301 8428
301 8430

Burall InfoSys Limited

CONTACT SMART CARD READER

HARDWARE DESCRIPTION AND

COMMUNICATION PROTOCOL SPECIFICATION

Applicable Products: BIS1601 - Voyager

Release 1.00 Issue Date 28th July 1999

BIS1601 CONTACT READER MODULE

The BIS1601 is a contact smart card reader/writer module.

The standard BIS1601 will function with two types of card, namely the ST14C02 and the SLE4442. Both devices offer 256 bytes of data storage, the ST14C02 is an unprotected device and the SLE4442 is a password protected device.

The module operates from a single 5 Volt supply at 20mA.

The module has one red LED, one green LED and a buzzer to allow user feedback.

The reader module also has a Random Access Memory (RAM) buffer, which allows a mirror image of the card to be maintained, this allows multiple card programming and card copying at high speed.

The command set for interfacing to a host system is a simple ASCII based command set.

The module supports RS 232 and TTL 232 communications at a baud rate of 9600, no parity, 8 bit, 1 stop bit format.

The module uses a high quality landed contact reader with short circuit detection.

The module has a 256 byte EEPROM fitted on the board for communication parameters and user data.

Hardware Connection

The following describes the connection to the circuit board for 232 operation.

All connections may be made via the 10 way IDC ribbon cable header PL1.

Both RS232 and TTL232 are supported.

Pin 1 - Txd	TTL 232 Transmit
Pin 2 - Rx	RS 232 Receive *see note
Pin 3 - Tx	RS 232 Transmit
Pin 4 - Rxd	TTL 232 receive *see note
Pin 5 - Gnd	Ground
Pin 6 - Gnd	Ground
Pin 7 - Vdd	+5 volts
Pin 8 - IRQ0	
Pin 9 - DTR	
Pin 10 - DSR	

Note:- To use TTL communications, Jumper marked **TTL/RS** must be **removed**, It must be **fitted** for RS232 communications to function.

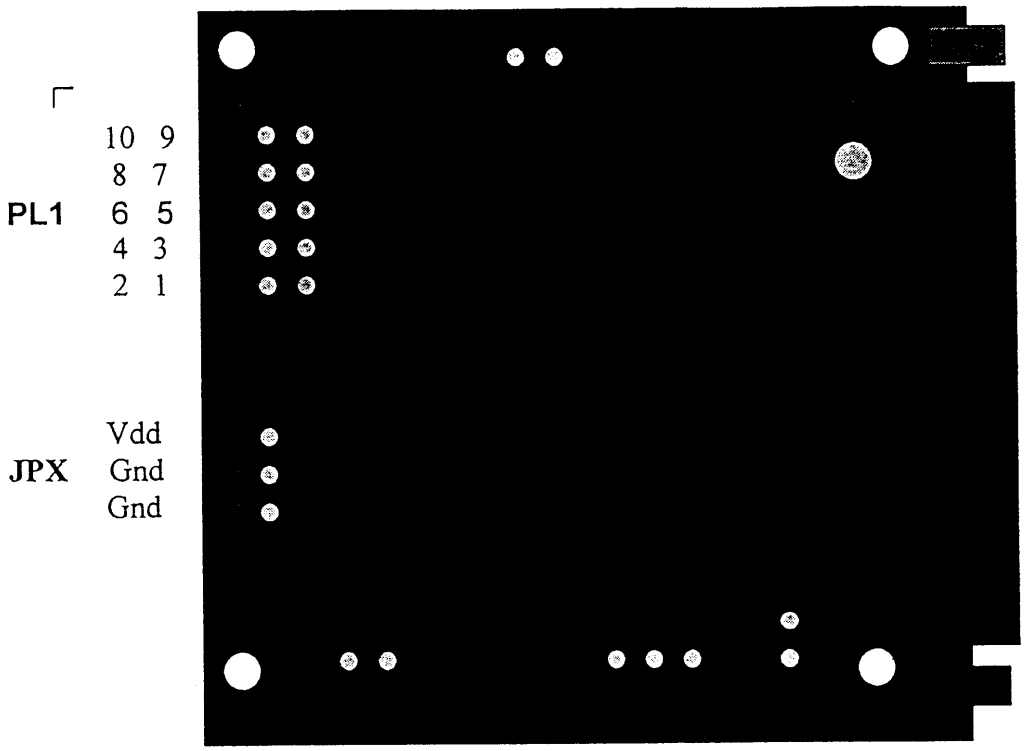
Note:- The jumpers marked **JP1** and **RS Lnk** must be fitted to the board to function correctly. **No** jumper should be fitted to **J10**

ALTERNATE POWER

The board may also be powered to **JPX**
The board requires 5 Volts DC. This should be connected as follows:-

Pin 1 - Vdd	+5 Volts
Pin 2 - Gnd	Ground
Pin 3 - Gnd	Ground

RS/TTL



COMMUNICATION PROTOCOL COMMANDS

Communications between the host system and the reader is initiated by a command sent from the host to the reader. When receiving the command, the reader carries out the task assigned to it. After having performed the task the reader sends a response to the host. The host should not send another command until a response has been received, as the reader ignores communications whilst carrying out internal processing with the card.

The frames for commands and responses are always of the same format. The command begins with an ASCII character indicating the command type, followed by the relevant data for that command.

The response mirrors the host command by returning the ASCII command code followed by two ASCII characters this is then followed by any data relevant to the executed command.

If an error occurs then an error character '!' will be returned along with two ASCII characters, which indicates the error type. This error code informs the host of any errors in the execution of the given command by the reader.

Error Codes. All Error codes are preceded by a return of the '!' character. The following is a list of error codes.

20 **Length error**
The expected length of the received command string is incorrect.

21 **Incorrect Password**
The password supplied did not match the cards password. **Note** after three incorrect attempts the card will be permanently locked.

22 **Card short circuit**
A short circuit on the contact mechanism was detected.

23 **No card present**
There is no card currently in the mechanism.

24 **Block error**
The current supported cards will not generate this error

25 **Syntax error**
An error in the structure of the command was received.

26 **Bad block checksum**
The internal RAM buffer has been corrupted.

27 **Card write error**
An error occurred while writing to a card.

28 **No such command**
The command sent does not exist.

29 **Card deactivated**
An error has deactivated the card, re-insert the card to reset the module.

2A **Verify error**
After writing a byte the verification of that byte failed.

2B **EEPROM not functioning**
After writing a byte to the Eeprom the verification of that byte failed.

2C **Password not required**
The card currently in the module does not require a password.

2D **Card locked**
The card currently in the module is locked and will no longer function.

30 **Card read error**
Card reading error.

NOTES:- For ALL Following Communication Protocol definitions

All command codes from the host are accepted in **UPPER CASE ONLY**. The command code in the data response is always upper case.

A carriage return character <CR> terminates all messages
This character is **0Dh,** decimal value 13.

Both supported cards are 256 byte EEPROM based devices, hence they have a memory space starting at location **00h** (0 decimal) and finishing at **0FFh** (256 decimal).

A single Data byte is transmitted as two ASCII characters, for example, a hexadecimal byte with a hex value of **45h** would be split into an **ASCII 4** and an **ASCII 5**, hence the values **34h** and **35h** would be transmitted.

Spaces and brackets are shown only to aid readability, these characters are **Not** to be sent to the reader module.

ST is a 2 digit status number, this is used as a diagnostic number, and this may be ignored.

Error messages are returned as ! (ER) - exclamation mark followed by the 2 digit error number.

QUERY STATUS

This command allows the user to interrogate the BIS1601 module as to the current status of that module. There are four queries that can be requested.

Query Smart Card

Allows the host to request the status of the card inserted into the reader. There are three possible data responses.

Data from host - **Q S <CR>**
Data response - **Q ST Data <CR>**

Data is a variable length string which has one of the three following formats:-

I2C	indicates that a ST14C02 card present
SLE A2131091	indicates that a SLE4442 card present
*	Indicates that no card is present

Note:- the 8 digit number following the SLE is the cards ATR (Answer to Reset).

Query Hardware

Allows the host to request the status of the module hardware.

Data from host - **Q H <CR>**
Data response - **Q ST Data <CR>**

Data is a 2 digit number, the respective bit positions have the following meanings.

	ABV	Description	Binary	Meaning
MSbit	Unused		0	None
	DSR	DSR Present	0 1	No Yes
	SCSH	Smart card short circuit	0 1	No Yes
	SCP	Smart card present	0 1	No Yes
	Vdd	Vdd level	0 1	3 Volts 5 Volts
	E2	Eeprom fitted	0 1	No Yes
	RAM	Expansion RAM fitted	0 1	No Yes
LSbit	PROC	Processor type	0 1	Mask Flash

Query Communications

Allows the host to request the status of the modules current communications configuration.

Data from host - **Q C <CR>**
Data response - **Q ST Data <CR>**

The format of **Data** is **BBTTSSXXPP.**
The following table shows the meaning of the returned data string.

Baud Rate **BB**	Data Bits **TT**	Stop Bits **SS**	Parity **PP**
30 = 1200	37 = 7	31 = 1	30 = None
31 = 2400	38 = 8	32 = 2	31 = Odd
32 = 4800			32 = Even
33 = 9600			
34 = 19200			

XX is not used and may be ignored.

The default communications protocol is 9600,n,8,1 (9600, no parity, 8 bit, 1 stop bit).

If a problem is experienced with the communications, then insert a card before powering up the module, then on power up, the module will default to 9600,n,8,1.

Note:- On power up the module outputs the following message
'Burall Infosys Contact Reader V1.0 July 1999'

Query Version

Allows the host to request the status of the modules current software version number.

Data from host - **Q V <CR>**
Data response - **Q ST Data <CR>**

Data is in the format **xxxxx:vv:rr**

Xxxxx is the software number.
Vv is the version number.
Rr is the revision number.

READ DATA FROM SMART CARD

Reads data from the smart card and sends it to the host. The data is **NOT** stored in the RAM buffer.

Data from host - **R AD LN <CR>**
Data response - **R ST DATA..... <CR>**

AD is the start address within the card, 2 ASCII characters, legal values must range from **00h to FFh.**

LN is the length of data to read, 2 ASCII characters.

DATA.... Is the returned data, 2 ASCII characters per byte.

Note:- The maximum value of **LN**, the read length is **80h**, if a length greater than 80h is requested, the module will force the length to the maximum length of 80h, this is also true if 00h is used.

Note:- If a start location is specified with a length that passes location 0FFh, the module will wrap-around to location 00h and continue to return data from this location.

PASSWORD CONTROL

These functions are only applicable if using a SLE4442, the function will generate an error if it is used with the ST14C02. The 6 digit password must be validated as being correct for the smart card being used, before it is possible to write to any of the locations within the cards memory.

WARNING:- After three failed attempts to validate a password the card will become permanently locked.

Password Validate

This function must be performed correctly before an SLE4442 card can to written to

Data from host - **PV PASSWD <CR>**
Data response - **PV ST A <CR>**

PASSWD is the 6 digit hexadecimal password to be compared to the password within the smart card.

A is the remaining attempts before being permanently locked out. The number of set bits represents the remaining attempts, hence **7** (**0111** in binary) is 3 attempts, **6** (**0110** in binary) is 2 attempts and **4** (**0100** in binary) is 1 attempt.

If a password has been validated as being correct then subsequent attempts at sending a password (including a different password) will be responded to with a **P007**.

A card only requires a password to be re-sent after the card has been reset, removed or deactivated.

Password Read Remaining Attempts

This function allows the user to determine how many remaining attempts are permitted, before using another attempt.

Data from host - **PR <CR>**
Data response - **PR ST AT 6digit <CR>**

AT is the remaining attempts before being permanently locked out. The number of set bits represents the remaining attempts, hence **07** (**00000111** in binary) is 3 attempts, **06** (**00000110** in binary) is 2 attempts and **04** (**00000100** in binary) is 1 attempt and **00** is locked.

6digit is always 000000

Password Write

This function allows the user to change the password, the password validate function must have been successful for this function to operate.

Data from host - **PW PASSWD <CR>**
Data response - **PW ST AT 6digit <CR>**

PASSWD is the new 6 digit password that is being written to the card.

AT is the remaining attempts before being permanently locked out. The number of set bits represents the remaining attempts, hence **07** is 3 attempts, **06** is 2 attempts and **04** is 1 attempt and **00** is locked.

6digit is always 000000

WRITE DATA TO SMART CARD

Writes data from the host to the smart card. The data is **NOT** stored in the RAM buffer.

Data from host - **W AD Data..... <CR>**
Data response - **W ST <CR>**

AD is the start address within the card, 2 ASCII characters, legal values must range from **00h to FFh.**

DATA.... Is the data to be written to the card, 2 ASCII characters per byte.

Note:- The maximum length of Data is **256** characters.

Note:- An error will occur if an odd number of characters are used.

Note:- If a start location is specified with a length that passes location 0FFh, the module will wrap-around to location 00h and continue to write data to this location.

SECURITY LOCK BYTES

This function is only applicable to SLE4442's.

The first 32 bytes within this device have a special function, they can be individually locked by the user. Indeed a number of these bytes are locked at the time of silicon manufacture (for example the ATR and the manufacturers ID). The bytes that are not locked may be used as many times as the user requires, using the standard read and write functions.

Note:- That programming a continuous string in this area that includes a pre-locked byte will cause a verify error.

Security Read

This function allows the user to check the current status and to permantly lock individual bytes within the first section of 32 bytes.

Data from host - **SR <CR>**
Data response - **SR ST 0CFFF81F <CR>**

The returned 8 digits, **0CFFF81F** is an example from a new card.
This number in binary is **0000 1100 1111 1111 1111 1000 0001 1111**
The 32 bits each represent the lock/unlocked status of the first 32 bytes.
A zero in a bit position represents a locked byte and a one represents an unlocked byte.

Security Write

This function allows the user to lock individual bytes within the first section of 32 bytes.

Data from host - **SW AD <CR>**
Data response - **SW ST AD VL <CR>**

The two digit **AD** is the address of the byte the user requires locking, valid range is **00 to 1F**.

The two digit **VL** is the value that was locked into the byte.

HARDWARE MANIPULATION

Allows the host access to the LEDS, Buzzer and Voltage selection.

Data from host LEDs - **O L X <CR>**
Data from host Buzzer - **O B X <CR>**
Data from host Voltage - **O V X <CR>**
Data response - **O ST <CR>**

The ASCII value of **X** is defined in the table below for the corresponding function required for LED's and Buzzer.

For Voltage selection **X** = 0 selects 3 volt, **X** = 1 selects 5 volt.
The default voltage selection on power up is 5 volt.

X	LED 1 (RED)	LED 2 (GREEN)	BUZZER
0	Off	X	Off
1	1 at 1's length	X	1 high bleep
2	2 at 1's length	X	2 high bleeps
3	Continuous 1's	X	3 high bleeps
4	1 at 2's length	X	Continuous high bleeps
5	2 at 2's length	X	1 low bleep
6	Continuous 2's	X	2 low bleeps
7	On	X	3 low bleeps
8	X	Off	Continuous low bleeps
9	X	1 at 1's length	2 tone bleep
A	X	2 at 1's length	2 tone twice
B	X	Continuous 1's	2 tone 3 times
C	X	1 at 2's length	2 tone continuous
D	X	2 at 2's length	Off
E	X	Continuous 2's	High continuous
F	X	On	Low continuous

BLOCK SELECT

This function is for future expansion. It allows access to cards with memory capacities larger than 256 bytes. All references to block select in this document may be ignored as the supported cards only have the one block and the module defaults to block zero.

Data from host - **B X <CR>**
Data response - **B ST <CR>**

X Is the required block number

RAM BUFFER COMMANDS

Download Data

Programs the whole of the 256 bytes of the smart card from the contents of the modules RAM buffer. The contents of the card are then verified against the RAM buffer.

Data from host - **D <CR>**
Data response - **D ST <CR>**

Note:- Exception, the first 32 bytes of the SLE4442 are not verified, as this could cause a verify fail error on pre-locked bytes.

Upload Data

Copies the data from the smart card to the modules RAM buffer. A checksum is generated over this data to maintain its integrity.

Data from host - **U <CR>**
Data response - **U ST <CR>**

Get RAM

Transmits the requested length of the modules RAM buffer to the host.

Data from host - **G AD LN <CR>**
Data response - **G ST DATA..... <CR>**

AD is the start address within the modules RAM buffer, 2 ASCII characters, legal values must range from **00h to FFh.**

LN is the length of data to transmit, 2 ASCII characters.

DATA.... Is the returned data, 2 ASCII characters per byte.

Note:- The maximum value of **LN** is **80h**, if a length greater than 80h is requested, the module will force the length to the maximum length of 80h, this is also true if 00h is used.

Note:- If a start location is specified with a length that passes location 0FFh, the module will wrap-around to location 00h and continue to return data from this location.

Memory Block Fill

Allows the host to fill a section of the modules RAM buffer with a specified value.

Data from host - **M AD LN VL <CR>**
Data response - **M ST <CR>**

AD is the start address within the modules RAM buffer, 2 ASCII characters, legal values must range from **00h to FFh.**

LN is the length of section to fill, 2 ASCII characters.

VL is the value to fill each location with, 2 ASCII characters.

Fill RAM

Allow the host to fill the modules RAM buffer with specified data.

Data from host - **F AD Data..... <CR>**
Data response - **F ST <CR>**

AD is the start address within the modules RAM buffer, 2 ASCII characters, legal values must range from **00h to FFh.**

DATA.... Is the data to be written to the modules RAM buffer, 2 ASCII characters per byte.

Note:- The maximum length of Data is **256** characters.

Note:- An error will occur if an odd number of characters are used.

Note:- If a start location is specified with a length that passes location 0FFh, the module will wrap-around to location 00h and continue to write data to this location.