

A

A

B

B

C

C

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/>



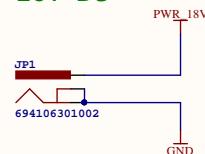
Title		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_0.SchDoc	Drawn By:

A

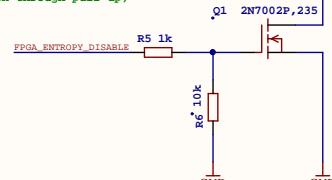
A

### Entropy source power

#### Main power input 18V DC

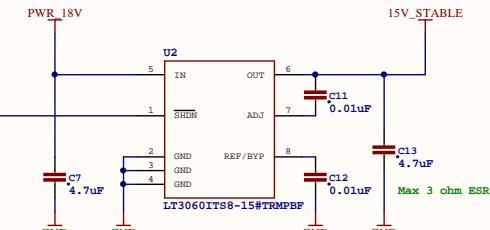


To mitigate component ageing in the avalanche noise circuit, this jumper can be used to decide if FPGA/ARM/None should be allowed to turn off the entropy source (default On through pull-up)



XXX verify symbol

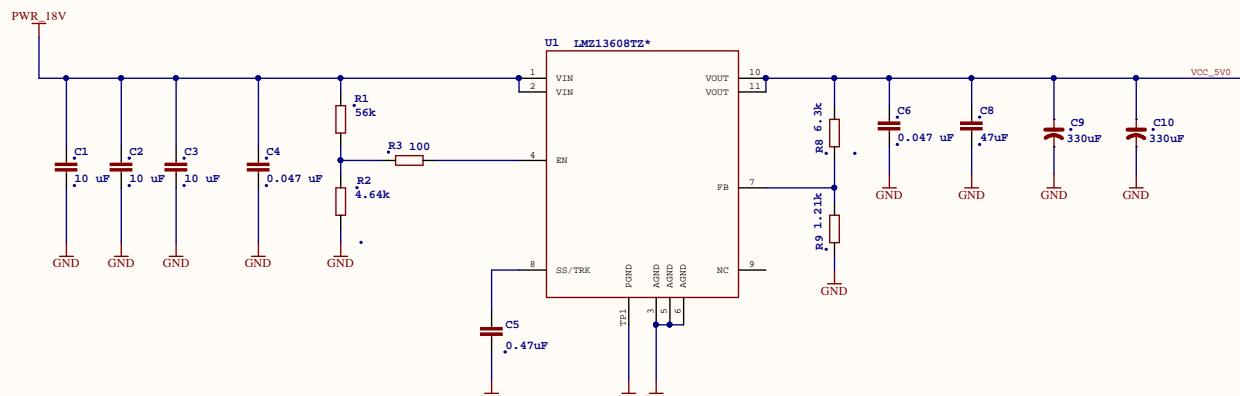
15V LDO powered from external 18V and supplying stable 15V to noise source



B

B

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



\*)  $VCC\_5V0 = 0.8V \times (1 + 6.3/1.21) = 4.965V$   
 \*) Current sharing not used  
 \*) SYNC is not used

C

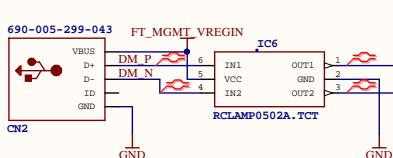
C

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

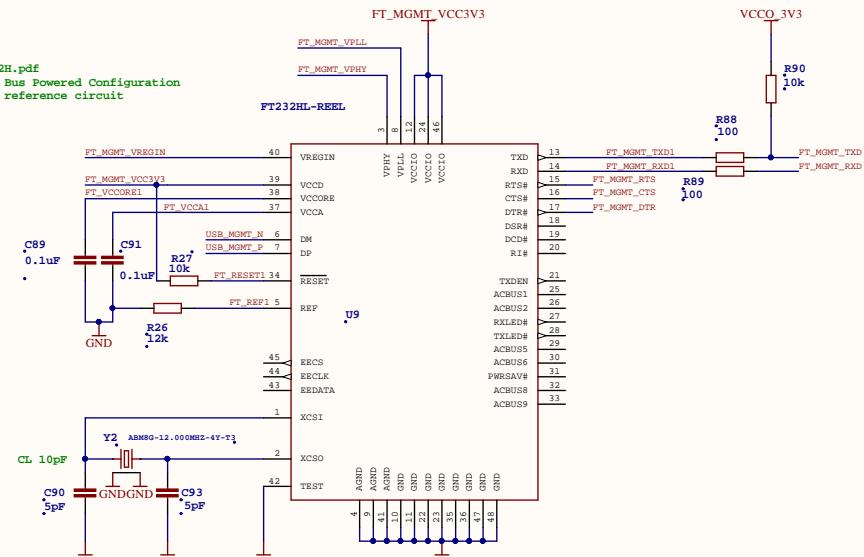
A

1

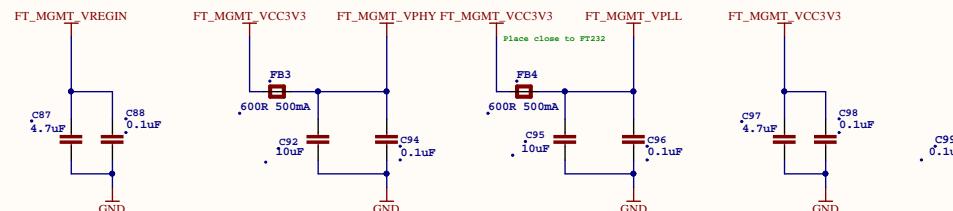
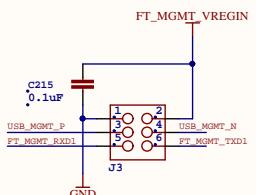
### Management access USB UART



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



D

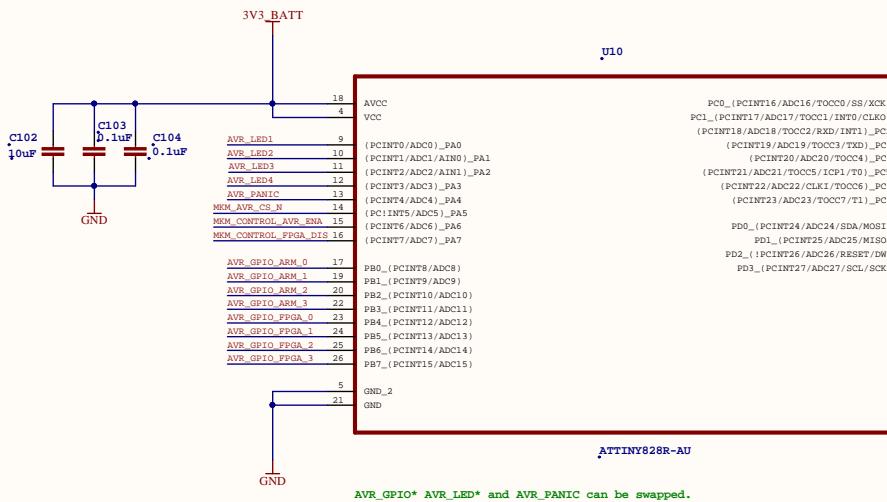
1

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

A

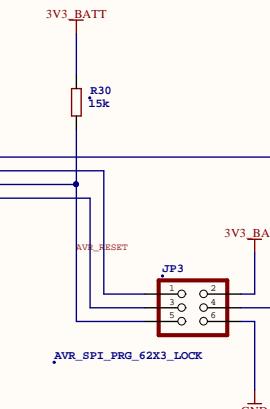
A

### AVR Tiny Tamper Detect MCU

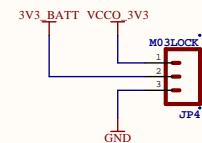


J10

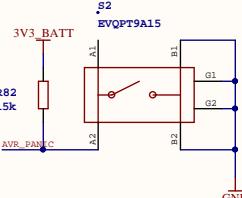
PC0\_(PCINT16/ADC16/T0CC0/SS/XCK)  
 PC1\_(PCINT17/ADC17/T0CC1/INT0/CLK0)  
 (PCINT18/ADC18/T0CC2/RXD/INT1)\_PC2  
 (PCINT19/ADC19/T0CC3/TX1)\_PC3  
 (PCINT20/ADC20/T0CC4)\_PC4  
 (PCINT21/ADC21/T0CC5/ICP1/TD)\_PC5  
 (PCINT22/ADC22/CLK1/T0CC6)\_PC6  
 (PCINT23/ADC23/T0CC7/T1)\_PC7  
 PDO\_(PCINT24/ADC24/SDA/MOSI)  
 PD1\_(PCINT25/ADC25/MISO)  
 PD2\_(PCINT26/ADC26/RESET/DW)  
 PD3\_(PCINT27/ADC27/SCL/SCK)



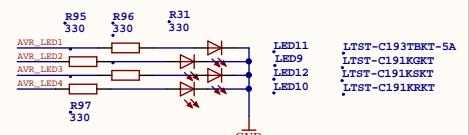
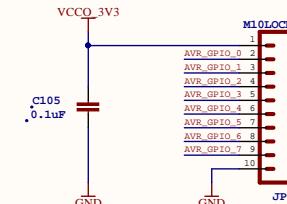
Connector for external 3V3 battery.  
 Place a jumper between pins 1-2 to "emulate" having a battery present.



