

サイドチャネル攻撃用標準評価基板
SASEBO-B 仕様書

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

[第1版]

2008年4月1日

(独) 産業技術総合研究所
情報セキュリティ研究センター

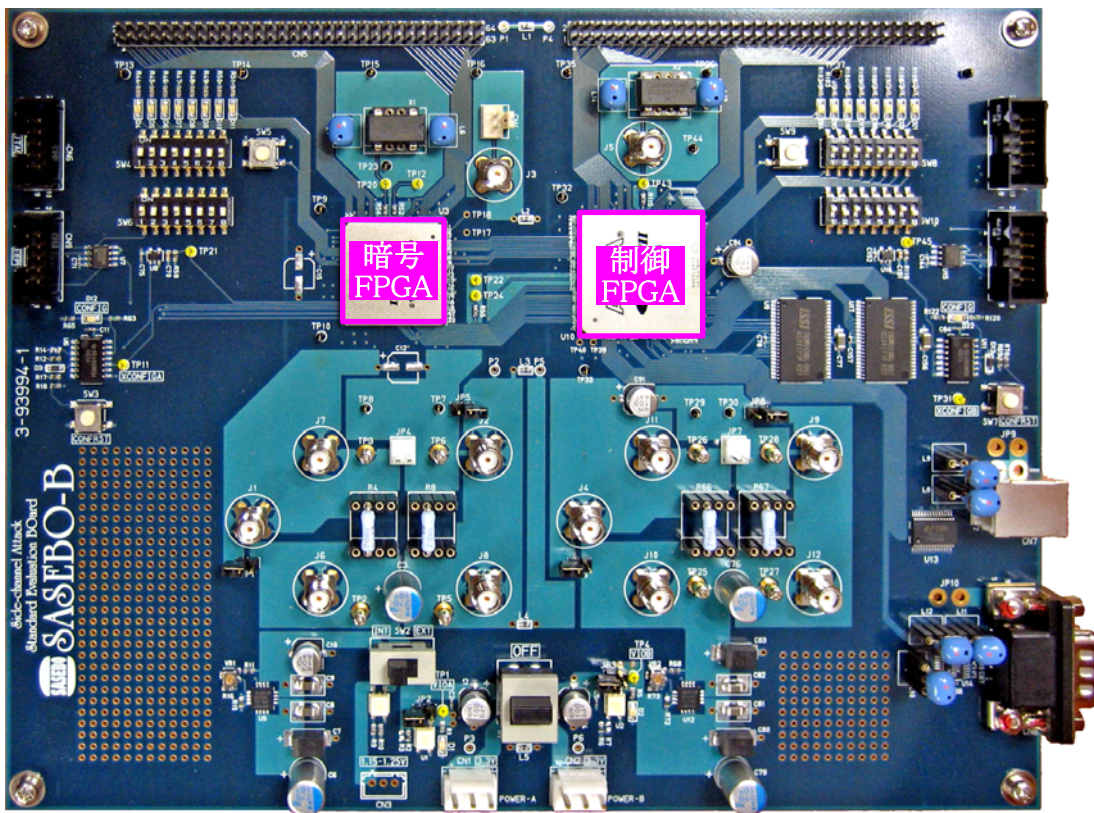
目次

	Page
1. 概要	2
2. 暗号 LSI および制御 FPGA の入出力信号	3
3. ボード設定	11
4. 回路図・基板レイアウト図	15

1. 概要

サイドチャネル攻撃用標準評価 FPGA 基板(以下 SASEBO(Side-channel Attack Standard Evaluation Board)-B と呼ぶ)は、暗号モジュールの物理解析攻撃の研究を目的に開発された、ALTERA 社製 FPGA を搭載する実験用ボードである。図 1 にその概観を、また以下に SASEBO-B の概要を示す。

- 基板サイズ 230 mm×180 mm×1.6mm(板厚), ガラスエポキシ材, 8 層構造。
- ALTERA 社製 Stratix II シリーズの 2 つの FPGA EP2S15F484C5N と EP2S30F672C5N を実装し, 主に前者を暗号回路用, 後者を制御 FPGA として使用する。2 つの FPGA 間は, 入力と出力別々の 16 ビットデータバスと 16 ビットアドレスバスで接続され, 信号(RD, WT, RESET, CLOCK)で制御。
- 最大動作周波数動作 24MHz. 2 つの FPGA に共通のクロック IC を搭載し, 外部クロックによる制御も可能。
- 電源は外部コネクタより直流 3.3V を供給し, 基板上のレギュレータが FPGA 用に 1.2V を生成。また, 暗号回路用 FPGA のコア電源は外部から直接供給も可能。
- FPGA のコア電源ラインおよびグラウンドライン上に抵抗を挿入し, 電力波形測を観測することが可能。
- ボードの制御は外部に接続した PC から, RS232C または USB のシリアル I/F を通して行う。



2. 暗号 FPGA および制御 FPGA の入出力信号

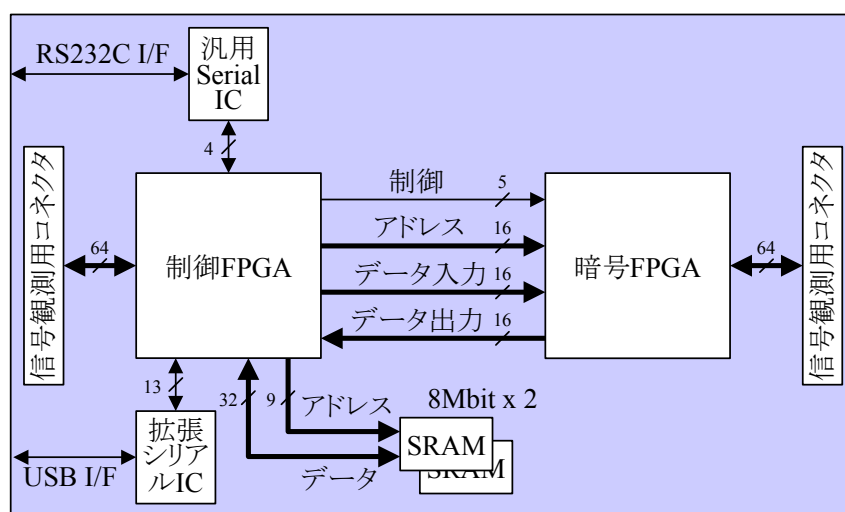


図 2 主要な入出力信号

- 暗号 LSI(コンポーネント U3)用

表 1 基本制御信号

信号名	端子	入出力	用途・接続先
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

表2 制御 FPGA I/F

信号名	端子	入出力	接続先 (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

表3 モニタ信号

信号名	端子	入出力	用途・接続先
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

表4 汎用モニタピン

信号名	端子	入出力	用途・接続先
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

● 制御 FPGA(U10)用信号

表 5 FPGA 設定信号

信号名	端子	入出力	用途・接続先
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
OSCX	A12	OUT	Clock
RESETB	Y20	IN	RESET
CLK	P22,P23	IN	X2

表 6 シリアル I/F

信号名	端子	入出力	用途・接続先
TX	D2	OUT	シリアル I/F
RX	C1	IN	シリアル I/F
CTS	E1	OUT	シリアル I/F
RTS	E2	IN	シリアル I/F

表 7 モニタ信号

信号名	端子	入出力	接続先
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

表 8 暗号回路用 FPGA I/F

信号名	端子	入出力	接続先 (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

表9 USB I/F

信号名	端子	入出力	接続先
USB0	F2	IO	シリアル I/F
USB1	G1	IO	シリアル I/F
USB2	G2	IO	シリアル I/F

USB3	J1	IO	シリアル I/F
USB4	F1	IO	シリアル I/F
USB5	H1	IO	シリアル I/F
USB6	J2	IO	シリアル I/F
USB7	H2	IO	シリアル I/F
USBTXE	M2	IN	シリアル I/F
USBRXF	M1	IN	シリアル I/F
USBRD	K1	OUT	シリアル I/F
USBWR	L2	OUT	シリアル I/F
USBWREN	K2	IN	シリアル I/F

表 10 Memory I/F

信号名	端子	入出力	接続先
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. ボード設定

● 電源回路

図3に電源回路ブロックの構成を、表4に電源コネクタの設定を示す。また図4.4は電源投入時の各電源ラインの立ち上がり方を示している。

直流 $3.3V \pm 0.16V$ を CN1(暗号 LSI 側)および CN2(制御 FPGA)から供給する。電源投入時にはメインパワースイッチ SW1 を OFF にしておくこと。暗号 LSI のコア電源を外部から供給する場合は SW2 を EXT 側設定し、CN3 から直流 $1.2V \pm 0.05V$ を供給する。コア電源を外部供給しない場合は SW2 を INT 側に設定する。なお、SW2 の切り替えは電源投入前に行っておくこと。電源が入ると暗号 FPGA 側と制御 FPGA 側の LED D1 と D2 がそれぞれ点灯する。

表4 電源コネクタの設定

コネクタ		CN1	CN2	CN3
用途		暗号 FPGA レギュレータ電源	制御 FPGA 用 レギュレータ電源	暗号 FPGA 用 外部入力電源
SW2		INT	INT	EXT
ピン	1	$3.3V \pm 0.16V$	$3.3V \pm 0.16V$	$1.2V \pm 0.05V$
	2	0V	0V	0V
	3	未接続	未接続	未接続

