APPLICATION NOTE

TDA8006AH/C113 application for Mondex cards in BskyB STB

AN/98006

Philips Semiconductors

PHILIPS

Abstract

This application note describes the software implemented in TDA8006AH mask 13 and presents the layout recommendations for the BskyB set top boxes manufacturers.

APPLICATION NOTE

TDA8006AH/C113 application for Mondex cards in BskyB set top boxes

Author(s) :
Jean Pierre BOURNAS / Michel BRUN

Application Laboratory - Paris
France

Keywords
TDA8006
Smart card interface
Mondex™
ISO7816-3&4
E.M.V.

Date : February 1998

TABLE OF CONTENTS

1. Introduction

TDA8006AH is a smart card coupler providing all the analog electrical interface signals to the smart card and is able to manage asynchronous cards due to its specific ISO7816 UART and to its embedded 80C52 microcontroller core.
This masked version (mask 13) has been developped to be used in a in a BskyB set top box in order to handle the second slot for the banking card.
The software embedded in this device is able to support any ISO7816 asynchronous smart card (T=0 or T=1 protocol) and handles completely the communication layer between the card and the host system.
A specific protocol called « ALPAR » has been defined on the serial interface between TDA8006 and the host system; it uses the APDUs frame types to convey the card commands.

This mask version (TDA8006AH/C113) has been approved by Mondex™ International as a component handling the hardware electrical interface and the transport layer for Mondex™ cards.

2. Serial interface

2.1. Physical lines

The serial link between the TDA8006 and the host controller is made by using the 2 lines Rx and Tx ; Rx is used to receive data from the system controller and Tx is used to transmit data to the system controller.

No flow control or supplementaty lines are used . A security feature has been implemented on the TDA8006 receive procedure in order to avoid any blocking of the serial interface. This will be explained on chapter 5.10.

2.2. Data link layer

Serial data format

1 start bit

8 data bits
1 stop bit, no parity

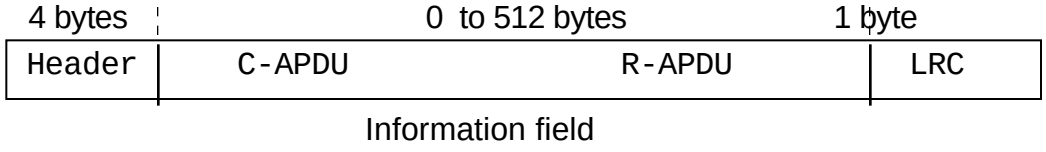
Baud rate 38400 bauds (P10 in open circuit ; default configuration)
9600 Bauds (P10 connected to GND)

Data is exchanged between the system controller and TDA8006 in blocks, each made up of binary characters on one byte:

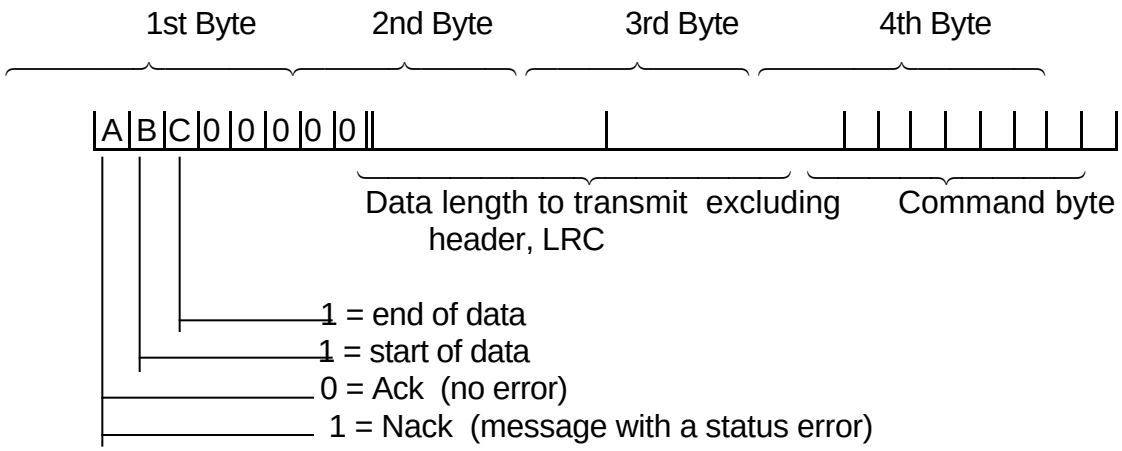
4 header characters
0 to 512* data characters (C-APDU or R-APDU)
1 LRC character

* : EMV specifies 256 bytes.