### 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:

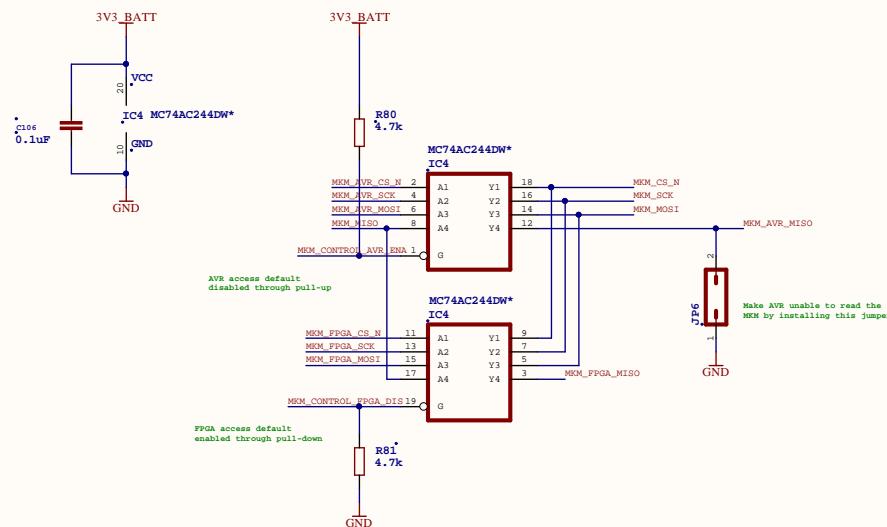
A

A

**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.

B

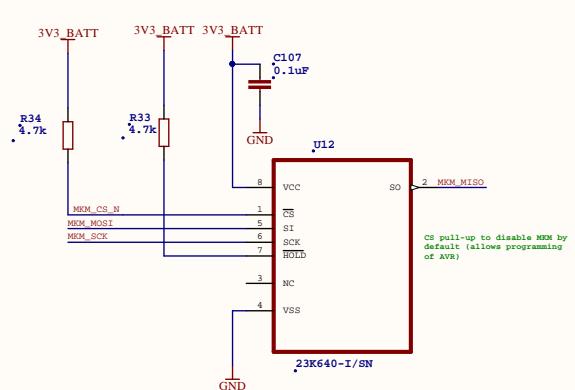
B



C

C

### Master Key Memory

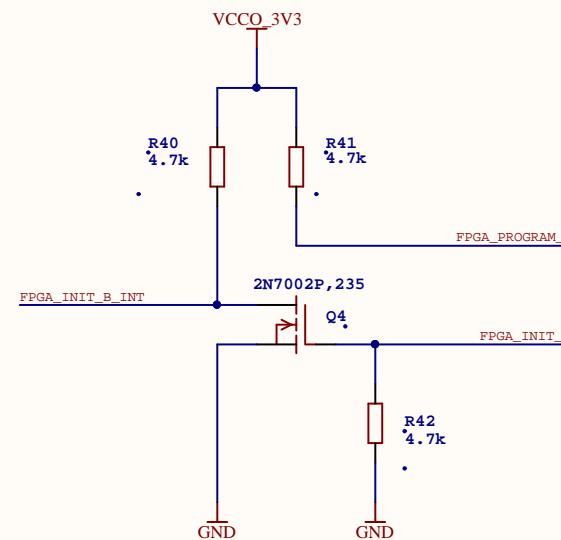
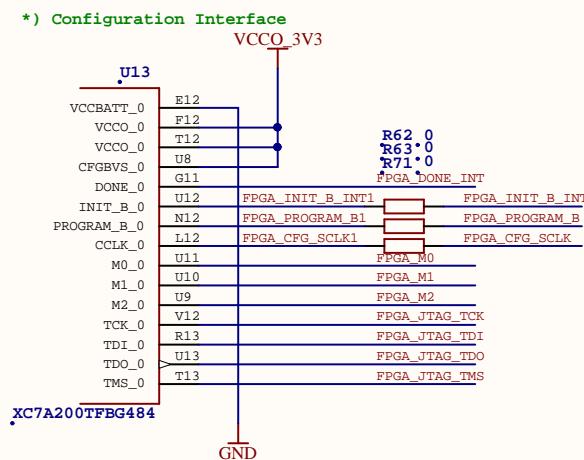


D

D

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

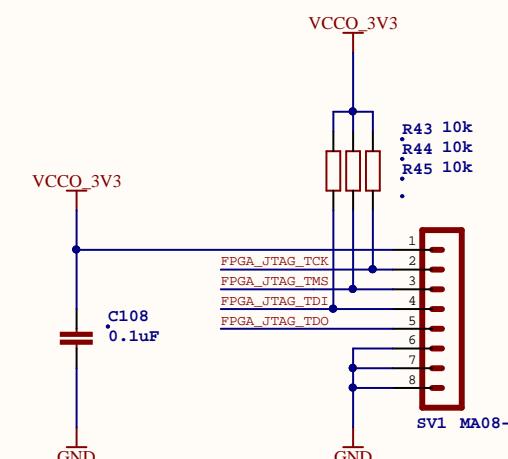
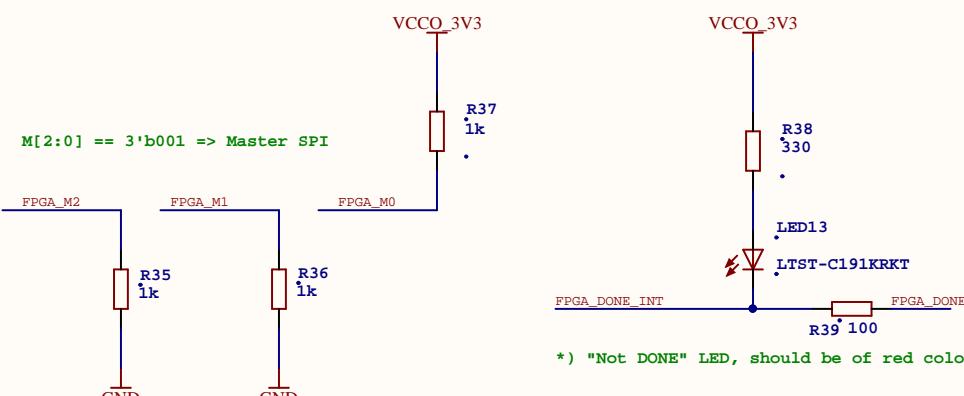
A



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

C

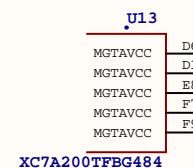
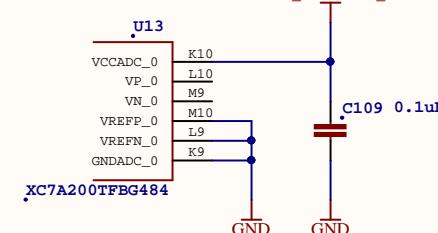


D

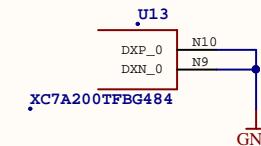
Title		
FPGA configuration interface		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\..\rev02_13.SchDoc	Drawn By:

A

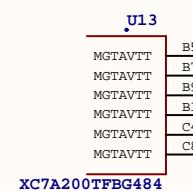
\*) Transceivers [NOT USED]

\*) XADC [NOT USED]  
FPGA\_VCCAUX\_1V8

\*) Temperature Sensor [NOT USED]



