Side-channel Attack Standard Evaluation Board

SASEBO-G

Specification

– Version 1.0 –

October 1, 2008

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

Index

1. Overview

The Side-channel Attack Standard Evaluation Board (SASEBO-G) is an FPGA board specifically designed to develop standard evaluation schemes to secure the cryptographic module against physical attacks. The SASEBO-G version board incorporates a Xilinx FPGA. Figure 1 is a photograph of the SASEBO-G. The basic features of the SASEBO-G are as follows:

- 230 mm x 180 mm x 1.6 mm, FR-4, eight layers.
- Two Xilinx Virtex-II Pro series FPGAs
  - Cryptographic FPGA: xc2vp7-fg456-5
  - Control FPGA: xc2vp30-fg676-5

  These FPGAs are connected through a 16-bit bidirectional data bus and a 16-bit address bus, controlled by four signals: RD, WT, RESET, and CLOCK.
- Two on-board oscillators provide each FPGA with clock signals at the same frequency of 24 MHz. External clock inputs are also supported.
- External power source supplies on-board power regulators and the FPGAs with 3.3 V. The power regulators convert the 3.3-V input into 2.5 V, 1.8 V, and 1.5 V for the FPGAs. The core voltage of 1.5 V of the cryptographic FPGA can also be applied directly through an external power connector.
- Shunt resistors are provided for power measurement of the FPGAs.
- The host PC controls and communicates with the board via RS-232 or USB port.

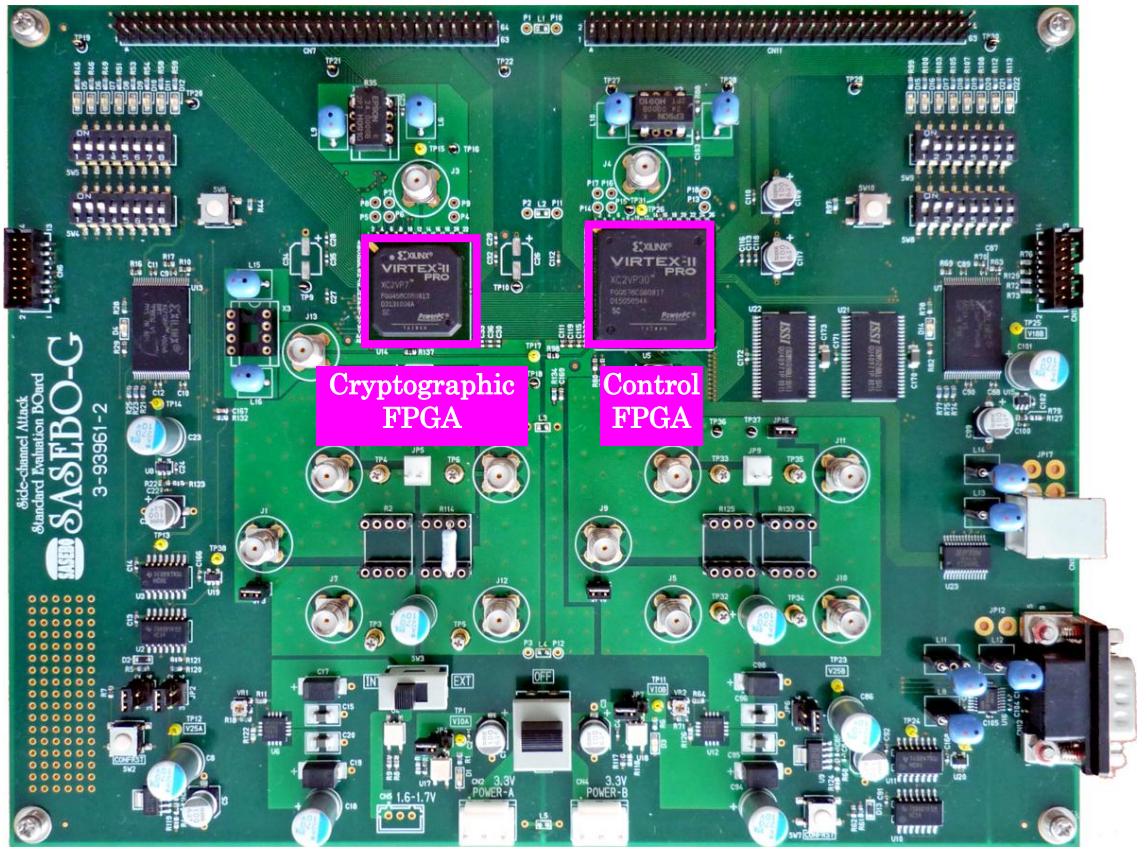


Figure 1: SASEBO-G

2. I/O Assignments

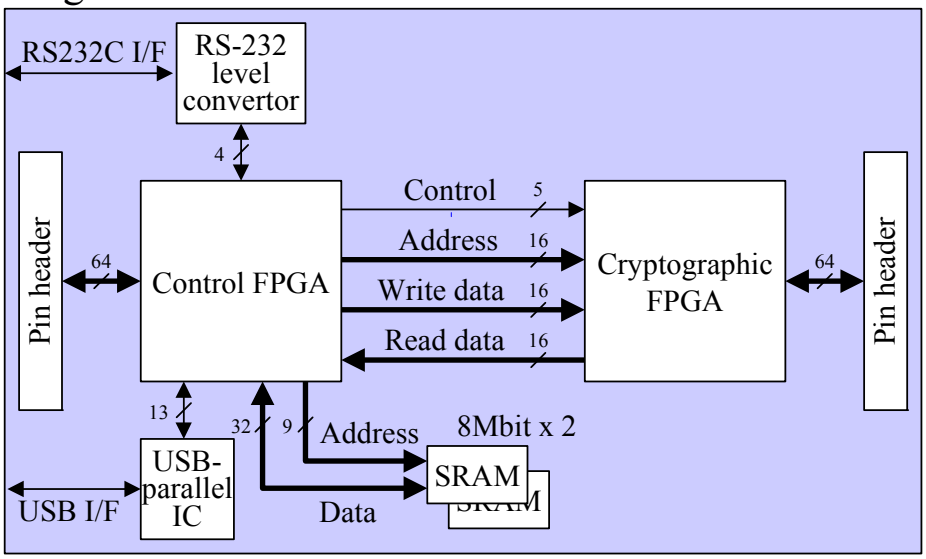


Figure 2: I/O signals

- Pin assignments of the cryptographic FPGA (U14)

Table 1: FPGA control

Signal Name	Pin Number	Input/Output	Description/Destination
CDA0	V17		Config
CDA1	V16		Config
CDA2	W16		Config
CDA3	Y16		Config
CDA4	Y7		Config
CDA5	W7		Config
CDA6	V7		Config
CDA7	V6		Config
BUSY	W18		Config
INIT_B	W17		Config
GCLK	W20		Config
PROG_B	B1		Config
DONE	Y18		Config
M0	Y4		SW4-1
M1	W3		SW4-2
M2	Y2		SW4-3
TCLK	B22		JTAG
TDI	D3		JTAG
TDO	D20		JTAG
TMS	A21		JTAG
PWRDWN_B	Y19		SW4-4
HSWAP_EN	A2		SW4-5
VBATT	C19		P4
DXP	C4		P5
DXN	C5		P6
OSCX	Y12	IN	Clock
RESETA	W8	IN	RESET
CLK	C12	IN	X1

Table 2: Cryptographic circuit interface

Signal Name	Pin Number	Input/Output	Description/Destination
FPGA_DI0	P21	IN	U2
FPGA_DI1	T18	IN	Y4
FPGA_DI2	U19	IN	Y3
FPGA_DI3	U21	IN	Y2
FPGA_DI4	U22	IN	Y1
FPGA_DI5	N21	IN	T2
FPGA_DI6	N22	IN	T1
FPGA_DI7	T21	IN	W2
FPGA_DI8	T22	IN	W1
FPGA_DI9	P20	IN	V6
FPGA_DI10	M21	IN	R2
FPGA_DI11	M19	IN	R1
FPGA_DI12	N19	IN	U3
FPGA_DI13	N20	IN	V4
FPGA_DI14	P19	IN	V3
FPGA_DI15	R21	IN	V2
FPGA_DO0	R20	OUT	V5
FPGA_DO1	AA22	OUT	AD1
FPGA_DO2	AB21	OUT	AD2
FPGA_DO3	M20	OUT	R4
FPGA_DO4	Y21	OUT	AC2
FPGA_DO5	Y22	OUT	AC1
FPGA_DO6	R22	OUT	V1
FPGA_DO7	T20	OUT	AA5
FPGA_DO8	W21	OUT	AB2
FPGA_DO9	W22	OUT	AB1
FPGA_DO10	T19	OUT	Y5
FPGA_DO11	P22	OUT	U1
FPGA_DO12	V19	OUT	AA4
FPGA_DO13	V20	OUT	AA3
FPGA_DO14	V21	OUT	AA2
FPGA_DO15	V22	OUT	AA1
FPGA_A0	V3	IN	P25
FPGA_A1	AA1	IN	AE26
FPGA_A2	Y2	IN	T26
FPGA_A3	Y1	IN	AD26
FPGA_A4	W2	IN	R26
FPGA_A5	W1	IN	AC26
FPGA_A6	N2	IN	W25
FPGA_A7	P2	IN	Y25
FPGA_A8	V2	IN	AD25
FPGA_A9	V1	IN	AB26
FPGA_A10	R1	IN	W26
FPGA_A11	M2	IN	V25
FPGA_A12	U2	IN	AC25
FPGA_A13	U1	IN	AA26
FPGA_A14	P1	IN	V26
FPGA_A15	N1	IN	U26
FPGA_WR	T2	IN	T25

FPGA_RD	T3	IN	AB25
FPGA_RSV0	T1		Y26
FPGA_RSV1	T4		R25
FPGA_RSV2	R3		U25
FPGA_RSV3	R2		AA25

Table 3: LEDs and switches

Signal Name	Pin Number	Input/Output	Description/Destination
LED0	E7	OUT	D5
LED1	C10	OUT	D6
LED2	D5	OUT	D7
LED3	F9	OUT	D8
LED4	D7	OUT	D9
LED5	B11	OUT	D10
LED6	C8	OUT	D11
LED7	C7	OUT	D12
DIPSW0	E10	IN	SW5-1
DIPSW1	D10	IN	SW5-2
DIPSW2	D11	IN	SW5-3
DIPSW3	C11	IN	SW5-4
DIPSW4	E9	IN	SW5-5
DIPSW5	F10	IN	SW5-6
DIPSW6	F11	IN	SW5-7
DIPSW7	E11	IN	SW5-8
PUSH	D9	IN	SW6

Table 4: Pin header

Signal Name	Pin Number	Input/Output	Description/Destination
IOA0	L2	IO	CN7-1
IOA1	K1	IO	CN7-2
IOA2	K2	IO	CN7-3
IOA3	J1	IO	CN7-4
IOA4	J2	IO	CN7-5
IOA5	H1	IO	CN7-6
IOA6	H2	IO	CN7-7
IOA7	G1	IO	CN7-8
IOA8	G2	IO	CN7-9
IOA9	F1	IO	CN7-10
IOA10	F2	IO	CN7-11
IOA11	E1	IO	CN7-12
IOA12	E2	IO	CN7-13
IOA13	D1	IO	CN7-14
IOA14	D2	IO	CN7-15
IOA15	C1	IO	CN7-16
IOA16	C2	IO	CN7-17
IOA17	L6	IO	CN7-18
IOA18	K6	IO	CN7-19
IOA19	L3	IO	CN7-20
IOA20	K5	IO	CN7-21
IOA21	K3	IO	CN7-22

IOA22	K4	IO	CN7-23
IOA23	J3	IO	CN7-24
IOA24	H5	IO	CN7-25
IOA25	H3	IO	CN7-26
IOA26	H4	IO	CN7-27
IOA27	G3	IO	CN7-28
IOA28	G4	IO	CN7-29
IOA29	G5	IO	CN7-30
IOA30	E3	IO	CN7-31
IOA31	E4	IO	CN7-32
IOA32	C21	IO	CN7-33
IOA33	C22	IO	CN7-34
IOA34	D21	IO	CN7-35
IOA35	D22	IO	CN7-36
IOA36	E21	IO	CN7-37
IOA37	E22	IO	CN7-38
IOA38	F21	IO	CN7-39
IOA39	F22	IO	CN7-40
IOA40	G21	IO	CN7-41
IOA41	G22	IO	CN7-42
IOA42	H21	IO	CN7-43
IOA43	H22	IO	CN7-44
IOA44	J21	IO	CN7-45
IOA45	J22	IO	CN7-46
IOA46	K21	IO	CN7-47
IOA47	K22	IO	CN7-48
IOA48	L21	IO	CN7-49
IOA49	E19	IO	CN7-50
IOA50	E20	IO	CN7-51
IOA51	G18	IO	CN7-52
IOA52	G19	IO	CN7-53
IOA53	G20	IO	CN7-54
IOA54	H19	IO	CN7-55
IOA55	H20	IO	CN7-56
IOA56	H18	IO	CN7-57
IOA57	J20	IO	CN7-58
IOA58	K19	IO	CN7-59
IOA59	K20	IO	CN7-60
IOA60	K18	IO	CN7-61
IOA61	L20	IO	CN7-62
IOA62	K17	IO	CN7-63
IOA63	L17	IO	CN7-64

- Pin assignment of the control FPGA (U5)

Table 5: FPGA control

Signal Name	Pin Number	Input/Output	Description/Destination
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		SW8-1
M1	AF3		SW8-2
M2	AD4		SW8-3
TCLK	B26		JTAG
TDI	D3		JTAG
TDO	D24		JTAG
TMS	B24		JTAG
PWRDWN_B	AF24		SW8-4
HSWAP_EN	B3		SW8-5
VBATT	A24		P13
DXP	A3		P14
DXN	C4		P15
RESETB	Y9	IN	RESET
CLK	B13	IN	X2
OSCX	AE1	OUT	Clock