Frame structure:



The 4 header bytes includes:



LRC byte:

The LRC (longitudinal redundancy check) byte is such that the exclusive-oring of all bytes including LRC is null.

2.3. Dialog structure

The System controller is the master for the transmission ; each command from the master is followed by an answer from TDA8006 including the same command byte as the input command. The only commands which are outgoing only commands from TDA8006 are the commands related to a card insertion or extraction or a time out command on Rx line.

2.3.1. Successful command

System to TDA8006

60	XX	XX	YY	nnnnnnnnnnnnnnnnnnnn	ZZ
ACK	length		code	data (C-APDU)	LRC

TDA8006 to System

60	UU	UU	YY	mmmmmmmmmmmmmm	TT
ACK	length		code	data (R-APDU)	LRC

The same command byte YY is returned in the answer from TDA8006.

2.3.2. Unsuccessful command

System to TDA8006

60	XX	XX	YY	nnnnnnnnnnnnnnnnnnnn	ZZ
ACK	length		code	data (C-APDU)	LRC

TDA8006 to System

E0	UU	UU	YY	SS	TT
NACK	length		code	STATUS	LRC

The status is giving the error code information (see error list).

2.3.3. Card removal

TDA8006 to System

60	00 01	A0	00	ZZ
ACK	length	code	data	LRC

2.3.4. Card insertion

TDA8006 to System

60	00 01	A0	01	ZZ
ACK	length	ode	data	LRC

2.3.5. Answer with an acknowledge (power_down, negoce, set_clock_card)

System to TDA8006

60	00 00	4D	ZZ
ACK	length	code	LRC

TDA8006 to System

60	00 00	4D	ZZ
ACK	length	code	LRC

In the case where the answer is an acknowledge of the command the TDA8006 sends back a frame with the same content of the command.

3. Command bytes

The following command bytes are available:

Command:	code	Answer from reader
send_num_mask	0AH	1 parameter giving the mask number
power_up_3V	6DH	ATR from card + status byte or error message
power_up_5V	6EH	ATR from card + status byte or error message
power_down	4DH	Acknowledge or error message
card command (APDU)	00H	card command (APDU) or error message
negoce (PTS)	10H	Acknowledge or error message
set_clock_card	11H	Acknowledge or error message
set _divider	0B H	Acknowledge or error message

Outgoing commands (only):

	code	parameter
card_take_off	A0 H	00 H
card insertion	A0 H	01 H

These commands are sent as soon as a card is inserted or extracted without any command coming from the system. These commands are using the same operating code but the extra parameter gives the additionnal information.

time_out	FF$_H$	Time out problem on (TDA8006)Rx line

This command is used in order to warn the host controller that the last communication has broken down (time out problem) so that the Rx line of TDA8006 does not remain blocked.

4. Error list

The error list gives the status code idendification and a brief signification of the status error code.

Status code:	meaning:
80 $_H$	Card mute (after power on)
81 $_H$	Time out (waiting time exceeded)
82 $_H$	3 parity errors on TS
83 $_H$	3 parity errors in reception
84 $_H$	3 parity errors in transmission
85 $_H$	ATR too long
86 $_H$	Bad FiDi
87 $_H$	card clock frequency not accepted (after a set_clock_card command)
40 $_H$	card deactivated
C0 $_H$	card absent
C1 $_H$	I/O line locked at low level (a deactivation is processed)
C2 $_H$	Protocol is neither T=0 nor T=1
C3 $_H$	Checksum error
C4 $_H$	TS is neither 3B nor 3F
C5 $_H$	Bad Fi Di

C6 H	ATR not supported (more than 32 interface characters [i>8])
C7 H	VPP is not supported
C8 H	Parameter error in function Power_up
C9 H	Card removed
CA H	class error, card still active
CB H	class error, card deactivated