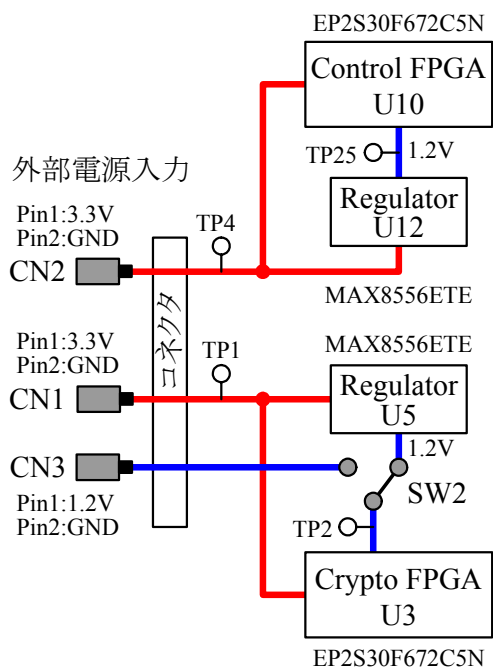
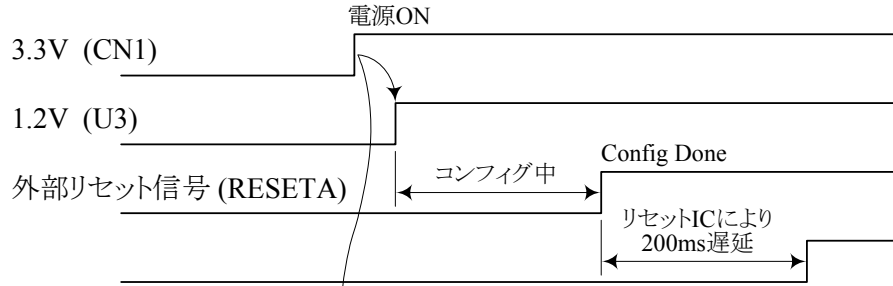
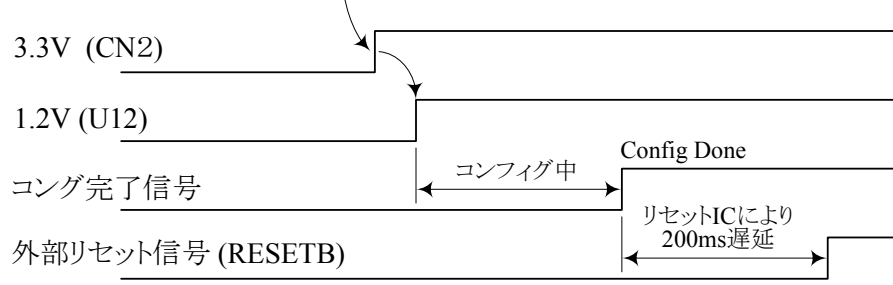


図3 電源回路ブロックの構成

● VIOA側 (暗号FPGA側)



● VIOB側 (制御FPGA側)



↓ ダウンロードおよびコンフィグスイッチ
 押下時はここからスタート

図 4 電源シーケンス

● ジャンパ設定

表 12 ジャンパ設定

用途	ピン番号	設定	説明
電源供給タイミングの選択	JP2	Short	暗号 FPGA 側の電源をレギュレータから直接供給
		Open	MOS リレー経由で供給
	JP3	Short	制御 FPGA 側の電源をレギュレータから直接供給
		Open	MOS リレー経由で供給
電力波形測定設定	JP1	Short	暗号 FPGA の I/O 電源側シャント抵抗 R4 をバイパス
		Open	暗号 FPGA の I/O 電源側シャント抵抗 R4 を使用
	JP4	Short	暗号 FPGA のコア電圧をGNDにショート
		Open	暗号 FPGA のコア電圧を 1.2V に有効化
	JP5	Short	暗号 FPGA の I/O-GND 側シャント抵抗 R8 をバイパス
		Open	暗号 FPGA の I/O-GND 側シャント抵抗 R8 を使用
	JP6	Short	制御 FPGA のコア電源側シャント抵抗 R66 をバイパス
		Open	制御 FPGA のコア電源側シャント抵抗 R66 を使用
	JP7	Short	暗号 FPGA のコア-GND 側シャント抵抗 R67 をバイパス
		Open	暗号 FPGA のコア-GND 側シャント抵抗 R67 を使用
JP9	Short	制御 FPGA のコア電圧を GND にショート	
	Open	制御 FPGA のコア電圧を 1.2V に有効化	

● コンフィギュレーション

図 5 に JTAG チェーン の接続関係を示す. 暗号 FPGA(U3)と制御 FPGA(U10)それぞれ独立に FPGA 書き込み用コネクタ CN6 と CN11, Flash ROM U7 と U15 書き込み用 CN9 と CN12 を有している. 表 13 に JTAG コネクタのピンアサインを, 表 14 にコンフィギュレーションモードの指定を行う DIP スイッチ(暗号 FPGA 用は SW6, 制御 FPGA 用は SW10)の設定を示す. それぞれの FPGA において, PC または PROM からのコンフィギュレーションが成功すると, ダイオード D12 または D22 が点灯する. また, プッシュスイッチ SW3 または SW7 の押下によって, それぞれの PROM からの再コンフィギュレーションが行われる.

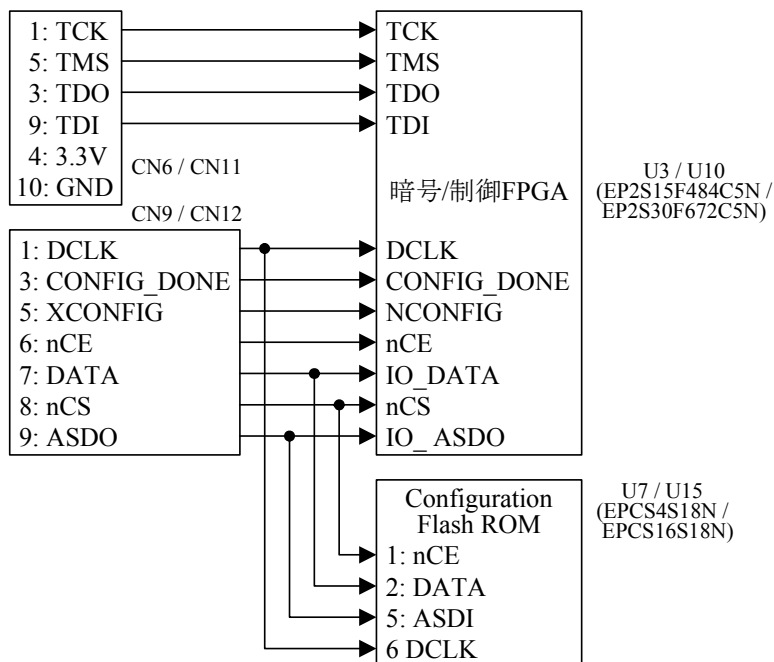


図 5 JTAG チェーン

表 13 JTAG コネクタのピンアサイン

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

表 14 モード切替 DIP スイッチ SW6/SW10 の AS(Active Serial)Mode 設定

Dip1			ON
Dip2	PORSEL	パワーオンリセット時間設定 OFF:12ms ON:100ms	OFF
Dip3	PULLUP	コンフィグ中プルアップ指定 OFF:プルアップ無効 ON:有効	OFF
Dip4	PLLENA	PLL 指定 OFF:PLL 無効 ON:有効	ON
Dip5	MSEL4		OFF
Dip6	MSEL3		OFF
Dip7	MSEL1		ON
Dip8	MSEL0		OFF

● クロック系統

図6にSASEBO-Bのクロック系統図を示す。暗号FPGAと制御FPGAは、それぞれ独立した24MHzのクロック源X1とX2を有している。また、各クロックは、SMAコネクタJ3、J5を通して、それぞれ独立に外部から供給することも可能である。

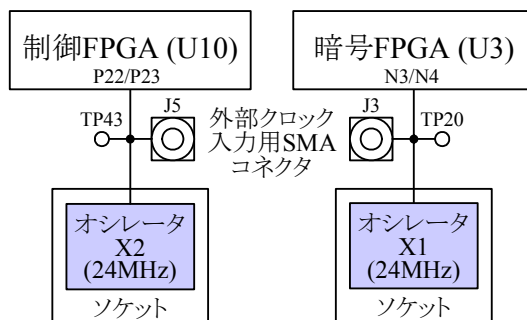


図6 クロック系統図

● インタフェース部

SASEBO-Bは外部PCとの通信用に、RS232CとUSBの2種類のシリアル・インタフェースを有している。表15と16に、それぞれRS232CとUSBのコネクタからFPGAまでの信号線の接続関係を示す。なおRS232Cによる通信は9pinストレートケーブルを使用する。USBインタフェースICにはFTDI(Future Technology Device International Ltd.)社のFT245RLを使用しており、Windows用のデバイスドライバは下記のURLからダウンロードすることができる。

