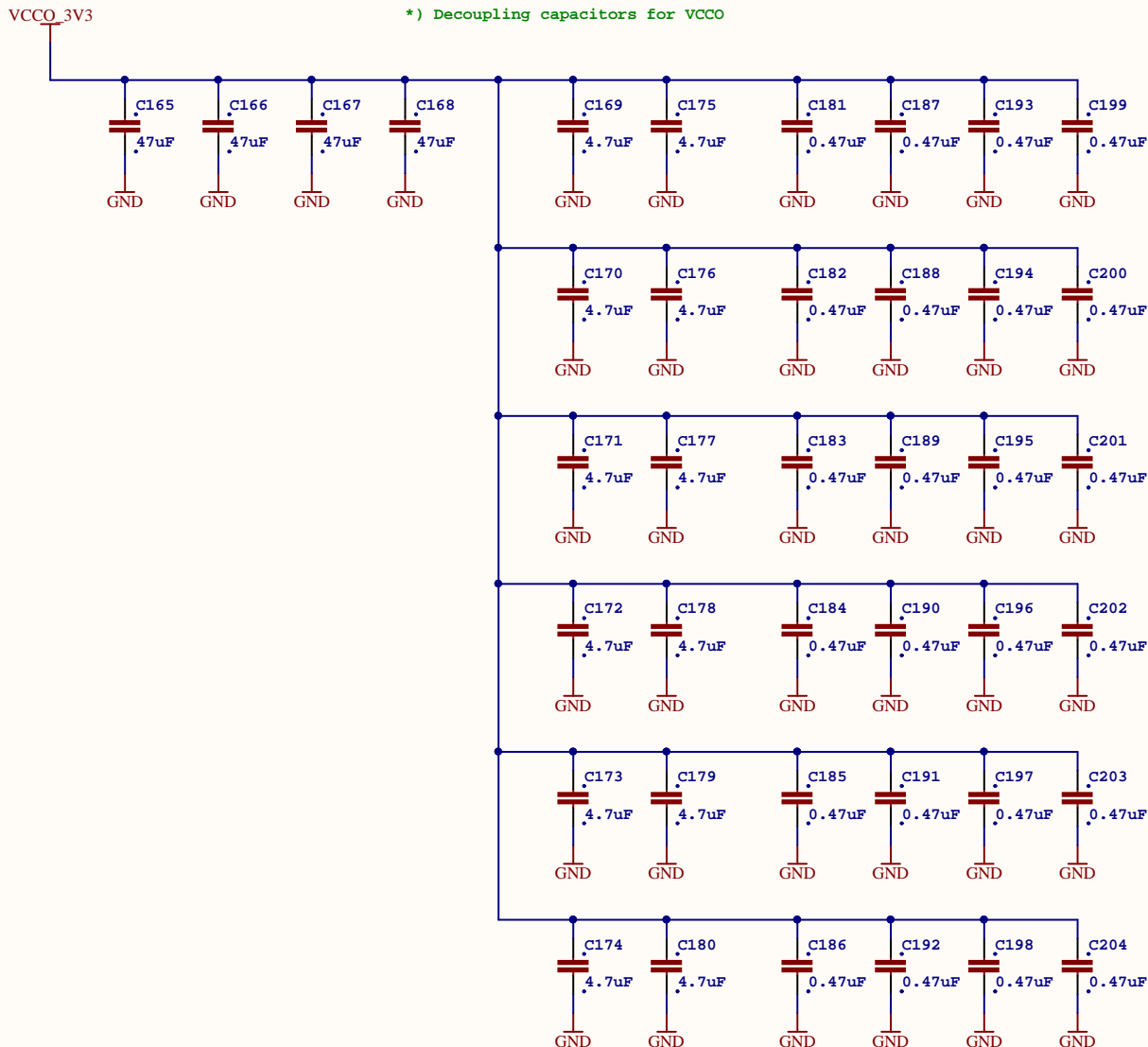
D

D

Title		
FPGA CORE and AUX capacitors		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_22.SchDoc	Drawn By:

A

A



<-- 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

B

B

C

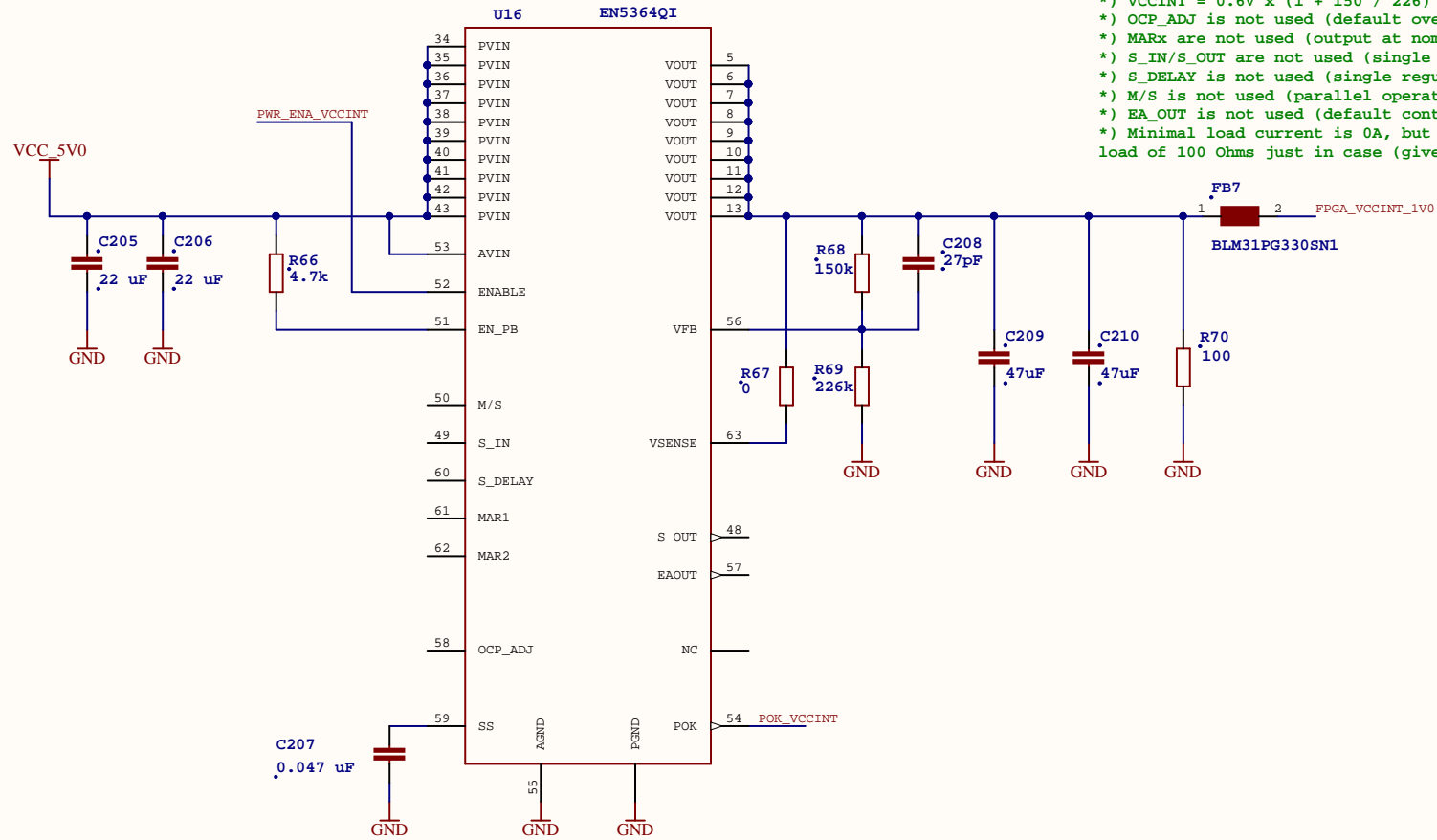
C

D

D

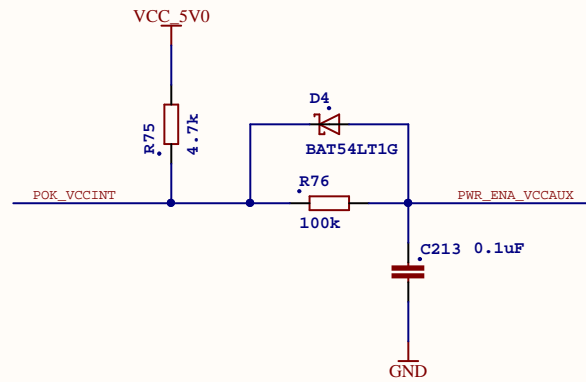
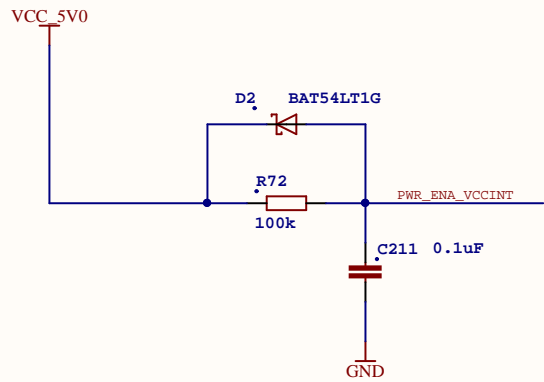
Title		
FPGA VCCO bypass capacitors		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_23.SchDoc	Drawn By:

*) FPGA Power Subsystem -- CORE

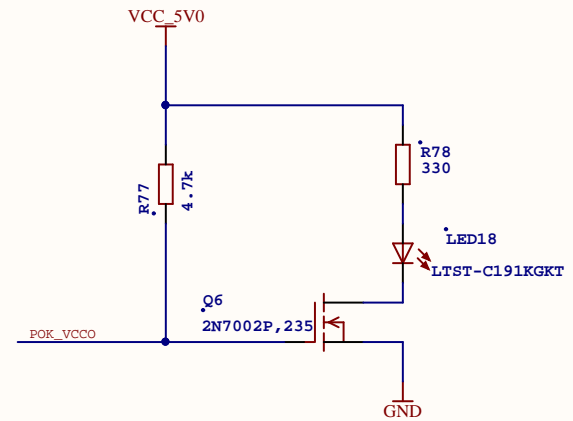
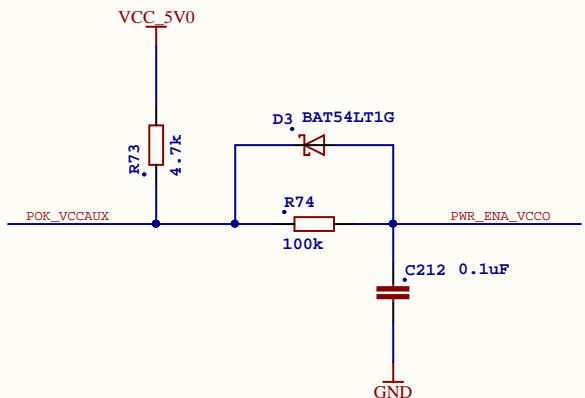


- *) VCCINT = 0.6V x (1 + 150 / 226) = 0.998V
- *) OCP_ADJ is not used (default over-current threshold)
- *) MARx are not used (output at nominal 100%)
- *) S_IN/S_OUT are not used (single regulator mode)
- *) S_DELAY is not used (single regulator mode)
- *) M/S is not used (parallel operation not needed)
- *) 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)

Title		
FPGA CORE voltage regulators		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_24.SchDoc	Drawn By:



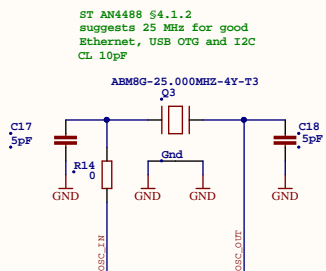
*) Recommended power-up sequence:
 1) VCCINT
 2) VCCAUX
 3) VCCO
 --->
 RC network values are preliminary,
 should be tweaked after experiments



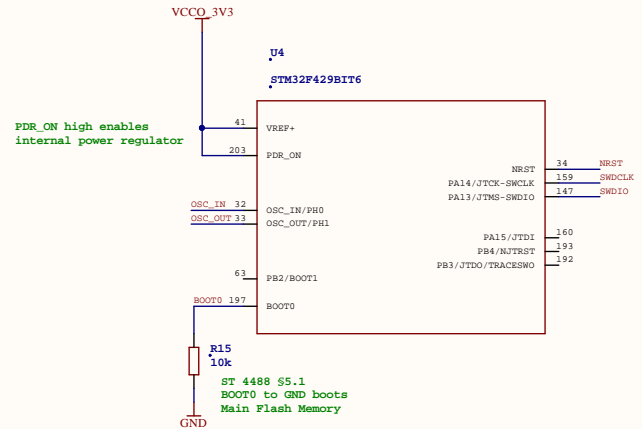
*) "Power OK" LED, should be of green color