30 H	Non negociable mode (TA2 is present)
31 H	Protocol is neither T=0 nor T=1 (negoce command)
32 H	T=1 is not accepted (negoce command)
33 H	PTS answer is different from PTS request
34 H	error on TCK (negoce command)
A0 H	Procedure byte error
20 H	wrong APDU
21 H	Too short APDU
22 H	Card mute now (during T=1 exchange)
24 H	Bad NAD
25 H	Bad LRC
26 H	Resynchronised
27 H	Chain aborted
28 H	Bad PCB
29 H	Overflow from card (512 bytes max)
55 H	Unknown command

5. Commands description

5.1. Send_num_mask

This command is used to identify the software version which is masked in TDA8006 ROM.
For example the software approved by Mondex™ will be coded as :
13 release 1.3 (14 ASCII characters)

5.2. Power_up_3V

This commands allows to activate the card at a VCC of 3V. All the signals going to the card will be referenced to this VCC=3V.
An activation sequence is processed following the ISO7816-3 normalisation (VCC is rising, I/O is enabled, CLK is started and RST is processed). If the card answers

to this command, the answer will content all the ATR parameters plus a specific status byte; these parameters are memorized in TDA8006 and will be taken into account during all the card session (till the card is deactivated or till a warm reset is processed). The status byte will give some warning or error message if the ATR of the card is not fully ISO7816-3 compliant or if some parameters of the ATR are not supported by TDA8006. If the ATR is accepted without any problem, the status byte is 00H.
The stucture of the answer is the following:

System to TDA8006

60	XX	XX	6E	nnnnnnnnnnnnnnnnnnn	SS	ZZ
ACK	length		code	ATR parameters	Status Byte	LRC

The status byte can be either 00H if the ATR is fully accepted or can take one of the error status codes (such as 86H or a non ISO FiDi couple proposed in the ATR) in order to warn the host processor, which will take the decision to continue the session with the card or to deactivate it.

If power_up_5V command is given when a class B only card (T=15 specified in the ATR) is present, the card will be automatically deactivated and an status error message will be sent to the application.
Every card that does not specify a specific card class (according to ISO7816-3 Dec 96) will be considered as a 5V only card (class A).

If the card is in specific mode, TDA8006 will process the next command directly using the new interface parameters of this specific mode. If the card proposes a different Fi/Di in the ATR than the default value (Fi/Di=372), it is up to the application to make a PTS command by using the negoce command. If the card proposes 2 different protocols in its ATR, it is up to the application to make a PTS command by using the negoce command.
If the card does not answer to the reset, a status giving an error code is returned to the application.
This command can be used to generate a warm reset if the card is already activated.

5.3. Power up 5V

This commands allows to activate the card at a VCC of 5V. All the signals going to the card will be referenced to this VCC=5V.
see power_up_3V for the other characteristics.

5.4. Power down

This command is used to deactivate the card whatever it has been activated for 3V or 5V operation. A deactivation sequence is processed following the ISO 7816-3 normalization in about 100µs.

5.5. Card command (APDU)

This command is used to transmit cards commands under APDU format from system to TDA8006. Short or extended commands can be used.
An answer to such a command is also made in APDU format from TDA8006 to the system.

5.6. Negoce

This command is used to make a PTS to the card, if in its ATR the card proposes a different Fi/Di or 2 different protocols. By using this command a PTS will be made to the card with the Fi/Di combination proposed in the ATR. The protocol type may be entered as a parameter.

Example:
System to TDA8006: 60 00 01 10 PP LRC PP is 00_H for T=0 or 01_H for T=1

TDA8006 to System: 60 00 01 10 PP LRC

If the command is acknowledged all the subsequent exchanges between the card and TDA8006 will be made by using the new parameters.

5.7. Set_clock-card

This command is used for changing the card clock frequency. The default value is set to FXTAL/4 which is 3.68625 MHz.
A parameter has to be transmitted in order to chose the card clock frequency:

From System to TDA8006: 60 00 01 11 PAR LRC

Frequency	Parameter
Fxtal/2=7.37MHz	02 H
Fxtal/4=3.68MHz	04 H
Fxtal/8=1.84MHz	06 H

After a card clock frequency change, all the waiting times are internally set to the new value.

If the card has answered in its ATR a Fi parameter of 372 or 558 (fmax ≤ 6MHz) a change of the card clock frequency to Fxtal/2 (7.37MHz) will not be processed and an error status will be sent to the application.