B

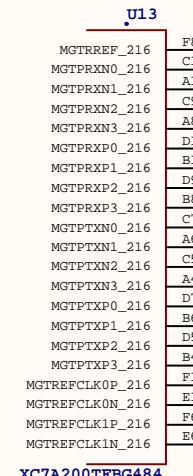


A

B

C

C



D

C

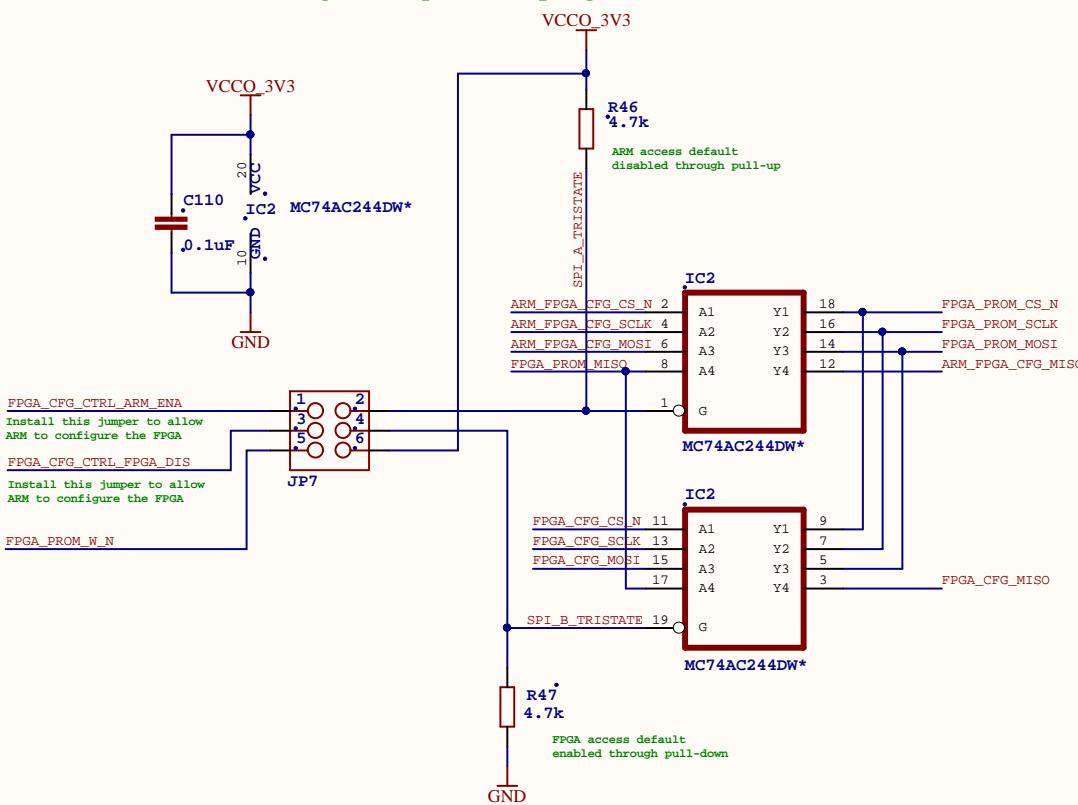
D

Title

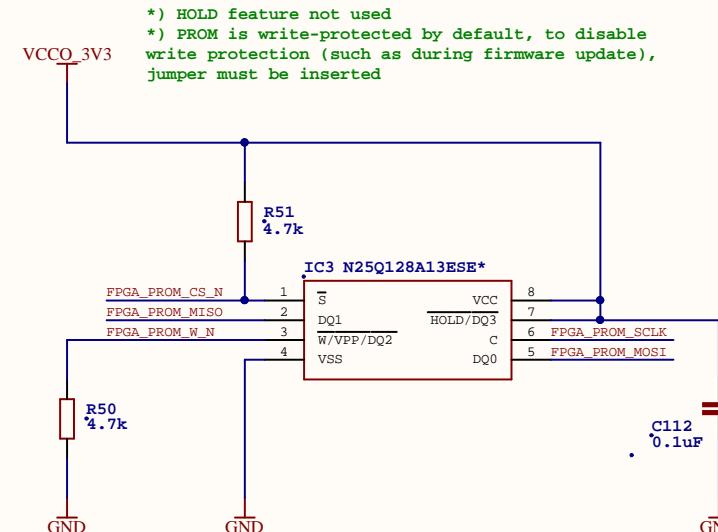
**FPGA unused**

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

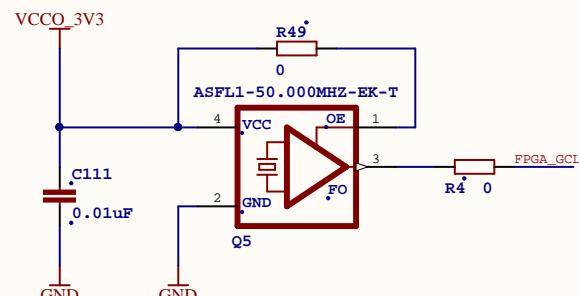
**SPI mux to let ARM override access to  
FPGA config memory (to reprogram FPGA)**



**FPGA config memory, 128 Mbit**



**FPGA clock**

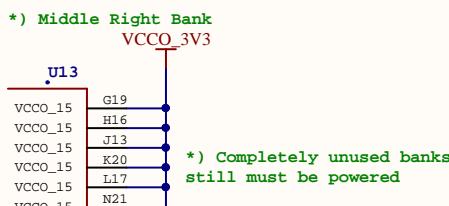


Title **FPGA supporting components**

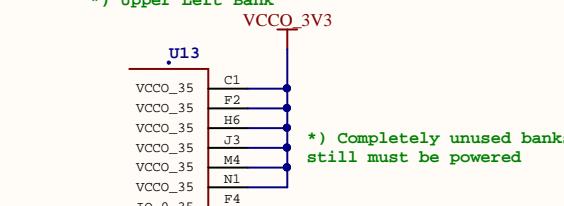
Size	Number	Revision
A4		
Date: 30.05.2016	Sheet of	
File: C:\SHARE\..\rev02_15.SchDoc		Drawn By:

A

## \*) Middle Right Bank



## \*) Upper Left Bank



B

IO\_L1P\_TO\_ADP15, IO\_L1N\_TO\_ADN15, IO\_L2P\_TO\_ADP15, IO\_L2N\_TO\_ADN15, IO\_L3P\_TO\_DQS\_ADP15, IO\_L3N\_TO\_DQS\_ADI15, IO\_L4P\_TO\_15, IO\_L4N\_TO\_15, IO\_L5P\_TO\_ADP15, IO\_L5N\_TO\_ADN15, IO\_L6P\_TO\_15, IO\_L6N\_TO\_VREF15, IO\_L7P\_T1\_ADP2P15, IO\_L7N\_T1\_AD2N15, IO\_L8P\_T1\_ADIOP15, IO\_L8N\_T1\_AD10N15, IO\_L9P\_T1\_DQS\_ADP3P15, IO\_L9N\_T1\_DQS\_ADI3N15, IO\_L10P\_T1\_ADI1P15, IO\_L10N\_T1\_ADI1N15, IO\_L11P\_T1\_SRCC15, IO\_L11N\_T1\_SRCC15, IO\_L12P\_T1\_MRCC15, IO\_L12N\_T1\_MRCC15, IO\_L13P\_T2\_MRCC15, IO\_L13N\_T2\_MRCC15, IO\_L14P\_T2\_SRCC15, IO\_L14N\_T2\_SRCC15, IO\_L15P\_T2\_DQS15, IO\_L15N\_T2\_DQS\_ADV\_B15, IO\_L16P\_T2\_A2815, IO\_L16N\_T2\_A2715, IO\_L17P\_T2\_A2615, IO\_L17N\_T2\_A2515, IO\_L18P\_T2\_A2415, IO\_L18N\_T2\_A2315, IO\_L19P\_T2\_A2215, IO\_L19N\_T3\_A21\_VREF15, IO\_L20P\_T3\_A2015, IO\_L20N\_T3\_A1915, IO\_L21P\_T3\_DQS15, IO\_L21N\_T3\_DQS\_A1815, IO\_L22P\_T3\_A1715, IO\_L22N\_T3\_A1615, IO\_L23P\_T3\_FOE\_B15, IO\_L23N\_T3\_FWE\_B15, IO\_L24P\_T3\_RS115, IO\_L24N\_T3\_RS015, IO\_2515

XC7A200TFBG484

XC7A200TFBG484

A

B

C

D

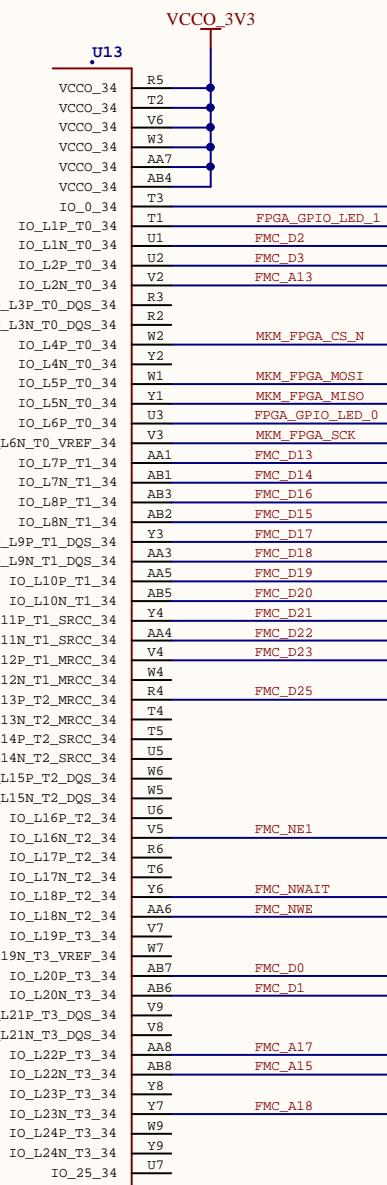
Title

FPGA unused banks

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

A

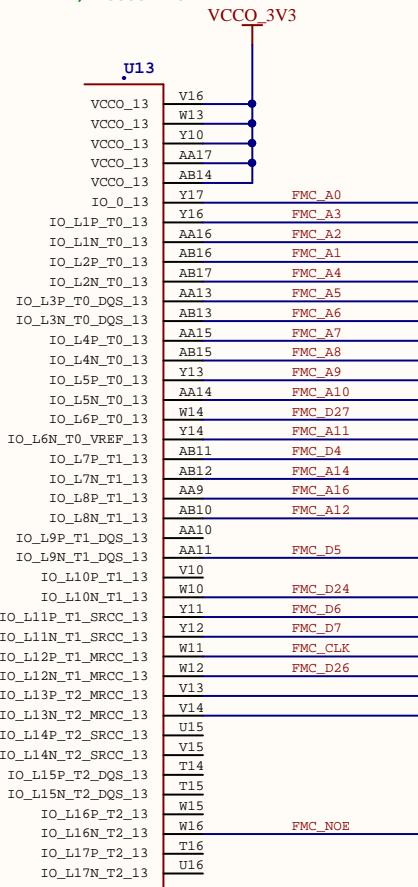
## \*) Lower Left Bank



A

B

## \*) Bottom Bank



B

C

<-- 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)

C

D

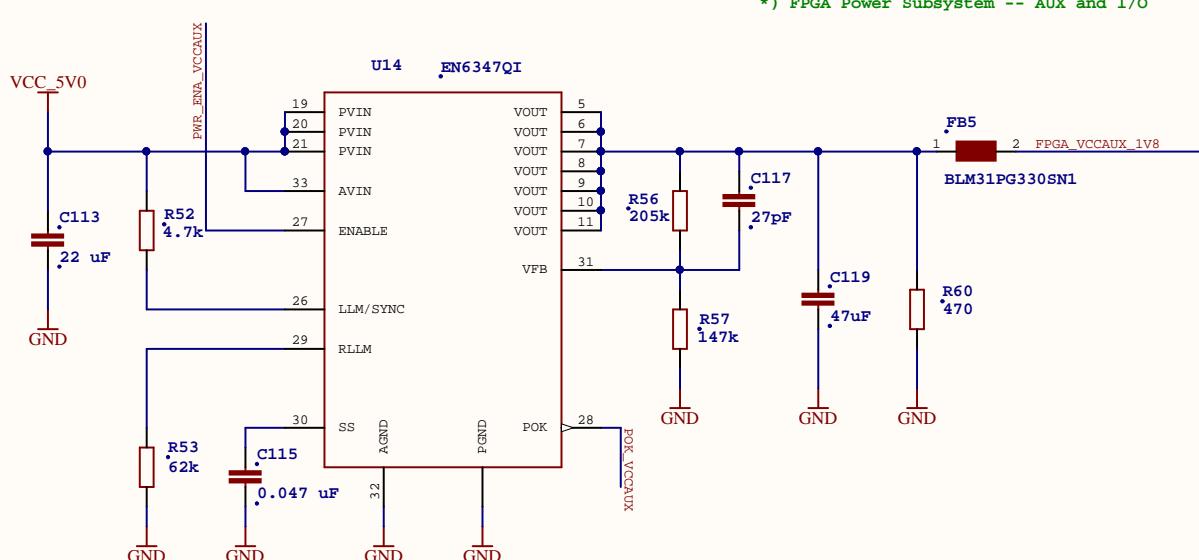
Title

FPGA FMC interface

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

A

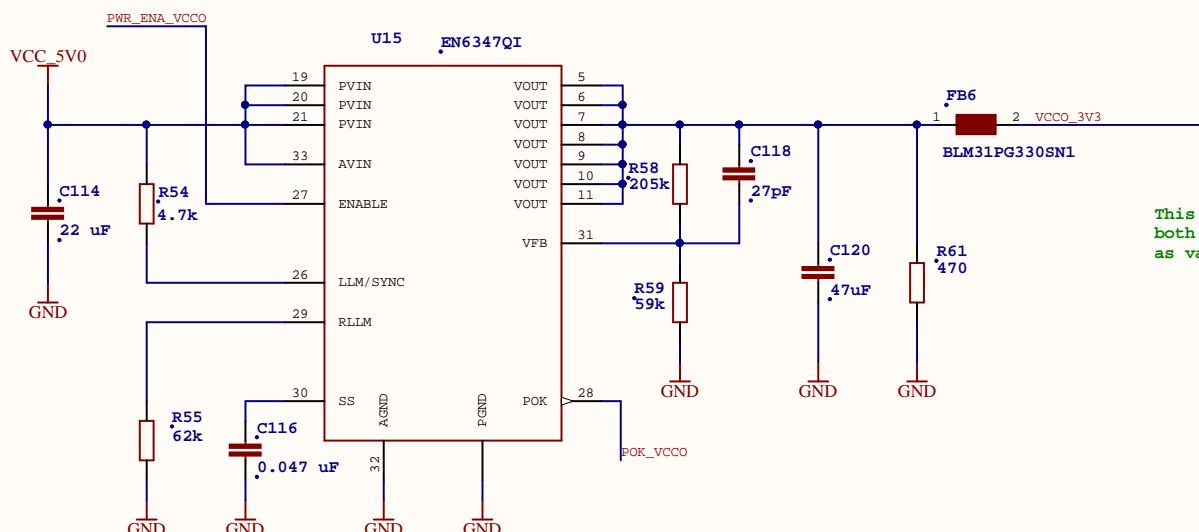
A



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

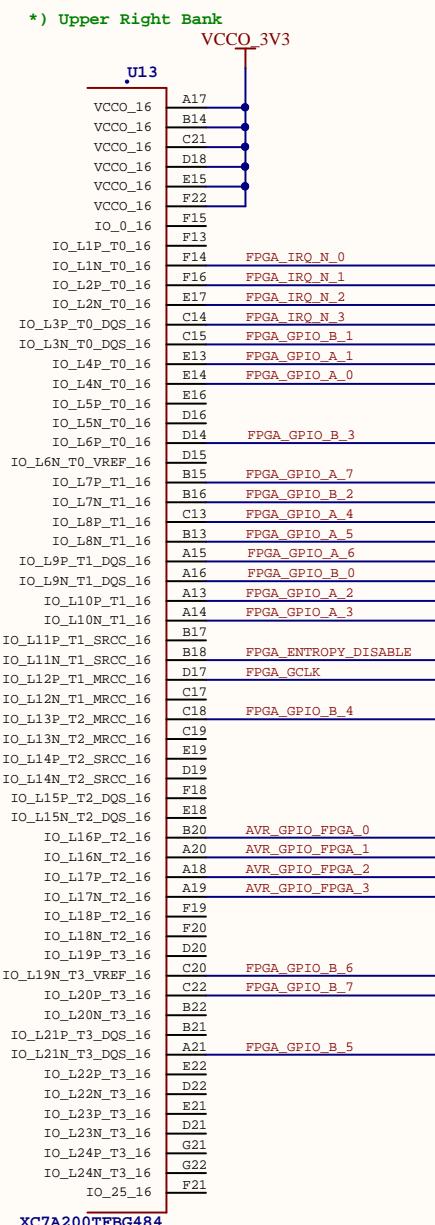
B

B



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

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



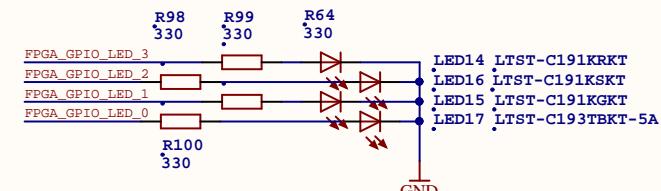
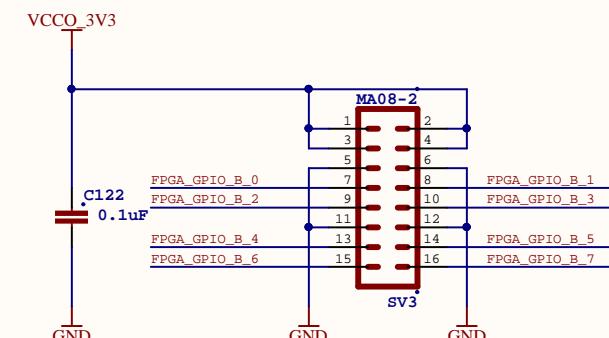
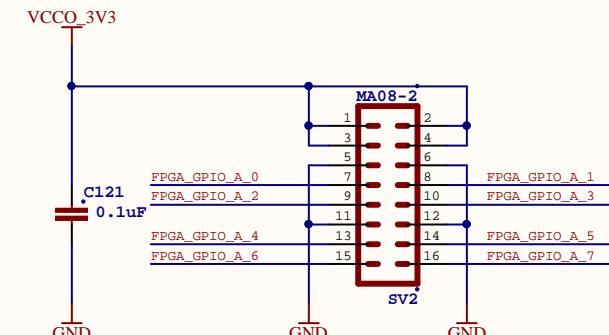
**NOTE:** One of the **FPGA\_GPIO\_\*** pins should be connected to one of the MRCC pins.

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

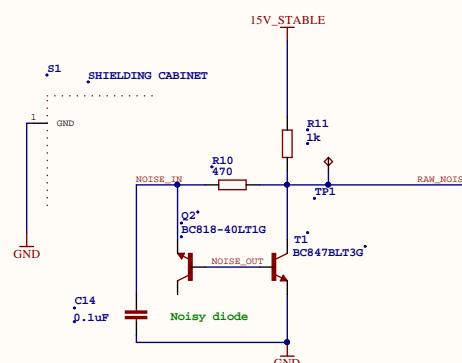
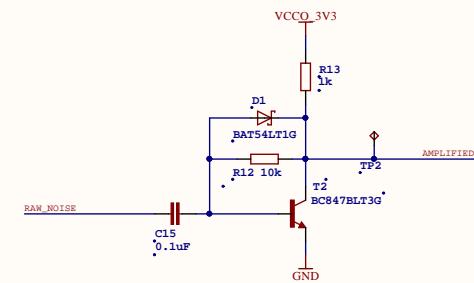
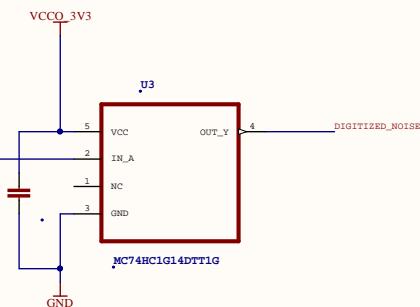
**\*) Signals, that are allowed to be swapped, can be swapped with each other and/or moved to different pins within their bank.**



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

A

A

**Noise generator****Amplifier****Digitizer**

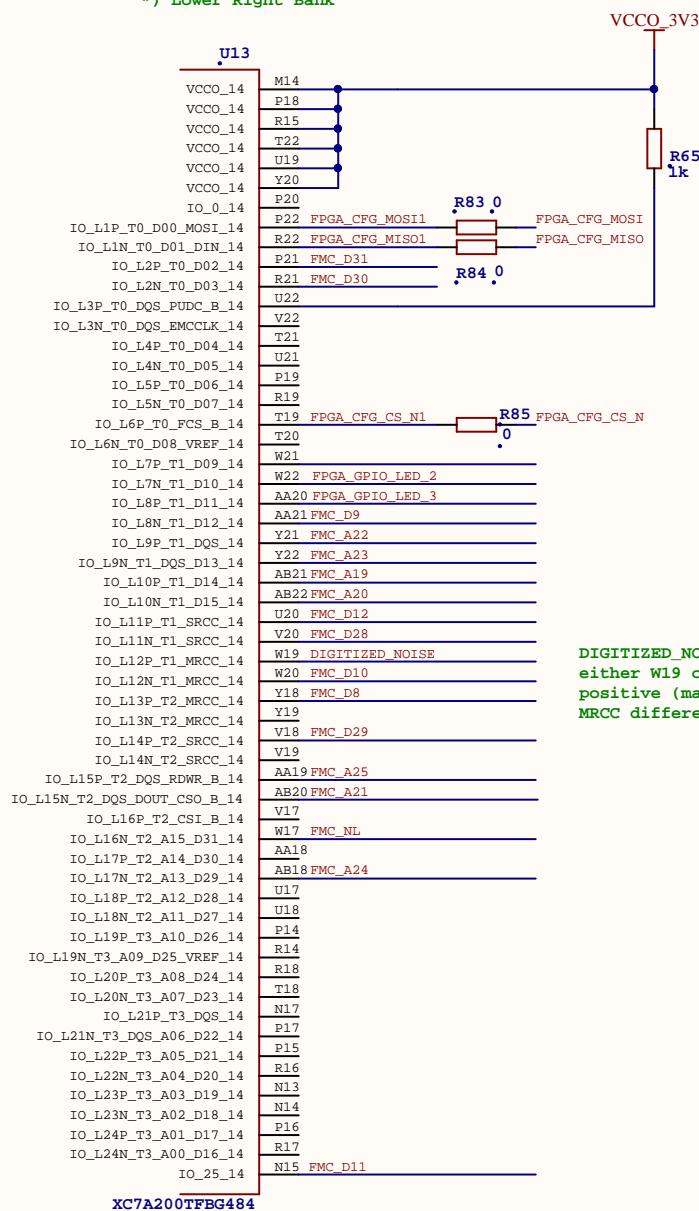
AGND is connected to GND on the board using polygons  
(found no other good way) - not visible in schematics.

This whole sheet's 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:

A

## \*) 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)

B

A

B

C

C

D

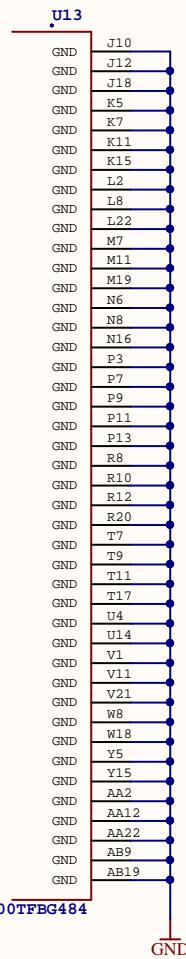
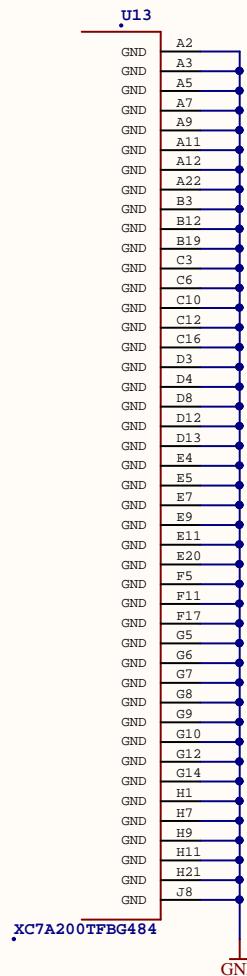
D

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

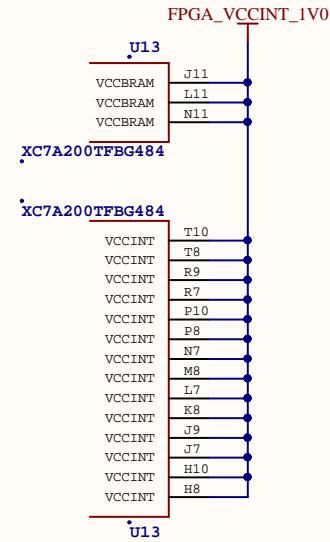
A

A

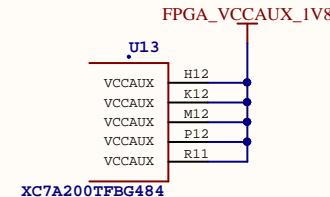
## \*) Ground Pins



## \*) Power - CORE &amp; BRAM



## \*) Power - AUX



B

B

C

C

D

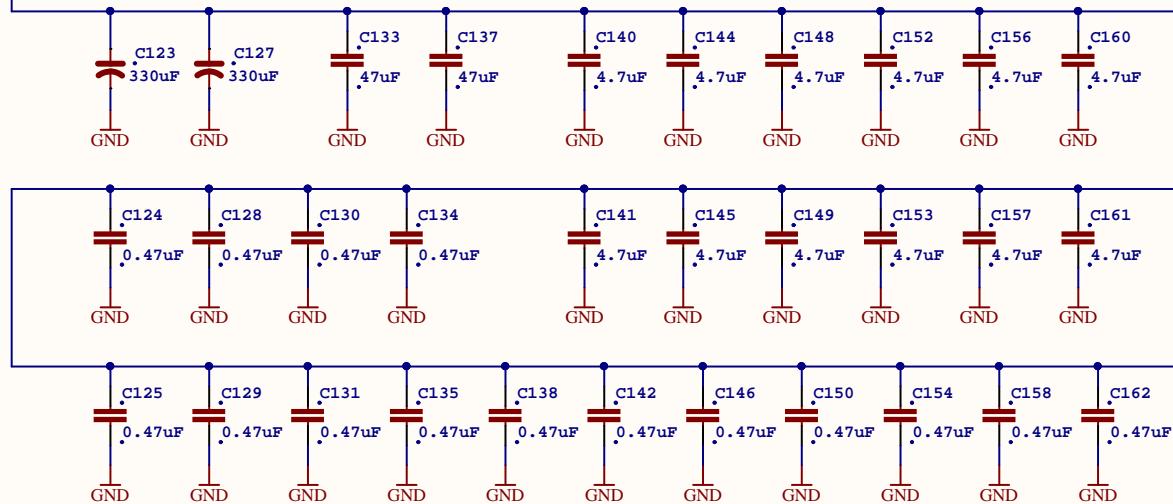
D

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

A

FPGA\_VCCINT\_1V0

\*) Decoupling capacitors for VCCINT and VCCBRAM

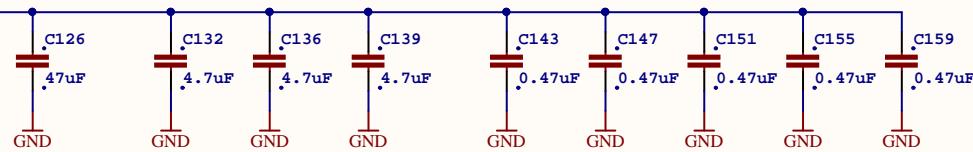


<-- Place small 0.47 uF caps right under the BGA package  
 <-- Place medium 4.7 uF caps very close to the BGA package  
 <-- Place large 47 uF and 330 uF caps not far from the BGA package  
 <-- Distribute smaller caps evenly under the BGA package  
 <-- Distribute larger caps evenly around the BGA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