<http://www.ftdichip.com/Products/FT245R.htm>

表15 RS232Cインタフェースの信号線

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

表16 USBインタフェースの信号線

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

4. 回路図・基板レイアウト図

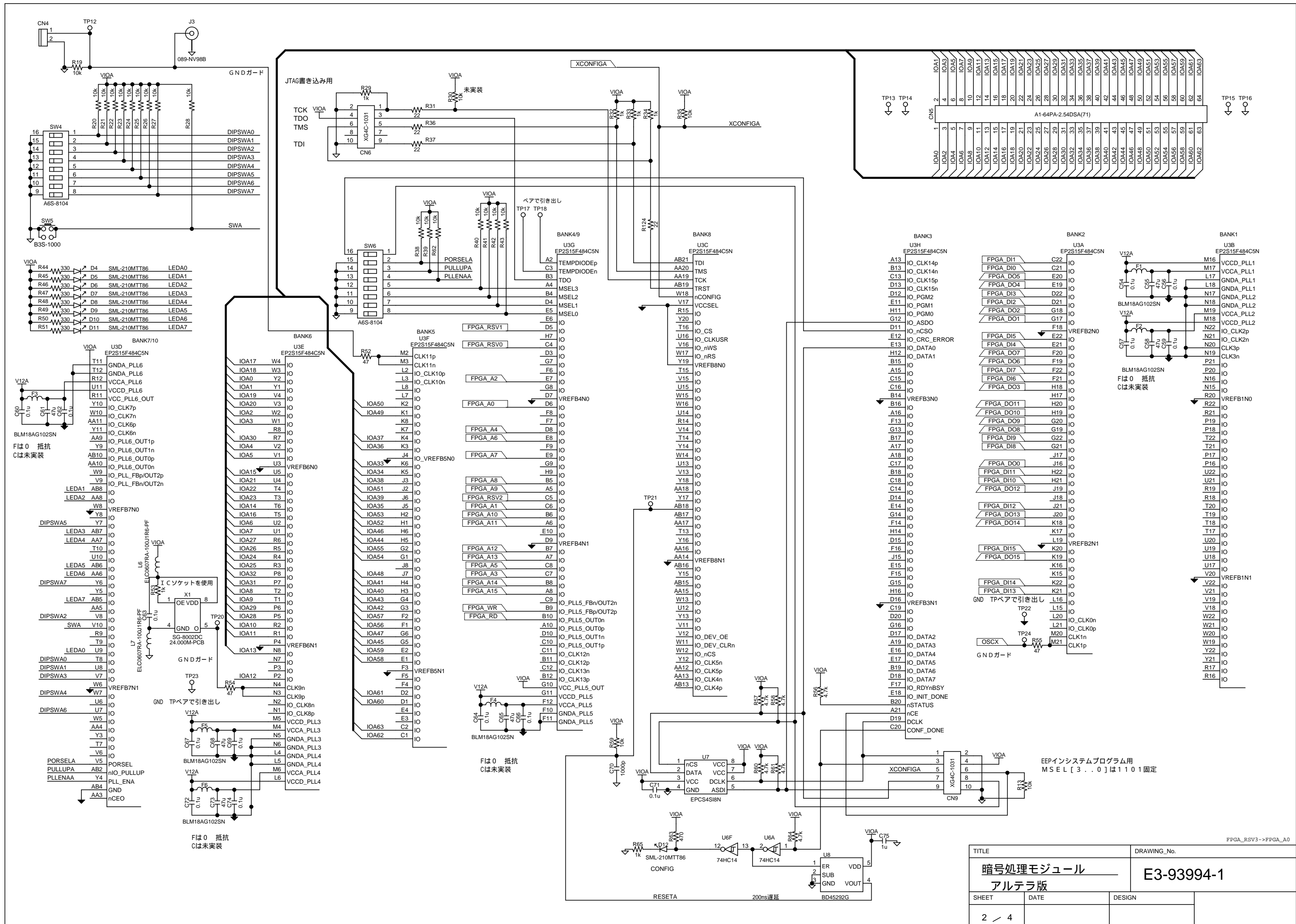
表 17 に SASEBO-B の部品表を, ページ 18~33 に下記の通り回路図と基板レイアウト図を示す.

● 暗号 FPGA 周辺回路	
FPGA 接続部, 電源部, コンフィギュレーション部 18 ページ
FPGA接続部 19 ページ
● 制御 FPGA 周辺回路	
FPGA 接続部, 電源部, コンフィギュレーション部 20 ページ
FPGA接続部 21 ページ
● 部品図	
部品面シルク図 22 ページ
部品面レジスト図 23 ページ
半田面シルク図 24 ページ
半田面レジスト図 25 ページ
● マスク図	
L1(部品面パターン) 26 ページ
L2(内層パターン) 27 ページ
L3(内層パターン) 28 ページ
L4(内層パターン) 29 ページ
L5(内層パターン) 30 ページ
L6(内層パターン) 31 ページ
L7(内層パターン) 32 ページ
L8(半田面パターン) 33 ページ

表 17 部品表

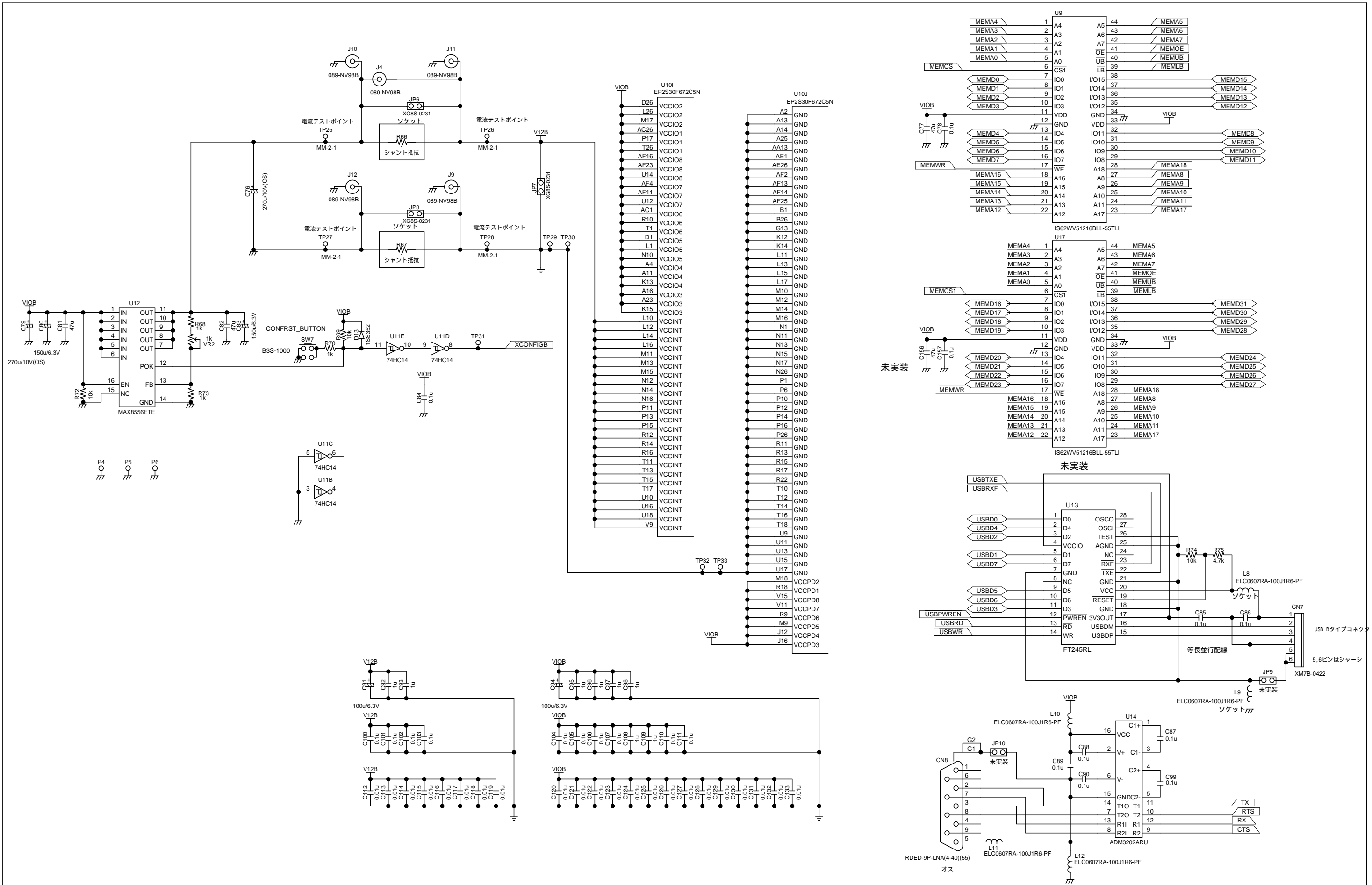
セット名	SASEBO-B			
基板番号	E3-93994-1			
品名	型名	メーカー	数量	部品番号
積層セラ C (チップ)	GRM155F11H103ZA57E	ムラタ	22	C32,C33,C34,C35,C36,C37,C38,C39,C40, C41,C42,C43,C44,C45,C46,C47,C48,C49, C50,C51,C52,C53,C112,C113,C114,C115, C116,C117,C118,C119,C120,C121,C122, C123,C124,C125,C126,C127,C128,C129, C130,C131,C132,C133
積層セラ C (チップ)	GRM155F11E104ZA01D	ムラタ	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
積層セラ C (チップ)	GRM188B11H102KA01D	ムラタ	2	C70,C151
積層セラ C (チップ)	GRM155F10J105ZE01D	ムラタ	10	C13,C14,C16,C17,C18,C19,C75,C92,C93, C95,C96,C97,C98,C108,C109,C152,
積層セラ C (チップ)	JMK316BJ476ML-T	太陽誘電	11	C8,C9,C55,C58,C61,C65,C68,C73,C77, C81,C82,C135,C138,C141,C146,C149, C154,C156
アルミ電解 (チップ)	EMV-6R3ADA101MF55G	日ケミ	5	C1,C4,C10,C12,C15,C91,C94
OS コンデン サ	EEFUE0J151	松下	3	C7,C80,C83
OS コンデン サ	APSA100ELL271MHB5S	日ケミ	4	C3,C6,C76,C79
チップ抵抗	RK73Z1JTTD 0Ω	KOA	6	F1,F2,F3,F4,F5,F6
チップ抵抗	RR0816-101-D	進工業	2	R2,R3,R6,R7,R14
チップ抵抗	RR0816-103-D	進工業	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
チップ抵抗	RR0816-102-D	進工業	20	R11,R13,R16,R18,R29,R32,R33,R34,R53, R65,,R68,R70,R71,R73,R77,R88,R89,R90, R112,R122
チップ抵抗	RR0816-201-D	進工業	2	R9,R10
チップ抵抗	RR0816-220-D	進工業	8	R31,R36,R37,R92,R93,R94,R124,R125
チップ抵抗	RR0816-331-D	進工業	18	R1,R5,R44,R45,R46,R47,R48,R49,R50, R51,R102,R103,R104,R105,R106,R107, R108,R109
チップ抵抗	RR0816-472-D	進工業	7	R56,R57,R58,R60,R61,R64,R75
チップ抵抗	RR0816-470-D	進工業	4	R52,R54,R55,R115
チップ抵抗	RR0816-471-D	進工業	2	R63,R120
ダイオード (チップ)	ISS352(-TPH3)	東芝	2	D3,D13