5.8. Card take off and card insertion:

These two commands are directly send to the system processor as soon as a card extraction or insertion has occured.

5.9. Set divider

This command is used mainly for cards which are not fully ISO 7816-3 compliant about specific and negociable mode. In fact some cards are in specific mode but they do not give TA2 parameter in their answer to reset. So the UART has to be set to the right baud rate by the means of this specific command which programs the divider ratio (the prescaler is set to the default value 31).

Example:
System to TDA8006: 60 00 01 0B XX LRC XX is the value of the divider
TDA8006 to System: 60 00 01 0B XX LRC

For an etu of 372 clock cycles XX=0C (372=31x12)
For NDS cards, an etu of 93 clock cycles XX=03 (93=31x3)

5.10. Time out

This command is sent from TDA8006 to the host controller if when during a transmission from the host controller to TDA8006, the time difference between 2 characters exceeds 10ms. This timing is calculated between each character of a frame and starts after the first character and is disabled after the last character of the frame. This feature has been implemented in order to avoid any blocking of the transmission line between the host controller and TDA8006.

Example:
From TDA8006 to System: E0 00 00 FF LRC

6. Information field

The information field that can include up to 512 bytes is composed of APDUs (Application Protocol Data Unit) according to the ISO7816-4 normalization definition. Extended messages are supported up to the data buffer limit (512 bytes).

Different examples are given according to Annex A of the EMV'96 in T = 0.

Case 1 command

TAL (System) TTL (TDA8006)
{60, 00, 04, 00, CLA, INS, P1, P2, LRC} ⇒
4 header bytes ⇐ {60, 00, 02, 00, 90, 00, LRC}

Case 2 command

Le = Licc or ≥ Licc
TAL TTL
{60, 00, 05, 00, CLA, INS, P1, P2, 00, LRC} ⇒

4 header bytes ⇐ {60, Licc+2, 00, [Data (Licc)], 90, 00, LRC}
2 bytes

Case 3 command

TAL TTL

{60, Lc+5, 00, CLA, INS, P1, P2, Lc, [data Lc], LRC} ⇒

4 header bytes ⇐ {60, 00, 02, 00, 90, 00, LRC}

Case 4 command

TAL TTL

Lc ≥ Licc

{60, Lc+5+1, 00, CLA, INS, P1, P2, Lc, [data Lc], 00, LRC} ⇒

4 header bytes ⇐ {60, Licc+2, 00, [data Licc], 90, 00, LRC}

Case 2 command using the 61 and 6C procedure byte

Le = Licc or Le ≥ Licc

TAL TTL

{60, 00, 05, 00, CLA, P1, P2, 00, LRC} ⇒

⇐{60, D1+D2+Dn+2, 00, [data D1+D2+Dn], 90, 00, LRC}

Other possible procedure

TAL TTL

{00 00 05 00 CLA P1 P2 00 LRC} ⇒

⇐ {40,D1,00, [data D1], LRC}
⇐ {40,D2,00, [data D2], LRC}
⇐ {40,D3,00, [data D3], LRC}
⇐ {20,Dn+2,00, [data Dn], 90, 00, LRC}

7. Hardware implementation

7.1. Introduction

A reference board (BskyB2.1) has been built with a specific Amphenol card reader (reference C702 10M008 2594) and a TDA8006AH/C113 (QFP44 package).
The electrical diagram is given on figure 1 and the layout diagram is given on annex 1.

7.2. Electrical diagram

The electrical diagram is presented on the next page.
The specific Amphenol card reader is able to handle cards up and down on the first slot. Mondex™ cards will be inserted with the card contacts face up and the analog BskyB cards will be inserted with the card contacts face down.

In order to meet the Mondex™ requirements (VCC shall not go over 7V in any case), it is advised to place a zener diode (Vz=6.8V) on the supply voltage, so that it will never be supplied over 7V. In this case we can fully garanty that the supply voltage on VCC will never be over VUP (6.5V max) in any case. If the supply section of the set top box is safely protected, this zener diode can be removed.