Table 6: RS-232

Signal Name	Pin Number	Input/Output	Description/Destination
TX	M25	OUT	Level converter
RX	M26	IN	Level converter
CTS	N25	OUT	Level converter
RTS	L26	IN	Level converter

Table 7: LEDs and switches

Signal Name	Pin Number	Input/Output	Description/Destination
LED0	C17	OUT	D15
LED1	B19	OUT	D16
LED2	D17	OUT	D17
LED3	A19	OUT	D18
LED4	C20	OUT	D19
LED5	D18	OUT	D20
LED6	E17	OUT	D21
LED7	C18	OUT	D22
DIPSW0	E21	IN	SW9-1
DIPSW1	D20	IN	SW9-2
DIPSW2	E19	IN	SW9-3
DIPSW3	D15	IN	SW9-4
DIPSW4	C15	IN	SW9-5
DIPSW5	B14	IN	SW9-6
DIPSW6	E15	IN	SW9-7
DIPSW7	E16	IN	SW9-8
PUSH	E22	IN	SW10

Table 8: General monitor pins

Signal Name	Pin Number	Input/Output	Description/Destination
IOB0	N3	IO	CN11-1
IOB1	M4	IO	CN11-2
IOB2	L3	IO	CN11-3
IOB3	K3	IO	CN11-4
IOB4	K4	IO	CN11-5
IOB5	G3	IO	CN11-6
IOB6	G4	IO	CN11-7
IOB7	F3	IO	CN11-8
IOB8	F4	IO	CN11-9
IOB9	E4	IO	CN11-10
IOB10	N2	IO	CN11-11
IOB11	M1	IO	CN11-12
IOB12	M2	IO	CN11-13
IOB13	L1	IO	CN11-14
IOB14	L2	IO	CN11-15
IOB15	K1	IO	CN11-16
IOB16	K2	IO	CN11-17
IOB17	J1	IO	CN11-18
IOB18	J2	IO	CN11-19
IOB19	H1	IO	CN11-20
IOB20	H2	IO	CN11-21
IOB21	G1	IO	CN11-22
IOB22	G2	IO	CN11-23
IOB23	F1	IO	CN11-24
IOB24	F2	IO	CN11-25
IOB25	E1	IO	CN11-26
IOB26	E2	IO	CN11-27
IOB27	D1	IO	CN11-28
IOB28	D2	IO	CN11-29
IOB29	C1	IO	CN11-30
IOB30	C2	IO	CN11-31
IOB31	E23	IO	CN11-32
IOB32	F23	IO	CN11-33
IOB33	F24	IO	CN11-34
IOB34	G23	IO	CN11-35
IOB35	G24	IO	CN11-36
IOB36	H22	IO	CN11-37
IOB37	J21	IO	CN11-38
IOB38	J22	IO	CN11-39
IOB39	K23	IO	CN11-40
IOB40	J24	IO	CN11-41
IOB41	L22	IO	CN11-42
IOB42	K24	IO	CN11-43
IOB43	M23	IO	CN11-44
IOB44	M22	IO	CN11-45
IOB45	N24	IO	CN11-46
IOB46	N23	IO	CN11-47
IOB47	C25	IO	CN11-48
IOB48	C26	IO	CN11-49

IOB49	D25	IO	CN11-50
IOB50	D26	IO	CN11-51
IOB51	E25	IO	CN11-52
IOB52	E26	IO	CN11-53
IOB53	F25	IO	CN11-54
IOB54	F26	IO	CN11-55
IOB55	G25	IO	CN11-56
IOB56	G26	IO	CN11-57
IOB57	H25	IO	CN11-58
IOB58	H26	IO	CN11-59
IOB59	J25	IO	CN11-60
IOB60	J26	IO	CN11-61
IOB61	K25	IO	CN11-62
IOB62	K26	IO	CN11-63
IOB63	L25	IO	CN11-64

Table 9: Cryptographic circuit interface

Signal Name	Pin Number	Input/Output	Description/Destination
FPGA_DI0	U2	OUT	P21
FPGA_DI1	Y4	OUT	T18
FPGA_DI2	Y3	OUT	U19
FPGA_DI3	Y2	OUT	U21
FPGA_DI4	Y1	OUT	U22
FPGA_DI5	T2	OUT	N21
FPGA_DI6	T1	OUT	N22
FPGA_DI7	W2	OUT	T21
FPGA_DI8	W1	OUT	T22
FPGA_DI9	V6	OUT	P20
FPGA_DI10	R2	OUT	M21
FPGA_DI11	R1	OUT	M19
FPGA_DI12	U3	OUT	N19
FPGA_DI13	V4	OUT	N20
FPGA_DI14	V3	OUT	P19
FPGA_DI15	V2	OUT	R21
FPGA_DO0	V5	IN	R20
FPGA_DO1	AD1	IN	AA22
FPGA_DO2	AD2	IN	AB21
FPGA_DO3	R4	IN	M20
FPGA_DO4	AC2	IN	Y21
FPGA_DO5	AC1	IN	Y22
FPGA_DO6	V1	IN	R22
FPGA_DO7	AA5	IN	T20
FPGA_DO8	AB2	IN	W21
FPGA_DO9	AB1	IN	W22
FPGA_DO10	Y5	IN	T19
FPGA_DO11	U1	IN	P22
FPGA_DO12	AA4	IN	V19
FPGA_DO13	AA3	IN	V20
FPGA_DO14	AA2	IN	V21
FPGA_DO15	AA1	IN	V22
FPGA_A0	P25	OUT	V3
FPGA_A1	AE26	OUT	AA1

FPGA_A2	T26	OUT	Y2
FPGA_A3	AD26	OUT	Y1
FPGA_A4	R26	OUT	W2
FPGA_A5	AC26	OUT	W1
FPGA_A6	W25	OUT	N2
FPGA_A7	Y25	OUT	P2
FPGA_A8	AD25	OUT	V2
FPGA_A9	AB26	OUT	V1
FPGA_A10	W26	OUT	R1
FPGA_A11	V25	OUT	M2
FPGA_A12	AC25	OUT	U2
FPGA_A13	AA26	OUT	U1
FPGA_A14	V26	OUT	P1
FPGA_A15	U26	OUT	N1
FPGA_WR	T25	OUT	T2
FPGA_RD	AB25	OUT	T3
FPGA_RSV0	Y26		T1
FPGA_RSV1	R25		T4
FPGA_RSV2	U25		R3
FPGA_RSV3	AA25		R2

Table 10: USB

Signal Name	Pin Number	Input/Output	Description/Destination
USBD0	AE8	IO	USB-Parallel IC
USBD1	AD12	IO	USB-Parallel IC
USBD2	AD9	IO	USB-Parallel IC
USBD3	AF19	IO	USB-Parallel IC
USBD4	AF8	IO	USB-Parallel IC
USBD5	AD15	IO	USB-Parallel IC
USBD6	AD17	IO	USB-Parallel IC
USBD7	AE14	IO	USB-Parallel IC
USBTXE	AB8	IN	USB-Parallel IC
USBRXF	AC7	IN	USB-Parallel IC
USBRD	AD20	OUT	USB-Parallel IC
USBWR	AD7	OUT	USB-Parallel IC
USBWREN	AE19	IN	USB-Parallel IC

Table 11: SRAM

Signal Name	Pin Number	Input/Output	Description/Destination
MEMD0	AB17	IO	Memory
MEMD1	AB16	IO	Memory
MEMD2	Y15	IO	Memory
MEMD3	AB15	IO	Memory
MEMD4	AA15	IO	Memory
MEMD5	AD14	IO	Memory
MEMD6	AC14	IO	Memory
MEMD7	AE13	IO	Memory
MEMD8	AC10	IO	Memory
MEMD9	AD10	IO	Memory
MEMD10	AA9	IO	Memory
MEMD11	AB9	IO	Memory
MEMD12	AB11	IO	Memory
MEMD13	AC12	IO	Memory

MEMD14	AB12	IO	Memory
MEMD15	AB13	IO	Memory
MEMD16	AA19	IO	Memory
MEMD17	AB20	IO	Memory
MEMD18	AB19	IO	Memory
MEMD19	AC20	IO	Memory
MEMD20	AC18	IO	Memory
MEMD21	AD18	IO	Memory
MEMD22	AB18	IO	Memory
MEMD23	AC17	IO	Memory
MEMD24	AA8	IO	Memory
MEMD25	Y11	IO	Memory
MEMD26	Y18	IO	Memory
MEMD27	Y19	IO	Memory
MEMD28	R22	IO	Memory
MEMD29	R23	IO	Memory
MEMD30	P24	IO	Memory
MEMD31	P23	IO	Memory
MEMA0	W13	OUT	Memory
MEMA1	V13	OUT	Memory
MEMA2	W12	OUT	Memory
MEMA3	W10	OUT	Memory
MEMA4	W8	OUT	Memory
MEMA5	Y8	OUT	Memory
MEMA6	W9	OUT	Memory
MEMA7	W11	OUT	Memory
MEMA8	W17	OUT	Memory
MEMA9	W19	OUT	Memory
MEMA10	AA18	OUT	Memory
MEMA11	AB14	OUT	Memory
MEMA12	AB10	OUT	Memory
MEMA13	AA12	OUT	Memory
MEMA14	AA13	OUT	Memory
MEMA15	Y12	OUT	Memory
MEMA16	W18	OUT	Memory
MEMA17	AA11	OUT	Memory
MEMA18	W15	OUT	Memory
MEMCS	W14	OUT	Memory
MEMWR	W16	OUT	Memory
MEMUB	AD13	OUT	Memory
MEMLB	AC13	OUT	Memory
MEMOE	V12	OUT	Memory
MEMUB1	P21	OUT	Memory
MEMLB1	P22	OUT	Memory

3. Operational Instructions

➢ Power Supply

Figure 3 shows the composition of the power supply block on the SASEBO-G. Table 12 shows the functions of the power supply connectors. Figure 4 shows the power sequence of the SASEBO-G.

An external power source supplies the SASEBO-G with a DC voltage of 3.3 V through both CN2 (Cryptographic FPGA side) and CN4 (Control FPGA side). When the external power source is activated, the main power switch (SW1) must be off. Toggle SW2 to "EXT" to optionally supply the cryptographic FPGA core voltage of 1.2 V through CN3. The power must be off when SW2 is turned. LEDs D1 and D2 turn on to indicate that the DC 3.3 V is supplied through CN1 and CN2, respectively.

Table 12: Power supply settings

Connector		CN2	CN4	CN5
Description		Cryptographic FPGA power regulator	Control FPGA power regulator	Cryptographic FPGA core voltage
SW2		INT	INT	EXT
Pin	1	3.3V	3.3V	1.5V
	2	GND	GND	GND
	3	NC	NC	NC

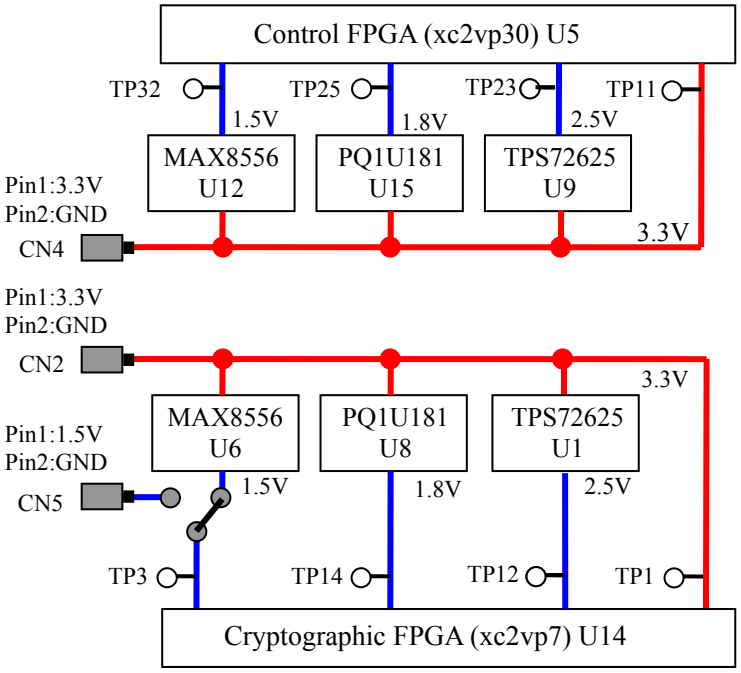


Figure 3: Power supply block on the SASEBO-G

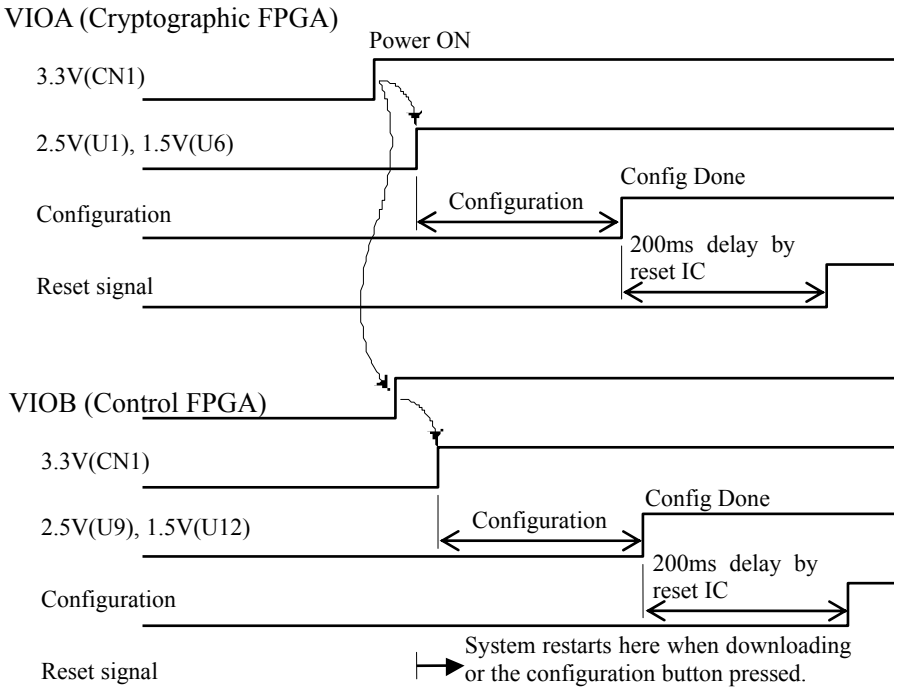


Figure 4: Power sequence of the SASEBO-G

- Jumper Settings

Table 13: Jumper settings

Function	Pin	Setting	Description
Power sequence options	JP4	Short	Disable the power sequence of the cryptographic FPGA
		Open	Enable the power sequence of the cryptographic FPGA
	JP7	Short	Disable the power sequence of the control FPGA
		Open	Enable the power sequence of the control FPGA
	JP1	Short	Cryptographic FPGA configuration begins after 2.5 V stabilizes
		Open	Cryptographic FPGA configuration begins after 1.5 V stabilizes
	JP2	Short	VIOB supply begins after 2.5 V stabilizes
		Open	VIOB supply begins after 1.5 V stabilizes
	JP6	Short	Control FPGA configuration begins after 2.5 V stabilizes
		Open	Control FPGA configuration begins after 1.5 V stabilizes
Power consumption measurement options	JP3	Short	Bypass R2 shunt resistor on the cryptographic FPGA core VCC line
		Open	Enable R2 shunt resistor on the cryptographic FPGA core VCC line
	JP8	Short	Bypass R114 shunt resistor on the cryptographic FPGA core GND line
		Open	Enable R114 shunt resistor on the cryptographic FPGA core GND line
	JP10	Short	Bypass R125 shunt resistor on the control FPGA core VCC line
		Open	Enable R125 shunt resistor on the control FPGA core VCC line
	JP16	Short	Bypass R133 shunt resistor on the control FPGA core GND line
		Open	Enable R133 shunt resistor on the control FPGA core GND line

➢ FPGA Configuration

Figure 5 depicts a block diagram of the FPGA's JTAG chain. The cryptographic FPGA (U14) and control FPGA (U5) each have a JTAG chain. In the respective chains, while JTAG connector CN6 and flash ROM U13 are connected with FPGA U14, JTAG connector CN10 and flash ROM U7 are linked with FPGA U5. Table 14 shows the pin assignment of CN6 and CN10. Configuration mode settings with the DIP switches (SW4 for the cryptographic FPGA and SW8 for the control FPGA) are listed in Table 15. For the FPGAs, LEDs D4 and D14 light up to indicate that the cryptographic and control FPGAs have been successfully configured respectively. Push down SW6 or SW10 to reconfigure the cryptographic or control FPGA with the PROM.

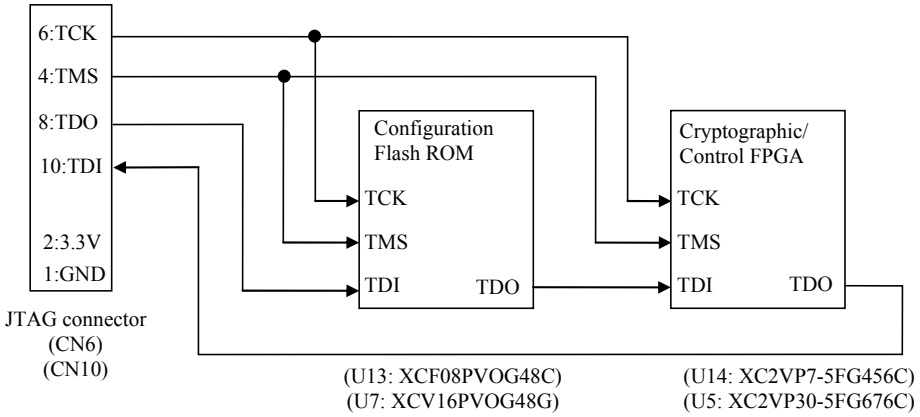


Figure 5: JTAG chain for FPGA configuration

Table 14: Pin assignment of the JTAG connector (CN6/CN10)

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 15: Configuration mode settings (SW4/SW8)

Dip1	M0	ON
Dip2	M1	ON
Dip3	M2	ON
Dip4	PWRDWN	OFF
Dip5	HSWAP_EN	OFF
Dip6	NC	OFF
Dip7	NC	OFF
Dip8	NC	OFF

➢ Clock Source

The clock source connection of the SASEBO-G is shown in Figure 6. A 24-MHz oscillator and an SMA connector (J3/J5) are connected to each FPGA individually.

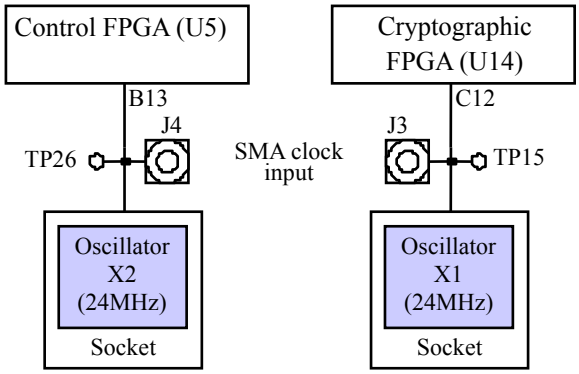


Figure 6: Clock source connection

➢ Host Interface

RS-232 and USB are provided on the SASEBO-G for communication with the host PC. Table 16 and 17 show the signal assignments of the RS-232 and USB interfaces. A 9-pin female-female straight cable connects the SASEBO-G to the PC through the RS-232 interface. The driver software and API of the USB interface are provided by FTDI. (Future Technology Device International Ltd. http://www.ftdichip.com/Products/FT245R.htm)

Table 16: Signal assignment on the RS-232 interface

Signal	CN12 (XM2C-0912-111)	U16 (ADM3202ARU)		U5 (xc2vp30)
TX	2pin	14pin	11pin	M25
RX	3pin	13pin	12pin	M26
CTS	8pin	7pin	10pin	N25
RTS	7pin	8pin	9pin	L26

Table 17: Signal assignment on the USB interface

Signal	CN13 (XM7B-0442)	U23 (FT245RL)	U5 (xc2vp30)
USBDP	2pin	15pin	-
USBDM	3pin	16pin	-
USBD0	-	1pin	AE8
USBD1	-	5pin	AD12
USBD2	-	3pin	AD9
USBD3	-	11pin	AF19
USBD4	-	2pin	AF8
USBD5	-	9pin	AD15
USBD6	-	10pin	AD17
USBD7	-	6pin	AE14
USBTXE	-	22pin	AB8
USBRXF	-	23pin	AC7
USBRD	-	13pin	AD20
USBWR	-	14pin	AD7
USBPWREN	-	12pin	AE19

4. Board Schematic and Layout

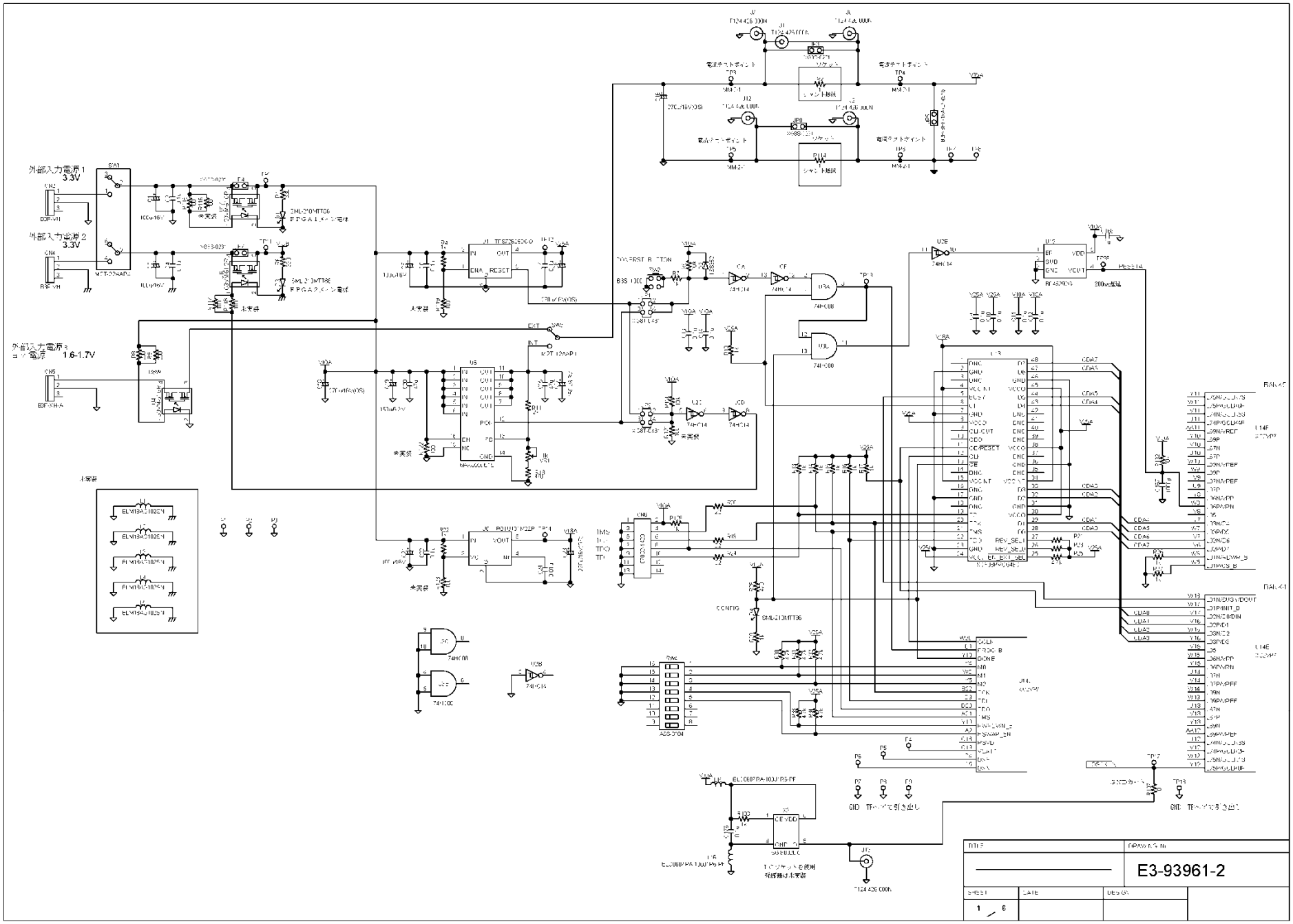
The parts list for the SASEBO-G is shown in Table 18. The board schematics and layouts of the SASEBO-G are presented on pages 16 to 36.

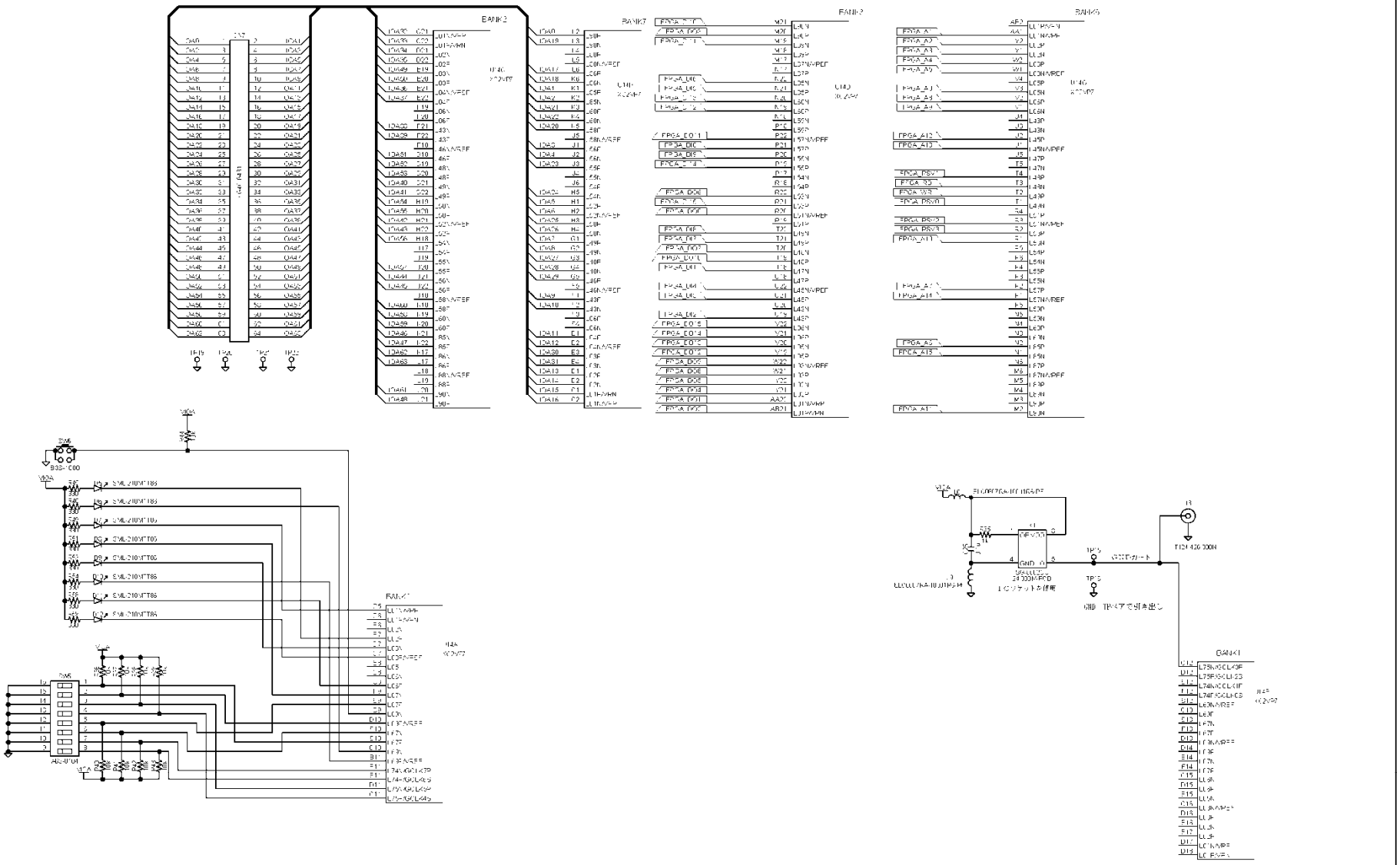
Table 17: Parts List

Board name	SASEBO-G
Model number	E3-93961-2

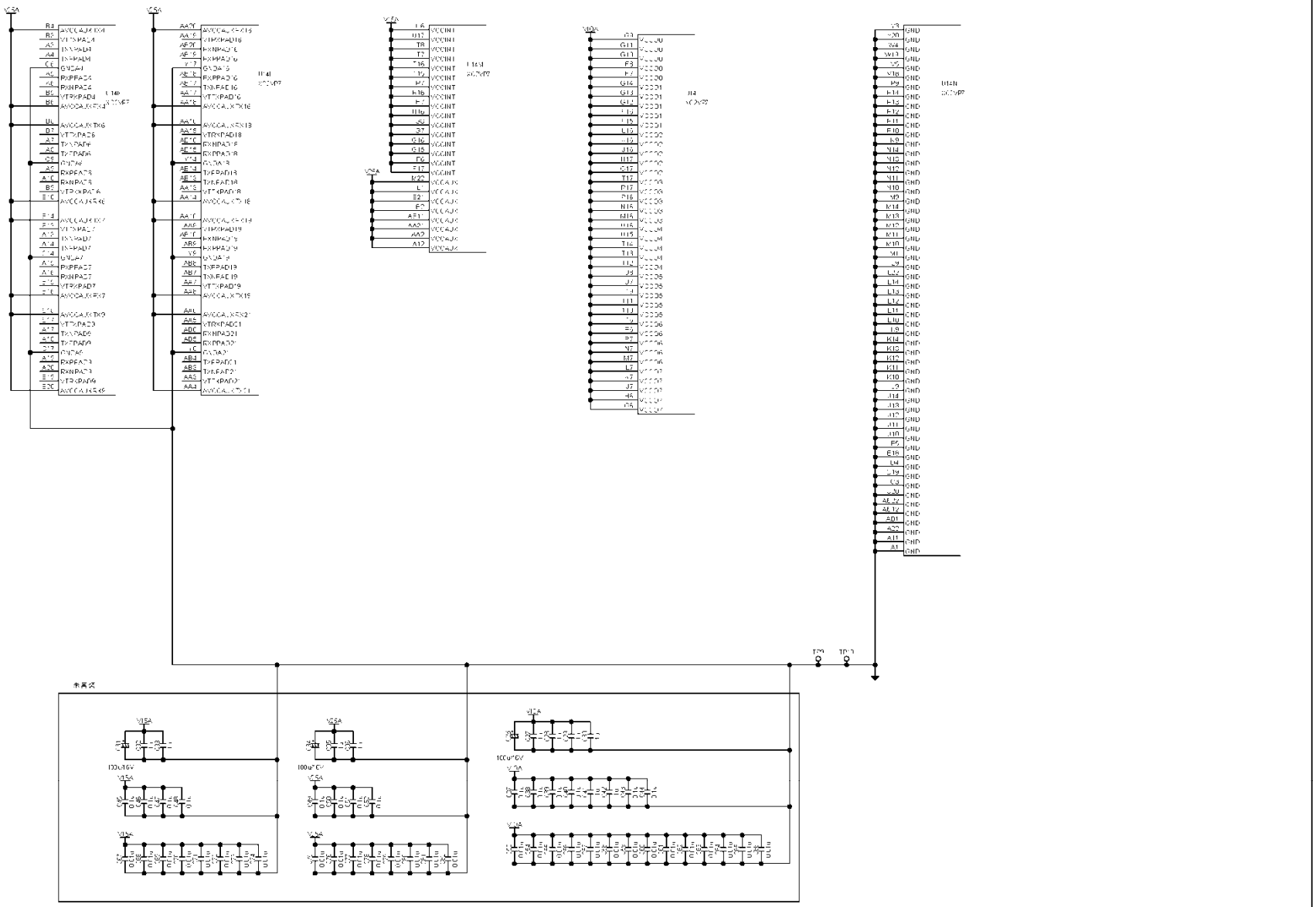
Description	Part Number	Maker	Qty	Reference Designator
Ceramic Capacitor	GRM155B11E103KA01D	MURATA	32	C24,C53,C54,C55,C56,C57,C58, C59,C60,C61,C62,C63,C64,C65, C66,C67,C68,C69,C70,C71,C72, C73,C74,C75,C76,C77,C78,C79, C80,C81,C82,C102,C136,C137, C138,C139,C140,C141,C142 ,C143, C144,C145, C146,C147,C148,C149, C150,C151,C152, C153,C154,C155, C156,C157,C158,C159,C160,C161, C162,C163,C164,C165
Ceramic Capacitor	GRM155F11E104ZA01D	MURATA	46	C2,C4,C6,C7,C9,C10,C11,C12,C13, C14,C22,C25,C37,C38,C39,C40, C43,C44,C45,C46,C47,C48,C49, C50,C51,C52,C84,C85,C87,C88, C89,C90,C91,C92,C100,C103,C104, C105,C106,C107,C108,C120,C121, C122,C123,C126,C127,C128,C129, C130,C131,C132,C133,C134,C135, C171,C172,C174,C175,C176
Ceramic Capacitor	GRM188F11H102KA01D	MURATA	2	C167, C169
Ceramic Capacitor	GRM155F10J105ZE01D	MURATA	12	C27, C28, C29, C30, C32, C33, C35, C36, C41, C42, C110, C111, C112, C113, C115, C116, C118, C119, C124, C125, C166, C168
Ceramic Capacitor	GRM31CB30J476ME18L	MURATA	6	C15, C20, C95, C96, C170, C173
Electrolytic Capacitor	EMVK6R3ADA101MF55G	Nippon Chemi-Con	9	C1, C3, C5, C21, C26, C31, C34, C83, C99, C109, C114, C117
Capacitor	EEFUE0J151R	Panasonic	4	C17, C19, C94, C98
Capacitor	APSA100ELL271MHB5S	Nippon Chemi-Con	8	C8, C16, C18, C23, C86, C93, C97, C101
Diode	1SS352(-TPH3)	TOSHIBA	2	D2, D13
Filter	BLM18AG102SN1D	MURATA	5	L1, L2, L3 L4 L5
Inductor	ELC0607RA-100J1R6-PF	TDK	11	L6, L7, L8, L9, L10, L11, L12, L13, L14, L15, L16
Reset IC	BD45292G	ROHM	2	U19, U20
Regulator IC	PQ1U181M2ZPH	SHARP	2	U8, U15
Regulator IC	TPS72625DCQ	TI	2	U1, U9
Regulator IC	MAX8556ETE+	MAXIM	2	U6, U12
FPGA	XC2VP30-5FG676C	Xilinx	1	U5
FPGA	XC2VP7-5FG456C	Xilinx	1	U14
ROM	XCF08PVOG48C	Xilinx	1	U13
ROM	XCF16PVOG48C	Xilinx	1	U7
CMOS	SN74HC08NS	TI	2	U3, U11
CMOS	SN74HC14NSE4	TI	2	U2, U10
SRAM	IS62WV51216BLL-55TLI	ISSI	2	U21, U22
USB IC	FT245RL	FDI	1	U23
RS0232 Level Converter	ADM3202ARUZ	Analog Devices	1	U16

LED	SML-210MTT86	ROHM	20	D1, D3, D4, D5, D6, D7, D8, D9, D10, D11, D12, D14, D15, D16, D17, D18, D19, D20, D21, D22
MOS Relay	G3VM-61GR1	OMRON	3	U4, U17, U18
SG-8002DC	24.000M-PCB	EPSON	2	X1, X2, X3(Socket)
Shunt	XG8T-0431	OMRON	3	JP1, JP2, JP6
Shunt	XG8S-0231	OMRON	6	JP3, JP4, JP7, JP8, JP10, JP16
Connector	B2P-SHF-1AA(LF)(SN)	JST	2	JP5, JP9
Connector	87832-1420	Molex	2	CN6, CN10
Resistor	RK73Z1JTD 0Ω	KOA	2	R98, R137
Resistor	RR0816P-103-D	SSM	22	R5, R36, R37, R38, R39, R40, R41, R42, R43, R61, R89, R90, R91, R92, R93, R94, R95, R96, R120, R132, R134, R135
Resistor	MCR03EZPFX1001	ROHM	29	R4, R7, R10, R13, R14, R15, R16, R17, R22, R26, R27, R29, R35, R60, R62, R63, R66, R67, R68, R69, R70, R79, R80, R81, R82, R88, R128, R129, R138
Resistor	RR0816P-201-D	SSM	2	R8, R9
Resistor	RR0816Q-220-D	SSM	6	R19, R20, R24, R72, R73, R76
Resistor	RR0816P-331-D	SSM	18	R1,R6,R45,R46,R49,R51,R53,R54, R58,R59,R99,R100,R103,R105, R107,R108,R112,R113
Resistor	RR0816P-472-D	SSM	19	R21,R23,R25,R30,R31,R32,R33, R34,R44,R74,R75,R77,R83,R84, R85,R86,R87,R97,R136
Resistor	RR0816P-471-D	SSM	4	R18, R28, R71, R78
Resistor	RR0816P-202-D	SSM	2	R11, R64
Resistor	RR0816P-101-D	SSM	11	R115,R116,R117,R118,R119, R121,R122,R123,R124,R126,R127
Trimmer	ST-32ETA 1KΩ	COPAL	2	VR1, VR2
SMA Connector	T124 426 000N	TAKITEK	13	J1, J2, J3, J4, J5, J6, J7, J8, J9, J10, J11, J12, J13
USB Connector	XM7B-0442	OMRON	1	CN13
D-sub Connector	XM2C-0912-111	OMRON	1	CN12
Connector	A1-64PA-2.54DSA(71)	HIROSE	2	CN7, CN11
Connector	B3P-VH(LF)(SN)	JST	2	CN2, CN4
Connector	B3B-XH-A(LF)(SN)	JST	1	CN5
Resistor	ERX1SJ1R0	Panasonic	4	R2, R114, R125, R133
DIP Switch	A6S-8104-H	OMRON	4	SW4, SW5, SW8, SW9
Push Button	B3S-1000	OMRON	4	SW2, SW6, SW7, SW10
Switch, Slide	CS-12AAP1	Nikkai	1	SW3
Switch, Slide	CS-22AAP1	Nikkai	1	SW1
Resistor	ERX1SJ	Panasonic	24	Supplement

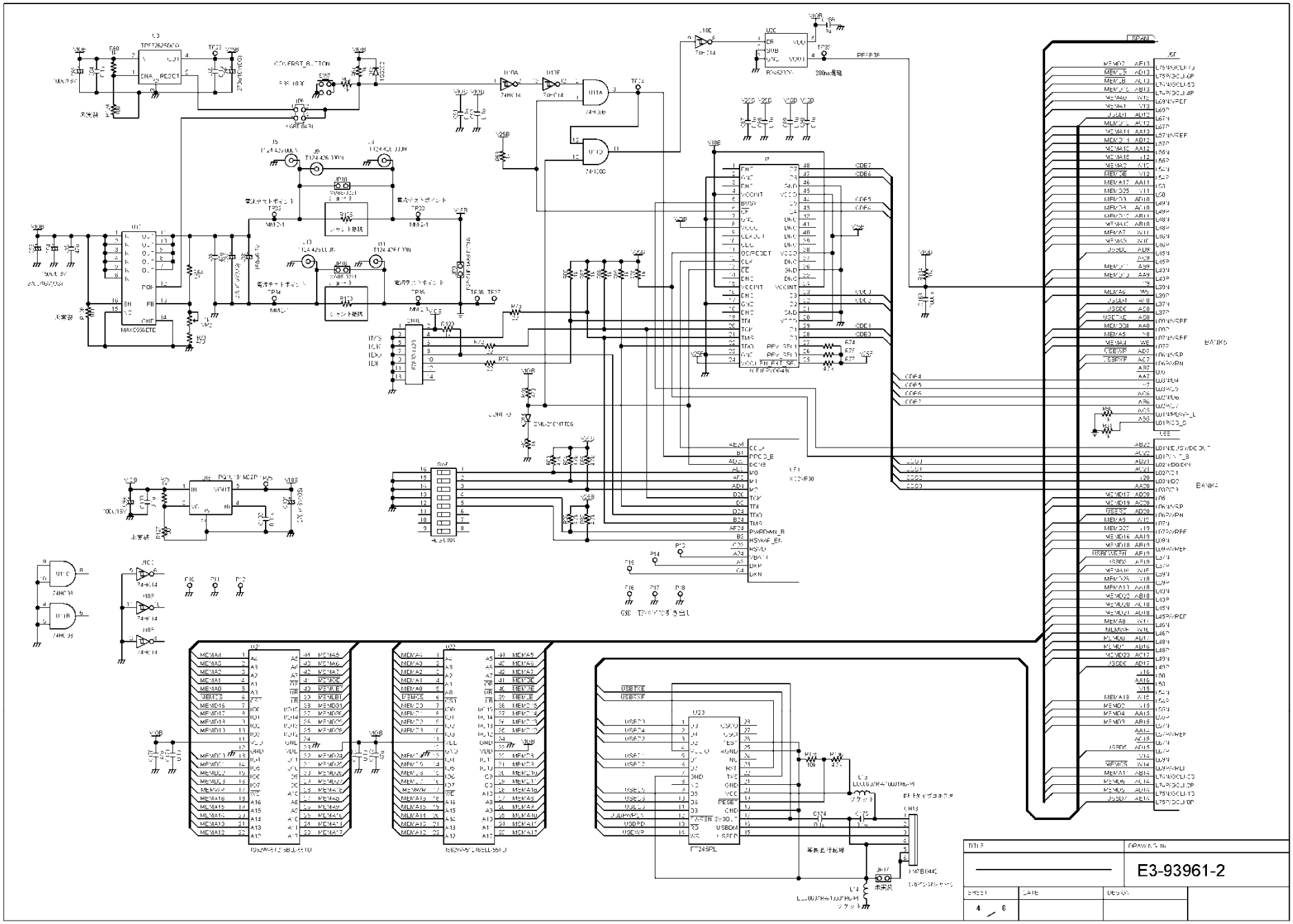

外部入力電源1
3.3V
外部入力電源2
3.3V
外部入力電源3
1.6-1.7V
E3-93961-2

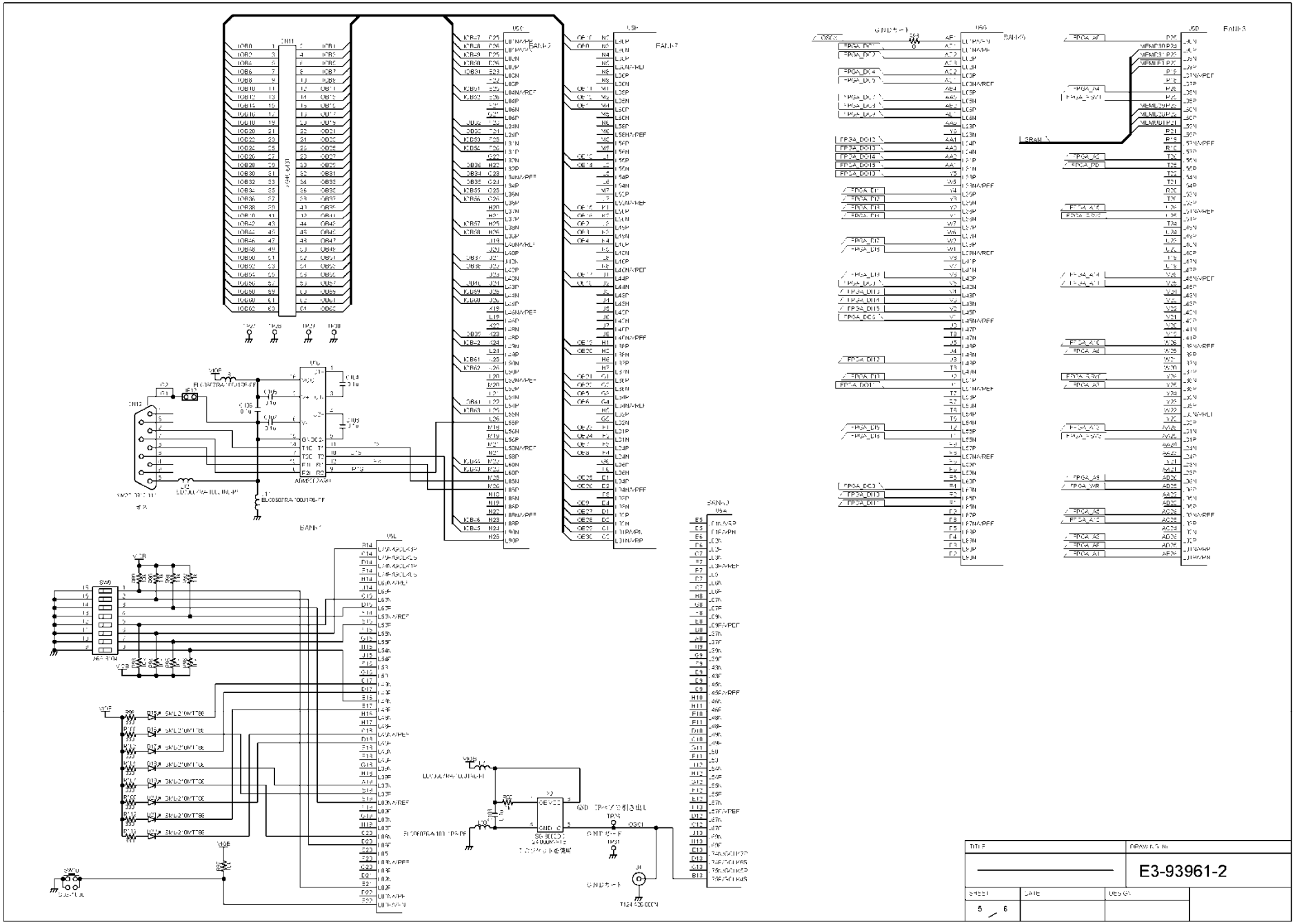


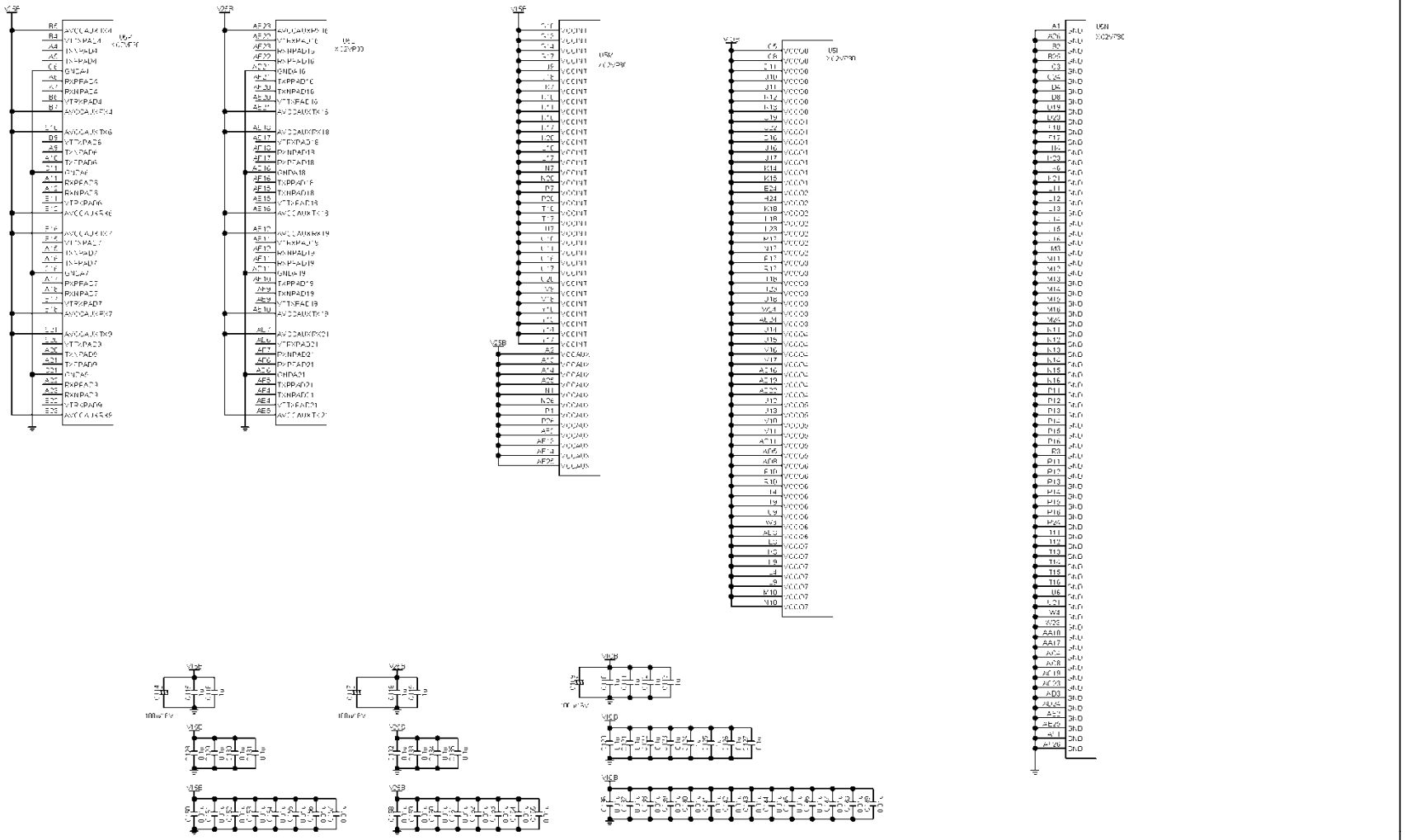
TITLE	DRAWING No.
	E3-93961-2
SHEET 2 / 6	DATE



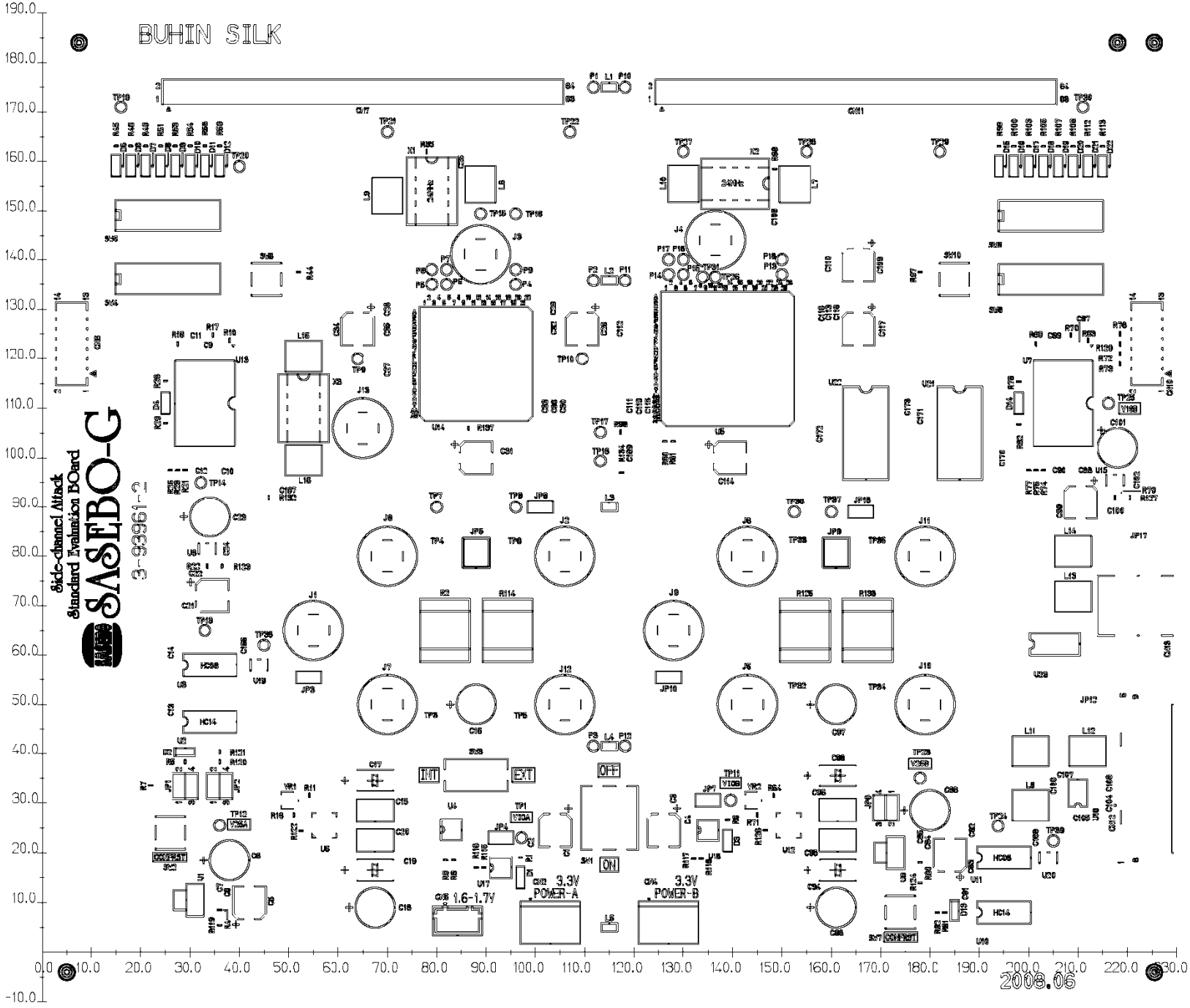
TITLE		DRAWING No.
		E3-93961-2
SHEET	DATE	DESIGN
3 / 6		

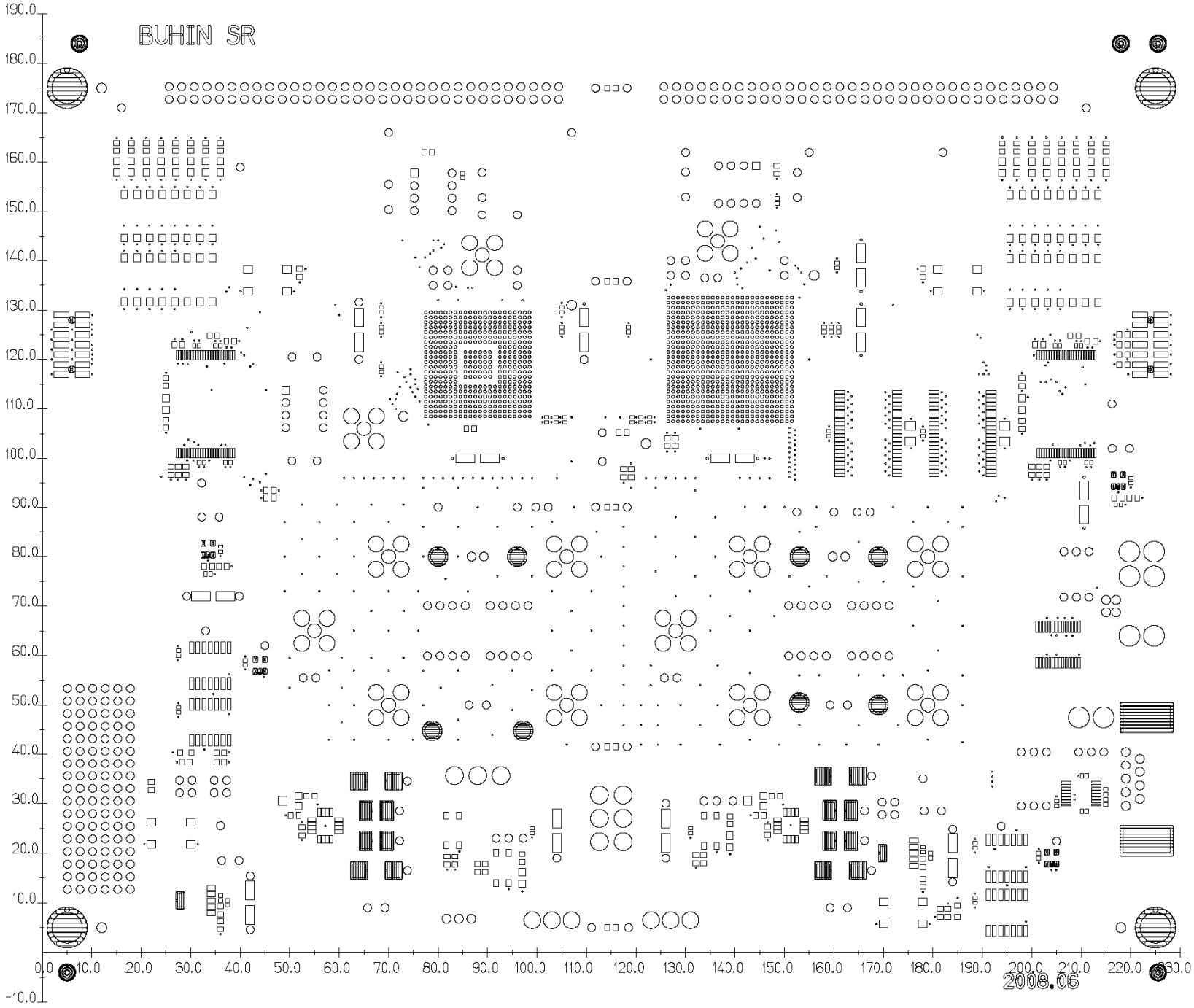

E3-93961-2

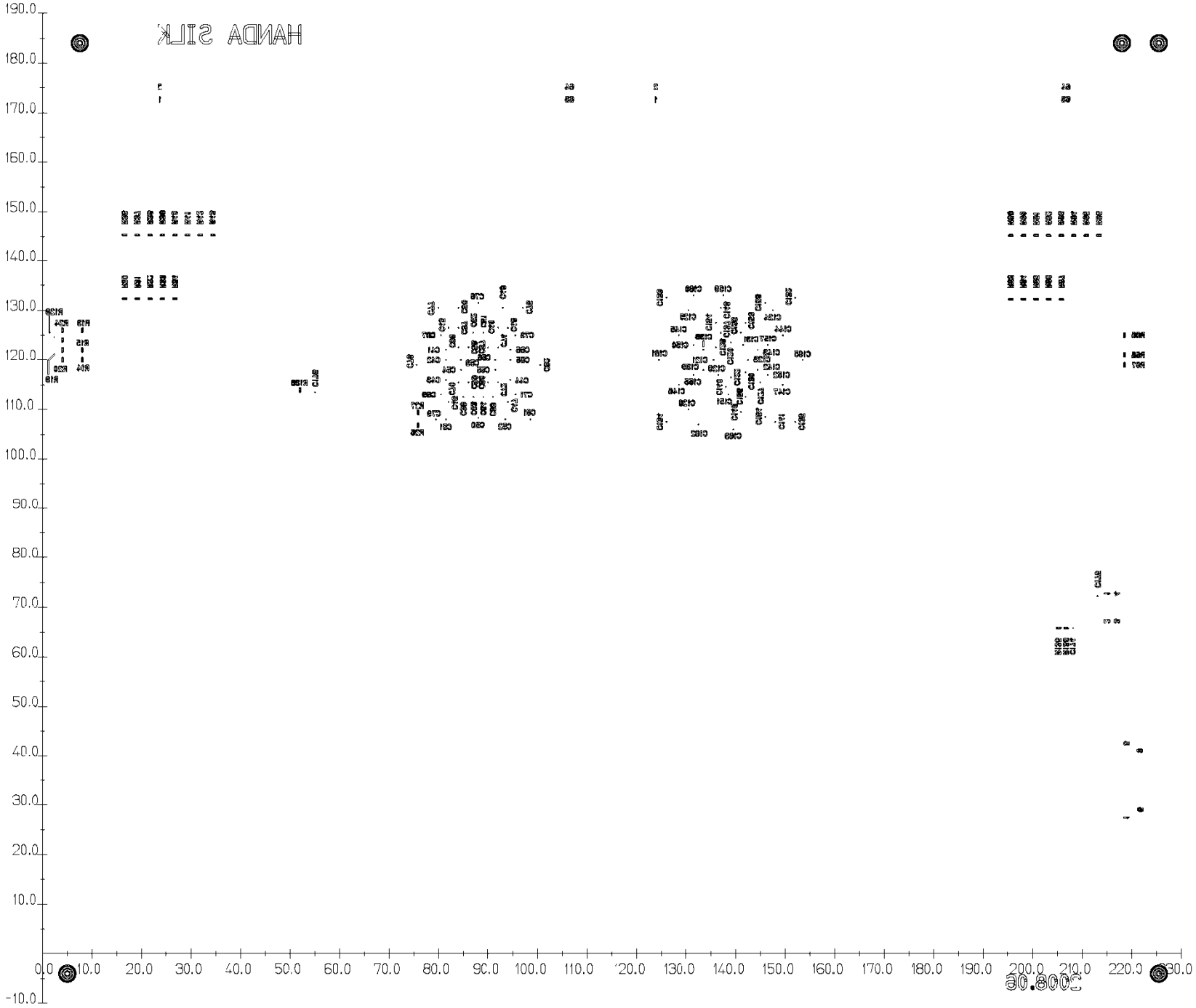

TITLE
DRAWING No.
E3-93961-2
SHEET
5 / 6
DATE
DESIGN

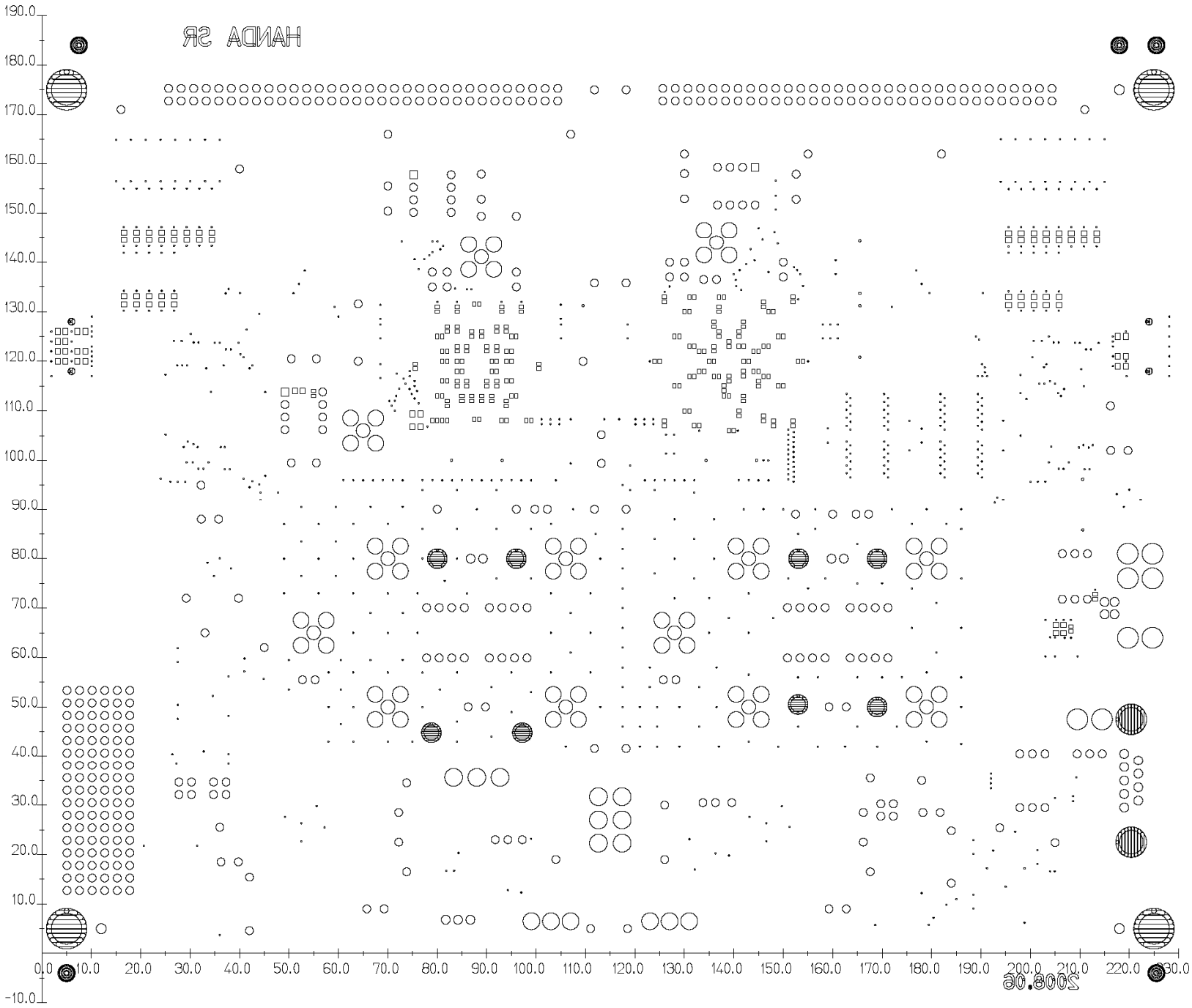


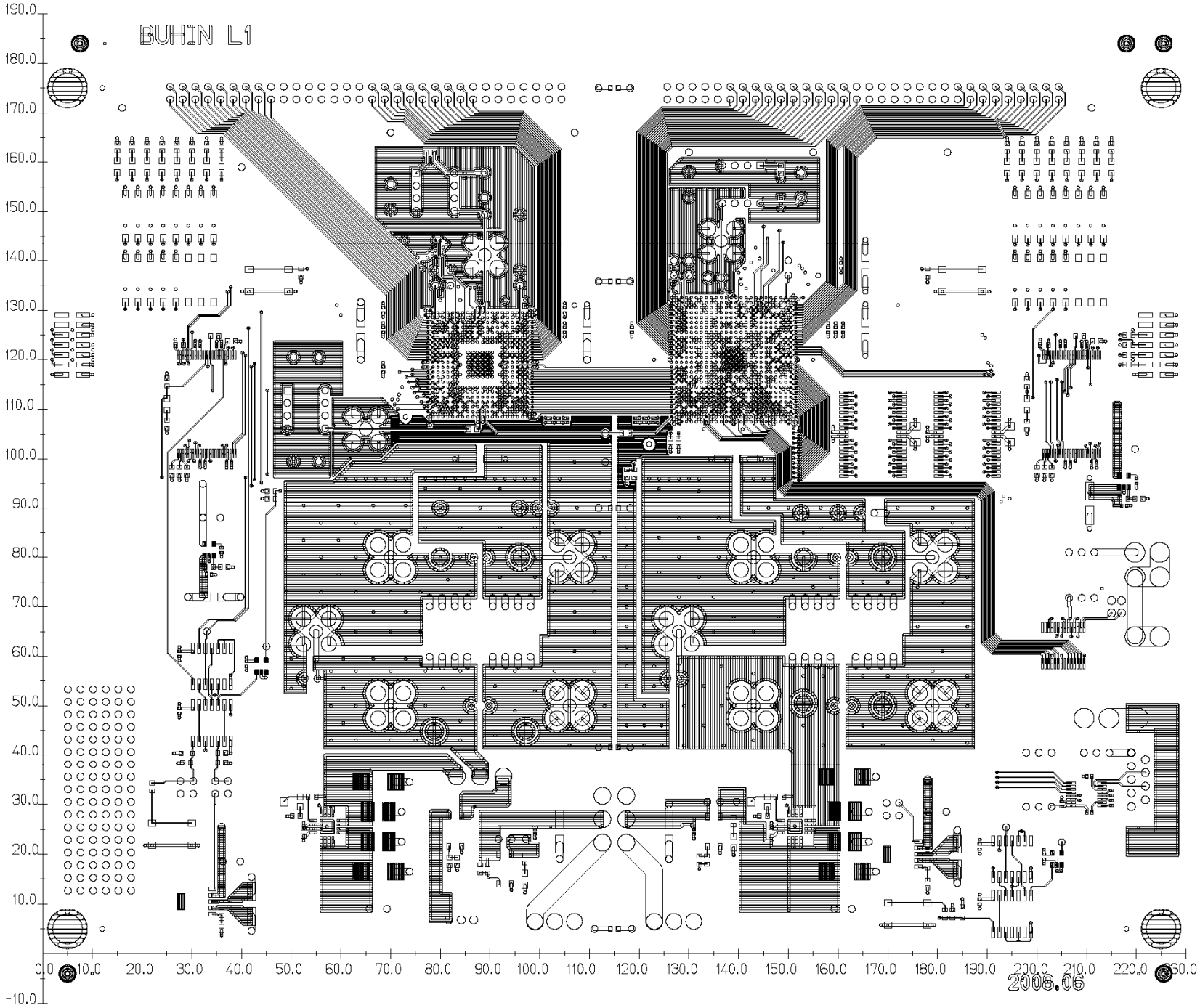
TITLE		DRAWING No.
		E3-93961-2
SHEET	DATE	DESIGN
6 / 6		

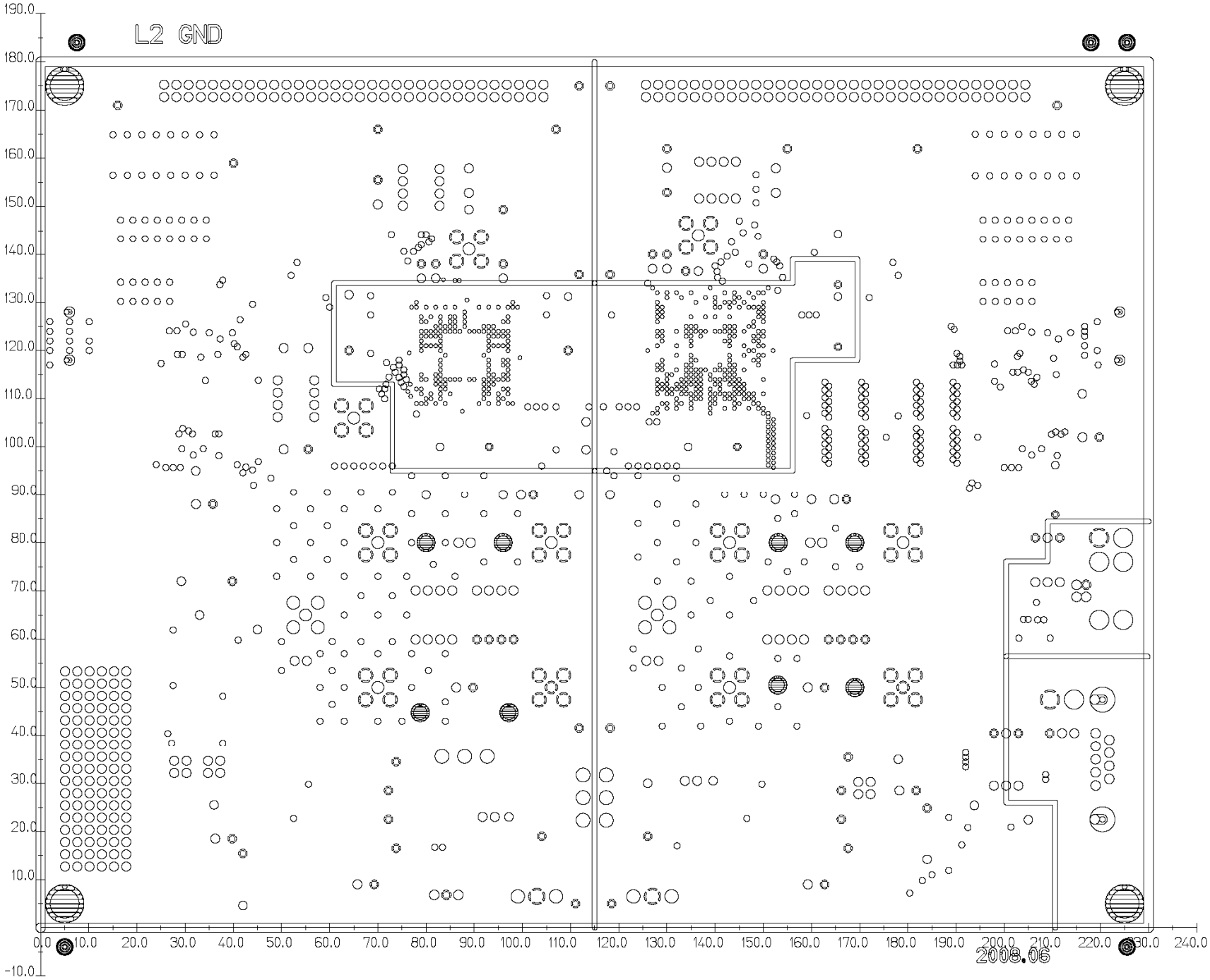

BUHIN SILK
Side-channel Attack
Standard Evaluation BOard
SASEBO-G
3-93961-2
2008.06
3.3V
POWER-A
3.3V
POWER-B
1.6-1.7V
INT
EXT
OFF
ON
240Hz

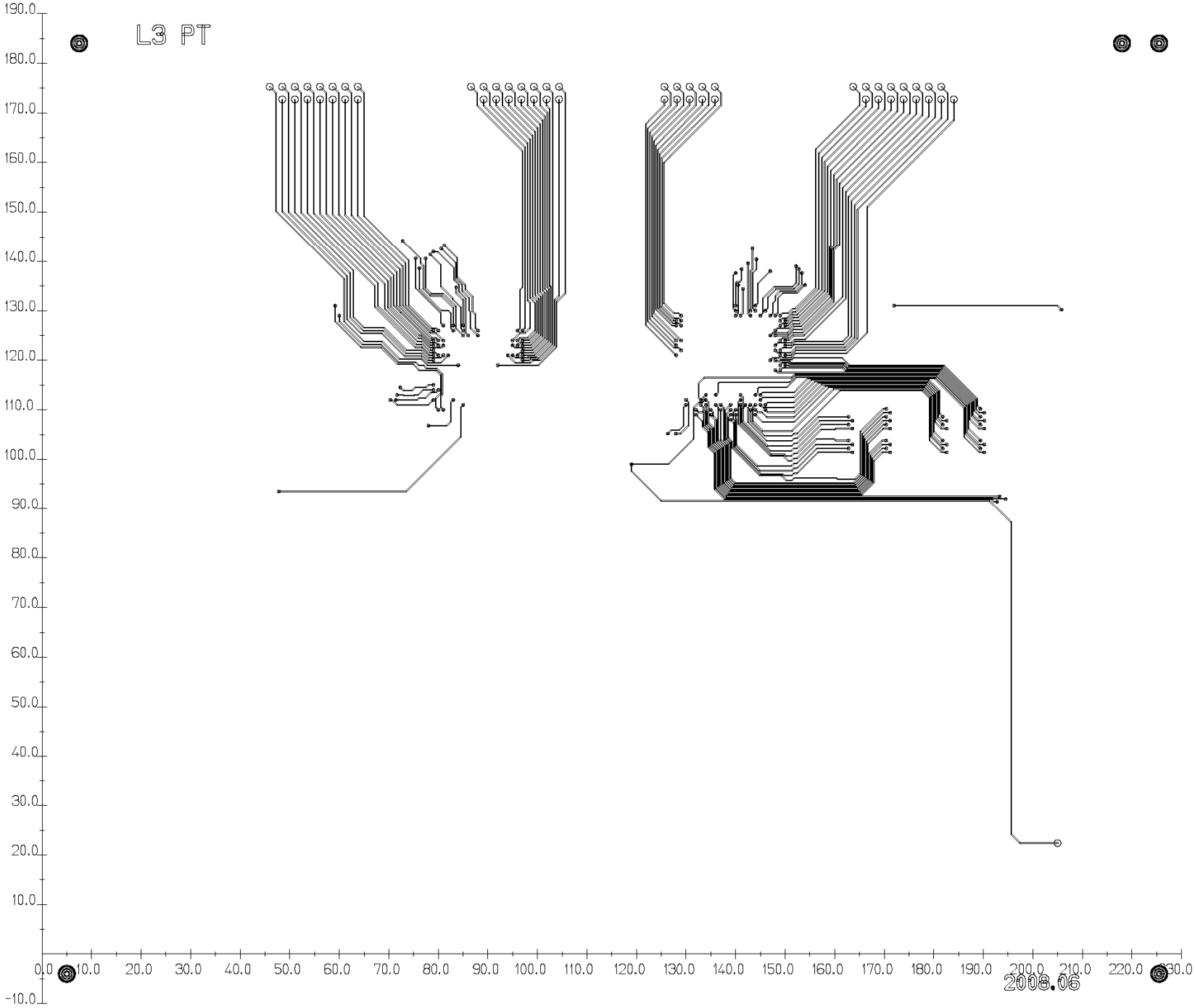

BUHIN SR
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
2008.06

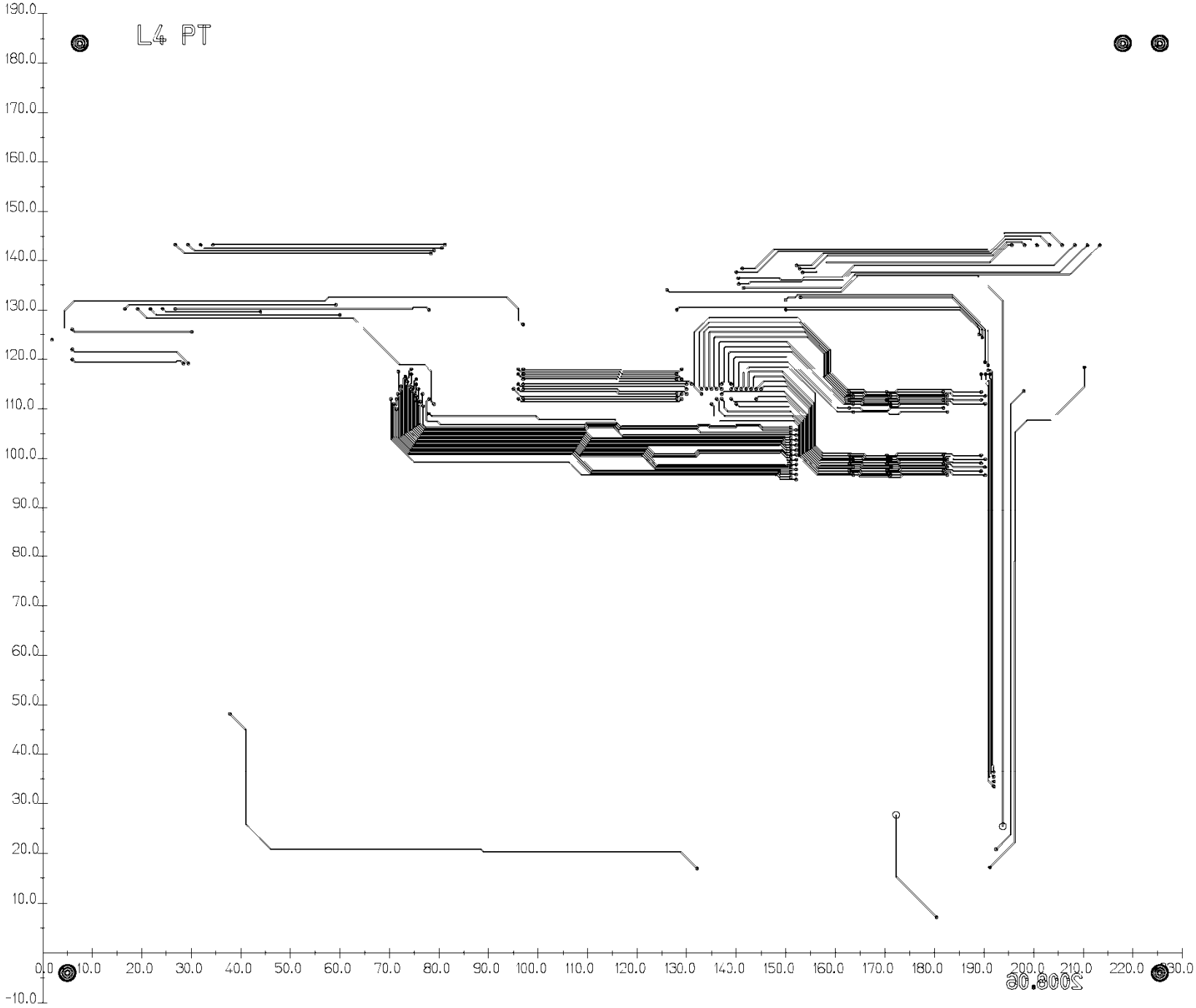

HANDA SILK
30.8008.06

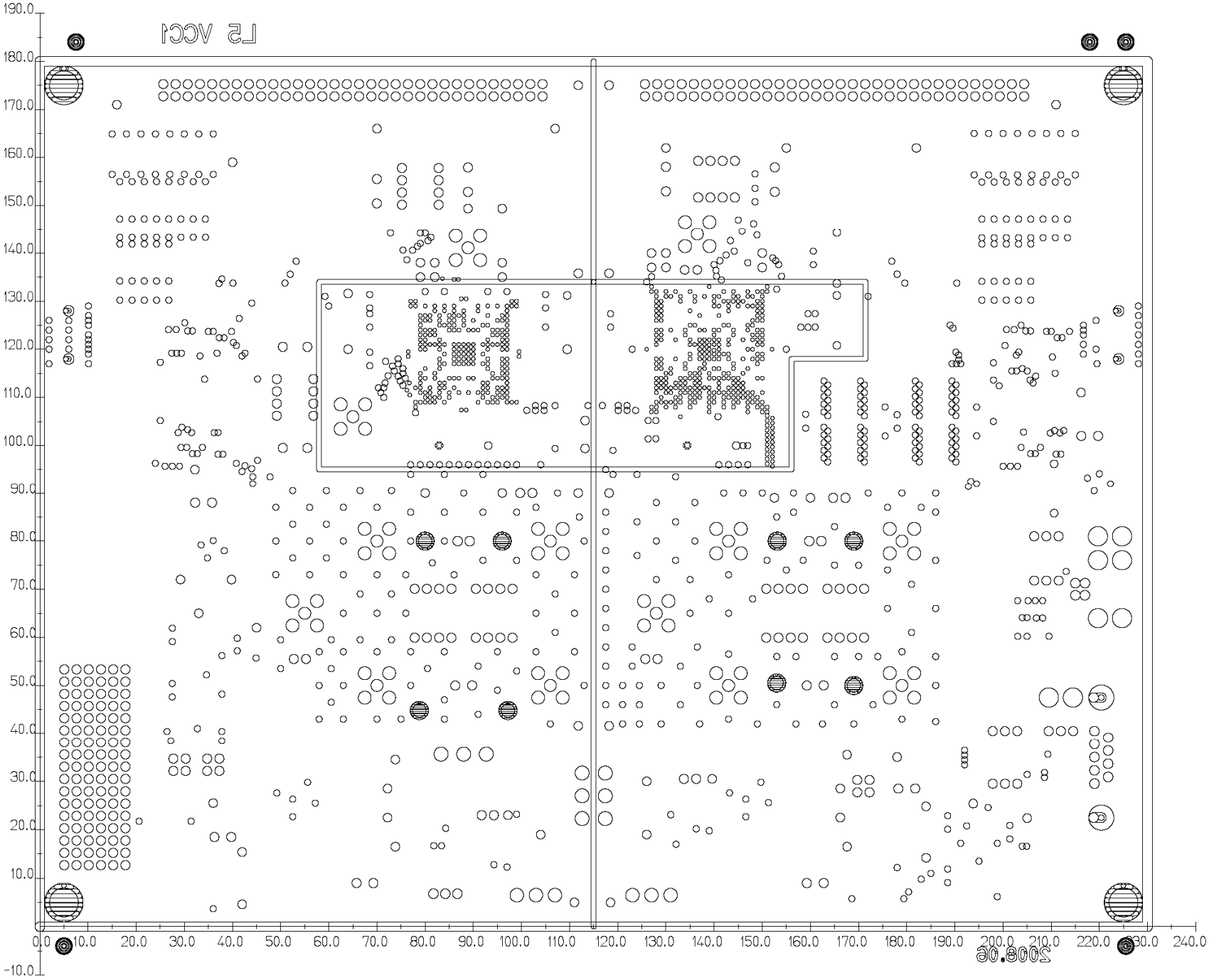

HANDA SR
2006.06
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0

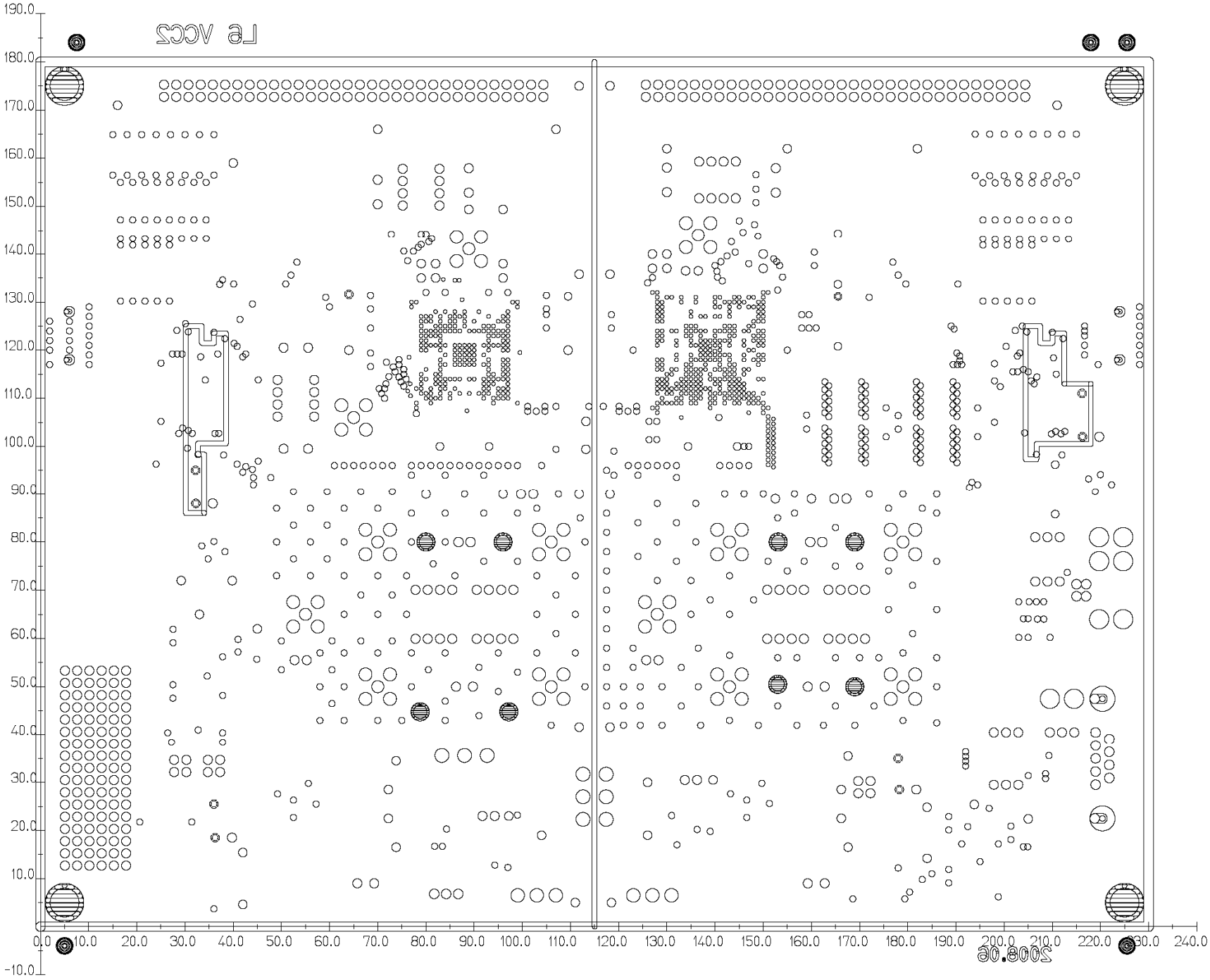

BUHIN L1
2008.06

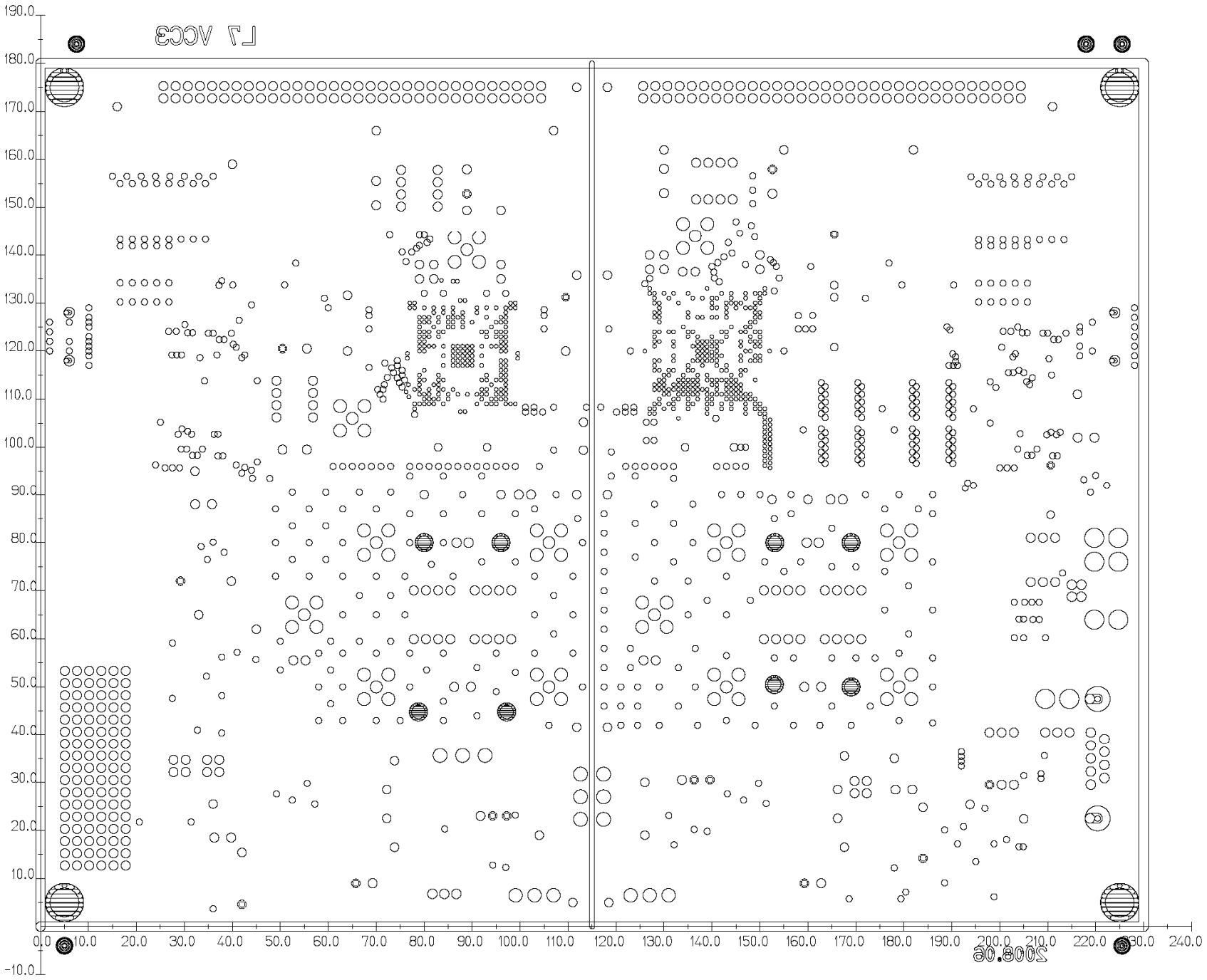

L2 GND
2008.06

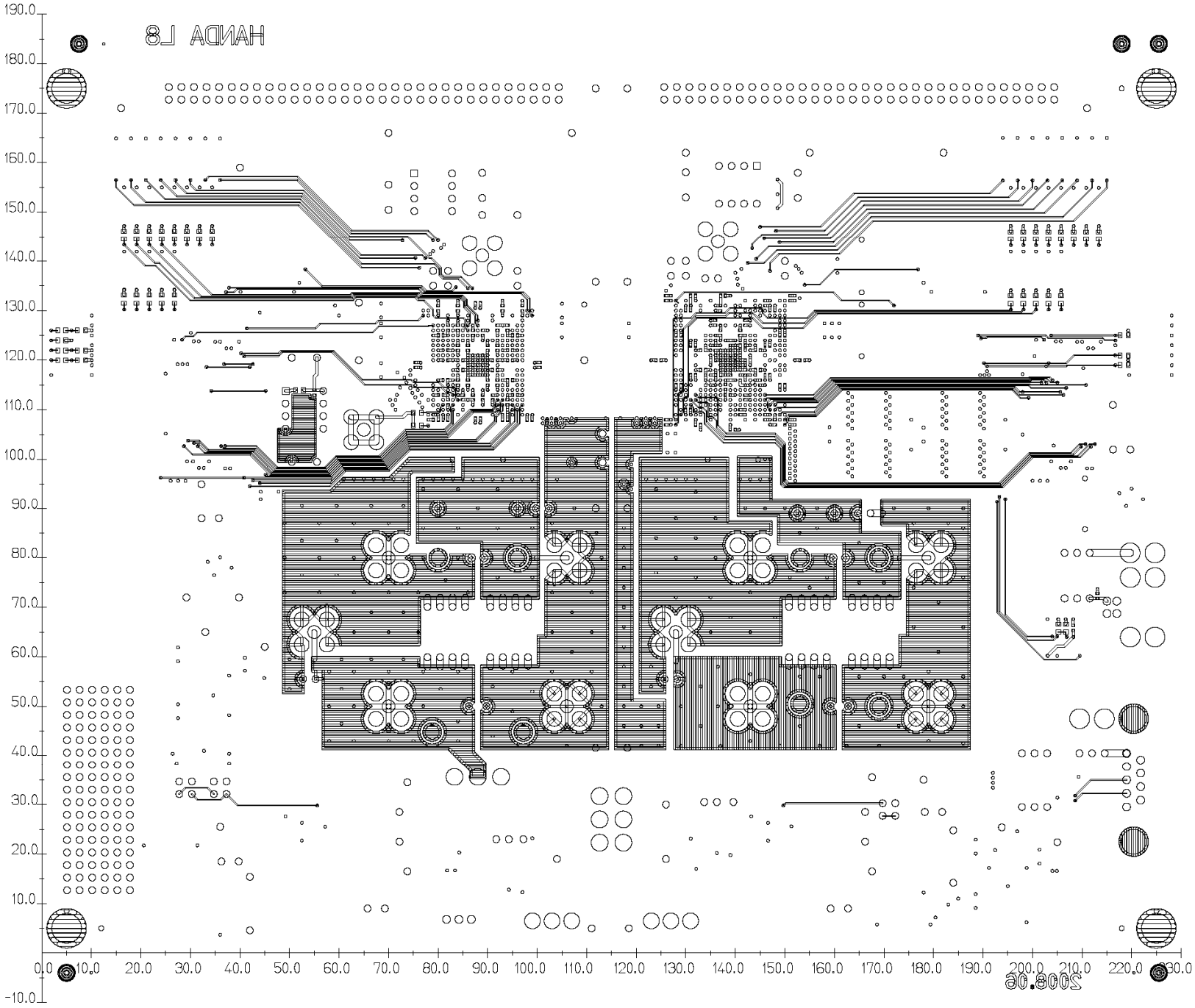

L3 PT
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
2008.06


L4 PT
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
2008.06


L5 VCC1
2008.06
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
240.0


L6 VCC2
2008.06


L7 VCC3
30.8002
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
240.0


HANDA L8
2008.06
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0

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