Side-channel Attack Standard Evaluation Board
SASEBO-B Specification

- Version 1.0 -

April 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) is an FPGA board specifically designed to develop standard evaluation schemes to secure the cryptographic module against physical attacks. The SASEBO-B version board incorporates an ALTERA FPGA. Figure 1 is a photograph of the SASEBO-B. The basic features of the SASEBO-B are as follows:

- 230 mm x 180 mm x 1.6 mm, FR-4, eight layers.
- Two ALTERA Stratix II series FPGAs
  - Cryptographic FPGA: EP2S15F484C5N
  - Control FPGA: EP2S30F672C5N

  These FPGAs 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 provided for each FPGA. External clock input is supported.
- Power regulators supply FPGA voltages with 3.3-V input. The core voltage of the cryptographic FPGA can be applied directly through an external power connector.
- Shunt resistance is provided for power measurement of the FPGAs.
- RS-232 and USB ports for communicating with the host PC.

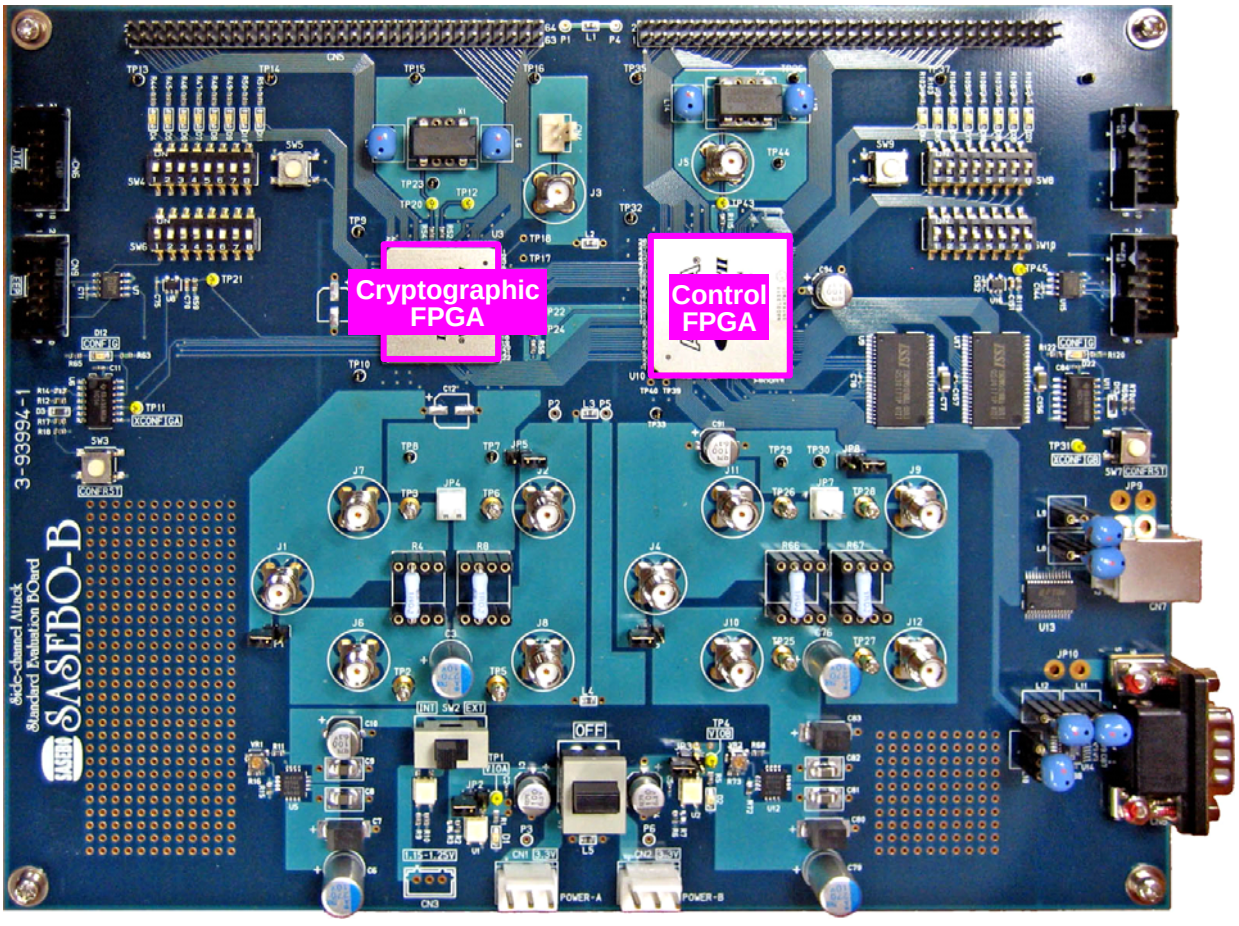


Figure 1 SASEBO-B

2. I/O Assignments

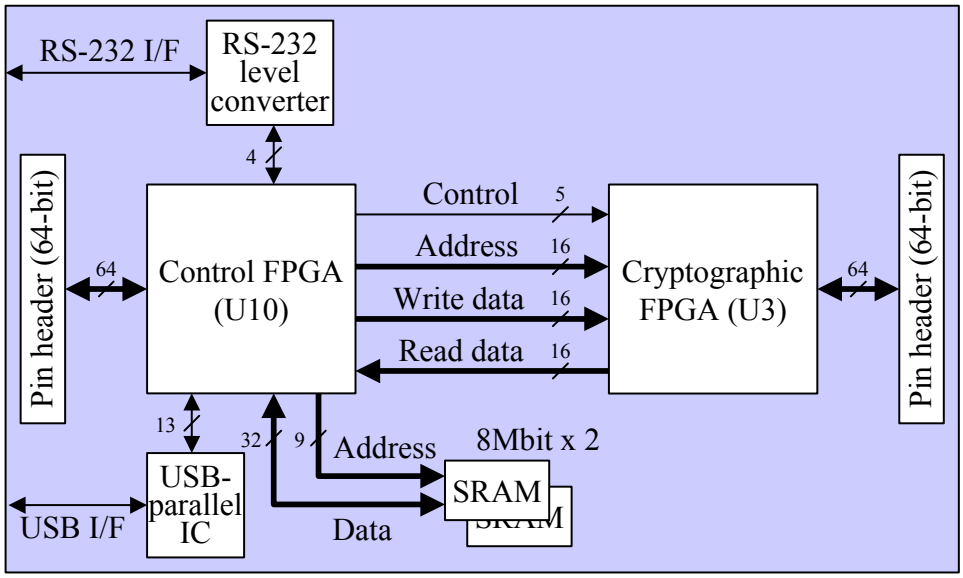


Figure 2: I/O signals

- Pin assignments of the cryptographic FPGA (U3)

Table 1: FPGA control

Signal Name	Pin Number	Input/Output	Description
MSEL3	A4		SW6-5
MSEL2	B4		SW6-6
MSEL1	D4		SW6-7
MSEL0	E5		SW6-8
TDI	AB21		JTAG
TMS	AA20		JTAG
TCK	AA19		JTAG
TRST	AB19		JTAG
TDO	B3		JTAG
nCONFIG	W18		Config
IO_ASDO	G12		Config
IO_nCSO	D11		Config
IO_DATA0	E13		Config
nSTATUS	B20		Config
nCE	A21		Config
DCLK	D19		Config
CONF_DONE	C20		Config
PORSELA	V5		Config
PULLUPA	AB2		Config
PLLENA	Y4		Config
OSCX	M20,M21	IN	Clock
RESETA	AB18	IN	RESET
CLK	N3,N4	IN	X1
CKK_EXT	M2,M3	IN	CN1

Table 2: Cryptographic circuit interface

Signal Name	Pin Number	Input/Output	Destination (U10)
FPGA_DI0	C21	IN	B11
FPGA_DI1	C22	IN	A10
FPGA_DI2	D21	IN	B10
FPGA_DI3	D22	IN	A9
FPGA_DI4	E21	IN	B9
FPGA_DI5	E22	IN	A8
FPGA_DI6	F21	IN	B8
FPGA_DI7	F22	IN	A7
FPGA_DI8	G21	IN	B7
FPGA_DI9	G22	IN	A6
FPGA_DI10	H21	IN	B6
FPGA_DI11	H22	IN	A5
FPGA_DI12	J21	IN	B5
FPGA_DI13	K21	IN	B4
FPGA_DI14	K22	IN	A3
FPGA_DI15	K20	IN	B3
FPGA_DO0	J16	OUT	F11
FPGA_DO1	G17	OUT	C11
FPGA_DO2	G18	OUT	E11
FPGA_DO3	H18	OUT	C10
FPGA_DO4	E19	OUT	D10
FPGA_DO5	E20	OUT	C9
FPGA_DO6	F19	OUT	D9
FPGA_DO7	F20	OUT	C8
FPGA_DO8	G19	OUT	D8
FPGA_DO9	G20	OUT	C7
FPGA_DO10	H19	OUT	D7
FPGA_DO11	H20	OUT	C6
FPGA_DO12	J19	OUT	D6
FPGA_DO13	J20	OUT	C5
FPGA_DO14	K18	OUT	C4
FPGA_DO15	K19	OUT	C3
FPGA_A0	D6	IN	C19
FPGA_A1	C6	IN	D18
FPGA_A2	E7	IN	C18
FPGA_A3	C7	IN	D17
FPGA_A4	D8	IN	C17
FPGA_A5	C8	IN	E17
FPGA_A6	E8	IN	C16
FPGA_A7	E9	IN	G16
FPGA_A8	B5	IN	B21
FPGA_A9	A5	IN	A21
FPGA_A10	B6	IN	B20
FPGA_A11	A6	IN	A20
FPGA_A12	B7	IN	B19
FPGA_A13	A7	IN	A19
FPGA_A14	B8	IN	B18
FPGA_A15	A8	IN	A18
FPGA_WR	B9	IN	B17

FPGA_RD	B10	IN	A17
FPGA_RSV0	C4		C21
FPGA_RSV1	D5		C20
FPGA_RSV2	C5		E18

Table 3: LEDs and switches

Signal Name	Pin Number	Input/Output	Destination
LEDA0	U9	OUT	
LEDA1	AB8	OUT	
LEDA2	AA8	OUT	
LEDA3	AB7	OUT	
LEDA4	AA7	OUT	
LEDA5	AB6	OUT	
LEDA6	AA6	OUT	
LEDA7	AB5	OUT	
DIPSWA0	T8	IN	SW4-1
DIPSWA1	U8	IN	SW4-2
DIPSWA2	V8	IN	SW4-3
DIPSWA3	V7	IN	SW4-4
DIPSWA4	W7	IN	SW4-5
DIPSWA5	Y7	IN	SW4-6
DIPSWA6	U7	IN	SW4-7
DIPSWA7	Y6	IN	SW4-8
SWA	V10	IN	SW5

Table 4: Pin header

Signal Name	Pin Number	Input/Output	Destination
IOA0	Y2	IO	CN5-1
IOA1	Y1	IO	CN5-2
IOA2	W2	IO	CN5-3
IOA3	W1	IO	CN5-4
IOA4	V2	IO	CN5-5
IOA5	V1	IO	CN5-6
IOA6	U2	IO	CN5-7
IOA7	U1	IO	CN5-8
IOA8	T2	IO	CN5-9
IOA9	T1	IO	CN5-10
IOA10	R2	IO	CN5-11
IOA11	R1	IO	CN5-12
IOA12	P2	IO	CN5-13
IOA13	N8	IO	CN5-14
IOA14	T6	IO	CN5-15
IOA15	U5	IO	CN5-16
IOA16	T5	IO	CN5-17
IOA17	W4	IO	CN5-18
IOA18	W3	IO	CN5-19
IOA19	V4	IO	CN5-20
IOA20	V3	IO	CN5-21
IOA21	U4	IO	CN5-22
IOA22	T4	IO	CN5-23

IOA23	T3	IO	CN5-24
IOA24	R4	IO	CN5-25
IOA25	R3	IO	CN5-26
IOA26	R5	IO	CN5-27
IOA27	R6	IO	CN5-28
IOA28	P5	IO	CN5-29
IOA29	P6	IO	CN5-30
IOA30	R7	IO	CN5-31
IOA31	P7	IO	CN5-32
IOA32	P8	IO	CN5-33
IOA33	K6	IO	CN5-34
IOA34	K5	IO	CN5-35
IOA35	J5	IO	CN5-36
IOA36	K3	IO	CN5-37
IOA37	K4	IO	CN5-38
IOA38	J3	IO	CN5-39
IOA39	J6	IO	CN5-40
IOA40	H3	IO	CN5-41
IOA41	H4	IO	CN5-42
IOA42	G3	IO	CN5-43
IOA43	G4	IO	CN5-44
IOA44	H5	IO	CN5-45
IOA45	G5	IO	CN5-46
IOA46	H6	IO	CN5-47
IOA47	G6	IO	CN5-48
IOA48	J7	IO	CN5-49
IOA49	K1	IO	CN5-50
IOA50	K2	IO	CN5-51
IOA51	J2	IO	CN5-52
IOA52	H1	IO	CN5-53
IOA53	H2	IO	CN5-54
IOA54	G1	IO	CN5-55
IOA55	G2	IO	CN5-56
IOA56	F1	IO	CN5-57
IOA57	F2	IO	CN5-58
IOA58	E1	IO	CN5-59
IOA59	E2	IO	CN5-60
IOA60	D1	IO	CN5-61
IOA61	D2	IO	CN5-62
IOA62	C1	IO	CN5-63
IOA63	C2	IO	CN5-64

- Pin assignments of the control FPGA (U10)

Table 5: FPGA control

Signal Name	Pin Number	Input/Output	Destination
MSEL3	F7		SW8-5
MSEL2	E6		SW8-6
MSEL1	B2		SW8-7
MSEL0	G8		SW8-8
TDI	AE25		JTAG

TMS	AD24		JTAG
TCK	AB22		JTAG
TRST	AB21		JTAG
TDO	F6		JTAG
nCONFIG	AA20		Config
IO_ASDO	G14		Config
IO_nCSO	E14		Config
IO_DATA0	E16		Config
nSTATUS	E21		Config
nCE	E22		Config
DCLK	C24		Config
CONF_DONE	B25		Config
PORSELB	Y8		Config
PULLUPB	AE2		Config
PLLENB	AB6		Config
OSCX	A12	IN	Clock
RESETB	Y20	IN	RESET
CLK	P22,P23	IN	X2

Table 6: RS-232

Signal Name	Pin Number	Input/Output	Destination
TX	D2	OUT	Level converter
RX	C1	IN	Level converter
CTS	E1	OUT	Level converter
RTS	E2	IN	Level converter

Table 7: LEDs and switches

Signal Name	Pin Number	Input/Output	Destination
LEDB0	AE24	OUT	
LEDB1	AF24	OUT	
LEDB2	AE23	OUT	
LEDB3	AE22	OUT	
LEDB4	AF22	OUT	
LEDB5	AE21	OUT	
LEDB6	AF21	OUT	
LEDB7	AE20	OUT	
DIPSWB0	AE19	IN	SW8-1
DIPSWB1	AF19	IN	SW8-2
DIPSWB2	AE18	IN	SW8-3
DIPSWB3	AF18	IN	SW8-4
DIPSWB4	AE17	IN	SW8-5
DIPSWB5	AF17	IN	SW8-6
DIPSWB6	AE16	IN	SW8-7
DIPSWB7	AD16	IN	SW8-8
SWB	AF20	IN	SW9

Table 8: Pin header

Signal Name	Pin Number	Input/Output	Destination
IOB0	C25	IO	CN10-1
IOB1	C26	IO	CN10-2

IOB2	D25	IO	CN10-3
IOB3	E25	IO	CN10-4
IOB4	E26	IO	CN10-5
IOB5	F25	IO	CN10-6
IOB6	F26	IO	CN10-7
IOB7	G25	IO	CN10-8
IOB8	G26	IO	CN10-9
IOB9	H25	IO	CN10-10
IOB10	H26	IO	CN10-11
IOB11	J25	IO	CN10-12
IOB12	J26	IO	CN10-13
IOB13	K25	IO	CN10-14
IOB14	K26	IO	CN10-15
IOB15	L25	IO	CN10-16
IOB16	M25	IO	CN10-17
IOB17	M26	IO	CN10-18
IOB18	P25	IO	CN10-19
IOB19	D24	IO	CN10-20
IOB20	E23	IO	CN10-21
IOB21	E24	IO	CN10-22
IOB22	F23	IO	CN10-23
IOB23	F24	IO	CN10-24
IOB24	G23	IO	CN10-25
IOB25	G24	IO	CN10-26
IOB26	H23	IO	CN10-27
IOB27	H24	IO	CN10-28
IOB28	J23	IO	CN10-29
IOB29	J24	IO	CN10-30
IOB30	K23	IO	CN10-31
IOB31	K24	IO	CN10-32
IOB32	L23	IO	CN10-33
IOB33	L24	IO	CN10-34
IOB34	M23	IO	CN10-35
IOB35	M24	IO	CN10-36
IOB36	U26	IO	CN10-37
IOB37	U25	IO	CN10-38
IOB38	V26	IO	CN10-39
IOB39	V25	IO	CN10-40
IOB40	W26	IO	CN10-41
IOB41	W25	IO	CN10-42
IOB42	Y26	IO	CN10-43
IOB43	Y25	IO	CN10-44
IOB44	AA26	IO	CN10-45
IOB45	AA25	IO	CN10-46
IOB46	AB26	IO	CN10-47
IOB47	AB25	IO	CN10-48
IOB48	AC25	IO	CN10-49
IOB49	AD26	IO	CN10-50

IOB50	AD25	IO	CN10-51
IOB51	U24	IO	CN10-52
IOB52	U23	IO	CN10-53
IOB53	V24	IO	CN10-54
IOB54	V23	IO	CN10-55
IOB55	W24	IO	CN10-56
IOB56	W23	IO	CN10-57
IOB57	Y24	IO	CN10-58
IOB58	Y23	IO	CN10-59
IOB59	AA24	IO	CN10-60
IOB60	AA23	IO	CN10-61
IOB61	AB24	IO	CN10-62
IOB62	AB23	IO	CN10-63
IOB63	AC24	IO	CN10-64

Table 9: Cryptographic circuit interface

Signal Name	Pin Number	Input/Output	Destination (U3)
FPGA_DI0	B11	OUT	C21
FPGA_DI1	A10	OUT	C22
FPGA_DI2	B10	OUT	D21
FPGA_DI3	A9	OUT	D22
FPGA_DI4	B9	OUT	E21
FPGA_DI5	A8	OUT	E22
FPGA_DI6	B8	OUT	F21
FPGA_DI7	A7	OUT	F22
FPGA_DI8	B7	OUT	G21
FPGA_DI9	A6	OUT	G22
FPGA_DI10	B6	OUT	H21
FPGA_DI11	A5	OUT	H22
FPGA_DI12	B5	OUT	J21
FPGA_DI13	B4	OUT	K21
FPGA_DI14	A3	OUT	K22
FPGA_DI15	B3	OUT	K20
FPGA_DO0	F11	IN	J16
FPGA_DO1	C11	IN	G17
FPGA_DO2	E11	IN	G18
FPGA_DO3	C10	IN	H18
FPGA_DO4	D10	IN	E19
FPGA_DO5	C9	IN	E20
FPGA_DO6	D9	IN	F19
FPGA_DO7	C8	IN	F20
FPGA_DO8	D8	IN	G19
FPGA_DO9	C7	IN	G20
FPGA_DO10	D7	IN	H19
FPGA_DO11	C6	IN	H20
FPGA_DO12	D6	IN	J19
FPGA_DO13	C5	IN	J20
FPGA_DO14	C4	IN	K18
FPGA_DO15	C3	IN	K19
FPGA_A0	C19	OUT	D6

FPGA_A1	D18	OUT	C6
FPGA_A2	C18	OUT	E7
FPGA_A3	D17	OUT	C7
FPGA_A4	C17	OUT	D8
FPGA_A5	E17	OUT	C8
FPGA_A6	C16	OUT	E8
FPGA_A7	G16	OUT	E9
FPGA_A8	B21	OUT	B5
FPGA_A9	A21	OUT	A5
FPGA_A10	B20	OUT	B6
FPGA_A11	A20	OUT	A6
FPGA_A12	B19	OUT	B7
FPGA_A13	A19	OUT	A7
FPGA_A14	B18	OUT	B8
FPGA_A15	A18	OUT	A8
FPGA_WR	B17	OUT	B9
FPGA_RD	A17	OUT	B10
FPGA_RSV0	C21		C4
FPGA_RSV1	C20		D5
FPGA_RSV2	E18		C5

Table 10: USB

Signal Name	Pin Number	Input/Output	Destination
USB0	F2	IO	USB-Parallel IC
USB1	G1	IO	USB-Parallel IC
USB2	G2	IO	USB-Parallel IC
USB3	J1	IO	USB-Parallel IC
USB4	F1	IO	USB-Parallel IC
USB5	H1	IO	USB-Parallel IC
USB6	J2	IO	USB-Parallel IC
USB7	H2	IO	USB-Parallel IC
USBTXE	M2	IN	USB-Parallel IC
USBRXF	M1	IN	USB-Parallel IC
USBRD	K1	OUT	USB-Parallel IC
USBWR	L2	OUT	USB-Parallel IC
USBWREN	K2	IN	USB-Parallel IC

Table 11: SRAM

Signal Name	Pin Number	Input/Output	Destination
MEMD0	W2	IO	Memory
MEMD1	W1	IO	Memory
MEMD2	V2	IO	Memory
MEMD3	V1	IO	Memory
MEMD4	U2	IO	Memory
MEMD5	U1	IO	Memory
MEMD6	T2	IO	Memory
MEMD7	R2	IO	Memory
MEMD8	AB1	IO	Memory
MEMD9	AA2	IO	Memory
MEMD10	AA1	IO	Memory
MEMD11	Y2	IO	Memory
MEMD12	AB2	IO	Memory
MEMD13	AC2	IO	Memory

MEMD14	AD1	IO	Memory
MEMD15	AD2	IO	Memory
MEMD16	AE5	IO	Memory
MEMD17	AE4	IO	Memory
MEMD18	AF3	IO	Memory
MEMD19	AE3	IO	Memory
MEMD20	AE6	IO	Memory
MEMD21	AF6	IO	Memory
MEMD22	AE7	IO	Memory
MEMD23	AF7	IO	Memory
MEMD24	AF9	IO	Memory
MEMD25	AE9	IO	Memory
MEMD26	AF8	IO	Memory
MEMD27	AE8	IO	Memory
MEMD28	AE10	IO	Memory
MEMD29	AF10	IO	Memory
MEMD30	AE11	IO	Memory
MEMD31	AD11	IO	Memory
MEMA0	Y6	OUT	Memory
MEMA1	W7	OUT	Memory
MEMA2	V7	OUT	Memory
MEMA3	U8	OUT	Memory
MEMA4	T9	OUT	Memory
MEMA5	T7	OUT	Memory
MEMA6	T8	OUT	Memory
MEMA7	V8	OUT	Memory
MEMA8	AB4	OUT	Memory
MEMA9	AC3	OUT	Memory
MEMA10	AA3	OUT	Memory
MEMA11	Y3	OUT	Memory
MEMA12	V4	OUT	Memory
MEMA13	W4	OUT	Memory
MEMA14	Y4	OUT	Memory
MEMA15	AB3	OUT	Memory
MEMA16	AA4	OUT	Memory
MEMA17	W3	OUT	Memory
MEMA18	AA5	OUT	Memory
MEMCS	Y1	OUT	Memory
MEMCS1	AF5	OUT	Memory
MEMWR	W5	OUT	Memory
MEMUB	Y7	OUT	Memory
MEMLB	AA6	OUT	Memory
MEMOE	W8	OUT	Memory

3. Operational Instructions

➢ **Power Supply**

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

DC 3.3V is supplied to the SASEBO-B 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 12: Power supply settings

Connector		CN1	CN2	CN3
Description		Cryptographic FPGA power supply	Control FPGA power supply	Cryptographic FPGA 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

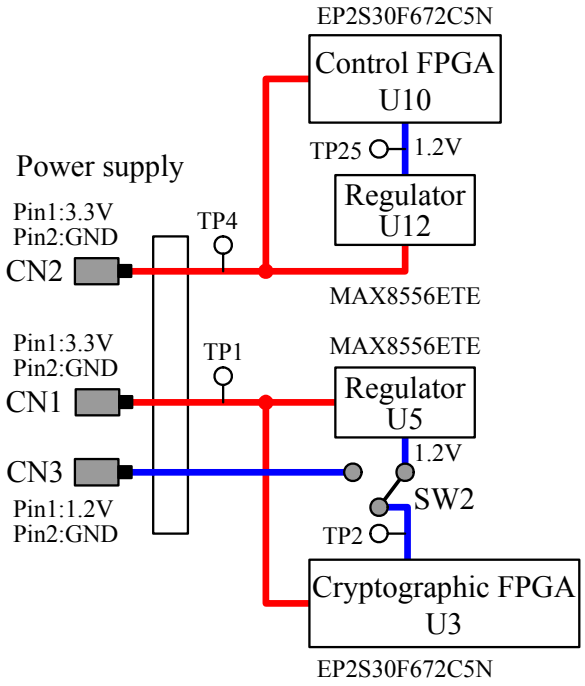


Figure 3: Power supply block on the SASEBO-B

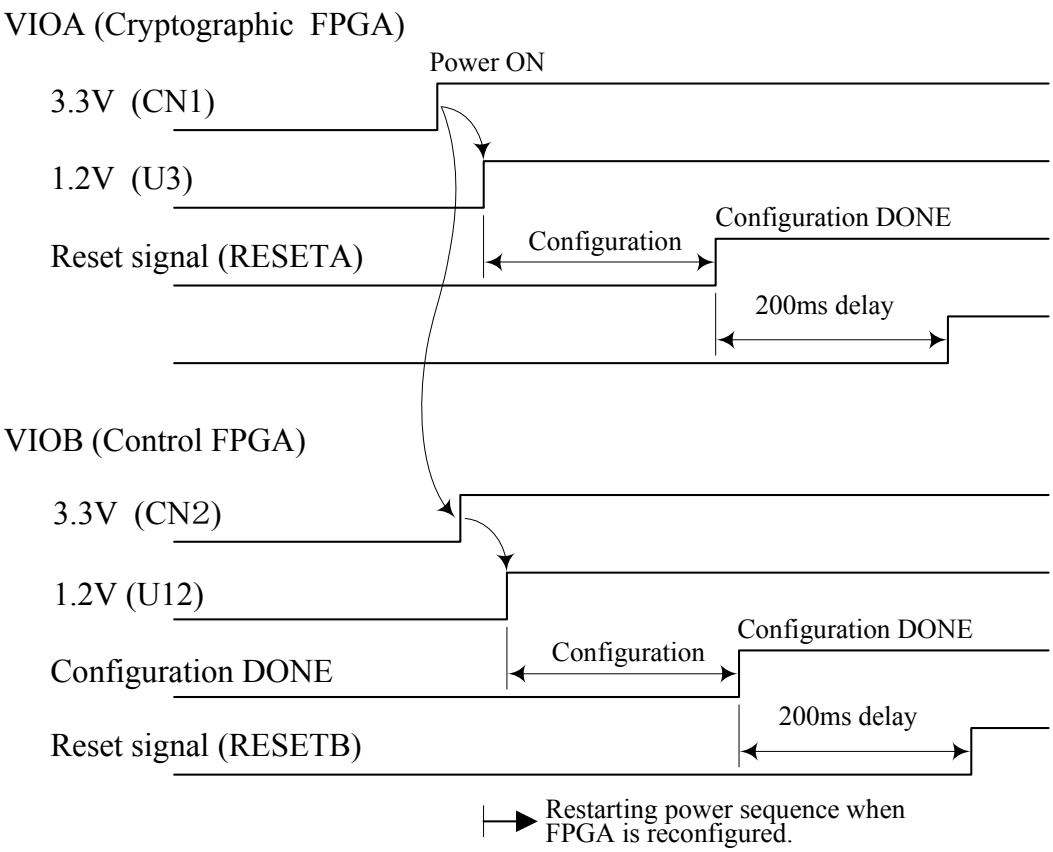


Figure 4: Power sequence of the SASEBO-B

- **Jumper Settings**

Table 13: Jumper settings

Function	Pin	Setting	Description
Power sequence	JP2	Short	Disable the power sequence of the cryptographic FPGA.
		Open	Enable the power sequence of the cryptographic FPGA.
	JP3	Short	Disable the power sequence of the cryptographic FPGA.
		Open	Enable the power sequence of the cryptographic FPGA.
Power consumption measurement	JP1	Short	Bypass R4 shunt resistor on core VCC of the cryptographic FPGA.
		Open	Enable R4 shunt resistor on core VCC of the cryptographic FPGA.
	JP5	Short	Bypass R8 shunt resistor on core GND of the cryptographic FPGA.
		Open	Enable R8 shunt resistor on core GND of the cryptographic FPGA.
	JP6	Short	Bypass R66 shunt resistor on core VCC of the control FPGA.
		Open	Enable R66 shunt resistor on core VCC of the control FPGA.
	JP7	Short	Bypass R67 shunt resistor on core GND of the control FPGA.
		Open	Enable R67 shunt resistor on core GND of the control FPGA.

JP4 and JP9 are voltage test points. DO NOT SHORT JP4 and JP9.

- **FPGA Configuration**

Figure 5 is a block diagram of the FPGA configuration chain of the FPGAs. The configuration chains of the FPGAs are separated. Configuration flash ROMs are programmed through CN9 and CN12 with an Altera USB Blaster. Direct configuration and monitoring is supported with CN6 and CN11. Table 14 shows the pin assignments of CN6 and CN11. FPGAs and Configuration ROMs settings (SW6/SW11) are listed in Table 15. LEDs D12 and D22 indicate that the FPGA is configured successfully. Push down SW3/SW7 to reconfigure the FPGAs.

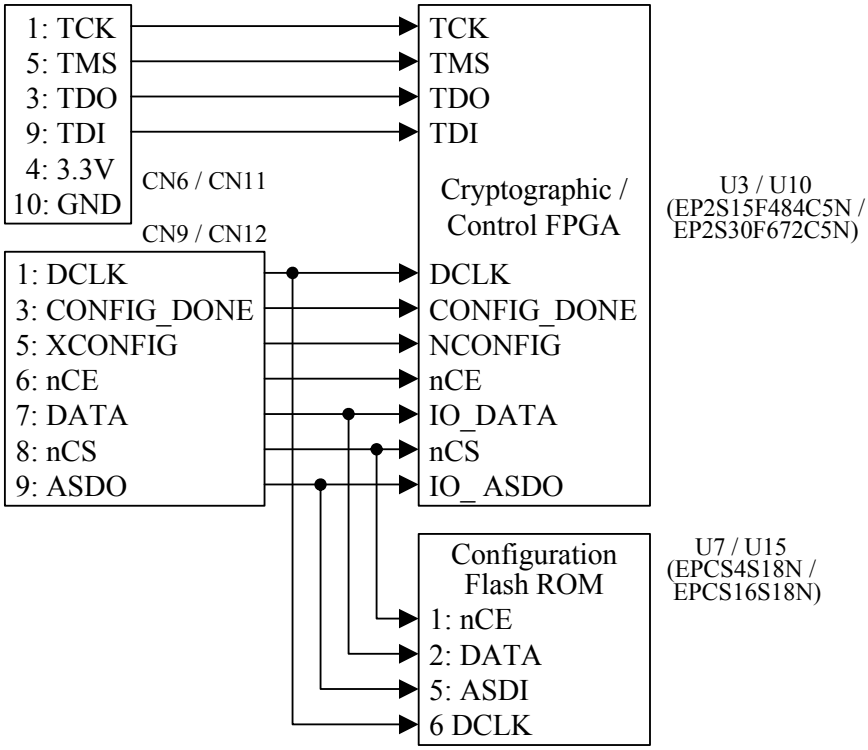


Figure 5: FPGA configuration chain on the SASEBO-B

Table 14: Pin assignment of the JTAG connector (CN6/CN11)

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

Table 15: Configuration mode settings (SW6/SW10)

Dip1			ON
Dip2	PORSEL	Reset interval setting OFF:12ms ON:100ms	OFF
Dip3	PULLUP	I/O pad pull-up setting OFF: pull-up ON: none	OFF
Dip4	PLLENA	PLL setting OFF: Disable ON: Enable	ON
Dip5	MSEL4		OFF
Dip6	MSEL3		OFF
Dip7	MSEL1		ON
Dip8	MSEL0		OFF

➢ **Clock Source**

The clock source connection of the SASEBO-B is shown in Figure 6. A 24-MHz oscillator and a SMA connector (J3/J5) ar connected to each FPGA individually. An external clock can be supplied to the FPGA through the SMA connector.

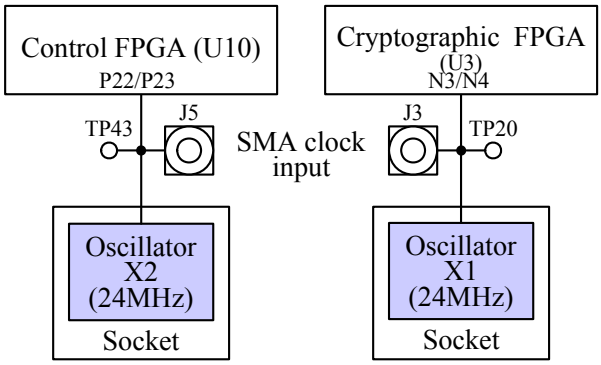


Figure 6: Clock source connection

➢ **Host Interface**

RS-232 and USB are provided on the SASEBO-B for communicating with the host PC. Tables 16 and 17 show the signal assignments of the RS-232 and USB interfaces. A 9-pin female-female straight cable connects the SASEBO-B 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 16: Signal assignment on the RS-232 interface

Signal	CN8 (XM2C-0912-111)	U14 (ADM3202ARN)		U10 (EP2S30F672C5N)
TX	2 pin	14 pin	D2	D2
RX	3 pin	13 pin	C1	C1
CTS	8 pin	7 pin	E1	E1
RTS	7 pin	8 pin	E2	E2

Table 17: Signal assignment on the USB interface

Signal	CN7 (XM7B-0422)	U13 (FT245RL)	U10 (EP2S30F672C5N)
USBDP	2 pin	15 pin	-
USBDM	3 pin	16 pin	-
USBD0	-	1 pin	F2
USBD1	-	5 pin	G1
USBD2	-	3 pin	G2
USBD3	-	11 pin	J1
USBD4	-	2 pin	F1
USBD5	-	9 pin	H1
USBD6	-	10 pin	J2
USBD7	-	6 pin	H2
USBTXE	-	22 pin	M2
USBRXF	-	23 pin	M1
USBRD	-	13 pin	K1
USBWR	-	14 pin	L2
USBPWREN	-	12 pin	K2

4. BOARD SCHEMATIC AND LAYOUT

The parts list for the SASEBO-B is shown in Table 18. The board schematic and layout of the SASEBO-B are presented on pages 19 to 35.

Table 18: Parts List

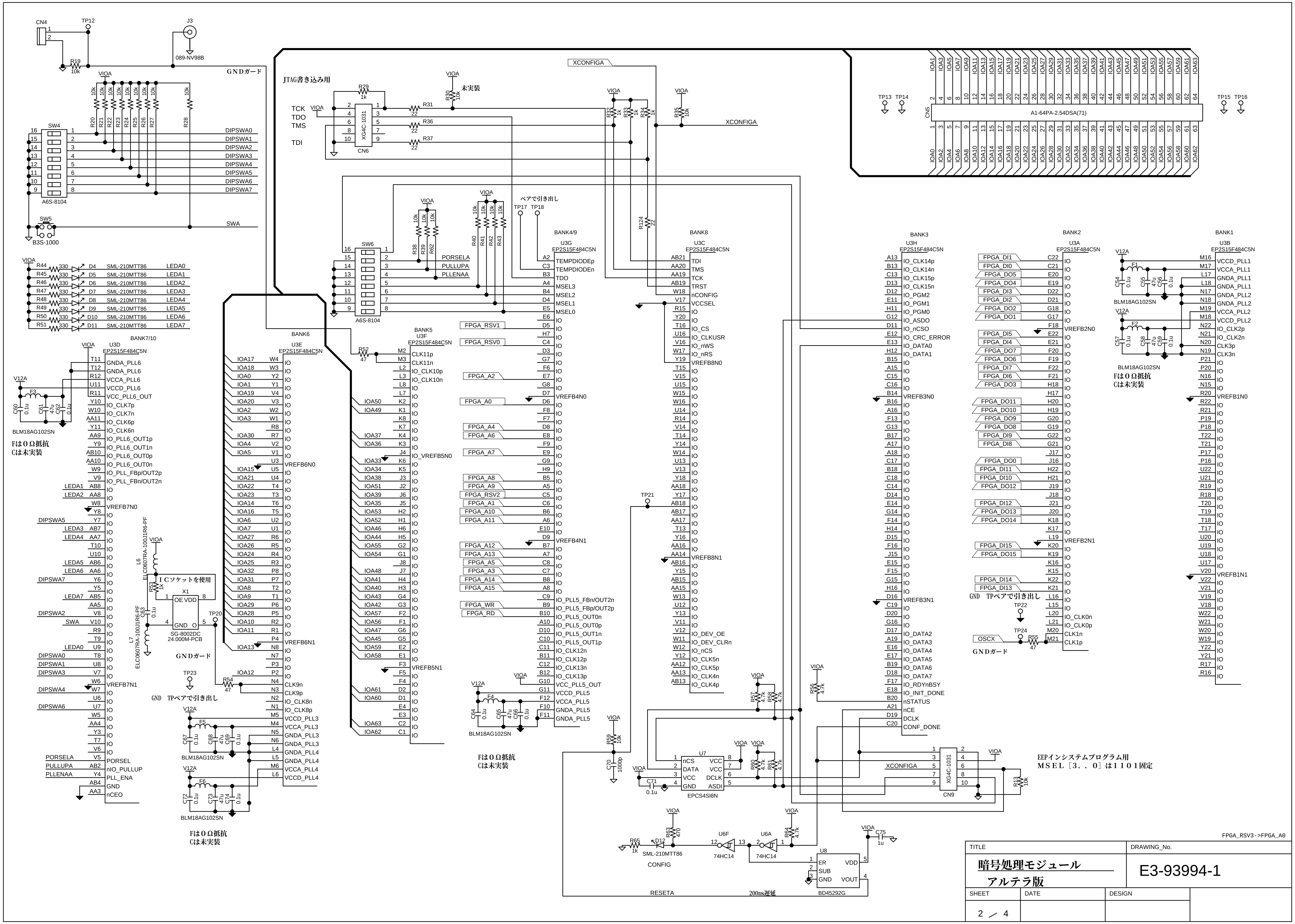
Board name	SASEBO-B
Model Number	E3-93994-1

Description	Part Number	Maker	Qty	Reference Designator
Ceramic Capacitor	GRM155F11H103ZA57E	MURATA	22	C32,C33,C34,C35,C36,C37,C38,C39,C40, C41,C42,C43,C44,C45,C46,C47,C48,C49, C50,C51,C52,C53,C112,C113,C114,C115, C116,C117,C118,C119,C120,C121,C122, C123,C124,C125,C126,C127,C128,C129, C130,C131,C132,C133
Ceramic Capacitor	GRM155F11E104ZA01D	MURATA	38	C2,C5,C11,C20,C21,C22,C23,C24,C25, C26,C27,C28,C29,C30,C31,C54,C56,C57, C59,C60,C62,C63,C64,C66,C67,C69,C71, C72,C74,C84,C85,C86,C87,C88,C89,C90, C99,C100,C101,C102,C103,C104,C105, C106,C107,C110,C111,C134,C136,C137, C139,C140,C142,C143,C144,C145,C147, C148,C150,C153,,C155,C78,C157
Ceramic Capacitor	GRM188B11H102KA01D	MURATA	2	C70,C151
Ceramic Capacitor	GRM155F10J105ZE01D	MURATA	10	C13,C14,C16,C17,C18,C19,C75,C92,C93, C95,C96,C97,C98,C108,C109,C152,
Ceramic Capacitor	JMK316BJ476ML-T	TAIYO YUDEN	11	C8,C9,C55,C58,C61,C65,C68,C73,C77, C81,C82,C135,C138,C141,C146,C149, C154,C156
Electrolytic Capacitor	EMV-6R3ADA101MF55G	Nippon Chemi-Con	5	C1,C4,C10,C12,C15,C91,C94
Capacitor	EEFUE0J151	Panasonic	3	C7,C80,C83
Capacitor	APSA100ELL271MHB5S	Nippon Chemi-Con	4	C3,C6,C76,C79
Resistor	RK73Z1JTTD 0Ω	KOA	6	F1,F2,F3,F4,F5,F6
Resistor	RR0816-101-D	SSM	2	R2,R3,R6,R7,R14
Resistor	RR0816-103-D	SSM	49	R12,R17,R19,R20,R21,R22,R23,R24,R25, R26,,R27,R28,R30,R35,R38,R39,R40,R41, R42,R43,,R59,R62,R69,R72,R74,R78,R79, R80,R81,R82,,R83,R84,R85,R86,R87,R91, R95,R96,R97,R98,R99,R100,R113,R114, R116,R117,R118,R119,R121,R123,R15
Resistor	RR0816-102-D	SSM	20	R11,R13,R16,R18,R29,R32,R33,R34,R53, R65,,R68,R70,R71,R73,R77,R88,R89,R90, R112,R122
Resistor	RR0816-201-D	SSM	2	R9,R10
Resistor	RR0816-220-D	SSM	8	R31,R36,R37,R92,R93,R94,R124,R125
Resistor	RR0816-331-D	SSM	18	R1,R5,R44,R45,R46,R47,R48,R49,R50, R51,R102,R103,R104,R105,R106,R107, R108,R109
Resistor	RR0816-472-D	SSM	7	R56,R57,R58,R60,R61,R64,R75
Resistor	RR0816-470-D	SSM	4	R52,R54,R55,R115
Resistor	RR0816-471-D	SSM	2	R63,R120
Diode	1SS352(-TPH3)	TOSHIBA	2	D3,D13
DIP Switch	A6S-8104-H	OMRON	4	SW4,SW6,SW8,SW10

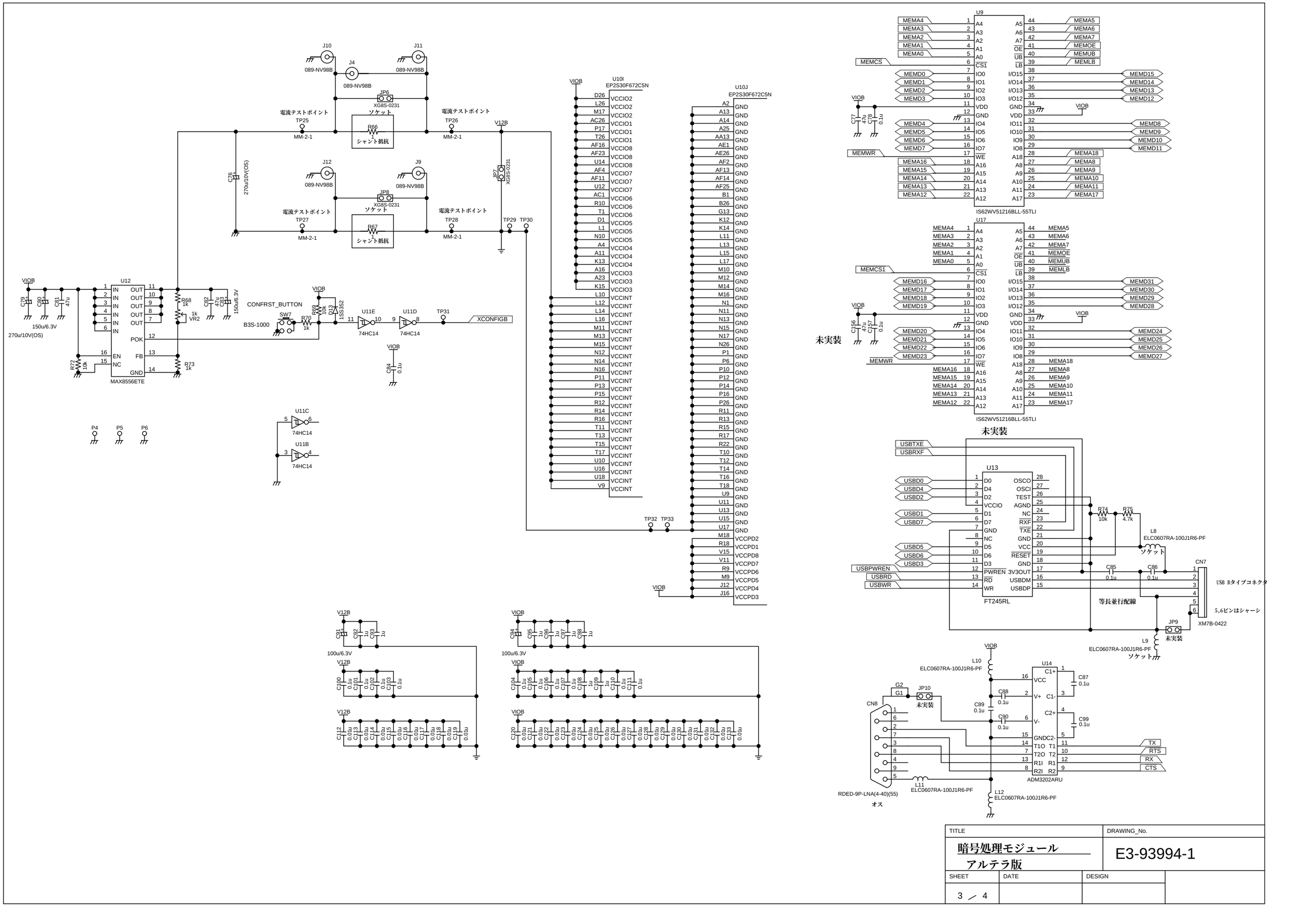
Push Button	B3S-1000	OMRON	4	SW3,SW5,SW7,SW9
Switch, Slide	CS-12AAP1	Nikkai	1	SW2
Switch, Slide	CS-22AAP1	Nikkai	1	SW1
FPGA	EP2S15F484C5N	Altera	1	U3
FPGA	EP2S30F672C5N	Altera	1	U10
EEPROM	EPCS16SI8N	Altera	1	U15
EEPROM	EPCS4SI8N	Altera	1	U7
CMOS	SN74HC14NSE4	TI	2	U6,U11
SRAM	IS62WV51216BLL-55TLI	ISSI	1	U9
USB IC	FT245RL	FDI	1	U13
RS-232 Level Converter	ADM3202ARUZ	Analog Devices	1	U14
Reset IC	BD45292G	ROHM	2	U8,U16
Regulator IC	MAX8556ETE	MAXIM	2	U5,U12
Inductor	ELC0607RA-100J1R6-PF	TDK	9	L6,L7,L8,L9,L10,L11,L12,L13,L14
Filter	BLM18AG102SN	MURATA	5	L1,L2,L3,L4,L5,F7,F8,F9,F10,F11,F12,
LED	SML-210MTT86	ROHM	20	D1,D2,D4,D5,D6,D7,D8,D9,D10,D11,D12, D14,D15,D16,D17,D18,D19,D20,D21,D22
Connector	DF1-2P-2.5DSA	HIROSE	1	CN4
Connector	XG4C-1031	OMRON	4	CN6,CN9,CN11,CN12
Connector	A1-64PA-2.54DSA(71)	HIROSE	2	CN5,CN10
Connector	B3P-VH(LF)(SN)	HIROSE	2	CN1,CN2
Connector	B3B-XH-A(LF)(SN)	JST	1	CN3
USB Connector	XM7B-0442	OMRON	1	CN7
D-sub Connector	XM2C-0912-111	OMRON	1	CN8
MOS Relay	G3VM-61GR1	OMRON	3	U1,U2,U4
SG-8002DC	24.000M-PCB	EPSON	2	X1,X2
SMA Connecotr	T124 426 000N	TAKITEK	12	J1,J2,J3,J4,J5,J6,J7,J8,J9,J10,J11,J12
Test Point	LC-3-G(Black)	MAC8	18	TP7,TP8,TP9,TP10,TP13,TP14,TP15,TP16, TP23,TP29,TP30,TP32,TP33,TP35,TP36, TP37,TP38,TP44
Test Point	MM-2-1	MAC8	8	TP2,TP3,TP5,TP6,TP25,TP26,TP27,TP28
Trimmer	ST-32EA 1KΩ(13)	COPAL	2	VR1,VR2
Resistor	ERX1SJ1R0	Panasonic	4	R4,R8,R66,R67
Shunt	XG8S-0231	OMRON	6	JP1,JP2,JP3,JP5,JP6,JP8
Connector	B2P-SHF-1AA(LF)(SN)	JST	2	JP4,JP7
Jumper Socket	XJ8A-0211	OMRON	8	
IC Socket	R110-91-308	PRECI-DIP	2	

外部入力電源１
3.3V
CN1
B3P-VH(LF)(SN)
SW1
CS-22AAP1
外部入力電源２
3.3V
CN2
B3P-VH(LF)(SN)
C1 C2 0.1u 100u/6.3V
C4 C5 0.1u 100u/6.3V
XG8S-0231
JP2
JP3
TP1 VIOA
TP4 VIOB
R1 330
R5 330
R2 100
R3 1M
R6 1M
R7 100
U1 AQV212GS
U2 AQV212GS
D1 SML-210MTT86
D2 SML-210MTT86
未実装
FPGA１メイン電源
FPGA２メイン電源
外部入力電源３
コア電源　1.15-1.25
CN3
B3B-XH-A(LF)(SN)
未実装（添付品）
R9 200
R10 200
1/8W
U4 AQV212GS
EXT
INT
SW2
CS-12AAP1
J6 J7 J1 J8 J2
089-NV98B
JP1 JP5 XG8S-0231
JP4 XG8S-0231
ソケット
R4 R8 1 シャント抵抗
電流テストポイント
TP2 TP3 TP5 TP6
MM-2-1
V12A
C3 270u/10V(OS)
TP7 TP8
U3I
EP2S15F484C5N
B22 L22 AA22 M22 AB12 AB20 AB3 AB11 AA1 M1 B1 L1 A3 A11 A12 A20
VCCIO2 VCCIO2 VCCIO1 VCCIO1 VCCIO8 VCCIO8 VCCIO7 VCCIO7 VCCIO6 VCCIO6 VCCIO5 VCCIO5 VCCIO4 VCCIO4 VCCIO3 VCCIO3
H8 J9 J11 J13 K10 K12 L11 L13 M8 M10 M12 M14 N11 N13 P9 P12 P14
VCCINT
270u/10V(OS)
C6 C7 150u/6.3V
C8 47u
U5
MAX8556ETE
IN OUT EN NC FB POK GND
C9 C10 47u 100u/6.3V
R11 1k
1k VR1
R15 10k
R16 1k
R12 10k
R14 100
未実装
U6C U6D 74HC14
C11 0.1u
VIOA
TP9 TP10
U3J
EP2S15F484C5N
A1 A9 A14 A22 AA2 AA21 AB1 AB9 AB14 AB22 B2 B21 H15 J1 J10 J12 J14 J22 K9 K11 K13 L10 L12 L14 M7 M9 M11 M13 M15 N10 N12 N14 P1 P11 P13 P22 R10
GND
K14 P15 R13 P10 N9 L9 H10 H13
VCCPD2 VCCPD1 VCCPD8 VCCPD7 VCCPD6 VCCPD5 VCCPD4 VCCPD3
L1 L2 L3 L4 L5
BLM18AG102SN
P1 P2 P3
CONFRST_BUTTON
SW3 B3S-1000
R17 2k
R18 1k
D3 1SS352
U6B U6E 74HC14
TP11
XCONFIGA
未実装
C12 C13 1u C14 1u 100u/6.3V
C15 C16 1u C17 1u C18 1u C19 1u 100u/6.3V
C20 C21 C22 C23 0.1u
C24 C25 C26 C27 C28 C29 C30 C31 0.1u
C32 C33 C34 C35 C36 C37 C38 C39 0.01u
C40 C41 C42 C43 C44 C45 C46 C47 C48 C49 C50 C51 C52 C53 0.01u

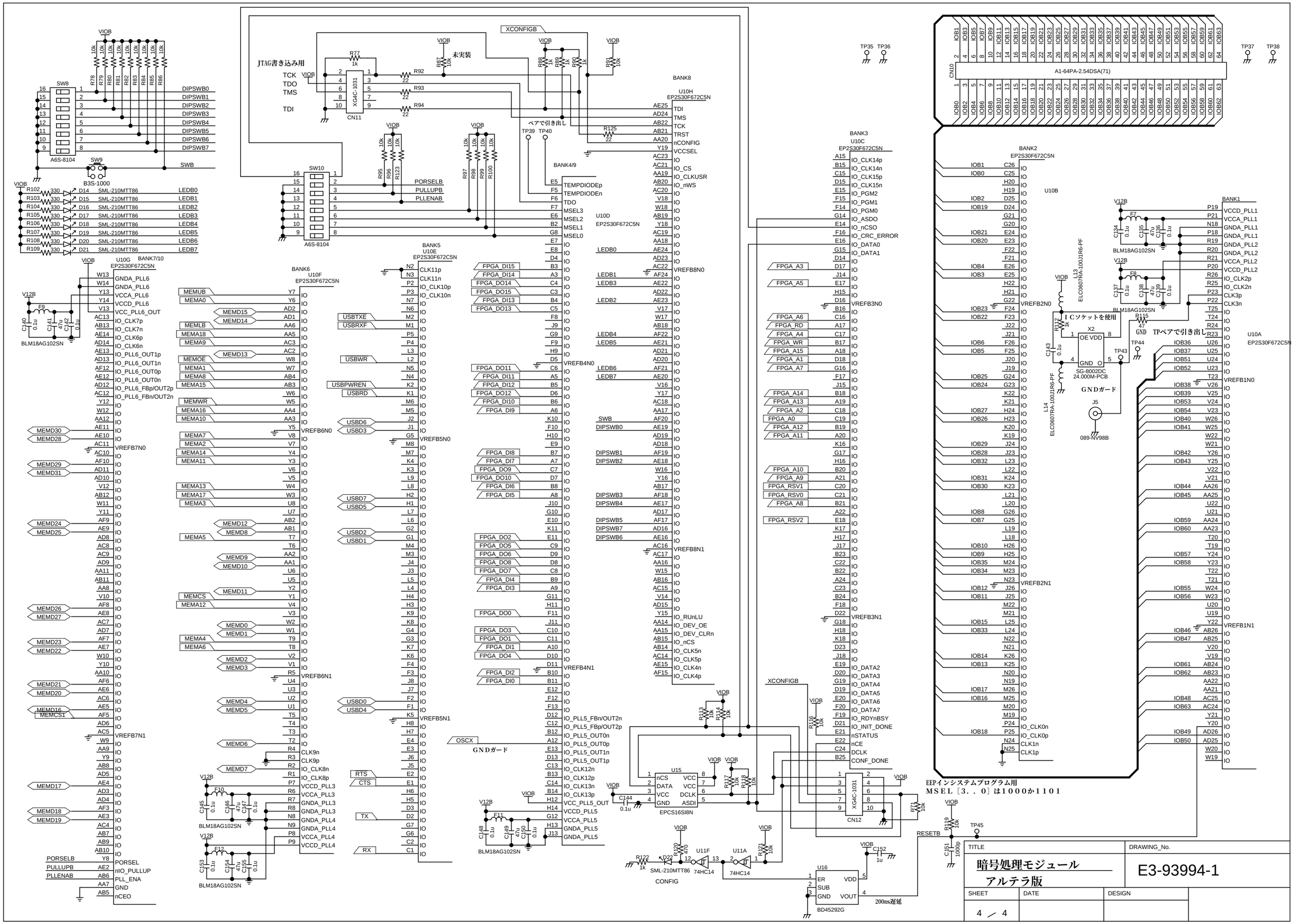
TITLE	DRAWING_No.
暗号処理モジュール アルテラ版	E3-93994-1
SHEET	DATE	DESIGN
1 ／ 4		



GNDガード
JTAG書き込み用
未実装
ペアで引き出し
ICソケットを使用
Fは0Ω抵抗
Cは未実装
GND TPペアで引き出し
EEPインシステムプログラム用
MSEL［3．．0］は1101固定
CONFIG
RESETA
200ms遅延
BD45292G
EP2S15F484C5N
EPCS4SI8N
SG-8002DC
24.000M-PCB
A1-64PA-2.54DSA(71)
FPGA_RSV3->FPGA_A0
TITLE
DRAWING_No.
暗号処理モジュール
アルテラ版
E3-93994-1
SHEET
DATE
DESIGN
2 ／ 4



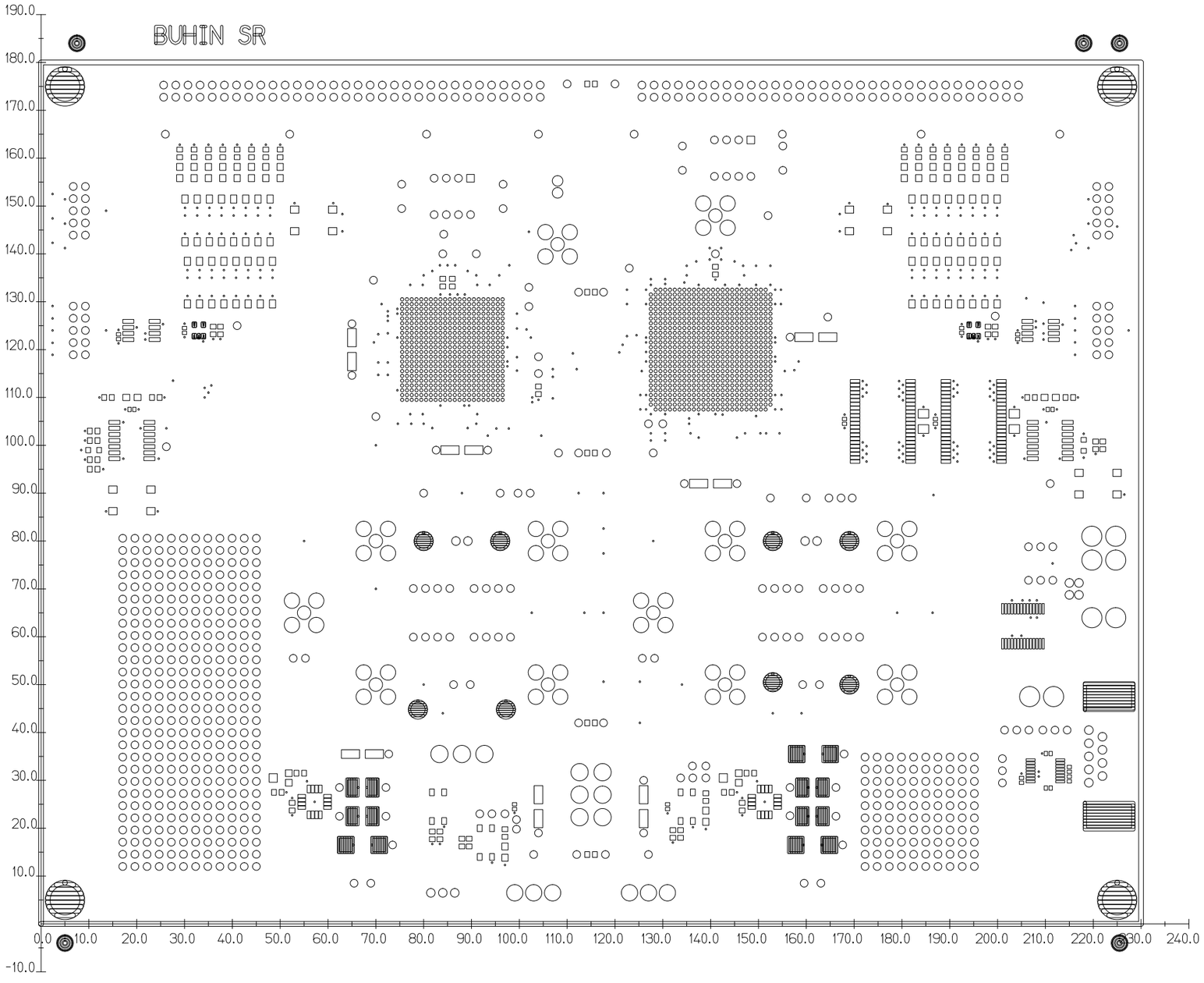
TITLE	DRAWING_No.
暗号処理モジュール アルテラ版	E3-93994-1
SHEET	DATE	DESIGN
3 ／ 4		

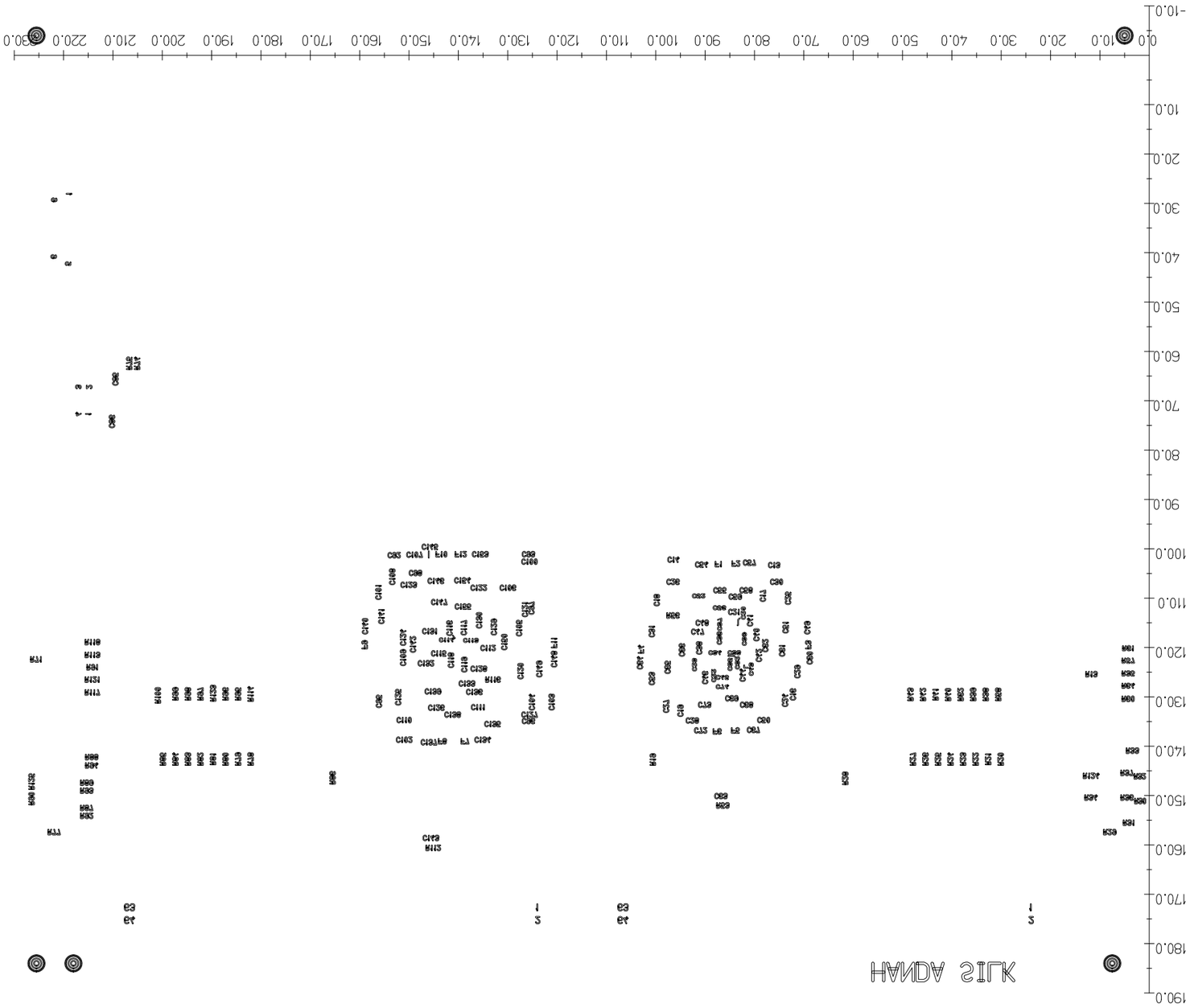

JTAG書き込み用
TCK
TDO
TMS
TDI
XCONFIGB
未実装
CN11
XG4C-1031
ペアで引き出し
TP39
TP40
SW8
SW9
SW10
A6S-8104
B3S-1000
DIPSWB0
DIPSWB1
DIPSWB2
DIPSWB3
DIPSWB4
DIPSWB5
DIPSWB6
DIPSWB7
SWB
PORSELB
PULLUPB
PLLENAB
LEDB0
LEDB1
LEDB2
LEDB3
LEDB4
LEDB5
LEDB6
LEDB7
SML-210MTT86
U10H
EP2S30F672C5N
BANK8
U10G
BANK7/10
U10F
BANK6
U10E
BANK5
U10D
BANK4/9
U10C
BANK3
U10B
BANK2
U10A
BANK1
TDI
TMS
TCK
TRST
nCONFIG
VCCSEL
IO_CS
IO_CLKUSR
IO_nWS
VREFB8N0
VREFB4N0
VREFB3N0
VREFB2N0
VREFB1N0
VREFB8N1
VREFB4N1
VREFB3N1
VREFB2N1
VREFB7N0
VREFB6N0
VREFB5N0
VREFB7N1
VREFB6N1
VREFB5N1
TEMPDIODEp
TEMPDIODEn
TDO
MSEL3
MSEL2
MSEL1
MSEL0
IO_RUnLU
IO_DEV_OE
IO_DEV_CLRn
IO_nCS
IO_CLK5n
IO_CLK5p
IO_CLK4n
IO_CLK4p
IO_CLK14p
IO_CLK14n
IO_CLK15p
IO_CLK15n
IO_PGM2
IO_PGM1
IO_PGM0
IO_ASDO
IO_nCSO
IO_CRC_ERROR
IO_DATA0
IO_DATA1
IO_DATA2
IO_DATA3
IO_DATA4
IO_DATA5
IO_DATA6
IO_DATA7
IO_RDYnBSY
IO_INIT_DONE
nSTATUS
nCE
DCLK
CONF_DONE
GNDガード
OSCX
CLK11p
CLK11n
IO_CLK10p
IO_CLK10n
CLK9n
CLK9p
IO_CLK8n
IO_CLK8p
IO_PLL5_FBn/OUT2n
IO_PLL5_FBp/OUT2p
IO_PLL5_OUT0n
IO_PLL5_OUT0p
IO_PLL5_OUT1n
IO_PLL5_OUT1p
IO_CLK12n
IO_CLK12p
IO_CLK13n
IO_CLK13p
VCC_PLL5_OUT
VCCD_PLL5
VCCA_PLL5
GNDA_PLL5
GNDA_PLL6
VCCA_PLL6
VCCD_PLL6
VCC_PLL6_OUT
IO_CLK7p
IO_CLK7n
IO_CLK6p
IO_CLK6n
IO_PLL6_OUT1p
IO_PLL6_OUT1n
IO_PLL6_OUT0p
IO_PLL6_OUT0n
IO_PLL6_FBp/OUT2p
IO_PLL6_FBn/OUT2n
CLK1p
CLK1n
CLK2p
CLK2n
CLK3p
CLK3n
IO_CLK0p
IO_CLK0n
FPGA_DI15
FPGA_DI14
FPGA_DO14
FPGA_DO15
FPGA_DI13
FPGA_DO13
FPGA_DO11
FPGA_DI11
FPGA_DI12
FPGA_DO12
FPGA_DI10
FPGA_DI9
FPGA_DI8
FPGA_DI7
FPGA_DO9
FPGA_DO10
FPGA_DI6
FPGA_DI5
FPGA_DO2
FPGA_DO5
FPGA_DO6
FPGA_DO8
FPGA_DO7
FPGA_DI4
FPGA_DI3
FPGA_DO0
FPGA_DO3
FPGA_DO1
FPGA_DI1
FPGA_DO4
FPGA_DI2
FPGA_DI0
FPGA_A3
FPGA_A5
FPGA_A6
FPGA_RD
FPGA_A4
FPGA_WR
FPGA_A15
FPGA_A1
FPGA_A7
FPGA_A14
FPGA_A13
FPGA_A2
FPGA_A0
FPGA_A12
FPGA_A11
FPGA_A10
FPGA_A9
FPGA_RSV1
FPGA_RSV0
FPGA_A8
FPGA_RSV2
MEMUB
MEMA0
MEMD15
MEMD14
MEMLB
MEMA18
MEMA9
MEMD13
MEMOE
MEMA1
MEMA8
MEMA15
MEMWR
MEMA16
MEMA10
MEMA7
MEMA2
MEMA14
MEMA11
MEMA13
MEMA17
MEMA3
MEMD12
MEMD8
MEMA5
MEMD9
MEMD10
MEMD11
MEMCS
MEMA12
MEMD0
MEMD1
MEMA4
MEMA6
MEMD2
MEMD3
MEMD4
MEMD5
MEMD6
MEMD7
MEMD30
MEMD28
MEMD29
MEMD31
MEMD24
MEMD25
MEMD26
MEMD27
MEMD23
MEMD22
MEMD21
MEMD20
MEMD16
MEMCS1
MEMD17
MEMD18
MEMD19
USBTXE
USBRXF
USBWR
USBPWREN
USBRD
USBD6
USBD3
USBD7
USBD5
USBD2
USBD1
USBD0
USBD4
RTS
CTS
TX
RX
CN10
A1-64PA-2.54DSA(71)
CN12
TP35
TP36
TP37
TP38
TP43
TP44
TP45
SG-8002DC
24.000M-PCB
089-NV98B
ICソケットを使用
GNDガード
TPペアで引き出し
EEPインシステムプログラム用
MSEL［3..0］は1000か1101
RESETB
CONFIG
200ms遅延
EPCS16SI8N
74HC14
BD45292G
BLM18AG102SN
ELC0607RA-100J1R6-PF
TITLE
暗号処理モジュール
アルテラ版
DRAWING_No.
E3-93994-1
SHEET
4 ／ 4
DATE
DESIGN

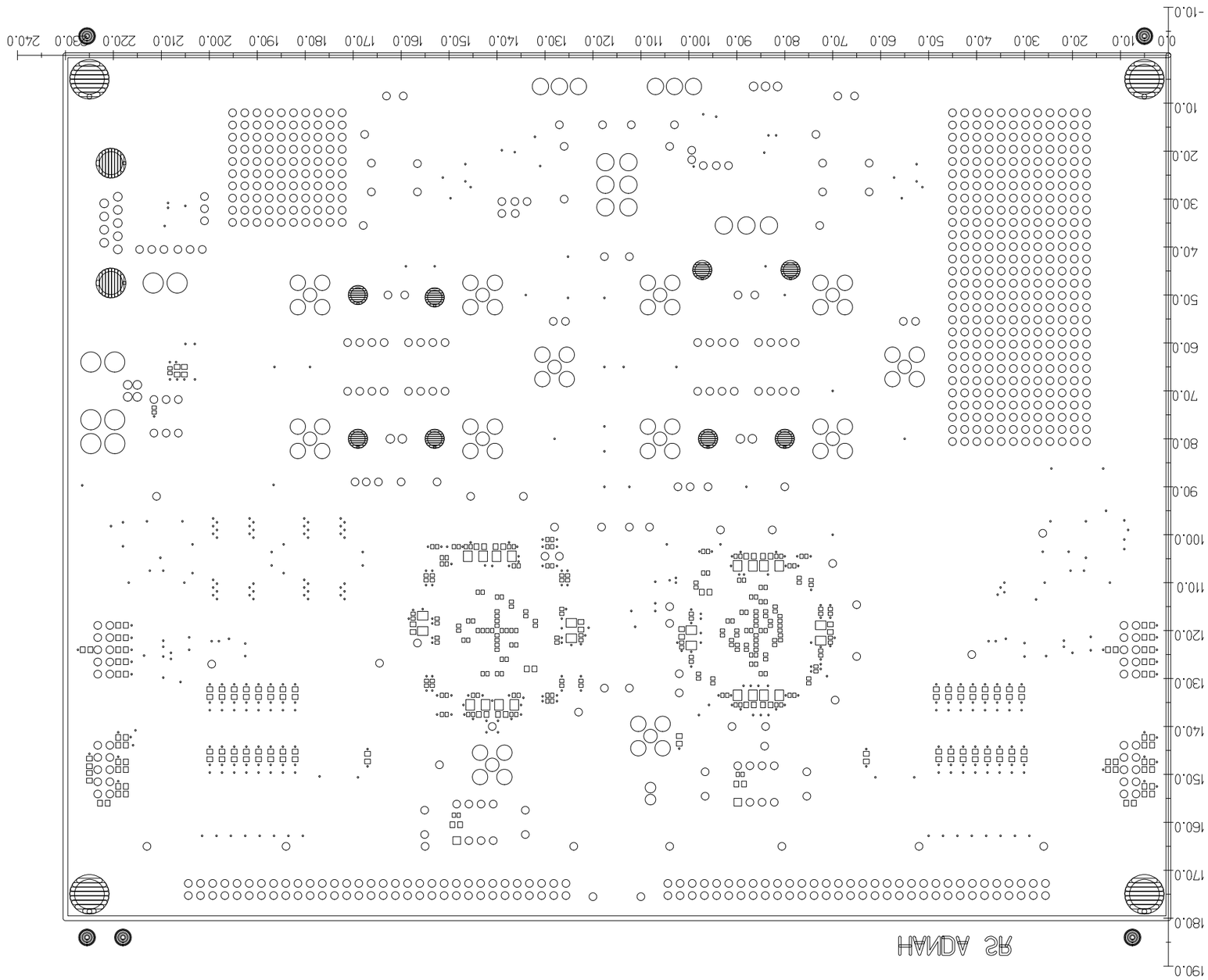
BUHIN SILK

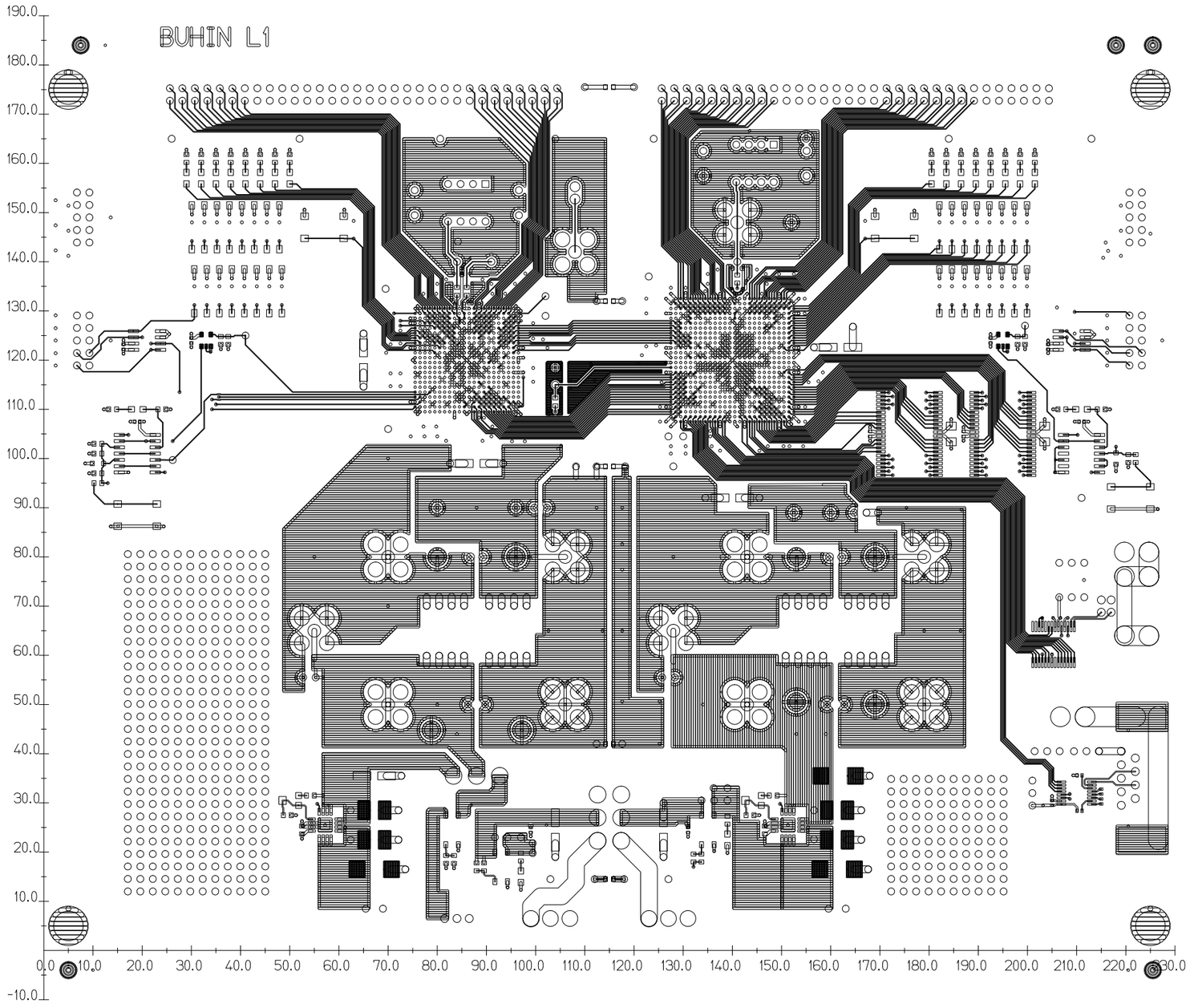
3-93994-1

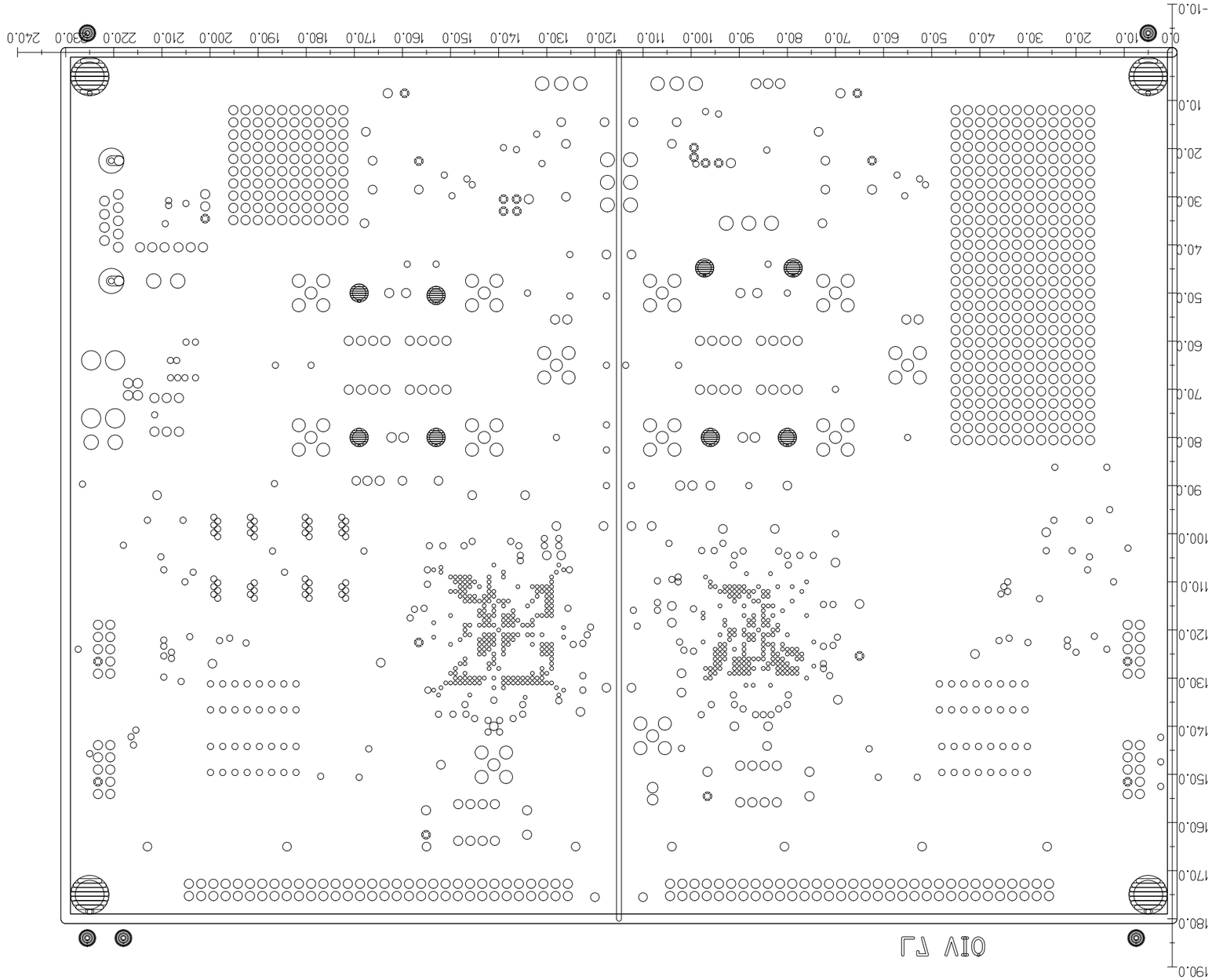
8ch-channel Attack
Standard Evaluation Board
SASEBO-B

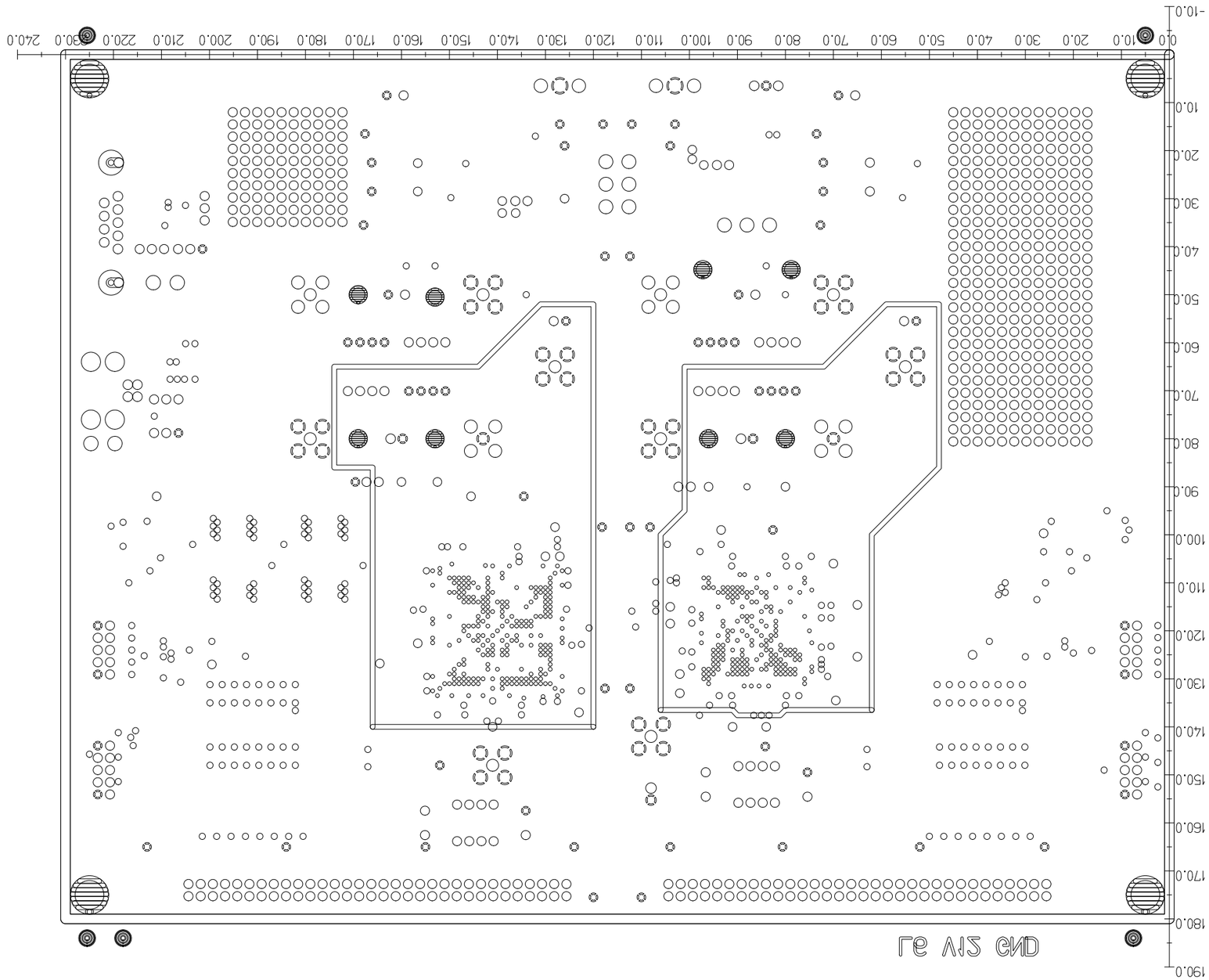

BUHIN SR
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
-10.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
240.0

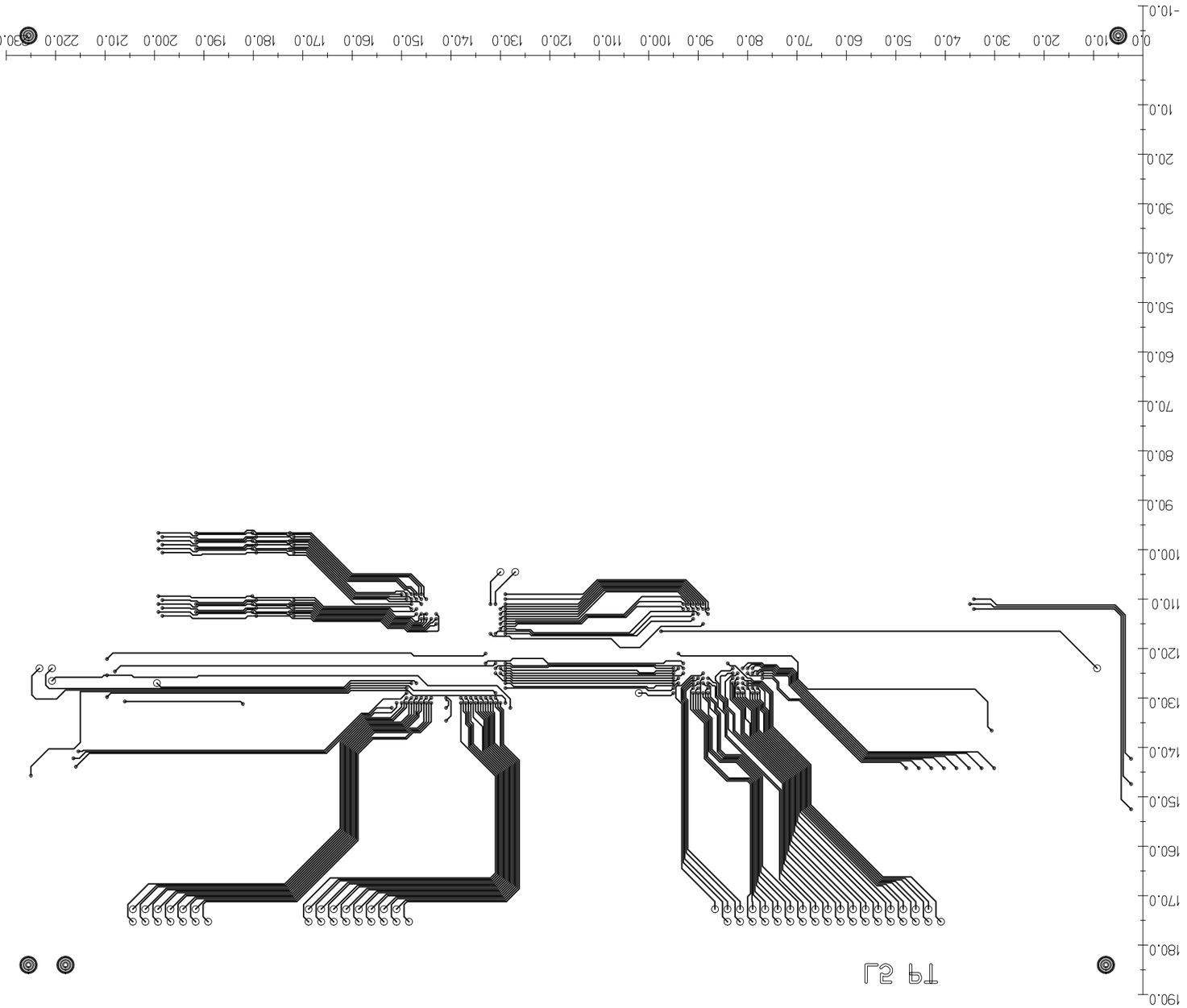

HANDA SILK

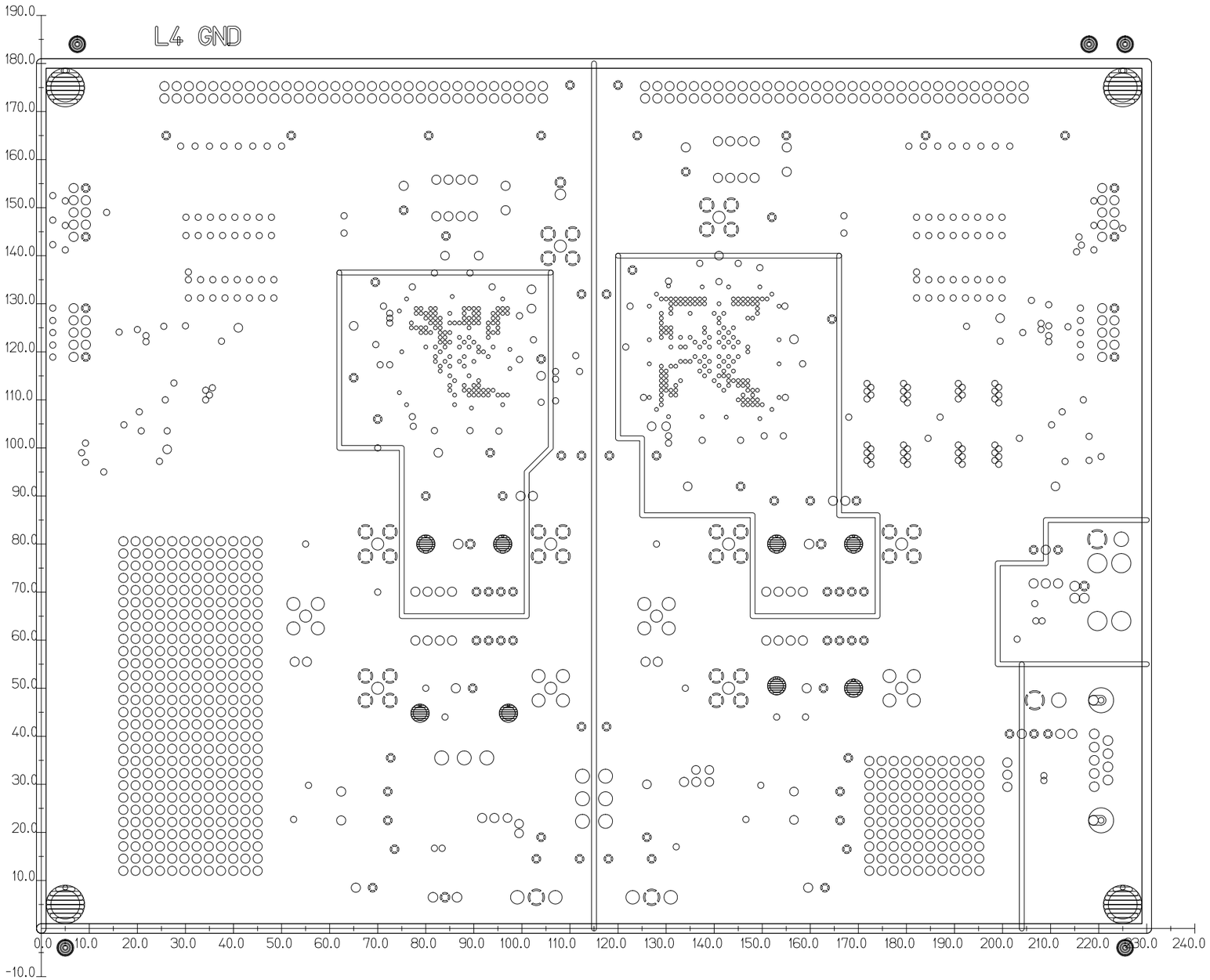

HANDA SR
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
240.0
-10.0

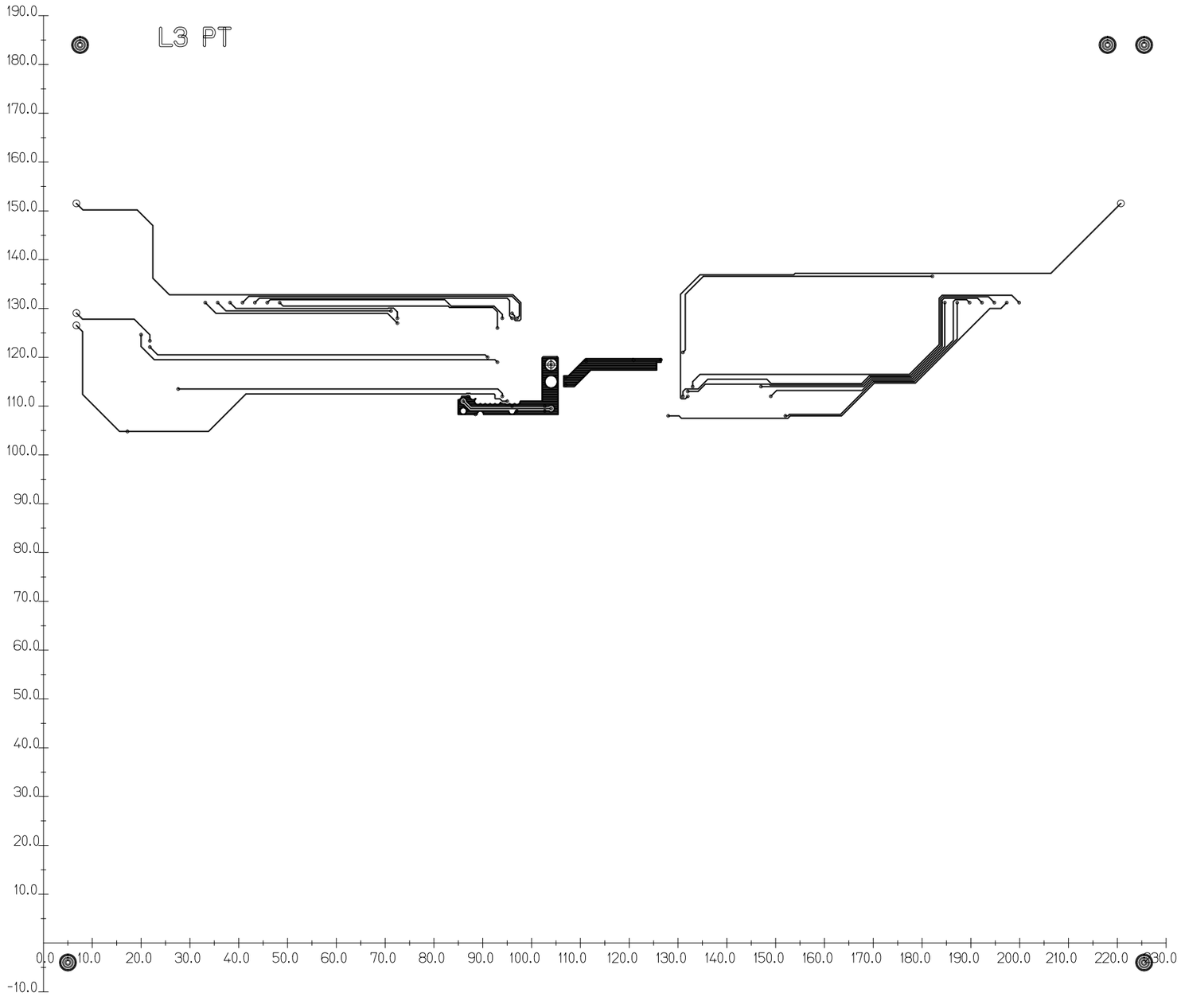

BUHIN L1
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
-10.0
0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0

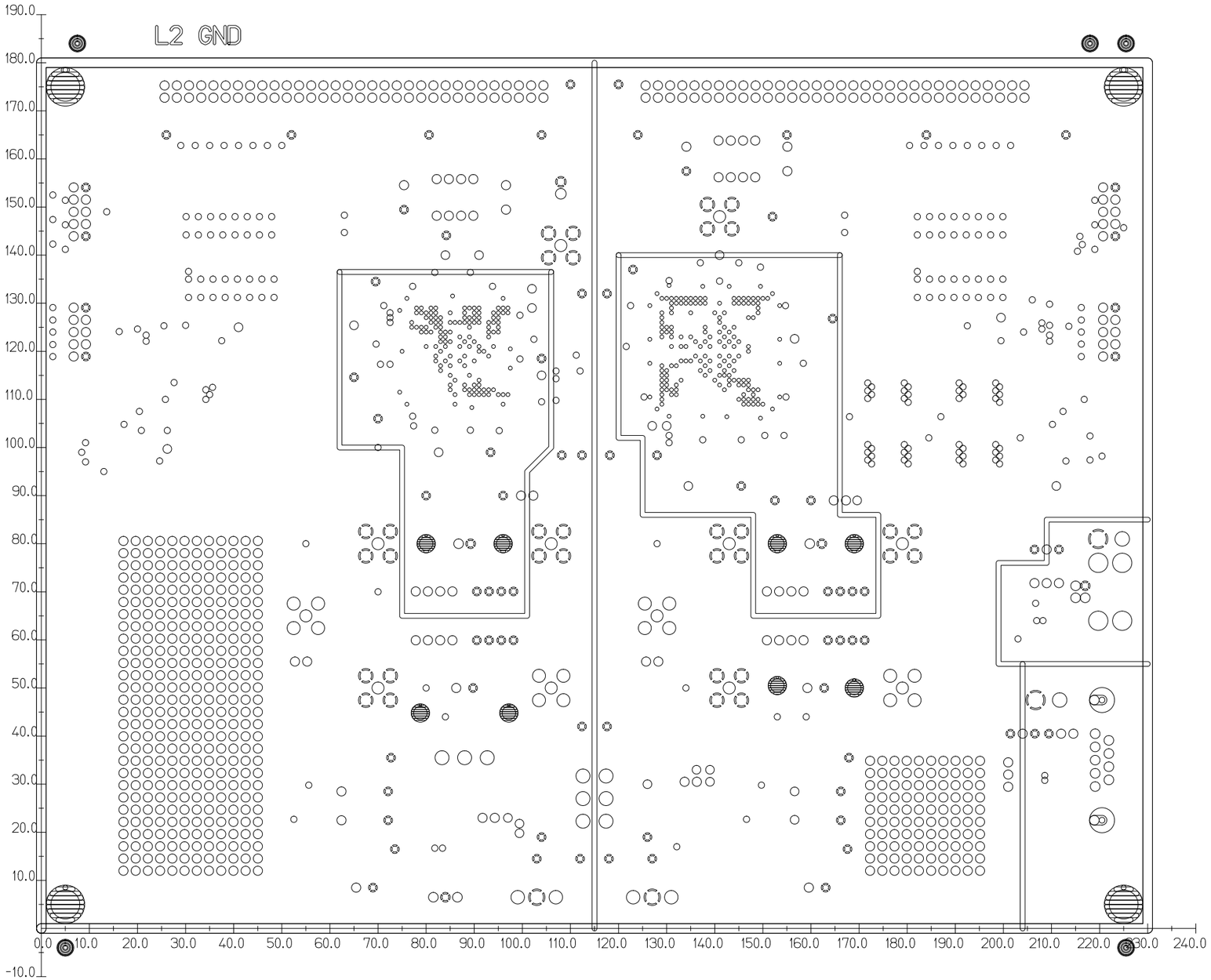

0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
-10.0
240.0
230.0
220.0
210.0
200.0
190.0
180.0
170.0
160.0
150.0
140.0
130.0
120.0
110.0
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
DIV FJ

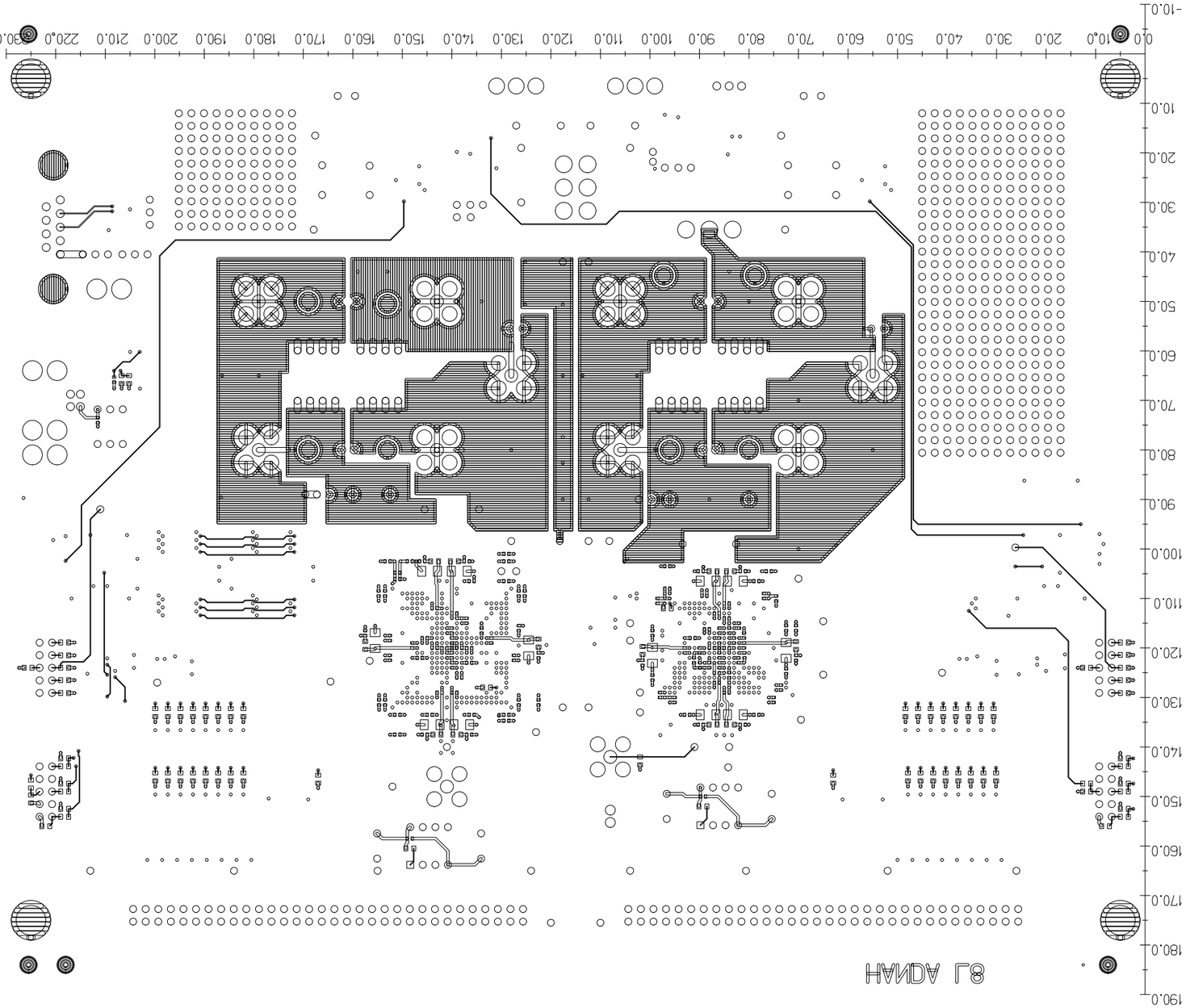

0.0
10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0
100.0
110.0
120.0
130.0
140.0
150.0
160.0
170.0
180.0
190.0
200.0
210.0
220.0
230.0
240.0
-10.0


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
-10.0
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
L2 T4


L4 GND
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


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
230.0


L2 GND
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
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