Title		
FPGA power sequencing		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_25.SchDoc	Drawn By:

Basic configuration, STM32

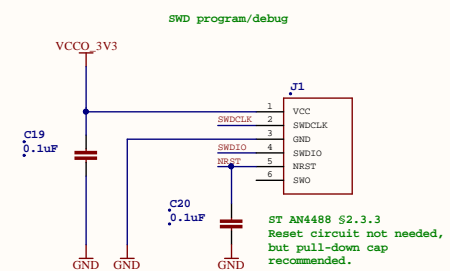


ST AN4488 §4.1.2 suggests 25 MHz for good Ethernet, USB OTG and I2C CL 10pF



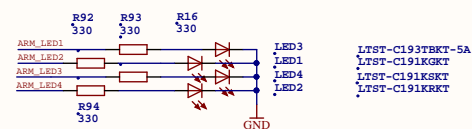
PDR_ON high enables internal power regulator

ST 4488 §5.1 BOOT0 to GND boots Main Flash Memory



SWD program/debug

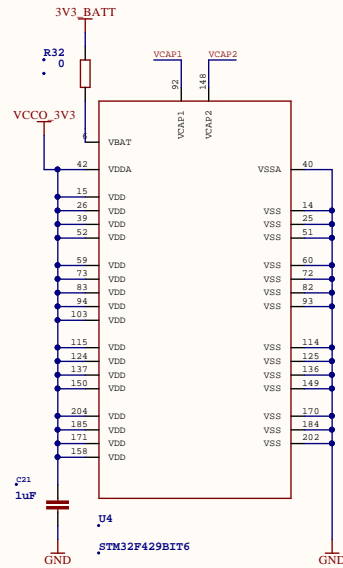
ST AN4488 §2.3.3 Reset circuit not needed, but pull-down cap recommended.



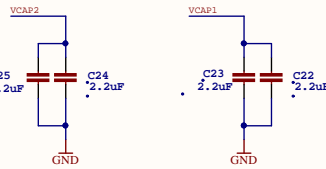
LTST-C193TEKT-5A
LTST-C191KGKT
LTST-C191KSKT
LTST-C191KRKT

Title		
ARM configuration		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_3.SchDoc	Drawn By:

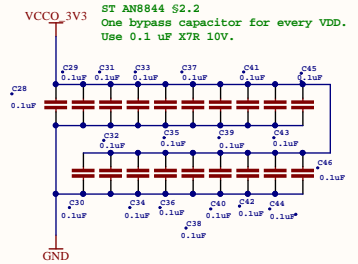
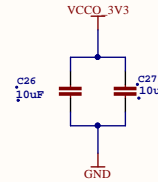
Power and bypass capacitors, STM32