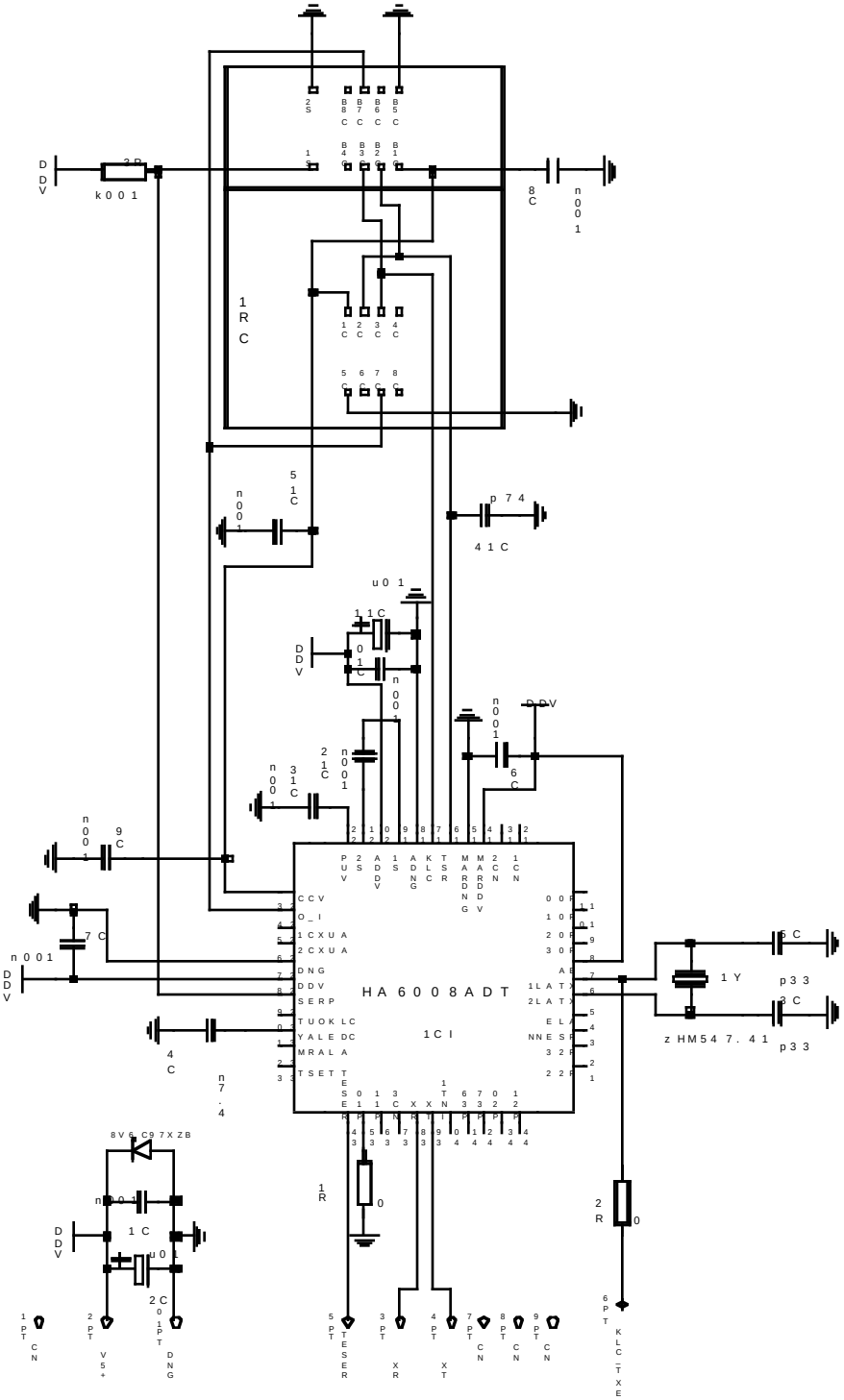
The resistor (R1) on P10 pin is optionnal; it is only needed to achieve 9600 bauds on the Rx,Tx lines.
The crystal oscillator can also be removed if a frequency of 14.7456MHz is already available in the set top box. For this the strap resistor R2 shall be placed on the printed circuit board.

The capacitors C12 (between S1 and S2) and C13 (tied to Vup) shall be placed as closed as possible to the TDA8006 pins as well as the discoupling capacitors (C10 and C11) between VDDA and GNDA.

Two 100nF capacitors shall be placed on the VCC line; one (C9) close to the VCC pin of TDA8006, the other (C15) as close as possible of the C1 contact of the

card reader. A third capacitor (C8) has been added on the VCC line in order to have a better discoupling for the contact C1B of the card reader for the analog BskyB cards.
A 47pF capacitor C14 is necessary on the RST line to filter some pollution due to CLK line.

TDA8006AH/C113
Application Note
application for Mondex cards in BskyB STB
AN98006



The VPP pin has been left open for the Mondex™ card and connected to VCC for the BskyB analog card.

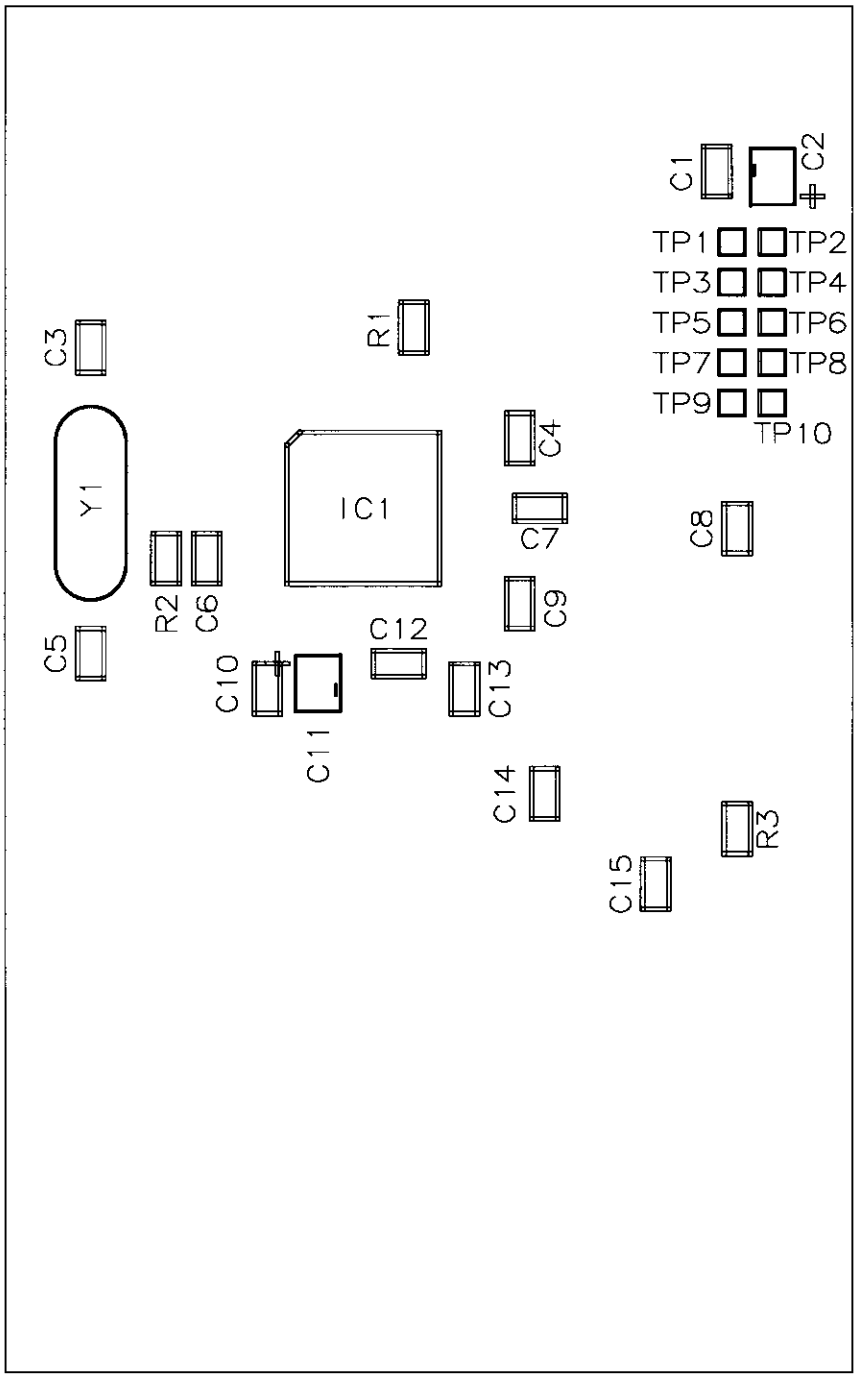
It is advised to isolate as much as possible with ground lines the tracks carrying the card signals (VCC, RST , I/O, CLK).

7.3. Layout

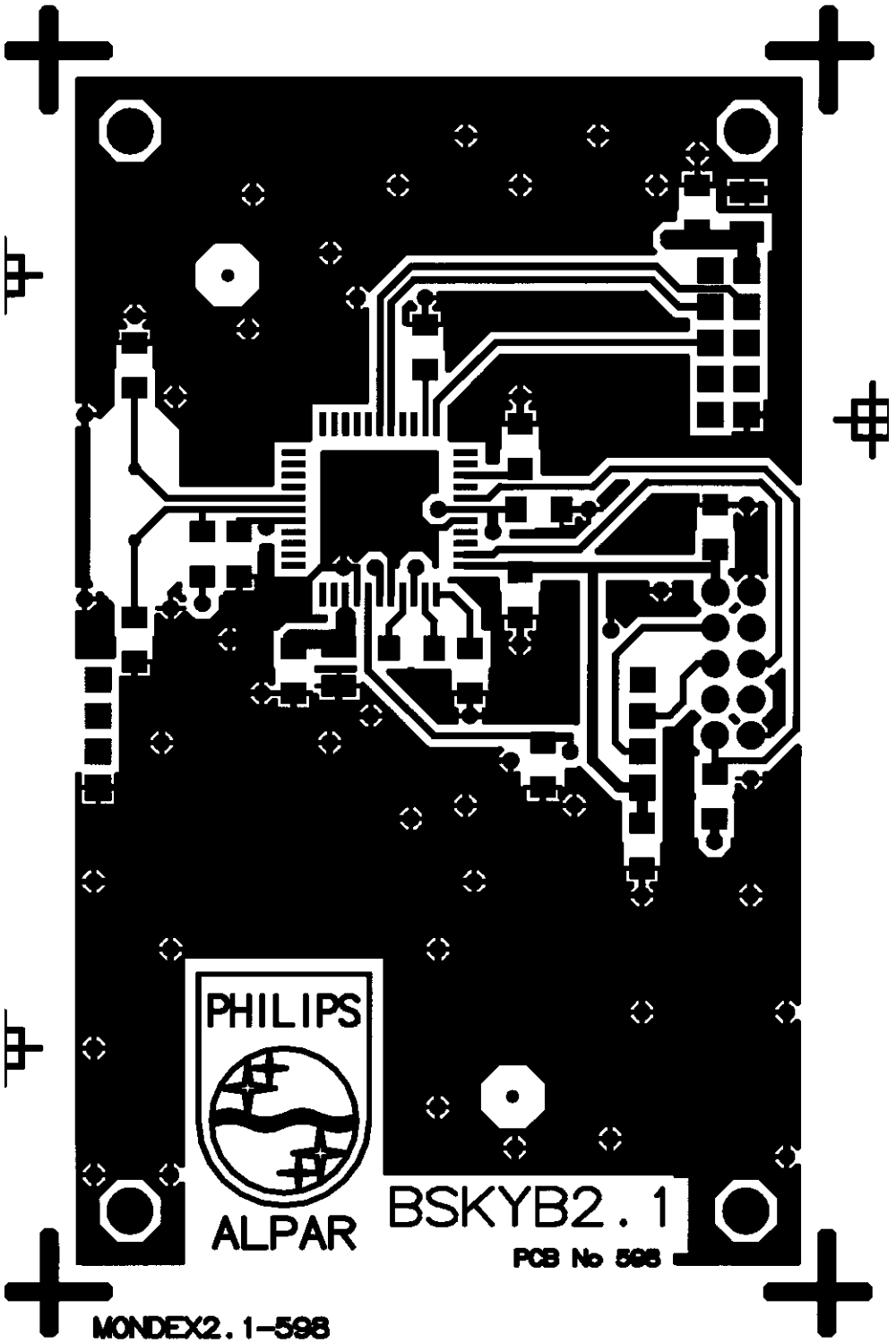
The layout which is presented does not include a zener diode for protection.

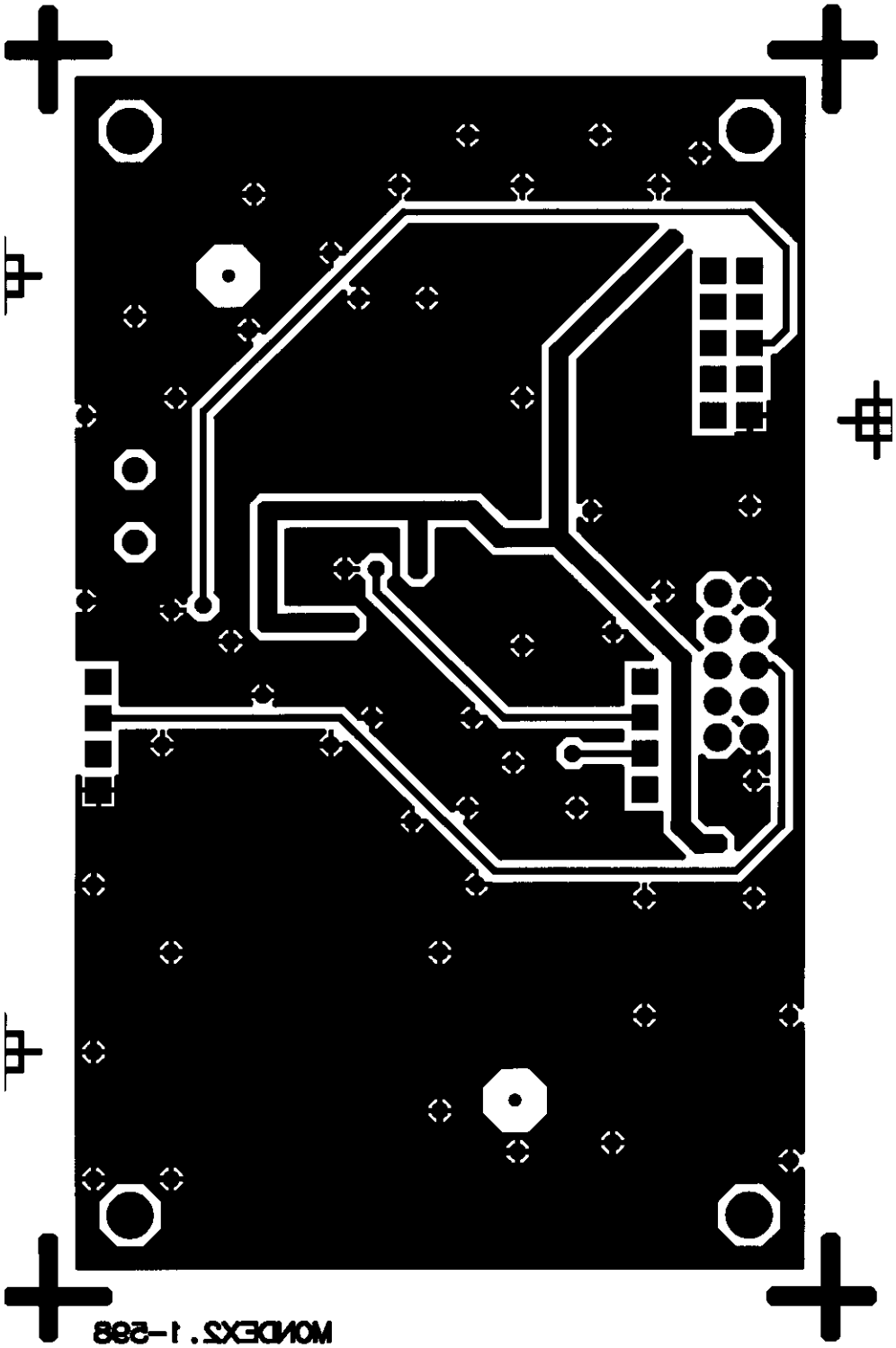
All the components are SMDs and are placed on the upper side of the board.
Some vias (metallized holes) have been placed between the two ground layers in order to improve the EMC behaviour.

The following pages are giving the component placement on the upper side of the board, the aspect of the upper side and the aspect of the lower side of the printed circuit board.



MONDEX2.1–598
COMPOSANTS FACE SUPERIEURE


PHILIPS
ALPAR
BSKYB2.1
PCB No 598
MONDEX2.1-598
VUE FACE SUPERIEURE


MONDEX2.1-SB8
VUE FACE INFERIEURE