

**Side-channel Attack Standard Evaluation Board
SASEBO-R Specification**

- Version 1.0 -



April 1, 200

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

Index

	Page
1. OVERVIEW	2
2. I/O ASSIGNMENTS	3
3. OPERATIONAL INSTRUCTIONS	10
4. BOARD SCHEMATIC	17

1. Overview

The Side-channel Attack Standard Evaluation Board (SASEBO) is a board specifically designed to develop standard evaluation schemes to secure the cryptographic module against physical attacks. The SASEBO-R board can incorporate a cryptographic LSI. Figure 1 is a photograph of the SASEBO-R. The basic features of the SASEBO-R are as follows:

- 230 mm x 180 mm x 1.6 mm, FR-4, eight layers.
- 160-pin QFP socket and footprint.
One cryptographic LSI (130-nm process, 160-pin QFP) is mounted on the socket.
(Cryptographic LSI)
- Xilinx Virtex-II Pro FPGA XC2VP30-5FG676C for LSI control.
(Control FPGA)
- The cryptographic LSI and the control FPGA are connected through a 16-bit bidirectional data bus and a 16-bit address signal, controlled by four signals: RD, WR, RESET, and CLOCK.
- A 24-MHz oscillator is mounted to the control FPGA. Two 8-pin dip sockets are provided in order to mount clock oscillators for the cryptographic LSI. External clock input is also supported.
- Power regulators supply the voltages of the cryptographic LSI and the control FPGA with a 3.3-V input. The core voltage of the cryptographic LSI can be applied directly through an external power connector.
- Shunt resistance is provided for power measurement of the devices.
- RS-232 and USB ports for communicating with the host PC

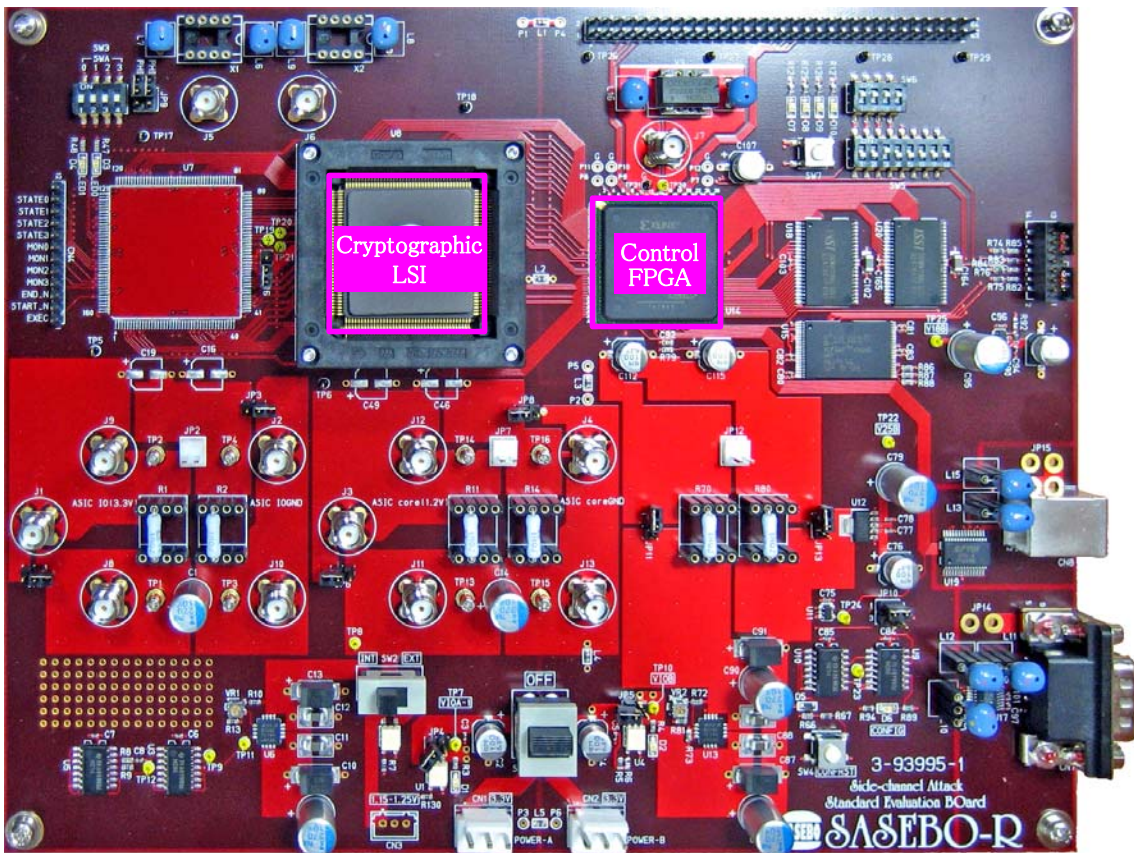


Figure 1: SASEBO-R

2. I/O Assignments

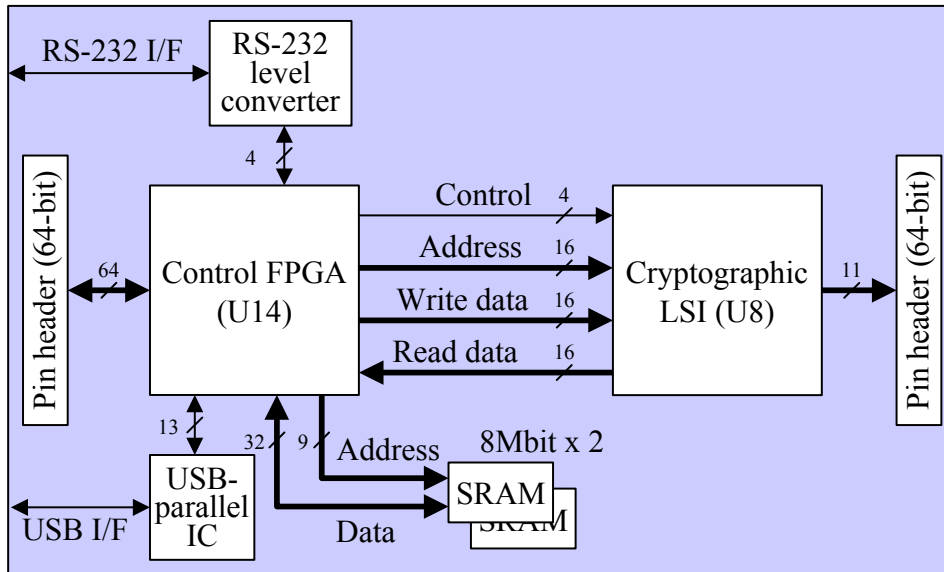


Figure 2: I/O signals

- Pin assignments of the cryptographic LSI (U8)

Table 1: LSI control

Signal Name	Pin Number	Input/Output	Description
CLKA	58	IN	CLOCK
HRST_N	63	IN	RESET
CLKB	56	IN	
LED0	135	OUT	
LED1	136	OUT	
SWA0	7	IN	SW3-8
SWA1	6	IN	SW3-7
SWA2	5	IN	SW3-6
SWA3	4	IN	SW3-5
PHIN0	10	IN	JP9
PHIN1	9	IN	JP9
PUSH	D9	IN	SW6

Table 2: Cryptographic circuit interface

Signal Name	Pin Number	INPUT/OUTPUT	Destination (U14)
FPGA_DI0	109	IN	F1
FPGA_DI1	110	IN	F2
FPGA_DI2	111	IN	E1
FPGA_DI3	112	IN	E2
FPGA_DI4	114	IN	D1
FPGA_DI5	115	IN	D2
FPGA_DI6	116	IN	C1
FPGA_DI7	117	IN	C2
FPGA_DI8	123	IN	K5
FPGA_DI9	124	IN	J4

FPGA_DI10	125	IN	J3
FPGA_DI11	126	IN	K4
FPGA_DI12	129	IN	K3
FPGA_DI13	130	IN	L5
FPGA_DI14	131	IN	L3
FPGA_DI15	132	IN	M4
FPGA_DO0	92	OUT	G2
FPGA_DO1	91	OUT	G1
FPGA_DO2	90	OUT	H2
FPGA_DO3	89	OUT	H1
FPGA_DO4	87	OUT	J2
FPGA_DO5	86	OUT	J1
FPGA_DO6	85	OUT	K2
FPGA_DO7	84	OUT	K1
FPGA_DO8	78	OUT	N5
FPGA_DO9	77	OUT	N4
FPGA_DO10	76	OUT	L2
FPGA_DO11	75	OUT	L1
FPGA_DO12	72	OUT	M2
FPGA_DO13	71	OUT	M1
FPGA_DO14	70	OUT	N2
FPGA_DO15	69	OUT	N6
FPGA_A0	52	IN	T2
FPGA_A1	51	IN	U1
FPGA_A2	50	IN	U2
FPGA_A3	49	IN	V1
FPGA_A4	46	IN	V2
FPGA_A5	45	IN	W1
FPGA_A6	44	IN	W2
FPGA_A7	43	IN	Y1
FPGA_A8	37	IN	Y2
FPGA_A9	36	IN	AA1
FPGA_A10	35	IN	AA2
FPGA_A11	34	IN	AB1
FPGA_A12	32	IN	AB2
FPGA_A13	31	IN	AC1
FPGA_A14	30	IN	AC2
FPGA_A15	29	IN	AD1
FPGA_WR	65	IN	R2
FPGA_RD	66	IN	R1
FPGA_RSV0	27	IN	AD2
FPGA_RSV1	26	IN	AE1

Table 3: LEDs and switches

Signal Name	Pin number	Input/Output	Description
STATE0	143	OUT	
STATE1	144	OUT	
STATE2	145	OUT	
STATE3	146	OUT	
EXEC	155	OUT	
MON0	149	-	

MON1	150	-	
MON2	151	-	
MON3	152	-	
START_N	138	-	
END_N	137	-	

- Pin assignments of the control FPGA (U14)

Table 4: Device control

Signal Name	Pin Number	Input/Output	Description
CDB0	AB21		Config
CDB1	AC21		Config
CDB2	Y20		Config
CDB3	AA20		Config
CDB4	AA7		Config
CDB5	Y7		Config
CDB6	AC6		Config
CDB7	AB6		Config
BUSY	AB22		Config
INIT_B	AC22		Config
GCLK	AE24		Config
PROG_B	B1		Config
DONE	AD23		Config
M0	AE3		SW5-1
M1	AF3		SW5-2
M2	AD4		SW5-3
TCLK	B26		JTAG
TDI	D3		JTAG
TDO	D24		JTAG
TMS	B24		JTAG
PWRDWN_B	AF24		SW5-4
HSWAP_EN	B3		SW5-5
VBATT	A24		P13
DXP	A3		P14
DXN	C4		P15
OSCX	N3	OUT	Clock
RESETB	Y9	IN	RESET
CLK	B13	IN	X3

Table 5: LEDs and switches

Signal Name	Pin Number	Input/Output	Description
D7	F24	OUT	LED
D8	J22	OUT	LED
D9	J24	OUT	LED
D10	J23	OUT	LED
DIPSW5	H22	IN	SW6-1
DIPSW6	K22	IN	SW6-2
DIPSW7	K23	IN	SW6-3
DIPSW8	K24	IN	SW6-4
PUSH	G22	IN	SW7

Table 6: RS-232

Signal Name	Pin Number	Input/Output	Destination
TX	AB14	OUT	Level converter
RX	AC15	IN	Level converter
CTS	AB15	OUT	Level converter
RTS	AA15	IN	Level converter

Table 7: Pin header

Signal Name	Pin Number	Input/Output	Destination
IOB0	F7	IO	CN6-1
IOB1	E6	IO	CN6-2
IOB2	E5	IO	CN6-3
IOB3	D6	IO	CN6-4
IOB4	D7	IO	CN6-5
IOB5	B8	IO	CN6-6
IOB6	A8	IO	CN6-7
IOB7	C9	IO	CN6-8
IOB8	C10	IO	CN6-9
IOB9	C7	IO	CN6-10
IOB10	F8	IO	CN6-11
IOB11	E8	IO	CN6-12
IOB12	E9	IO	CN6-13
IOB13	H9	IO	CN6-14
IOB14	D10	IO	CN6-15
IOB15	E10	IO	CN6-16
IOB16	E11	IO	CN6-17
IOB17	F11	IO	CN6-18
IOB18	E12	IO	CN6-19
IOB19	F12	IO	CN6-20
IOB20	C12	IO	CN6-21
IOB21	D12	IO	CN6-22
IOB22	F14	IO	CN6-23
IOB23	B14	IO	CN6-24
IOB24	C14	IO	CN6-25
IOB25	D14	IO	CN6-26
IOB26	E14	IO	CN6-27
IOB27	E15	IO	CN6-28
IOB28	E16	IO	CN6-29
IOB29	D17	IO	CN6-30
IOB30	E17	IO	CN6-31
IOB31	C15	IO	CN6-32
IOB32	C17	IO	CN6-33
IOB33	A19	IO	CN6-34
IOB34	B19	IO	CN6-35
IOB35	C20	IO	CN6-36
IOB36	F19	IO	CN6-37
IOB37	E19	IO	CN6-38
IOB38	D20	IO	CN6-39
IOB39	E20	IO	CN6-40
IOB40	D21	IO	CN6-41
IOB41	D22	IO	CN6-42
IOB42	E22	IO	CN6-43

IOB43	E21	IO	CN6-44
IOB44	G19	IO	CN6-45
IOB45	H17	IO	CN6-46
IOB46	J14	IO	CN6-47
IOB47	H11	IO	CN6-48
IOB48	H8	IO	CN6-49
IOB49	H10	IO	CN6-50
IOB50	G8	IO	CN6-51
IOB51	G11	IO	CN6-52
IOB52	E7	IO	CN6-53
IOB53	D5	IO	CN6-54
IOB54	H12	IO	CN6-55
IOB55	H14	IO	CN6-56
IOB56	F15	IO	CN6-57
IOB57	F16	IO	CN6-58
IOB58	G16	IO	CN6-59
IOB59	H19	IO	CN6-60
IOB60	F20	IO	CN6-61
IOB61	G20	IO	CN6-62
IOB62	H18	IO	CN6-63
IOB63	H16	IO	CN6-64

Table 8: Cryptographic circuit interface

Signal Name	Pin Number	Input/Output	Destination (U8)
FPGA_DI0	F1	OUT	109
FPGA_DI1	F2	OUT	110
FPGA_DI2	E1	OUT	111
FPGA_DI3	E2	OUT	112
FPGA_DI4	D1	OUT	114
FPGA_DI5	D2	OUT	115
FPGA_DI6	C1	OUT	116
FPGA_DI7	C2	OUT	117
FPGA_DI8	K5	OUT	123
FPGA_DI9	J4	OUT	124
FPGA_DI10	J3	OUT	125
FPGA_DI11	K4	OUT	126
FPGA_DI12	K3	OUT	129
FPGA_DI13	L5	OUT	130
FPGA_DI14	L3	OUT	131
FPGA_DI15	M4	OUT	132
FPGA_DO0	G2	IN	92
FPGA_DO1	G1	IN	91
FPGA_DO2	H2	IN	90
FPGA_DO3	H1	IN	89
FPGA_DO4	J2	IN	87
FPGA_DO5	J1	IN	86
FPGA_DO6	K2	IN	85
FPGA_DO7	K1	IN	84
FPGA_DO8	N5	IN	78
FPGA_DO9	N4	IN	77
FPGA_DO10	L2	IN	76
FPGA_DO11	L1	IN	75

FPGA DO12	M2	IN	72
FPGA DO13	M1	IN	71
FPGA DO14	N2	IN	70
FPGA DO15	N6	IN	69
FPGA A0	T2	OUT	52
FPGA A1	U1	OUT	51
FPGA A2	U2	OUT	50
FPGA A3	V1	OUT	49
FPGA A4	V2	OUT	46
FPGA A5	W1	OUT	45
FPGA A6	W2	OUT	44
FPGA A7	Y1	OUT	43
FPGA A8	Y2	OUT	37
FPGA A9	AA1	OUT	36
FPGA A10	AA2	OUT	35
FPGA A11	AB1	OUT	34
FPGA A12	AB2	OUT	32
FPGA A13	AC1	OUT	31
FPGA A14	AC2	OUT	30
FPGA A15	AD1	OUT	29
FPGA WR	R2	OUT	65
FPGA RD	R1	OUT	66
FPGA RSV0	AD2		27
FPGA RSV1	AE1		26

Table 9: USB

Signal Name	Pin Number	Input/Output	Destination
USB0	AB16	IO	USB I/F
USB1	AA16	IO	USB I/F
USB2	AB17	IO	USB I/F
USB3	AE14	IO	USB I/F
USB4	AC17	IO	USB I/F
USB5	AC14	IO	USB I/F
USB6	AD14	IO	USB I/F
USB7	AB20	IO	USB I/F
USBTXE	AE19	IN	USB I/F
USBRXF	AD20	IN	USB I/F
USBRD	AD17	OUT	USB I/F
USBWR	AF19	OUT	USB I/F
USBWREN	AD15	IN	USB I/F

Table 10: SRAM

Signal Name	Pin Number	Input/Output	Destination
MEMD0	U25	IO	Memory
MEMD1	V26	IO	Memory
MEMD2	V25	IO	Memory
MEMD3	W26	IO	Memory
MEMD4	W25	IO	Memory
MEMD5	Y26	IO	Memory
MEMD6	Y25	IO	Memory
MEMD7	AA26	IO	Memory
MEMD8	R26	IO	Memory
MEMD9	R25	IO	Memory

MEMD10	T26	IO	Memory
MEMD11	T25	IO	Memory
MEMD12	N25	IO	Memory
MEMD13	M26	IO	Memory
MEMD14	M25	IO	Memory
MEMD15	L26	IO	Memory
MEMD16	J26	IO	Memory
MEMD17	K25	IO	Memory
MEMD18	K26	IO	Memory
MEMD19	L25	IO	Memory
MEMD20	H26	IO	Memory
MEMD21	H25	IO	Memory
MEMD22	G26	IO	Memory
MEMD23	G25	IO	Memory
MEMD24	E25	IO	Memory
MEMD25	E26	IO	Memory
MEMD26	F25	IO	Memory
MEMD27	F26	IO	Memory
MEMD28	D26	IO	Memory
MEMD29	D25	IO	Memory
MEMD30	C26	IO	Memory
MEMD31	C25	IO	Memory
MEMA0	V22	OUT	Memory
MEMA1	U23	OUT	Memory
MEMA2	T22	OUT	Memory
MEMA3	R22	OUT	Memory
MEMA4	N22	OUT	Memory
MEMA5	N23	OUT	Memory
MEMA6	R21	OUT	Memory
MEMA7	R23	OUT	Memory
MEMA8	Y21	OUT	Memory
MEMA9	Y22	OUT	Memory
MEMA10	AA23	OUT	Memory
MEMA11	AD25	OUT	Memory
MEMA12	AD26	OUT	Memory
MEMA13	AC25	OUT	Memory
MEMA14	AC26	OUT	Memory
MEMA15	AB25	OUT	Memory
MEMA16	AB26	OUT	Memory
MEMA17	AE26	OUT	Memory
MEMA18	W22	OUT	Memory
MEMCS	U26	OUT	Memory
MEMCS1	J25	OUT	Memory
MEMWR	AA25	OUT	Memory
MEMUB	U24	OUT	Memory
MEMLB	V24	OUT	Memory
MEMOE	T24	OUT	Memory

3. Operational Instructions

➤ Power Supply

Figure 3 shows the composition of the power supply block on the SASEBO-R. Table 11 shows the functions of the power supply connectors. Figure 4 shows the power sequence of the SASEBO-R.

DC 3.3V is supplied to the SASEBO-R through both CN1 and CN2 by the power source, which has a maximum current capacity of 2.0 A. The main power switch (SW1) must be toggled off or the power source must be unplugged. D1 and D2 indicate that DC 3.3V is supplied through CN1 and CN2, respectively. Toggle SW2 to “EXT” supplying the cryptographic FPGA core voltage of 1.2 V through CN3. SW1 must be also toggling off SW2.

Table 11: Power supply settings

Connector		CN1	CN2	CN3
Description		Cryptographic LSI power supply	Control FPGA power supply	Cryptographic LSI core voltage
SW2 setting		INT	INT	EXT
Pin	1	3.3V±0.16V	3.3V±0.16V	1.2V±0.05V
	2	0V	0V	0V
	3	NC	NC	NC

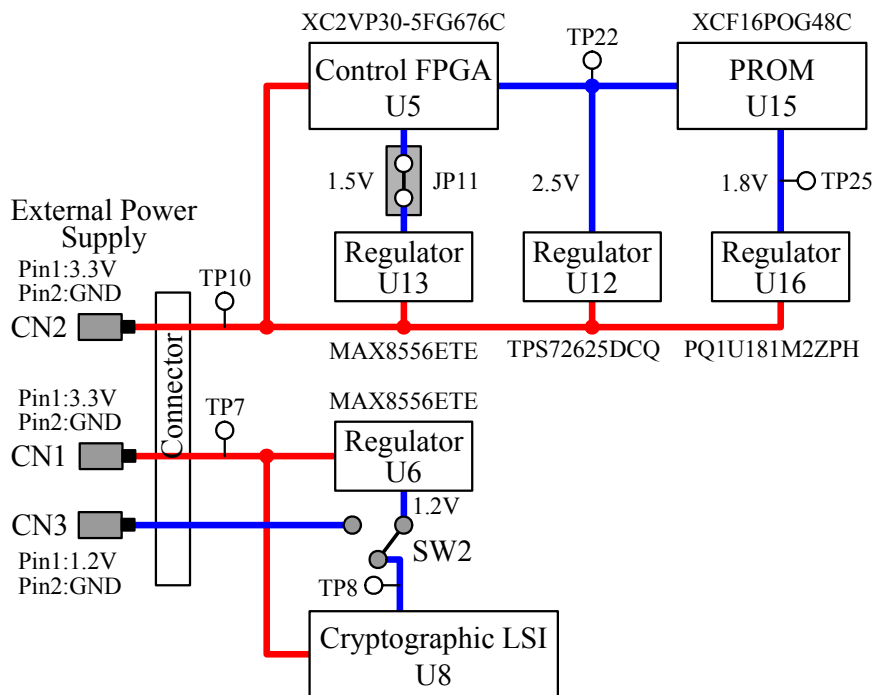


Figure 3: Power supply block on the SASEBO-R

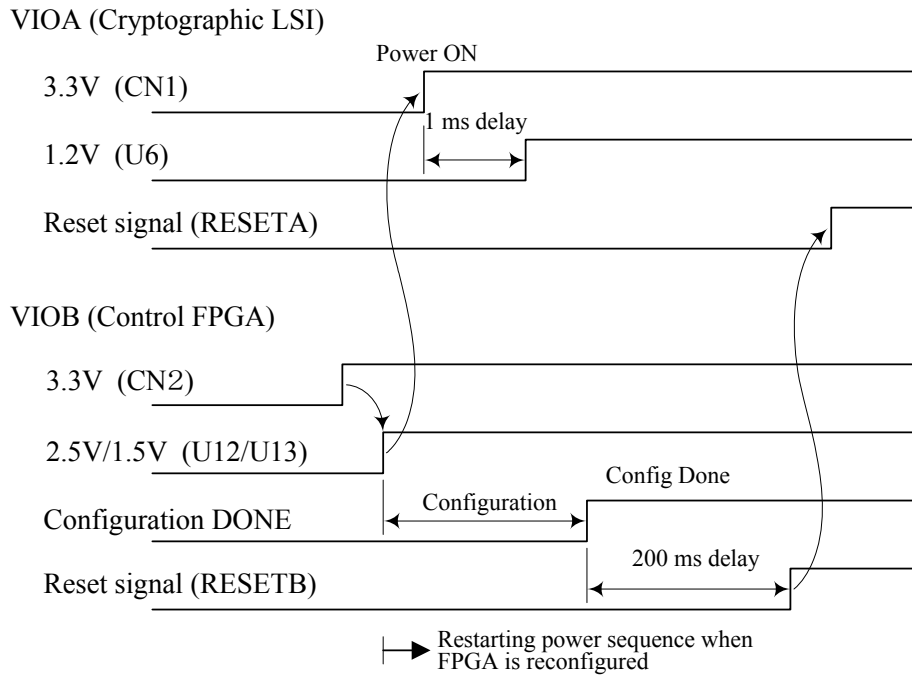


Figure 4: Power sequence of SASEBO-R

➤ **Jumper Settings**

Table 12: Jumper settings

Function	Pin	Setting	Description
Power sequence	JP4	Short	Disable the power sequence of the cryptographic LSI.
		Open	Enable the power sequence of the cryptographic LSI.
	JP5	Short	Disable the power sequence of the control FPGA.
		Open	Enable the power sequence of the control FPGA.
Configuration sequence	JP10	1-2Short	Configure the control FPGA after 2.5V line is stable.
		3-4Short	Configure the control FPGA after 1.5V line is stable.
Power consumption measurement	JP1	Short	Bypass R4 shunt resistor on I/O VCC of the cryptographic LSI.
		Open	Enable R4 shunt resistor on I/O VCC of the cryptographic LSI.
	JP3	Short	Bypass R2 shunt resistor on I/O GND of the cryptographic LSI.
		Open	Enable R2 shunt resistor on I/O GND of the cryptographic LSI.
	JP6	Short	Bypass R11 shunt resistor on core VCC of the cryptographic LSI.
		Open	Enable R11 shunt resistor on core VCC of the cryptographic LSI.
	JP8	Short	Bypass R14 shunt resistor on core GND of the cryptographic LSI.
		Open	Enable R14 shunt resistor on core GND of the cryptographic LSI.
JP11	Short	Bypass R70 shunt resistor on core VCC of the control FPGA.	
	Open	Enable R70 shunt resistor on core VCC of the control FPGA.	

JP2, JP7, and JP13 are voltage test points. DO NOT SHORT these points.

➤ **FPGA configuration**

Figure 5 is a block diagram of the control FPGA configuration chain. Table 13 shows the pin assignment of CN5. The configuration mode settings (SW5) are listed in Table 14. D6 indicates that FPGA is configured successfully. Push down SW4 to reconfigure the control FPGA.

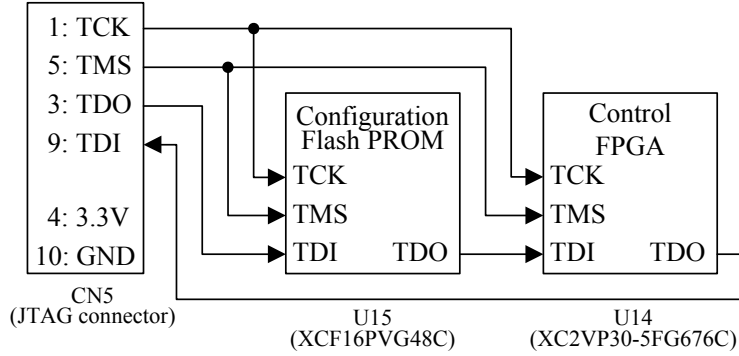


Figure 5: FPGA configuration chain on the SASEBO-R

Table 13: Pin assignment of the JTAG Connector (CN5)

Pin1	TCK	Pin2	GND
Pin3	TDO	Pin4	3.3V
Pin5	TMS	Pin6	
Pin7	TDI	Pin8	GND

Table 14: Configuration mode settings (SW5)

Dip1	M0	OFF
Dip2	M1	OFF
Dip3	M2	ON
Dip4	PWRDWN	OFF
Dip5	HSWAP	OFF
DipP6~8	Not used	

➤ **Clock source**

The clock source connection of the SASEBO-R is shown in Figure 6. One 24-MHz oscillator is connected to the control FPGA. Two clock sources are provided to the cryptographic LSI from the control FPGA, the clock oscillator socket (X1 and X2), and the SMA connector (J5 and J6). An external clock can be supplied to the control FPGA through the J7 SMA connector.

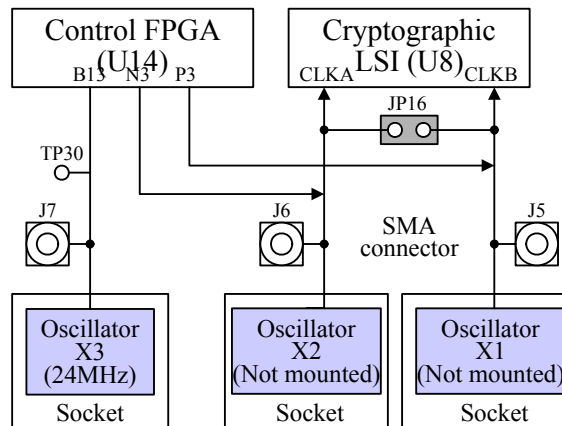


Figure 6: Clock source connection

➤ **Host Interface**

RS-232 and USB is provided on the SASEBO-R for communicating with the host PC. Tables 15 and 16 shows the signal assignments of the RS-232 and USB interfaces. A 9-pin female-female straight cable connects the SASEBO-R to the PC through the RS-232 interfaces. The driver and API of the USB interface for Windows/Linux/Macintosh are provided by FTDI (Future Technology Device International Ltd. <http://www.ftdichip.com/Products/FT245R.htm>).

Table 15: Signal assignment on the RS-232 interface

Signal	CN8 (XM2C-0912-111)	U17 (ADM3202ARN)		U14 (XC2VP30-5FG676C)
TX	2 pin	14 pin	11 pin	AB14
RX	3 pin	13 pin	12 pin	AC15
CTS	8 pin	7 pin	10 pin	AB15
RTS	7 pin	8 pin	9 pin	AA15

Table 16: Signal assignment on the USB interface

Signal	CN7 (XM7B-0422)	U13 (FT245RL)	U14 (XC2VP30-5FG676C)
USBDP	2 pin	15 pin	-
USBDM	3 pin	16 pin	-
USBD0	-	1 pin	AB16
USBD1	-	5 pin	AA16
USBD2	-	3 pin	AB17
USBD3	-	11 pin	AE14
USBD4	-	2 pin	AC17
USBD5	-	9 pin	AC14
USBD6	-	10 pin	AD14
USBD7	-	6 pin	AB20
USBTXE	-	22 pin	AE19
USBRXF	-	23 pin	AD20
USBRD	-	13 pin	AD17
USBWR	-	14 pin	AF19
USBPWREN	-	12 pin	AD15

4. BOARD SCHEMATIC AND LAYOUT

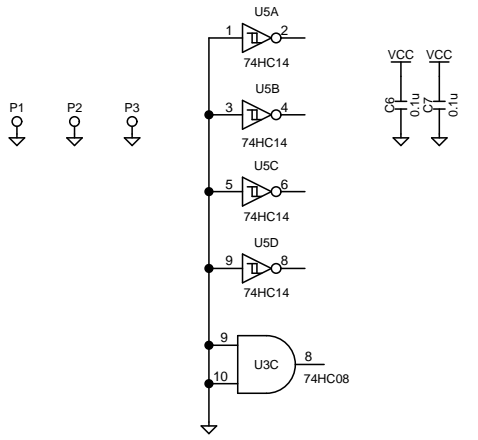
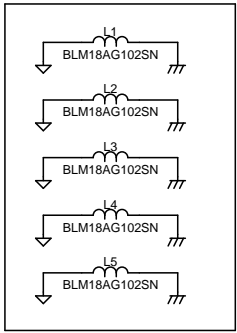
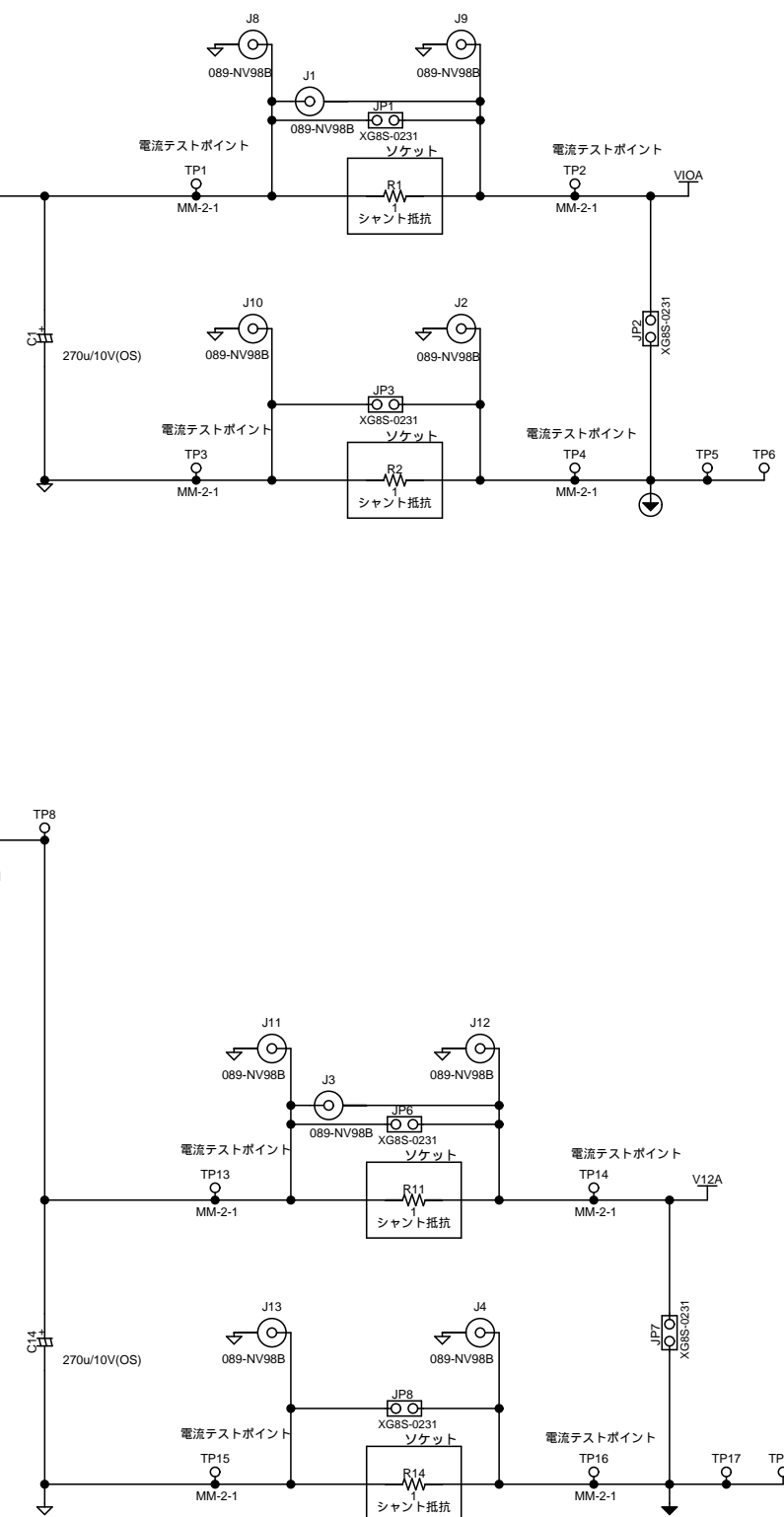
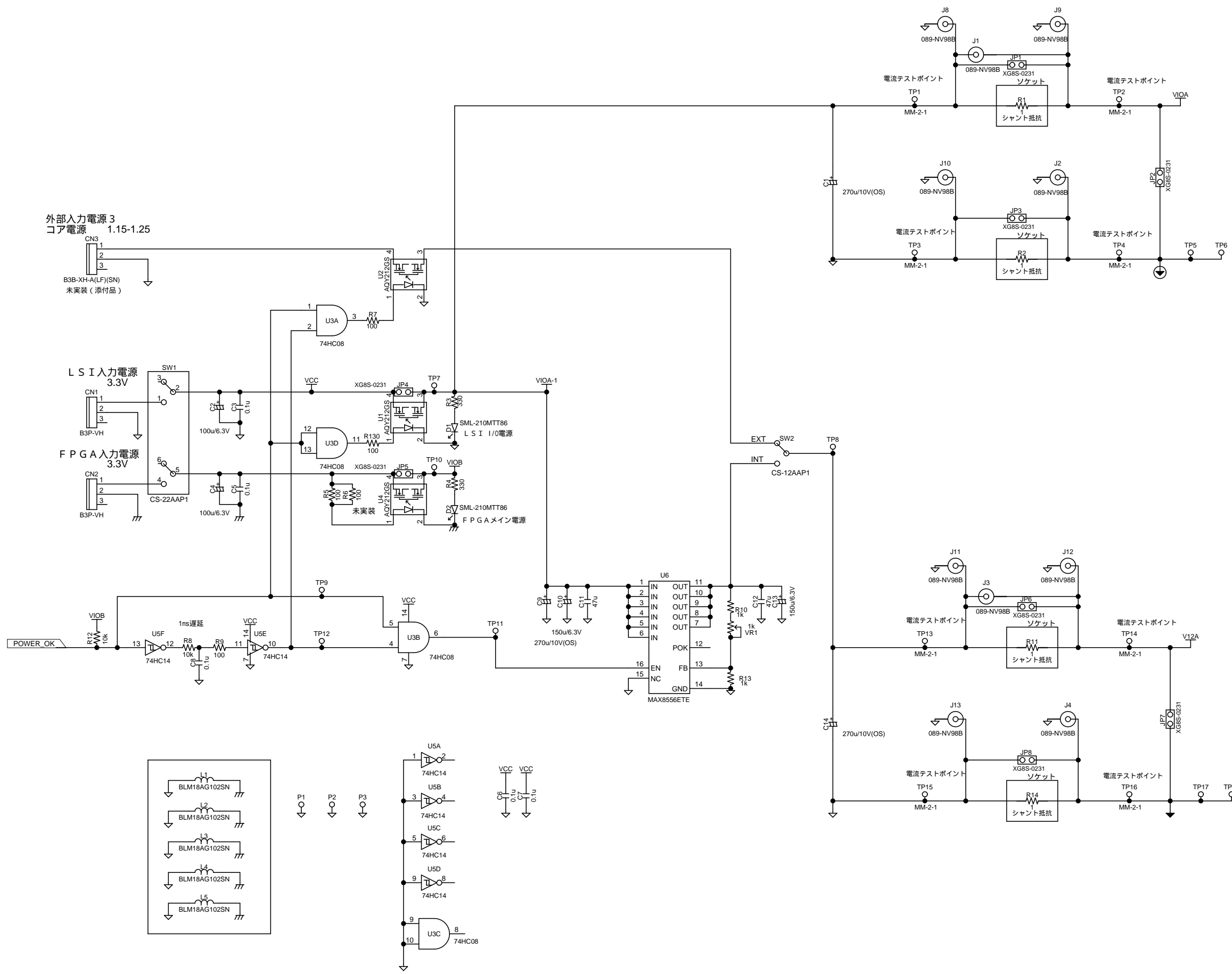
The parts list for the SASEBO-R is shown in Table 17. The board schematic and layout of the SASEBO-R are presented in pages 17 to 35.

➤ Cryptographic LSI Block		
Power supply	-----	page 17
QFP socket	-----	page 18
QFP footprint	-----	page 19
➤ Control FPGA Block		
FPGA I/O, Power supply, FPGA configuration	-----	page 20
FPGA I/O	-----	page 21
Power supply	-----	page 22
➤ Board Layout		
Dimensional drawing	-----	page 23
Part-side silk screen	-----	page 24
Part-side drawing	-----	page 25
Solder-side silk screen	-----	page 26
Solder-side drawing	-----	page 27
➤ Board		
L1 (Part-side)	-----	page 28
L2 (Internal layer)	-----	page 29
L3 (Internal layer)	-----	page 30
L4 (Internal layer)	-----	page 31
L5 (Internal layer)	-----	page 32
L6 (Internal layer)	-----	page 33
L7 (Internal layer)	-----	page 34
L8 (Solder-side)	-----	page 35

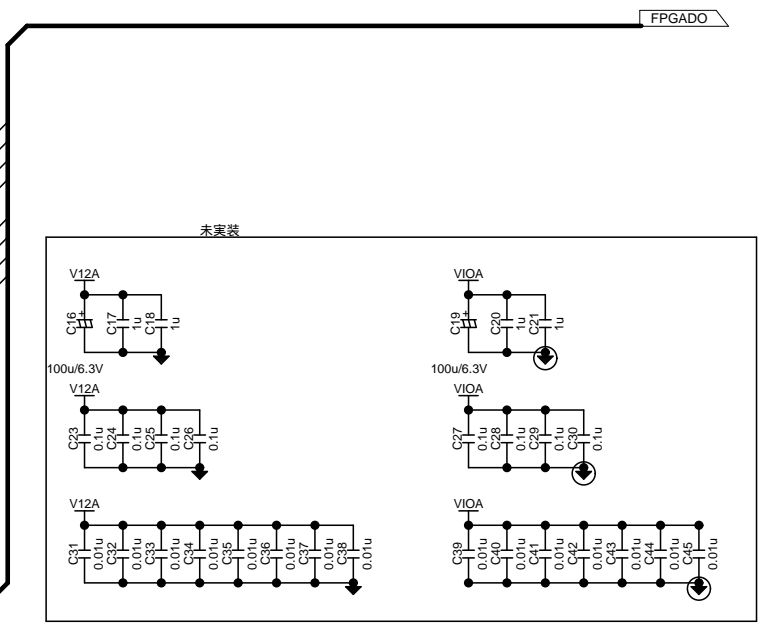
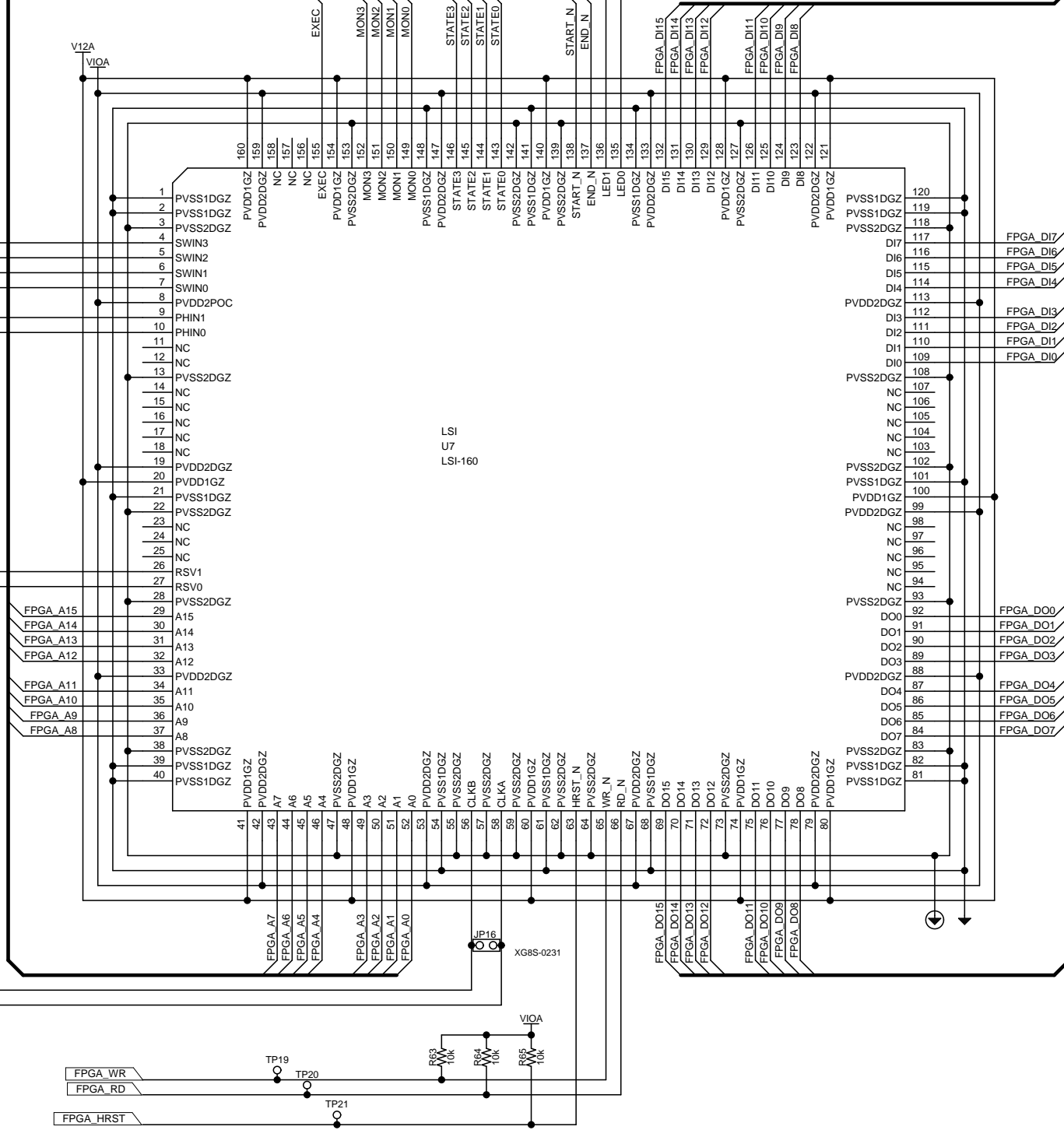
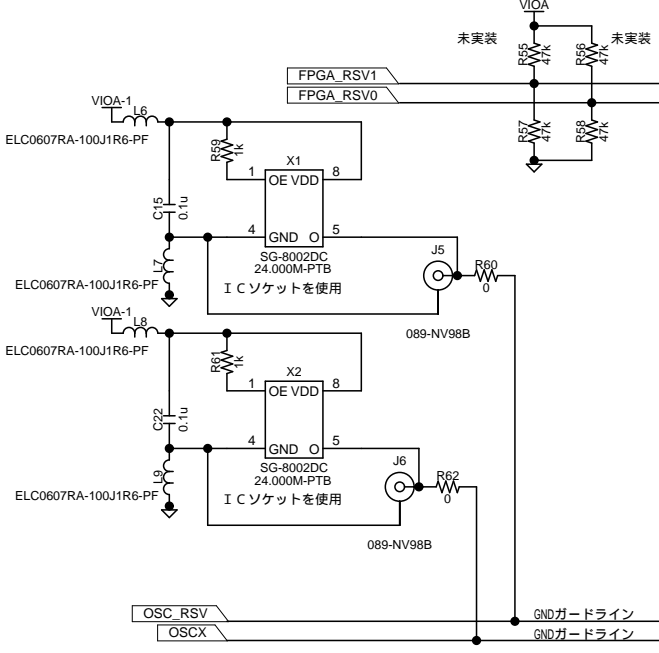
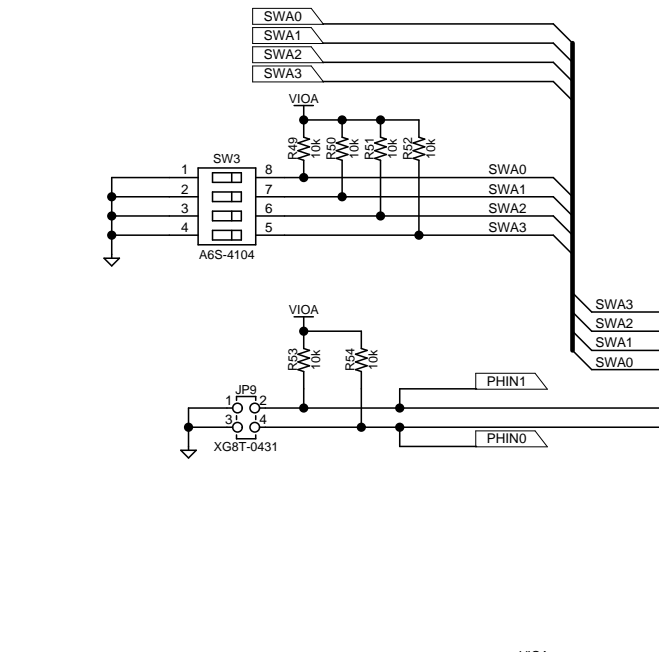
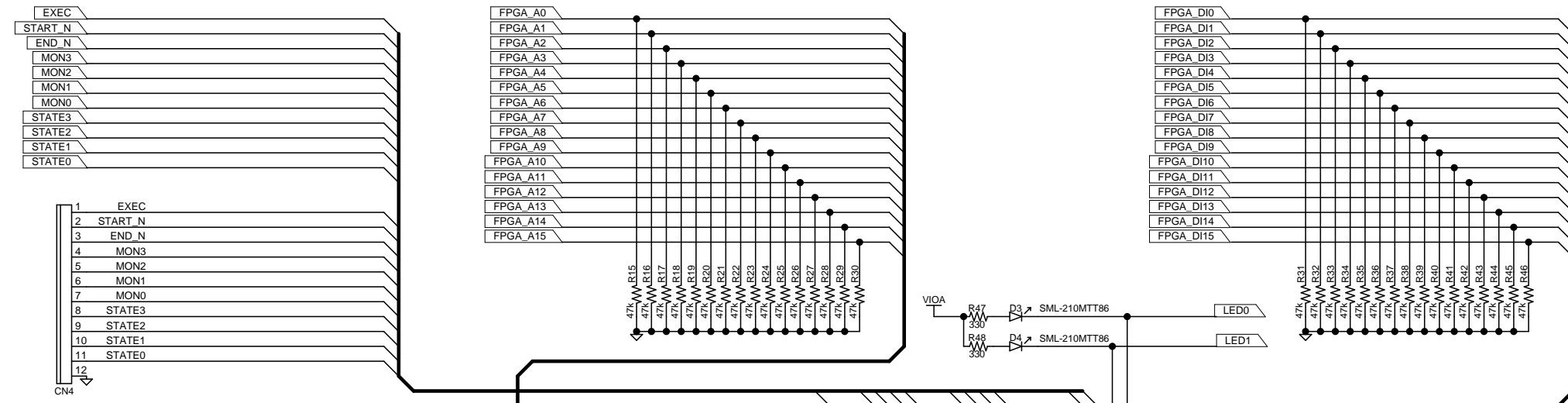
Table 17: Parts List

Board Name	SASEBO-R			
Model Number	E3-93995-1			
Description	Part Number	Maker	Qty	Reference Designator
Ceramic Capacitor	GRM155F11H103ZA57E	MURATA	31	C31,C32,C33,C34,C35,C36,C37,C38,C39,C40,C41,C42,C43,C44,C45,C60,C61,C62,C63,C64,C65,C66,C67,C68,C69,C70,C71,C72,C73,C74,C96,C134,C135,C136,C137,C138,C139,C140,C141,C142,C143,C144,C145,C146,C147,C148,C149,C150,C151,C152,C153,C154,C155,C156,C157,C158,C159,C160,C161,C162,C163
Ceramic Capacitor	GRM155F11E104ZA01D	MURATA	39	C3,C5,C6,C7,C8,C15,C22,C23,C24,C25,C26,C27,C28,C29,C30,C52,C53,C54,C55,C56,C57,C58,C59,C77,C78,C80,C81,C82,C83,C84,C85,C94,C97,C98,C99,C100,C101,C104,C105,C106,C118,C119,C120,C121,C124,C125,C126,C127,C128,C129,C130,C131,C132,C133,C103,C165
Ceramic Capacitor	GRM188B11H102KA01D	MURATA	1	C92
Ceramic Capacitor	GRM155F10J105ZE01D	MURATA	11	C17,C18,C20,C21,C47,C48,C50,C51,C75,C108,C109,C110,C111,C113,C114,C116,C117,C122,C123
Ceramic Capacitor	JMK316BJ476ML-T	TAIYO YUDEN	5	C11,C12,C88,C89,C102,C164
Capacitor	EMV-6R3ADA101MF55G	Nippon Chemi-Con	7	C2,C4,C16,C19,C46,C49,C76,C93,C107,C112,C115
Capacitor	EEFUE0J151	Panasonic	4	C10,C13,C87,C91
Capacitor	APSA100ELL271MHB5S	Nippon Chemi-Con	7	C1,C9,C14,C79,C86,C90,C95
Resistor	RK73Z1JTTD 0Ω	KOA	4	R60,R62,R100,R101
Resistor	RR0816-101-D	SSM	4	R5,R6,R7,R9,R69,R92,R130
Resistor	RR0816-103-D	SSM	20	R8,R12,R49,R50,R51,R52,R53,R54,R63,R64,R65,R66,R73,R79,R118,R119,R120,R121,R122,R129
Resistor	RR0816-102-D	SSM	18	R10,R13,R59,R61,R67,R68,R71,R74,R75,R76,R77,R78,R83,R90,R91,R93,R94,R128
Resistor	RR0816-220-D	SSM	3	R82,R84,R85
Resistor	RR0816-202-D	SSM	1	R72
Resistor	RR0816-331-D	SSM	8	R3,R4,R47,R48,R124,R125,R126,R127
Resistor	RR0816-472-D	SSM	9	R86,R87,R88,R95,R96,R97,R98,R99,R123
Resistor	RR0816-471-D	SSM	2	R81,R89
Resistor	RR0816-473-D	SSM	50	R15,R16,R17,R18,R19,R20,R21,R22,R23,R24,R25,R26,R27,R28,R29,R30,R31,R32,R33,R34,R35,R36,R37,R38,R39,R40,R41,R42,R43,R44,R45,R46,R55,R56,R57,R58,R102,R103,R104,R105,R106,R107,R108,R109,R110,R111,R112,R113,R114,R115,R116,R117
Diode	1SS352(-TPH3)	TOSHIBA	1	D5
DIP Switch	A6S-4104-H	OMRON	2	SW3,SW6
DIP Switch	A6S-8104-H	OMRON	1	SW5

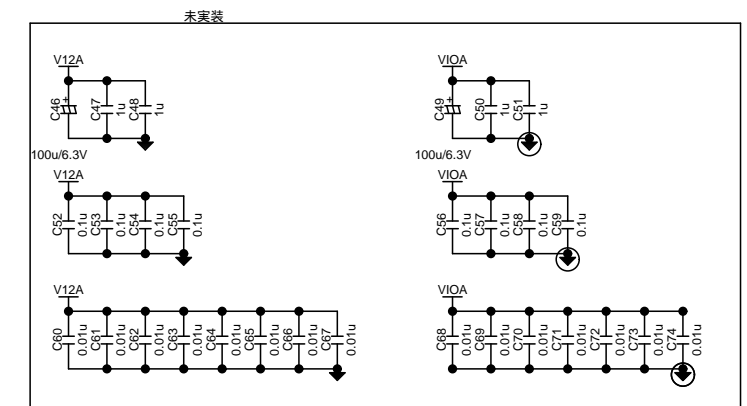
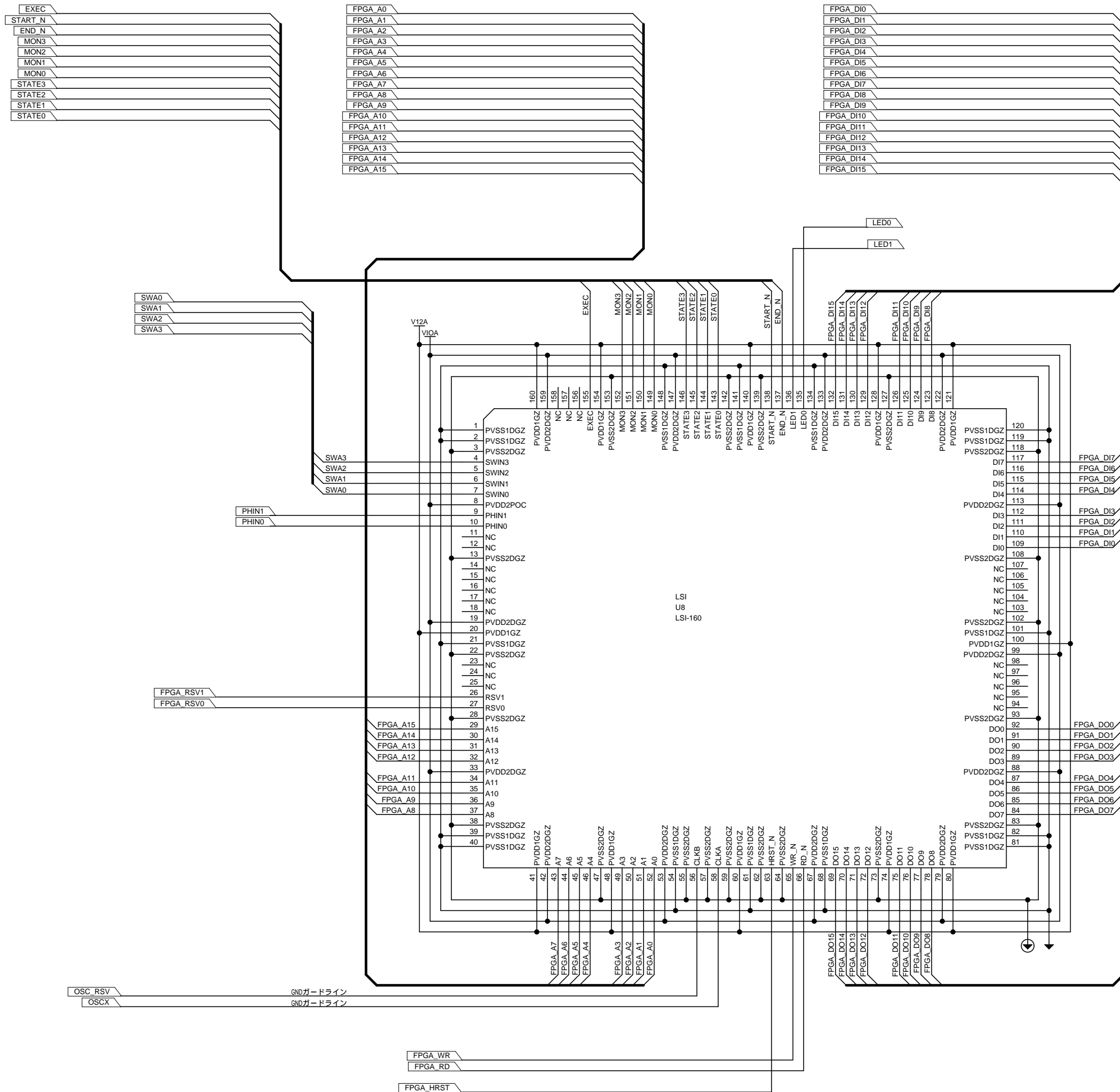
Push Button	B3S-1000	OMRON	2	SW4,SW7
Switch, Slide	CS-12AAP1	Nikkai	1	SW2
Switch, Slide	CS-22AAP1	Nikkai	1	SW1
LSI	LSI-160	TSMC	1	U7
QFP Socket	OTQ-160-0.65-5	Enplas	1	U8
FPGA	XC2VP30-5FG676C	Xilinx	1	U14
EEPROM	XCF16PVOG48C	Xilinx	1	U15
CMOS	SN74HC08NS	TI	2	U3,U9
CMOS	SN74HC14NS	TI	2	U5,U10
SRAM	IS62WV51216BLL-55TLI	ISSI	1	U18,U20
USB IC	FT245RL	FDI	1	U19
RS-232 Level Converter	ADM3202ARUZ	Analog Devices	1	U17
Reset IC	BD45292G	ROHM	1	U11
Regulator IC	MAX8556ETE	MAXIM	2	U6,U13
Regulator IC	PQ1U181M2ZP	SHARP	1	U16
Regulator IC	TPS72625DCQ	TI	1	U12
Inductor	ELC0607RA-100J1R6-PF	TDK	11	L6,L7,L8,L9,L10,L11,L12,L13,L14,L15,L16
Filter	BLM18AG102SN	MURATA	5	L1,L2,L3,L4,L5
LED	SML-210MTT86	ROHM	9	D1,D2,D3,D4,D6,D7,D8,D9,D10
Pin Header	A1-64PA-2.54DSA(71)	HIROSE	1	CN6
Connector	B3P-VH(LF)(SN)	JST	1	CN3
Connector	87832-1420	MOLEX	1	CN5
USB Connector	XM7B-0442	OMRON	1	CN8
D-sub Connector	XM2C-0912-111	OMRON	1	CN7
MOS Relay	G3VM-61GR1	OMRON	3	U1,U2,U4
SG-8002DC	24.000M-PTB	EPSON	1	X1,X2,X3
SMA Connector	T124 426 000N	TAKITEK	13	J1,J2,J3,J4,J5,J6,J7,J8,J9,J10,J11,J12,J13
Resistor	ERX1SJ1R0	Panasonic	6	R1,R2,R11,R14,R70,R80
Shunt	XG8S-0231	OMRON	9	JP1,JP3,JP4,JP5,JP6,JP8,JP11,JP13,JP16
Connector	B2P-SHF-1AA(LF)(SN)	JST	3	JP2,JP7,JP12
Jumper Socket	XG8T-0431	OMRON	2	JP9,JP10
IC Socket	R110-91-308	PRECI-DIP	3	



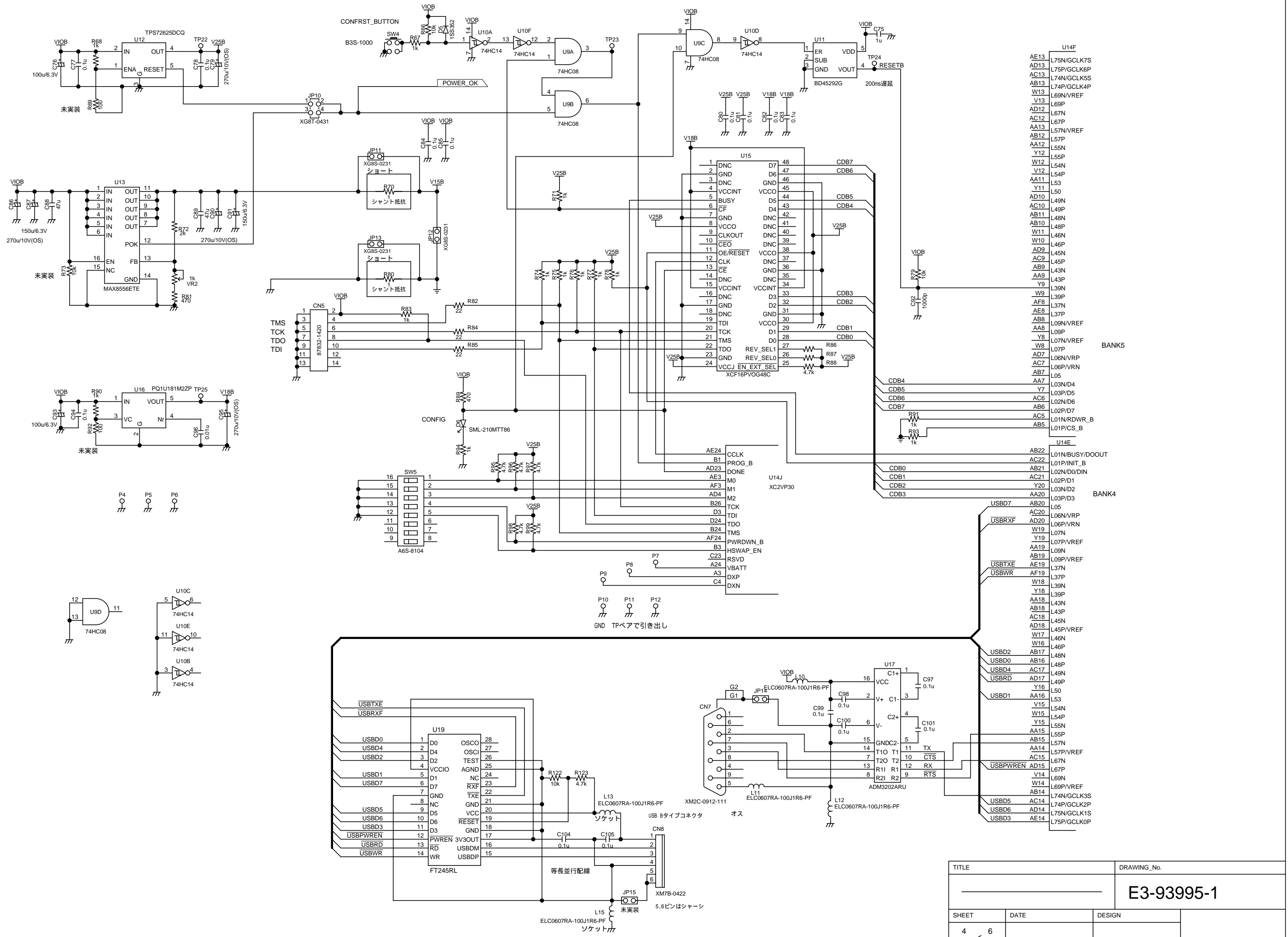
TITLE		DRAWING_No.	
		E3-93995-1	
SHEET	DATE	DESIGN	
1	6		



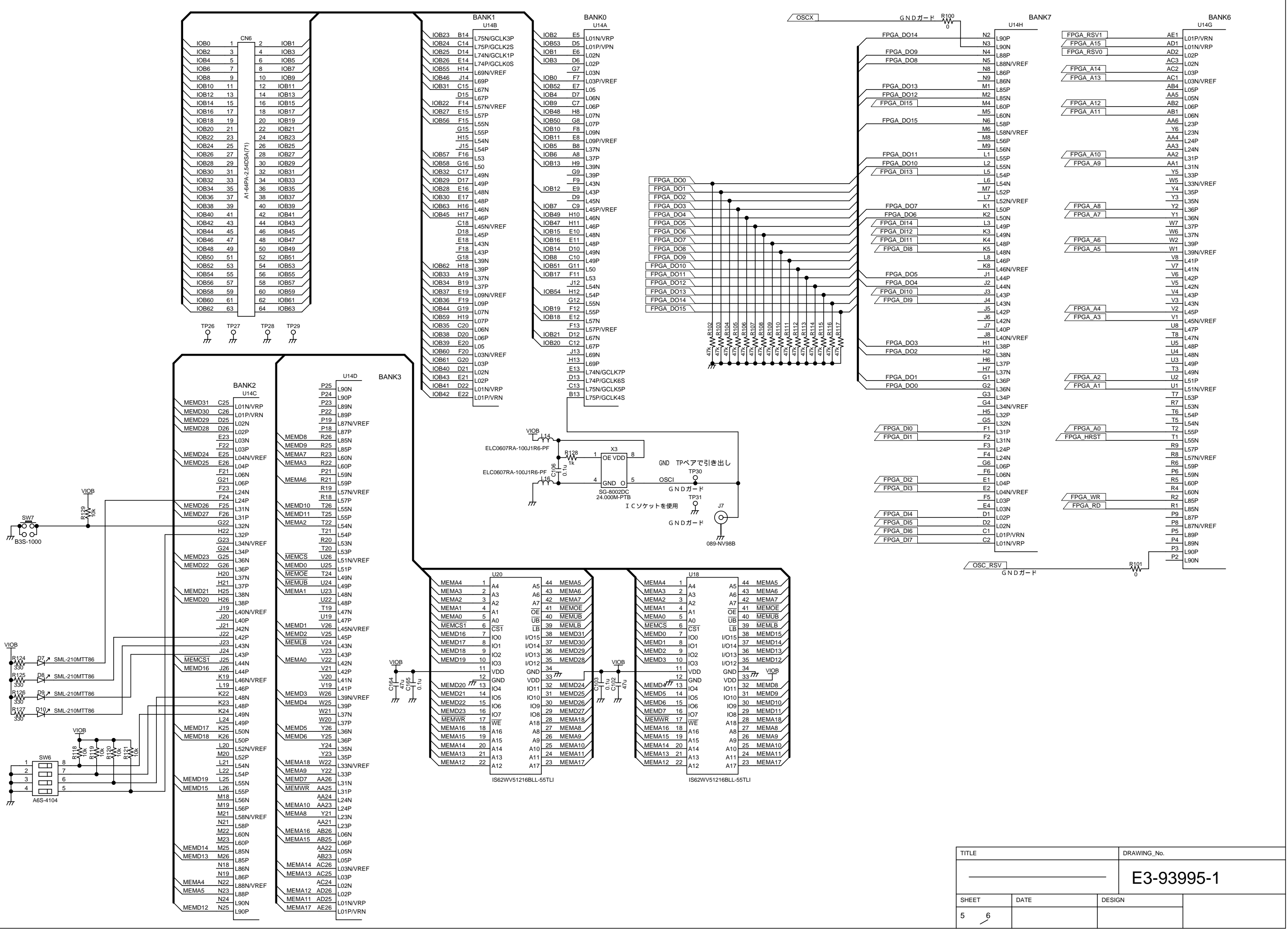
TITLE		DRAWING_No.	
		E3-93995-1	
SHEET	DATE	DESIGN	
2	6		



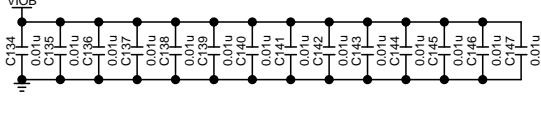
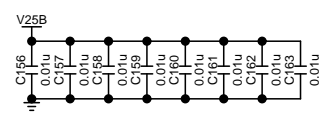
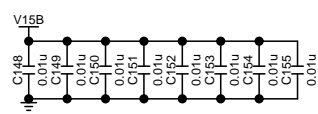
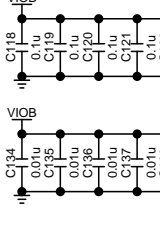
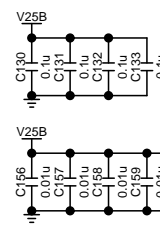
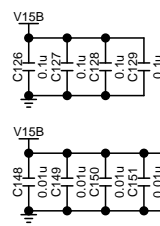
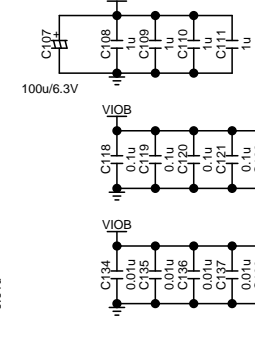
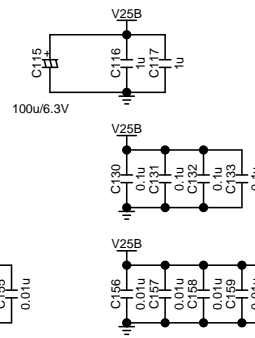
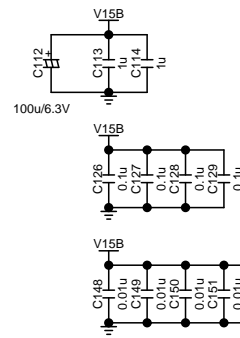
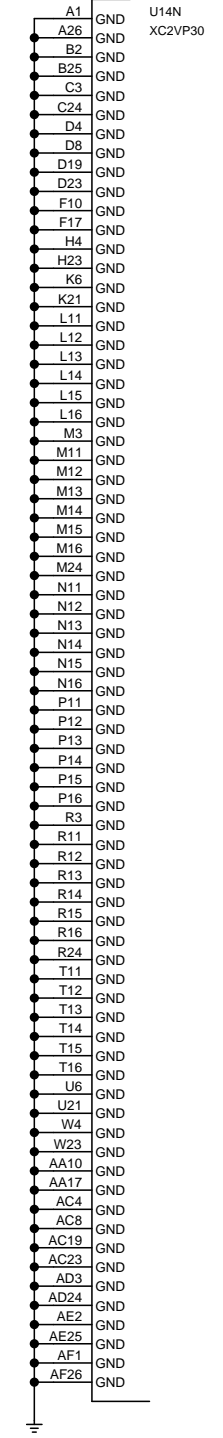
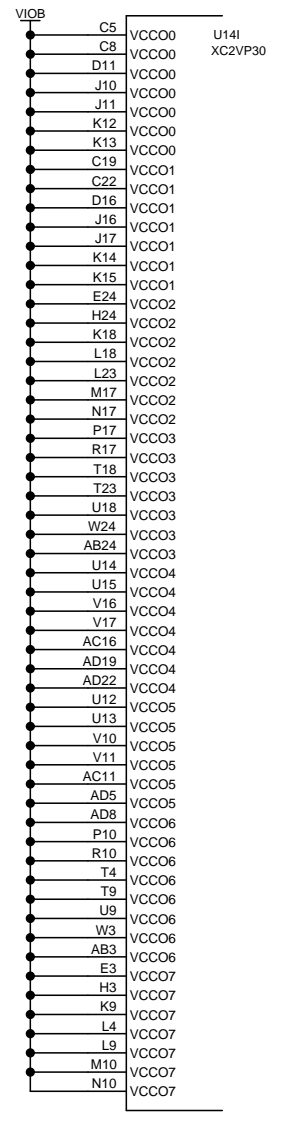
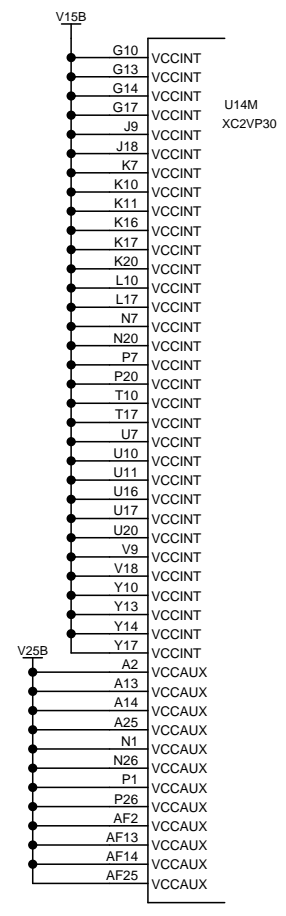
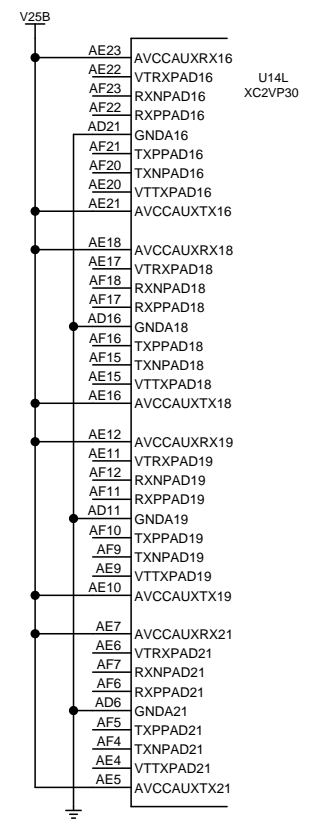
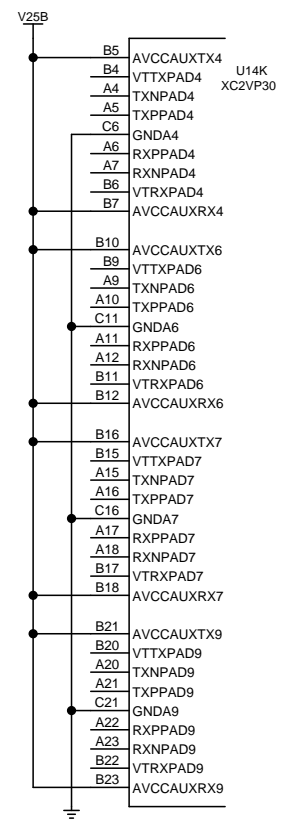
TITLE		DRAWING_No.	
		E3-93995-1	
SHEET	DATE	DESIGN	
3	6		



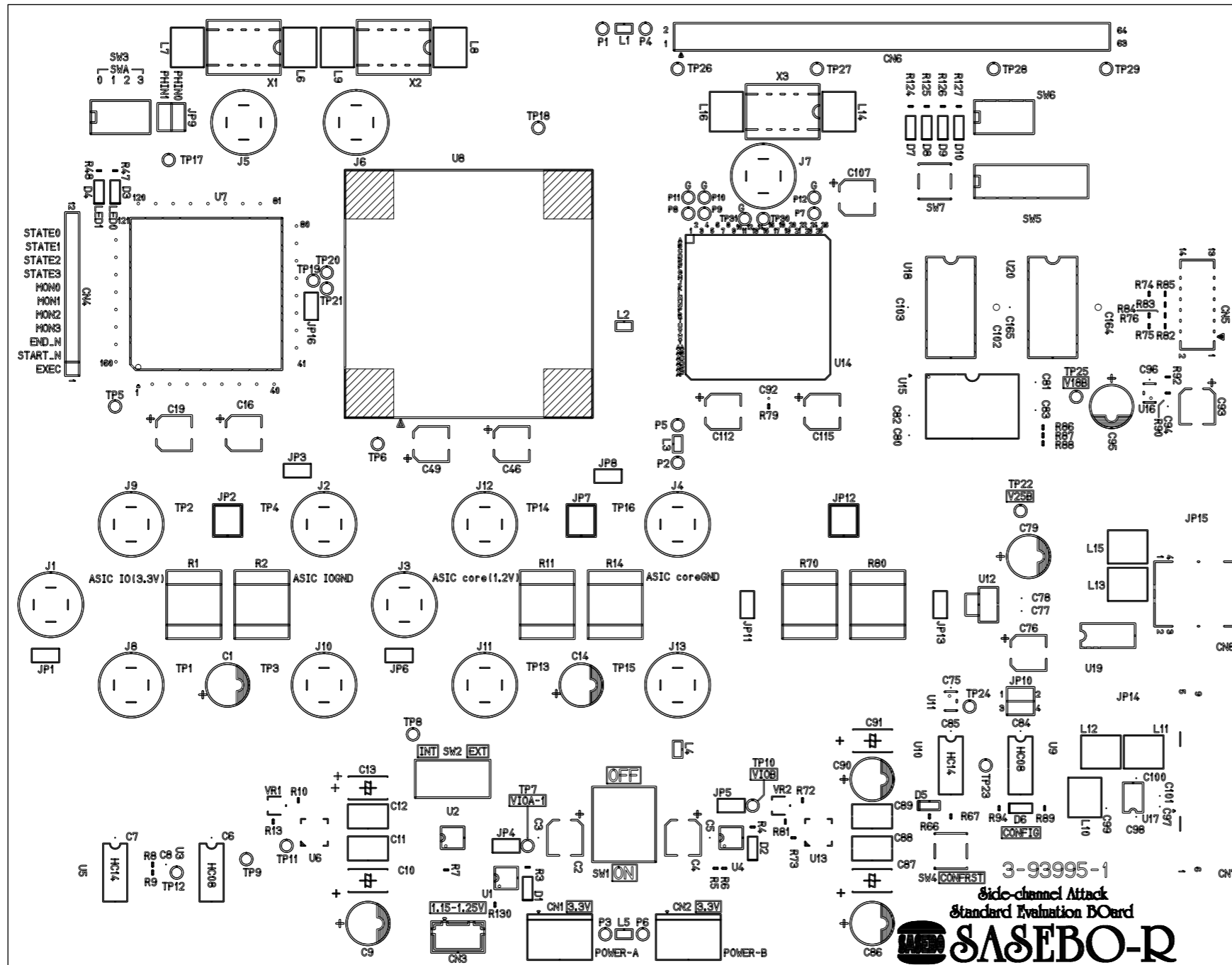
TITLE		DRAWING_No.	
		E3-93995-1	
SHEET	DATE	DESIGN	
4	6		



TITLE		DRAWING_No.	
		E3-93995-1	
SHEET	DATE	DESIGN	
5	6		

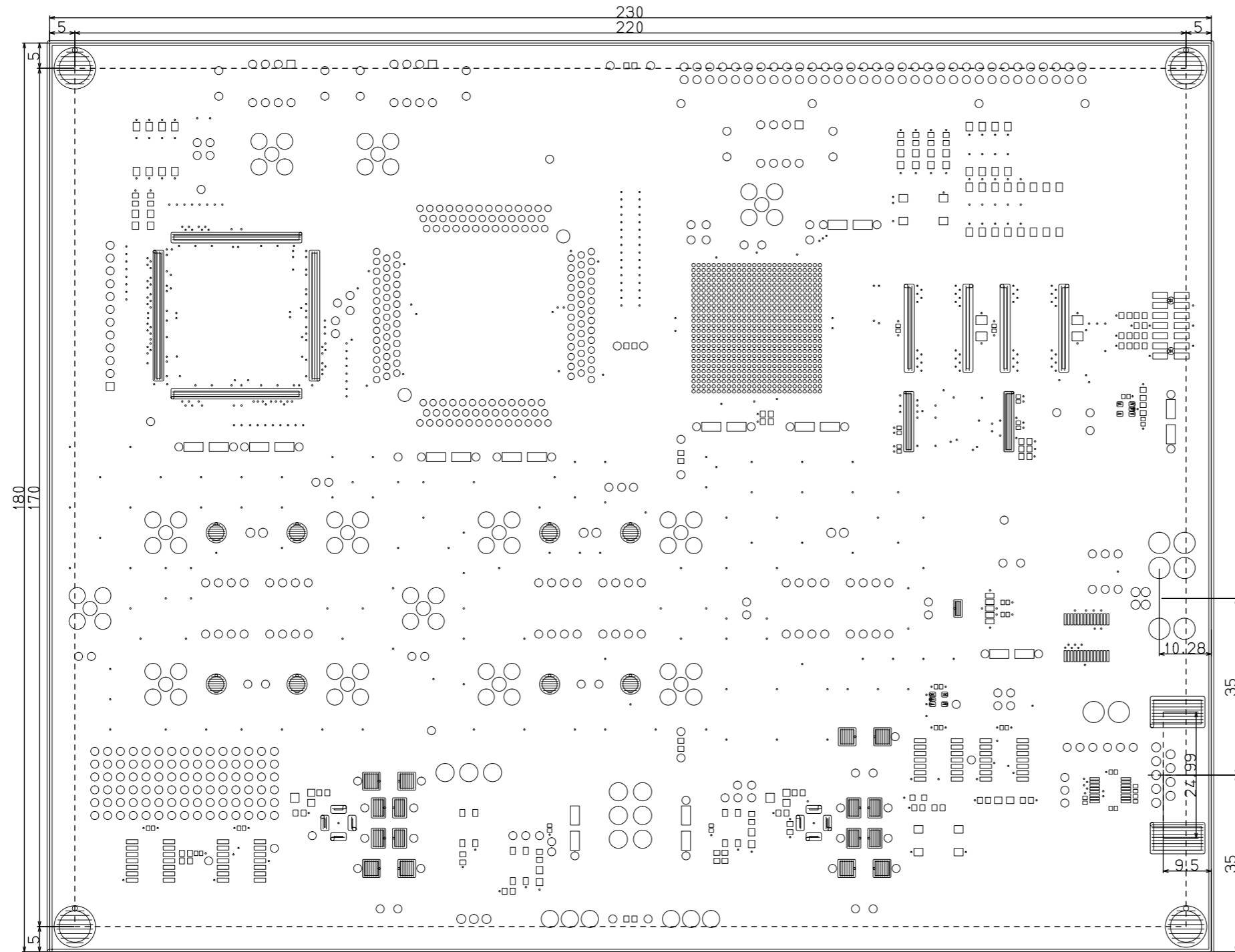


TITLE		DRAWING_No.	
		E3-93995-1	
SHEET	DATE	DESIGN	
6	6		

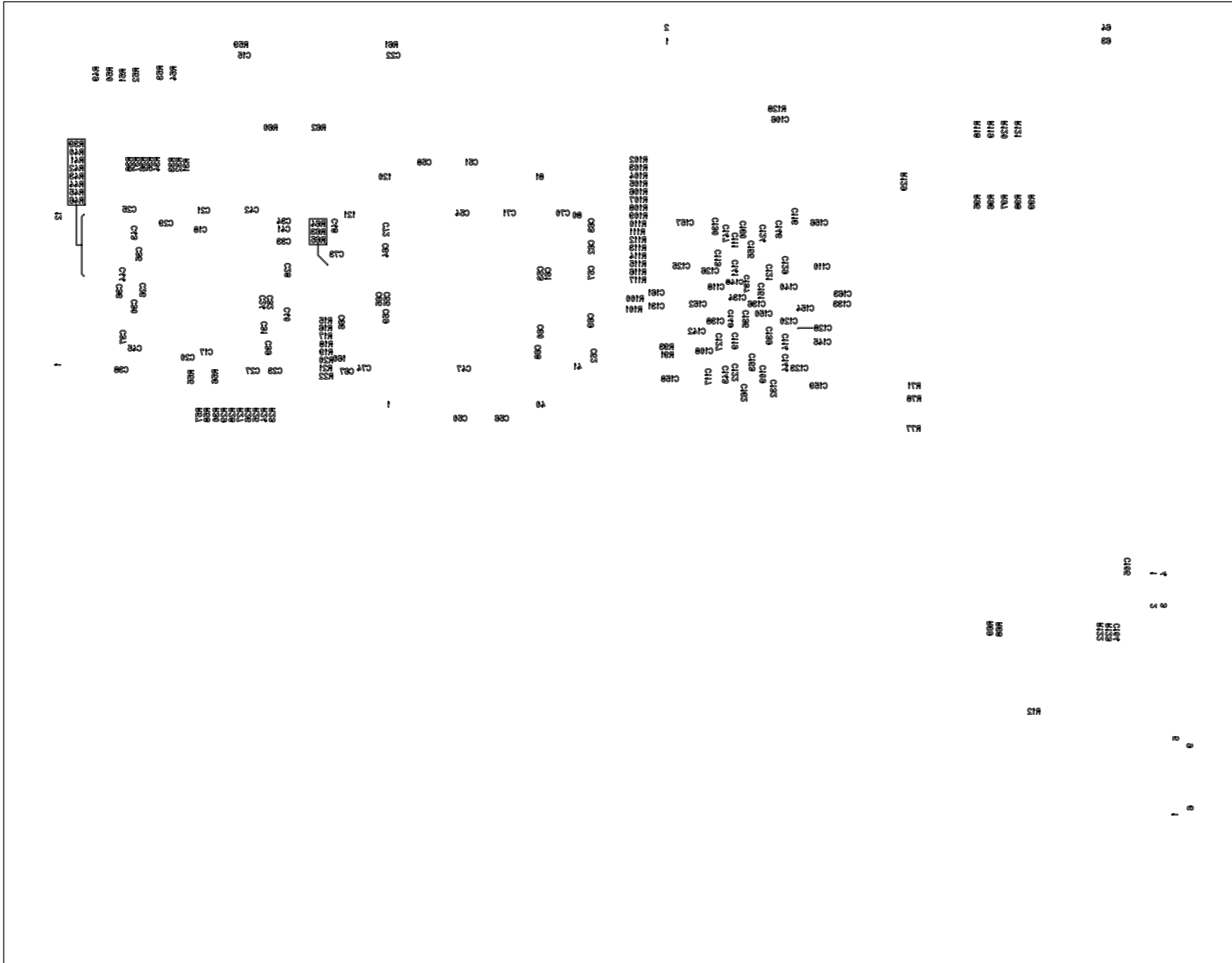


3-93995-1
 Side-channel Attack
 Standard Evaluation Board
SASEBO-R

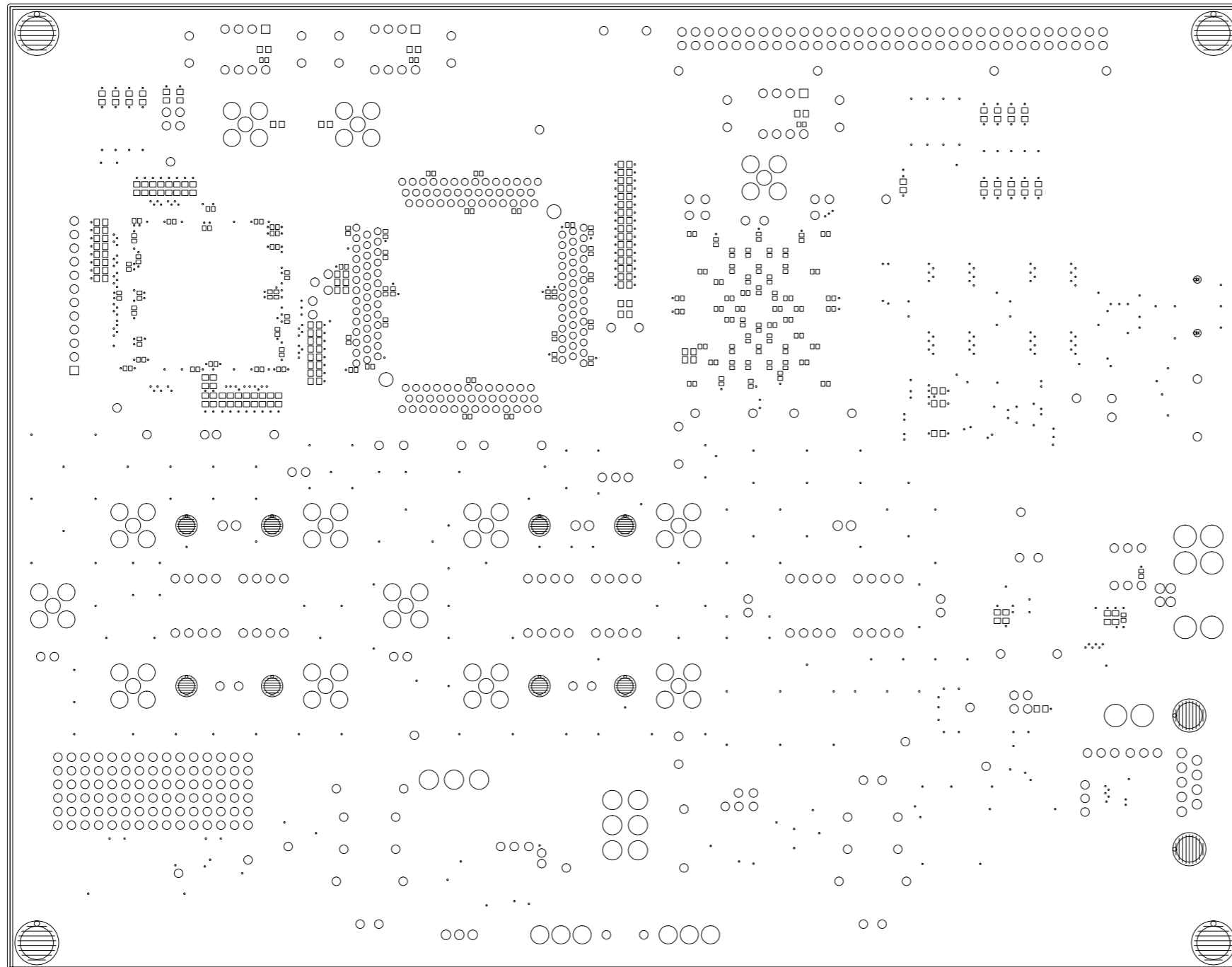
CS



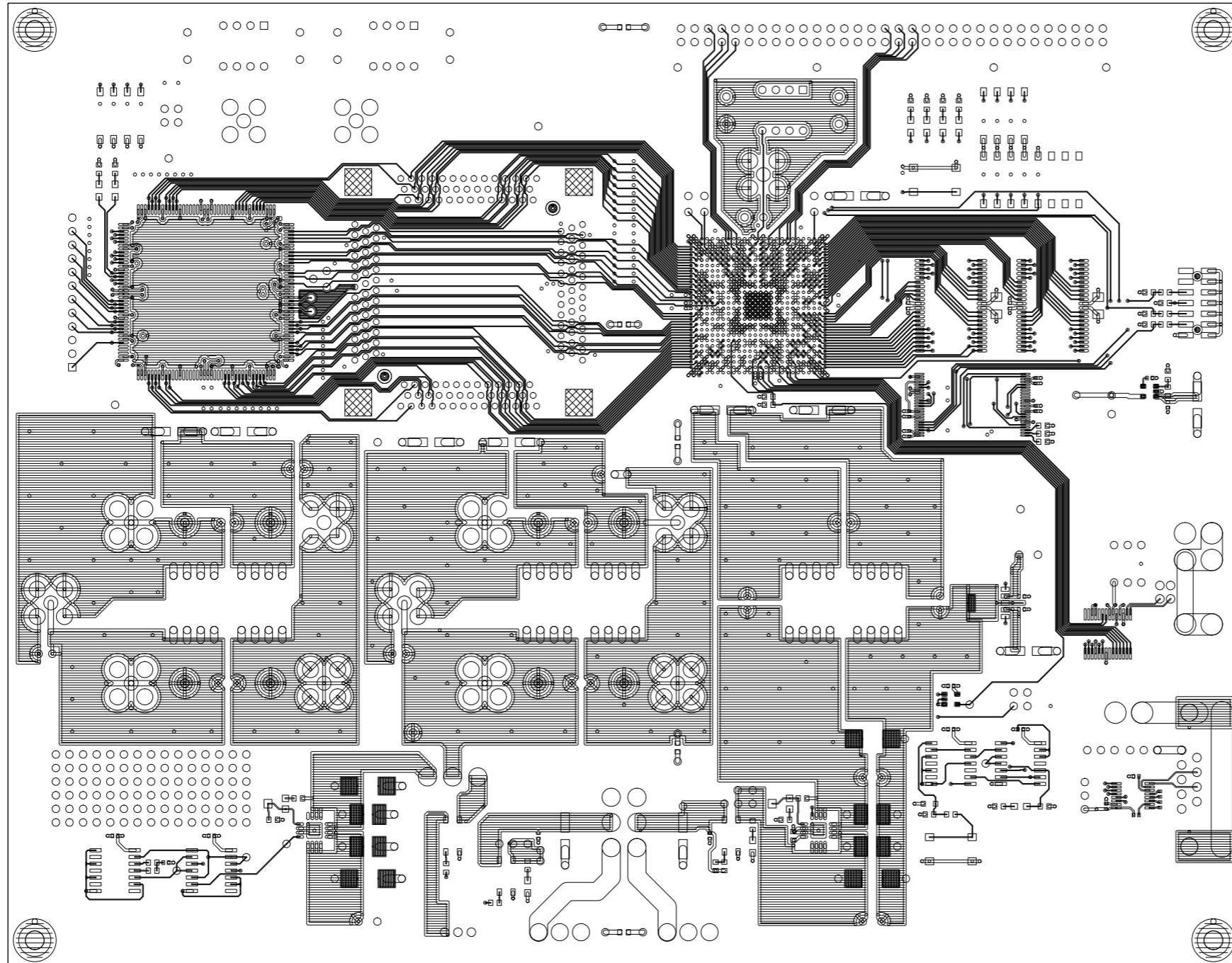
CR



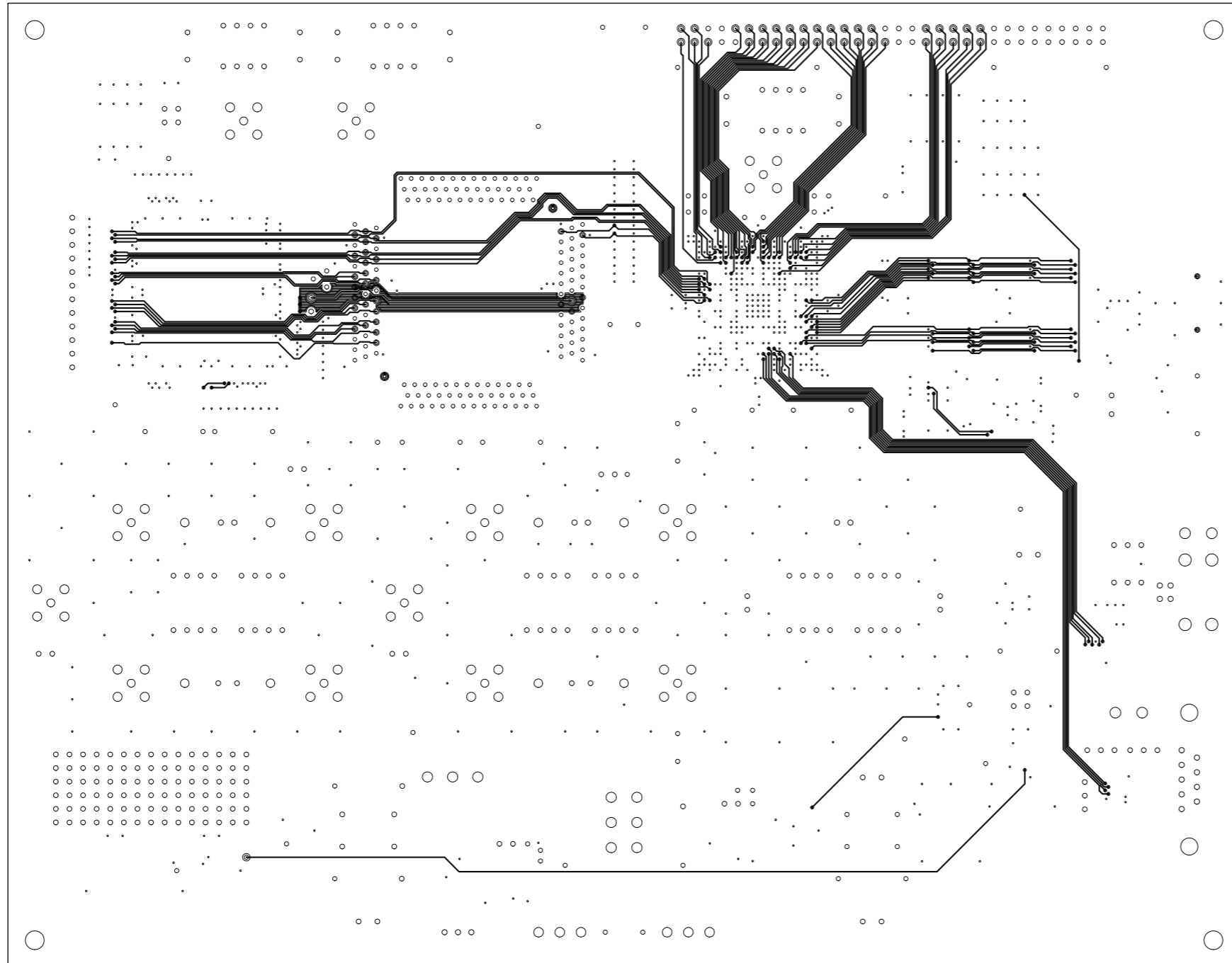
SS



SR

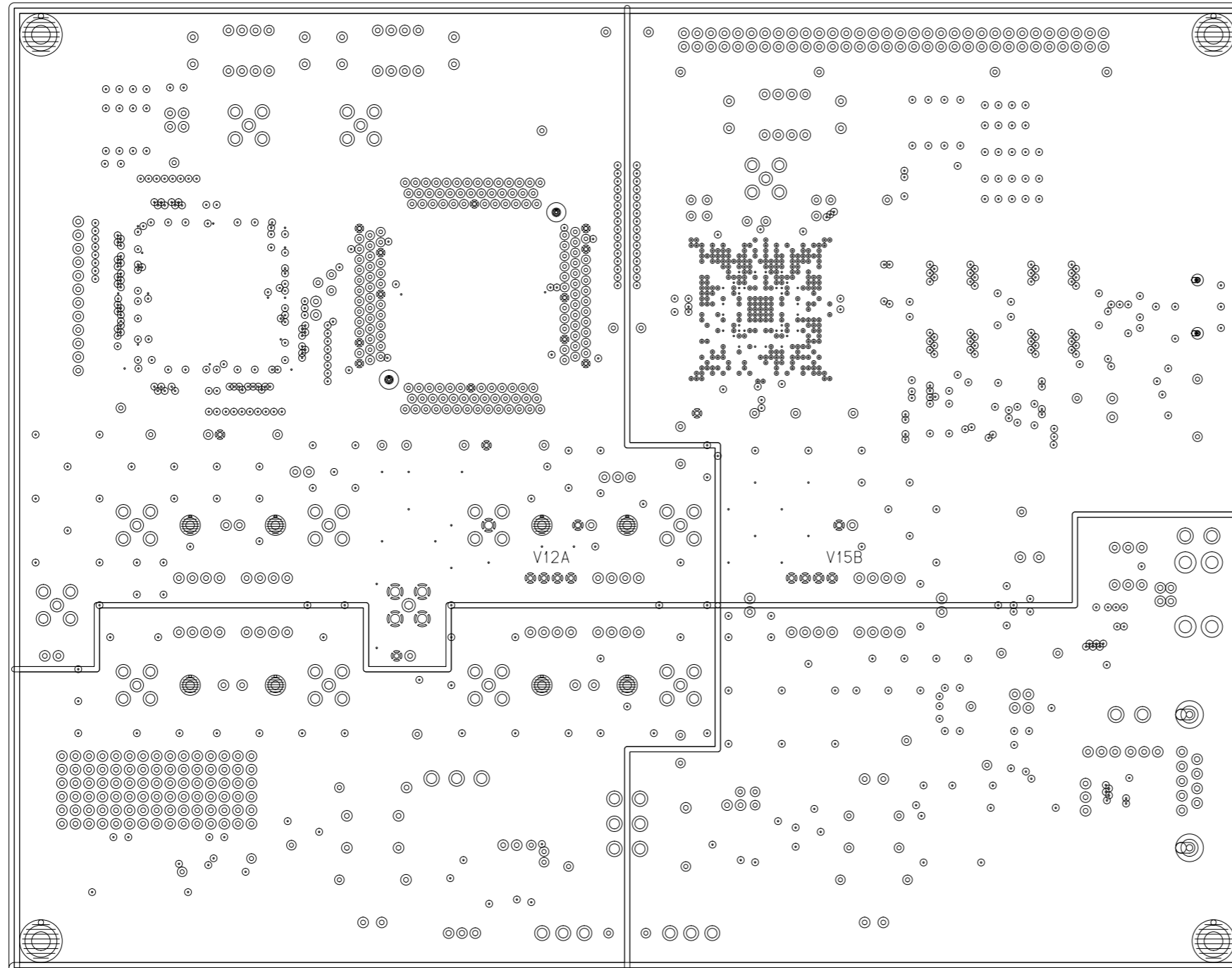


L1

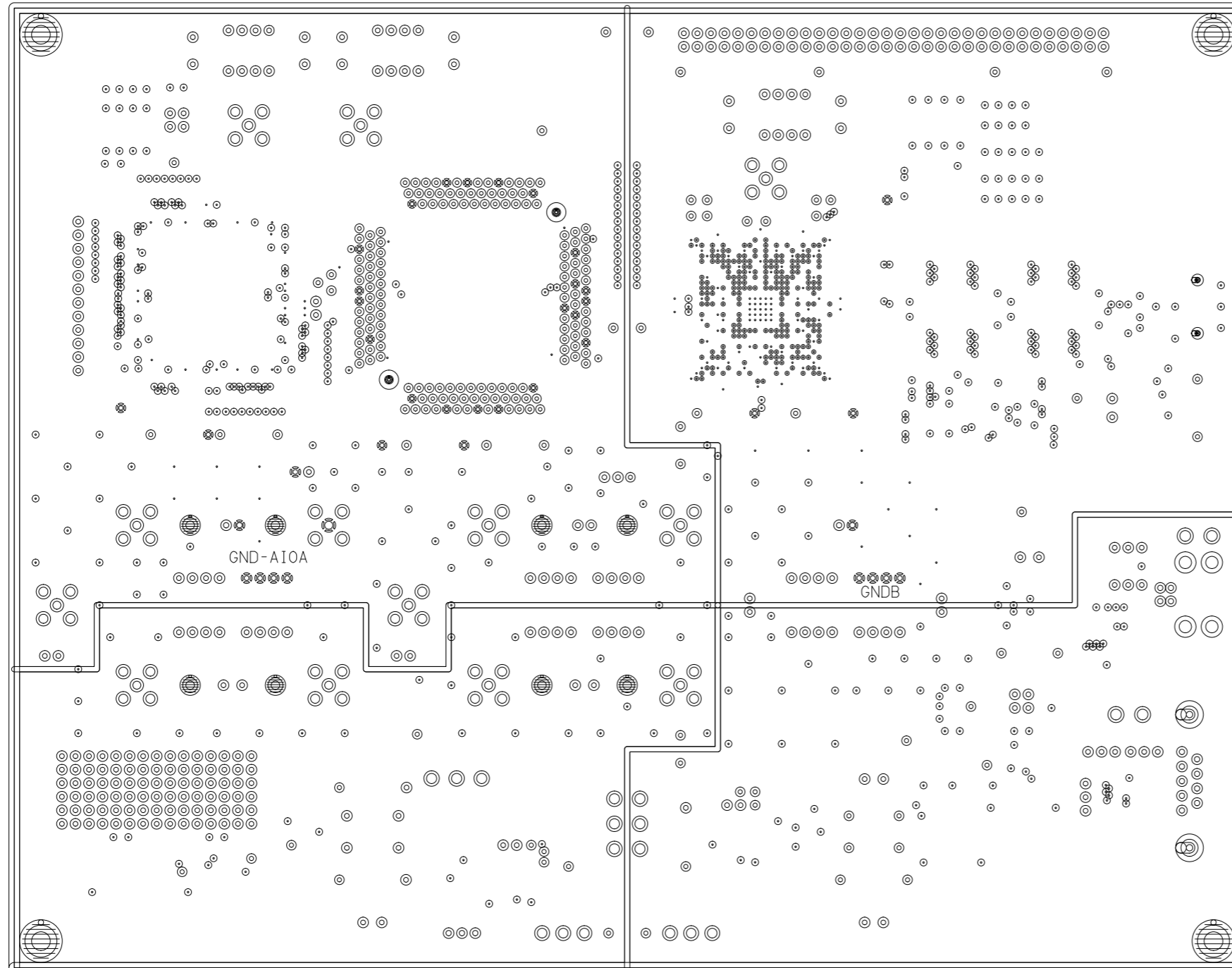


L5 sig

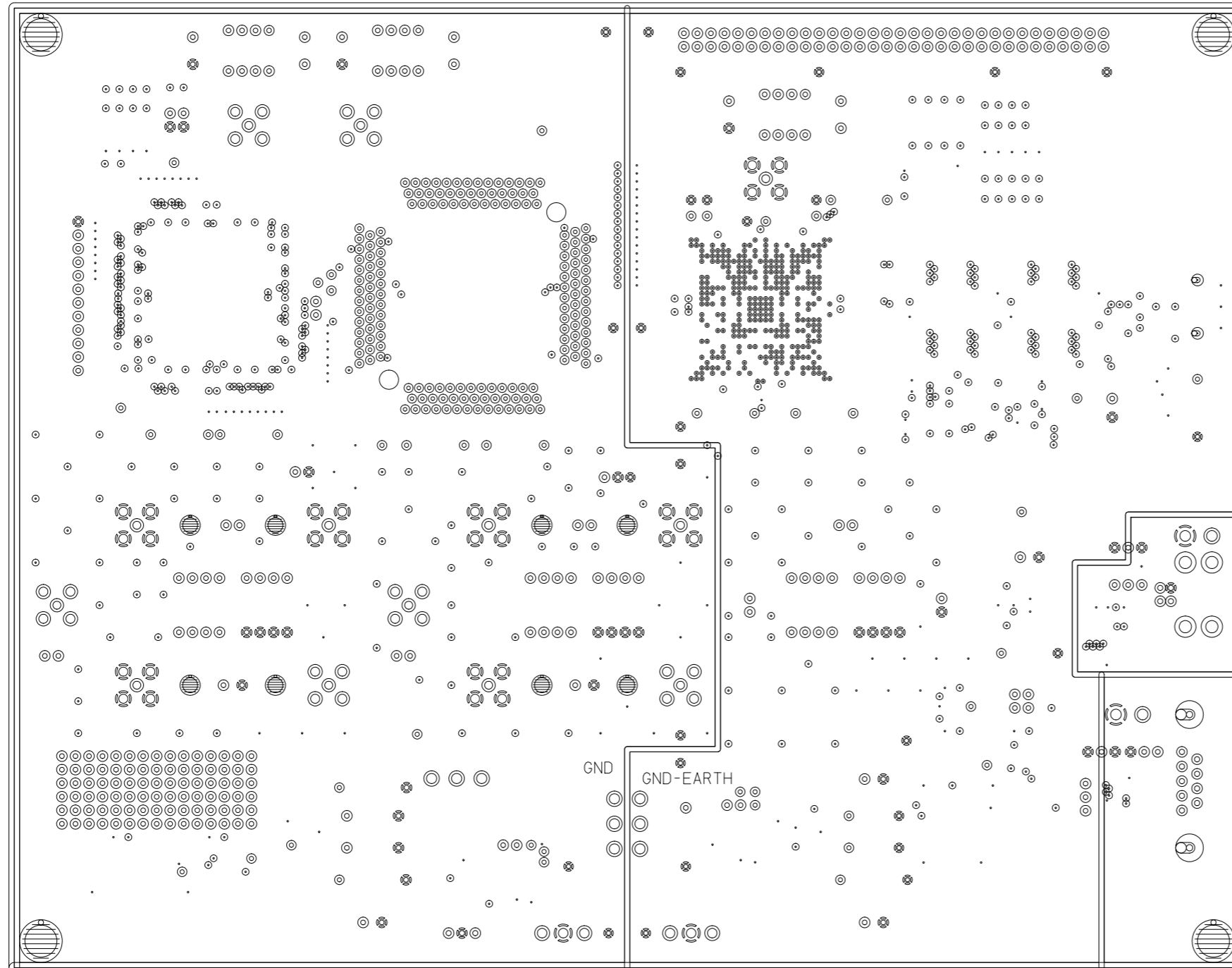
Evaluation Board LSI版
3-93995-1 2008/01/11



L4 V12A V15B

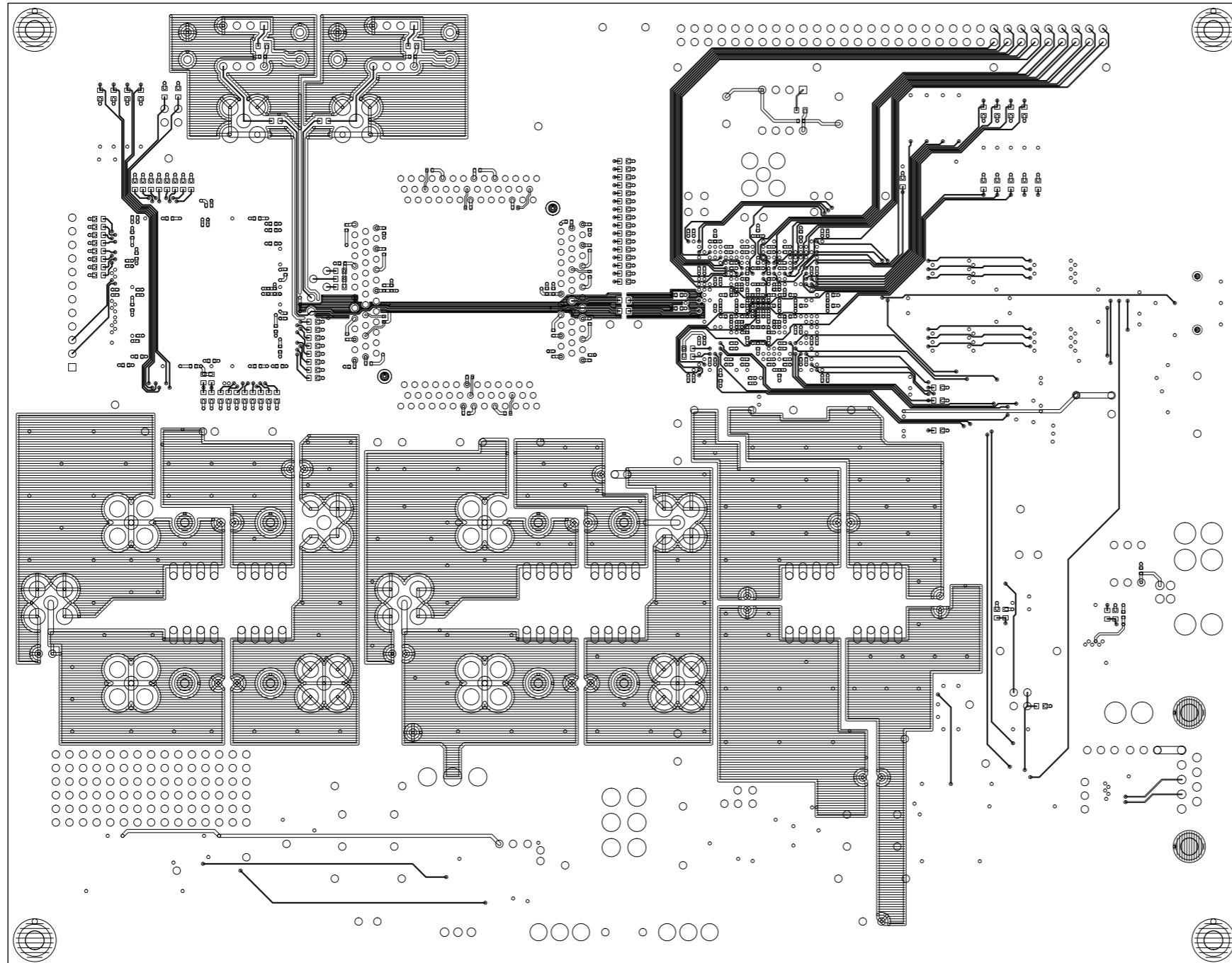


L3 GND-A10A GNDB

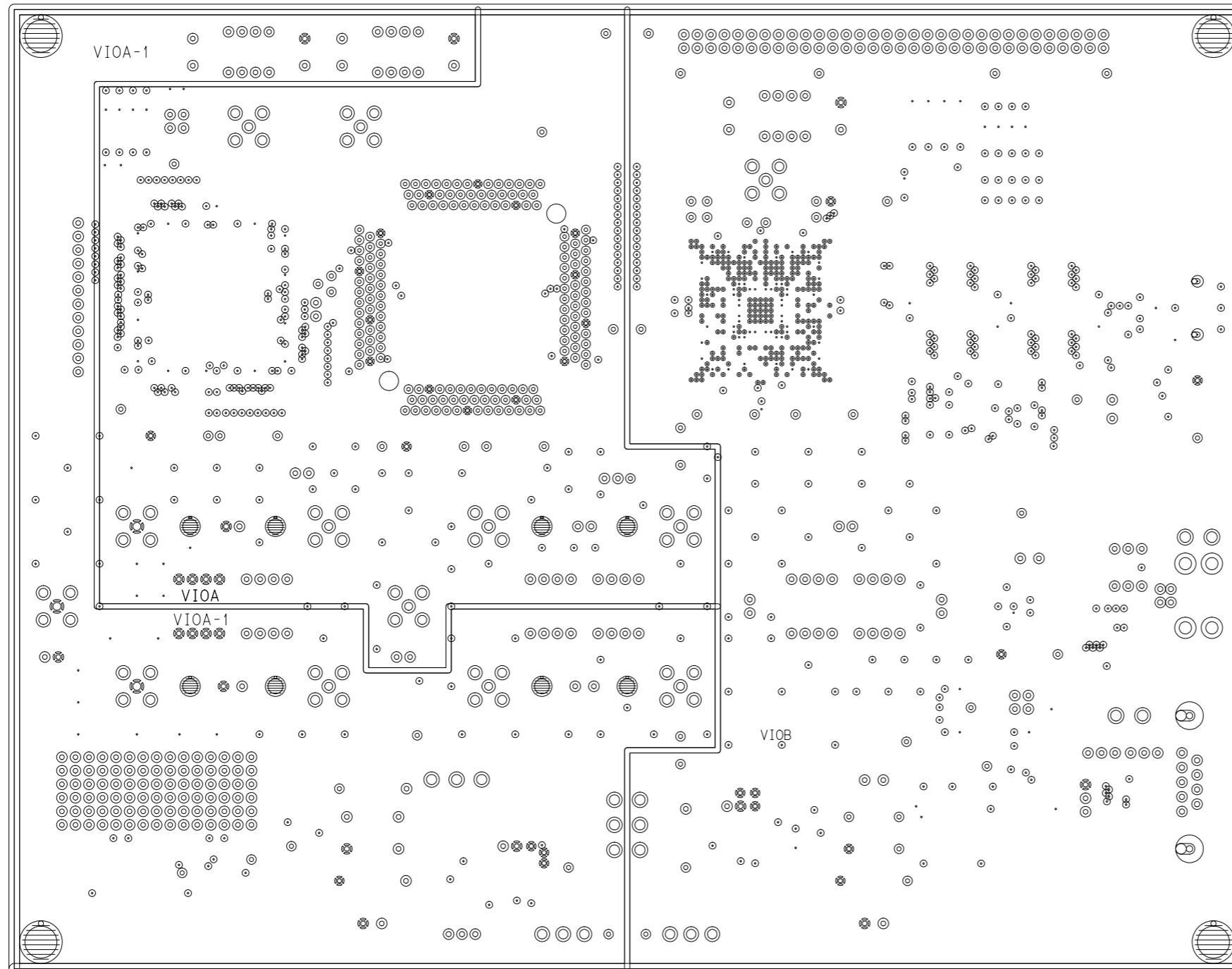


L2 GND GND-EARTH

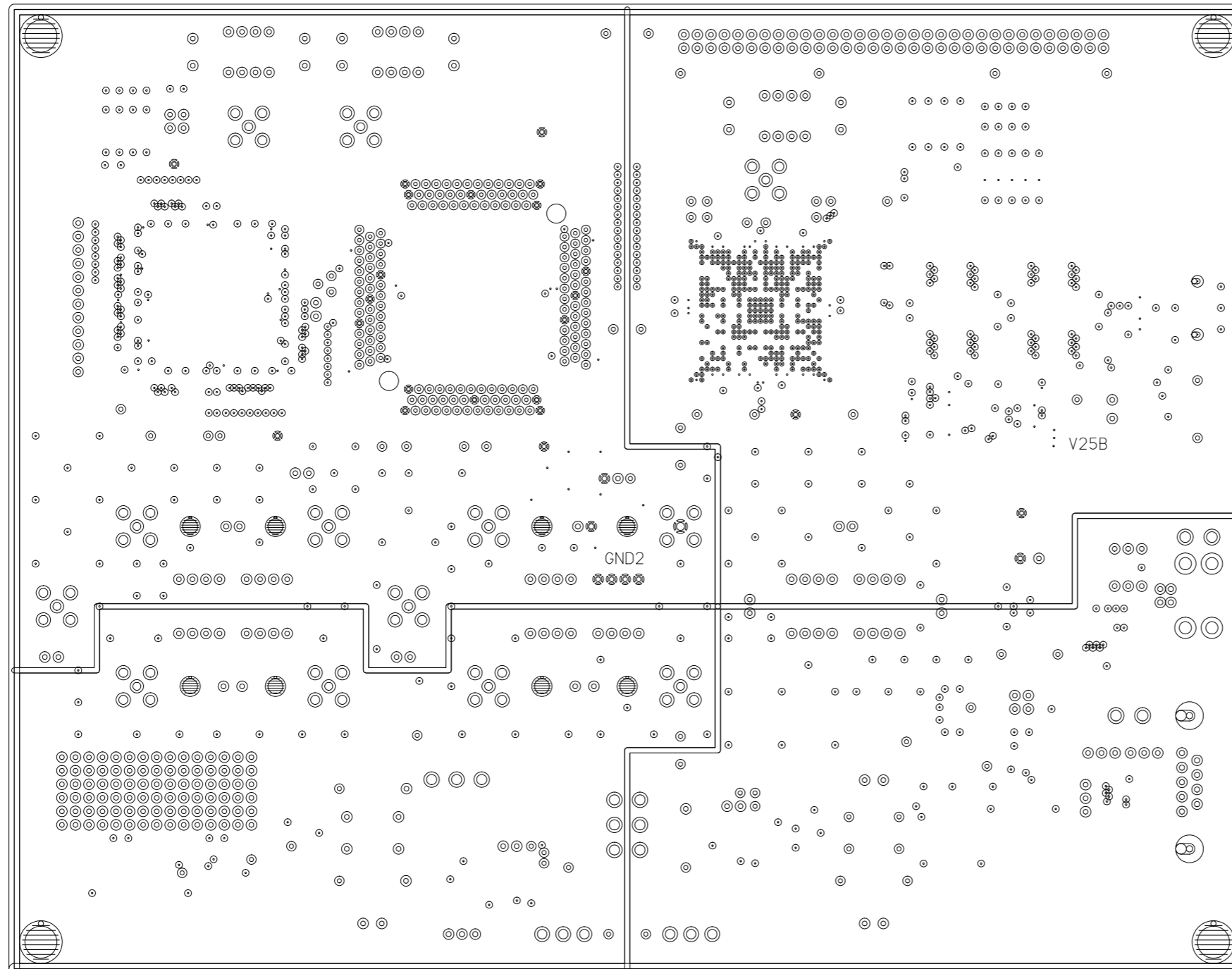
Evaluation Board LSI版
3-93995-1 2008/01/11



L8



L7 VIO



L6 GND2 V25B

Evaluation Board LSI版
3-93995-1 2008/01/11

*1 The copyright of this product belongs to the National Institute of Advanced Industrial Science and Technology (AIST), and the copyright of this manual belongs to the Ministry of Economy, Trade and Industry (METI).

*2 Copying this manual, in whole or in part, is prohibited without written permission from METI.

*3 Only personal use of this manual is granted. Any other use of this manual is not allowed without written permission from METI.

*4 The specifications of this product are subject to revision without notice.

Technical inquiries:

National Institute of Advanced Industrial Science and Technology (AIST)

Research Center for Information Security (RCIS)

Akihabara-Daibiru 11F Room 1102

1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan

TEL: +81-3-5298-4722

FAX: +81-3-5298-4522