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



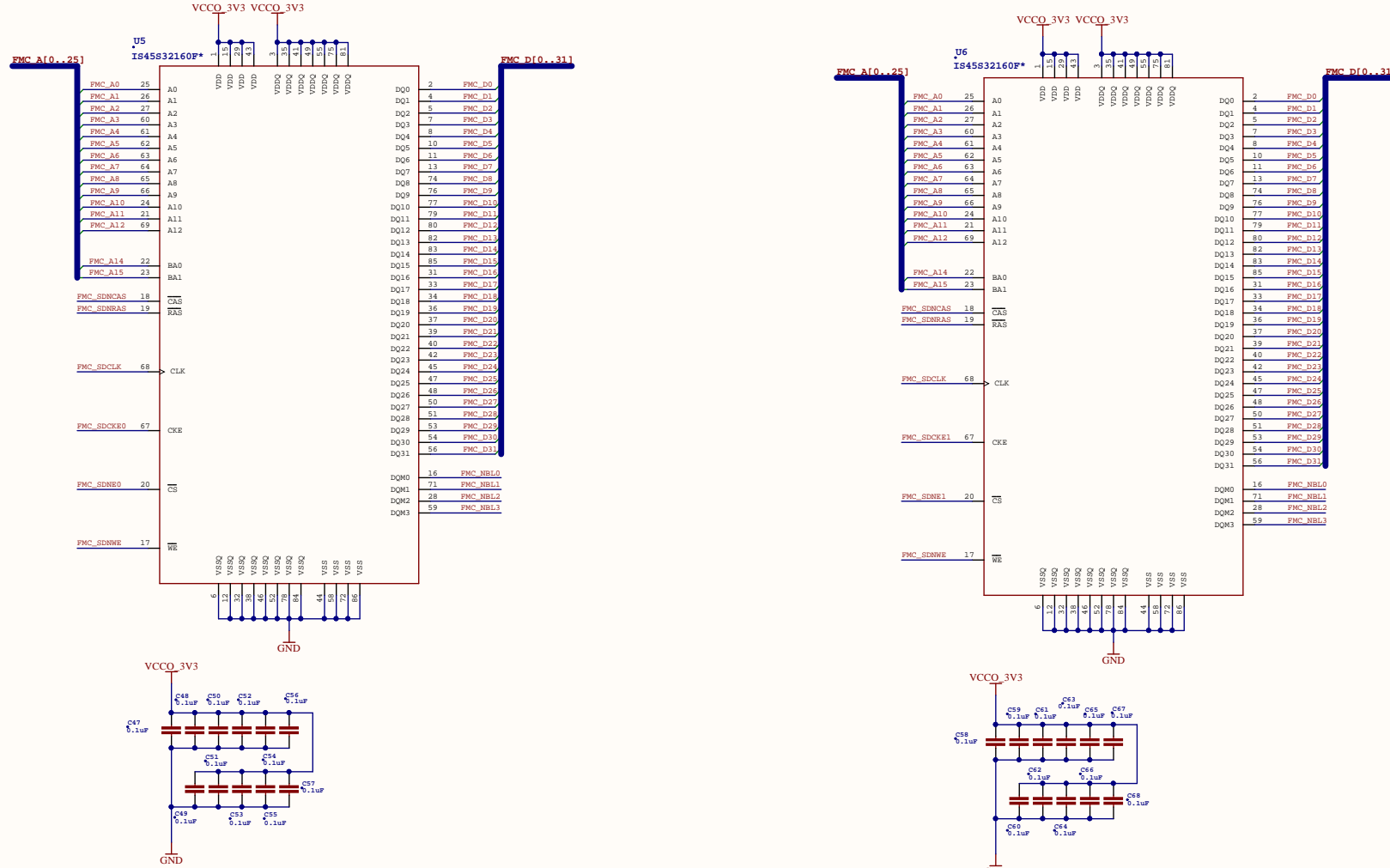
ST AN8844 §2.2
One 10uF bypass cap for the package.
(two used for extra comfort)



Title		
ARM power		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_4.SchDoc	Drawn By:

2x512 Mbit SDRAM memory for the ARM

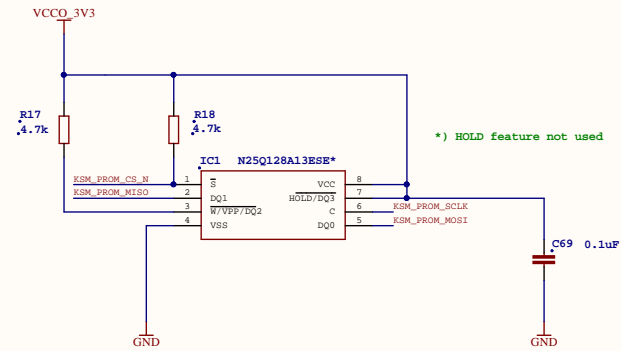
These packages are TSSOP, but if new packages are to be created for layout, BGA package is preferred.



Title		
SDRAM		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_6.SchDoc	Drawn By:

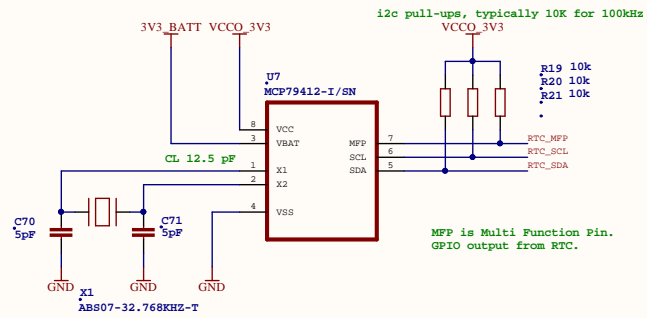
Keystore memory, 128 Mbit

This memory holds cryptographic keys wrapped with the master key.



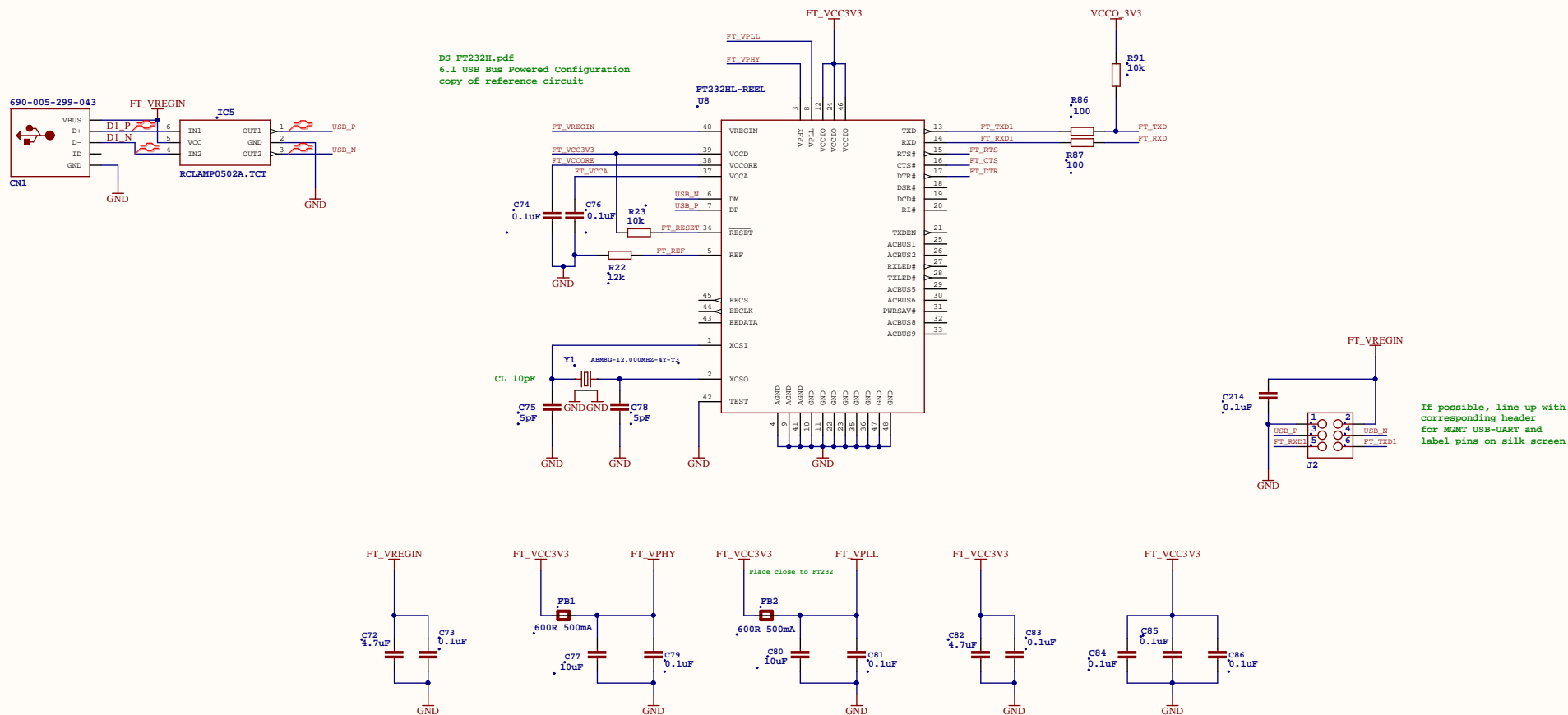
Title		
Keystore memory		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_7.SchDoc	Drawn By:

Real Time Clock



Title		
Real Time Clock		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_8.SchDoc	Drawn By:

Application access USB UART



Title		
USB-UART interface		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...rev02_9.SchDoc	Drawn By: