Dedicated to graf_chokolo, dantehades, israyel & PS3 sceners
Logo by moneef

DOCUMENT HISTORY

V1.0 – Initial version

V1.1 – 07/19/11

- SPANSION NOR reference added: S29GL128P90TFIR2,
- GPIO assignment update to use the LTC4411 STAT signal (GPIO#4 & GPIO#5 are now unusable),
- “Official” PNM logo inserted in the document.

INTRODUCTION

SLIM PS3 consoles use an 8Mx16bits **NOR** FLASH (**128Mbits** of non-volatile memory).

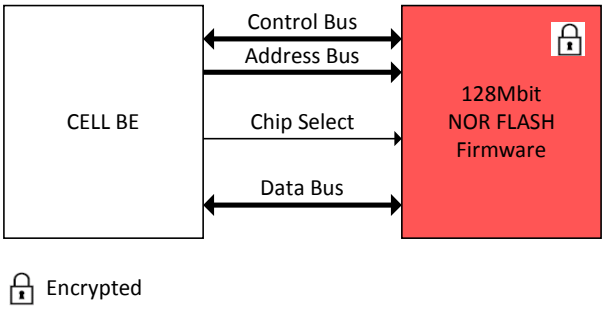
The memory could be one of the following references:

- **K8Q2815UQB-PI4B** (Manufacturer: **SAMSUNG**),
- **S29GL128P90TFIR2** (Manufacturer: **SPANSION**).

Please refer to the datasheet for further information.
The FLASH is packaged in a **TSOP56** (Thin Small-Outline Package).

This memory embeds a part of the firmware used by the CELL BE itself (asecure_loader, eEID, …).
The other part of the firmware is stored on the internal HDD.

The following diagram illustrates the architecture used between the CELL BE and the NOR FLASH:



Please note that the FLASH content is **ENCRYPTED**.

PNM is a project using a FPGA and 2 NOR FLASH sockets.
It requires a direct access to the PS3 CELL EBU (signals are located on the motherboard).
This may be the riskier step due to the number of signals involved.
The embedded NOR must have been removed or disabled to avoid electrical conflicts.

PNM is designed with several hardware/software features in mind:

- ✓ **DUMP**
  This command dumps (reads) the content of a NOR FLASH.

- ✓ **UPDATE**
  This command updates (writes) the content of a NOR FLASH.

- ✓ **COPY**
  This command copies the content of a NOR FLASH to another NOR FLASH.

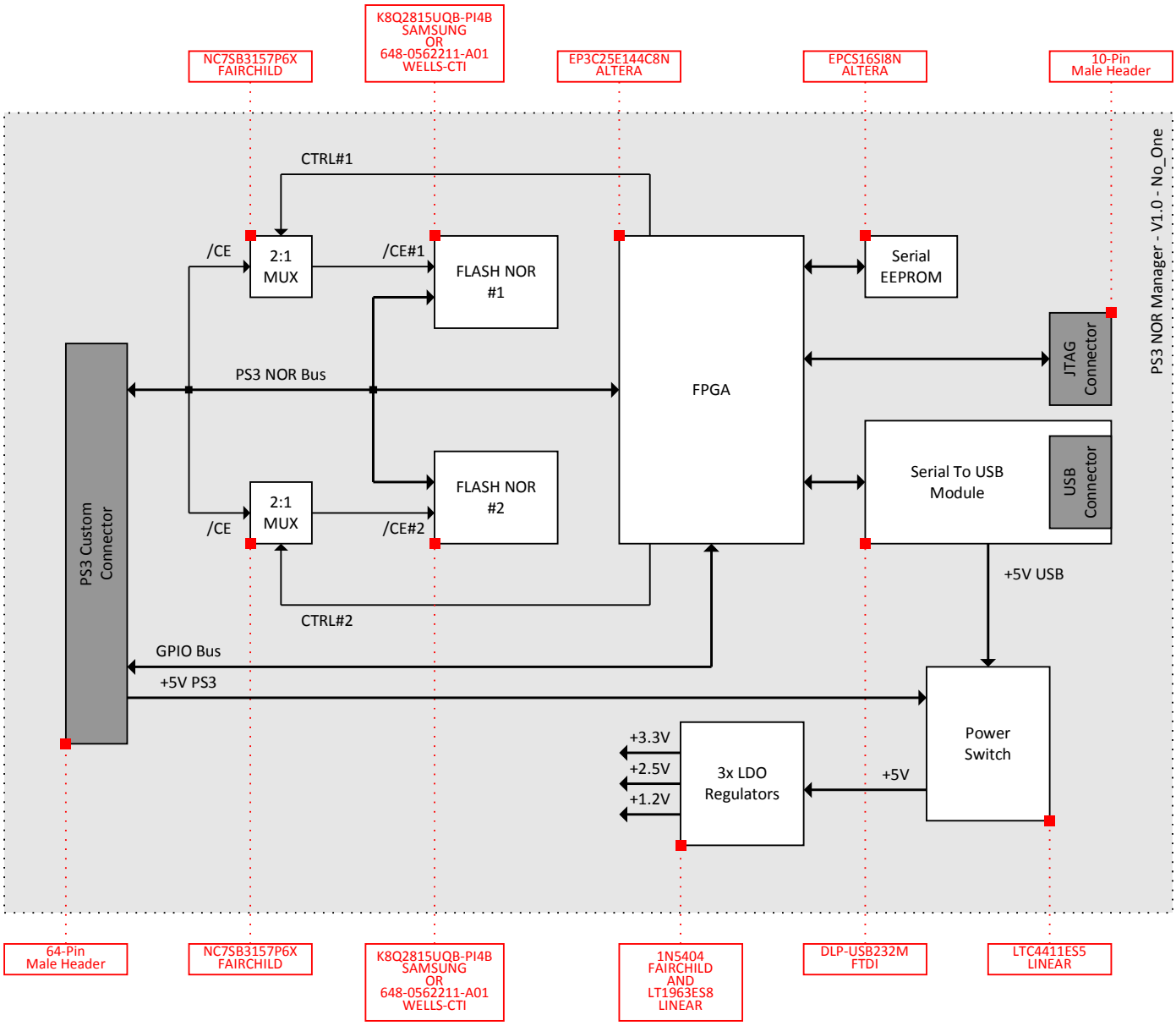
- ✓ **STATIC SWITCH**
  This command defines the NOR FLASH to be used (before starting the PS3 console).

- ✓ **DYNAMIC SWITCH**
  This command defines the NOR FLASH used with programmable conditions (from host).

- ✓ **CAPTURE**
  This command captures the NOR bus activities.
  Programmable conditions could be used (number of samples to be defined).

- ✓ **…**

The following diagram illustrates the architecture used:



QUICK DESCRIPTION OF THE HARDWARE

POWER MANAGEMENT

In a standalone use, PNM is powered by the USB port (+5V).
Once connected to the PS3, PNM is powered by the console itself even if USB port is used.
Here is the power management rules:

P5VUSB	P5VPS3	PNM	Comments
NO	NO	-	PNM is OFF
NO	YES	Powered by P5VPS3	-
YES	NO	Powered by P5VUSB	-
YES	YES	Powered by P5VPS3	The USB port is used for communication

PNM must be powered before starting the console otherwise the CELL cannot boot properly.
Please notice that NOR maintenance features (DUMP, UPDATE…) are disabled when PNM is powered by the PS3. This prevents from electrical conflicts. Multiplexing features are still active (SWITCH functions).

PNM power consumption is about **0.4W** when sockets are empty.

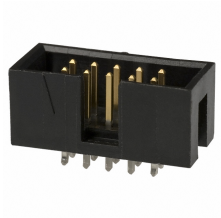
USB PORT

The USB port is mainly used in the standalone mode.
PNM uses a module (**DLP-USB232M**) manufactured by **FTDI**.
Please refer to the following website for more details (http://www.ftdichip.com).
Drivers are provided to handle the USB communication (Virtual COM Port).
The transfer bandwidth is limited to **3Mbauds**.
A LED indicates whenever communication is active between PNM and host.
The host system (PC) must be capable to deliver up to **1W** on the power line.

JTAG CONNECTOR (10-PIN MALE HEADER)

The JTAG connector is used to debug/program the embedded FPGA.
The pinout has been chosen to fit the **JTAG USB-Blaster** product specifications (**ALTERA**):

Pin #	Name
1	TCK
2	GND
3	TDO
4	+3.3V
5	TMS
6	-
7	-
8	-
9	TDI
10	GND

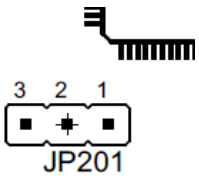


Please refer to the following website for more details (http://www.altera.com).
Please notice that this connector is only used for FPGA debug purposes.
A **LED** indicates the correct FPGA configuration (each time PNM is switched ON).
If this LED remains ON, the FPGA configuration failed.

Another **LED** indicates that the software is running.
Different blinking rates will be defined according to the function which is executed.

JUMPER

A **Jumper** selects the NOR socket used for booting the PS3 (STATIC SWITCH).



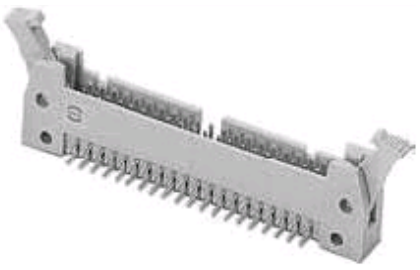
Jumper	Comments
1-2	SOCKET #2
2-3	SOCKET #1

The FLASH **socket #1 is active by default** (when no jumper used).

PS3 CONNECTOR (64-PIN MALE HEADER)

The PS3 connector (a DIN 41612 connector) is used to connect PNM to the console.
The pinout is totally customized:

Pin #	Name	Comments	Pin #	Name	Comments
1	A0	ADDRESS BIT #0 - LSB	33	DQ8	-
2	A1	-	34	DQ9	-
3	A2	-	35	DQ10	-
4	A3		36	DQ11	-
5	A4	-	37	DQ12	-
6	A5	-	38	DQ13	-
7	A6	-	39	DQ14	-
8	A7	-	40	DQ15	DATA BIT #15 - MSB
9	A8	-	41	GND	GROUND
10	A9	-	42	NCE	/CHIP_SELECT
11	A10	-	43	NOE	/OUTPUT_ENABLE
12	A11	-	44	NWE	/WRITE_ENABLE
13	A12	-	45	NWPACC	/WRITE_PROTECT
14	A13	-	46	RYNBY	/READY_BUSY
15	A14	-	47	NRESET	/RESET
16	A15	-	48	GND	GROUND
17	A16	-	49	NC	NOT CONNECTED
18	A17	-	50	NC	NOT CONNECTED
19	A18	-	51	GPIO5	GLOBAL PURPOSE I/O #5
20	A19	-	52	GPIO4	-
21	A20	-	53	GPIO3	-
22	A21	-	54	GPIO2	-
23	A22	ADDRESS BIT #22 - MSB	55	GPIO1	-
24	GND	GROUND	56	GPIO0	GLOBAL PURPOSE I/O #0
25	DQ0	DATA BIT #0 - LSB	57	GND	GROUND
26	DQ1	-	58	GND	GROUND
27	DQ2	-	59	NC	NOT CONNECTED
28	DQ3	-	60	NC	NOT CONNECTED
29	DQ4	-	61	GND	GROUND
30	DQ5	-	62	GND	GROUND
31	DQ6	-	63	P5VPS3	+5.0V
32	DQ7	-	64	P5VPS3	+5.0V



The P5VPS3 is a power line coming from the console (+5V).
When not in standalone mode, the **P5VPS3** MUST be active before switching on the PS3.
It is important to wire this line to a **permanently** active power (on the motherboard).

6 global purpose I/O are provided (GPIO0 to GPIO5).
Each generic I/O can be programmed and meets the following specifications:

- ✓ **Direction**
  It can be INPUT (default) or OUTPUT.

- ✓ **Data**
  It can be "0" (default) or "1".

Digital signals on this connector have LVCMOS/LVTTL **+3.3V logic levels**.
An **4.7Ohm resistor** has been inserted on each line to prevent from temporary short-circuits.

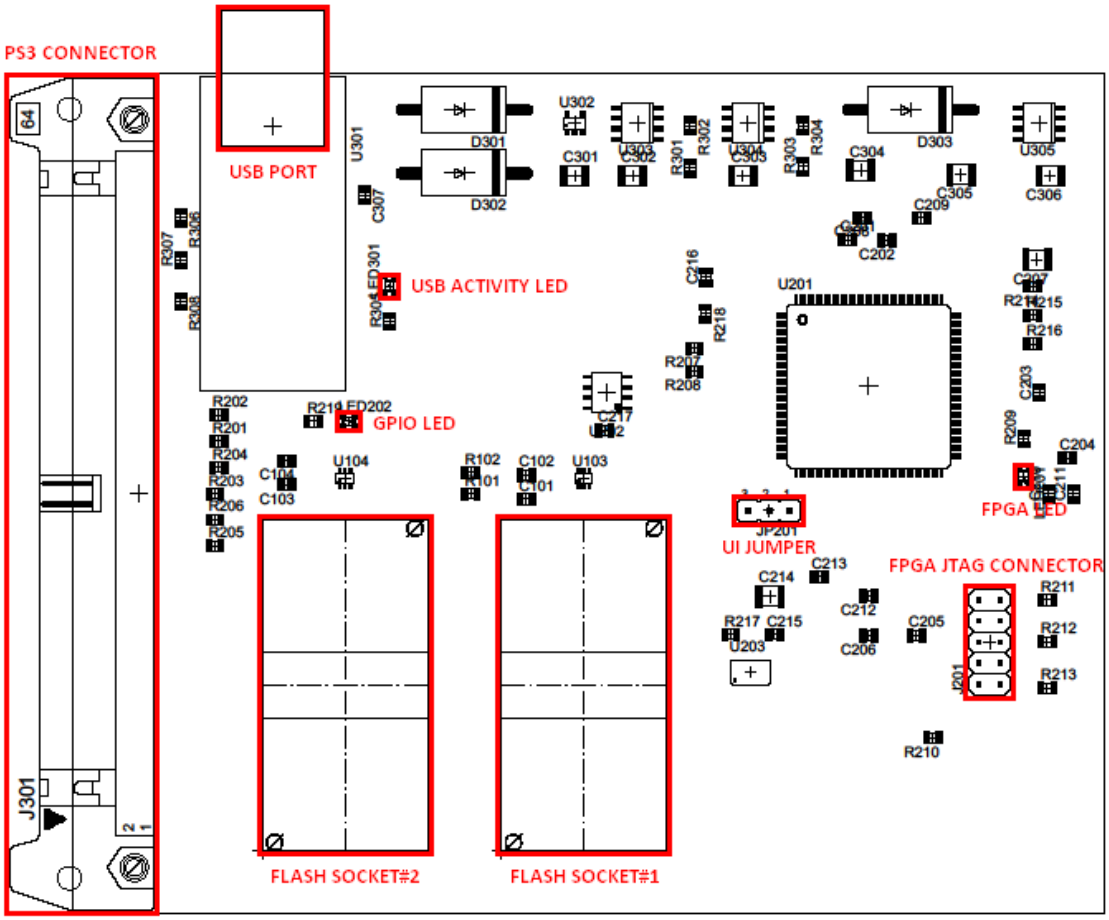
Current GPIO assignment:

GPIO	Comments	
#5	OUTPUT	This GPIO drives the UI LED – **Cannot be used anymore**
#4	INPUT	This GPIO reads the power STAT (LTC4411) – **Cannot be used anymore**
#3 to #0	BIDIR	General Purpose Input/Output

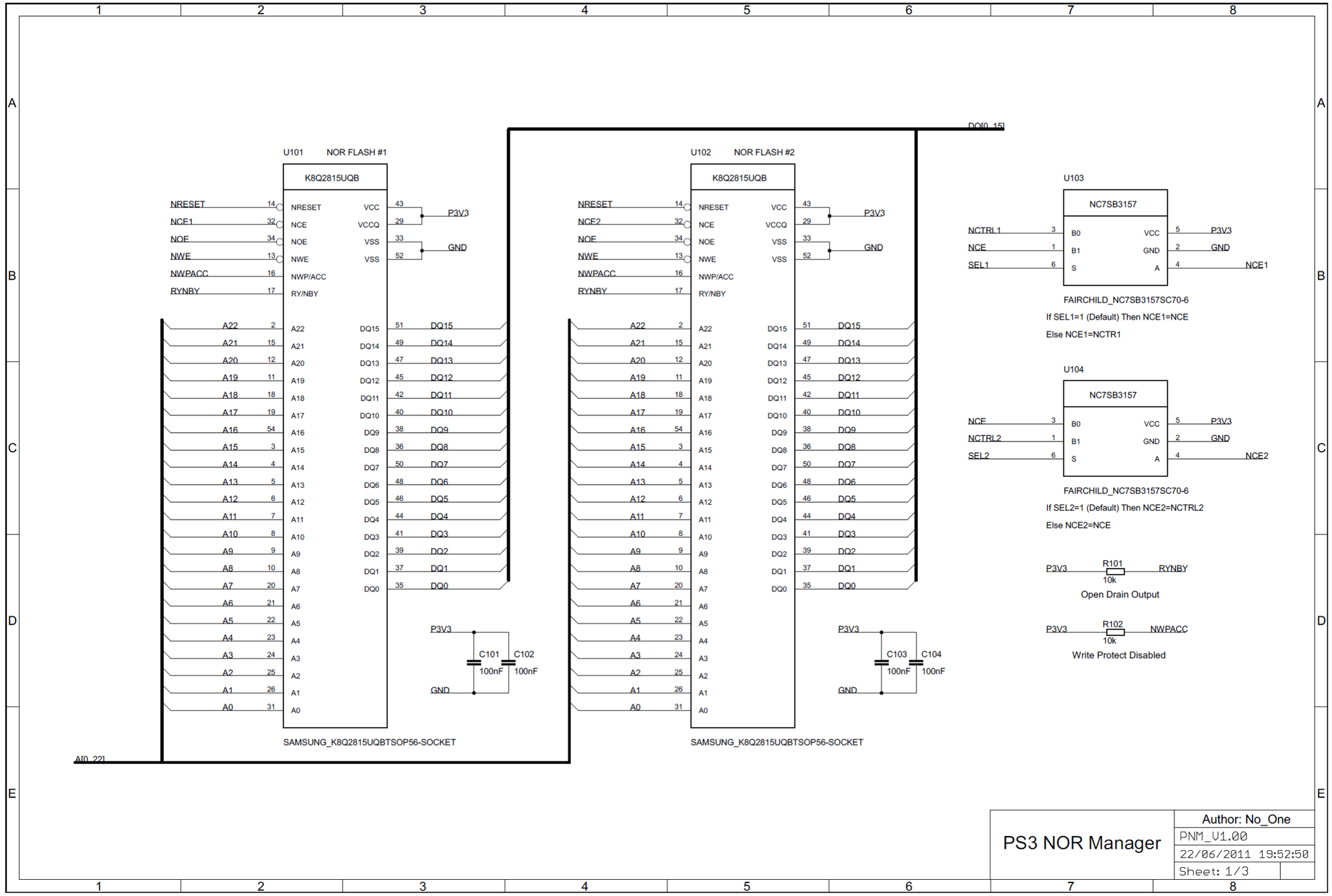
FLASH SOCKETS
PNM has 2 NOR FLASH sockets (push-pull).

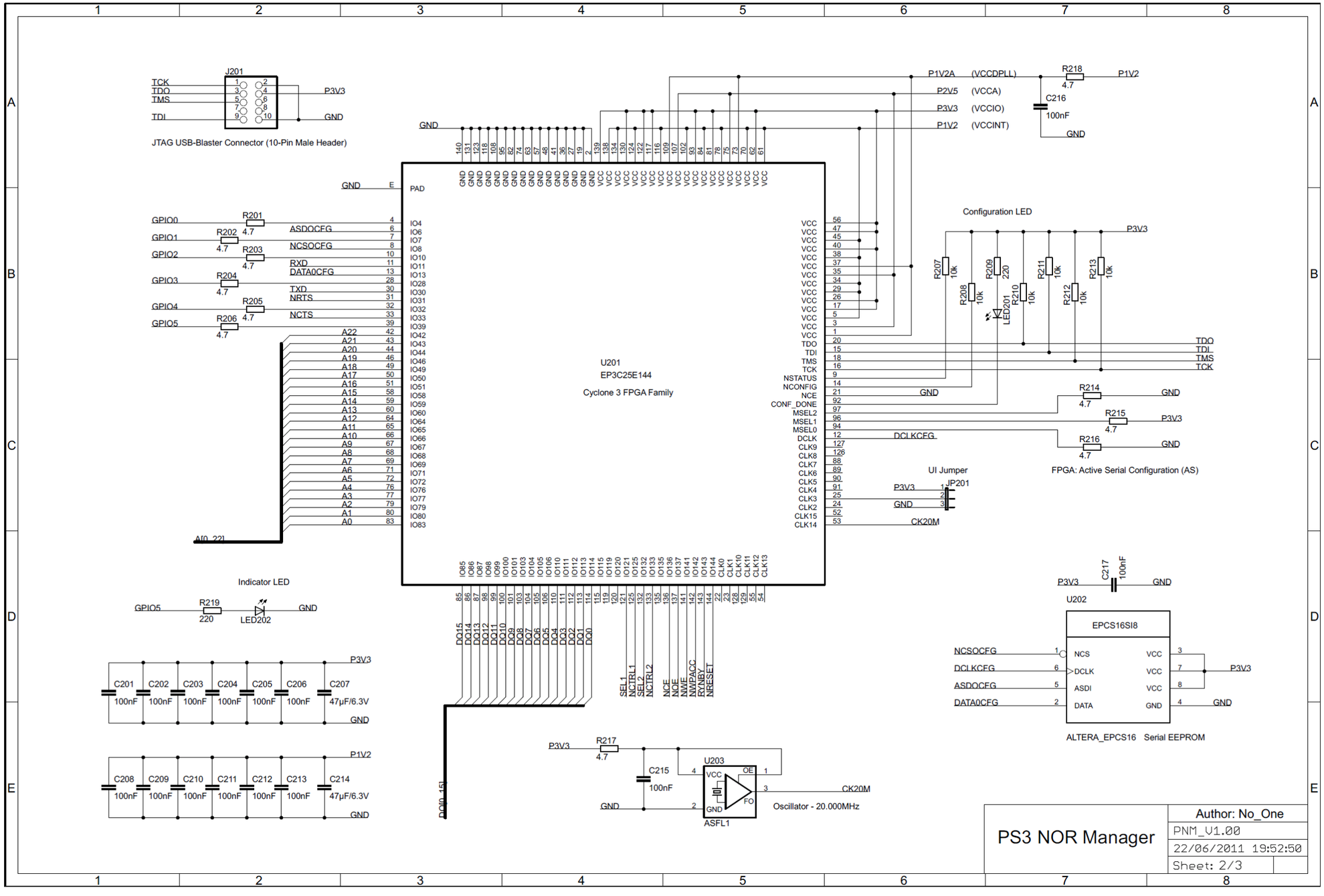
Both are connected to the PS3 CELL EBU.
The FLASH socket #2 is active only when requested by the host (PC) or the jumper.
The FPGA ensures that only one FLASH can be active to prevent from short-circuits.

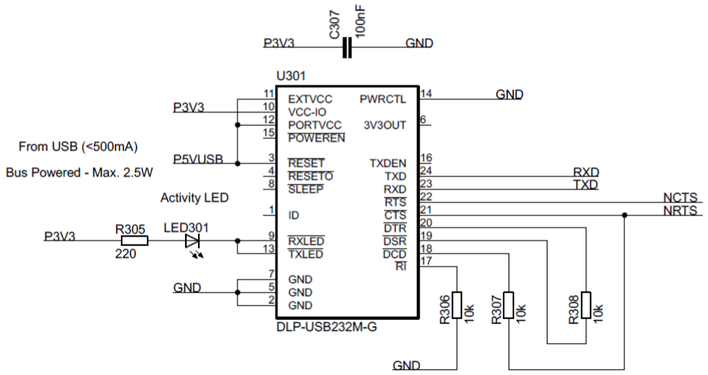
The following top view shows the different user interfaces (LEDS, SOCKETS, JUMPER and CONNECTORS):

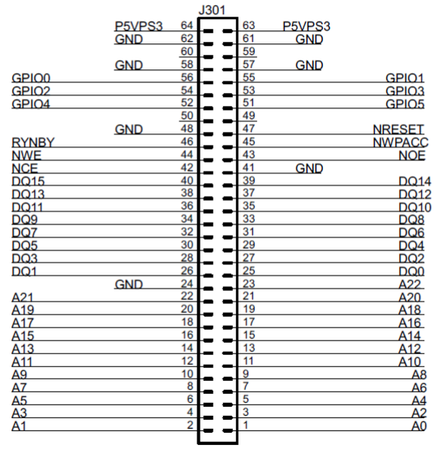


SCHEMATICS

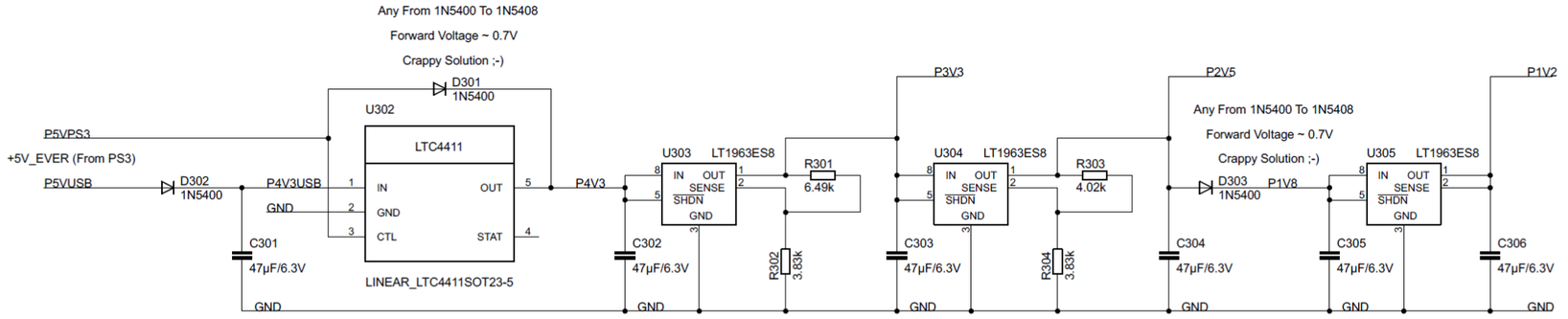

U101 NOR FLASH #1
K8Q2815UQB
NRESET 14
NCE1 32
NOE 34
NWE 13
NWPACC 16
RYNBY 17
A22 2
A21 15
A20 12
A19 11
A18 18
A17 19
A16 54
A15 3
A14 4
A13 5
A12 6
A11 7
A10 8
A9 9
A8 10
A7 20
A6 21
A5 22
A4 23
A3 24
A2 25
A1 26
A0 31
NRESET
NCE
NOE
NWE
NWP/ACC
RY/NBY
A22
A21
A20
A19
A18
A17
A16
A15
A14
A13
A12
A11
A10
A9
A8
A7
A6
A5
A4
A3
A2
A1
A0
VCC 43
VCCQ 29
VSS 33
VSS 52
DQ15 51
DQ14 49
DQ13 47
DQ12 45
DQ11 42
DQ10 40
DQ9 38
DQ8 36
DQ7 50
DQ6 48
DQ5 46
DQ4 44
DQ3 41
DQ2 39
DQ1 37
DQ0 35
P3V3
GND
C101 100nF
C102 100nF
SAMSUNG_K8Q2815UQBTSOP56-SOCKET
A[0..22]
U102 NOR FLASH #2
K8Q2815UQB
NRESET 14
NCE2 32
NOE 34
NWE 13
NWPACC 16
RYNBY 17
A22 2
A21 15
A20 12
A19 11
A18 18
A17 19
A16 54
A15 3
A14 4
A13 5
A12 6
A11 7
A10 8
A9 9
A8 10
A7 20
A6 21
A5 22
A4 23
A3 24
A2 25
A1 26
A0 31
NRESET
NCE
NOE
NWE
NWP/ACC
RY/NBY
A22
A21
A20
A19
A18
A17
A16
A15
A14
A13
A12
A11
A10
A9
A8
A7
A6
A5
A4
A3
A2
A1
A0
VCC 43
VCCQ 29
VSS 33
VSS 52
DQ15 51
DQ14 49
DQ13 47
DQ12 45
DQ11 42
DQ10 40
DQ9 38
DQ8 36
DQ7 50
DQ6 48
DQ5 46
DQ4 44
DQ3 41
DQ2 39
DQ1 37
DQ0 35
P3V3
GND
C103 100nF
C104 100nF
SAMSUNG_K8Q2815UQBTSOP56-SOCKET
DQ[0..15]
U103
NC7SB3157
NCTRL1 3
NCE 1
SEL1 6
B0
B1
S
VCC 5
GND 2
A 4
P3V3
GND
NCE1
FAIRCHILD_NC7SB3157SC70-6
If SEL1=1 (Default) Then NCE1=NCE
Else NCE1=NCTR1
U104
NC7SB3157
NCE 3
NCTRL2 1
SEL2 6
B0
B1
S
VCC 5
GND 2
A 4
P3V3
GND
NCE2
FAIRCHILD_NC7SB3157SC70-6
If SEL2=1 (Default) Then NCE2=NCTRL2
Else NCE2=NCE
P3V3
R101 10k
RYNBY
Open Drain Output
P3V3
R102 10k
NWPACC
Write Protect Disabled
PS3 NOR Manager
Author: No_One
PNM_V1.00
22/06/2011 19:52:50
Sheet: 1/3


J201
TCK
TDO
TMS
TDI
P3V3
GND
JTAG USB-Blaster Connector (10-Pin Male Header)
P1V2A (VCCDPLL)
P2V5 (VCCA)
P3V3 (VCCIO)
P1V2 (VCCINT)
R218
4.7
P1V2
C216
100nF
GND
GPIO0
GPIO1
GPIO2
GPIO3
GPIO4
GPIO5
R201
R202
R203
R204
R205
R206
4.7
ASDOCFG
NCSOCFG
RXD
DATA0CFG
TXD
NRTS
NCTS
A[0..22]
U201
EP3C25E144
Cyclone 3 FPGA Family
Configuration LED
P3V3
R207
R208
R209
220
LED201
R210
R211
R212
R213
10k
TDO
TDI
TMS
TCK
GND
R214
R215
R216
DCLKCFG
UI Jumper
JP201
CK20M
FPGA: Active Serial Configuration (AS)
Indicator LED
R219
220
LED202
C201
C202
C203
C204
C205
C206
C207
100nF
47µF/6.3V
C208
C209
C210
C211
C212
C213
C214
P1V2
DQ[0..15]
R217
C215
U203
ASFL1
Oscillator - 20.000MHz
C217
U202
EPCS16SI8
NCS
DCLK
ASDI
DATA
VCC
ALTERA_EPCS16 Serial EEPROM
PS3 NOR Manager
Author: No_One
PNM_V1.00
22/06/2011 19:52:50
Sheet: 2/3





PS3 Connector (64-Pin Male Header)



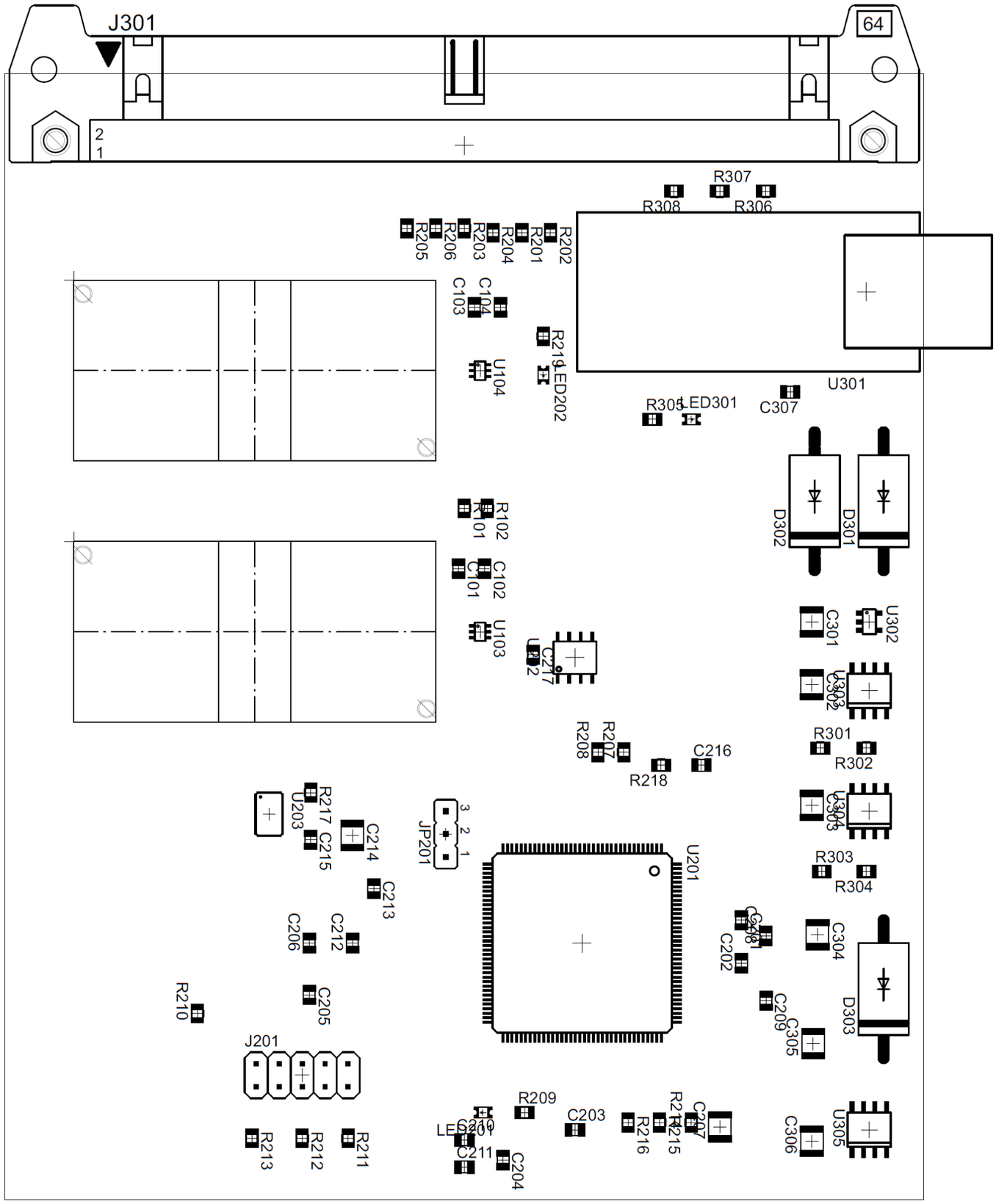
P5VUSB	P5VPS3	Output
No	No	Don't Care
No	Yes	P5VPS3
Yes	No	P5VUSB
Yes	Yes	P5VPS3

PS3 NOR Manager	Author: No_One
	PNM_V1.00
	22/06/2011 19:52:50
	Sheet: 3/3

BILL OF MATERIALS

Qty	Value	Device	Manufacturer	Parts
1		5104338-1	TE CONNECTIVITY / AMP	J201
1		09185647913	HARTING	J301
1		-	-	JP201
2		648-0562211-A01	WELLS-CTI	U101, U102
2	3.83K	MCTC0525B3831T5E	MULTICOMP	R302, R304
1	4.02K	MCTC0525B4021T5E	MULTICOMP	R303
1	6.49K	MCTC0525B6491T5E	MULTICOMP	R301
11	4R7	CRCW08054R70FKEA	VISHAY DRALORIC	R201, R202, R203, R204, R205, R206, R214, R215, R216, R217, R218
3	220R	CRCW0805220RFKEA	VISHAY DRALORIC	R209, R219, R305
11	10K	CRCW080510K0FKEA	VISHAY DRALORIC	R101, R102, R207, R208, R210, R211, R212, R213, R306, R307, R308
20	100nF/16V	CC0805KRX7R7BB104	YAGEO	C101, C102, C103, C104, C201, C202, C203, C204, C205, C206, C208, C209, C210, C211, C212, C213, C215, C216, C217, C307
8	47µF/6.3V	C1210C476M9PACTU	KEMET	C207, C214, C301, C302, C303, C304, C305, C306
3		1N5400	FAIRCHILD	D301, D302, D303
3		LGR971-Z	OSRAM	LED201, LED202, LED301
1		ASFL1-20.000MHZ-EK-T	ABRACON	U203
1		DLP-USB232M-G	DLP DESIGN / FTDI	U301
1		EP3C25E144C8N	ALTERA	U201
1		EPCS16SI8N	ALTERA	U202
2		NC7SB3157P6X	FAIRCHILD	U103, U104
1		LTC4411ES5	LINEAR TECHNOLOGY	U302
3		LT1963ES8	LINEAR TECHNOLOGY	U303, U304, U305

TOP VIEW


J301
64
2
1
R307
R308
R306
R205
R206
R203
R204
R201
R202
C104
C103
U104
R219
LED202
U301
R305
LED301
C307
D302
D301
R102
R101
C102
C101
U103
U302
C301
U303
C302
R301
R302
C216
R207
R208
R218
U304
C303
R303
R304
C304
D303
C202
C209
C305
U305
C306
U201
JP201
C214
C215
U203
R217
C213
C212
C206
C205
R210
J201
R209
C203
C207
R215
R216
LED201
C211
C204
R213
R212
R211