DIP スイッチ	A6S-8104-H	オムロン	4	SW4,SW6,SW8,SW10
タクトスイッチ	B3S-1000	オムロン	4	SW3,SW5,SW7,SW9
スライドスイッチ	CS-12AAP1	日開	1	SW2
スライドスイッチ	CS-22AAP1	日開	1	SW1
FPGA	EP2S15F484C5N	アルテラ	1	U3
FPGA	EP2S30F672C5N	アルテラ	1	U10
EEPROM	EPCS16SI8N	アルテラ	1	U15
EEPROM	EPCS4SI8N	アルテラ	1	U7
CMOS	SN74HC14NSE4	TI	2	U6,U11
SRAM	IS62WV51216BLL-55TLI	ISSI	1	U9
USB IC	FT245RL	FDI	1	U13
通信 IC	ADM3202ARUZ	アナデバ	1	U14
リセット IC	BD45292G	ローム	2	U8,U16
レギュレータ IC	MAX8556ETE	マキシム	2	U5,U12
インダクタ	ELC0607RA-100J1R6-PF	TDK	9	L6,L7,L8,L9,L10,L11,L12,L13,L14
フィルタ	BLM18AG102SN	ムラタ	5	L1,L2,L3,L4,L5,F7,F8,F9,F10,F11,F12,
LED	SML-210MTT86	ローム	20	D1,D2,D4,D5,D6,D7,D8,D9,D10,D11,D12, D14,D15,D16,D17,D18,D19,D20,D21,D22
コネクタ	DF1-2P-2.5DSA	ヒロセ	1	CN4
コネクタ	XG4C-1031	オムロン	4	CN6,CN9,CN11,CN12
コネクタ	A1-64PA-2.54DSA(71)	ヒロセ	2	CN5,CN10
コネクタ	B3P-VH(LF)(SN)	ヒロセ	2	CN1,CN2
コネクタ	B3B-XH-A(LF)(SN)	日圧	1	CN3
USB コネクタ	XM7B-0442	オムロン	1	CN7
D サブコネクタ	XM2C-0912-111	オムロン	1	CN8
MOS リレー	G3VM-61GR1	オムロン	3	U1,U2,U4
SG-8002DC	24.000M-PCB	エプソントヨコム	2	X1,X2
SMA レセプタクル	T124 426 000N	タキテック	12	J1,J2,J3,J4,J5,J6,J7,J8,J9,J10,J11,J12
テストポイント	LC-3-G(黒)	MAC8	18	TP7,TP8,TP9,TP10,TP13,TP14,TP15,TP16, TP23,TP29,TP30,TP32,TP33,TP35,TP36, TP37,TP38,TP44
電流テストポイント	MM-2-1	MAC8	8	TP2,TP3,TP5,TP6,TP25,TP26,TP27,TP28
トリマ	ST-32EA 1K Ω (13)	コパル	2	VR1,VR2
シャント抵抗	ERX1SJ1R0	松下	4	R4,R8,R66,R67
ジャンパポスト	XG8S-0231	オムロン	6	JP1,JP2,JP3,JP5,JP6,JP8
コネクタ	B2P-SHF-1AA(LF)(SN)	日圧	2	JP4,JP7
短絡ソケット	XJ8A-0211	オムロン	8	
IC ソケット	R110-91-308	プレジディップ	2	

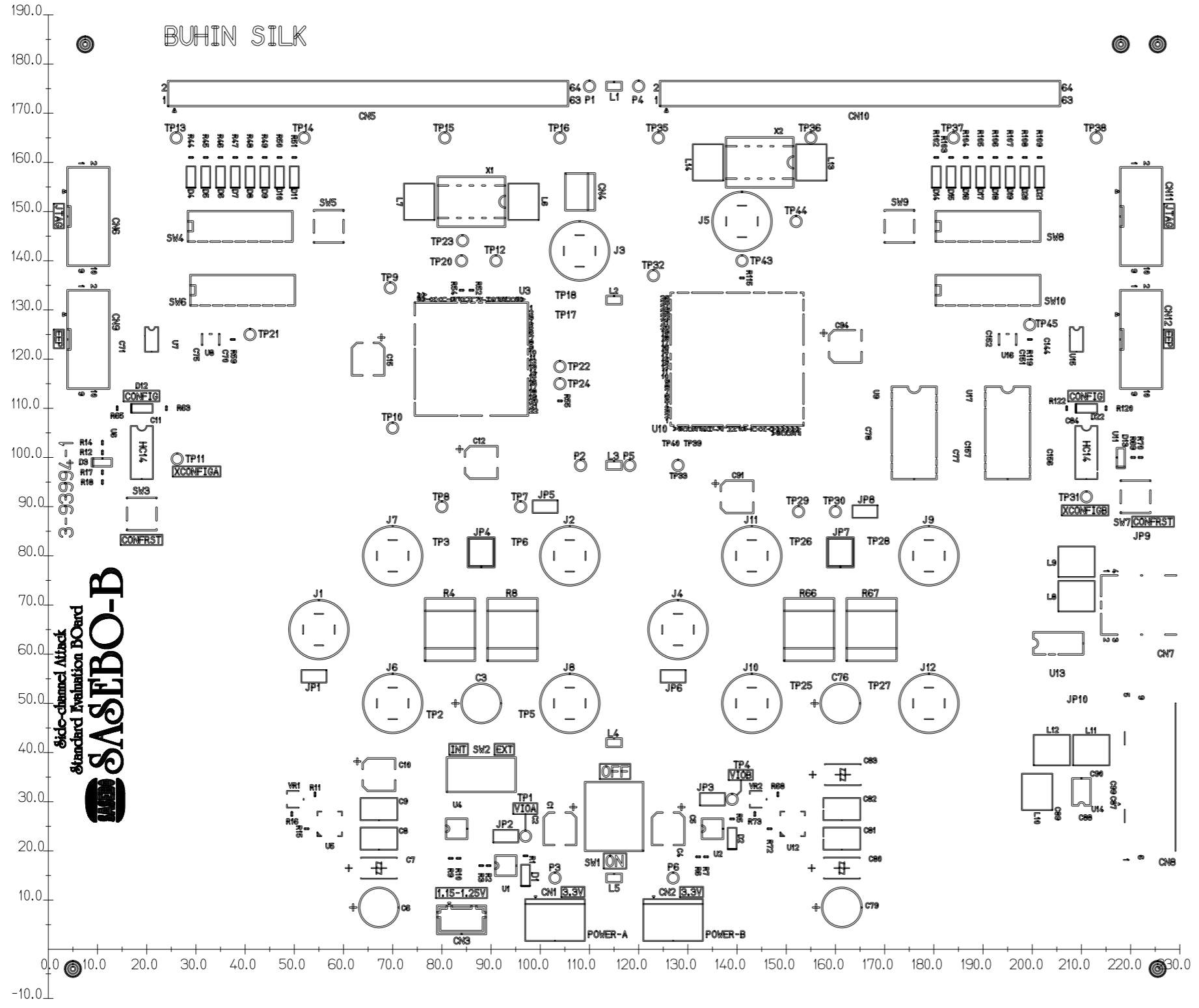


TITLE		DRAWING.No.	
暗号処理モジュール		E3-93994-1	
アルテラ版			
SHEET	DATE	DESIGN	
2 / 4			

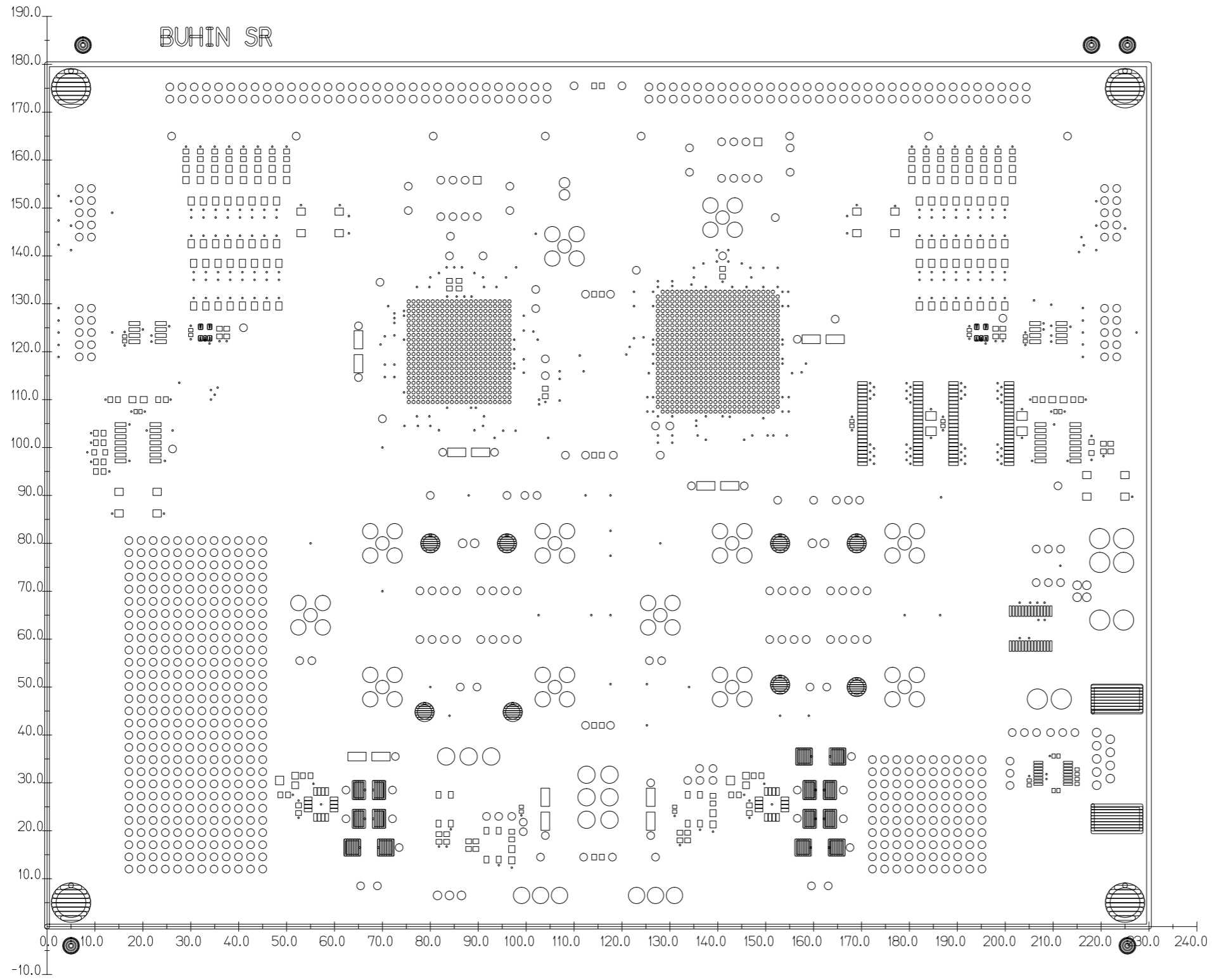
FPGA_RSV3->FPGA_A0

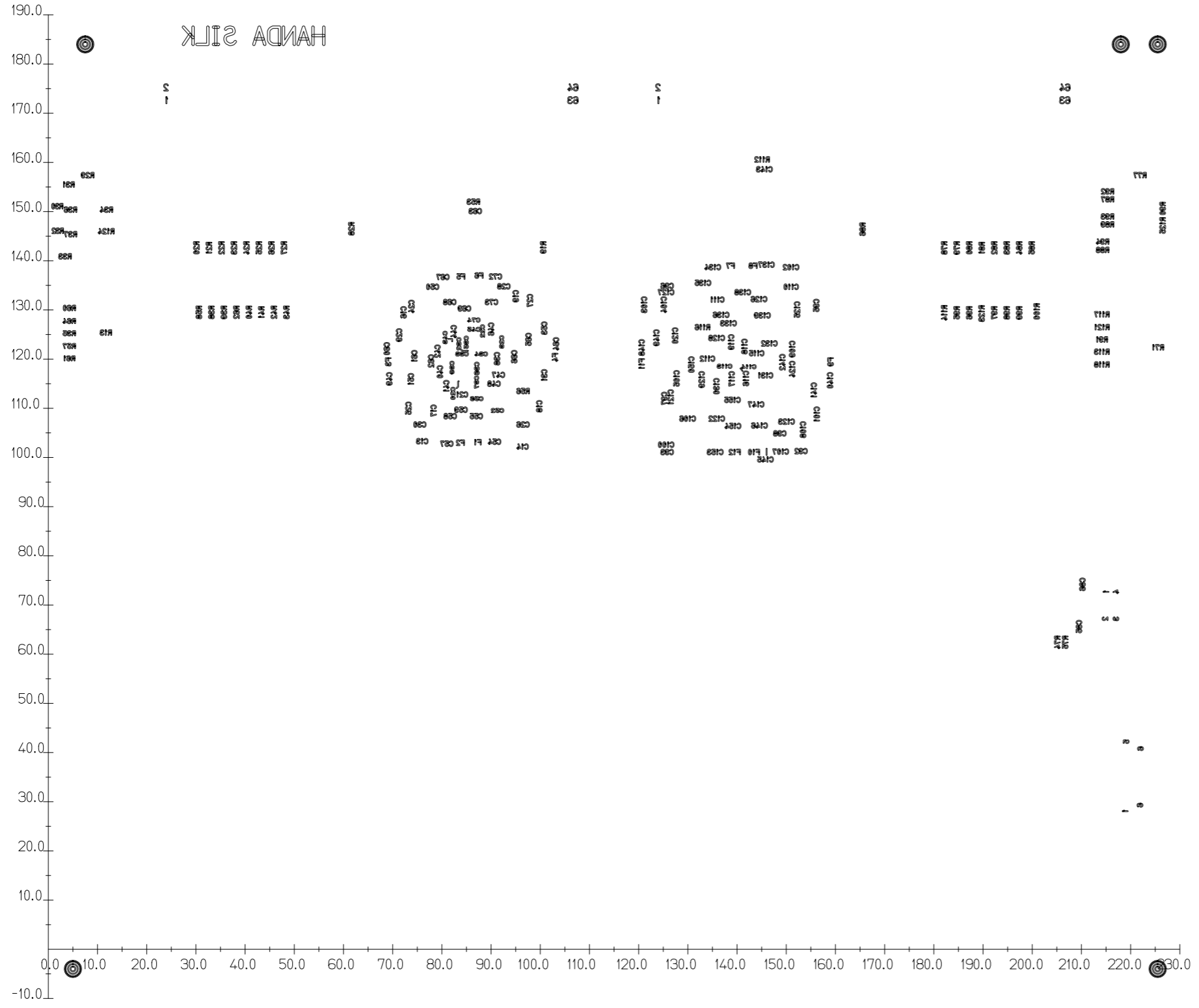


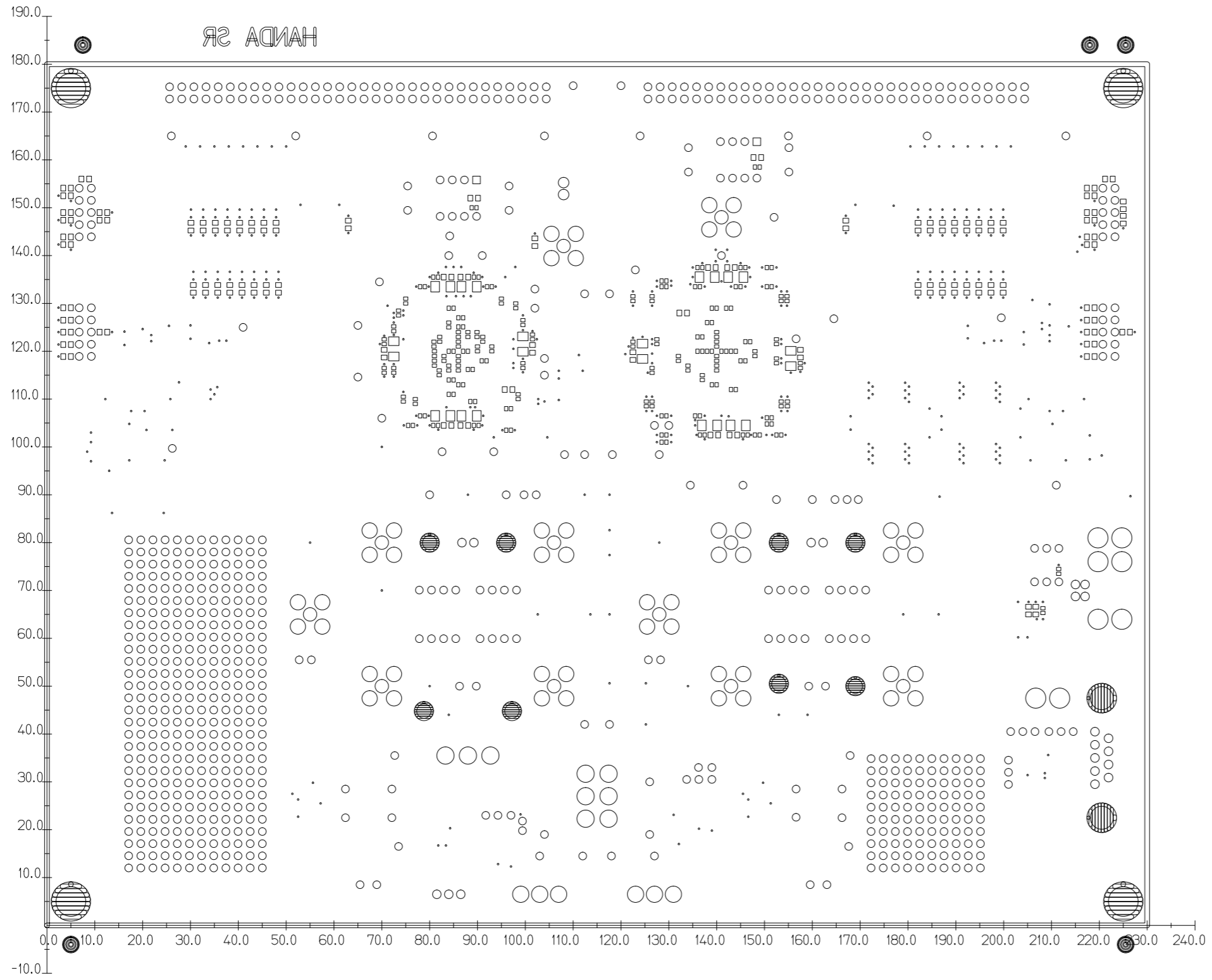
TITLE		DRAWING_No.	
暗号処理モジュール		E3-93994-1	
アルテラ版			
SHEET	DATE	DESIGN	
3 / 4			

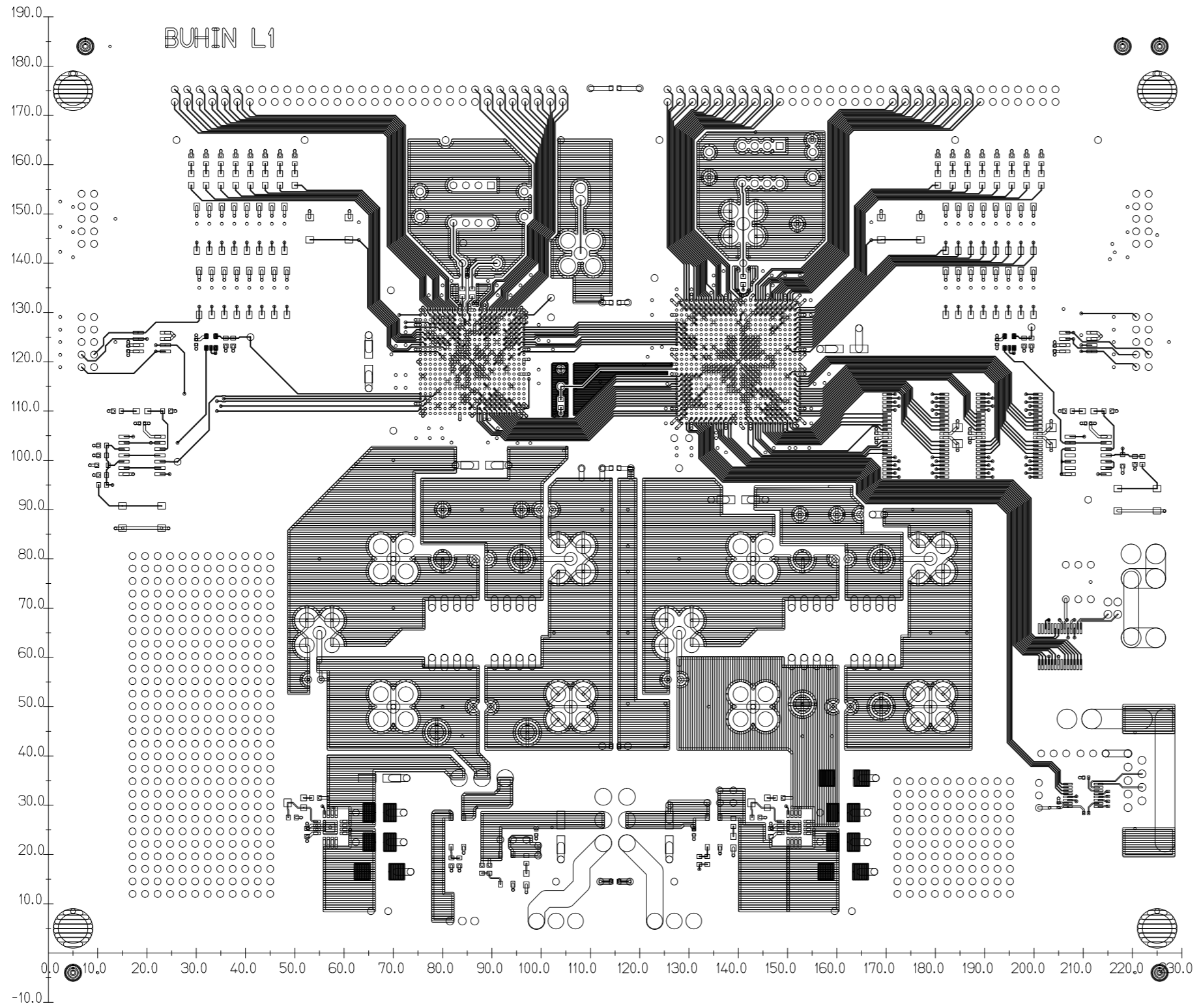


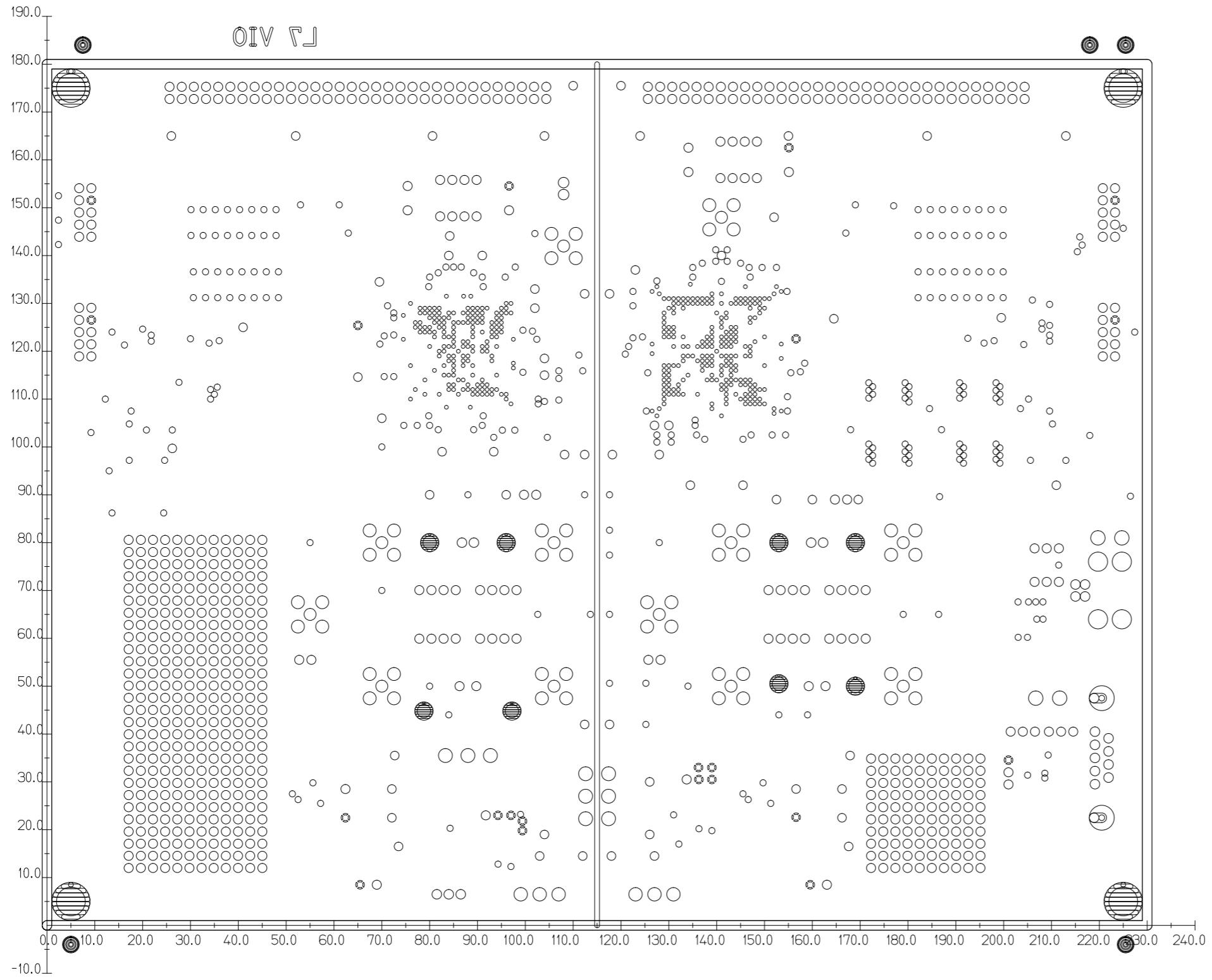
3-93994-1
 8-channel Allback
 Standard Evaluation Board
ASASBO-B

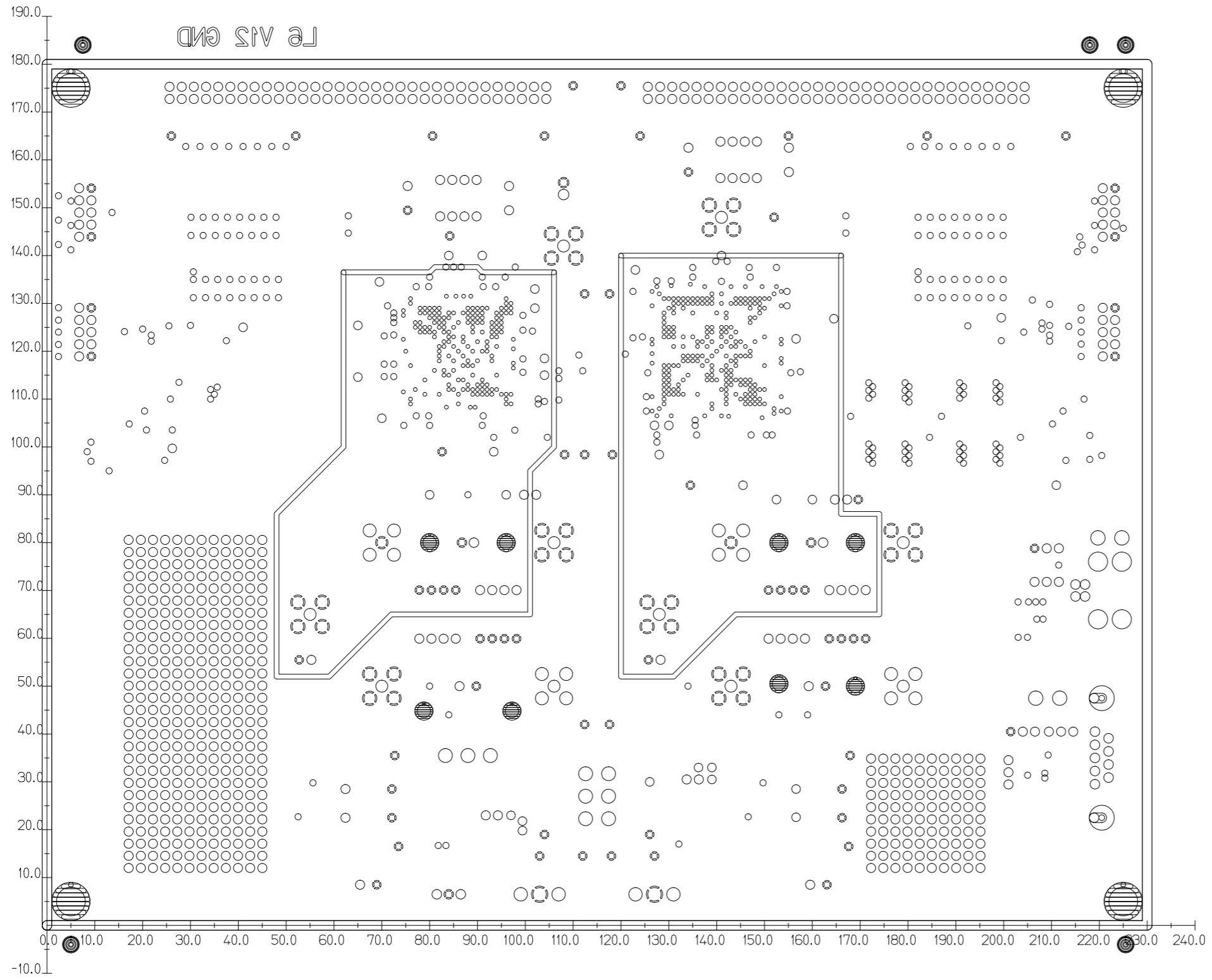


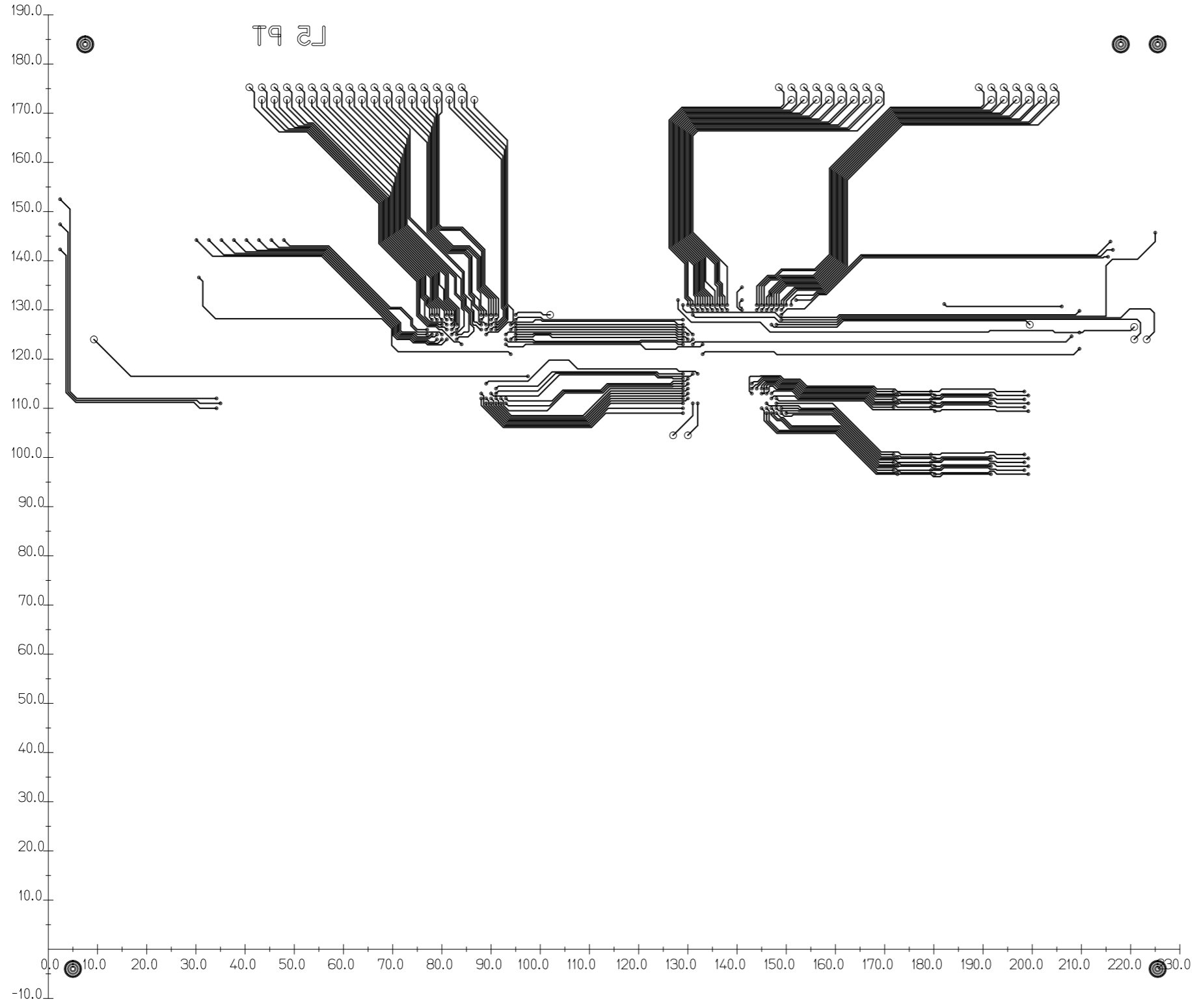


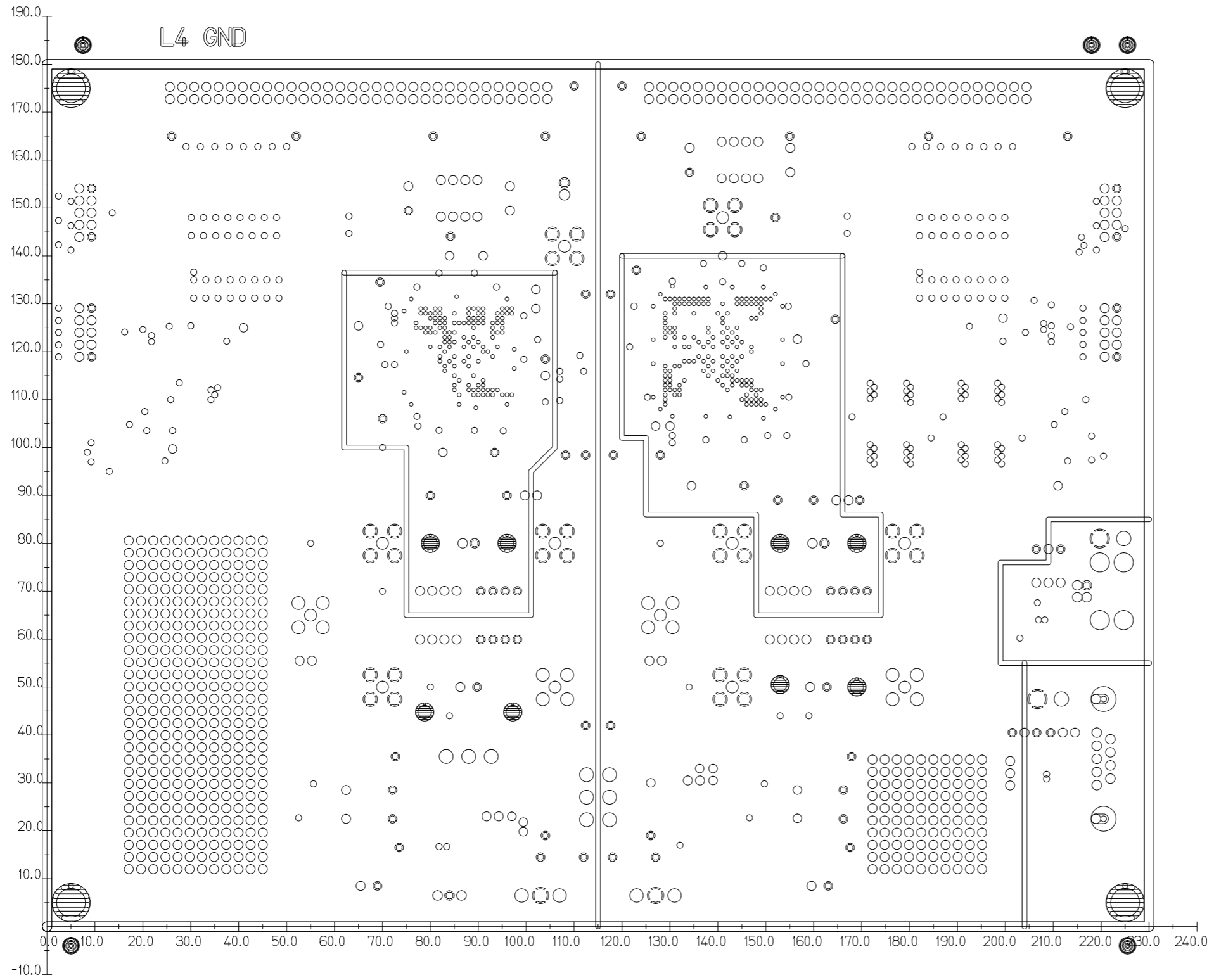


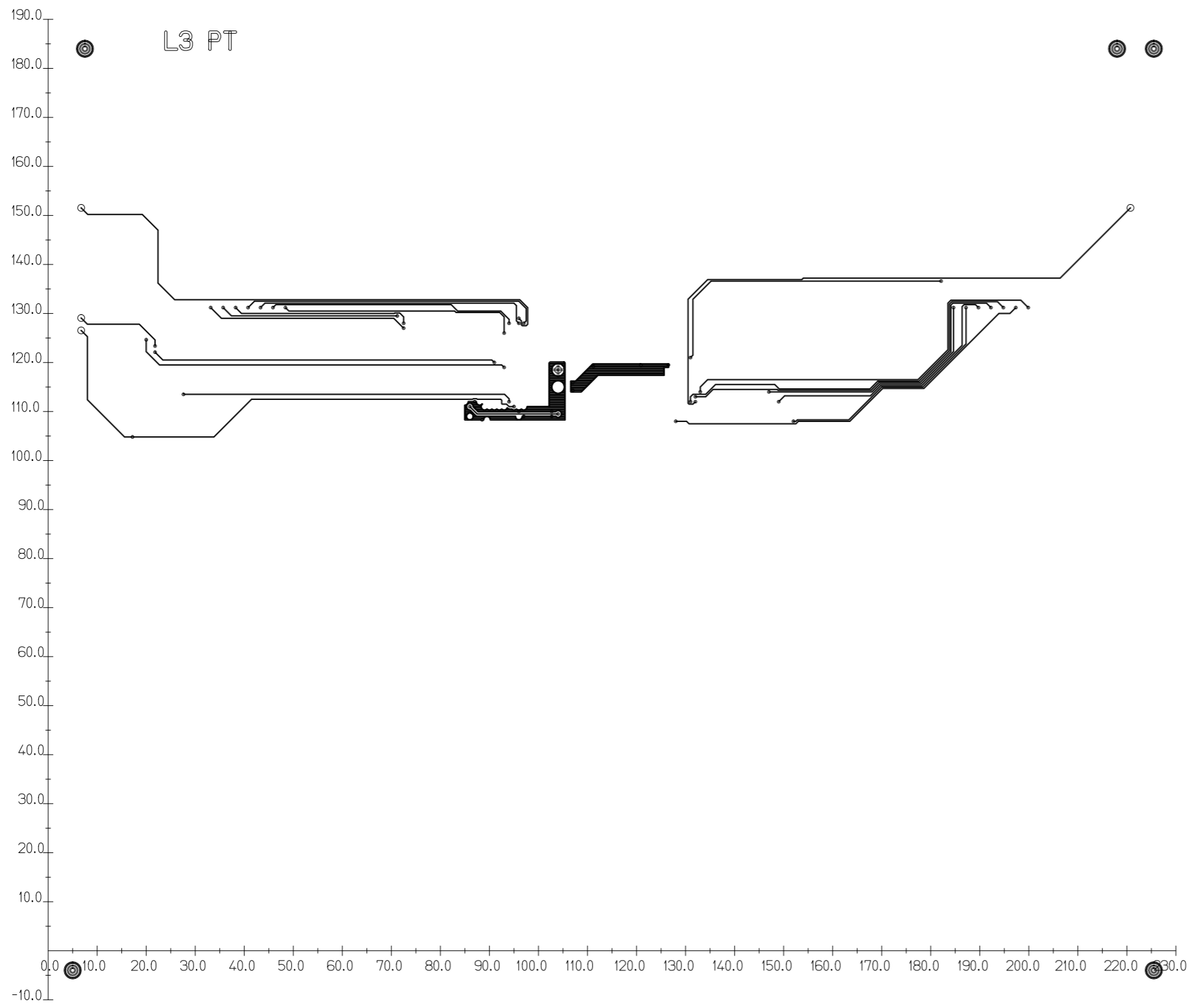


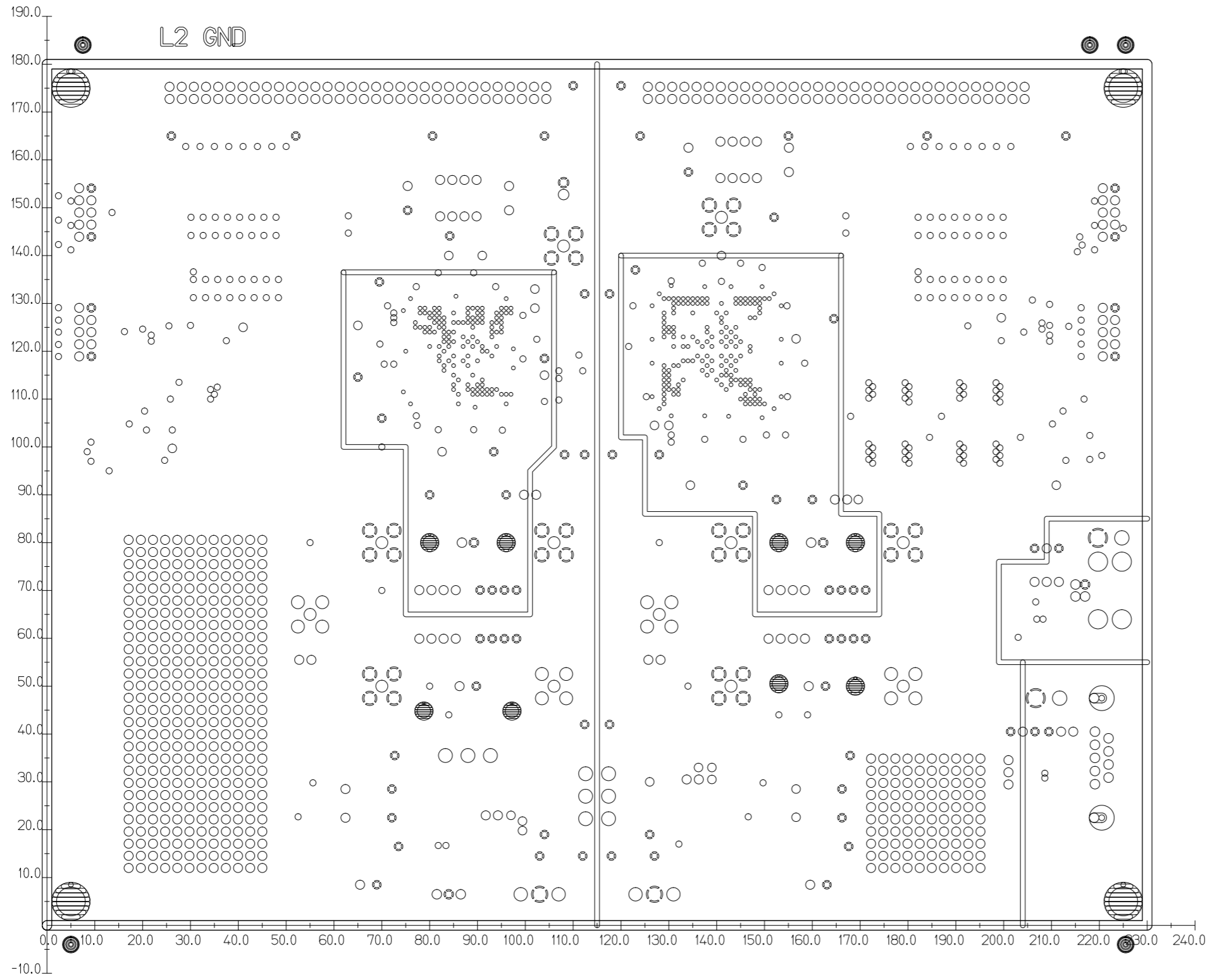


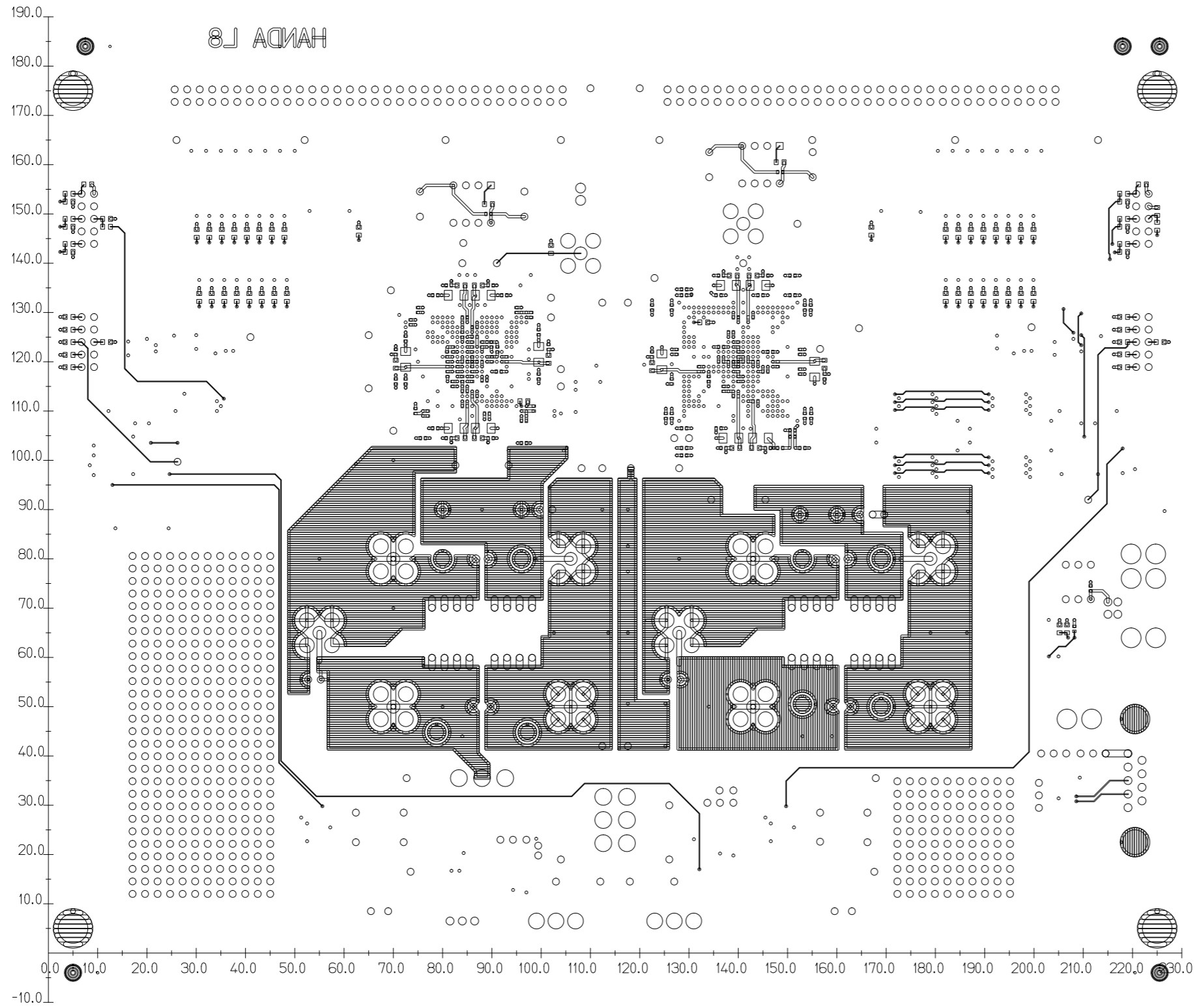












- ※1 本ボードの著作権は(独)産業技術総合研究所に、本仕様書の著作権は経済産業省に帰属します。
- ※2 本ボードおよび本仕様書の全部または一部を、著作権者に無断で複写、複製することはできません。
- ※3 ボードおよび本仕様書は、個人として利用するほかは、著作権者に無断で使用することはできません。
- ※4 本ボードの仕様は、将来予告なく変更することがあります。

FPGA はザイリンクス社の登録商標です。

その他、記載されている社名・製品名は各社の商標および登録商標です。

【問合せ先】

(独) 業技術総合研究所 情報セキュリティ研究センター

〒101-002

東京都千代田区外神田 1-18-13 秋葉原ダイビル 11 階 1102 号室

TEL : 03-5298-4722

FAX : 03-5298-4522