Side-channel Attack Standard Evaluation Board SASEBO-GII Specification

[Version 1.01]

November 30, 2009

Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology

Table of Contents

1. OVERVIEW

The SASEBO/SASEBO-G/SASEBO-B were designed and developed for the purpose of side-channel attack experiments within a single cryptographic circuit. In contrast, the SASEBO-GII is a newly developed FPGA board suitable for additional extended experiments such as one for security evaluation for a comprehensive cryptographic system combining various elemental technologies or one for a large circuit implemented with a variety of countermeasures. The board features the latest Xilinx Virtex-5 LX30/LX50 as the target FPGA for implementation evaluation that has about 4 to 7 times larger logic area than Xilinx Virtex-II pro xc2vp7 used in the SASEBO/SASEBO-G. It has gained not only extended logic area but also a mechanism that provides the user various means to access the reconfiguration function of the FPGA. In addition, based on the knowledge we obtained through experiments with the SASEBO/SASEBO-G, we have improved the board by altering the shape of the shunt-resistor for power measurement and both restricting and separating the clock source. We have also significantly simplified the experimental environment and improved the user interface by unifying the power source, configuration, and data communication within a single USB. While we have improved these functionalities, and through streamlined parts mounting technology, we have reduced the surface area of the PCB by one third.

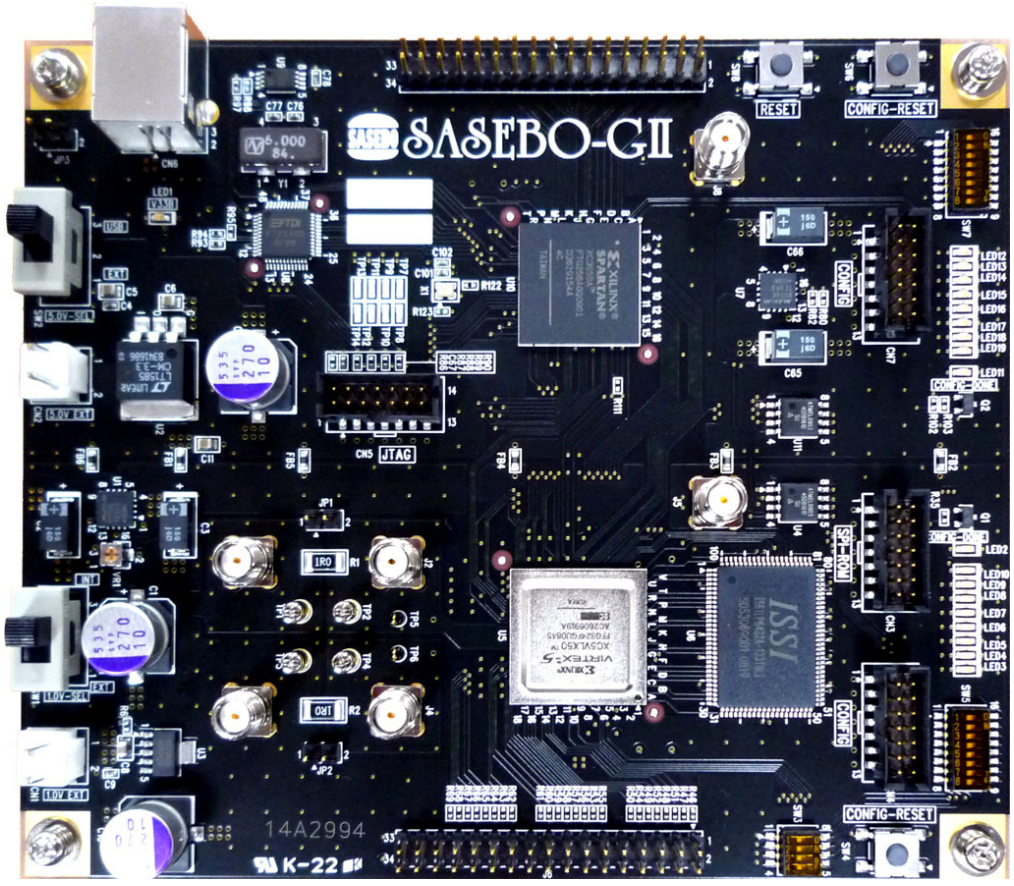


Figure 1 SASEBO-GII Top View

Figure 1 shows the top view of the board, and Figure 2 depicts its block diagram. The overview specification of the SASEBO-GII is as follows:

- 140mm x 120mm x 1.6mm, glass epoxy, eight layers

- Two Xilinx FPGAs
  - Cryptographic FPGA : XC5VLX30 or XC5VLX50 -1FFG324 (Virtex-5 series)
  - Control FPGA : XC3S400A-4FTG256 (XC3S50AN-4FT256 for initial versions) (Spartan-3A series)

  These FPGAs are connected through a 38-bit general-purpose input/output common bus with fully-flexibility in signal assignment.
- The on-board oscillator provides the control FPGA with a clock signal of 24MHz. An external clock input is also supported.
- External power source supplies the on-board power regulators and the FPGAs with 5.0 V. The power regulators convert the 5-V input into 3.3 V, 1.8 V, 1.2 V, and 1.0 V for the FPGAs. The core voltage of 1.0 V of the cryptographic FPGA can also be applied directly through the external power connector.
- Shunt resistors are provided to insert on the core VDD and/or ground lines of the cryptographic FPGA for measuring power traces.
- The host PC controls and communicates with the board via the USB port.

For Virtex-5, the cryptographic FPGA, the operable configuration methods are SPI-ROM and Slave-SelectMap. Spartan-3A, the control FPGA, controls these configuration mechanisms. This scheme makes not only dynamic reconfiguration but also static entire or partial reconfiguration possible. In addition, the SPI-ROM connected to the control FPGA has a sufficient capacity for configuring the cryptographic FPGA. We have selected the FT2232D by FTDI Inc., which is equipped with additional JTAG functions, to be the USB control IC to support FPGA configuration through JTAG without a special cable.

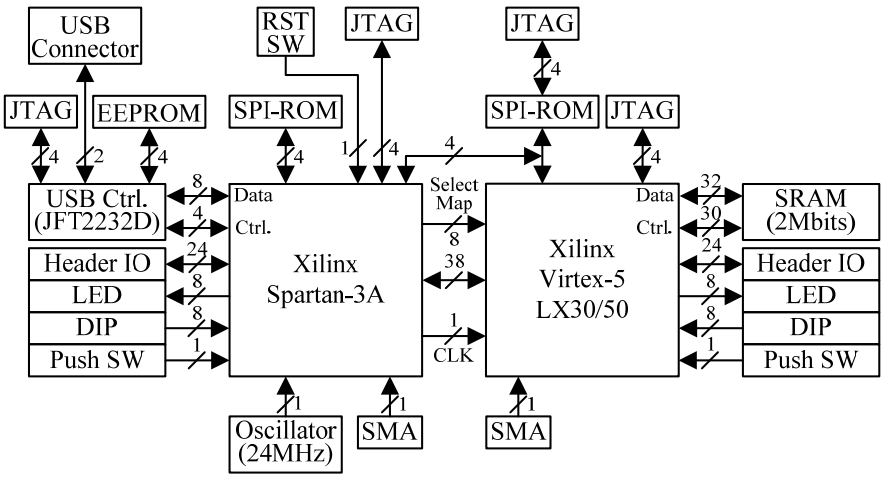


Figure 2 SASEBO-GII Block Diagram

A stable power supply is particularly important for power analysis experiments. In fact, power-equipment-related troubles occasionally occurred on the SASEBO boards at the research organizations where the boards were distributed. In addition, because off-the-shelf DC power supplies have limited portability simplifying the experimental environment has been a priority. Thus, we made a few prototypes of power supply circuit utilizing the 5-V power line of a USB port, and eventually implemented one of them onto the SASEBO-GII. Initially, the SASEBO boards required a stabilized power supply with a current of 2.0 A or higher. However, detailed power consumption observations revealed that the 2.0A of current was only required during power-on and FPGA configuration. By adding a capacitor sufficient to supply that current flow, we significantly reduced the power requirement. However, two additional problems with the USB power supply surfaced: relatively large noise content and a limited current capacity of 500 mA. To address these problems, we formulated the following three conditions through a few prototypes, and designed a circuit meeting these conditions, so that supplying

low-noise power via USB has become possible.

- For noise isolation, an inductor shall be inserted in each of the 3.3-V and GND lines of the power supplied to the target FPGA.
- A 100 uF or larger ceramic capacitor, or a 330 uF or larger electrolytic capacitor shall be placed in the output stage.
- A 0.1 uF or larger ceramic capacitor shall be placed in the input stage. If the linear regulator has a limited quality, a further increase in capacitance in accordance with the quality shall be given.

Figure represents the trial USB power supply circuit designed to determine the best method for supplying power to the SASEBO-GII. Figure 4 is the photograph of its experimental implementation on the SASEBO-R.

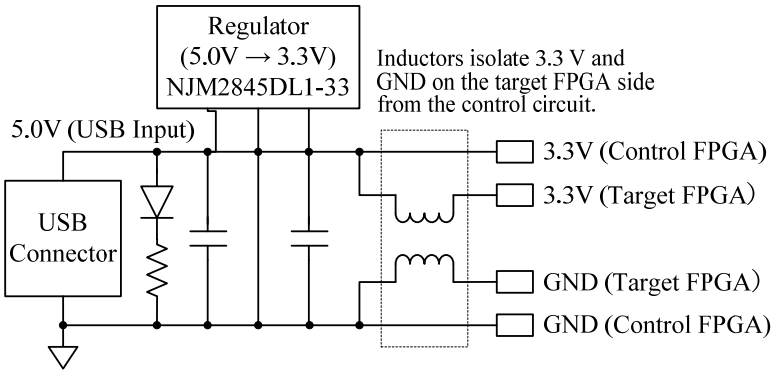


Figure 3　USB power supply circuit diagram

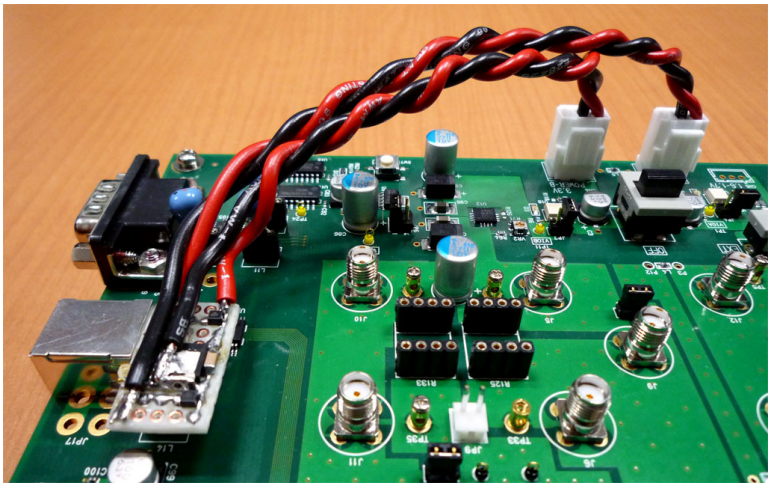


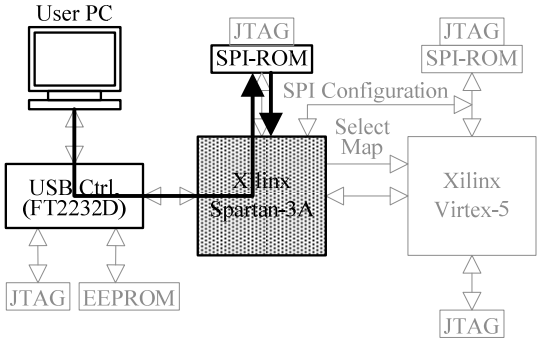
Figure 4　USB power supply circuit experimentally implemented on the SASEBO-GII

The board also features ability for hosting extra experiments enabled by the Virtex-5; it houses an embedded processor, connects with an on-board SRAM for storing data, and has the pins assigned to user I/Os including power lines and a pair of dedicated clock lines. These allow the board to add other interfaces for extra experiments such as a DAC/ADC for software radio or an Ethernet controller for network filtering. Spartan-3A also has a similar user I/O including connection to the USB interface through which the host computer controls and communicates with the board. The USB control IC and the bus connecting between the both FPGAs are compatible with those of the preceding boards so that it is possible to reutilize the control circuits, software and analysis tool already developed for the boards. To improve frequency characteristics for power measurement, in addition to the similar probing points as

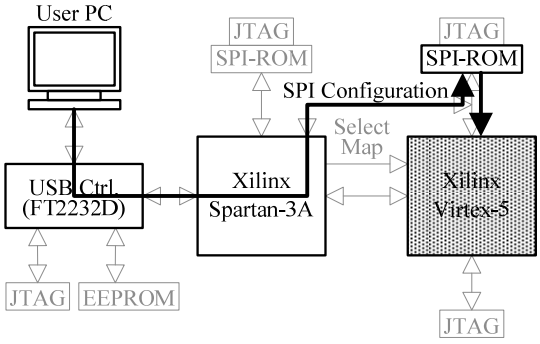
other SASEBO boards, the SASEBO-GII has chip-form shunt resistors instead of radial-lead ones, and SMA receptacles for jumpers instead of header pins.

The configuration mechanisms, such as SelectMap, SPI-ROM and JTAG, usable on the SASEBO-GII are flexibly selective in accordance with the applications making use of the reconfiguration function of the FPGA, by configuring Spartan-3A with an appropriate circuit. Figure 5(a) and (b) depict the static reconfiguration paths where the user PC reprograms the SPI-ROM of Spartan-3A and Virtex-5, respectively, via USB. Figure 5(c) shows the other path where the user PC reconfigures Virtex-5 directly and quickly with the power kept on, through 8-bit-wide SelectMap. Supported by Virtex-5, the dynamic partial reconfiguration path shown in Figure 5(d) changes the corresponding logic part contained in the FPGA through the 32-bit bus without suspending the external I/O.

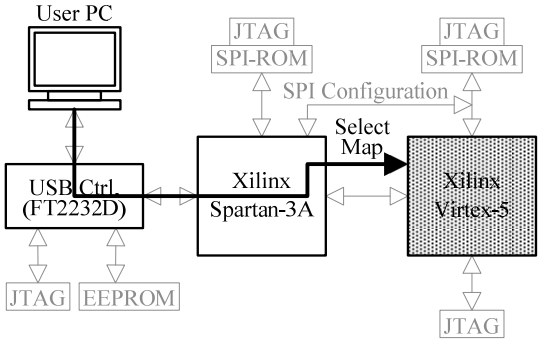
(a) Static Reconfiguration of Spartan-3 from ROM



(b) Static Reconfiguration of Virtex-5 from ROM



(c) Static Reconfiguration of Virtex-5



(d) Dynamic Partial Reconfiguration of Virtex-5

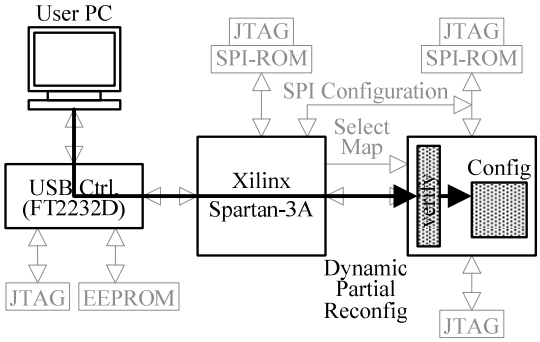


Figure 5 FPGA Configuration Paths

2. I/O SIGNAL OF THE FPGAS

- Pin assignments of the cryptographic FPGA (U5)

Table 1 Basic Control Signals

Signal Name	Pin Number	Input/Output	Description/Destination
VIR5_CONFD0	P12	IO	Config
VIR5_CONFD1	P13	IO	Config
VIR5_CONFD2	M11	IO	Config
VIR5_CONFD3	N11	IO	Config
VIR5_CONFD4	T13	IO	Config
VIR5_CONFD5	T14	IO	Config
VIR5_CONFD6	M10	IO	Config
VIR5_CONFD7	N10	IO	Config
VIR5_BUSY	T6	IO	Config
VIR5_INITB	M8	IO	Config
VIR5_PROGB	U18	IO	Config
VIR5_DONE	P8	IO	Config
VIR5_CSB	R16	O	Config
VIR5_RDWRB	P15	IO	Config
VIRT5_CCLK	N8	IO	Config
VIRT5-D_IN	R7	O	Config
VIRT5-MOSI	P9	O	Config
VIRT5-FCS_B	P10	O	Config
M0	N12	I	SW3-8
M1	L11	I	SW3-7
M2	N13	I	SW3-6
TCK	M9	--	JTAG
TDI	U5	--	JTAG
TDO	U6	--	JTAG
TMS	V5	--	JTAG
HSWAP_EN	T17	I	PU-R
VBATT	T18	I	PU-R
DXP	L10	NC	NC
DXN	L9	NC	NC
VREFP	K10	--	PU-R
VREFN	J9	--	PU-R
RSVD	P14	NC	NC
RSVD	R14	NC	NC

Table 2 Control FPGA I/F

Signal Name	Pin Number	Input/Output	Destination(U10)
VIR5-UD0	N17	IO	F13
VIR5-UD1	P17	IO	E14
VIR5-UD2	M16	IO	D15
VIR5-UD3	M18	IO	D16
VIR5-UD4	V16	IO	D14
VIR5-UD5	P18	IO	E13
VIR5-UD6	N18	IO	C15
VIR5-UD7	U16	IO	C13

VIR5-UD8	V18	IO	D13
VIR5-UD9	T16	IO	B14
VIR5-UD10	V17	IO	B15
VIR5-UD11	U15	IO	D11
VIR5-UD12	V15	IO	C12
VIR5-UD13	M15	IO	A13
VIR5-UD14	N16	IO	A14
VIR5-UD15	R17	IO	A11
VIR5-UD16	U14	IO	C11
VIR5-UD17	R15	IO	A10
VIR5-UD18	N15	IO	B10
VIR5-UD19	V13	IO	D9
VIR5-UD20	M14	IO	A9
VIR5-UD21	U13	IO	C9
VIR5-UD22	V12	IO	D8
VIR5-UD23	T12	IO	C8
VIR5-UD24	V11	IO	B8
VIR5-UD25	M13	IO	A8
VIR5-UD26	V10	IO	B6
VIR5-UD27	U10	IO	A6
VIR5-UD28	T9	IO	C6
VIR5-UD29	R12	IO	D7
VIR5-UD30	T8	IO	C5
VIR5-UD31	U9	IO	A5
VIR5-UD32	U8	IO	B4
VIR5-UD33	V8	IO	A4
VIR5-UD34	V6	IO	B3
VIR5-UD35	V7	IO	A3
VIR5-UD36	R9	IO	D5
VIR5-UD37	T7	IO	C4

Table 3 Monitor Signals

Signal Name	Pin Number	Input/Output	Description/Destination
LED0	F11	OUT	LED3
LED1	G11	OUT	LED4
LED2	G10	OUT	LED5
LED3	F9	OUT	LED6
LED4	E12	OUT	LED7
LED5	D12	OUT	LED8
LED6	F8	OUT	LED9
LED7	G9	OUT	LED10
DIPSW1	A8	IN	SW5-1
DIPSW2	A9	IN	SW5-2
DIPSW3	B9	IN	SW5-3
DIPSW4	B10	IN	SW5-4
DIPSW5	E9	IN	SW5-5
DIPSW6	D9	IN	SW5-6
DIPSW7	E10	IN	SW5-7
DIPSW8	E11	IN	SW5-8
RESET-CONFIG	U18	IN	SW4

Table 4 General Purpose Monitor Pins

Signal Name	Pin Number	Input/Output	Description/Destination
EXT-D0	A13	IO	J6-1
EXT-D1	B13	IO	J6-2
EXT-D2	A14	IO	J6-3
EXT-D3	B14	IO	J6-4
EXT-D4	B15	IO	J6-5
EXT-D5	A16	IO	J6-6
EXT-D6	B16	IO	J6-7
EXT-D7	A17	IO	J6-8
EXT-D8	A18	IO	J6-11
EXT-D9	B18	IO	J6-12
EXT-D10	C17	IO	J6-13
EXT-D11	C18	IO	J6-14
EXT-D12	D17	IO	J6-15
EXT-D13	D18	IO	J6-16
EXT-D14	E17	IO	J6-17
EXT-D15	E16	IO	J6-18
EXT-D16	F18	IO	J6-21
EXT-D17	F17	IO	J6-22
EXT-D18	C15	IO	J6-23
EXT-D19	C16	IO	J6-24
EXT-D20	D15	IO	J6-25
EXT-D21	D14	IO	J6-26
EXT-D22	E15	IO	J6-27
EXT-D23	E14	IO	J6-28
EXTPORT-CLKP	A6	IO	J6-31
EXTPORT-CLKN	A7	IO	J6-32

Table 5 Memory I/F

Signal Name	Pin Number	Input/Output	Destination(U6)
SRAM-A0	F1	OUT	37
SRAM-A1	F3	OUT	36
SRAM-A2	G1	OUT	35
SRAM-A3	G4	OUT	34
SRAM-A4	H1	OUT	33
SRAM-A5	H3	OUT	32
SRAM-A6	V1	OUT	100
SRAM-A7	T4	OUT	99
SRAM-A8	K1	OUT	82
SRAM-A9	J2	OUT	81
SRAM-A10	B5	OUT	44
SRAM-A11	B4	OUT	45
SRAM-A12	C3	OUT	46
SRAM-A13	D3	OUT	47
SRAM-A14	E4	OUT	48
SRAM-A15	E1	OUT	49
SRAM-ADSC_N	L2	IO	85
SRAM-ADSP_N	L1	IO	84
SRAM-ADV_N	K2	IO	83

SRAM-BW1_N	M1	IO	93
SRAM-BW2_N	M3	IO	94
SRAM-BW3_N	N1	IO	95
SRAM-BW4_N	N3	IO	96
SRAM-BWE_N	V3	IO	87
SRAM-CE_N	T1	IO	98
SRAM-CE2	P3	IO	97
SRAM-CLK	V2	IO	89
SRAM-DQA0	A2	IO	52
SRAM-DQA1	A1	IO	53
SRAM-DQA2	B1	IO	56
SRAM-DQA3	C2	IO	57
SRAM-DQA4	C1	IO	58
SRAM-DQA5	D4	IO	59
SRAM-DQA6	E5	IO	62
SRAM-DQA7	F4	IO	63
SRAM-DQB0	J4	IO	68
SRAM-DQB1	J3	IO	69
SRAM-DQB2	L3	IO	72
SRAM-DQB3	M5	IO	73
SRAM-DQB4	N5	IO	74
SRAM-DQB5	P4	IO	75
SRAM-DQB6	R4	IO	78
SRAM-DQB7	T3	IO	79
SRAM-DQC0	U1	IO	2
SRAM-DQC1	T2	IO	3
SRAM-DQC2	R2	IO	6
SRAM-DQC3	P2	IO	7
SRAM-DQC4	N2	IO	8
SRAM-DQC5	M4	IO	9
SRAM-DQC6	L4	IO	12
SRAM-DQC7	K4	IO	13
SRAM-DQD0	H2	IO	18
SRAM-DQD1	G3	IO	19
SRAM-DQD2	F2	IO	22
SRAM-DQD3	E2	IO	23
SRAM-DQD4	D2	IO	24
SRAM-DQD5	C5	IO	25
SRAM-DQD6	B3	IO	28
SRAM-DQD7	A3	IO	29
SRAM-GW_N	U3	IO	88
SRAM-MODE	A4	IO	31
SRAM-OE_N	U4	IO	86
SRAM-ZZ	G5	IO	64

- Pin assignments of the control FPGA (U10)

Table 6 FPGA Configuration Signals

Signal Name	Pin Number	Input/Output	Description/Destination
D0/MISO	T14	IO	SPI-ROM
CCLK	R14	IO	SPI-ROM
MOSI/CSIB	P10	IO	SPI-ROM
CSOB	T2	IO	SPI-ROM

GCLK2	R9	IO	CLOCK
VIR5_CONFD0	K15	O	Config
VIR5_CONFD1	K14	O	Config
VIR5_CONFD2	K16	O	Config
VIR5_CONFD3	J16	O	Config
VIR5_CONFD4	J14	O	Config
VIR5_CONFD5	H14	O	Config
VIR5_CONFD6	H15	O	Config
VIR5_CONFD7	H16	O	Config
VIR5_BUSY	K12	I	Config
VIR5_INITB	N16	O	Config
VIR5_PROGB	T13	O	Config
VIR5_DONE	P16	I	Config
VIR5_CSB	J13	I	Config
VIR5_RDWRB	J12	IO	Config
VIRT5_CCLK	N13	I	Config
VIRT5-D_IN	N14	I	Config
VIRT5-MOSI	P15	I	Config
VIRT5-FCS_B	R15	I	Config
PROG_B	A2	--	Config
DONE	T15	--	Config
M0	P4	IN	PU-R
M1	N4	IN	PD-R
M2	R2	IN	PD-R
TCK	A15	--	JTAG
TDI	B1	--	JTAG
TDO	B16	--	JTAG
TMS	B2	--	JTAG
VS0	P5	IN	PU-R
VS1	N6	IN	PD-R
VS2	T3	IN	PU-R

Table 7 Cryptographic FPGA I/F

Signal Name	Pin Number	Input/Output	Destination(U5)
VIR5-UD0	F13	IO	N17
VIR5-UD1	E14	IO	P17
VIR5-UD2	D15	IO	M16
VIR5-UD3	D16	IO	M18
VIR5-UD4	D14	IO	V16
VIR5-UD5	E13	IO	P18
VIR5-UD6	C15	IO	N18
VIR5-UD7	C13	IO	U16
VIR5-UD8	D13	IO	V18
VIR5-UD9	B14	IO	T16
VIR5-UD10	B15	IO	V17
VIR5-UD11	D11	IO	U15
VIR5-UD12	C12	IO	V15
VIR5-UD13	A13	IO	M15
VIR5-UD14	A14	IO	N16
VIR5-UD15	A11	IO	R17
VIR5-UD16	C11	IO	U14
VIR5-UD17	A10	IO	R15
VIR5-UD18	B10	IO	N15
VIR5-UD19	D9	IO	V13

VIR5-UD20	A9	IO	M14
VIR5-UD21	C9	IO	U13
VIR5-UD22	D8	IO	V12
VIR5-UD23	C8	IO	T12
VIR5-UD24	B8	IO	V11
VIR5-UD25	A8	IO	M13
VIR5-UD26	B6	IO	V10
VIR5-UD27	A6	IO	U10
VIR5-UD28	C6	IO	T9
VIR5-UD29	D7	IO	R12
VIR5-UD30	C5	IO	T8
VIR5-UD31	A5	IO	U9
VIR5-UD32	B4	IO	U8
VIR5-UD33	A4	IO	V8
VIR5-UD34	B3	IO	V6
VIR5-UD35	A3	IO	V7
VIR5-UD36	D5	IO	R9
VIR5-UD37	C4	IO	T7
SP3-VIR5_24MCLK	C16	O	U11

Table 8 Monitor Signals

Signal Name	Pin Number	Input/Output	Destination
LED0	U10.T10	OUT	LED12
LED1	U10.R11	OUT	LED13
LED2	U10.T11	OUT	LED14
LED3	U10.N11	OUT	LED15
LED4	U10.P11	OUT	LED16
LED5	U10.P12	OUT	LED17
LED6	U10.T12	OUT	LED18
LED7	U10.R13	OUT	LED19
DIPSW1	U10.F4	IN	SW7.16
DIPSW2	U10.E4	IN	SW7.15
DIPSW3	U10.J7	IN	SW7.14
DIPSW4	U10.H7	IN	SW7.13
DIPSW5	U10.K6	IN	SW7.12
DIPSW6	U10.K5	IN	SW7.11
DIPSW7	U10.L6	IN	SW7.10
DIPSW8	U10.L5	IN	SW7.9
PUSH	N10.L7	IN	SW8

Table 9 General Purpose Monitor Pins

Signal Name	Pin Number	Input/Output	Description/Destination
FPGAB-D0	U10.C1	IO	J9-1
FPGAB-D1	U10.C2	IO	J9-2
FPGAB-D2	U10.D3	IO	J9-3
FPGAB-D3	U10.D4	IO	J9-4
FPGAB-D4	U10.E1	IO	J9-5
FPGAB-D5	U10.D1	IO	J9-6
FPGAB-D6	U10.G1	IO	J9-7
FPGAB-D7	U10.F1	IO	J9-8
GND		IO	J9-9
GND		IO	J9-10
FPGAB-D8	U10.H1	IO	J9-11

FPGAB-D9	U10.G2	IO	J9-12
FPGAB-D10	U10.J3	IO	J9-13
FPGAB-D11	U10.H3	IO	J9-14
FPGAB-D12	U10.J1	IO	J9-15
FPGAB-D13	U10.J2	IO	J9-16
FPGAB-D14	U10.K1	IO	J9-17
FPGAB-D15	U10.K3	IO	J9-18
GND		IO	J9-19
GND		IO	J9-20
FPGAB-D16	U10.L2	IO	J9-21
FPGAB-D17	U10.L1	IO	J9-22
FPGAB-D18	U10.J6	IO	J9-23
FPGAB-D19	U10.J4	IO	J9-24
FPGAB-D20	U10.L3	IO	J9-25
FPGAB-D21	U10.K4	IO	J9-26
FPGAB-D22	U10.L4	IO	J9-27
FPGAB-D23	U10.M3	IO	J9-28
GND		IO	J9-29
GND		IO	J9-30
FPGAB-XCLKN	U10.P9	IO	J9-31
FPGAB-XCLKP	U10.N9	IO	J9-32
V33B		IO	J9-33
V33B		IO	J9-34

Table 10 USB I/F

Signal Name	Pin Number	Input/Output	Destination
USBBDBUS0	U10.R3	IO	U8.40
USBBDBUS1	U10.R5	IO	U8.39
USBBDBUS2	U10.T4	IO	U8.38
USBBDBUS3	U10.T6	IO	U8.37
USBBDBUS4	U10.T5	IO	U8.36
USBBDBUS5	U10.N8	IO	U8.35
USBBDBUS6	U10.P7	IO	U8.33
USBBDBUS7	U10.T8	IO	U8.32
USBBCBUS0	U10.P2	IO	U8.30
USBBCBUS1	U10.R1	IO	U8.29
USBBCBUS2	U10.M4	IO	U8.28
USBBCBUS3	U10.N3	IO	U8.27
V33B	--	--	U8.26

3. BOARD CONFIGURATION

- Power Circuit

Figure 6 shows the power circuit block diagram of the SASEBO-GII. Table 11 represents the power connector settings on SW1 and SW2. Figure 7 illustrates the power initiation sequences involving each power line. For supplying the entire board with power via USB, SW1 and SW2 shall be turned to INT. Otherwise, SW2 shall be turned to EXT with CN2 supplied with 5.0 VDC. SW1 shall be toggled to EXT to optionally supply the cryptographic FPGA core voltage of 1.0 V through CN1. The power must be off when SW1 or SW2 is turned. LED1 turns on to indicate that the 5.0 VDC is supplied through either USB(CN6) or external source(CN2).

Table 11 Power Settings

Selection SW	SW2		SW1	
	INT	EXT	INT	EXT
Power Source	USB (CN6) : 5V	CN2 : 5V	Regulator U1 : 1V	CN1 : 1V
Description	USB Power for Control/Cryptographic FPGA	External Power for Control/Cryptographic FPGA	Internal Series Power Supply for Cryptographic FPGA Core	External Power for Cryptographic FPGA Core

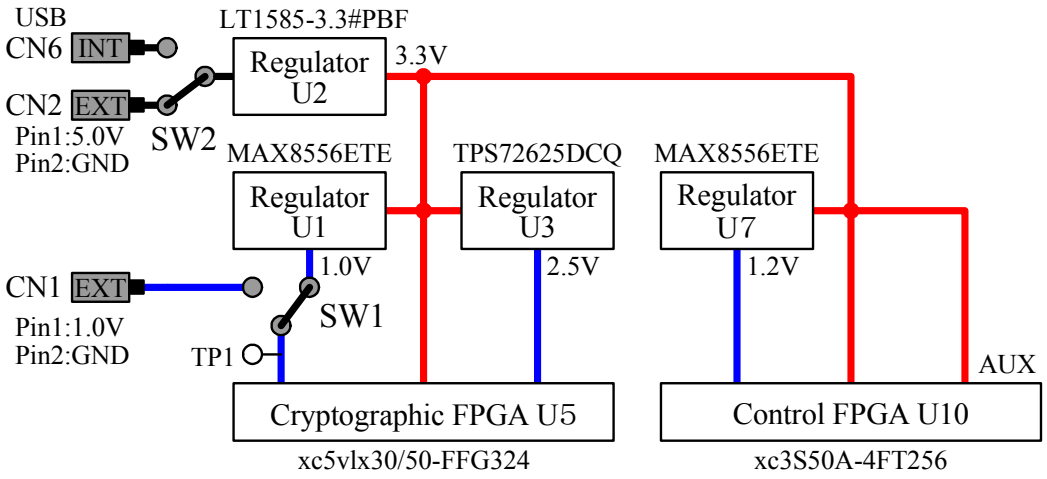


Figure 6 Power Circuit Block Diagram

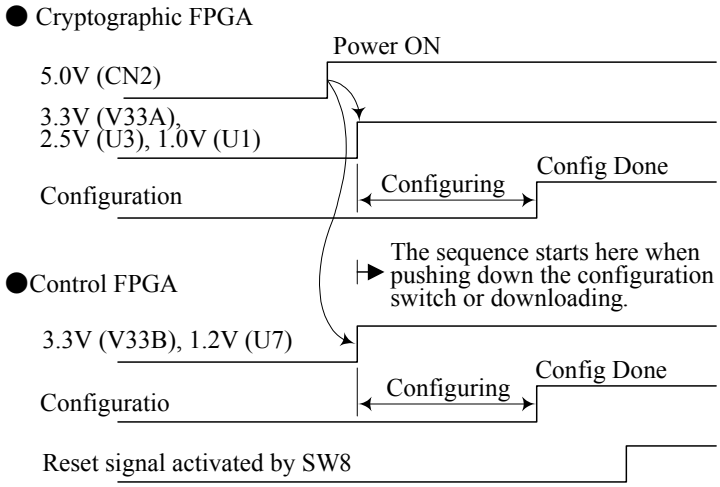


Figure 7 Power-On Sequences

- Jumper Settings

Table 12 Jumper Settings

Purpose	Pin Number	State	Description
USB-CASE Connection	JP3	Short	Connects the USB connector case to GND.
		Open	Makes no connections for the USB connector case.
Power Trace Measurement Settings	JP1	Short	Bypasses the core-power-side shunt resistor R1 for the cryptographic FPGA
		Open	Enables the core-power-side shunt resistor R1 for the cryptographic FPGA
	JP2	Short	Bypasses the core-power-side shunt resistor R2 for the control FPGA
		Open	Enables the core-power-side shunt resistor R2 for the control FPGA

- Configuration

Figure 8 shows JTAG chain schematics. The cryptographic FPGA (U5) and control the FPGA (U10) each have connector CN3 and CN7 for programming, respectively, and the SPI-ROM U4 and U11, respectively. Table 13 shows pin assignments for the JTAG connectors. Table 14 shows mode settings for SW3, the mode selection DIP switch for the cryptographic FPGA (The control FPGA is fixed to the SPI mode). For each FPGA, when configuration from SPI-ROM is successfully done, the LED2 or LED11 lit. Pressing SW4 or SW8 initiates reconfiguration of the corresponding FPGA from the SPI-ROM.

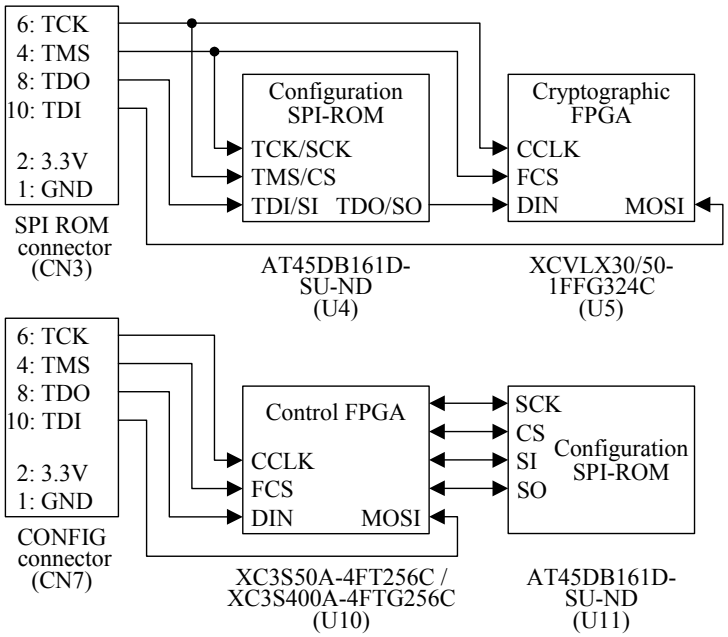


Figure 8 JTAG Chains

Table 13 Pin Assignment of the JTAG/CONFIG Connector

Pin1	GND	Pin2	3.3V
Pin3	GND	Pin4	TMS
Pin5	GND	Pin6	TCK
Pin7	GND	Pin8	TDO
Pin9	GND	Pin10	TDI
Pin11	GND	Pin12	NC
Pin13	GND	Pin14	NC

Table 14 Mode Settings on the Mode Selection DIP Switch SW3

Dip1	M0	ON
Dip2	M1	ON
Dip3	M2	ON
Dip4	NC	OFF

- Clock System

The clock source connection of the SASEBO-GII is shown in Figure 9. The on-board 24-MHz oscillator X1 connects with the control FPGA. It provides the cryptographic FPGA with a clock signal through the control FPGA. An external clock source may supply each of the FPGAs via SMA connector J3 or J4.

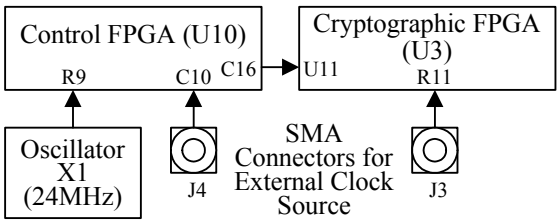


Figure 9 Clock System

- Host Interface

A USB interface is provided on the SASEBO-GII for communication with the host PC. Table 15 shows the signal assignments of the USB interface circuit.

Table 15 USB Interface Signals

Signal Name	CN6 (XM7B-0442)	U8 (FT2232D)	U10 (XC3S50A-FT256 / XC3S400A-FTG256)
USBDM	2 pin	8 pin	-
USBDP	3 pin	7 pin	-
USBBDBUS0	-	40 pin	U10.R3
USBBDBUS1	-	39 pin	U10.R5
USBBDBUS2	-	38 pin	U10.T4
USBBDBUS3	-	37 pin	U10.T6
USBBDBUS4	-	36 pin	U10.T5
USBBDBUS5	-	35 pin	U10.N8
USBBDBUS6	-	33 pin	U10.P7
USBBDBUS7	-	32 pin	U10.T8
USBBCBUS0	-	30 pin	U10.P2
USBBCBUS1	-	29 pin	U10.R1
USBBCBUS2	-	28 pin	U10.M4
USBBCBUS3	-	27 pin	U10.N3
FT2232-TCK	-	24 pin	-
FT2232-TDI	-	23 pin	-
FT2232-TDO	-	22 pin	-
FT2232-TMS	-	21 pin	-
FT2232-GPIOH0	-	15 pin	-
FT2232-GPIOH1	-	13 pin	-
FT2232-GPIOH2	-	12 pin	-
FT2232-GPIOH3	-	11 pin	-
FT2232-GPIOL0	-	20 pin	-
FT2232-GPIOL1	-	19 pin	-
FT2232-GPIOL2	-	17 pin	-
FT2232-GPIOL3	-	16 pin	-

4. PARTS LIST, CIRCUIT DIAGRAM, AND BOARD LAYOUT

The parts list for the SASEBO-GII is shown in Table 16. The board schematics and layouts of the SASEBO-GII are presented on pages 17 to 18.

Table 16　Parts List

Board name	SASEBO-GII			
Description	Part Number	Maker	Qty	Reference Designator
Ceramic Capacitor	GRM155B11A104K	MURATA	54	C4,C9,C53,C54,C55,C56, C57,C58,C59,C60,C61,C62, C63,C64,C67,C69,C70,C71, C72,C73,C75,C78,C79,C80, C81,C82,C83,C84,C85,C86, C87,C88,C89,C90,C91,C93, C94,C95,C96,C97,C98,C99, C100,C101,C103,C104,C105, C106,C107,C108,C109,C110, C111,C112
Ceramic Capacitor	GRM219B31A106K	MURATA	9	C5,C6,C8,C11,C39,C40,C41, C68,C92
Ceramic Capacitor	GRM155B11A104K	MURATA	38	C12,C13,C14,C15,C16,C17, C18,C19,C20,C21,C22,C23, C24,C25,C26,C27,C28,C29, C30,C31,C32,C33,C34,C35, C36,C37,C38,C42,C43,C44, C45,C46,C47,C48,C49,C50, C51,C52
Ceramic Capacitor	C3216JB0J336M	TDK	1	C74
Ceramic Capacitor	GRM1552C1H270JZ01D	MURATA	2	C76,C77
Ceramic Capacitor	GRM155B31A105KE15D	MURATA	1	C102
OS Capacitor	10SVP270M	SANYO	3	C1,C7,C10
Electrolytic Capacitor	6PTB150M	SANYO	4	C2,C3,C65,C66
LED	SML-310MTT86	ROHM	19	LED1,LED2,LED3,LED4,LED5, LED6,LED7,LED8,LED9, LED10,LED11,LED12,LED13, LED14,LED15,LED16,LED17, LED18,LED19
Ferrite Bead	MPZ1608S600A	TDK	6	FB1,FB2,FB3,FB4,FB5,FB6
Regulator IC	LT1585CM-3.3#PBF	LTC	1	U2
Regulator IC	TPS72625DCQ	TI	1	U3
Regulator IC	MAX8556ETE+	MAXIM	2	U1,U7
FPGA	XC5VLX30-1FFG324	XILINX	1	U5
FPGA	XC3S400A-4FT256 / XC3S400A-FTG256	XILINX	1	U10
ROM	AT45DB161D-SU-ND	ATMEL	2	U4,U11
SRAM	IS61LP6432A-133TQ-ND	ISSI	1	U6
USB IC	FT2232D	FTDI	1	U8
SROM	93LC46B_IST	MICROCHIP	1	U9
Crystal Oscillator	ECS	ECS	1	X1
Crystal Oscillator	NX1255GB	NDK	1	Y1
Connector	B2P	JST	2	CN1,CN2
Connector	87832	MOLEX	4	CN3,CN4,CN5,CN7
Connector	XM7B-0442	OMRON	1	CN6
Shunt	XG8S-0231	OMRON	3	JP1,JP2,JP3

Jumper Socket	HIF3GA-2.54SP	HIROSE	1	JS1
SMA Socket	T124 426 000N		6	J1,J2,J3,J4,J5,J8
Connector	A1-34PA-2.54DSA	HIROSE	2	J6,J9
Transistor	2SC2712BL	TOSHIBA	2	Q1,Q2
Resistor	RK73BW2HTTD1R0J	KOA	2	R1,R2
Resistor	RK73B1ETTP472J	KOA	59	R3,R10,R11,R12,R13,R14, R16,R17,R18,R19,R20,R27, R28,R29,R30,R31,R32,R34, R35,R36,R37,R38,R39,R40, R41,R42,R43,R44,R80,R81, R83,R84,R85,R92,R99,R100, R103,R104,R105,R106,R108, R109,R113,R114,R117,R118, R121,R124,R125,R126,R127, R128,R129,R130,R131,R132, R133,R135,R136
Resistor	RK73B1ETTP102J	KOA	2	R4,R6
Resistor	RK73B1JTTD151J	KOA	19	R5,R33,R72,R73,R74,R75, R76,R77,R78,R79,R101, R137,R138,R139,R140,R141, R142,R143,R144
Resistor	RK73H1ETTP1000F	KOA	2	R7,R8
Resistor	RK73B1ETTP220J	KOA	35	R9,R25,R46,R47,R48,R49, R50,R51,R52,R53,R54,R55, R56,R57,R58,R59,R60,R61, R62,R63,R64,R65,R66,R67, R68,R69,R70,R71,R86,R87, R88,R89,R90,R111,R122
Resistor	RK73B1ETTP331J	KOA	2	R15,R102
Resistor	MCR01MZPJ000	ROHM	16	R21,R22,R23,R24,R26,R45, R96,R107,R110,R112,R115, R116,R119,R120,R123,R134
Resistor	RK73B1ETTP332J	ROHM	1	R82
Resistor	RK73B1ETTP471J	ROHM	1	R91
Resistor	RK73B1ETTP270J	ROHM	2	R93,R94
Resistor	RK73B1ETTP152J	ROHM	1	R95
Resistor	RK73B1ETTD103J	ROHM	1	R97
Resistor	RK73H1ETTP2201F	ROHM	1	R98
Trimmer	ST-32ETA 2kΩ	COPAL	1	VR1
Switch, Slide	CS-12AAP1	NIKKAI	2	SW1,SW2
DIP Switch	CHS-04B	COPAL	1	SW3
Push Button	B3FS-1000	OMRON	3	SW4,SW6,SW8
DIP Switch	CHS-08B	COPAL	2	SW5,SW7
Terminal	MM-2-1	MAC8	4	TP1,TP2,TP3,TP4
Terminal	LC-33-G-KURO	MAC8	2	TP5,TP6

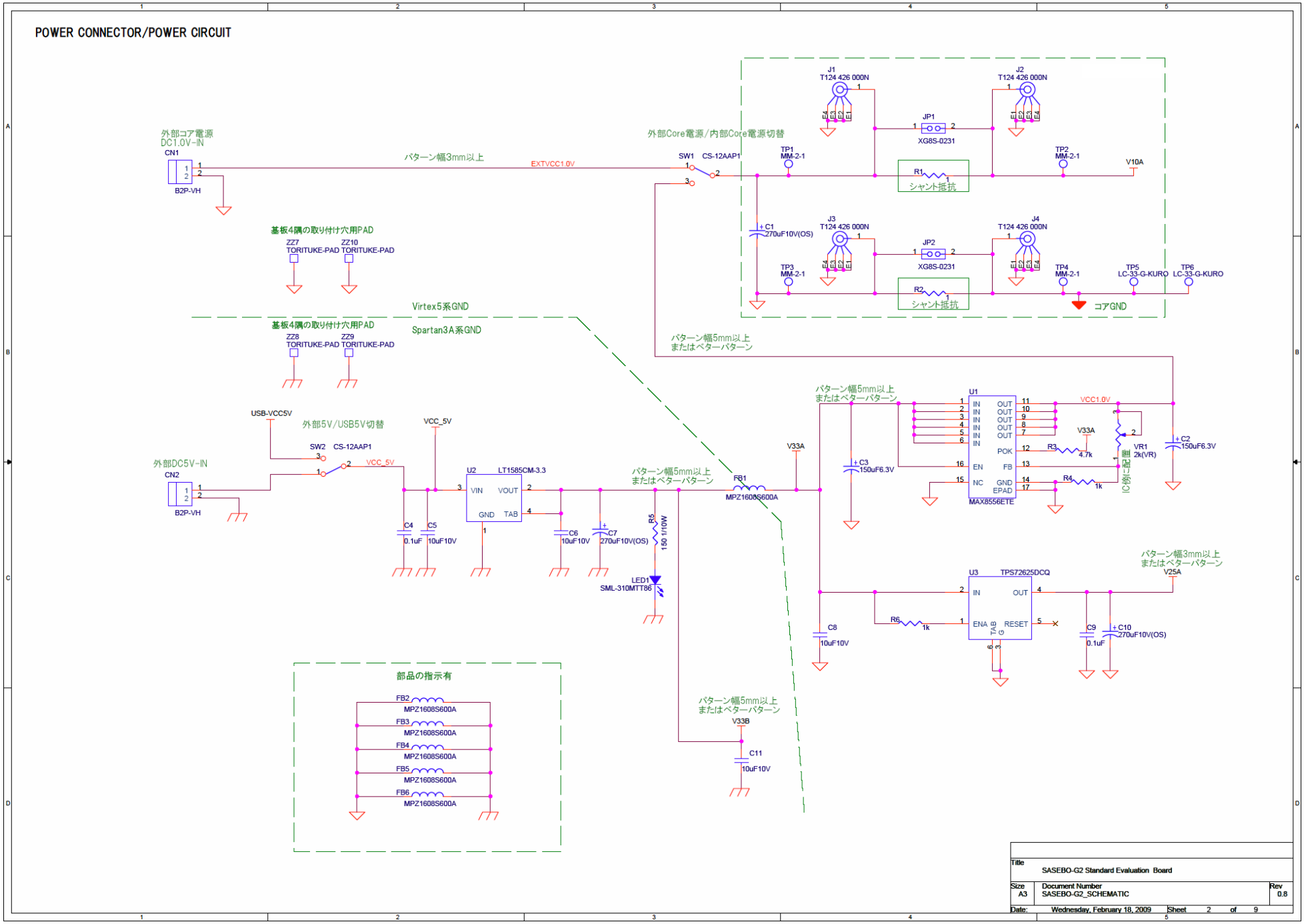


Figure 10 Cryptographic FPGA Block − Power Connectors, Core Power Circuit

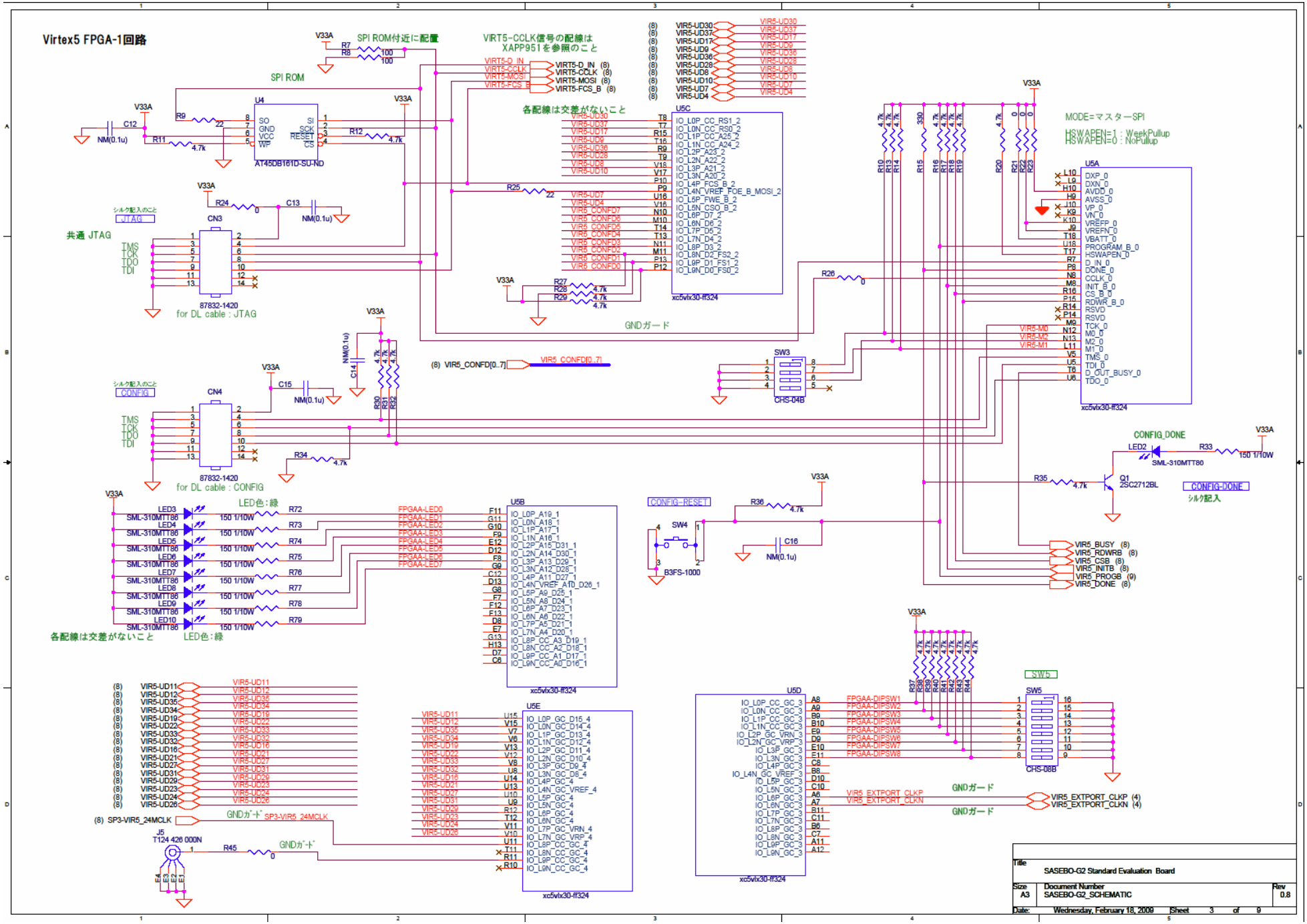


Figure 11 Cryptographic FPGA Block − FPGA I/O, Power Circuit, FPGA Configuration

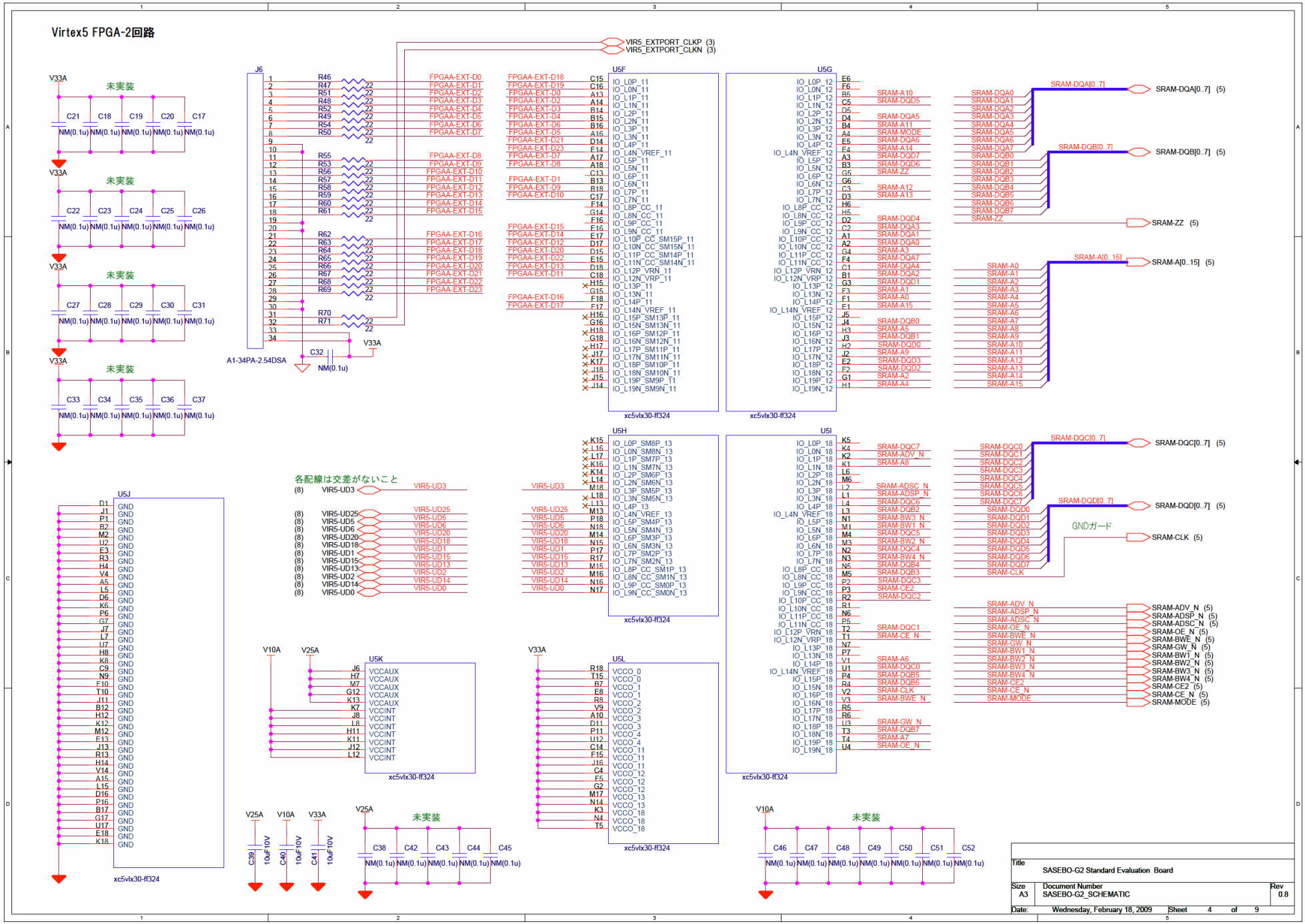


Figure 12 Cryptographic FPGA Block − FPGA I/O

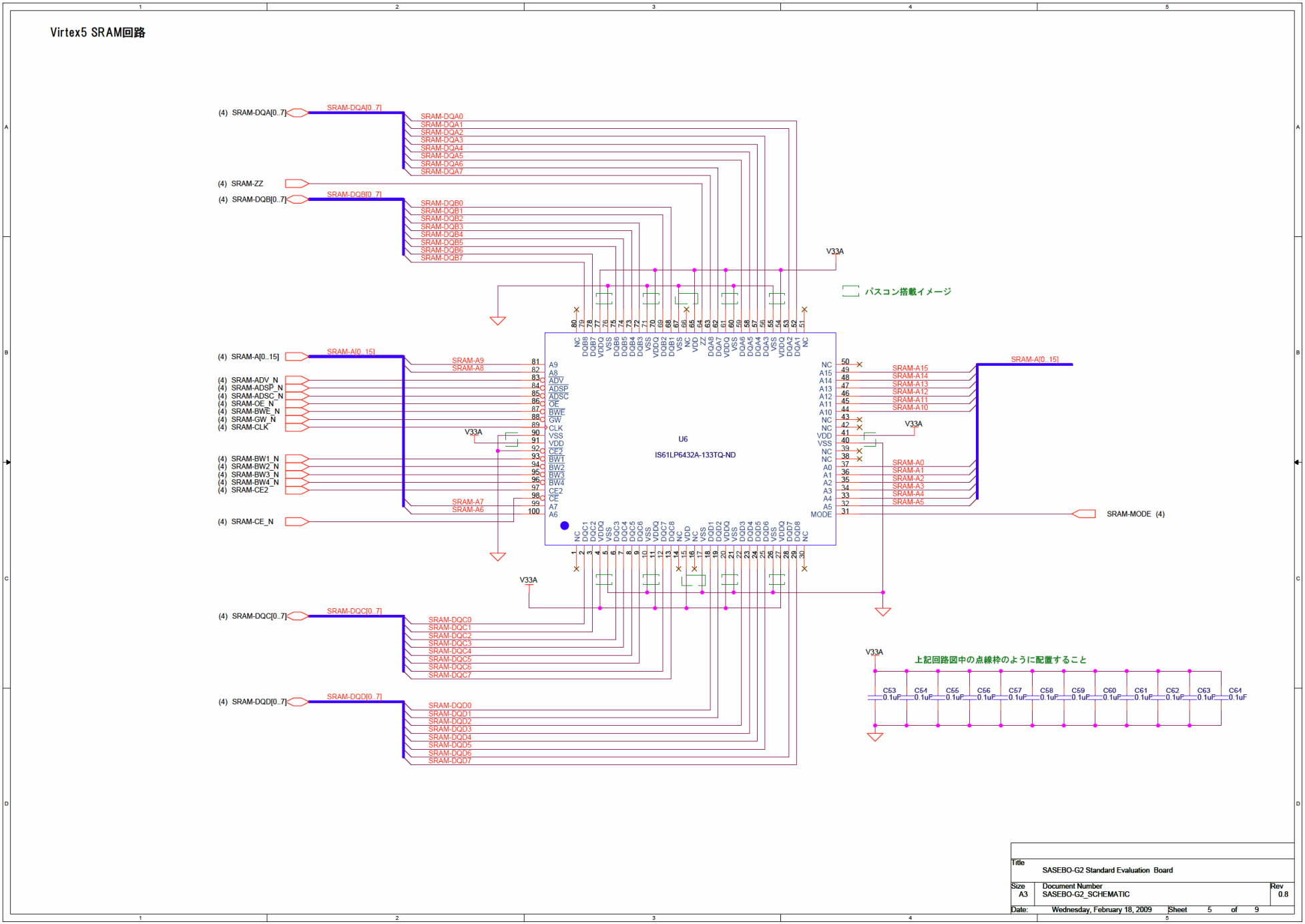


Figure 13 Cryptographic FPGA Block − SRAM

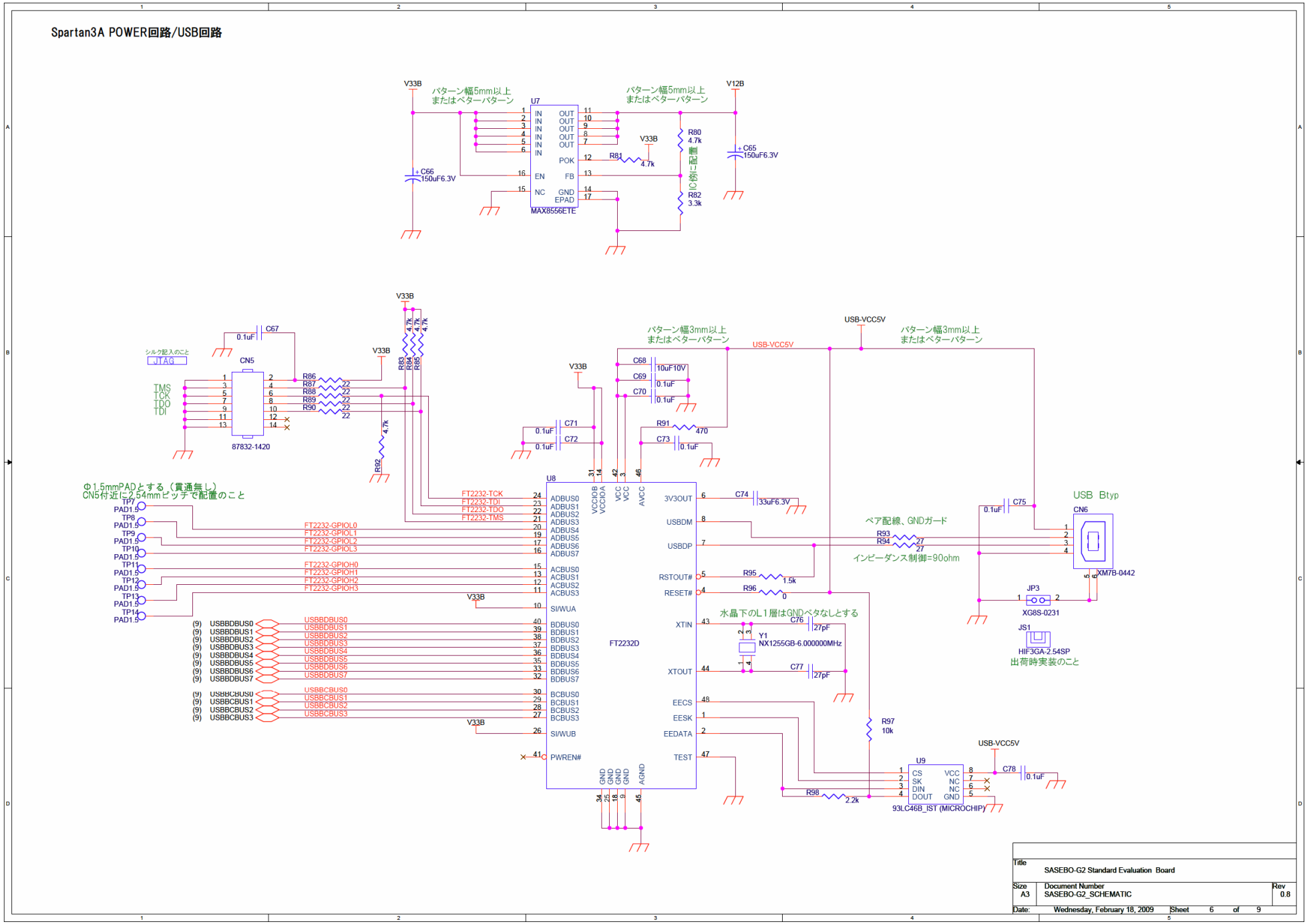


Figure 14　Control FPGA Block − Power Circuit, USB Circuit

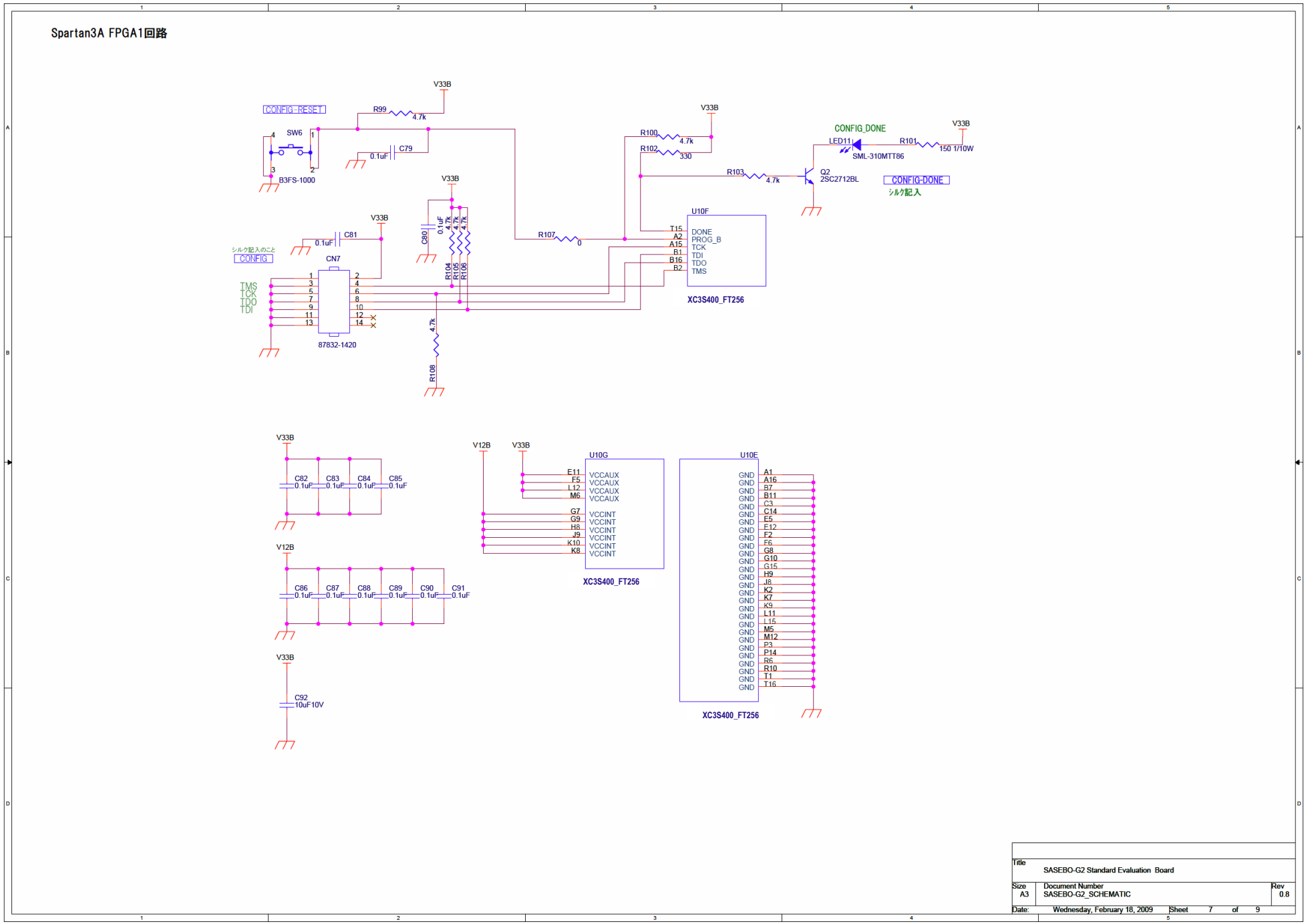


Figure 15 Control FPGA Block − Power Circuit, FPGA Configuration

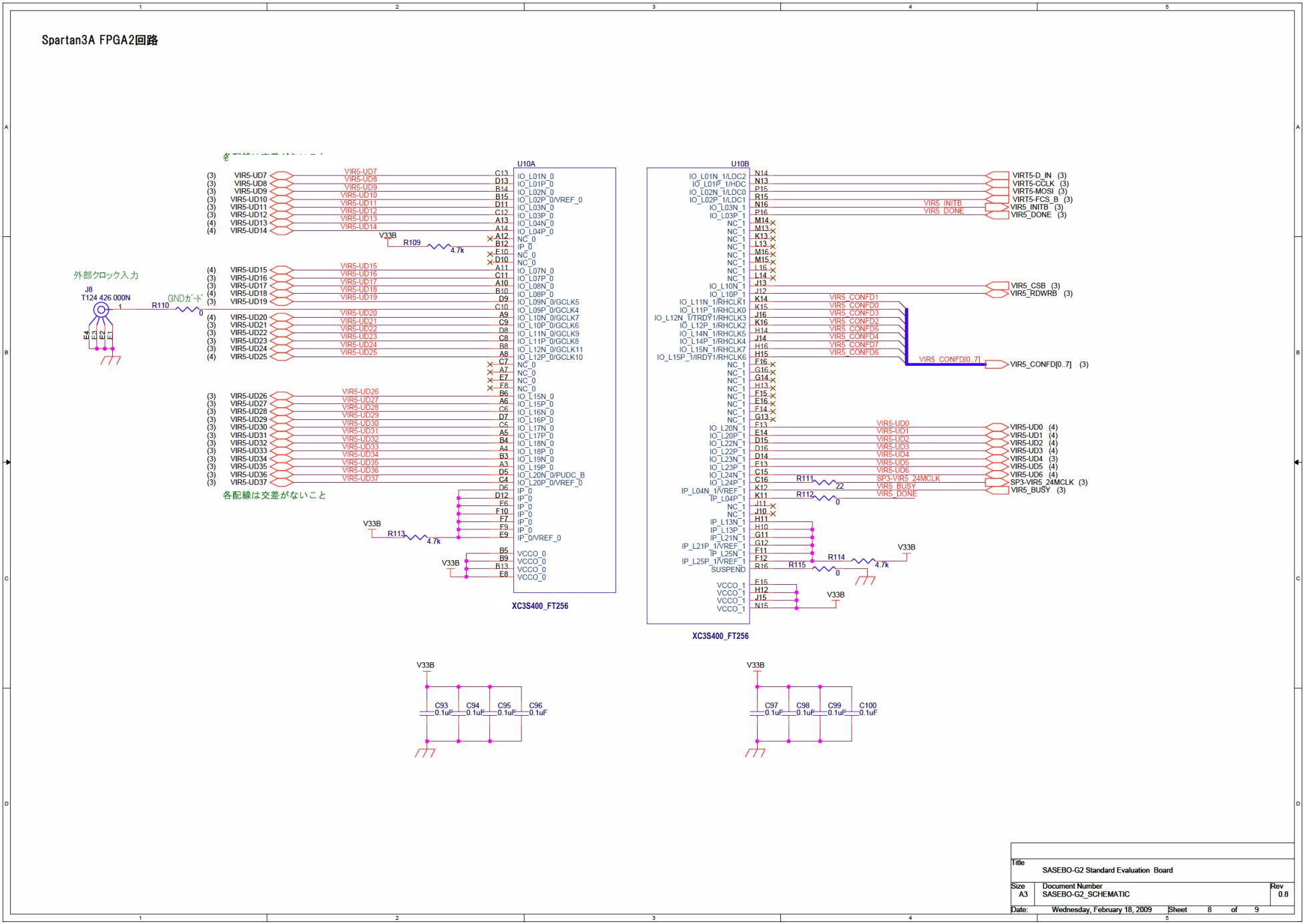


Figure 16 Control FPGA Block − FPGA I/O

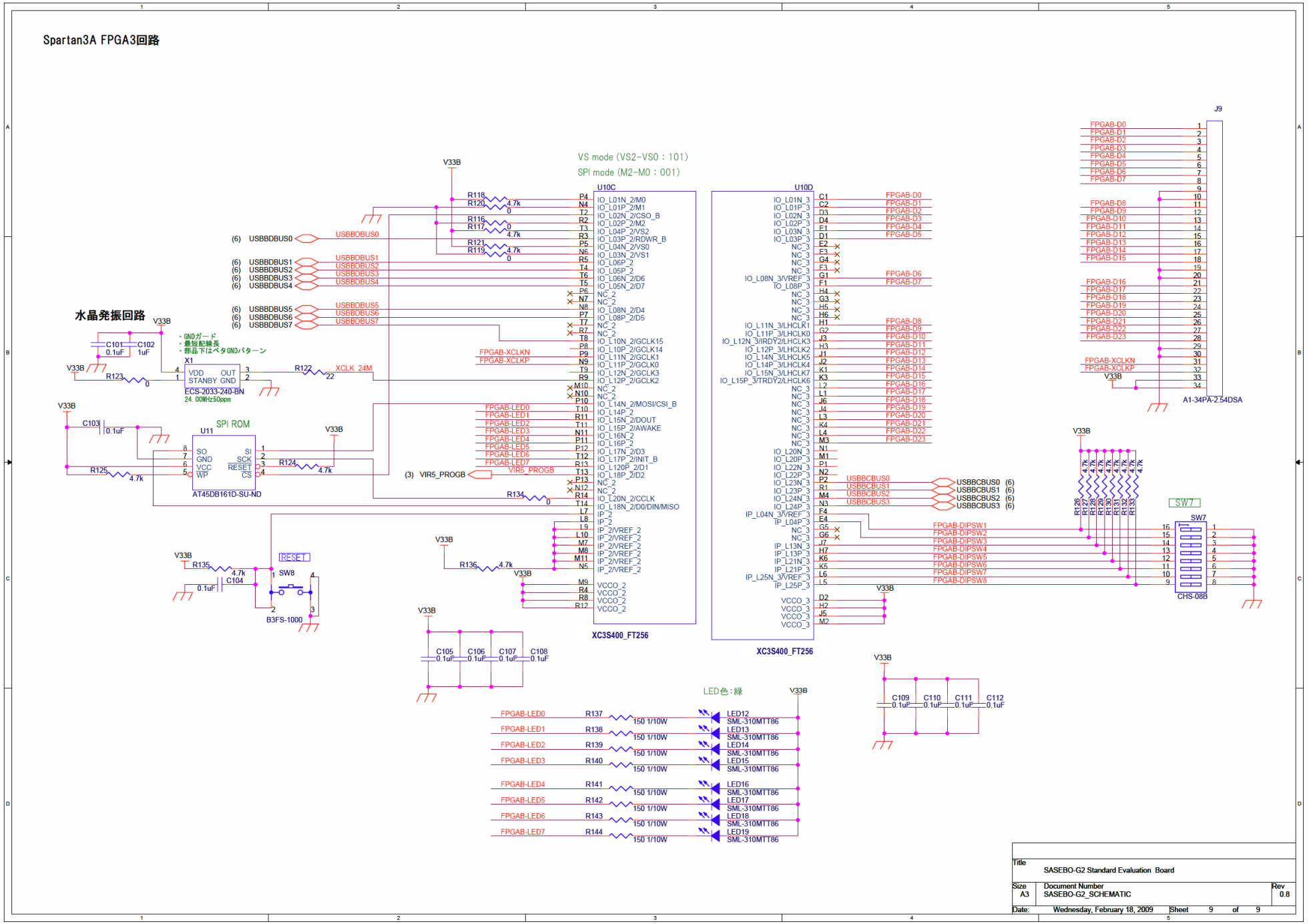


Figure 17　Control FPGA Block − FPGA I/O

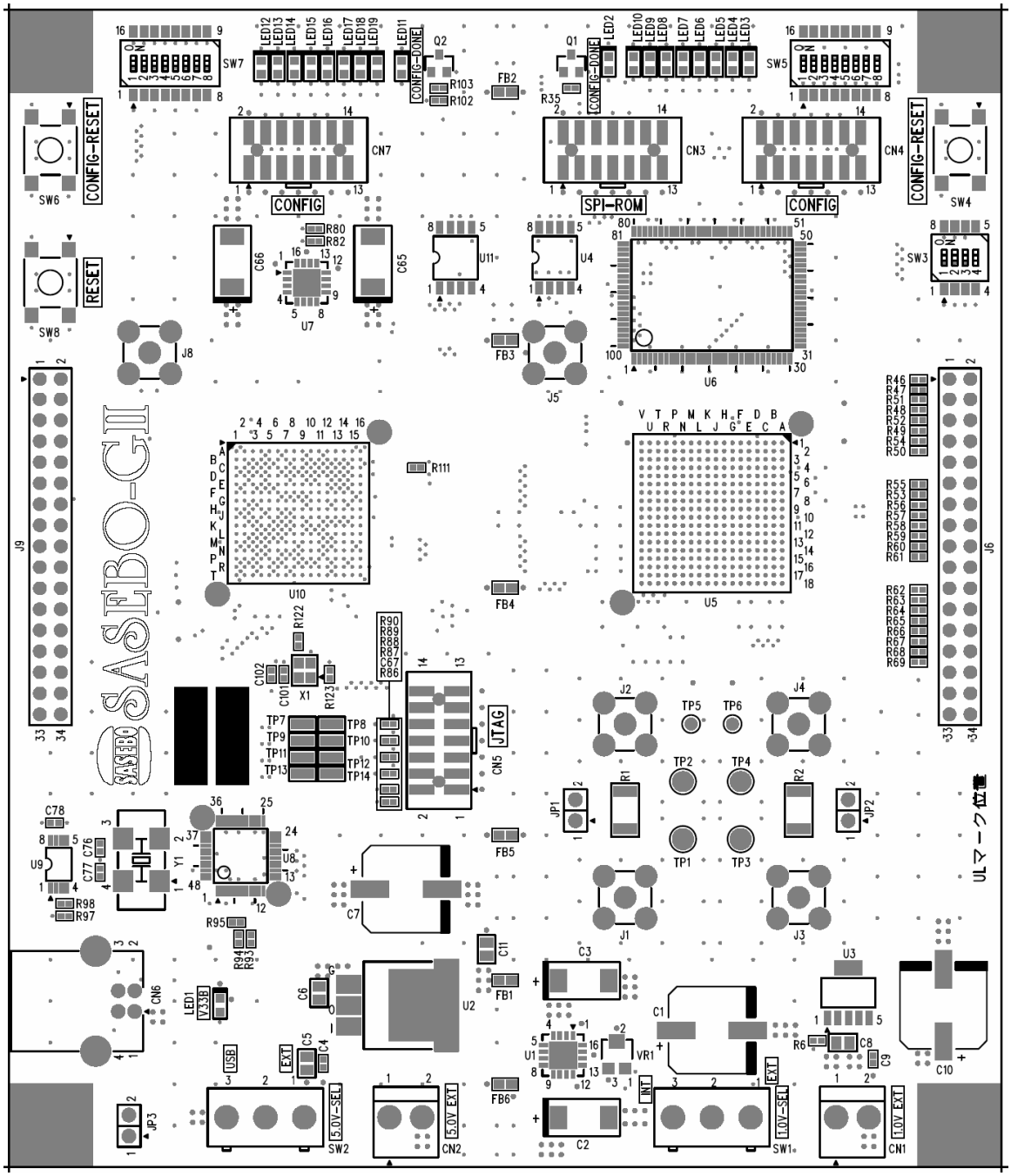


Figure 18 Part-side Silk Screen / Drawing

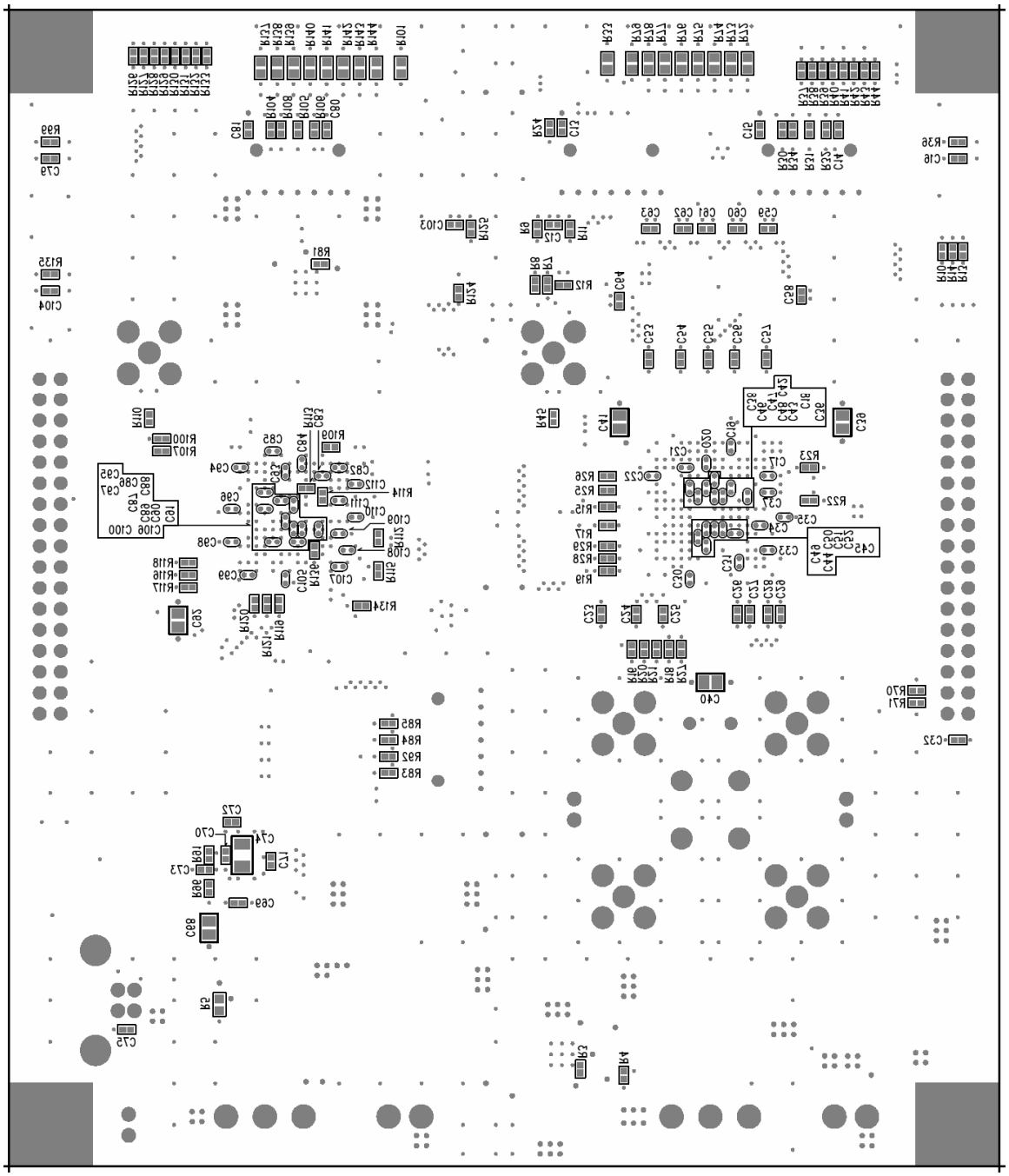


Figure 19 Solder-side Silk Screen / Drawing

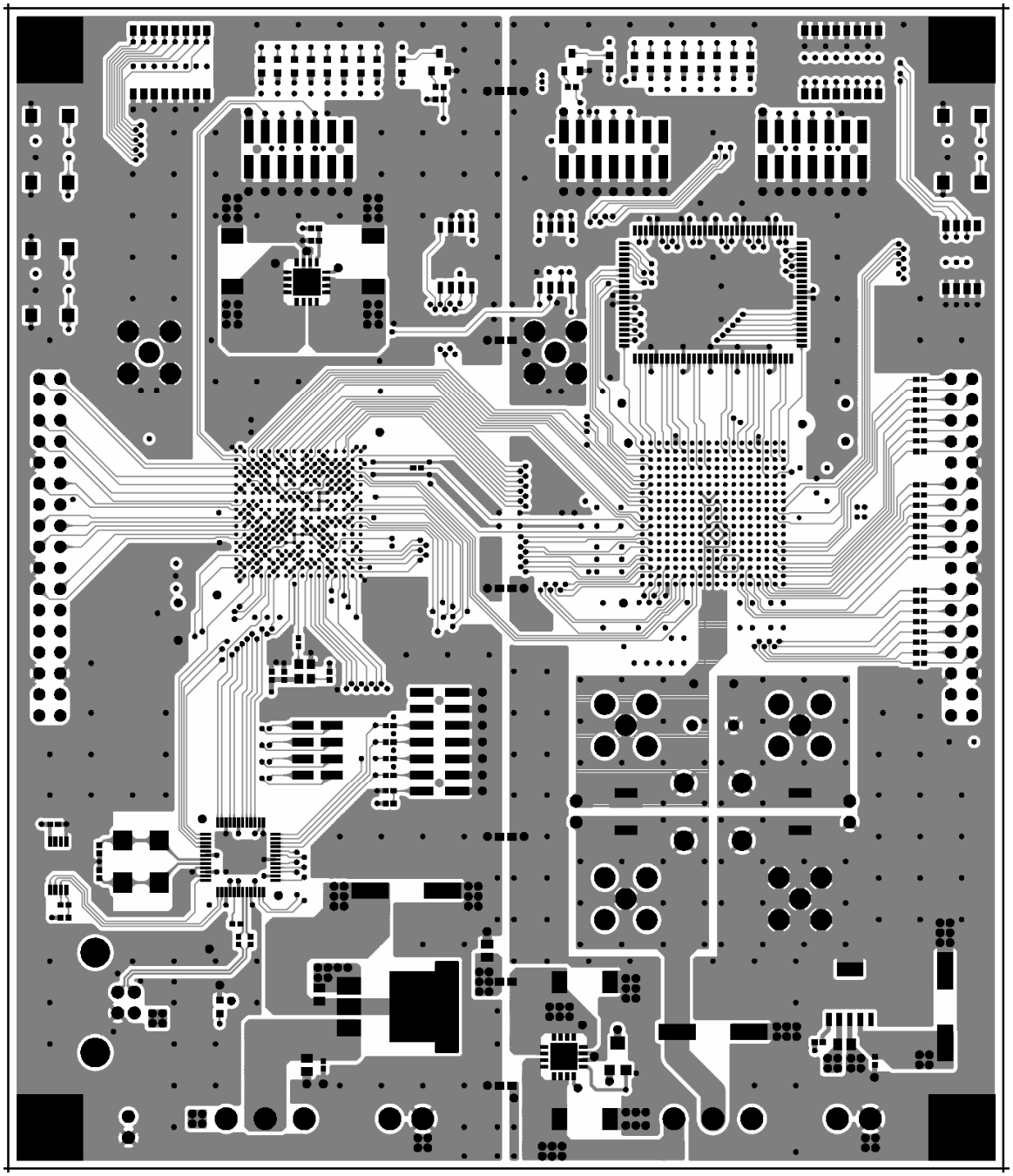


Figure 20　L1 Mask Pattern (Part side)

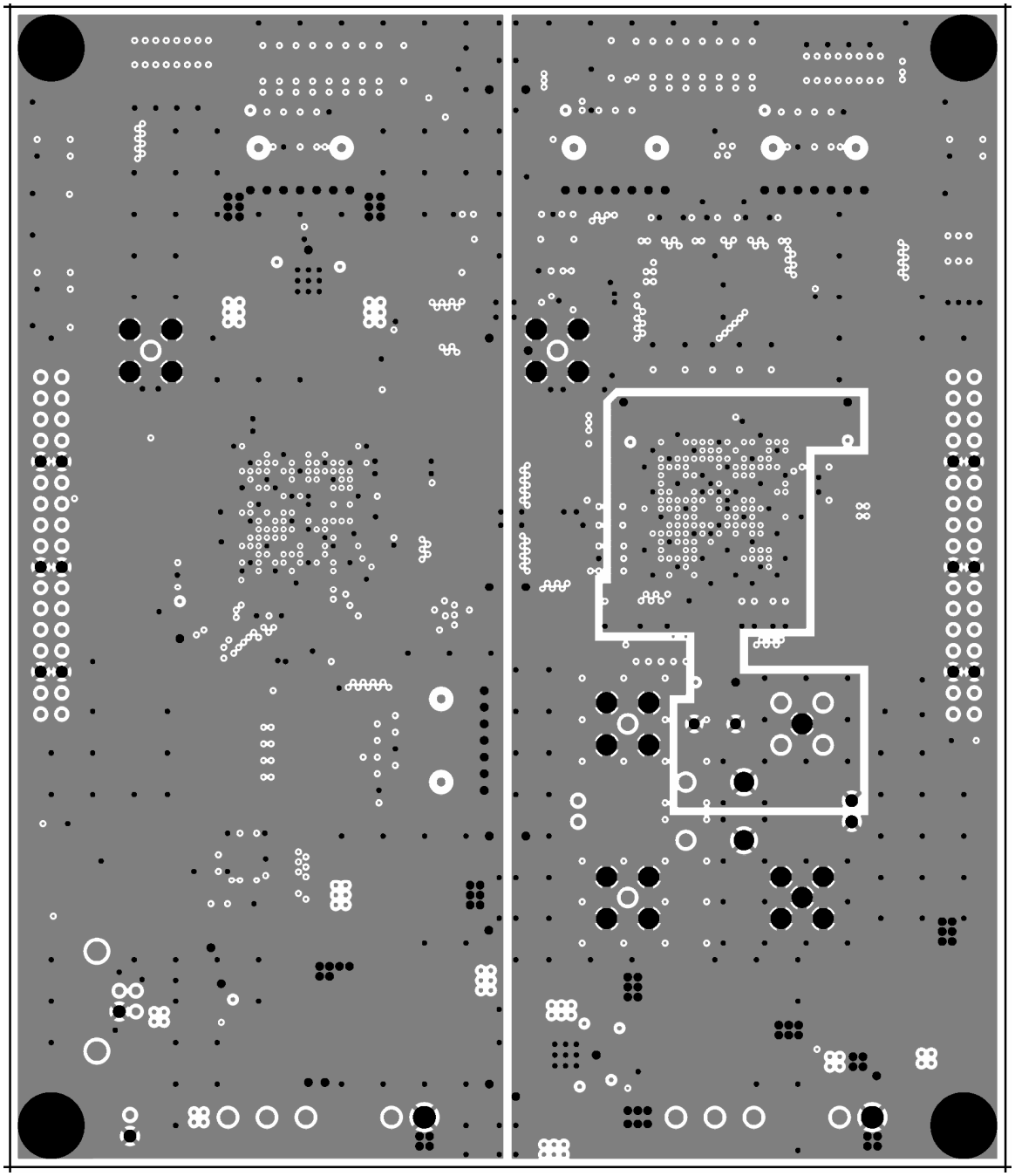


Figure 21 L2 Mask Pattern (Internal layer)

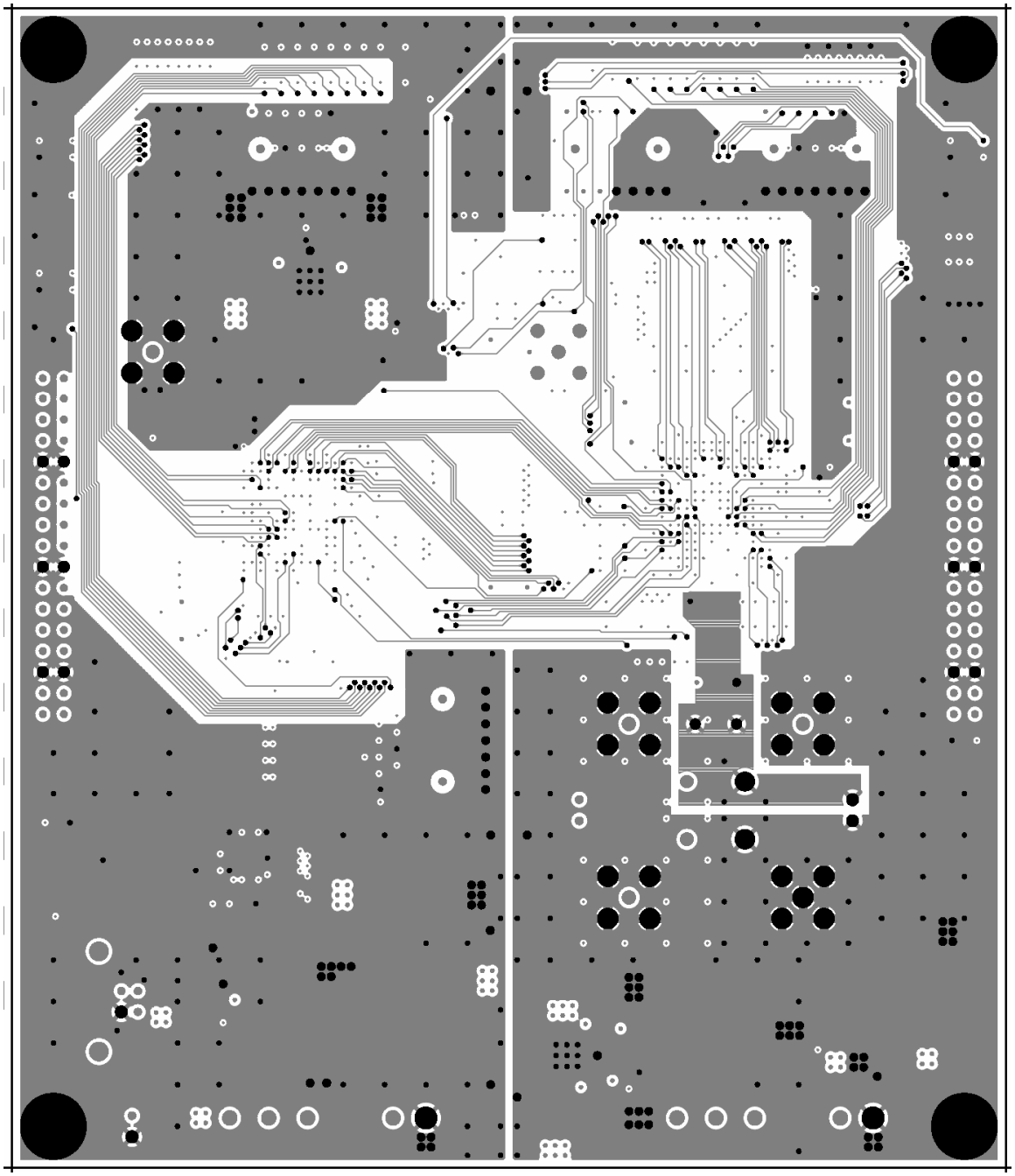


Figure 22 L3 Mask Pattern (Internal layer)

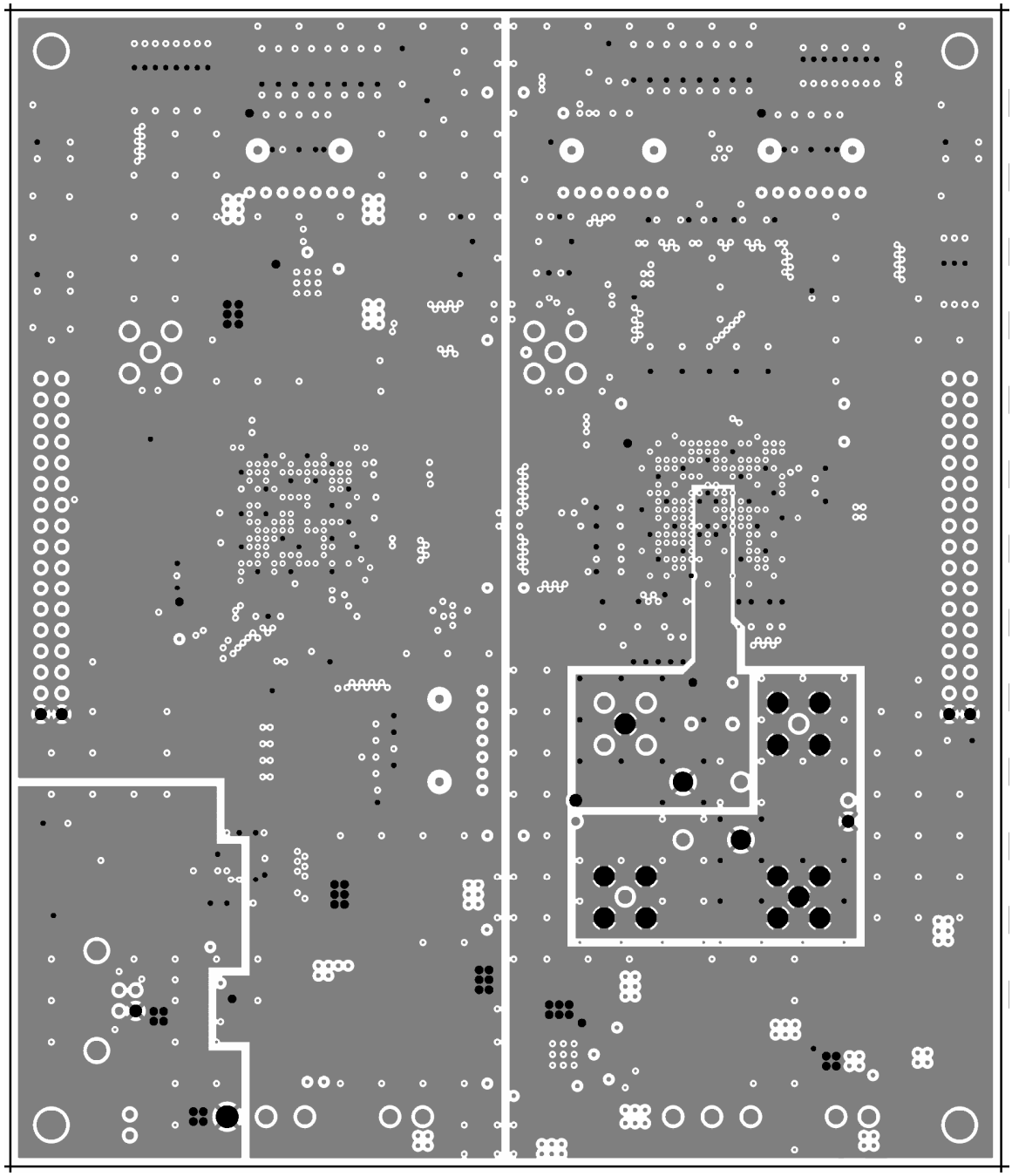


Figure 23 L4 Mask Pattern (Internal layer)

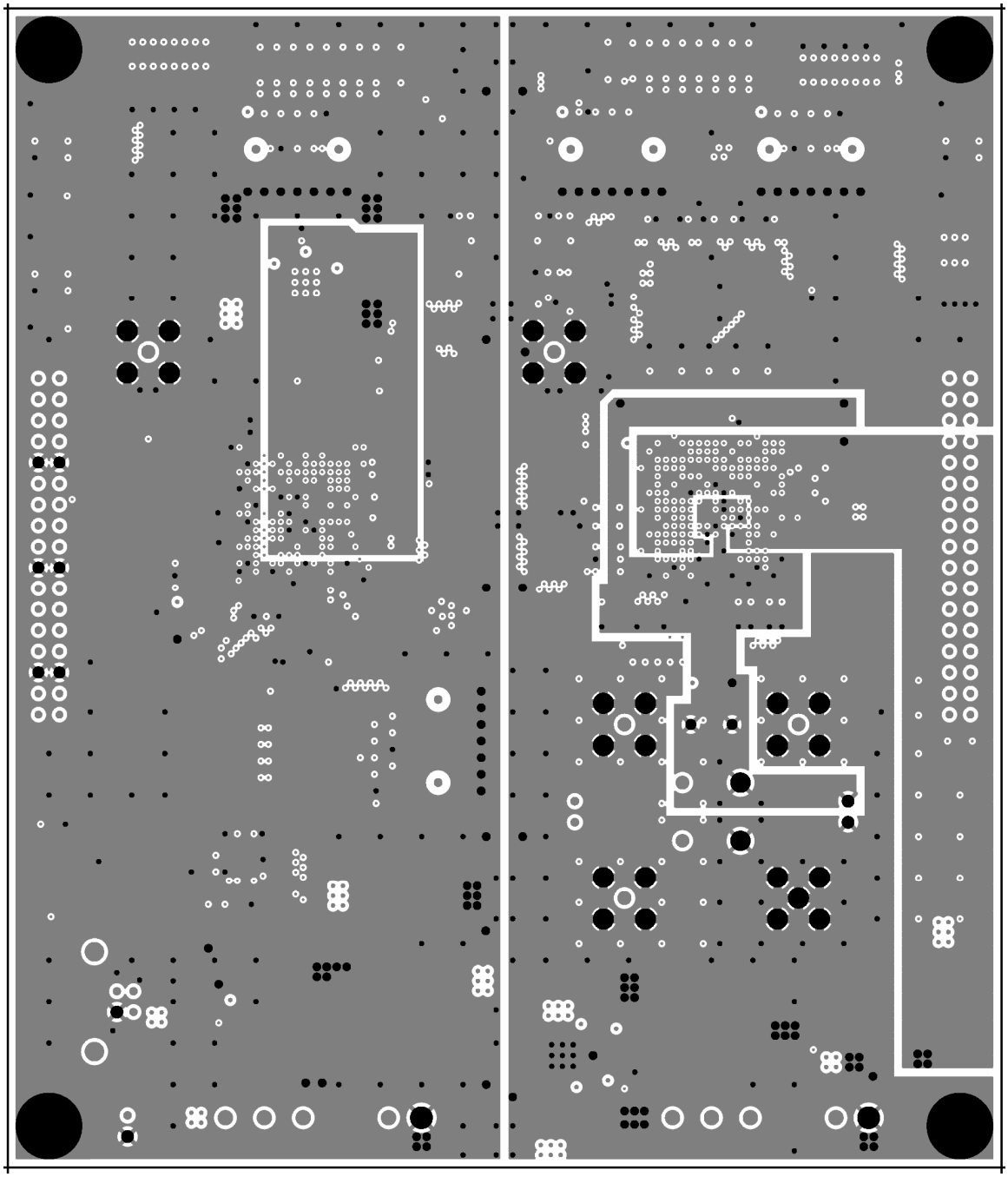


Figure 24 L5 Mask Pattern (Internal layer)

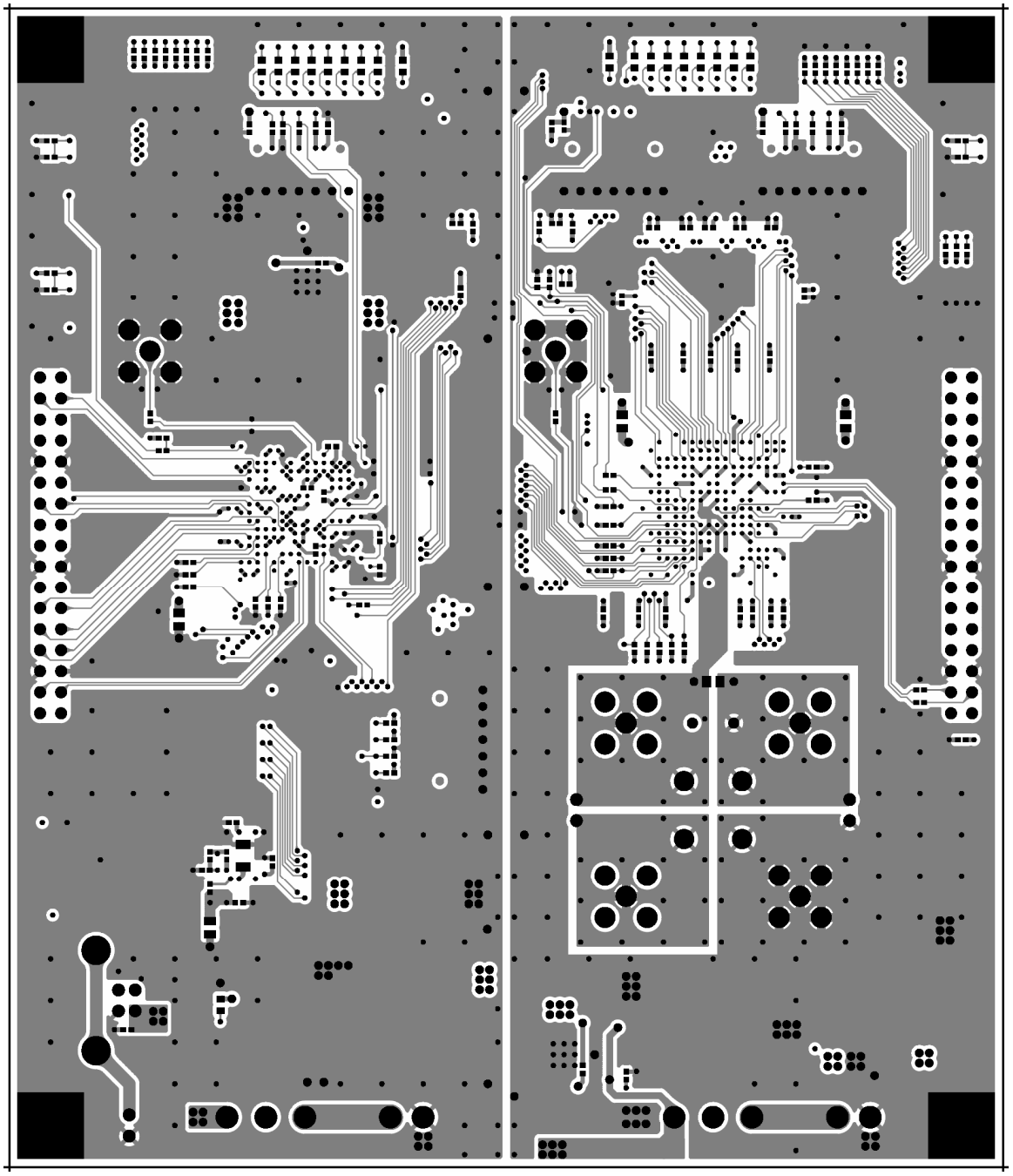


Figure 25　L6 Mask Pattern (Solder side)

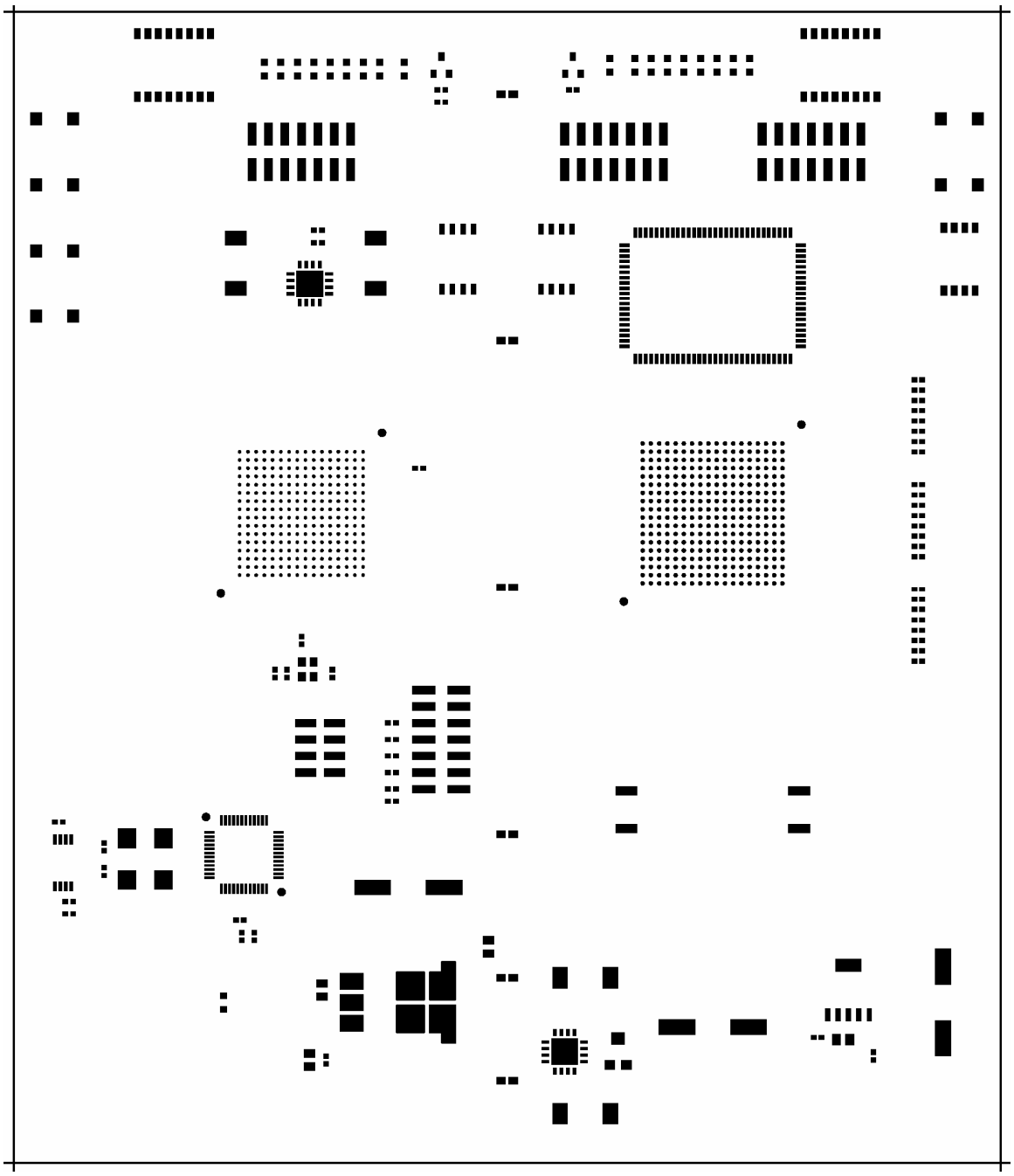


Figure 26 M1 Metal Mask Pattern (Part side)

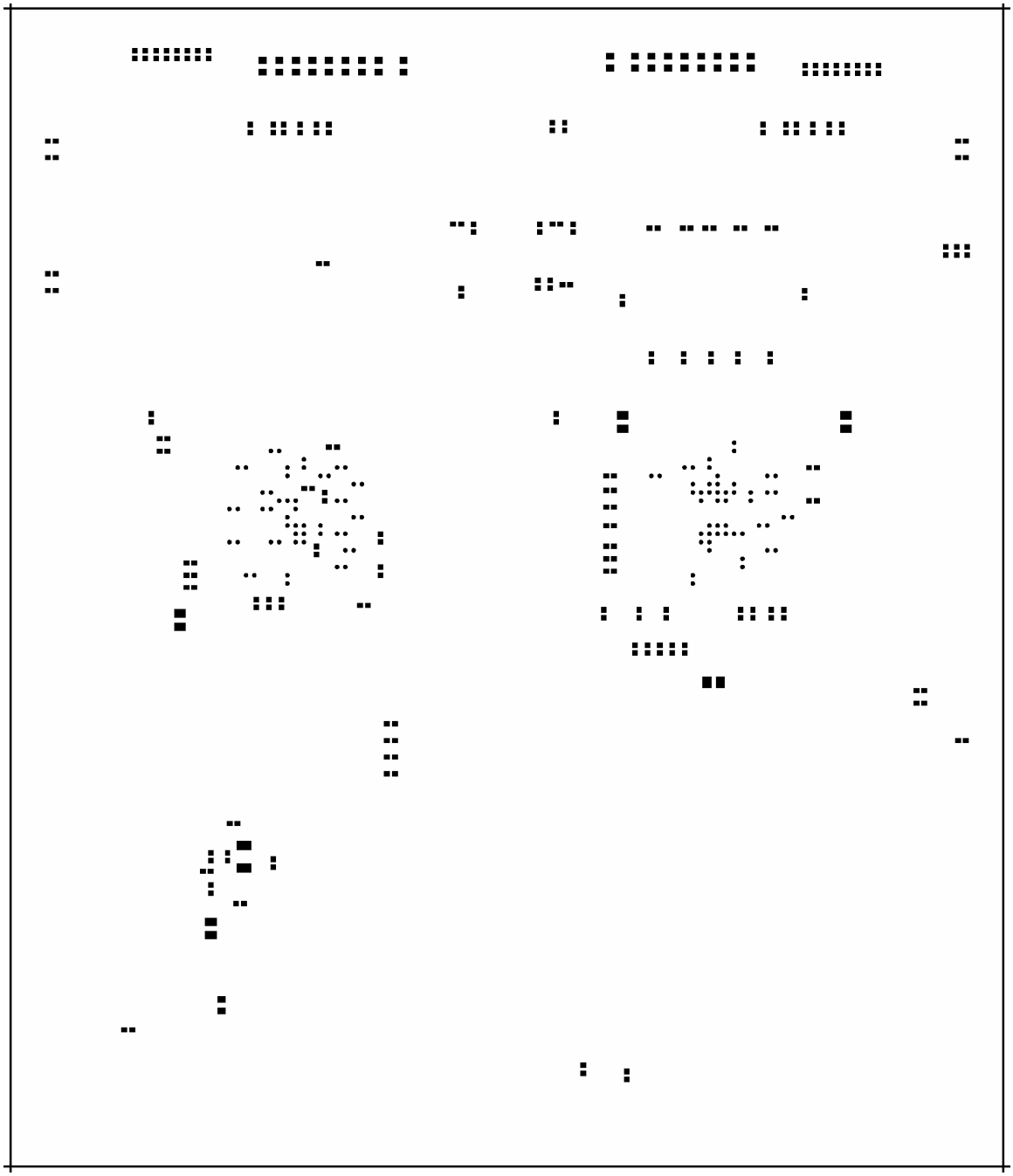


Figure 27　M2 Metal Mask Pattern (Solder side)

The SASEBO-GII board was developed by AIST (the National Institute of Advanced Industrial Science and Technology) in undertaking projects sponsored by METI (Ministry of Economy, Trade and Industry, Japan)

Technical inquiries:
National Institute of Advanced Industrial Science and Technology (AIST)
Research Center for Information Security (RCIS)
Akihabara-Daibiru 10F Room 1003
1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan
TEL: +81-3-5298-4722
FAX: +81-3-5298-4522