B

FPGA\_VCCAUX\_1V8

\*) Decoupling capacitors for VCCAUX



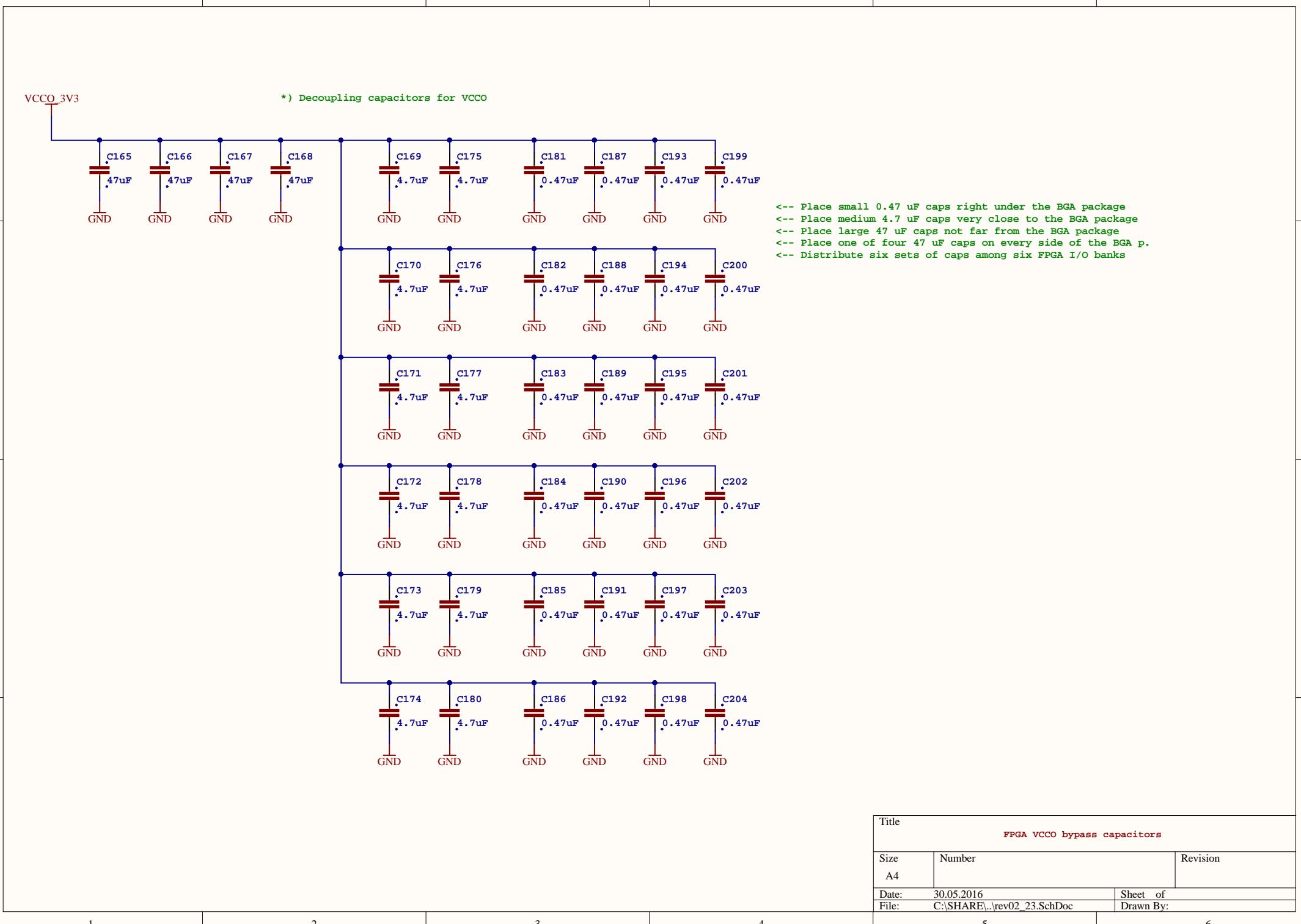
<-- Place small 0.47 uF caps right under the BGA package  
 <-- Place medium 4.7 uF caps very close to the BGA package  
 <-- Place large 47 uF caps not far from the BGA package  
 <-- Try to place smaller caps next to FPGA balls

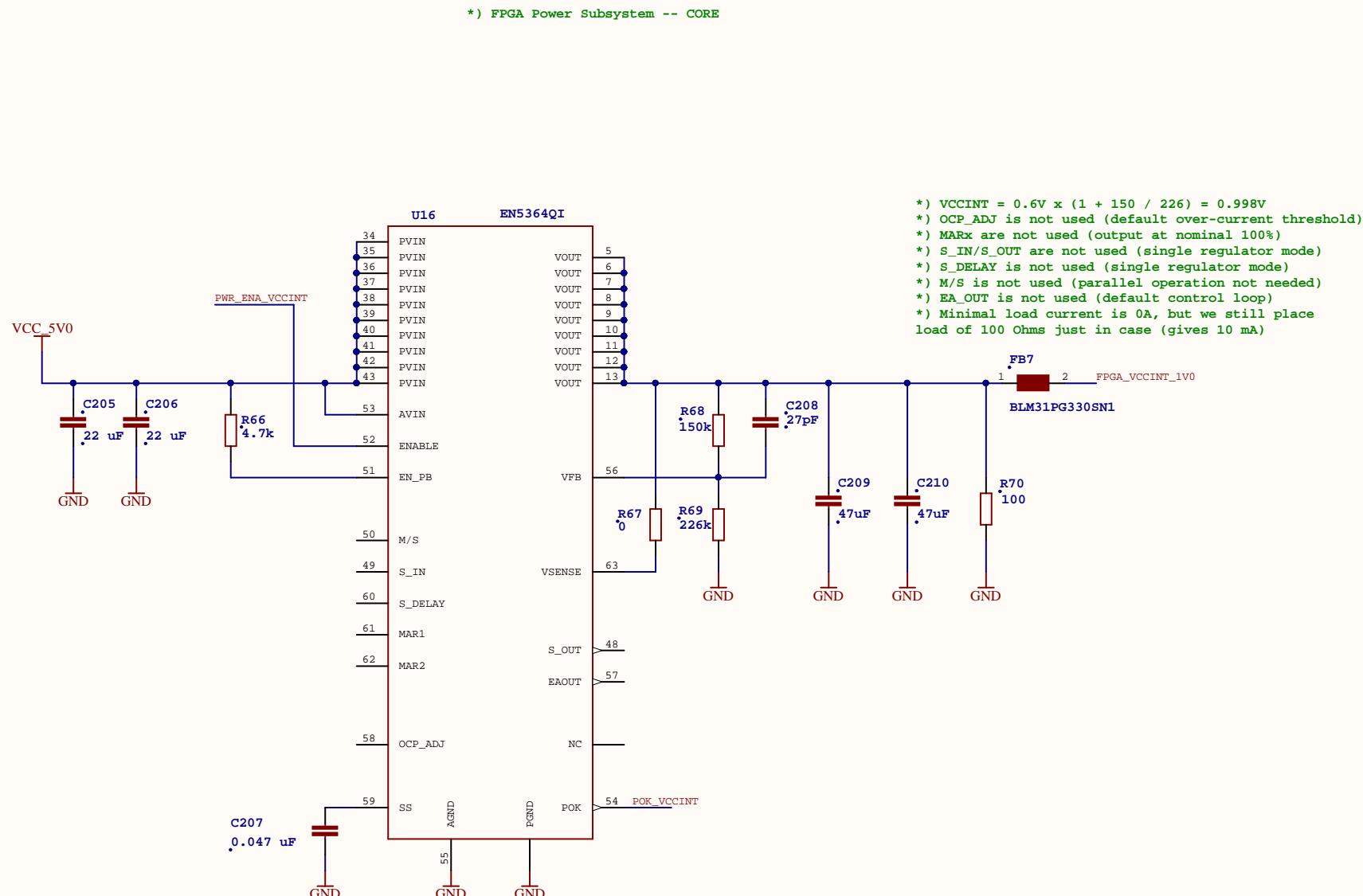
D

Title

FPGA CORE and AUX capacitors

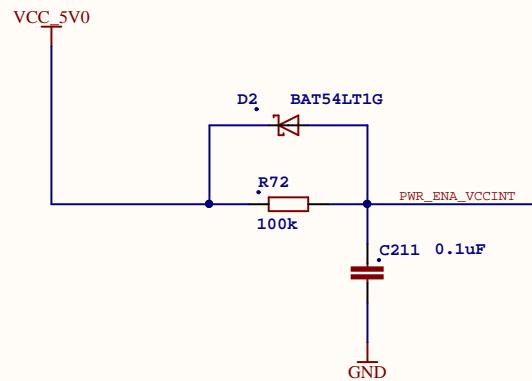
Size	Number	Revision
A4		
Date: 30.05.2016	Sheet of	
File: C:\SHARE\..\rev02_22.SchDoc	Drawn By:	



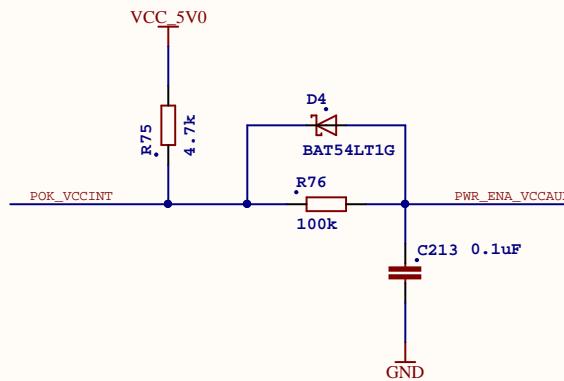


Title		
FPGA CORE voltage regulators		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\..\rev02_24.SchDoc	Drawn By:

A

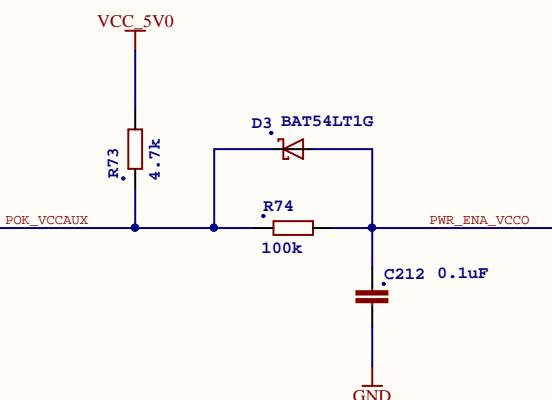


---&gt;



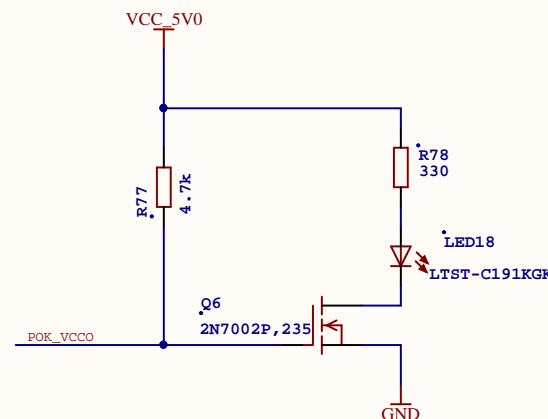
\*) Recommended power-up sequence:  
 1) VCCINT  
 2) VCCAUX  
 3) VCCO      --->  
 RC network values are preliminary,  
 should be tweaked after experiments

B



---&gt;

---&gt;

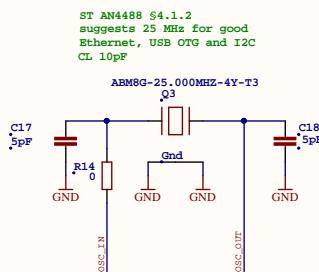


\*) "Power OK" LED, should be of green color

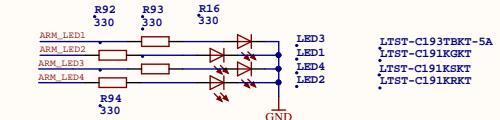
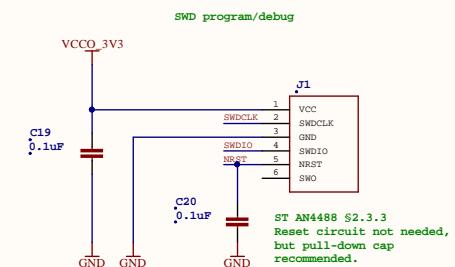
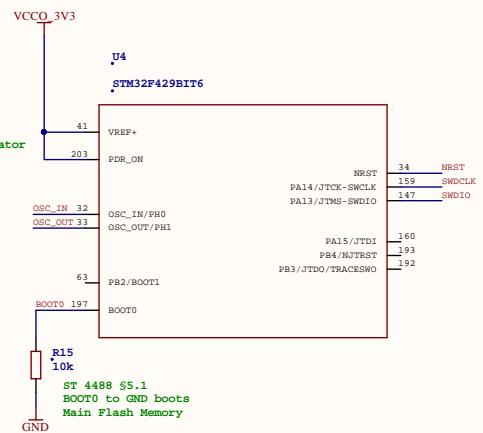
D

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

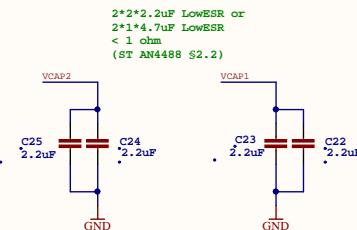
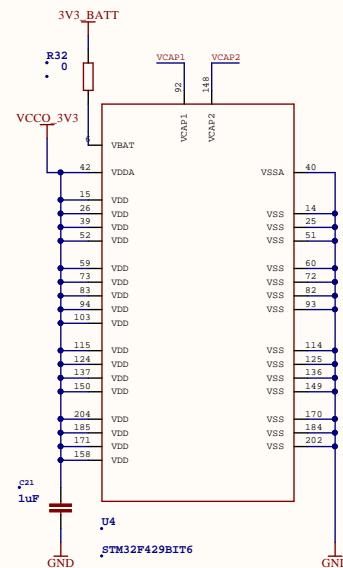


PDR\_ON high enables internal power regulator

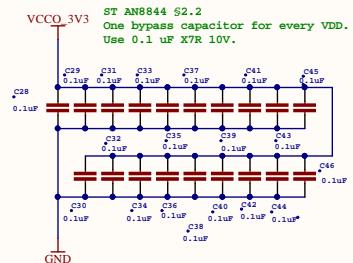


Title		
ARM configuration		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_3.SchDoc	Drawn By:

## Power and bypass capacitors, STM32

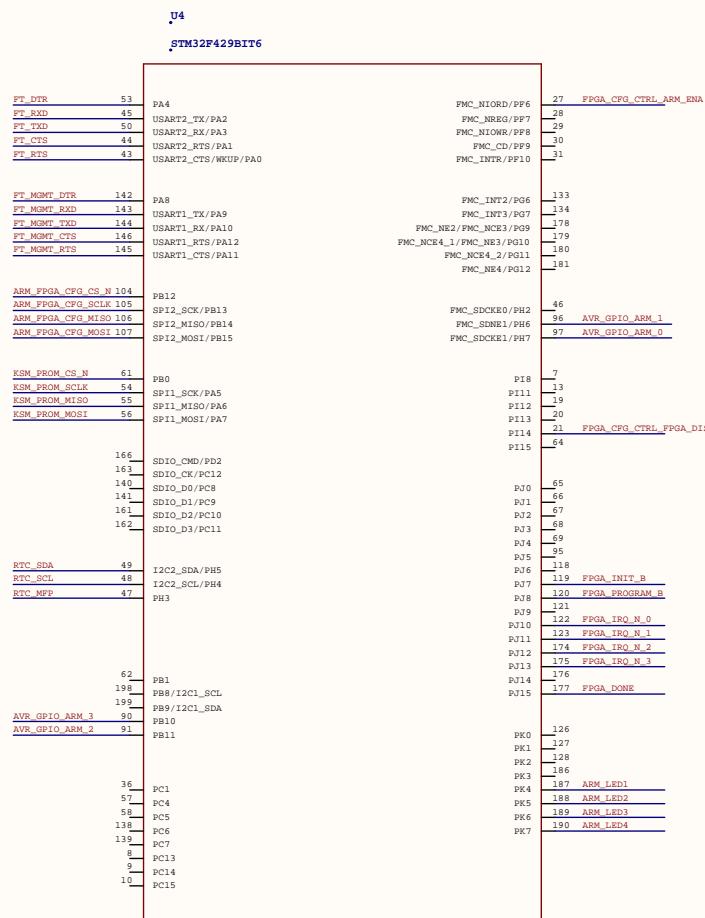


ST AN8844 S2.2  
One 10uF bypass cap for the package.  
(two used for extra comfort)

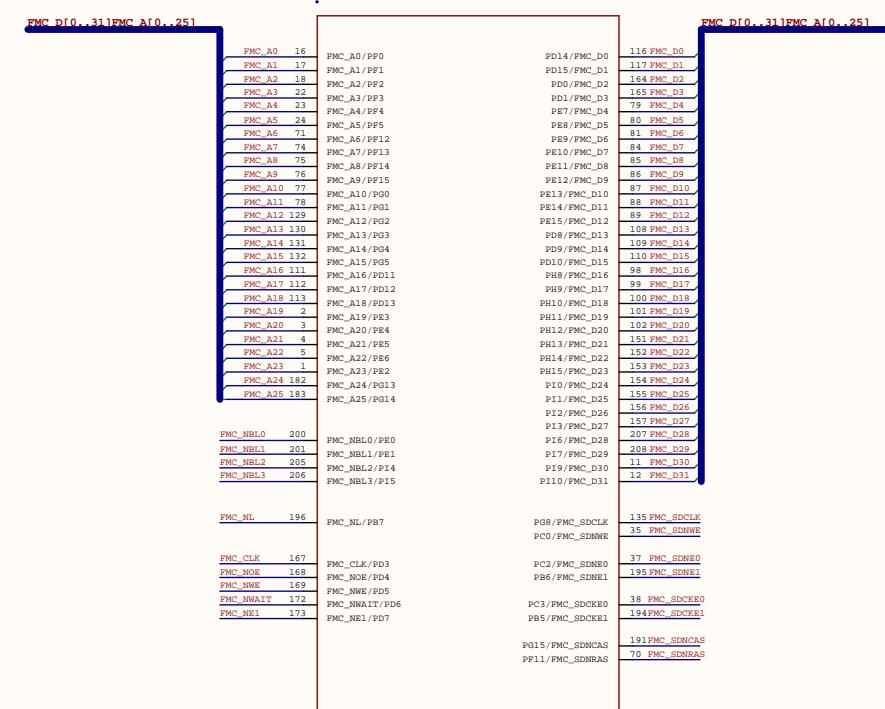


Title		
Size	Number	Revision
A4		
Date:	30.05.2016	Sheet of
File:	C:\SHARE\...\rev02_4.SchDoc	Drawn By:

## A Input/output, STM32



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



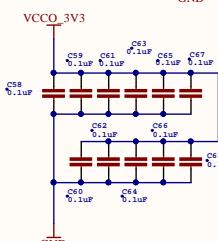
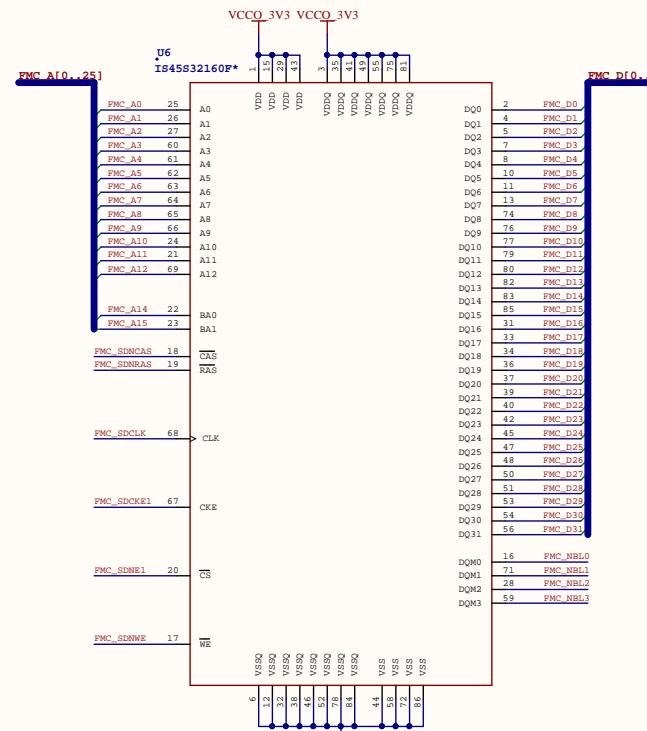
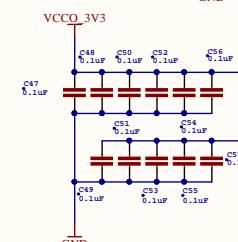
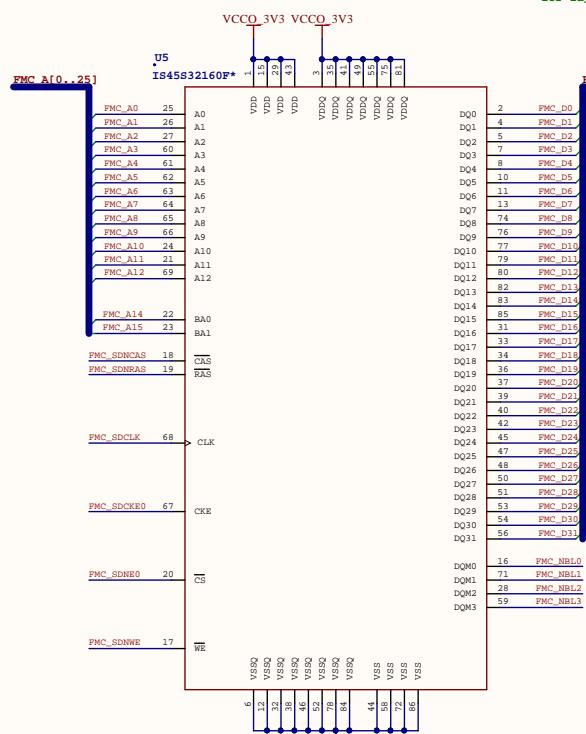
Title ARM I/O		
Size A4	Number	Revision
Date: 30.05.2016		Sheet of
File: C:\SHARE\...\rev02_5.SchDoc		Drawn By:

A

A

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

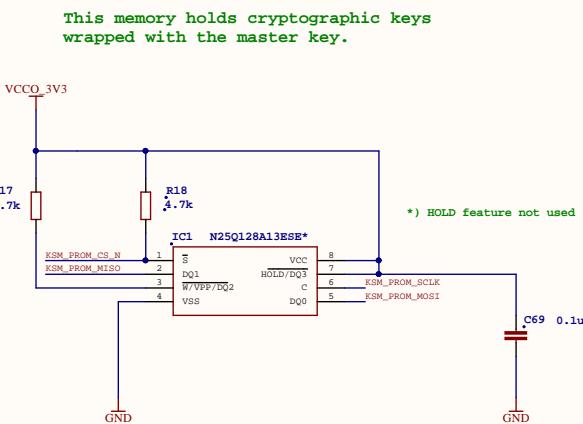
A

A

## Keystore memory, 128 Mbit

B

B



C

C

D

D

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

A

A

B

B

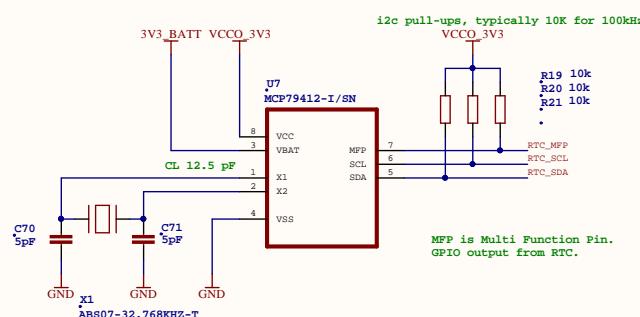
C

C

D

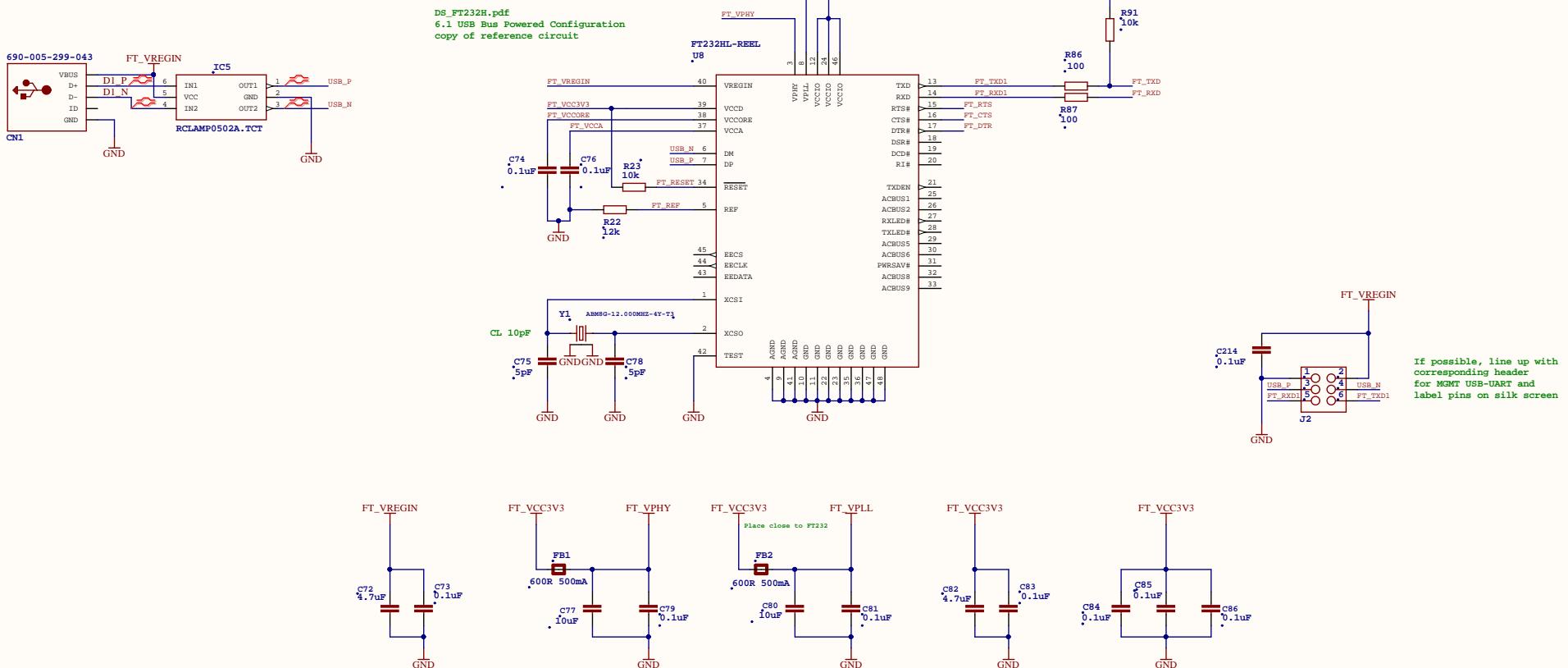
D

### Real Time Clock



Title		
<b>Real Time Clock</b>		
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: